



Организация  
Объединенных Наций по  
вопросам образования,  
науки и культуры

# Этические аспекты новых технологий. Обзор

Мэри Рандл и Крис Конли  
Geneva Net Dialogue



**IFAP – Программа «Информация для всех»**  
Сектор коммуникации и информации

Комиссия Российской Федерации по делам ЮНЕСКО  
Федеральное агентство по культуре и кинематографии  
Российский комитет Программы ЮНЕСКО «Информация для всех»  
Межрегиональный центр библиотечного сотрудничества  
Российская национальная библиотека

# Этические аспекты НОВЫХ ТЕХНОЛОГИЙ. Обзор

Мэри Рандл и Крис Конли

Geneva Net Dialogue

Москва



Издательство «Права человека»  
2007

УДК 174:004  
ББК 87.75  
Э 90

Координатор издания: Боян Радойков

Перевод с английского: Малявская Е.В.  
Редакторы русского издания: Кузьмин Е.И., Мурована Т.А.,  
Фирсов В.Р.

*Идеи, факты и мнения, высказанные в данной публикации, принадлежат авторам и не всегда совпадают с точкой зрения ЮНЕСКО. За мнение авторов Организация ответственности не несет.*

**Рекомендованный раздел каталога:**

ЮНЕСКО. Программа «Информация для всех».  
Э 90 **«Этические аспекты новых технологий. Обзор»**

Департамент информационного общества, Сектор коммуникации  
и информации (под редакцией Бояна Радойкова) – Париж:  
ЮНЕСКО, 2007.

Опубликовано в 2007 г. Организацией Объединенных Наций  
по вопросам образования, науки и культуры  
Франция, F-75352 Париж 07 SP, Пляс-де-Фонтенуа, 7

Издание на русском языке опубликовано в 2007 г. по инициативе  
Российского комитета Программы ЮНЕСКО «Информация для  
всех» и Межрегионального центра библиотечного сотрудничества  
при финансовой поддержке Федерального агентства по культуре  
и кинематографии. Публикуется с разрешения ЮНЕСКО.

ISBN 978-5-7712-0379-9

Все права защищены  
CI-2007/WS/2-CLD 31112  
© ЮНЕСКО, 2007  
© Межрегиональный центр библиотечного сотрудничества,  
перевод, 2007

## ЭТИЧЕСКИЕ АСПЕКТЫ НОВЫХ ТЕХНОЛОГИЙ. ОБЗОР

Мэри Рандл и Крис Конли\*

### БЛАГОДАРНОСТИ

В ходе подготовки данного отчета своим мнением о ситуации и перспективах ее развития поделились с нами многие выдающиеся представители научных сообществ, связанных с глобальным развитием информационных технологий и инфоэтикой: Hal Abelson, Ben Adida, Ang Peng Hwa, Kader Asmal, Ted Barnett, Stefan Bechtold, Peter Berghammer, Scott Bradner, Stefan Brands, Kim Cameron, Shunling Chen, David Clark, John Clippinger, Urs Gasser, Lauren Gelman, Georg Greve, Dick Hardt, Dewayne Hendricks, Chris Hoofnagle, Hai Huang, Ben Laurie, Ronaldo Lemos, Lawrence Lessig, Jamie Lewis, Abdel-Hamid Mamdouh, Desiree Milosevich, Nicholas Negroponte, Cory Ondrejka, David Reed, Eric Rescorla, Jonathan Robin, Judit Rius Sanjuan, Wendy Seltzer, Lara Srivastava, William Terrill, Paul Trevithick, Jake Wachman, David Weinberger, Ian Wilkes, Jonathan Zittrain.

\* Мэри Рандл – сотрудник Центра Беркмана «Интернет и общество» (Berkman Center for Internet and Society) при Гарвардской юридической школе (Harvard Law School) и внешний сотрудник Центра по вопросам Интернета и общества (Center for Internet and Society) при Стэнфордской юридической школе (Stanford Law School). Крис Конли имеет степень магистра в области вычислительной техники, которая была присвоена ему в Массачусетском технологическом институте (M.I.T.), и в настоящее время является соискателем степени доктора права в Гарвардской юридической школе, где он занимается вопросами взаимодействия закона и технологий. Настоящая работа выпущена под эгидой организации Geneva Net Dialogue (г. Женева) – открытой международной ассоциации, миссия которой заключается в «оказании содействия в деле реализации прав человека в информационном обществе путем установления связей между специалистами в области технологий, политическими деятелями и гражданским обществом на международном уровне».

# Этические аспекты новых технологий. Обзор

Мэри Рандл и Крис Конли

## Содержание

Предисловие	6
Предисловие к русскому изданию	8
Введение	10
Краткий рассказ о новых технологиях	12
Задачи инфоэтики в области нейтральных технологий	16
Этические проблемы новых технологий – конкретные примеры	33
• Семантическая сеть и другие метаданные	33
• Управление цифровой идентичностью	36
• Биометрия	43
• Радиочастотная идентификация (RFID)	47
• Датчики	58
• Геопространственная сеть и технология LBS	63
• Сети с ячеистой структурой	67
• Вычисления на основе Grid-технологий	71
• Новейшие вычислительные технологии	79
• Таблица: Краткий перечень инфоэтических проблем	83
Еще раз к рассказу о новых технологиях	86
Рекомендации	89
<b>ПРИЛОЖЕНИЕ</b>	
Демократическое информационное общество (краткое содержание интервью с Дэвидом П. Ридом)	93

# Предисловие

Соблюдение соответствующих этических принципов имеет огромное значение для построения инклюзивных обществ знаний, а повышение информированности об этических аспектах и принципах – основа сохранения фундаментальных ценностей, таких как свобода, равенство, солидарность, толерантность и общая ответственность. Именно поэтому ЮНЕСКО поощряет разработку и внедрение оптимальных методов и профессиональных этических принципов, регулирующих деятельность специалистов СМИ, производителей информации, провайдеров услуг и пользователей при должном уважении к свободе слова.

Ускоренный темп технологического развития оставляет разного рода уполномоченным лицам, законодателям и другим главным «игрокам» мало времени на прогнозирование и анализ, прежде чем они лицом к лицу встретятся с необходимостью адаптироваться к новому витку изменений. При отсутствии времени на длительные размышления международное сообщество часто стоит перед необходимостью принятия мгновенных политических решений, имеющих серьезные моральные и этические последствия. Нужно найти правильный ответ на такие вопросы, как: «Развивать общедоступную инфраструктуру или пре-

доставить инвесторам приоритет в ее использовании?», «Позволить рынку вынуждать людей взаимодействовать с цифровыми системами или поддерживать традиционный образ жизни?», «Дать технологиям возможность развиваться произвольно или попытаться регулировать их развитие с учетом защиты прав человека?».

«Инфоэтический анализ новых технологий», подготовленный неправительственной организацией Geneva Net Dialogue по просьбе ЮНЕСКО, призван проанализировать этические аспекты коммуникационных и информационных технологий будущего. Помимо этого, этот документ должен привлечь внимание государств-членов и партнеров ЮНЕСКО к растущему значению, экспансии и потенциальному влиянию новейших технологий на базовые права человека. Пожалуй, самый важный вывод, который делают авторы этой работы, заключается в том, что в наши дни все руководящие лица, разработчики, научные сотрудники корпораций и пользователи несут огромную ответственность за технологическое развитие и его влияние на будущую ориентацию обществ знаний.

Мы надеемся, что данное исследование поможет представителям власти, сообществу, производителям и пользователям понять необходимость пристального наблюдения за развитием коммуникационных и информационных технологий и предвидения этических и моральных последствий разрабатываемых технологических решений для прав человека в обществах знаний.

**Абдул Вахид Хан**

Заместитель Генерального  
директора ЮНЕСКО  
по коммуникации  
и информации

# Предисловие к русскому изданию

Из всего спектра влиятельных игроков, участвующих в формировании международной политики, направленной на построение глобального информационного общества, ЮНЕСКО – единственная организация, системно и последовательно изучающая наиболее общие культурные, этические, правовые и социальные аспекты и последствия набирающих силу процессов бурного развития и проникновения ИКТ во все сферы современной жизнедеятельности.

Именно ЮНЕСКО является выразителем взглядов той части мировой научной, культурной и политической элиты, которая считает, что совместные усилия правительств, международных организаций, гражданского общества и частного сектора могут и должны направить стихийное, во многом опасное развитие глобального информационного общества в сторону его гуманизации, преодоления неравенства, в том числе информационного, в сторону большей свободы выражения мнений, обеспечения доступности информации и знаний, сохранения культурного разнообразия и многоязычия на планете.

В ответ на вызовы информационного общества ЮНЕСКО разработала и последовательно продвигает концепцию построения обществ знаний и учредила Межправительственную программу «Информация для всех».

Российский комитет Программы ЮНЕСКО «Информация для всех» – это общественный экспертно-консультативный орган при Комиссии Российской Федерации по делам ЮНЕСКО, основными задачами которого являются:

- продвижение идей Программы ЮНЕСКО «Информация для всех» в России;
- организация и реализация мероприятий, направленных на построение информационного общества для всех;
- выявление, анализ и прогнозирование тенденций развития информационного общества, а также международной и российской практики в этой области.

С 2002 г. Российский комитет осуществляет сбор, систематизацию и анализ (совместно с ведущими российскими библиотеками и их ассоциациями, образовательными учреждениями, научными и информационно-аналитическими центрами) актуальных документов России, ЮНЕСКО, ООН и других международных организаций по гуманитарным вопросам формирования глобального информационного общества в мире и в России. Часть этих материалов, наиболее тесно связанных с проблематикой Программы ЮНЕСКО «Информация для всех», переводится и издается на русском языке в печатном и электронном виде, а затем бесплатно распространяется среди



крупнейших федеральных и региональных библиотек, образовательных учреждений, научных и информационных центров России.

К Всемирному саммиту по информационному обществу ЮНЕСКО, считавшая свое участие в этом необычном двухэтапном форуме в Женеве (2003 г.) и в Тунисе (2005 г.) чрезвычайно ответственным и важным для укрепления престижа и авторитета Организации, подготовила и выпустила серию из десяти книг, посвященных анализу различных сторон формирующегося глобального информационного общества.

В рамках своей постоянной работы по мониторингу, изучению, отбору, переводу на русский язык, изданию, распространению и обсуждению основополагающих материалов ЮНЕСКО по проблематике информационного общества, Российский комитет Программы ЮНЕСКО «Информация для всех» совместно с Российской национальной библиотекой в 2003–2005 гг. издал все эти книги на русском языке. Россия является единственной страной, которая сделала и продолжает делать подобное.

Не менее значимым для понимания позиции ЮНЕСКО, ее взглядов на процессы и проблемы формирования глобального информационного общества является перевод на русский язык и издание в печатном и электронном виде новых материалов Межправительственного совета Программы ЮНЕСКО «Информация для всех», среди которых – отчет о реализации Программы ЮНЕСКО «Информация для всех» за 2004–2005 гг. и брошюра «Про-

грамма ЮНЕСКО «Информация для всех»».

Все эти издания в электронном виде размещаются на сайте Российского комитета <http://www.ifarcom.ru>, представляются и обсуждаются на крупнейших научно-практических конференциях работников библиотек, научных и образовательных учреждений в России и за рубежом.

Обзор «Этические аспекты новых технологий» – новая книга в серии изданий Программы ЮНЕСКО «Информация для всех». Перевод и публикация этого издания на русском языке стали для нас важной задачей в рамках деятельности по одному из приоритетных направлений Программы – развитию более глубокого понимания этических, правовых и социальных последствий использования ИКТ.

Мы надеемся, что продвижение взглядов ЮНЕСКО в этой области будет содействовать широкому обсуждению и более глубокому осмыслению этических последствий использования информационно-коммуникационных технологий и поможет тем, кто принимает решения о развитии и внедрении технологий, реализации стратегии развития информационного общества и вырабатывает соответствующую политику в этой сфере в России и странах СНГ.

**Е.И. Кузьмин**

Председатель Российского комитета Программы ЮНЕСКО «Информация для всех»,  
член Комиссии  
Российской Федерации  
по делам ЮНЕСКО

# Введение

Бурное развитие сети Интернет принесло обществу много пользы, открыв дорогу созданию новых технических средств и дав людям новые способы общения. Однако, как и многие другие технологические новшества, Интернет не лишен недостатков. Так, возникли новые проблемы, связанные с неприкосновенностью частной жизни («прайвеси»), спамом и вирусами. Более того, даже как средство коммуникации для всего мира он несет в себе угрозу изоляции людей, не имеющих к нему доступа.

Постоянно появляются новые решения в области информационных и коммуникационных технологий (ИКТ), и, хорошо это или плохо, но изменения, которые они несут, могут сделать общества намного более открытыми, чем это было на первом этапе интернет-революции. Возникла настоятельная необходимость учитывать последствия этих новых технологий и стимулировать использование таких технологий, которые оказывают положительное влияние на общество.

ЮНЕСКО имеет возможность и обязана привлечь внимание междуна-

родного сообщества к этим изменениям, в особенности к их этическим и социальным последствиям, которые названы в настоящем обзоре «инфоэтическими» проблемами. В этом отношении данная работа анализирует некоторые задачи ЮНЕСКО в свете новых технологий, которые приблизят нас к информационному обществу<sup>1</sup>, в частности таких как:

- 1. Семантическая сеть и другие метаданные** – метаданные или данные о данных, которые позволяют провести автоматический анализ больших массивов информации; Семантическая сеть обещает использовать метаданные для создания среды, в которой компьютеры будут работать не как инструменты, а скорее как интеллектуальные агенты.
- 2. Управление цифровой идентичностью и биометрия** – управление цифровой идентичностью позволяет накапливать и автоматически обрабатывать персональные данные; биометрия предоставляет средства, с помощью которых можно идентифицировать каждого человека.

<sup>1</sup> ЮНЕСКО все чаще использует термин «общества знаний», который соответствует плюралистическому обществу будущего, ориентированному как на развитие всего общества в целом, так и каждого человека в отдельности. Однако в нашей работе мы будем использовать термин «информационное общество».

