содержание

ДЕКАБРЬ 2008

ГЛАВНЫЕ ТЕМЫ НОМЕРА:

ежемесячный научно-информационный журнал

SCIENTIFIC AMERICAN
В мире науки

Учредитель и издатель: ЗАО «В мире науки»

Главный редактор: С.П. Капица
Заместители главного редактора: А.Ю. Мостинская, О.И. Стрельцова

Зав. отделом естественных наук: В.Д. Ардаматская

Зав. отделом российских исследований: Ю.Г. Юшкявичюте

Выпускающий редактор: М.А. Янушкевич

Корреспонденты: Е.В. Кокурина, Д.А. Мисюров

Над номером работали:
Г.А. Аветов, А.Г. Аствацатуров, А.В. Ващенко, А.А. Гендин, Г.И. Двоскин, Б.А. Квасов, А.Р. Кадырова, М.Б. Молчанов, Б.И. Перлина, И.П. Прошкина, И.Е. Сацевич, А.Д. Старостин, И.А. Фролова, Д.С. Хованский, А.П. Худолей, Б.В. Чернышев, Н.Н. Шафрановская, Ф.С. Янчилина

Арт-директор: Л.П. Рочева

Корректура: Я.Т. Лебедева

Генеральный директор ЗАО «В мире науки»: О.А. Василенко

Главный бухгалтер: Н.М. Воронина

Бухгалтер: О.В. Гузий

Отдел распространения, подписка: М.К. Бирюкова, Л.В. Леонтьева

Адрес редакции и издателя:
105005, Москва, ул. Радио, д. 22, к. 409
Телефон: (495) 727-35-30, тел./факс: (495) 925-03-72
e-mail: info@sciam.ru; **www.sciam.ru**

Иллюстрации предоставлены *Scientific American, Inc.*
В верстке использованы шрифты *Helios* и *BookmanC*

Отпечатано:
ООО ИД «Медиа-Пресса», 127147, Москва, ул. Правды, д. 24.

Заказ № 82170

Журнал зарегистрирован в Комитете РФ по печати.
Свидетельство ПИ №ФС77-19285 от 30.12.2004

ЗАО «В мире науки» входит в состав Гильдии издателей периодической печати

Тираж: 11 600 экземпляров
Цена договорная.

SCIENTIFIC AMERICAN

ESTABLISHED 1845

Editor in Chief: John Rennie
Editors: Mark Alpert, Steven Ashley, Peter Brown, Graham P. Collins, Mark Fichetti, Steve Mirsky, George Musser, Christine Soares
Chief news Editor: Philip M. Yam
Contributing editors: Marguerite Holloway, Michelle Press, Michael Shermer, Sarah Simpson, W. Wayt Gibbs
Chairman: Brian Napack
President: Steven Yee
Vice President and managing director, international: Kevin Hause
Vice President: Frances Newburg
Chairman emeritus: John J. Hanley
Art director: Edward Bell
Vice President and publisher: Bruce Brandfon

за стеклом

Заставит ли нас развитие высоких технологий выбирать между приватностью и свободой?

Некогда одному философу-моралисту пришел в голову блестящий проект идеальной тюрьмы. А сегодня мы все живем в ней.

Начиная с 1785 года английский философ Иеремия Бентам в течение десятилетий настойчиво призывал к постройке сооружения, которое он назвал «Паноптикум» — «место всеобщей видимости». Это здание в форме кольца, в центре которого башня с широкими окнами. Кольцеобразное здание разделено на камеры, в каждой два окна: одно выходит внутрь, напротив соответствующего окна башни, а другое наружу; таким образом, помещение просматривается насквозь. В башне прячется невидимый узникам наблюдатель. Бентам настаивал на том, что подобная тюрьма гораздо надежнее и эффективнее любой другой — и даже не потому, что за заключенными всегда следят. В постоянном надзоре просто нет нужды — важно лишь, чтобы узник знал, что за ним наблюдают, причем проверить, так это или нет, невозможно. По словам философа, он изобрел «новый способ достичь господства ума над умом».

Надо сказать, что британское правительство так и не утвердило окончательный проект «Паноптикума», несмотря на рвение Бентама (он даже предлагал себя на должность надсмотрщика, при этом будучи готовым работать бесплатно). Однако, по иронии судьбы, через несколько десятков лет сам Лондон стал одной из наиболее «просматриваемых» столиц мира: более чем 10 тыс. общественных камер слежения и гораздо большее количество частных, установленных хозяевами гостиниц, магазинов, домовладельцами.

В 1998 г. на Манхэттене насчитывалось около 2400 государственных и частных камер, и этот показатель резко рванул вверх, когда начали падать цены на видеотехнику. Министерство национальной безопасности США выделило сотни миллионов долларов на приобретение видеокамер в целях борьбы с терроризмом. Однако существующее положение дел, хотя бы в отношении уличной преступности, с трудом подтверждает то, что весь этот мониторинг действительно повышает безопасность.

Видеонаблюдение — только верхушка айсберга. В статьях этого номера журнала описано все многообразие технологий, многократно увеличивших наши возможности поделиться информацией о себе — и возможность шпионить за нами. Известный фантаст Дэвид Брин (David Brin) в своей книге *Transparent Society* («Прозрачное общество») доказывает, что современная концепция приватности исторически преходяща и устаревает столь же стремительно, как развиваются новые технологии. По его мнению, вместо того, чтобы изо всех сил пытаться сохранить свои секреты, мы должны сосредоточиться на предотвращении злоупотребления нашей личной информацией, настаивая на том, чтобы каждый, включая глав государств, был равно «открытой книгой».

Насколько успешно эта стратегия будет работать на практике — пока спорный вопрос. Несомненно то, что мы уже пользуемся новой открытостью. Миллионы людей публикуют самые интимные факты своей жизни на сайтах социальных сетей наподобие *FaceBook*, *MySpace*, или «Одноклассники» и «ВКонтакте» в Рунете. Некоторые компании успешно убеждают своих клиентов делиться частной информацией в обмен на услуги. В 1948 г. всезнающий Большой Брат Оруэлла был тоталитарным кошмаром; 60 лет спустя «Большой Брат» — название всемирного телевизионного реалити-шоу.

Существующее положение вещей нельзя назвать однозначно плохим. Думается, в первую очередь нам нужно понять не то, делает ли нас изменение понятия приватности более или менее счастливыми или защищенными. Главная проблема в том, что мы сталкиваемся, по вышеприведенному утверждению Бентама, с новой разновидностью «господства ума над умом». Заставит ли нас вечное подозрение, что кто-то следит за нами, злоупотребляет нашими тайнами, пожертвовать свободой ради того, чтобы быть собой и действовать по своему желанию? А когда приватность исчезнет, не прореагируем ли мы на это, спрятавшись от самих себя? ■

ОПРЕДЕЛИМСЯ С ТЕРМИНАМИ: ПРИВАТНОСТЬ

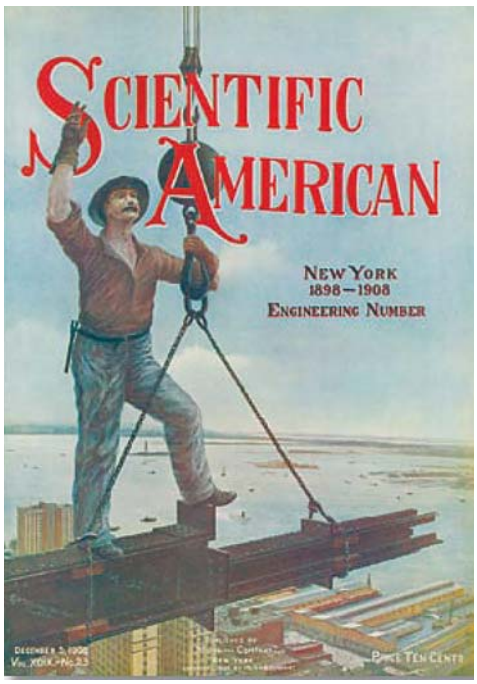
Слово «приватность», несмотря на то что выглядит вполне современно, было заимствовано в русский язык еще в XIX в. Происходит оно от лат. *privatus* — «частный, неофициальный». Словарь иностранных слов, изданный в 1992 г., маркирует это слово как устаревшее. Это легко можно объяснить историей России XX в., когда в рамках советской идеологии подобному понятию места не было. В начале же XXI в. и само понятие, и круг проблем, связанных с ним, стали актуальными и для нашей страны. Так слово «приватность» обрело в русском языке второе дыхание. Мы используем в этом номере слово «приватность», потому что оно емче и полнее со смысловой точки зрения, нежели все другие варианты обозначения этого понятия («конфиденциальность», «частная сфера» и т.д.). Приватность — это и сама личная жизнь человека во всем многообразии ее проявлений, и антоним публичности, и право человека на неприкосновенность его частной сферы.

■ УНИВЕРСАЛЬНОЕ ПОВЕДЕНИЕ ■ АЭРОПЛАН ДЛЯ ЭНТУЗИАСТОВ ■ СВЕЧА ГОРЕЛА ■

ДЕКАБРЬ 1958

ЭВОЛЮЦИЯ ПОВЕДЕНИЯ. «Возможно ли, что в основе всех индивидуальных вариаций поведения лежит некая внутренняя структура унаследованного поведения, характеризующая всех представителей данного вида, рода или более широкой таксономической группы, — в точности так же, как скелет первобытного предка определяет сложение и структуру всех современных млекопитающих? Да, это возможно! Позвольте мне привести пример, который, будучи на первый взгляд тривиальным, тем не менее имеет большое значение для этого вопроса. Каждый, кто наблюдал, как чешется собака, или как птица чистит перья, мог заметить, что они делают это одинаково. Птица, как и собака, тоже использует заднюю конечность (т.е. лапку), опуская крыло и протягивая лапку поверх плеча. Очевидно, что птице было бы проще достать конечностью головы напрямую, не двигая крылом, которое можно сложить и закинуть на спину, чтобы оно не мешало. Я не вижу иного объяснения этого неуклюжего действия, кроме допущения того, что оно врожденное» — Конрад Лоренц.

(*Лоренц получил Нобелевскую премию 1973 г. по физиологии и медицине совместно с Николасом Тинбергеном и Карлом фон Фришем.*)



НАВОДЯ МОСТЫ: создание связи между островом и большой землей, 1908 г.

РОБОТ-ПРЕПОДАВАТЕЛЬ. Может ли быть механизирован процесс обучения? Беррес Скиннер (Burrhus F. Skinner), профессор психологии в Гарварде, считает, что в условиях роста во всем мире спроса на образование это должно произойти. Он лично спроектировал и собрал несколько «обучающих машин», которые не только показывают материал студенту (как делают обычные аудиовизуальные устройства), но и постоянно тестируют его, проверяя степень усвоения информации. Скиннер и его коллеги использовали эти механизмы для преподавания части курса «Поведение человека» более чем 200 студентам Гарварда и Радклиффа.

ДЕКАБРЬ 1908

ВОЗДУШНАЯ БАРЫШНЯ. Известный бразильский экспериментатор Альберто Сантос-Дюмон создал очередную версию своего миниатюрного аэроплана. Чтобы улучшить поперечную остойчивость летательного аппарата, авиатор укрепил крылья под легким двугранным углом, а место пилота и мотор расположил примерно метром ниже. Подобная конструкция позволяет перенести центр тяжести под опорную линию. Размах крыльев моноплана — около 5 м. Небольшие размеры машины, которую изобретатель окрестил *Demoiselle* (фр. «барышня»), позволили Сантос-Дюмону доставить ее из Парижа на поле Сен-Сир, где должен был состояться полет, на автомобиле.

ПРЕОДОЛЕТЬ ИЗОЛЯЦИЮ. Проблему транспортных перевозок в Нью-Йорке делает чрезвычайно сложной и дорогостоящей тот факт, что на длинном узком острове, отделенном от материка широкими и глубокими реками, живут 2 млн человек и примерно столько же каждый день прибывают или отбывают. Выходом из ситуации станет построение по общественной и частной инициативе не менее 14 туннелей и трех мостов — одних из самых масштабных большепролетных мостов мира.