3. **Радиочастотная идентификация (RFID) и датчики** – эти технологии осуществляют мониторинг физического мира, используя коммуникационные технологии для распространения информации о конкретном регионе.
4. **Геопространственная сеть и технология LBS (услуги, основанные на технологии определения местоположения)** – технологии, которые служат для привязки цифровых данных к физическим объектам.
5. **Сети с ячеистой структурой** – сети в разных районах мира, не требующие наличия коммуникационной инфраструктуры. Технология построения сетей с ячеистой структурой может помочь в соединении районов, слабо охваченных сетевыми технологиями.
6. **Вычисления на основе Grid-технологий** – технология, которая может помочь в объединении вычислительной мощи всего мира и ресурсов хранения данных для предоставления необходимого уровня доступа.
7. **Новейшие вычислительные технологии** – вместе с перечисленными выше технологиями представляют собой мощную комбинацию оптических, квантовых вычислений и других новейших технологий, способных сформировать «глобальный мозг».

Поскольку выбор вариантов исполнения и использования таких технологий влечет за собой моральные последствия, эти технологии создают значимые инфозитические проблемы.

В данной работе мы рассмотрим эти проблемы в свете главных задач ЮНЕСКО в сфере инфозитики, в частности:

- (а) соблюдение прав человека и основных свобод в киберпространстве;
- (б) увеличение количества информации, представляющей собой общественное достояние;
- (в) обеспечение разнообразия контента в информационных сетях, а также
- (г) содействие большей доступности информации и средств коммуникации.

Приняв эти задачи как данность, мы используем их в качестве эталона при оценке возможных последствий различных вариантов развития технологий.

Прежде чем перейти к описанию результатов нашего исследования, мы вкратце расскажем о том, как связаны друг с другом перечисленные инфозитические задачи. После этого мы посвятим короткую главу тенденциям технологического развития, в которой дается краткий обзор каждой технологии и освещаются тенденции развития и проблемы. Затем мы подведем итоги нашего инфозитического исследования и вернемся к рассказу о новых технологиях. В заключение мы дадим рекомендации относительно способов решения инфозитических задач в преддверии появления новейших технологий.

# Краткий рассказ О НОВЫХ ТЕХНОЛОГИЯХ

За короткую историю информационного общества технологии перешли от «осмысления» киберпространства к «осмыслению» физического мира, и новые способы коммуникации обещают, что каждая область земного шара будет иметь равный и непрерывный доступ к Интернету.

В первой фазе развития Интернета люди начали обмениваться текстами, изображениями и другой информацией. С учетом огромного объема накопленной информации и созданных кодов компьютерам нужны для навигации уже взаимодействующие друг с другом метаданные, или данные о данных. **Семантическая сеть** должна предоставить такие метаданные. Этот новый язык метаданных позволяет предсказать устойчивый рост объема обмена информацией в киберпространстве. При этом лексикон метаданных сделает работу человека в Интернете более точной и эффективной или даже позволит компьютерам получать прямой доступ к контенту и анализировать его.

Поскольку действующими лицами на первой фазе развития Интернета были люди (и они же должны оставаться в центре внимания при всех по-

следующих нововведениях), имеет смысл предоставить компьютерам подробный набор терминов, который облегчил бы им обмен информацией от имени конкретного человека. Иными словами, поскольку навигацию в Сети осуществляют программы (когда веб-агенты опрашивают разные веб-сайты в поиске ответа на определенный заданный человеком вопрос), человек должен иметь возможность делегировать свою идентичность программе, с тем чтобы она думала и действовала от его имени – например, вела переговоры об аренде машины выбранной им модели, определяла, кто из его друзей может иметь доступ к его рабочему календарю, или платила налоги при онлайнowych сделках. Именно поэтому разрабатываются досье, которые содержат данные о различных элементах цифровой личности (имя, дату рождения, гражданство и т.п. для одного человека; псевдоним, любимые мелодии и т.п. – для другого). В этом случае метаданные выступают в качестве языка описания **цифровой идентичности**.

До сегодняшнего дня цифровая идентичность была, как правило, отделена от физической. Однако новая технология – **биометрия** – обе-

щает соединить их, связав различные элементы цифровой идентичности человека с его физическим воплощением. Физическое воплощение можно представить в цифровом виде посредством перевода «в цифру» уникальных атрибутов человека – отпечатков пальцев, радужной оболочки глаза или походки. Эти атрибуты становятся контрольными параметрами, когда биометрические данные переводятся в цифровые выражения, к которым компьютер может обращаться на своем машиночитаемом языке. Таким образом, физическая сущность человека может быть уникальным образом идентифицирована и затем представлена в виде данных.

Точно также **радиочастотная идентификация (RFID) и датчики** делают другие аспекты физического мира доступными для поиска и оперирования в мире цифровом. Метки RFID позволяют отслеживать физические объекты или людей с помощью недорогих цифровых технологий: человека с RFID-чипом легко идентифицировать для различных целей – к примеру, это не позволит врачам перепутать новорожденных в роддоме или обеспечит доступ в секретные помещения здания строго определенным людям. Подобным же образом можно отслеживать

путь какого-либо изделия (скажем, флакона шампуня) от конвейера до магазина, где он будет продан, и даже ассоциировать его с конкретным покупателем. Эту информацию можно использовать для разных целей – от повышения эффективности каналов поставок до отзыва бракованных изделий.

Кто-то скажет, что язык метаданных чисто лингвистически приравнивает человека к флакону шампуня. На это специалист по компьютерам ответит, что данная проблема решается, т.к. языки метаданных совершенствуются – они могут включать дополнительные параметры, описывающие и ценность объекта, и его атрибуты<sup>2</sup>.

Определенные признаки позволяют говорить о том, что процесс такого совершенствования уже начался, и отчасти он стимулирован взаимопроникновением физического мира и киберпространства. **Датчики** позволяют производить дальнейшую оцифровку физического мира – путем измерения определенных параметров, таких как уровень кислорода или ускорение, и последующего перевода их в цифровую форму. С приходом нового материала в киберпространство скелет чисто научной теории обрас-

---

<sup>2</sup> Эти вопросы касаются проблемы технологического нейтралитета, т.е. вопроса о том, могут ли технологии быть нейтральными, или они должны быть загружены ценностями. Ценности могут быть приданы им в ходе разработки языка, и кто-то должен или что-то должно выбирать, как определять элементы – например, решить, будут ли человек и предмет отнесены к одной категории, и как категории будут перекрываться.

тает живой плотью. Различные контексты обогащают Семантическую сеть дополнительными значениями, которые ей предстоит распознать.

Пока киберпространство занято импортированием реального мира, оно само экспортируется в реальное пространство с помощью **геопространственной сети и технологии LBS (услуги на базе технологии для определения местоположения)**. Эти интернет-услуги охватывают сферу реального мира и предлагают основанные на использовании Сети технологии, позволяющие увидеть разные географические точки вместе с соответствующей информацией (например, о ценах на внутреннем рынке, уровне преступности, туристических маршрутах). Граница между «реальным миром» и «киберпространством» уже стала стираться; со временем эти два мира могут стать одним.

Однако информационного общества еще нет. Огромные области мира еще не имеют выхода в Интернет, в особенности это касается развивающихся стран. Несмотря на то, что все эти территории кажутся огромными, на реализацию глобальной связи, скорее всего, много времени не потребуется. Внедрение **сетей с ячеистой структурой**, которые позволяют сетевым устройствам, таким как мобильные телефоны, устанавливать мгновенную прямую связь между абонентами, предлагает способ расширения сетевого ох-

вата, не требующий дорогой инфраструктуры. Развивающиеся возможности мобильных телефонов и других электронных устройств, позволяющие подключаться к Интернету и друг к другу, расширят зону охвата ячеистых сетей и, возможно, сделают использование глобальной сети повсеместным.

Понятно, что сеть, состоящая в основном из устройств, не обладающих большой вычислительной мощностью, ограничена в плане вычислительных ресурсов, хранения данных и предоставления доступа. Эту проблему могут решить **вычисления на основе Grid-технологий**, при которых мощности для обработки и хранения данных объединяются в сети, а люди обращаются к этим ресурсам по мере необходимости и получают их по мере возможности в соответствии с принятой схемой распределения затрат.

Если удастся скомбинировать системы повсеместной сети и Grid-вычислений, информационное общество окажется в среде **повсеместных технологий**, и в этот момент граница между физическим и цифровым мирами станет значительно менее явной. Каждый объект – включая двери, будильники, холодильники и даже наручные часы – сможет дать информацию своему окружению о своем статусе и о себе. Тем временем вычислительные мощности сами по себе могут продолжать свой экспоненциальный рост при поддержке но-

вейших технологий, в числе которых **оптические** или **квантовые вычисления**, очень важные для обработки колоссальных массивов данных. В сочетании с Grid-вычислениями эта сила может составить огромный виртуальный «мозг», который будет и дальше раздвигать границы вычислительных возможностей в расширяющейся Вселенной.

Наш рассказ – о радужном будущем, в котором новейшие технологии используются на благо всего человечества. Однако из истории мы знаем, что технологии можно использовать не только для развития человеческих прав и достоинства, но и для их ограничения. Именно поэтому важно рассматривать эти технологии с позиций их пользы или вреда для реализации инфозитических задач.

# Задачи инфоэтики в области нейтральных технологий

Информационные и коммуникационные технологии (ИКТ) представляют собой все более и более мощную силу современного мира. Их влияние ощущается во всех областях общественной жизни, начиная с бизнеса и образования и заканчивая политикой и международными отношениями. Эти технологии и, в особенности, Интернет также стали доминирующим механизмом для ведения частных дел и участия в общественной жизни. Передовая технология часто используется для облегчения выполнения привычного порядка действий и открывает совершенно новые возможности.

Более того, скорость, с которой развиваются технологии, также растет. Закон Мора<sup>3</sup> гласит, что вычислительная мощность одного микропроцессора растет экспоненциально, и эта истина применима и к другим технологиям. Интернет и связанные с ним технологии открывают дорогу новым идеям и изобретениям, которые распространяются намного быстрее, чем раньше, и стимулируют скорость технического развития.

Однако технология сама по себе нейтральна; она не вносит прямого вклада в развитие прав человека. Многие технологии имеют множество возможных приложений, и некоторые из них могут способствовать осуществлению этой задачи, а другие – мешать.

Именно поэтому стало обязательным анализировать новые технологии с точки зрения их влияния на права человека. Как мы говорили выше, задачи инфоэтики представляют систему для проведения подобного анализа. Первая задача инфоэтики, основанная на Всеобщей декларации прав человека<sup>4</sup>, гласит, что базовым приоритетом является задача постановки технологий на службу защиты прав человека. Из этого берут начало три другие задачи, которые предусматривают продвижение общедоступной информации, разнообразие контента и доступ к информации и средствам коммуникации, – причем все три задачи основаны на предположении, что все люди должны иметь возможность пользоваться благами ИКТ.

<sup>3</sup> См. [http://en.wikipedia.org/wiki/Moore%27s\\_law](http://en.wikipedia.org/wiki/Moore%27s_law) (просмотр 8 ноября 2006 г.).

<sup>4</sup> UN General Assembly Resolution (Резолюция Генеральной Ассамблеи ООН) 217 A (III) от 10 декабря 1948 г.



## Права человека и фундаментальные свободы

Технология может способствовать соблюдению прав человека или ограничивать их. Информационное общество должно стимулировать такое использование новых технологий, при котором их преимущества будут оптимизированы, а их отрицательное влияние сведено к минимуму. Во многих случаях это, скорее, вопрос надзора, чем технологического контроля: должна быть создана такая юридическая или регулятивная система, при которой технология, несущая в себе опасность злоупотреблений, этих злоупотреблений не допускает, а преимущества от данной технологии становятся всеобщим достоянием.

В качестве отправной точки при рассмотрении вопросов прав человека мы взяли Всеобщую декларацию прав человека. Многие из прав, перечисленных в этом документе, имеют особое значение для рассмотрения этических аспектов новых технологий и возможных способов их использования. Для целей нашего исследования перечислим основные положения.

### Статья 2:

**«Каждый человек должен обладать всеми правами и всеми свободами, провозглашенными настоящей Декларацией, без какого бы то ни было различия, как то: в отношении расы, цвета кожи, пола, языка, религии, политических или иных убе-**

**дений, национального или социального происхождения, имущественного, сословного или иного положения.**

**Кроме того, не должно проводиться никакого различия на основе политического, правового или международного статуса страны или территории, к которой человек принадлежит, независимо от того, является ли эта территория независимой, подопечной, самоуправляющейся, или как-либо иначе ограниченной в своем суверенитете».**

ИКТ позволяют осуществлять сбор и анализ информации и, как следствие, допускают мириады классификаций. Персональные данные можно подразделять на такие категории, как этническая принадлежность, пол, религия, национальность, общественно-экономический статус. С позиций инфоэтики важно, чтобы классификация данных по указанным направлениям не нарушала права и свободы человека.

### Статья 3:

**«Каждый человек имеет право на жизнь, на свободу и на личную неприкосновенность».**

Право человека на жизнь, свободу и неприкосновенность – одно из фундаментальных прав, включенных во Всеобщую декларацию прав человека, и при этом оно остается самым сложным для определения. Это право охватывает право досту-

па ко всем необходимым для жизни вещам, включая пищу и кров.

ИКТ способствуют улучшению здоровья человека и даже сохранению его жизни, начиная с технологий очищения воздуха и координированных медицинских исследований и заканчивая ранним оповещением о чрезвычайных ситуациях и быстрым доступом к медицинской информации. Включает ли право на жизнь всеобщий доступ к этим технологическим благам, независимо от платежеспособности?

Кроме того, экономическая эффективность, создаваемая ИКТ, может повысить качество жизни во многих областях мира. Так, экономическое благосостояние, как правило, дает человеку возможность более полно пользоваться правом на жизнь, свободу и неприкосновенность.

Если данная статья может считаться провозглашением права на доступ к информации, идеям, культуре и средствам коммуникации, позволяющим людям принимать участие в жизни общества, то ее можно воспринимать и как разрешение человеку *отказаться* от участия в системах ИКТ. Так, в соответствии с данным правом человеку может быть разрешено отказаться от вживления в свое тело устройства. Если такой имплантат станет де-факто обязательным условием участия человека в информационном обществе, то не следует ли при этом вступить в дело закону и разрешить это-

му человеку доступ ко всем предметам первой необходимости, включая пищу и кров, несмотря на его отказ от имплантанта?

### Статья 7:

**«Все люди равны перед законом и имеют право, без всякого различия, на равную защиту закона. Все люди имеют право на равную защиту от какой бы то ни было дискриминации, нарушающей настоящую Декларацию, и от какого бы то ни было подстрекательства к такой дискриминации».**

Концепция равной защиты может быть поддержана или приостановлена в результате развития ИКТ. Технологии, которые призваны предоставить всем людям равные возможности и доступ, без всякой дискриминации, соответствуют данному положению. Однако технологии можно также использовать для идентификации членов определенных групп и, таким образом, усугублять дискриминацию по отношению к этим группам.

### Статья 11:

**«1. Каждый человек, обвиняемый в совершении преступления, имеет право считаться невиновным до тех пор, пока его виновность не будет установлена законным порядком путем гласного судебного разбирательства, при котором ему обеспечиваются все возможности для защиты.**

**2. Никто не может быть осужден за преступление на основании совершения какого-либо деяния или за бездействие, которые во время их совершения не составляли преступления по национальным законам или по международному праву. Не может также налагаться наказание более тяжкое, нежели то, которое могло быть применено в то время, когда преступление было совершено».**

Данные, получаемые или анализируемые с помощью технологий, все чаще используются в судопроизводстве. Когда факты, полученные в результате применения технологий, противоречат показаниям человека, возникает дилемма – какое свидетельство заслуживает большего доверия. Несмотря на существующую в обществе тенденцию больше доверять фактам, предоставленным машиной, исходя из общей статистической точности, компьютерный код может содержать ошибки или быть намеренно испорченным. Таким образом, в использовании технологий для получения «доказательств» также существует ряд инфоэтических нюансов.

### **Статья 12:**

**«Никто не может подвергаться произвольному вмешательству в его личную и семейную жизнь, произвольным посягательствам на неприкосновенность его жилища, тайну его корреспонденции или на его честь и репутацию. Каждый человек**

**имеет право на защиту закона от такого вмешательства или таких посягательств».**

ИКТ могут служить делу защиты или ограничения права человека на неприкосновенность его личной и семейной жизни (прайвеси). Например, технологии шифрования могут сделать коммуникацию между частными лицами конфиденциальной или могут быть модифицированы таким образом, чтобы заинтересованные лица (например, со стороны правительства) перехватывали эту коммуникацию. Точно так же технологии наблюдения могут охранять частную жизнь, а могут использоваться для нарушения этого принципа.

ИКТ могут предоставлять анонимность, позволяя людям чувствовать себя в безопасности при обмене идеями, которые они никогда бы не озвучили, если бы их имена ассоциировались с этими идеями. В этом смысле прайвеси и анонимность в коммуникации тесно связаны с правом на поиск, получение и распространение информации (статья 19), а также с правом на собрания и объединение в союзы (статья 20).

Однако попытки защитить прайвеси могут заставить общество пойти на дополнительные расходы, а усилия по защите других прав могут иметь последствия для прайвеси. Так, любая защита, предоставляемая технологией для анонимной, безопасной коммуникации, может снизить

эффективность защиты от атак на «честь и достоинство» человека.

Проблемы защиты прайвеси вызваны также ростом объема персональной информации, собираемой частными и государственными организациями. Вопрос, вызывающий к себе все большее внимание, касается обязательств частных компаний по охране персональных данных потребителей, в особенности в глобальном интернет-контексте. Другие вопросы касаются того, как обращаются государственные организации с персональной информацией, в частности, какие правила существуют для государственных организаций, обменивающихся подобной информацией<sup>5</sup>.

Понятно, что есть вопросы относительно того, что считать «произвольным» и «вмешательством». Если политика применяется повсеместно и основывается на достаточно разумных аргументах, то может ли она считаться «произвольной»? Если наблюдение не доставляет никаких неудобств, следует ли считать его «вмешательством»?<sup>6</sup>

### Статья 18:

**«Каждый человек имеет право на свободу мысли, совести и религии; это включает свободу менять свою религию или убеждения и свободу**

**исповедовать свою религию или убеждения как единолично, так и сообщая с другими, публичным или частным образом в учении, богослужении и выполнении религиозных и ритуальных порядков».**

ИКТ, мысль, совесть и религия могут взаимодействовать самыми разными способами. Первый и самый простой – это когда ИКТ используют в религиозных интересах и для облегчения общения по темам, связанным с верой. Если же использование технологий будет противоречить религиозным верованиям, то тогда соблюдение этих верований может быть поставлено под угрозу, при условии, что использование технологий станет обязательным или практически необходимым для функционирования в современном мире.

### Статья 19:

**«Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».**

Как и в случае с правом человека на прайвеси, право на свободу мнения и слова в информационном об-

---

<sup>5</sup> США и Евросоюз ведут горячие дебаты относительно раскрытия и использования информации об авиапассажирах. См. «Air Security Talks Fail» («Провал переговоров по вопросам воздушной безопасности»), Daily Mail, 2 октября, 2006, стр. 32.

<sup>6</sup> См. Lawrence Lessig, Code and Other Laws of Cyberspace (Кодекс и другие законы киберпространства), New York: Basic Books, 1999, раздел 11: «Личная жизнь».

ществе тесно связано с ИКТ. Технологии способны открывать каналы, по которым можно обмениваться информацией и выражать свои убеждения; однако их также можно использовать для ограничения имеющейся информации<sup>7</sup>, выявления и

вмешательства в жизнь людей, выражающих альтернативные взгляды<sup>8</sup>. В этом смысле данная проблема перекликается с темой прайвеси (статья 12) и правом на поиск, получение и распространение информации.

### Анонимность выражения мнения

*Венди Зельцер<sup>9</sup>*

Анонимность имеет давнюю и богатую историю. Вольтер и Джордж Элиот писали под псевдонимами. Поддержка ратификации Конституции США была обеспечена анонимными статьями в федералистских газетах. Современные блоггеры и составители списков рассылки могут не использовать такой же цветистый язык и элегантные псевдонимы, как их предшественники, но их право на свободу слова не менее важно. Технологии, которыми они пользуются, могут способствовать как идентификации, так и анонимности – и это отразится на объеме и содержании выражения мнения в режиме онлайн.

Анонимность может дать дорогу или усовершенствовать многие виды деятельности, связанные с выражением мнения. Свобода передавать информацию включает право на анонимное выражение мнения; свобода собраний включает право образовывать союзы, не раскрывая имен членов группы; свобода искать и получать информацию включает право слушать, смотреть и читать в частном порядке.

Защита анонимности жизненно необходима для демократического дискурса. Возможность скрыть свою личность, предоставленная диссидентам, позволяет им выражать взгляды меньшинства, критически важные для информированного демократического дискурса. В противном случае страх того, что личность может быть раскрыта и что человек может подвергнуться преследованиям за свои высказывания, может заставить его отказаться от высказываний вообще в политических, этнических, религиозных или других миноритарных группах. В свою очередь, такое молчание лишает все сообщество доступа к мнению этого человека.

<sup>7</sup> Например, в настоящее время многие страны используют программы-фильтры для ограничения информации, доступ к которой граждане могут получить через Интернет. См. <http://www.opennetinitiative.org/>.

<sup>8</sup> См. [http://www.rsf.org/article.php3?id\\_article=16402](http://www.rsf.org/article.php3?id_article=16402) (описание судебного заседания по делу диссидентов на основе информации, представленной на Yahoo!).

<sup>9</sup> Венди Зельцер – приглашенный доцент права в Бруклинской юридической школе (Brooklyn Law School) и сотрудник Центра Беркмана «Интернет и общество» (Berkman Center for Internet and Society) при Гарвардской юридической школе (Harvard Law School).

Более того, право на свободу убеждений и их выражение теряет свое значение без возможности сообщать о своих убеждениях другим. ИКТ можно использовать для создания общественного форума, на котором будет происходить подобное общение, или для ограничения выражения убеждений путем установки фильтров на возможность человека общаться с другими людьми. Таким образом, право на поиск, получение и распространение информации тесно связано со свободой собраний и объединения в союзы (статья 20), поскольку доступ к идеям и их распространение предполагают общение с другими людьми в информационном обществе.

### **Статья 20:**

- «1. Каждый человек имеет право на свободу мирных собраний и ассоциаций.**
- 2. Никто не может быть принужден вступать в какую-либо ассоциацию».**

Право на вступление в ассоциации по-разному связано с ИКТ. Технологии могут стимулировать применение данного права, предоставляя средства, облегчающие установление контактов, координируя обмен и взаимодействие с другими людьми в ассоциации. Однако технологии могут также затруднять применение данного права, если они будут использованы для выявления и раскрытия членов ассоциаций или для препятствования проведению мирных собраний.

Технология также представляет угрозу для права воздерживаться от участия в ассоциациях. Это «право на одиночество» в немалой степени зависит от выбора индивида не взаимодействовать с другими людьми. Технологии могут нарушать это право, требуя от человека общаться с другими для получения всех преимуществ, доступных членам общества. Они также могут способствовать идентификации и общественному осуждению тех, кто решает не вступать в какую-либо ассоциацию.

Как замечено выше, право на личную и семейную жизнь (прайвеси) (статья 12) и право на поиск, получение и распространение информации (статья 19) связаны с данным пакетом прав – и технологии только усиливают эту связь.

### **Статья 21:**

- «1. Каждый человек имеет право принимать участие в управлении своей страной непосредственно или через свободно избранных представителей.**
- 2. Каждый человек имеет право равного доступа к государственной службе в своей стране.**
- 3. Воля народа должна быть основой власти правительства; эта воля должна находить себе выражение в периодических и нефальсифицированных выборах, которые должны проводиться при всеобщем и равном избирательном праве, путем тайного голосования или же посредством**

**других равнозначных форм, обеспечивающих свободу голосования».**

Демократические выборы, как и многие другие атрибуты современной жизни, все больше начинают зависеть от технологий. Политические кандидаты полагаются на СМИ и коммуникационные сети для выражения своих взглядов и координации действий своих сторонников. В этом кандидаты далеко не одиноки; политически активные группы также все шире используют Интернет для получения поддержки населения по своим предложениям и для создания своего электората.

Использование ИКТ в политических целях может быть вредно, если технологии будут незаконно использоваться для продвижения политического кандидата или его программы<sup>10</sup>. Более того, рост присутствия технологий в политике может стать барьером на пути групп людей, которых удается эффективно отстранить от политической активности, если эти люди лишены полноценного доступа к ИКТ. Наконец, поскольку электронное голосование стало методом проведения выборов, защищенность его результатов от подделки все больше зависит от специалистов в этой области.

## **Статья 26:**

- «1. Каждый человек имеет право на образование. Образование должно быть бесплатным по меньшей мере в том, что касается начального и общего образования. Начальное образование должно быть обязательным. Техническое и профессиональное образование должно быть общедоступным, и высшее образование должно быть одинаково доступным для всех на основе способностей каждого.**
- 2. Образование должно быть направлено на полное развитие человеческой личности и на увеличение уважения к правам человека и основным свободам. Образование должно содействовать взаимопониманию, терпимости и дружбе между всеми народами, расовыми и религиозными группами и должно содействовать деятельности Организации Объединенных Наций по поддержанию мира.**
- 3. Родители имеют право приоритета в выборе вида образования для своих малолетних детей».**

Образование начинает зависеть от технологий по двум причинам: во-первых, наблюдается рост значимости и ценности технического образования по мере превращения технологий в важный элемент бизнеса, и, следовательно, оно начинает

<sup>10</sup> Например, штатные сотрудники некоторых депутатов Конгресса США вносили изменения в онлайн-овые записи в энциклопедии, касающиеся их работодателя, и иногда стирали данные, показывающие Сенатора или Представителя в невыгодном свете. См. <http://news.bbc.co.uk/2/hi/technology/4695376>.

рассматриваться как целесообразный путь для развития карьеры многими студентами. Во-вторых, технология используется для обучения широкому спектру предметов, открывая студентам доступ к внешним источникам информации, мультимедийным образовательным материалам и новым возможностям взаимодействия с преподавателями и сокурсниками.

По этим причинам единственной большой угрозой, которую представляют собой ИКТ для права на образование, является возможность использования ИКТ как средства расслоения населения по уровню доходов и доступу к технологиям. Поскольку ИКТ становятся ключевым компонентом в системе образования, ученики, не имеющие возможности получить доступ к технологиям, лишаются значительной доли ресурсов; более того, качество нетехнических образовательных ресурсов может падать в связи с тем, что все больше внимания отдается онлайн-обучению. Поддержка программ, призванных предотвратить этот негативный результат, должна стать главной заботой правительств и специалистов по инфоэтике<sup>11</sup>.

Наконец, технологии могут влиять на способность родителей выбирать образование своим детям. ИКТ предоставляют широкий выбор вариантов, вплоть до индивидуальных про-

грамм, которые составляются школой и родителями. Также и наоборот: простота доступа, которую предоставляют технологии, может помешать родителям фильтровать поток информации, доступной их детям в рамках программ обучения.

### Статья 27:

- «1. Каждый человек имеет право свободно участвовать в культурной жизни общества, наслаждаться искусством, участвовать в научном прогрессе и пользоваться его благами.**
- 2. Каждый человек имеет право на защиту его моральных и материальных интересов, являющихся результатом научных, литературных или художественных трудов, автором которых он является».**

Пожалуй, самым главным обещанием ИКТ является концепция действительно общей информационной территории – среды, позволяющей очень быстро находить и распространять новые идеи. В то же время технология может стать барьером на пути распространения новых идей. Так, если идеи представлены только на одном специфическом носителе, это может ограничить права тех, кто не имеет доступа к данной технологии. Более того, даже те, кто имеет доступ к Интернету и другим формам ИКТ, могут быть техническими средствами отстранены от полноценного участия в культурной

---

<sup>11</sup> Двумя такими программами являются: «One Laptop for Child» в М.И.Т. (см. текстовую врезку ниже и <http://laptop.media.mit.edu/>) и «Global Education and Learning Community» (см. <http://www.sun.com/products-n-solutions/edu/gelc/>).



жизни – например, в случае, когда технологии применяются для ограничения пользования данными.

Технологии также ставят под угрозу существующий режим интеллектуальной собственности и, как результат, защиту интересов правообладателей. Файлообменные сети и другие возможности, ставшие доступными благодаря новым технологиям, сильно повысили вероятность нарушения авторского права и затруднили предотвращение подобных действий, а также их преследование в судебном порядке.

Чтобы сделать полноценную и насыщенную жизнь доступной каждому человеку, инфоэтика должна проанализировать как положительную, так и отрицательную роль, которую может сыграть технический прогресс в отношении реализации права на интеллектуальную собственность.

### **Доступ к информации и коммуникации**

Чтобы права человека обрели полную силу в информационном обществе, людям нужен доступ к информации, для чего, в свою очередь, требуется доступ к средствам ее передачи. Поэтому задачи инфоэтики должны также быть направлены на три основных аспекта доступа к информации и коммуникации, существенных для реализации прав человека: (i) общий доступ к знаниям и творческим произведениям; (ii) разнообразии материала в информаци-

онных и коммуникационных сетях и (iii) ничем не ограниченный доступ к такой информации (помимо прочего, наличие средств для передачи контента и умение его использовать).