ДЕКАБРЬ 1858

СВЕТ ВО ТЬМЕ. Свечи — одно из самых ранних изобретений наших предков, и несмотря на существование горючего, газа и нефти, они все равно занимают свое заслуженное место среди осветительных приборов: роскошь для богачей, благословение для бедных. Однако хлопот с ними не оберешься: они жирны, коптят, часто гаснут, на них постоянно образуется нагар. Мы хотим представить изобретение, которое поможет избегнуть этих бед: запатентован метод упрочнения обычных свечей, так что они во всем становятся подобны самым дорогим спермацетовым свечам. Специальное покрытие, плавящееся при гораздо более высокой температуре, чем жир, позволяет горящей свече сохранять форму и предотвращает погасание.

СЛОНЫ-РАБОЧИЕ. Газета «Цейлонский обозреватель» сообщает, что губернатор сэр Генри Уорд (Henry Ward) недавно посетил кирпичные заводы. Они находятся примерно в 9,5 км от Коломбо и производят около 20 тыс. кирпичей в день. Глиняную массу для кирпичей готовят слоны. И дикие, и ручные животные работают вместе, при этом и те, и другие пытаются увиливать от работы, стремясь поставить ноги в свои старые следы вместо того, чтобы месить вязкую глину. ■

ВЫШЕЛ ИЗ ПЕЧАТИ ОЧЕРЕДНОЙ НОМЕР ЖУРНАЛА «НАУКА И ЖИЗНЬ»

ТЕМАТИКА СТАТЕЙ НОМЕРА, КАК ВСЕГДА, ШИРОКА И РАЗНООБРАЗНА

■

Археологические раскопки в древнем Новгороде, которые ведутся уже много лет под руководством академика В.Л. Янина, приносят все новые и новые открытия. И не только в истории, в том, что касается уклада жизни наших предков и взаимоотношений между людьми, но и в лингвистике. Каждую осень вот уже более 20 лет в МГУ с публичной лекцией выступает известный лингвист, специалист в области современной и исторической грамматики русского языка, сравнительного и общего языкознания академик А.А. Зализняк. Свои ставшие традиционными лекции он посвящает расшифровке берестяных грамот, найденных в новом сезоне. Слушатели — а это не только студенты и аспиранты, но и все, кому интересно заглянуть в далекое прошлое, — становятся участниками захватывающего процесса, приобщиться к которому имеют возможность и читатели журнала «Наука и жизнь».

Ст. «Берестяные “окна” в прошлое»

■

Можно ли научится летать на самолете, которого еще нет? Да, с помощью авиационного тренажера, который и помогает летчику заранее освоить новую модель, и позволяет инженерам и конструкторам внести в проект необходимые изменения. Работа над созданием авиационных тренажеров началась в СССР более 40 лет назад. Но, несмотря на отдельные успехи, советские тренажеры в целом заметно уступали зарубежным образцам. Сейчас Центральный аэрогидродинамический институт (ЦАГИ) осуществляет разработки совместно с Центром научно-технических услуг «Динамика», и у нас появилась возможность создавать технику, конкурентоспособную на мировом рынке.

Ст. «В небо, не отрываясь от земли»

■

Характер эпидемии СПИДа в России изменился. Хотя темпы распространения эпидемии снизились, поводов для тревоги не убавилось: выйдя из когорты «грешников», болезнь начала поражать социально благополучную молодежь. Если сначала вирус распространялся в основном среди потребителей инъекционных наркотиков, то сейчас в эпицентр эпидемии все больше втягиваются молодые люди, не употребляющие наркотики и не вовлеченные в коммерческий секс.

Ст. «СПИД в сегодняшней России»

■

«Семейные хроники и родословная кланов — это моделирование исторической России. Осмысление ее прошлого и настоящего. Попытка понять смысл жертв». Эти слова — о вышедшей в издательстве «Вече» книге Игоря Шумейко «Голицыны и вся Россия», в которой авторитетный литературовед Лев Аннинский увидел не просто сборник биографий представителей известного дворянского рода, но поиск исторических корней, восстановление связей между прошлым и настоящим.

Ст. «Русь — взгляд из-под голицы»

ISSN 0028-1263

НАУКА И ЖИЗНЬ

12 2008

● Не удивительно ли: ботаники каждый год открывают около двух тысяч новых видов растений! ● Рынок — кризис — государство: уравнение с тремя неизвестными ● Гипотезы, предположения, факты: в истории остаётся только культура, остальное сгорает ● Осторожно: пребывание человека в разрежённом воздухе гор губительно влияет на мозг ● Растительное масло: знакомство продолжается ● Чудеса света: 1 + 6 и другие.

■

Загадочной и опасной представлялась нашим предкам Красная планета, названная Марсом в честь древнеримского бога войны. Во многом неразгаданной она остается и сегодня. Не ясен, например, вопрос, вынесенный в заголовок статьи:

«Есть ли вода на Марсе?».

■

Совсем недавно качество растительного масла определяли лишь по двум показателям: мутное или прозрачное, есть осадок или нет. Современному покупателю несравненно тяжелей, ибо полки магазинов уставлены множеством стеклянных и пластиковых бутылок с разными видами растительного масла.

О вкусовых, кулинарных и полезных свойствах растительных масел, а также о некоторых уловках производителей, каждый из которых утверждает, что его масло «самое лучшее и качественное», читайте в статье

«Кашу маслом не испортишь?».

■

Электронная версия ISSN 1683-9528 представлена в сети Интернет, ежемесячно регистрируется более 60 000 обращений.
Адрес редакции: 101990, Москва, Центр, ул. Мясницкая, д. 24. Тел.(495) 624-1835, факс (495) 625-0590.
Служба распространения и связей с общественностью: Ю.А. Сигорская — (495) 621-9255. Рекламная служба: (495) 628-5965.
http://www.nkj.ru, e-mail: mail@nkj.ru.
Продолжается подписка на журнал «Наука и жизнь». Подписные индексы: 70601, 79179, 99349, 99469, 34174.