### **■ Общественное достояние**

Одна из приоритетных задач инфоэтики состоит в расширении общедоступной информационной зоны, т.е. определении объема знаний, информации, набора культурных и творческих произведений, которые должны быть доступны каждому человеку. В эту категорию в числе прочего обязательно входят:

- **правительственные документы**, позволяющие информированному демократическому обществу отслеживать и оценивать действия избранных им лидеров. Таким образом, все люди получают возможность участвовать в процессе управления;
- **информация о персональных данных**, имеющаяся в распоряжении юридических лиц, позволяющая индивидам понимать степень конфиденциальности информации;
- **данные по науке и истории**, которые позволяют всем людям получать неограниченный доступ к знаниям для понимания событий и дальнейшего развития знаний;
- **информация, касающаяся опасности для здоровья**, которая позволяет людям осознать возможные риски, которым они подвергаются, и действовать соответственно;

- **информация о состоянии технологий**, которая позволяет обществу понять, каким образом информационное общество может защищаться от информационных войн и других угроз правам человека;
- **творческие работы**, составляющие часть общей культурной базы, которая позволяет людям активно участвовать в общественной и культурной жизни.

Рекомендация ЮНЕСКО о развитии и использовании многоязычия и всеобщем доступе к киберпространству, принятая на 32-й сессии Генеральной конференции ЮНЕСКО в октябре 2003 г., предлагает следующее определение информации, являющейся общественным достоянием: **«Информация, являющаяся общественным достоянием** – доступная для общественности информация, использование которой не нарушает ни прав, установленных законом, ни обязательств сохранения конфиденциальности. Таким образом, это определение охватывает, с одной стороны, все произведения или объекты смежных прав, которые каждый может использовать без получения разрешения, например, когда на основании национального или международного

права не предоставляется охрана или когда истекает срок действия охраны. С другой стороны, оно охватывает данные, являющиеся общественным достоянием, и официальную информацию, произведенную и добровольно предоставленную правительствами или международными организациями».

Объем общедоступной информации часто подвергается пересмотру. Открытый доступ к правительственным документам и совещаниям ограничен, как правило, по соображениям секретности в определенных делах; точно так же доступ к персональной информации ограничен по соображениям конфиденциальности. Некоторые страны предпочитают исключать ряд материалов из области общедоступной информации, считая обнародование таких материалов вредным для населения в целом<sup>12</sup>. Доступ к результатам научных исследований и научным знаниям может быть ограничен правительственным постановлением часто по этическим соображениям<sup>13</sup>. Законы относительно интеллектуальной собственности часто ограничивают свободный доступ общества к информации, предоставляя исключительную лицензию на творческие произведе-

<sup>12</sup> В Германии, например, действует запрет на материалы, пропагандирующие неонацистские организации или отрицающие Холокост. См. Deutsche Welle, «Trial Highlights Limits of Free Speech in Germany» (Суд определил границы свободы слова в Германии), <http://www.dw-world.de/dw/article/0,2144,1896750,00.html> (описание судебного процесса над Эрнстом Цюндедем, обвиняемым в «разжигании расовой ненависти» по факту его отрицания Холокоста).

<sup>13</sup> ООН недавно приняла резолюцию, призывающую государства-члены запретить клонирование человека в любой форме, но не смогла достичь согласия для придания этой резолюции обязательного статуса. См. United Nations Declaration on Human Cloning, U.N. Doc. No. A/59/516/Add.1 (2005).

ния владельцу прав на интеллектуальную собственность и разрешая разные степени добросовестного использования материала<sup>14</sup>.

Однако инфоэтика, пожалуй, не должна определять, является ли существующая граница между «общедоступной информацией» и «информацией ограниченного использования», а также интеллектуальной собственностью, «справедливой». Вместо этого инфоэтика должна сосредоточиться на том, чтобы сделать информацию из категории общественного достояния действительно общедоступной. Информация о рисках для здоровья, которые связаны с новыми технологиями, должна быть доступна без ограничений и распространяться среди всех потенциальных пользователей. Творческие работы, составляющие общественное достояние, должны быть четко маркированы как общедоступные. Правительства должны разрешить доступ к документам, которые не являются секретными<sup>15</sup>, включая передачу этих документов по широко распространенным коммуникационным и информационным каналам.

### ■ Разнообразие контента в информационных сетях

ИКТ оказывают также большое влияние на разнообразие контента в информационных сетях. В идеальном обществе контент информационных сетей должен отражать разнообразие легитимных предпочтений населения. Кроме того, информационные сети должны быть открыты для контента из всех источников, позволяя любому заинтересованному индивиду стать создателем контента, а не просто его рядовым потребителем.

СМИ, такие как телевидение и радио, позволяют быстро передавать контент потребителям, находящимся в самых удаленных регионах мира. Однако эти средства стремятся удовлетворить потребности таких сегментов населения, которые обладают наибольшим экономическим потенциалом; значительные затраты на запуск телевизионного канала или радиостанции ограничивают распространение контента, ориентированного на нишевую аудиторию<sup>16</sup>. Существующие каналы могут быть не заинтересованы в

<sup>14</sup> См. Ruth Okediji, «Towards an International Fair Use Doctrine» («В поддержку международной доктрины добросовестного использования»), 39 Columbia J. Transnat L. 75 (2000).

<sup>15</sup> Южная Африка предоставляет каждому право на действие для получения информации, находящейся в ведении частных организаций. См. Promotion of Access to Information Act, Act no. 2 of 2000 (The Republic of South Africa).

<sup>16</sup> Некоторые государства сделали попытки решить эту проблему государственным регулированием. В Германии, например, каждая земля должна либо предоставлять общественную сеть, содержащую разнообразный контент, либо регулировать работу частных сетей и обеспечить предоставление ими разнообразного контента, отвечающего интересам определенных групп населения. См. Uli Widmaier, «German Broadcast regulation: A Model for a New First Amendment?» («Закон о немецком вещании: модель новой первой поправки?»), 21 B.C. Int'l & Comp. L. Rev. 75, 93–99 (1998).

том, чтобы принимать контент из других источников или обеспечить его разнообразие<sup>17</sup>.

В Бразилии обозреватели выразили озабоченность относительно разнообразия контента, предоставляемого по сетям сотовой связи<sup>18</sup>. Эти сети в настоящее время стали основным средством распространения интерактивного контента; если доступ к сотовым телефонам имеют 45% населения, только 12% имеют доступ к Интернету. Поэтому не удивительно, что сети сотовой связи все чаще становятся носителями разных форм контента помимо голосовой телефонии; музыка, видео, интерактивные игры и другие материалы также доступны по каналам сети сотовой связи. Подобно традиционным СМИ компании сотовой связи могут получить эксклюзивный контроль над контентом, доступным значительной доле населения, и, таким образом, получить возможность поддерживать или ограничивать передачу имеющегося контента.

ИКТ предоставляют средства для преодоления подобных препятствий в деле достижения разнообразия контента.

В принципе, ИКТ значительно сокращают стоимость производства и

распространения контента, создавая дополнительные возможности для творчества и его субъектов. Способствуя большей интерактивности контента, они превращают потребителей в активных участников процесса.

### ■ Неограниченный доступ к информации

Усилия по созданию общедоступной информационной базы и поддержке разнообразия контента в информационных сетях заслуживают всяческого одобрения. Однако действительная их реализация зависит от практической способности людей получать доступ и использовать разнообразный контент и информацию, которые предоставляет им общая информационная база. Таким образом, одной из основных задач инфоэтики является достижение общего доступа ко всему легальному контенту. Задача эта включает две достаточно разные составляющие: обеспечение возможности *получить* контент и обеспечение условий, при которых все люди смогут *использовать* контент, который они получают.

Возможность получить контент требует доступа к информационным сетям или другим каналам передачи информации. Она может быть

---

<sup>17</sup> США попытались регулировать отношения между телевизионными сетями и создателями телевизионных программ, но оставили эти попытки. См. Christopher S. Yoo, «Beyond Network Neutrality» («За пределами нейтралитета Сети»), 19 Harvard J. L. & tech. 1, Fall 2005, p. 49 n. 188.

<sup>18</sup> Электронная переписка с Рональдо Лемосом, Creative Commons Brazil, февраль 2006 г.

обеспечена либо путем увеличения доступа к конкретному каналу, либо путем предоставления дополнительных каналов распространения информации. Так, например, страна, граждане которой имеют ограниченный доступ к компьютерам и Интернету, не может выполнить задачу всеобщего доступа к информации, просто обеспечив наличие контента в онлайн. Вместо этого она должна выработать оптимальную стратегию, которая позволит сделать этот контент действительно доступным для населения. Это можно сделать путем развития и внедрения новых технологий, таких как подключение к сети мобильных телефонов, или предоставление контента в других формах людям, которые не могут получить доступ к нему в онлайн.

Разнообразие контента сильно зависит от сохранения «нейтралитета сети», когда никакая организация не может ограничить доступ к (легальному) контенту<sup>19</sup>. При нейтралитете сети каждый узел сети «слеп к содержанию» и передает трафик без учета его типа или контента. Таким образом, при условии внедрения принцип нейтралитета сети требует, чтобы все узлы (включая провайдеров интернет-услуг) передавали трафик без учета (или даже

без идентификации) его происхождения, адресата и контента.

Однако полный нейтралитет также несет в себе определенную опасность: сеть, полностью нейтральная к контенту, не только стимулирует разнообразие легального контента, но и допускает разные виды нелегального – от порнографии до спама и вирусов. Поэтому инфоэтика должна стремиться формировать будущие ИКТ так, чтобы они сохраняли положительные свойства сетевого нейтралитета, и стимулировать разработки, которые сглаживают отрицательные стороны этого нейтралитета<sup>20</sup>. Ключевым вопросом при этом будет следующий: могут ли периферийные устройства лучше справляться с негативными аспектами, чем изменения в самой сети, ведь периферийные устройства могут быть более совершенными технически и легче поддаются контролю со стороны пользователя.

Поисковые машины – еще одна точка доступа, в которой может происходить ограничение практической доступности контента. Учитывая объем данных, доступных в Интернете, многие пользователи полагаются на поисковые машины при поиске необходимого контента; в результате любой контент, который не может обнаружить поисковая ма-

---

<sup>19</sup> См. Mark N. Cooper ed., *Open Architecture as Communications Policy* (Открытая архитектура как политика в области коммуникации), Center for Internet and Society at Stanford Law School, 2004.

<sup>20</sup> См. Jonathan Zittrain, «Without a Net» («Без Сети»), *Legal Affairs* (январь–февраль 2006), [http://www.legalaffairs.org/issues/January-February-2006/feature\\_zittrain\\_jan-feb06.msp](http://www.legalaffairs.org/issues/January-February-2006/feature_zittrain_jan-feb06.msp).

шина, становится недоступным. Как и провайдеры интернет-услуг, поисковые машины способны стать «узким местом» маршрута и повлиять на разнообразие контента, передаваемого по сети, продвигая какой-то контент за счет размещения его в верхней части списка результатов поиска и осуществляя избирательную фильтрацию другого контента. Так, Google фильтровал результаты поиска, осуществляемого через его французские и немецкие сайты, удаляя те, которые ссылались на материалы нацистского или антисемитского содержания<sup>21</sup>. Однако эта способность как таковая не подлежит критике с этической точки зрения; она просто требует контроля, который бы обеспечил ее использование исключительно для удаления незаконного контента<sup>22</sup>.

Если информация распространяется с помощью ИКТ, то доступ к ней невозможен без доступа к самой технологии. Все чаще запускаются проекты, призванные исправить недостаток доступа к ИКТ; они предоставляют решение проблемы, которое может быть более экономически целесообразным и более оптимальным, чем проекты по предоставлению информации в различных офлайн-форматах. Так, ор-

ганизация под названием One Laptop per Child Foundation (Фонд «Каждому ребенку – по лэптопу») стремится использовать развивающуюся технологию для производства дешевых, неэнергоемких компьютеров с возможностью подключения к беспроводной сети, которые можно было бы широко распространить в самых бедных регионах мира<sup>23</sup>. (См. врезку ниже.) Более того, как мы покажем в следующих разделах, проблеме изоляции можно сделать менее острой за счет снижения стоимости сетевых коммуникаций.

Однако даже если стоимость ИКТ снизится настолько, что современные технологии станут доступными всем, все равно будут появляться новые разработки, доступ к которым на начальных стадиях будет ограничен. В этом смысле сам процесс распространения ИКТ требует внимания.

При развитии информационных сетей важно, чтобы организации по стандартизации и аналогичные им не попали под влияние конкретных программ. Если разрешить какой-то одной группе «захватить» регулятивную или устанавливающую стандарты организацию, то этой органи-

<sup>21</sup> См. <http://cyber.law.harvard.edu/filtering/google/results1html>; сравнить: Isabell Rorive, «Freedom of expression in the Information Society» («Свобода слова в информационном обществе»), рабочий документ для подготовительной группы по правам человека, силе закона и информационному обществу, п. 8, 15 сентября 2004 г. (обсуждение цензуры в действиях поисковых машин во Франции, Германии и Китае).

<sup>22</sup> Помимо этого, пользователи могли настраивать персональные фильтры для предотвращения доступа к нежелательному контенту.

<sup>23</sup> <http://laptop.org/>.

зации уже не удастся достичь баланса интересов. Создателям сетевых технологий следует выдать мандат или стимулировать их предлагать большую выгоду для общества в целом, а не поддерживать требования отдельных групп (таких, например, как владельцы защищенного авторским правом контента).

Создание ситуации, при которой все люди могут пользоваться контентом, который они получают, тут же рождает новые проблемы. Даже когда контент «доступен», ценность его невелика, если понять и использовать его сложно. Таким образом,

всеобщий доступ к информации требует, чтобы контент распространялся на разных языках или чтобы технологии позволяли осуществлять его перевод в приемлемую форму. Точно так же технологию можно использовать для того, чтобы сделать информацию доступной людям с физическими недостатками. Помимо этого, контент должен быть легко машиночитаем; в частности, контент общественного достояния должен выпускаться в таком формате, который имеет широкое распространение и не требует особых прикладных программ или устройств обеспечения доступа к нему.

### Каждому ребенку – по ноутбуку: ноутбук за 100 долларов

*Сэмюэль Кляйн*

Проект «Каждому ребенку – по ноутбуку» (One Laptop per Child, OLPC), задуманный в Media Lab MIT и объявленный впервые в январе 2005 года, стал попыткой начать массовое производство дешевых, надежных ноутбуков и распространять их по всему миру для повышения качества обучения детей. Целью проекта стало «обеспечение детей по всему миру новыми возможностями для исследования, эксперимента и самовыражения». Если проект пойдет, как было задумано, эти возможности будут предоставлены посредством ноутбуков с бесплатным программным обеспечением, которые станут инструментами создания и получения контента.

До настоящего времени проект был ориентирован на разработку дешевых и надежных компьютерных компонентов (в особенности, недорогих дисплеев) – по цене 100 долларов за ноутбук на начальных стадиях проекта (в дальнейшем – дешевле), – а также на создание партнерской сети, способной содействовать производству необходимого технического и программного обеспечения. Проект основан на экономии, обусловленной ростом масштабов производства: график подразумевает производство, как минимум, 5 миллионов ноутбуков. Эти компьютеры будут иметь встроенные адаптеры беспроводной связи и работать в составе ячеистой сети в условиях отсутствия доступа к глобальной сети. Они также должны работать от инновационных источников энергии, в частности, предоставлять возможность ручного запуска.

Предполагается, что ноутбуки будут распространяться в определенных регионах по принципу «один ноутбук – каждому ребенку в школе или в регионе». Распределение должно происходить через школы при содействии национальных правительств. Руководитель проекта – Николас Негропонтэ (Nicholas Negroponte) – говорит, что команда приступила к переговорам с официальными лицами Китая, Индии, Бразилии, Аргентины, Египта, Нигерии и Таиланда<sup>24</sup>, однако команда понимает: если страна не в состоянии предоставить каждому ребенку по ноутбуку, придется принимать нелегкие решения о том, где и как должно происходить распределение компьютеров.

Помимо технических задач проект должен решить еще и философские. Ноутбуки были выбраны частично потому, что дети могут принести их домой и приобщить к технологиям всю семью. Говорится о намерении отдать ноутбуки детям в собственность, даже если они будут самыми дорогими и необычными предметами во всей округе.

Разработка плана распространения ноутбуков и обучения – от дизайна ПО и контента, который будет загружен в машину, до исследований и предложений методов внедрения эффективной обучающей среды «One Laptop per Child» – одна из недавно сформулированных задач проекта. В настоящее время проект готов рассмотреть предложения по осуществлению и изучению данной задачи<sup>25</sup>. Несмотря на то, что OLPC – это образовательный проект, он не ограничивается педагогикой. Распределение миллионов ноутбуков в регионах, где компьютеры – редкость, и предоставление каждому младшему члену сообщества возможности «выйти в мир» (т.е. экзотический прибор и совершенно неизвестное старшему поколению знание) сильно нарушают статус-кво.

Методы выбора контента, распределение ноутбуков и рекомендации по их использованию для того, чтобы необходимые изменения прошли без ненужных социальных и культурных потрясений, – критически важные вопросы, в решении которых захотят участвовать многие группы. Для проекта такого масштаба OLPC непривычно широко открыт для предложений; проект имеет подготовленный для публичного редактирования перечень задач, в числе которых просьба к мыслящим людям изучить некоторые из поставленных вопросов и дать свои предложения и рекомендации<sup>26</sup>.

---

<sup>24</sup> Из One Laptop Per Child FAQ: [http://laptop.org/faq.en\\_US.html](http://laptop.org/faq.en_US.html) (просмотр 8 ноября 2006 г.).

<sup>25</sup> [http://wiki.laptop.org/wiki/OLPC\\_software\\_task\\_list#Educational\\_community\\_engagement](http://wiki.laptop.org/wiki/OLPC_software_task_list#Educational_community_engagement) (просмотр 8 ноября 2006 г.): «Мы предлагаем подключить интеллектуалов, художников, представителей общественности к созданию команды с разным опытом и знаниями».

<sup>26</sup> Id., [http://wiki.laptop.org/wiki/OLPC\\_software\\_task\\_list#Strategic\\_research](http://wiki.laptop.org/wiki/OLPC_software_task_list#Strategic_research) (просмотр 8 ноября 2006 г.).



# 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<sup>27</sup> обещает предоставить такие метаданные.

---

<sup>27</sup> 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<sup>28</sup>. 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 дружелюбен 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»<sup>29</sup>, 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<sup>30</sup> 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.

---

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

<sup>29</sup> <http://www.w3.org/Consortium/activities#SemanticWebActivity>.

<sup>30</sup> 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 разли-

чий 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<sup>31</sup>.

<sup>31</sup> 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-ideological-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 усложняю-

щийся 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 гово-

рят 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»<sup>32</sup>.

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<sup>33</sup>. 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 онлайн-форму, не рискует ли человек стать жертвой мошенничества?<sup>34</sup>

---

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

<sup>33</sup> Riva Richmond, «Internet Scams, Breaches Drive Buyers Off the Web, Survey Finds», Wall Street Journal, 23 июня, 2005, стр. В3, отчет об исследовании Гартнера 5000 онлайн-новых потребителей. В статье говорится, что более 42% онлайн-новых покупателей и 28% людей, осуществляющих в онлайн-банковские операции, отказываются от этих возможностей по причинам безопасности и недостаточной защиты прайвеси.

<sup>34</sup> 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 онлайн-сделку. И, хотя это надоевшее дело многих раздражает, людей уже «приучили» предоставлять о себе информацию таким способом и делать это, не задумываясь<sup>35</sup>.

Специалисты в данной области говорят, что средства управления цифровой идентичностью сделают онлайн-обмен информацией намного более безопасным и удобным, поскольку эта технология помогает установить более жесткий контроль над цифровой информацией, касающейся личности<sup>36</sup>.

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<sup>37</sup>, 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<sup>38</sup> 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

---

<sup>35</sup> 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 онлайн-взаимодействия.

<sup>36</sup> 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>.

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

<sup>38</sup> 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<sup>39</sup> (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 онлайн-покупку, 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 онлайн-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

---

<sup>39</sup> 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 метку 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 вернуть 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<sup>40</sup>, 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<sup>41</sup>. Вместо того, чтобы оперировать самими цифровыми идентичностями,

---

<sup>40</sup> Планируется, что Windows Vista получит массовое распространение в начале 2007 г.

<sup>41</sup> Управляет системой Higgins сообщество открытого кода Eclipse Foundation.



Higgins сочетает разные системы, делая возможным обмен информацией между ними по заданию пользователей<sup>42</sup>. Привлекательной видится перспектива мобильности в системах оценки репутации, которая позволит человеку «перенести» репутацию, которую он заслужил в сообществе eBay<sup>43</sup>, в мир Second Life<sup>44</sup>. 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»<sup>45</sup>. В этом смысле средства управления цифровой идентичностью

---

<sup>42</sup> 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.

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

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

<sup>45</sup> 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 персо-

нальных 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<sup>46</sup>. Конечно, рынок может подстегнуть развитие технологий, архитектура которых гарантирует честное поведение, а закон вполне сможет стиммулировать эту инициативу<sup>47</sup>.

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

---

<sup>46</sup> 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.

<sup>47</sup> 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<sup>48</sup>. 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, пожа-

луй, 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»<sup>49</sup>.

---

## Биометрия

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

---

<sup>48</sup> 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.

<sup>49</sup> 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:

- |  |  |
|--|--|
| <ul style="list-style-type: none"><li>• ДНК;</li><li>• типы лица;</li><li>• отпечатки пальцев;</li><li>• походка;</li><li>• радужная оболочка глаза.</li></ul> | <ul style="list-style-type: none"><li>• типы сетчатки глаза;</li><li>• запаха;</li><li>• подпись;</li><li>• почерк;</li><li>• голос.</li></ul> |
|--|--|

Несмотря на то, что, как известно, биометрия была известна в Китае еще в XIV веке<sup>50</sup>, она считается новой технологией, потому что сбор, оценка и анализ биометрических данных все чаще автоматизируются и представляются в цифровой форме. Как таковая, биометрия может сочетаться с другими технологичес-

кими 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

<sup>50</sup> 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...»<sup>51</sup> 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 нежелатель-

ных задержек самолетов, экипажей, пассажиров и грузов, в особенности в отношении законов по иммиграции, карантину, таможене и таможенным пошлинам». ICAO заявила, что проект поможет государствам-участникам «внедрить по всему миру стандартизированную систему подтверждения идентичности»<sup>52</sup>.

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-

<sup>51</sup> 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/>.

<sup>52</sup> 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 онлайн-транзакций; он также сможет помочь в обеспечении порядка и защиты от кибератак. Кроме того, он предоставит глобальный метод 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.<sup>53</sup> 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<sup>54</sup>. Вполне предсказуемо, что взять на себя эту роль может быть предложено некоему международному агентству. В свете того, что международные организации не за-

страхованы 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.<sup>55</sup>

Наряду со смертью анонимности мы сможем наблюдать и такое явление,

---

<sup>53</sup> 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.

<sup>54</sup> 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.

<sup>55</sup> 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 приватности, 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<sup>56</sup>. 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-

---

<sup>56</sup> 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>).

мая его прохождения через считывающее устройство – например, во время погрузки или разгрузки. В розничной торговле RFID-чипы должны полностью заменить штрих-коды, поскольку новая технология позволяет присваивать метки на уровне составных элементов<sup>57</sup>.

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<sup>58</sup>. 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<sup>59</sup>. 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<sup>60</sup>. 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.

---

<sup>57</sup> 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.).

<sup>58</sup> 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.).

<sup>59</sup> Данные требования по маркировке шин сформулированы в TREAD Act, принятом 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.).

<sup>60</sup> Приняв проект «Dedicated Short Range Communications», международная автомобильная промышленность дала согласие на коротко- и среднедальнейшей беспроводной протокол, созданный специально для использования в автомобилях ([http://www.standards.its.dot.gov/Documents/advisories/dsrc\\_advisory.htm](http://www.standards.its.dot.gov/Documents/advisories/dsrc_advisory.htm) – информация Министерства транспорта США, [http://www.ictsb.org/ITSSG/Documents/Mandate\\_M270.pdf](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<sup>61</sup>. В 2005 г. Cisco стала продавать RFID-серверы, работающие с RFID-чипами, вставленными в форменную одежду для определения местонахождения сотрудника<sup>62</sup>. В целях иммиграционного контроля многие страны внедряют RFID-чипы в паспорта для выполнения требований ICAO по бесконтактным машиночитаемым проездным документам. (См. соответст-

вуюющую дискуссию в примере по биометрии.)<sup>63</sup>

RFID-чипы применялись также в области здравоохранения: в 2003 г. они были встроены в персональные бейджи в двух больницах Сингапура<sup>64</sup>, 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<sup>65</sup>.

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

<sup>61</sup> 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.

<sup>62</sup> «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.).

<sup>63</sup> 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 приватность») 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 Pertont «US Issues First RFID Passports» («США выпускают первые паспорта с RFID-чипами»), Engadget, <http://www.engadget.com/2006/03/13us-issues-first-rfid-passports/>.

<sup>64</sup> В пилотном проекте принимали участие Alexandra Hospital и National University Hospital.

<sup>65</sup> «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.

<sup>66</sup> «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<sup>67</sup>. Имплантаты могут также быть использованы на рабочих местах: ряд работодателей применял их, чтобы не допустить проход сотрудника на сверхсекретные объекты. В 2004 г. имплантанты поставили нескольким сотрудникам Министерства юстиции Мексики в целях запрета доступа на определенные объекты и в качестве средства слежения на случай их похищения<sup>68</sup>. 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<sup>69</sup>. 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...»<sup>70</sup>

Имплантаты 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<sup>71</sup>. В рамках совместной пилотной программы организации Digital Angel Corporation<sup>72</sup> и Brazilian

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

<sup>68</sup> [http://www.verichipcorp.com/images/GSN\\_Mar06.pdf](http://www.verichipcorp.com/images/GSN_Mar06.pdf).

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

<sup>70</sup> «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.aspx?id=67264> (просмотр 16 июня 2006 г.).

<sup>71</sup> 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](http://www.infoworld.com/products/print_friendly.jsp?link=/article/05/12/05/HNchickenflu_1.html)), просмотр 11 октября 2006 г.

<sup>72</sup> 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»<sup>73</sup>.

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)<sup>74</sup>.

Для слабовидящих и слепых людей компания En-Vision America разра-

ботала 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<sup>75</sup>.

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<sup>76</sup>. Последние оптовые цены на пассивные RFID-чи-

---

<sup>73</sup> [http://digitalangelcorp.com/about\\_pressreleases.asp?RELEASE\\_ID=217](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.

<sup>74</sup> Pacific Health Summit's Health and Information Technology and Policy Briefing Book, Health Information Technology and Policy Workshop, июнь 2006, стр. 6.

<sup>75</sup> <http://www.envisionamerica.com/scriptalk.htm> (просмотр 3 октября 2006 г.).

<sup>76</sup> «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<sup>77</sup>. Учитывая такое широкое использование RFID-чипов, специалисты предсказывают, что к 2010 году ежегодно в обращении будут находиться более 500 миллиардов RFID-чипов<sup>78</sup>.

### 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 акти-

визирует 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<sup>79</sup>.

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 передает ответный сигнал от входящего сигнала. Пассивные RFID-чипы могут настолько малы, что их практически не видно. Например, к

---

<sup>77</sup> 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.

<sup>78</sup> 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.).

<sup>79</sup> <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<sup>80</sup> 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<sup>81</sup>. (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 широкомас-

штабное 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-

---

<sup>80</sup> <http://www/glandi.com/epacking/htm>.

<sup>81</sup> Там же.

ляет полиции использовать каждый чип как радиомаяк<sup>82</sup>.

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)<sup>83</sup>.

Из всех обследованных компаний ни одна не информировала своих сотрудников об этих дополнитель-

ных возможностях применения чипов, оставляя их в убеждении, что RFID-чипы использовались исключительно для контроля над доступом. В общем, четких писанных 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<sup>84</sup>.

В связи с пристальным вниманием Европейского Союза к защите пер-

---

<sup>82</sup> Лекция Кэтрин Альбрехт в Гарвардском Университете 7 апреля 2006 г. (<http://www.nocards.org/>).

<sup>83</sup> 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.

<sup>84</sup> 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 унижительных» форм мониторинга сотрудников. Национальная комиссия по информатике и праву (Commission nationale de l'informatique et des libertés) 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<sup>85</sup>.