ЕГЭ стал обязательным

Эксперимент по введению Единого государственного экзамена (ЕГЭ), который длился восемь лет, завершился. Теперь тестовая система оценки знаний школьников переходит в «штатный» режим и будет реализована, как это предписано в законе

А.А. Фурсенко и Л.Н. Глебова

ЕГЭ с самого начала был болезненным почти для всех: школьников, их родителей, педагогов. Были беспокойства, сомнения, действительно ли нужна тестовая оценка знаний детей. «Пути назад нет», — заявил министр образования и науки А.А. Фурсенко, открывая в октябре заседание коллегии Минобрнауки России, посвященной подведению итогов проведения ЕГЭ в 2008 г. и планам его организации в 2009.

Что же ожидает выпускников? В форме ЕГЭ они будут сдавать два обязательных экзамена: по русскому языку и математике. Остальные могут выбирать — сдавать в традиционной форме или ЕГЭ. Опыт проведения Единого государственного есть уже по 13 предметам. Если раньше экзамены начинались в середине мая, то теперь они будут проходить 25 мая, что позволит не нарушать образовательный процесс.

По заявлению руководителя Федеральной службы по надзору в сфере образования и науки Л.Н. Глебовой, система ЕГЭ стала хорошим инструментом измерения состояния школьного образования, способностей учеников, уровня подготовки специалистов. Например, до сих пор не совсем ясно, как следует проводить итоговую аттестацию, и как вузы будут использовать ее результаты при приеме студентов. Нельзя назвать совершенными тестовые задания или контрольно-измерительные материалы (КИМ). Продолжается работа над тем, чтобы сделать их менее формальными, более эффективными. Обсуждается возможность введения альтернативных, компетентностных КИМ, выявляющих способности выпускников. Пока начат такой эксперимент с экзаменом по математике, на очереди остальные предметы.

Другая проблема связана с двоечниками, которых, как показала практика, немало. Если раньше действовало правило «плюс один балл», то теперь подобных поблажек не будет. Правда, неуспевающие все же будут иметь шанс исправить ситуацию. При получении одной двойки по общеобразовательному предмету они могут пересдать экзамен в дополнительные дни. Если и во второй раз не удастся получить положительную отметку, то вместо аттестата им выдадут лишь справку об обучении в общеобразовательной школе. При получении двух двоек выпускник не допускается к пересдаче. Снова сдавать экзамены можно будет только через год. Поступать в государственные вузы двоечники не смогут — ни на бюджетные места, ни на платные. Возможность учиться у них будет только в учреждениях начального профессионального образования.

Больше внимания станут уделять школьникам с ограниченными возможностями здоровья. В частности, разработаны КИМ для детей с глубокими нарушениями зрения — для этого используется шрифт Брайля. Позаботились и о специалистах, участвующих в процессе проведения ЕГЭ: если раньше их собирали и готовили на федеральном уровне, то теперь они смогут учиться на местах, в субъектах РФ. Особая ситуация с победителями олимпиад: они будут иметь возможность поступать в профильные вузы либо на льготных условиях, либо без экзаменов.

Заседание коллегии, по словам А.А. Фурсенко, было принципиальным — прозвучали критические замечания, предложения. Многие из них будут учтены при подготовке документов, а с нового года начнется новый этап, когда ЕГЭ будут сдавать все выпускники.

Фирюза Янчилина

КАК УЛУЧШИТЬ образование?

Инженерное образование в России — непреходящая ценность, а его качество — основа будущего технологического процветания страны. В связи с реформированием системы образования во время мирового финансового кризиса уровень обучения в высших технических учебных учреждениях выходит на первый план. Острейшие проблемы втузов, пути их решения, новые подходы и перспективы сотрудничества обсуждались на международной научно-методической конференции «Управление качеством инженерного образования и инновационные образовательные технологии» в МГТУ им. Н.Э. Баумана.

В конференции приняли участие преподаватели более 30 университетов России и Украины, представители Федерального агентства по образованию, Федеральной службы по надзору в сфере образования, представители промышленности и бизнеса. Всех волновал вопрос низкого уровня подготовленности выпускников технических университетов. Открывая конференцию, проректор по учебной работе МГТУ им. Н.Э. Баумана Е.Г. Юдин напомнил факт практически полного отсутствия наших вузов в международных рейтингах университетов мира. При этом наше государство вкладывает немалые деньги в сферу высшего образования, лаборатории вузов оснащаются самым лучшим современным оборудованием.

По мнению некоторых докладчиков, одно из объяснений — в отсутствии у студентов мотивации хорошо учиться. В советское время управлять качеством учебы можно было в том числе с помощью стипендии. Успешно сдавшие экзамены получали неплохой ежемесячный доход, на который можно было жить. Сейчас стипендии настолько маленькие, что они не могут быть стимулом для молодых людей. Кроме того, во всех вузах много «платников», т.е. обучающихся на собственные средства. Поэтому нужно искать другие рычаги управления качеством учебы.

Заслуженный профессор Казанского технического университета (КГТУ) Ю.Е. Польских и другие сотрудники вуза предложили ввести кроме экзаменов еще и тестовую (по типу ЕГЭ) оценку знаний студентов после первого и второго уровня обучения. Это позволит обеспечить вариативность и мобильность образования. Главная проблема — составить вопросы, по ответам на которые можно было бы судить, насколько хорошо будущий инженер владеет знаниями, необходимыми в его профессии, и умеет ли он их применять на практике. По итогам оценок руководство любого профильного предприятия может понять, действительно ли нужен тот или иной молодой специалист. Немаловажный вклад в «цену» выпускника внесет и так называемый психологический портрет. Такой портрет психологи могут составить также на основе специальных тестовых заданий.

Генеральный директор Института испытаний и сертификации вооружений и военной техники И.Н. Животкевич обратил внимание, что наши вузы дают студентам общие знания, и затем выпускники идут работать не совсем по специальности. А американские и европейские технические университеты готовят специалистов для конкретных крупных предприятий. Нашим вузам не мешало бы хотя бы частично позаимствовать такой опыт.

Конференция была своевременной и плодотворной. По заверению организаторов, подобные мероприятия будут проходить регулярно, что позволит участникам обмениваться опытом и повышать уровень образования в технических вузах.

Фирюза Янчилина

ЕЩЕ ОДИН ГЕН болезни Альцгеймера

Выявленная недавно генетическая мутация повышает риск возникновения самой распространенной формы болезни Альцгеймера — это уже второй ген, связанный с данным нейродегенеративным состоянием.