Работодатели говорят, что защита и общественная безопасность оправдывают использование RFID-чипов. Однако в дополнение к угрозе для приватности 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 обстоя-

тельства, 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<sup>86</sup>.

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<sup>87</sup>. Даже если такие меры весьма целесообразны в деле охраны здоровья населения, защита приватности и свободы собраний требует серьезного внимания к тем

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

<sup>86</sup> Там же.

<sup>87</sup> 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 имплантаты, и тогда непонятно, будет ли у людей право

отказаться от этих мер.<sup>88</sup> 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 Дезира 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

---

<sup>88</sup> 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<sup>89</sup>.

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

Если закрыть глаза на эти проблемы, то широкомасштабное использование RFID может способствовать решению самых разных этических 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-

---

<sup>89</sup> 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/%7Ekevinful/papers/RFID-CC-manuscript.pdf> (просмотр 23 октября 2006 г.).

<sup>90</sup> Хакеры – Аннали Ньюйтц 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<sup>91</sup>.

### 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.<sup>92</sup>

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

---

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

<sup>92</sup> 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)<sup>93</sup>. 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 «род» (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<sup>94</sup>.

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, подходящий 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<sup>95</sup>. (Такие устройства иногда на-

---

<sup>93</sup> [http://en.wikipedia.org/wiki/Remote\\_sensor](http://en.wikipedia.org/wiki/Remote_sensor) (просмотр 7 ноября 2006 г.).

<sup>94</sup> 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.

<sup>95</sup> 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»)<sup>96</sup>.

### 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<sup>97</sup>.

Даже данные, полученные для явно благих целей, могут оказаться вредными, если их использовать для це-

лей, 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 онлайн-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<sup>98</sup>.

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-

---

<sup>96</sup> См. исследование *infra* по технологии LBS.

<sup>97</sup> 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.

<sup>98</sup> 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<sup>99</sup>.

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 улики.

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-

---

<sup>99</sup> Majja 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)<sup>100</sup>, 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»<sup>101</sup>.

В то время как подобные проблемы обычно рассматриваются с юридической точки зрения, ученые настоятельно 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<sup>102</sup>. 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-

---

<sup>100</sup> 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.

<sup>101</sup> Интервью с Дэвидом Кларком в MIT, 11 ноября 2005 г.

<sup>102</sup> 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<sup>103</sup>.

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.

---

<sup>103</sup> 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](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, геопространственной 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)<sup>104</sup>, 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

---

<sup>104</sup> 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»<sup>105</sup>.

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 инерци-

альных датчиков для разработки недорогих систем слежения...»<sup>106</sup>

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<sup>107</sup>.

### 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<sup>108</sup>. Тем самым, можно сказать, что они помогают человеку осуществлять свое право на собрания. Это право может служить для поддержки демократии и свободы в

---

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

<sup>106</sup> 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.

<sup>107</sup> Веб-сайт VeriChip: <http://www/verichipcorp.com/> (просмотр 22 июня 2006 г.).

<sup>108</sup> См. [www.Dodgeball.com](http://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, определяют, 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 пожнать 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<sup>109</sup>.

### 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-

---

<sup>109</sup> Статья по ячеистым сетям в Wikipedia, [http://en.wikipedia.org/wiki/Mesh\\_network](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<sup>110</sup>.

Ячеистые сети отличаются способностью предоставлять множество разнообразных маршрутов для передачи данных, и такая избыточность делает эти сети надежными даже в случае выхода из строя ка-

кого-либо узла<sup>111</sup>. 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)<sup>112</sup>.

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.

---

<sup>110</sup> 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>.

<sup>111</sup> Этот метод аналогичен методу работы Интернета и других сетей, использующих равноправную маршрутизацию.

<sup>112</sup> 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»<sup>113</sup>.

---

<sup>113</sup> 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 сете-

вого 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 Хендриком<sup>114</sup>*

Ключевым фактором, объясняющим интеграцию Интернета в нашу жизнь, является его проникновение во все ее сферы. Там, где Интернет 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<sup>115</sup>.

Дуэйн Хендрикс – специалист в области спектров частот – считает, что «деление спектра радиочастот на отгороженные стеной охранные зоны – пережиток прошлого. Лицензируя спектр частот, политики внедрилы 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.

<sup>114</sup> Дуэйн Хендрикс (Dewayne Hendricks) является Генеральным директором Dandin Group.

<sup>115</sup> 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».



Отдельные права защищены

Данная работа защищена лицензией Creative Commons «Attribution 2.0»<sup>116</sup>.

## 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 памя-

ти. 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-

<sup>116</sup> <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<sup>117</sup>.

В виде идеи **вычисления на основе Grid-технологий** существуют уже несколько десятилетий, первые кон-

цепции 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<sup>118</sup>.

**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»<sup>119</sup>.

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

---

<sup>117</sup> 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).

<sup>118</sup> 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.

<sup>119</sup> <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...»<sup>120</sup>.

Oracle рекламирует свои услуги следующим образом: «**Grid-технологии** позволяют вам создать единую ИТ-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»<sup>121</sup>.

### **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**<sup>122</sup>.

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

---

<sup>120</sup> [http://www-1.ibm.com/grid/about\\_grid/benefits.shtml](http://www-1.ibm.com/grid/about_grid/benefits.shtml), просмотр 5 марта 2006 г.

<sup>121</sup> <http://www.oracle.com/technology/tech/grid/index.html>, просмотр 27 января 2006 г.

<sup>122</sup> <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»<sup>123</sup>.

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<sup>124</sup>. 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...»<sup>125</sup> 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-

---

<sup>123</sup> <http://gridcafe.web.cern.ch/gridcafe/challenges/challenges.html>, просмотр 5 марта 2006 г.

<sup>124</sup> <http://gridcafe.web.cern.ch/gridcafe/challenges/challenges/access.html>, просмотр 5 марта 2006 г.

<sup>125</sup> <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 перекрывающихся 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)<sup>126</sup> в 2001 г. В настоящее время эта группа работает над стандартом «Открытая архитектура Grid-сервисов», который, как ожидается, станет основным стандартом функционирования Grid<sup>127</sup>. В дополнение к этому общему архитектурному стандарту компания Globus Alliance выпустила про-

граммный пакет с открытым кодом «Globus Toolkit»<sup>128</sup>, 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<sup>129</sup>. Однако в последние годы многие компании разработали технологию, способную эффективно различать разные

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

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

<sup>128</sup> 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.

<sup>129</sup> «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<sup>130</sup>.

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

*Георг Греве<sup>131</sup>*

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 обуславливает 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

---

<sup>130</sup> 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.).

<sup>131</sup> 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<sup>132</sup>.

## 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-

<sup>132</sup> 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 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 приве-

сти к дискриминации отдельных групп пользователей сети.

Также Grid-архитектура подразумевает необходимость различения контента. Технология, которая используется в настоящее время для такого различия, 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<sup>133</sup>**

*Дэвид Вайнбергер<sup>134</sup>, 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.



Отдельные права защищены

Защищено в соответствии с лицензией Creative Commons «Attribution-NonCommercial-ShareAlike 2.0». (<http://creativecommons.org/licenses/by-nc-sa/2.0/>).

## Новейшие вычислительные технологии

Закон Мура гласит, что вычислительная мощность одного чипа бу-

дет удваиваться каждые 18 месяцев<sup>135</sup>. Каждый раз, когда нам кажется, что мы приближаемся к пределу этого экспоненциального роста и имеющаяся технология достигла своего «потолка», появляется но-

<sup>133</sup> [http://www.hyperorg.com/blogger/mtarchive/reading\\_and\\_libraries\\_two>note.html#comments](http://www.hyperorg.com/blogger/mtarchive/reading_and_libraries_two>note.html#comments).

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

<sup>135</sup> Wikipedia, Moore's Law, [http://en.wikipedia.org/wiki/Moore%27s\\_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<sup>136</sup>. В этом разделе мы кратко 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 двумерны; 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 средст-

вом 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<sup>137</sup>.

### **Оптические и квантовые вычисления**

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

---

<sup>136</sup> Ray Kurzweil, «The Singularity Is Near» («Оригинальность уже близка»), раздел 3 (2005).

<sup>137</sup> 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 призматической 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 возможностей.

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 доминирующей

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, видекамерами и другими пунктами сбора данных. В связи с этим опять следует под-

черкнуть, 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 получают 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
<b>Семантическая сеть</b>	<ul style="list-style-type: none"> <li>• Расширяет доступ к информации.</li> <li>• Может приводить к поляризации и нарушению общественного диалога, хотя эта вероятность считается спорной.</li> <li>• 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).</li> </ul>	<ul style="list-style-type: none"> <li>• Может облегчить блокирование доступа к различным типам контента.</li> <li>• Может способствовать тому, что люди не захотят делиться контентом (из-за угрозы для определенного контента или конкуренции со стороны новых участников).</li> <li>• Может поставить людей на один уровень с предметами.</li> </ul>
<b>Управление цифровой идентичностью</b>	<ul style="list-style-type: none"> <li>• Может содействовать защите частной жизни и безопасности.</li> <li>• Может способствовать свободе собраний, помогая людям находить других людей со схожими интересами.</li> <li>• 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).</li> </ul>	<ul style="list-style-type: none"> <li>• Делает возможным сговор между провайдерами идентичности и третьей стороной и составление досье на пользователей.</li> <li>• Может легко превратиться в систему государственного контроля.</li> <li>• Может способствовать дискриминации.</li> <li>• Может поставить людей в зависимость от машин, действующих от их имени как агенты.</li> <li>• Может увеличить угрозу несанкционированного раскрытия или потери защищенной информации.</li> </ul>
<b>Биометрия</b>	<ul style="list-style-type: none"> <li>• Может помочь создать систему отчетности, что, по мнению некоторых, непосредственно связано с правами человека на жизнь, свободу и безопасность.</li> <li>• Может дать государству новые возможности по оказанию услуг населению (напри-</li> </ul>	<ul style="list-style-type: none"> <li>• Применение вместе с технологией управления цифровой идентичностью может стать обязательным условием участия в жизни информационного общества.</li> <li>• Может привести к созданию международной системы централизованного ад-</li> </ul>

	<p>мер, ускорить процедуру проверки паспортов в аэропортах). Некоторые считают, что это будет способствовать соблюдению прав человека</p>	<p>министрирования, при этом международные организации не смогут предотвратить злоупотребление властью.</p> <ul style="list-style-type: none"> <li>• Может создать условия для масштабного наблюдения, нарушая, таким образом, право на невмешательство в частную жизнь, свободу собраний и слова и т. д.</li> </ul>
<b>RFID</b>	<ul style="list-style-type: none"> <li>• Может способствовать эффективной работе каналов поставок (повышая уровень жизни, что, по мнению многих людей, непосредственно связано с правами человека на жизнь, свободу и безопасность).</li> <li>• Может повысить уровень безопасности, увеличивая возможности принуждения к выполнению законов.</li> </ul>	<ul style="list-style-type: none"> <li>• Может влиять на свободу убеждений, если имплантанты будут необходимы для участия в информационном обществе.</li> <li>• Может создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы.</li> </ul>
<b>Датчики</b>	<ul style="list-style-type: none"> <li>• Могут использоваться в качестве средств спасения, что напрямую связано с правами человека на жизнь, свободу и безопасность.</li> <li>• Могут оптимизировать производство и распределение (внести вклад в экономическую эффективность и, следовательно, помогая реализовать права человека на жизнь, свободу и безопасность).</li> </ul>	<ul style="list-style-type: none"> <li>• Могут добавить неясность в ситуацию с информацией, являющейся общественным достоянием, доступом к информации и средствам коммуникации.</li> <li>• Могут стать причиной серьезного беспокойства по поводу государственного суверенитета и безопасности.</li> <li>• Могут создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы.</li> </ul>
<b>Геопространственная сеть и LBS</b>	<ul style="list-style-type: none"> <li>• Может помочь людям в осуществлении права на свободу собраний.</li> <li>• Расширяя возможности служб спасения, укрепляют права человека на жизнь, свободу и безопасность.</li> </ul>	<ul style="list-style-type: none"> <li>• Может нарушать право на невмешательство в частную жизнь, давая возможность отслеживать местонахождение.</li> <li>• Может приводить к дискриминации и нарушению права на свободу собраний и слова, давая возможность отслеживать местонахождение.</li> </ul>

<p><b>Сети с ячеистой структурой</b></p>	<ul style="list-style-type: none"> <li>• Могут снять ограничения на контент (например, фильтрацию информации и выделение канала).</li> <li>• Могут помочь слабо развитым регионам получить доступ к средствам коммуникации.</li> </ul>	<ul style="list-style-type: none"> <li>• Могут сосредоточить власть в точках соединения опорного Интернета.</li> <li>• 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).</li> </ul>
<p><b>Grid-технологии</b></p>	<ul style="list-style-type: none"> <li>• Могут предоставлять малоимущему населению вычислительные мощности, память для хранения данных и средства поиска информации.</li> <li>• Повышают эффективность работы за счет оптимизации распределения ресурсов.</li> </ul>	<ul style="list-style-type: none"> <li>• Могут создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы.</li> <li>• Могут приводить к дискриминации и другим ограничениям за счет перекрытия доступа.</li> </ul>
<p><b>Новейшие вычислительные технологии</b></p>	<ul style="list-style-type: none"> <li>• Рост вычислительной мощности поможет эффективно осуществлять перевод на разные языки и объединять людей.</li> <li>• При использовании вместе с Grid-системами могут расширить возможности доступа к информации.</li> </ul>	<ul style="list-style-type: none"> <li>• Могут создать условия для масштабного наблюдения за людьми, нарушая этим право на невмешательство в частную жизнь и другие свободы.</li> <li>• Могут нарушить геополитический баланс (предоставляя возможность расшифровки секретных сведений).</li> </ul>

# Еще раз к рассказу о НОВЫХ ТЕХНОЛОГИЯХ

Как уже было сказано, **семантическая сеть** даст компьютерам метаданные, которые помогут отфильтровывать огромный объем информации, генерируемой и предоставляемой Интернетом. Сегодня люди пока еще помогают разрабатывать эти метаданные, но по мере развития информационного общества машины все чаще будут брать на себя задачу по созданию собственного словаря. На лингвистическом уровне метаданные могут приравнивать человека к объекту – к примеру, относят и человека, и его багаж к категории вещей, проходящих через контрольные терминалы аэропортов. Однако они также способны организовать мир таким образом, что его ресурсы станут доступны людям в удобной для них форме (например, с помощью метаданных можно особым образом «подписать» цифровые фотографии, чтобы вашим друзьям было проще их рассматривать). Адекватное программирование компьютеров, которое научит их помещать данные о людях на более высокий уровень, чем данные об объектах, может со временем решить проблему приоритетности информации.