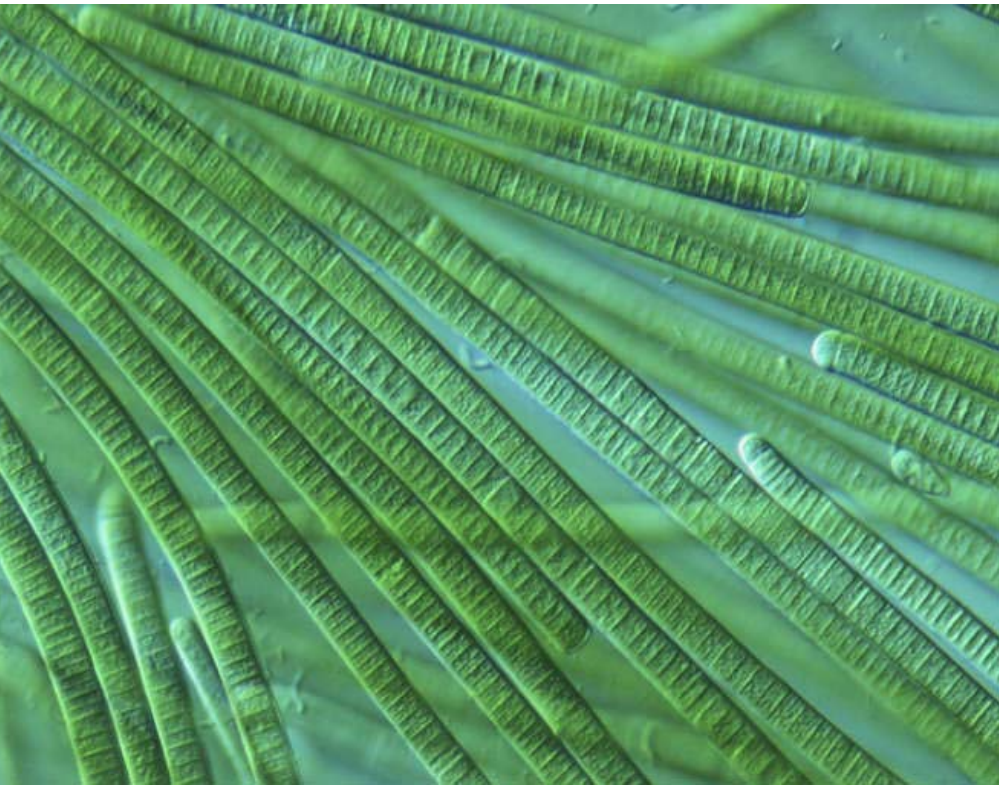
Мутация происходит в гене *CALHM1*, который управляет концентрацией кальция в нервных клетках. Исследователи наблюдали, что мутантный ген приводил к усилению образования бета-амилоидных бляшек — клейких сгустков белка, характерных для данного недуга.

В США болезнь Альцгеймера поражает одного из 20 взрослых людей в возрасте от 65 до 74 лет; обладание одной дефектной копией гена *CALHM1* повышает риск до 1/14 (и до 1/10 для тех, кто несет две дефектные копии). Мутация также ведет к возникновению заболевания в более раннем возрасте.

Ген *CALHM1*, как и первый ген болезни Альцгеймера, *APOE*, открытый 15 лет назад, будет иметь большое значение при скрининге на предрасположенность к данному заболеванию.

Барбара Джункоза

ЦИАНОБАКТЕРИИ В УСЛОВИЯХ ВЫСОКОГОРЬЯ



В связи с глобальными изменениями климата высокогорные ледники сегодня быстро тают во многих регионах мира, в том числе и в Андах.

В условиях высокогорья на обнажившихся после таяния ледников участках видимая невооруженным глазом растительность (лишайники и мхи) появляется лишь спустя десятилетия. В течение такого длительного времени освобожденная из ледяного плена поверхность выглядит совершенно безжизненной. Тем не менее определенные процессы на ней происходят и в конце концов она становится пригодной для жизни растений.

В результате таяния высокогорных ледников обнажаются участ-ки земной поверхности, которые были покрыты льдами в течение многих тысячелетий. На этих участках со временем развивается богатая микробная жизнь. Исследование, проведенное Андах в Перу, показало, что ключевую роль в микробных сообществах играют цианобактерии (сине-зеленые водоросли). Микробы постепенно насыщают почву органикой и азотом, подготавливая ее для заселения растениями.

Ранние «дорастительные» этапы развития экосистемы в подобных местах изучены пока слабо. Группа американских исследователей под руководством Стива Шмидта (Steve Schmidt) из Колорадского университета в Боулдере изучила жизнь на поверхностях, обнажающихся в ходе таяния ледников в высокогорьях Анд (в Кордильере-де-Вильканота, на юго-востоке Перу, на границе департаментов Куско и Пуно, в 80 км к юго-востоку от города Куско).

Имеющиеся сведения позволили ученым предположить три возможных механизма постепенного превращения стерильного грунта в почву, пригодную для растительной жизни.

Согласно первой гипотезе, основой для развития жизни становится древняя органика, сохранившаяся в грунте еще с доледниковых времен. В этом случае первыми массовыми обитателями образующихся почв должны быть гетеротрофные (питающиеся готовой органикой) микроорганизмы.

Вторая гипотеза предполагает, что органика попадает сюда вместе с пыльцой, спорами низших растений и грибов и другими мелкими объектами органической природы, разносимыми ветром. Согласно этой версии, первопоселенцами высокогорных пустынь тоже должны быть гетеротрофные микробы, питающиеся занесенной ветром органикой.

Наконец, третья гипотеза предполагает, что на освобожденных из-подо льда безжизненных участках могут развиваться автотрофные (фотосинтезирующие, производящие органику из углекислого газа и воды) микробы, в первую очередь цианобактерии. Именно эти микроорганизмы и играют главную роль в постепенном обогащении высокогорных почв.

Разумеется, перечисленные гипотезы не являются взаимоисключающими, все три механизма могут работать одновременно, вопрос лишь в том, какой из них важнее.

Ученые также обнаружили, что вышедшие из-под ледника грунты со временем становятся менее сыпучими и более прочными. Скорее всего, это тоже объясняется активностью цианобактерий.

Известно, что подобные микробы выделяют большие количества клейких веществ, которые могут скреплять частицы грунта. Таким образом, цианобактерии не только обогащают почву питательными веществами, но и защищают ее от эрозии.

Михаил Молчанов
(По материалам Elementy.ru)

РАННЕЕ НАСТУПЛЕНИЕ ВЕСНЫ

Глобальное потепление развивается так быстро, что многие животные и растения оказываются плохо приспособленными к уже изменившимся условиям. Так, в Западной Европе весна по фенологическим признакам (например, распускание листьев на определенных породах деревьев) начинается в среднем на 12–14 дней раньше, чем 40–50 лет назад. Вместе с тем известно, что многие сезонные явления в жизни растений и животных настроены не на изменения температуры, а на изменения длины светового дня — фотопериод.

Подробные данные о биологии синиц в лесу Уайтэм близ Оксфорда свидетельствуют, что за 47 лет наблюдений (с 1961 по 2007 г.) самки большой синицы (*Parus major*) стали откладывать яйца на 14 дней раньше. Если же сравнить средний срок откладки яиц и количество тепла, полученного в тот или иной год за весну (сумму максимальных за день температур для периода с 1 марта по 25 апреля), то выясняется, что величины эти демонстрируют четкую корреляцию: чем теплее весна, тем раньше синицы приступают к размножению.

Стратегия сдвига сроков размножения на более раннее время оказывается жизненно важной, так как выкармливающие птенцов родители могут застать обилие гусениц, составляющих основную часть их добычи. В окрестностях Оксфорда важную роль в составе пищи, приносимой родителями птенцам, играют гусеницы зимней пяденицы (*Operophtera brumata*).

Дата максимума биомассы гусениц за многолетний период наблюдений тоже сместилась на более ранние сроки, и, как в случае со средней датой откладки синицами яиц, выявляется четкая корреляция ее с суммой температур за март-апрель. Не удивительно, что положительная корреляция обнаруживается также между датой максимума биомассы гусениц и средней датой откладки яиц большой синицей.

Ученые пришли к выводу, что наблюдаемое смещение сроков размножения в популяции синиц из леса Уайтэм объясняется не естественным отбором, а индивидуальной пластичностью в поведении особей. В пользу такого предположения свидетельствует то, что одни и те же птицы, размножающиеся более одного сезона, меняют дату откладки яиц в зависимости от того, насколько теплая стоит весна. Расчет сдвига средних дат и даты откладки яиц показывает, что скорость его изменения за 47 лет слишком велика, чтобы ее можно было объяснить отбором в популяции, где средняя длительность генерации — около двух лет. Выявление индивидуальной изменчивости по признаку даты откладки яиц показывает, что она незначительна. Другими словами, все особи ведут себя более или менее сходно.

Михаил Молчанов
(По материалам Elementy.ru)

ТОВАРИЩИ ПО ИГРАМ КАК ИСТОЧНИК ЗАРАЗЫ

Всем родителям хорошо известно, что в детских садах и школах дети легко заражаются друг от друга респираторными заболеваниями. По всей видимости, то же самое происходит и у шимпанзе: согласно результатам новых исследований, совместные игры детенышей способствуют распространению инфекции.

Ученые под руководством Хьялмара Кюля (Hjalmar Kuehl) и Петера Валша (Peter Walsh) из Института эволюционной антропологии им. Макса Планка в Лейпциге, Германия, исследовали две группы шимпанзе в национальном парке Тай в Кот-д'Ивуаре. Чем больше малыши играли вместе, тем они были более подвержены гибели от респираторных заболеваний (обычно это происходит во время сезона массового созревания плодов, когда животные собираются вместе). В возрасте от двух до трех лет приматы проводят до 18% времени дня в тесном физическом контакте со своими сверстниками. Данный период является пиком их социального взаимодействия и способствует сплочению членов группы.

Как только среди играющих совместно шимпанзе начиналась вспышка заболевания, его подхватывали детеныши всех возрастов. Смертность среди малышей в совокупности с браконьерством, изменением климата и давлением хищников стала серьезным бременем для местной популяции шимпанзе, отмечает Кюль, исследование которого опубликовано в июньском выпуске *PLoS ONE*. По его словам, в наши дни лишь немногим из детенышей удается достичь взрослого возраста, при этом «лишь четверо из десяти доживают до пяти лет».

Барбара Джункоза

СОВМЕСТНЫЕ ИГРЫ помогают социальному развитию шимпанзе, но они же способствуют распространению инфекции

Дело о приматах

Решение, принятое в Швейцарии по соображениям этики, приведет к закрытию ряда фундаментальных исследований мозга

СЛИШКОМ ПОХОЖИ НА ЛЮДЕЙ? Экспериментаторы ценят макаков резусов за их сходство с людьми. По всей видимости, нейробиологи из Швейцарии вскоре уже не смогут проводить на них фундаментальные исследования

Вопрос об использовании наших собратьев-приматов для проведения научных экспериментов остается одним из самых спорных в нейробиологии. Они сходны с человеком по своим когнитивным способностям, сложности социальной организации и нейроанатомии и благодаря этому могут служить хорошей моделью для изучения мозга. Однако по этим же самым причинам у многих приматов возникает желание окружить особой заботой. За последние годы в европейских странах принимались все более строгие правила проведения экспериментов с приматами, что заставляет многих нейробиологов опасаться за будущее своих исследований. Швейцарский Верховный суд может вскоре создать самый жесткий прецедент, что вызывает беспокойство у всего мирового сообщества исследователей мозга.

В 2006 г. два исследователя из Швейцарского института нейроинформатики в Цюрихе Даниэль Кипер (Daniel Kiper) и Кеван Мартин (Kevan Martin) подали в местную ветеринарную службу документы для продления лицензии на проведение экспериментальной работы с обезьянами (ученые уже неоднократно проходили эту рутинную процедуру, повторяющуюся раз в три года). Кипер предлагал изучить, как изменяется мозг животного, когда оно приобретает новые навыки: такие данные могли помочь больным, перенесшим инсульт. В ходе экспериментов обезьянам планировалось имплантировать электроды и ограничивать потребление ими воды. Мартин, возглавляющий институт, собирался изучать на макаках связи в неокортексе, которые обеспечивают выполнение таких высших функций, как пространственное воображение и сознательное мышление. В его исследованиях предусматривалось вводить животным специальные вещества-метки и затем усыплять их.