определить, что на самом деле есть человек. На ранней стадии развития компьютерной лингвистики было важно описать человека не в контекстуальных терминах вроде «частый арендатор машин» или «обладатель высокого страхового риска», а скорее в терминах, связанных с существенными, неотъемлемыми и постоянными атрибутами индивида, например, правом на поиск, получение и отправку информации. В этом отношении средства управления цифровой идентичностью могли бы использоваться для реализации прав и автоматического исправления ситуации в случае их нарушения.

Если машины будут запрограммированы на особенно бережное отношение к данным о человеке, они автоматически станут обрабатывать данные об отпечатках пальцев, радужной оболочке глаза или походке иначе, чем оцифровывать, к примеру, грязь, автомобильный двигатель или бегущую собаку. В этом случае **биометрия** будет служить для защиты права на невмешательство в частную жизнь и права на свободу собраний, а не действовать против этих свобод. Эту технологию можно использовать во благо, например,

помогая людям узнавать друг друга и получать доступ ко множеству доменов.

Аналогично, **RFID, датчики, геопро-странственная сеть и сервис по определению местоположения (LBS-технология)** могут отслеживать различные действия человека: совершение покупок, эмоциональные реакции, передвижения по физическому миру. Эти данные становятся такими же управляемыми и доступными для поиска, как и другой оцифрованный контент, который могут собирать, анализировать и использовать самые разные люди. Для человека может оказаться сложным понимание того, чему он подвергается, или опровержение данных, которым общество склонно доверять больше, чем его показаниям. Рассматривая технологии под другим углом зрения, мы увидим их преимущества – так, RFID-чипы обещают снизить затраты компаний на производство, датчики помогут убедиться, что установка по очистке воды экологически безопасна, а LBS-сервис и геопространственная сеть помогут вернуть домой потерявшегося ребенка. Все эти технологии обещают развитие новых форм контента. Чтобы быть уверенными, что информационное общество примет правильное решение в отношении этих технологий, нужно сначала определить, как следует подходить к использованию разных типов данных, при условии, что конечная цель – это содействие реализации законных прав и свобод.

Что касается **сетей с ячеистой структурой**, то они предлагают развивающимся странам возможности, при которых новые способы соединения положат конец маргинализации экономики и населения. В то время как одни существующие компании могут опасаться конкуренции, а другие – считать неконтролируемую коммуникацию угрозой, обмен информацией по ячеистым сетям способен внести вклад в дело демократизации информационного общества. Таким образом, данный способ соединения может стимулировать разнообразие контента в информационных сетях, помогая сообществам людей с общей культурой и людям разных культур лучше понимать друг друга. В этом смысле технология ячеистых сетей способна максимизировать преимущества образовательного, информационного и культурного контента за счет расширения доступа к информации. Действительно, технологии такого типа могут расширить сферу действия Интернета и превратить всеобщий доступ к информации в реальность.

Когда простые устройства, подключенные к ячеистым сетям, и значительно более мощные компьютеры вместе подключаются к **Grid-системе**, они могут столкнуться с разными ограничениями, в зависимости от того, потребляют они ресурсы или предоставляют их. Здесь важно будет проследить, чтобы все люди получили равные права на доступ и в процессе аутентификации и авто-

ризации не подвергались дискриминации на основе критериев, не связанных с вычислительной мощностью или объемом памяти компьютера. И снова следует упомянуть, что в основу систем контроля доступа лягут программы, которые сегодня человек создает для компьютеров, и руководствоваться при их создании следует Всемирной декларацией прав человека.

Разработка правильных систем на этом этапе будет иметь решающее значение для будущего, построенного на таких **новейших технологиях**, как оптические или квантовые вычисления. От сегодняшних решений может зависеть, станет ли глобальный виртуальный «мозг», который появится в будущем, использовать свою интеллектуальную силу

для защиты людей и их прав. Если информационное общество изначально сделает правильный выбор, то мощные машины будущего станут уважать ценности, которые были в них заложены. В этом смысле вычислительные мощности будущего потенциально способны на более эффективную защиту прав человека, чем сегодняшние. Однако если все случится наоборот, то нас ждут довольно мрачные перспективы.

Подводя итоги, отметим еще раз, что фундаментальным вопросом является не собственно информация, а свободы, которые она дает. Поэтому цель информационного общества состоит в том, чтобы способствовать выполнению задач инфоэтики, учитывая ее принципы при разработке, внедрении и использовании технологий.



# Рекомендации

Новые технологии дают ЮНЕСКО и ее партнерам много новых возможностей и методов действия для выполнения соответствующих мандатов и активного участия в развитии информационного общества, как показывает приведенный ниже список рекомендаций:

## 1. Выступить в качестве лаборатории идей посредством:

### 1.1. Организации Консультативного совета

Международная работа над этическими аспектами новых технологий должна выиграть от регулярных рекомендаций Консультативного совета. Политические деятели и широкая общественность хотят знать мнение ведущих экспертов в области технологий, а интересы ЮНЕСКО пересекаются с программами ряда академических институтов, специализирующихся на технологиях. И ЮНЕСКО, и упомянутые институты ориентированы на такие цели, как уважение к правам человека и доступ к знаниям. Таким образом, наличие специального Консультативного совета по вопросам инфозтики позволило бы ЮНЕСКО использовать знания ведущих специалистов в области технологий и их авторитет в научных кругах.

Такая группа экспертов могла бы помочь ЮНЕСКО продолжать работу в рамках сотрудничества, начатого в ходе Всемирного саммита по информационному обществу (ВСИО), избегая при этом вопросов политики, которыми перегружены подобные форумы высокого уровня.

Чтобы сделать результаты работы группы адаптивными и далеко идущими, Консультативный совет должен помимо экспертов по технологиям и инфозтике включать в состав детей и молодежь со всего мира.

Кроме того, ЮНЕСКО могла бы наладить сотрудничество с академическими институтами для проведения сессий «мозгового штурма», посвященных неотложным проблемам, связанным с будущим.

## 1.2. Учреждения сообщества технических специалистов в целях защиты персональных данных

Как отмечалось выше, контроль над потоком персональных данных окажется решающим фактором для реализации прав человека и доступа к информации в информационном обществе. Этот фактор мы считаем одним из важнейших, так как вероятность использования технологий для установления контроля над жизнью человека становится все выше.

Поскольку управление цифровой идентичностью будет служить основным компонентом других технологий, связанных с потоком персональной информации, и поскольку промышленность готовится в ближайшие месяцы выпустить новые технические средства, мы предлагаем сделать данную технологию предметом особого внимания и поводом для сотрудничества.

Чтобы заполнить пробел в области международной защиты персональных данных, требуется значительная работа. На сегодня существует настоятельная потребность в защите персональных данных. Эта потребность признается международной группой комиссаров по защите данных и прайвеси, которая приняла в сентябре 2005 г. Декларацию Монтре, призывающую к соблюдению многосторонних принципов. Она признается также специалистами в области вычислительной техники и в особенности ведущими деятелями промышленной группы Identity Gang и WWW-Консорциума, понимающих, что их работа потенциально способна принести как большую пользу, так и большой вред, и желающих получить рекомендации относительно принципов, на которые им нужно ориентироваться при разработке кода.

Естественно, тема защиты персональных данных не нова: чтобы в век информации противостоять некорректному обращению с персональными данными, Организация экономического сотрудничества и развития (ОЭСР) и Совет Европы (СЕ) более 20 лет назад разработали свои правила<sup>138</sup>. В совокупности эти инициативы представляют собой значительный по объему свод правил. Принципы ОЭСР включа-

---

<sup>138</sup> В 1980 г. члены ОЭСР приняли «Руководящие принципы по защите частной жизни и трансграничных потоков персональных данных» («Guidelines on the Protection of Privacy and Transborder Flows of Personal Data»). В 1981 г. СЕ принял Конвенцию «О защите физических лиц при автоматизированной обработке персональных данных» (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data), CETS 108. Документы, принятые этими организациями впоследствии, развили положения данных документов.

ют ограничение на сбор информации, качество данных, указание цели, ограничение на использование данных, гарантии защиты, открытость, индивидуальное участие и отчетность. Статья 6 Конвенции СЕ добавляет к этому списку еще и положение об антидискриминации.

Однако правила ОЭСР не носят обязательного характера, а правила СЕ распространяются только на тех, кто поставил свою подпись под этим документом<sup>139</sup>. Даже если принять эти правила в обязательном порядке во всех странах мира, они будут иметь только юридический статус и потому будут бесполезны в качестве гарантии надлежащего обращения с персональными данными со стороны машин, находящихся в разных точках планеты. Действуя совместно с WWW-Консорциумом и академическими институтами, ЮНЕСКО могла бы помочь индустрии технологий разработать такие технические инструменты, которые бы обеспечили защиту персональных данных в ситуациях, когда закон не в состоянии этого сделать.

## 2. Выполнять роль разработчика стандартов

### 2.1. Изучение возможности подготовки закона об этике

Желательно составить Этический кодекс, который стал бы международным руководством по этике в информационном обществе. Основная цель этого инструмента – заставить «ведущих игроков» осознать их общую ответственность за соблюдение принципов инфоэтики в информационном обществе.

### 2.2. Подготовка анализа нейтральности сети

Рекомендуется проанализировать правила управления информационными сетями в разных государствах (соблюдаются ли правила нейтралитета и пр.) и сами сети, которые образуются в результате таких условий. ОЭСР могла бы проследить, соответствуют ли международные нормы или стандарты принципу нейтральности сети, и при необходимости вмешаться, приняв участие в дискуссиях. Возможно обращение за помощью к академическим институтам.

<sup>139</sup> В числе стран, поставивших свои подписи под этим документом, – 38 стран Европы, 33 из которых ратифицировали данную Конвенцию.

### **2.3. Пропаганда инфоэтических аспектов международного нормотворчества и принятия стандартов**

Состав Консультативного совета и групп «мозгового штурма» должен быть относительно небольшим, чтобы обеспечить эффективность дискуссий. Однако важные вопросы должны выноситься на широкую публику через веб-сайт, а краткое изложение дискуссий – составляться в письменной форме и быть доступным всем заинтересованным лицам, даже тем, кто проживает в регионах, еще не подключенных к Интернету. Встречи могут проводиться в режиме общения в реальном времени или транслироваться по Сети.

## **3. Содействовать общественному просвещению в сфере развития технологий**

---

Другое важное направление деятельности – это обсуждение вопросов о том: а) имеет ли общественность право знать о состоянии развития технологий; б) если да, то как нужно осуществлять это право; в) каким образом люди могут научиться понимать принцип работы технологий и в условиях кризиса уважительно относиться к правам друг друга.

ЮНЕСКО должна поддерживать открытые стандарты и протоколы, выработанные в результате демократических процессов, неконтролируемых крупными корпорациями.

Следует поощрять использование открытых форматов, таких как OpenDocument Format, поскольку они помогают избавить людей от жесткой зависимости от определенных технологий<sup>140</sup>. Другие заслуживающие внимания инициативы включают разработку свободного и открытого ПО, а также «Roadmap for Open ICT Ecosystems»<sup>141</sup> («Дорожную карту по открытым системам ИКТ»), разработанную в прошлом году.

Для продвижения этих начинаний ЮНЕСКО должна принимать участие в работе организаций по стандартизации и устраивать консультации с техническими специалистами. Это поможет организации лучше понимать суть дела и действовать более энергично.

---

<sup>140</sup> Дополнительная информация представлена на <http://en.wikipedia.org/wiki/OpenDocument> (просмотр 15 марта 2006 г.).

<sup>141</sup> См. <http://cyber.law.harvard.edu/epolicy/roadmap.pdf>.

# ПРИЛОЖЕНИЕ

## Демократическое информационное общество (краткое содержание интервью с Дэвидом П. Ридом)

Дэвид Рид<sup>142</sup> – специалист по вычислительной технике, оказавший большое влияние на развитие Интернета, считает, что «общедоступность компьютерных ресурсов и всеобщий доступ к Сети дают эффект синергии: вместе эти технологии обеспечат внедрение глобальных систем совместного пользования информацией».

В данном разделе мы представим интервью с Дэвидом Ридом.

### Наследство иерархических структур

До недавнего времени компьютерные вычисления во всем мире регулировались теми учреждениями, где изначально зародились компьютерные технологии – то есть небольшой частью общества (к которой относились и крупные организации вроде министерств обороны, и представители большого бизнеса, поскольку они могли позволить себе приобретение последних технологических новинок). Эта небольшая группа в основном использовала технологии для обработки и хра-

нения записей. В результате подход к использованию компьютерных технологий был характерным для всех для крупных корпораций – «командно-административная» иерархическая культура, во главе которой стоит директор и топ-менеджеры. Этот ограниченный контингент определял, какая именно информация интересна для данной группы, у кого и с кем есть право делиться ею.

На ранних стадиях развития компьютерной техники, 30 или 40 лет назад, решения по многим системам принимались в рамках подобных иерархических схем или культур. Так, например, компьютерная безопасность определялась следующим образом: *«Разрешено то, что хорошо для организации в целом, а что плохо – не разрешено»*. При этом не существовало демократического определения того, что хорошо для организации в целом. Безопасность в милитаристическом контексте была хорошо проработана и существовала в форме недискреционного контроля доступа – иными словами, человек не имел права

<sup>142</sup> Интервью с Дэвидом П. Ридом (David P. Reed), адъюнкт-профессором MIT Media Lab. Вместе с профессором MIT Дж. Зальцером и Дэвидом Д. Кларком (J.H. Saltzer and David D. Clark) Рид является автором «end-to-end» (сквозного, «терминал – терминал») принципа построения Интернета, сформулировал «Закон Рида».

самостоятельно решать, с кем ему делиться информацией. Смысл такой политики заключался в том, что индивидуальные решения должны были совпадать с общими целями, а цели претворялись в жизнь в соответствии с продиктованными сверху правилами, инструкциями и политическими установками. При этом люди должны были принимать правила как данность и строго им следовать, поскольку другого выбора просто не было.

Бизнес-среда отличалась большей гетерогенностью. Информационный поток циркулировал в пределах компаний, причем каждая из них имела свой собственный набор целей. Внутри каждой корпорации эти цели были общими для всех, и информация свободно курсировала как внутри разных департаментов, так и между ними. Однако обмен информацией с внешними организациями должен был осуществляться по правилам, установленным небольшой группой людей. (Иными словами, эта система тоже была иерархической, но более гибкой, чем военная.)