Ветеринарная служба одобрила продление лицензии, однако Комитет по экспериментам на животных выразил протест в связи с тем, что ожидаемые блага для человеческого общества недостаточны для оправдания бремени, возлагаемого на приматов. В результате комитет обратился в швейцарское Министерство здравоохранения, которое обязало исследователей прекратить проведение экспериментов.

Тем временем заявка, поданная другим ученым из того же института Гансом Шербергером (Hans Scherberger), использующим приблизительно такие же методики, как и Кипер, но изучающим способности мозга управлять движениями руки, была одобрена и не вызвала протеста. «Заявки различаются, — настаивает президент комитета Клаус Петер Риппе (Klaus Peter Rippe) и объясняет: — В экспериментах Шербергера разрабатываются нервные протезы, имеющие очевидную связь с благосостоянием человечества. Заявки на проведение экспериментов Кипера и Мартина недостаточно конкретны, и пройдет слишком много времени, прежде чем они смогут принести обществу пользу».

Кипер и Мартин согласны с тем, что их исследования не дадут немедленных результатов, однако они замечают, что работают ради лучшего понимания работы мозга, а это та основа, отталкиваясь от которой можно будет искать методы лечения различных заболеваний, в том числе болезни Альцгеймера или Паркинсона.

Кипер и Мартин обратились в Цюрихский административный суд, однако, к их удивлению, в своем решении от 27 марта 2008 г. суд поддержал исходный протест, сославшись на эволюционную близость макаков к людям и их когнитивные способности. Суд постановил, что долговре-

менный характер поставленных целей и неопределенность практической выгоды делают проведение данных исследований неприемлемым.

Для многих ученых такое решение означает, что результаты экспериментов на приматах должны приносить пользу обществу не позже, чем через три года (такова длительность периода лицензирования). Таким образом, любые фундаментальные исследования де-факто попадают под запрет. «Это антинаучно, — заявляет Кипер, — Так проявляются недоверие к ученым и отсутствие уважения к научному прогрессу в целом». Цюрихский университет и Федеральный технологический институт Цюриха, совместно основавшие Швейцарский институт нейроинформатики, в настоящее время обращаются в Федеральный Верховный суд — высшую судебную инстанцию в стране.

Данный случай укладывается в русло проявившейся недавно в Европе тенденции к установлению все более строгих правил проведения экспериментов на животных. Примечательно, что в сентябре 2007 г. в Европейский парламент была подана петиция, требующая остановить все эксперименты на приматах, и ее поддержали более половины парламентариев. Несмотря на то что Европейская комиссия отклонила петицию, уровень политической поддержки в ее пользу обеспокоил ученых, которые боятся, что предстоящий пересмотр правил серьезно осложнит проведение их исследований.

Лизи Бухен

ПЕРЕМЕЩЕНИЕ ГЛАЗ КАМБАЛООБРАЗНЫХ

Причудливая метаморфоза, произошедшая с палтусом и другими камбалообразными рыбами, озадачивала самого Чарлза Дарвина. В момент своего рождения эти рыбы имеют по одному глазу с каждой стороны черепа, однако по мере взросления оба ока оказываются на одной стороне. Очевидно, что для них, проводящих всю свою жизнь на морском дне, расположение обоих глаз на верхней стороне тела дает преимущества в выживании. Однако казалось, что не существует таких причин, которые подтолкнули бы эволюцию к формированию подобной односторонности: любые промежуточные стадии вряд ли приносили бы пользу. Некоторые биологи полагали, что эти рыбы возникли в результате резкой мутации.

Видимо, все происходило по-другому: Мэтт Фридман (Matt Friedman) из Полевого музея в Чикаго сообщает о находке недостающих звеньев. Он исследовал двух ископаемых примитивных камбалообразных рыб возрастом примерно в 50 млн лет, которые более ста лет пролежали в европейских музеях. Взрослые особи обладали немного асимметричными черепами, однако глаза у них все равно располагались по обеим сторонам головы. Видимо, даже неполная односторонность давала хищным обитателям дна лучший обзор мира по сравнению с полным отсутствием асимметрии, заключает Фридман. Читайте об этом исследовании в июльском выпуске *Nature*.

ГЛАЗАМИ ВВЕРХ: у камбалы и других родственных ей обитателей дна оба глаза расположены на одной стороне черепа

Чарлз Чой

НОВЫЙ КАМЕННЫЙ ВЕК

В XXI веке из-за глобального потепления климата у людей будут чаще образовываться камни в почках, заявляет Том Бриковски (Tom H. Brikowski) из Техасского университета в Далласе. Камни образуются при кристаллизации минеральных веществ, растворенных в моче, а недостаток жидкости способствует данному процессу. Такая дегидратация организма чаще происходит во время жары; например распространенность почечнокаменной болезни в юго-восточной части США на 50% выше, чем в северо-западном регионе страны, а у некоторых американских солдат, заброшенных в пустыню, камни в почках возникали уже через 90 дней. Учитывая ожидаемый подъем средней температуры в США (на 2–5° С в этом столетии) исследователи подсчитали, что к 2050 г. в стране будет на 1,6–2,2 млн больше пациентов с этим заболеванием. Такой прирост на 7–10% может вылиться в $1,3 млрд расходов на медицинское обслуживание. Результаты исследования опубликованы в июльском выпуске *Proceedings of the National Academy of Sciences USA*.