Такой подход к обмену информацией оказался нежизнеспособным: осуществив компьютеризацию, военные работать не смогли. Причина заключалась в том, что на практике люди не всегда точно следовали жестким военным правилам, в действительности имели достаточно возможностей для того, чтобы эти правила нарушать, и именно это позво-

ляло организации работать. То же самое происходило и в «гражданских» корпорациях, где информация циркулировала между организациями независимо от того, что предписывали правила. Коммерческие тайны хранились не так уж строго. Подобная гибкость позволяла компаниям приходиться к соглашениям, потому что люди могли иметь собственное мнение.

Сегодня все настолько компьютеризировано, что практически при каждом акте коммуникации, требующем обращения к компьютеру или подключения к сети, происходит модифицирование, фильтрация или адаптация информации. Система работает, несмотря на то, что разработчики компьютерного кода ориентировали компьютеры на соблюдение конкретного набора протоколов или процедур.

Разработчики системы всегда исходили из убеждения, что миф о том, как осуществляется коммуникация, действительно соответствует реальности. Они попытались навязать компьютерным системам тот способ, который, как предполагалось, общество использовало для общения: они пытаются применить этот миф к компьютерам подобно тому, как принтер подключают к рабочей станции. И каждый раз, когда разработчики кода пытаются насильно утвердить эту иерархию, они получают универсальный урок: история, которую общество рассказывает себе, – неправда.

Наше общество привыкло считать, что самая ценная информация хранится в самом дорогом компьютере или в головах начальников. Это не всегда так – на самом деле центральные персонажи не владеют почти никакой информацией. Они могут быть обладателями определенного опыта или мудрости, но основная информация сосредоточена на периферии или рассредоточена по всей культуре. Когда компьютеры проникают в эти области, информация высвобождается и становится более доступной для пользователей... тут-то и выясняется, что самая ценная информация – вовсе не та, что хранится в центре. Так корректируется «миф о том, где находится самая ценная информация».

Всеобщая компьютеризация и развитие сети подразумевают увеличение числа носителей наиболее ценной информации и внедрение наиболее эффективных решений. Вместе они становятся силой, которая вращает мир.

Вполне возможно, что у ЮНЕСКО есть свой миф о том, что не стоит ставить под вопрос авторитеты.

К примеру, способ управления, когда лидеры страны предпочитают политику концентрации власти и секретности, вреден для государства. Власть предрержащие в результате оказываются изолированными от того, что движет миром – от информации. Существует опасность, что

информация, которой располагают в центре, неверна – в конце концов, все, что секретно, вряд ли будет проходить проверку на соответствие реальности.

### Компьютеризация обходится на удивление дешево

Компьютеризация стоит на удивление недорого, и людям трудно поверить в то, что скоро она станет еще дешевле. Возьмем, к примеру, проект «Лэптоп за \$100». Неважно, начнется все с него или какого-то другого проекта, главное – просто понять, что через пару лет компьютер будет стоить именно столько. Чудо в том, что это первое компьютерное устройство, разработанное не как очередная офисная платформа, а как *средство самовыражения человека*. И эти машины, объединившись, могут стать «сетевыми средствами самовыражения». ИКТ уже не озабочены в первую очередь автоматизацией бизнес-процессов; основной ценностью, скорее, стало считаться образование: эти ИКТ распространяются среди *детей*. Смысл не в том, чтобы получить доступ к некому удаленному веб-сайту, а в том, чтобы дать группе людей возможность наладить коммуникацию на более локальной и более выгодной основе. Цель – содействовать выражению человеческой личности и обмену информацией, дать возможность для совместной работы. Это также может привести к созданию иерархии, но

ее структура не будет ни навязанной, ни постоянной.

Жесткие иерархии исторически существовали потому, что изначальное создание их было делом непростым; но сейчас формирование групп *ad hoc* (для данного случая) сильно упростилось. Этот принцип лежит в основе закона Рида, который представляет собой математический способ выражения относительно далекого от математики принципа: если вы снижаете стоимость процесса формирования групп или отношений, это очень ценный вклад, вы получите большую отдачу и хорошие дивиденды<sup>143</sup>.

Как отмечал Рональд Коуз (Ronald Coase), фирмы создавались для снижения коммерческих издержек<sup>144</sup>. Теперь они уже не так нужны. Теперь организации могут быть временными, эффективными и не требующими больших вложений. По мере развития технологий, обеспечивающих все более эффективные формы виртуальных технологических отношений, элементы общества приспособятся к самоорганизации для более эффективного выполнения какой-либо задачи.

Более того, группы могут эффективно формироваться и на большой территории – например, Интернет позволяет эффективно фор-

мировать группы *планетарного масштаба*.

### Удаленная, прокси- и мобильная коммуникация

Помимо снижения операционных издержек на организацию групп ИКТ предоставляют еще одну возможность, интересную в контексте нашей темы: поскольку сетевые технологии все более эффективно внедряются на локальном уровне, начинает доминировать «прокси-ком», а использование термина «телекоммуникация» – «телеком» уже не всегда корректно. Скорее, в данной ситуации правильнее говорить о локальной коммуникации на уровне сообщества, именуя ее «прокси-ком».

На раннем этапе развития телефонии внутри городов существовали небольшие локальные сети, кроме того, имелись отдельные сети для междугородней и даже международной связи. Телефонные компании посчитали, что могут установить высокие тарифы на междугородние звонки, поскольку в этом случае люди просто не имели другой альтернативы – ведь добраться до собеседника и поговорить было нельзя. Из-за того, что компаниям не удавалось сделать много денег на местных звонках (т.к. в этом случае люди могли просто ходить друг к

<sup>143</sup> Для математического выведения числа возможных подгрупп см. [http://en.wikipedia.org/wiki/Reed%27s\\_law](http://en.wikipedia.org/wiki/Reed%27s_law) (просмотр 14 марта 2006 г.).

<sup>144</sup> «The Nature of the Firm» («Природа фирмы») в Readings in Price Theory, Stigler and Boulding, editors. Chicago, IL: R.D. Irwin, 1952.



другу в гости), они установили единый тариф на местное обслуживание. Этот тариф привел к увеличению числа линий местной связи, расходы на которые покрывались за счет прибыли от междугородних звонков. Далее телефония перешла на сотовые сети, обладающие мобильностью, т.е. промышленно развитое общество перешло с междугородней связи на прокси-коммуникацию, а потом и на мобильную связь.

Архитекторы Интернета вынашивали грандиозную идею объединения всех коммуникационных сетей и превращения их в интероперабельную сеть. Значительное преимущество Интернета заключалось в предоставлении дешевой междугородней связи, т.к. люди получили возможность подключаться к компьютерам по всей стране. Сеть на самом деле давала доступ к данным по всему миру. Сегодня настало время бурного развития локальных сетей. Широкополосное соединение по-прежнему дает пользователю возможность доступа к сайтам в любой части мира, однако популярные новшества, такие как создание википедии, больше соответствуют локальному пространству. Людям больше волнует то, что происходит на местном уровне, и именно на этом строится сейчас Интернет.

Что касается телефонии, то мобильная коммуникация стала необходима, когда люди, раньше использовавшие локальную коммуникацию,

привыкли перемещаться, не прекращая общения. И сегодня информационное общество переходит на мобильный Интернет. После того, как локальные области были покрыты сетями, появилась мобильная коммуникация. Люди могут передвигаться и при этом подключаться к сети.

Эта стадия мобильного Интернета еще не началась. Она требует внедрения более мобильных компьютерных платформ. Проект «Лэптоп за \$100» интересен, потому что он предлагает мобильную «машину для самовыражения», которая к тому же предназначена, прежде всего, для работы не в офисе, а вне помещения. Использование беспроводной технологии Wi-Fi и программного обеспечения, позволяющего пользователям лэптопов отправлять файлы, дает группе людей организовать даже джем-сешн. Технология Wi-Fi – первый пример очень гибкой высокоскоростной мобильной сети. Она использует принцип вирусной коммуникации и относится к категории сетей, работающих без предварительно созданной инфраструктуры. Такие сети, формируемые самими устройствами, могут охватывать всю планету.

Технология достигла такого уровня, когда использование высокоэффективной радиосвязи уже не стоит больших денег. Исторически процесс тормозила именно медленная эволюция культуры. «Вирусная» коммуникация – все равно, что ви-

русный маркетинг – он разрастается за счет слухов... интереса... взаимного обучения людей. Успех технологических изменений зависит от их синхронизации с культурными ценностями. (Заметьте, кстати, что основной движущей силой вирусной коммуникации снова стали не военные – ведь они всегда жаждали иерархии, а иерархия предполагает добавление уровня, ограничивающего доступ. Попытки современных китайских властей блокировать коммуникацию – иллюстрация этой же теории.)

Средства коммуникации сами по себе не являются атрибутом культуры, скорее, культура накладывается на структуру Интернета, поскольку он предоставляет ей новые возможности для самовыражения. Провода и цифровые сети – это не культура, это – средство, с помощью которого культура может выразить себя. Культура не приходит с подключением к сети, она приходит с пользователями. Культура – явление экзогенное, а не эндогенное.

### **Способность к саморазвитию, росту и усилению**

Повсеместная компьютеризация и внедрение ячеистых сетей приведут к большим изменениям. Однако при этом возникает одна проблема: технология способна усилить что угодно – и хорошее, и плохое; она подобна эпидемии, процессу размножения вируса. Технология полезна, потому что позволяет людям

объединяться в группы, связываться друг с другом и распространять позитивную информацию. Однако тот же самый принцип действует в отношении компьютерных вирусов и «спама»: если кто-то захочет использовать сеть в дурных целях, у него есть для этого масса возможностей.

Глобальные недостатки сетей можно преодолеть путем демпфирования (намеренного замедления роста) или создания контрвирусов, способных преследовать и уничтожать негативные феномены. Последний подход чреват созданием лекарства, побочные эффекты которого страшнее самой болезни, как это случилось с препаратом DDT: его использовали для уничтожения комаров, но при этом гибли и птицы. Так что сеть способна нести обществу не одно только добро.

Сейчас все надежды возлагаются на образование в истинном смысле этого слова: нужно, чтобы каждый член информационного общества дорос до понимания того, как работает система и как люди могут коллективно ее использовать. Раньше общество справлялось с напастями с помощью командно-административной структуры. Теперь людям предстоит изучить систему, частью которой они все являются, – так, чтобы они могли в случае катастрофы принимать эффективные решения на локальном уровне. Потенциал «прокси-коммуникации» состоит в том, что этот вид соединения пред-

лагает более локальное и гибкое антикризисное решение – но только если люди смогут понять, как оно работает. Члены информационного общества должны получить соответствующее знание.

Короче говоря, общество должно научить людей понимать принципы работы самых систем. Это стало сейчас настоятельной потребностью.

### Заключение

Самыми важными условиями освоения парадигмы, в которую вступает сейчас информационное общество и которая подразумевает «гораздо более развитую глобальную компьютерную сеть и интенсивный обмен информацией», являются следующие:

1. Каждый человек должен понимать эту парадигму.
2. Каждый элемент системы в конечном счете отвечает: (а) за успех системы в целом и (б) за те значительные последствия, которые действия человека могут иметь для людей, находящихся от него на большом расстоянии и даже неизвестных ему лично.

Основная задача – научить всех людей жить в таком мире. Выгода от этого – огромна, а риск – общий для всех.

В результате развития технологии руководители организаций стали в гораздо меньшей степени, чем раньше, владеть информацией, не-

обходимой для решения проблем. Однако на совещаниях, где обсуждаются решения проблем, люди пока сохраняют привычку интересоваться лишь мнением руководства. Это при том, что представители молодежи в возрасте до 20 лет гораздо компетентнее в вопросах культуры и технологий, чем старшее поколение. Они лучше информированы о развивающихся технологиях, чем родители, которые полагают, что дети будут похожи на них. (Они не будут похожи.) Именно поэтому важно привлекать детей к выработке решений. Если общество не может разрешить им голосовать, оно должно, по крайней мере, прислушаться к тому, что они говорят, и честно попытаться понять людей, которые адаптируются к новым технологиям гораздо быстрее остальных. Места, в которых происходит освоение *de novo*, – это места для обучения. Эти люди осваивают и воспринимают новые технологии без предубеждений – и могут показать всем остальным участникам информационного общества, что возможно и что полезно. Проект «Лэптоп за \$100» – хороший пример такого подхода: он позволит узнать много нового о культурной адаптации к новой технологии.

Информационное общество должно признать, что масштаб явлений стал больше, равно как и область их действия. Люди должны научиться обращать внимание не только на локальные, но и на глобальные феномены.

## **Этические аспекты новых технологий. Обзор**

Мэри Рандл и Крис Конли

Редакторы *Е.И. Кузьмин, Т.А. Мурована, В.Р. Фирсов*

Ответственный за выпуск *И. Зайцев*

Технический редактор *Ю. Таранова*

Корректор *Т. Малинкина*

ИД № 02184 от 30.06.2000. Подписано в печать 03.09.2007.

Формат 60х90 1/16. Бумага офсетная. Гарнитура Ньютон.

Печать офсетная. Тираж 1000 экз.

Издательство «Права человека»,  
119992, Москва, Зубовский бульвар, 17  
веб-сайт: [www.hrpublishers.org](http://www.hrpublishers.org)

Фабрика офсетной печати, г. Обнинск, ул. Королева, 6

# Ethical Implications of Emerging Technologies: A Survey

Prepared by Mary Rundle and Chris Conley

Geneva Net Dialogue

ЮНЕСКО  
Сектор коммуникации и информации  
Отдел информационного общества  
1, rue Miollis  
75732, Paris Cedex 15  
France  
Tel.: + 33.1.45.68.45.00  
Fax: +33.1.45.68.55.83

Российский комитет Программы ЮНЕСКО  
«Информация для всех»  
105066, Москва, 1-й Басманный пер., д. 2а, стр. 1  
тел./факс: +7 (495) 267 33 34  
e-mail: ifap@ifapcom.ru  
<http://www.ifapcom.ru>

[www.unesco.org/webworld/ifap](http://www.unesco.org/webworld/ifap)

## Paris: UNESCO 2007

Перевод и издание на русском языке – Российский комитет Программы ЮНЕСКО «Информация для всех» и Межрегиональный центр библиотечного сотрудничества при поддержке Федерального агентства по культуре и кинематографии

Москва 2007