НА ПОПЕРЕЧНОМ СРЕЗЕ ПОЧКИ видны камни и образовавшиеся вокруг них полости

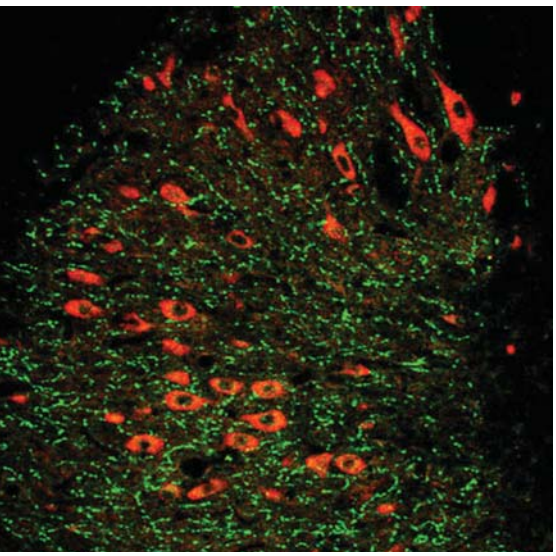
Филип Ям

ПЕРВЫЙ В СВОЕМ КЛАССЕ

Неудачный дебют заменителя никотина лишает надежды на его широкое применение

Весной 2008 г. Федеральное управление гражданской авиации США (*Federal Aviation Administration*) запретило пилотам и авиадиспетчерам принимать популярное средство для избавления от табачной зависимости — варениклин, продаваемое в США под названием *Chantix*. Несмотря на то что по всему миру за период с 2006 г. данный препарат был назначен 6,5 млн раз, широкий резонанс получили сообщения о том, что на фоне его приема возникали острые нарушения психики, включая эпилептические приступы, психозы и суицидальную депрессию. В мае некоммерческий Институт безопасной медицинской практики документировал 988 случаев таких «нежелательных явлений», что и послужило основанием для запрета на его использование сотрудниками авиации.

Управление по санитарному надзору за качеством пищевых продуктов и медикаментов США (*FDA*) добавило в инструкцию к вареникклину соответствующее серьезное предупреждение, а *Pfizer* (компания-производитель) в настоящее время ищет объяснение этим редким, но тяжелым случаям. Несмотря на то что плохая репутация может снизить продажи средства, наблюдатели отмечают, что ничего неожиданного в наличии нежелательных побочных эффектов у нового препарата нет. Вареникклин — не просто новое средство, помогающее бросить курить; это первое вещество в целом классе лекарств, специально разработанных в расчете на одну важную группу рецепторов. Никотиновые ацетилхолиновые рецепторы, располагающиеся на клетках мозга, влияют на восприятие боли, настроение, память, внимание и другие когнитивные функции.



НИКОТИНОВЫЕ РЕЦЕПТОРЫ (*красного цвета*) на поверхности клеток мозга служат мишенью новых препаратов, направленных на широкий круг когнитивных расстройств

Компании *Abbott Laboratories*, *Targacept* и *AstraZeneca* проводят клинические испытания препаратов, воздействующих на никотиновые рецепторы и направленных на лечение нарушений памяти, синдрома дефицита внимания с гиперактивностью, а также болевого синдрома. Национальный институт наркомании испытывает вареникклин как средство для лечения кокаиновой и алкогольной зависимости. На доклинической стадии находится исследование применения других соединений, воздействующих на никотиновые рецепторы, для лечения болезни Паркинсона, болезни Альцгеймера, депрессии, а также язвенного колита, что говорит о широком спектре функций данного семейства рецепторов.

Влияние никотиновых рецепторов настолько многообразно, что некоторые механизмы их участия еще не совсем понятны. Такой тип ацетилхолиновых рецепторов, которые также реагируют и на никотин, служит своего рода «регулятором мощности» для других нейромедиаторов. Даже небольшое количество никотина включает выделение медиаторов. Было показано, что он усиливает выделение дофамина, глутамата и ГАМК — всех основных нейромедиаторов.

Активация подтипа никотиновых рецепторов, известных как альфа-4бета2, приводит к выделению дофамина в той части мозга, которая обеспечивает подкрепляющее действие вознаграждения, и именно данный рецептор является основной мишенью вареникклина. Препарат действует как частичный агонист: он связывается с рецептором и умеренно стимулирует его, что в свою очередь избавляет от никотиновой абстиненции. Вареникклин не дает самому никотину связываться с этими рецепторами, и в результате сигарета уже не вызывает у курильщика выброса порции дофамина.

Как показали клеточные исследования, вареникклин также действует как мощный полный агонист другого подтипа рецепторов, называемого альфа7, с которым связывают некоторые позитивные стороны воздействия никотина, в том числе улучшение концентрации внимания. Предполагается, что те трудности, которые испытывают больные шизофренией, когда тщетно пытаются перестать обращать внимание на какие-либо либо звуки или иные стимулы, связаны с изменениями в гене, кодирующем альфа7-рецептор.

С учетом сложности нейропсихологических систем, в которых участвуют никотиновые рецепторы, необходимо признать, что большая часть случаев побочного действия вареникклина, возможно, никогда не найдет объяснения. Представители компании *Pfizer* указывают на то, что в самой группе курильщиков тревожность и депрессивные расстройства встречаются чаще и без того. Это означает, что легкое или невыявленное психическое заболевание, существовавшее задолго до этого, может затем внести свой вклад в реакцию на препарат. Более того, такие симптомы, как тревож-

ное возбуждение и суицидальные мысли, являются хорошо известными побочными эффектами табачной абстиненции, отмечает Анджан Чаттерджи (Anjan Chatterjee), медицинский директор компании *Pfizer*:

Антидепрессанты группы селективных ингибиторов обратного захвата серотонина (ИОЗС), появившиеся более 20 лет назад, также вызывали различные нежелательные явления, в том числе суицидальные мысли. Однако первое поколение этих препаратов, к которому принадлежал прозак, приобрело дурную славу даже из-за более безобидных побочных эффектов, в число которых входили нарушения пищеварения и расстройства половой сферы. В последующих поколениях препаратов данной группы удалось избавиться от некоторых побочных действий, встроив в них блокаторы определенных подтипов рецепторов серотонина, чтобы исключить их нежелательное воздействие.

«Как и в случае с серотонином, было обнаружено, что подтипы рецепторов сами разделяются на еще более мелкие подтипы. Я думаю, что со временем появятся никотиновые препараты с более тонким действием», — говорит Эдвард Левин (Edward D. Levin), специалист по фармакологии поведения из Университета Дьюка, выступавший консультантом для компании *Targacept* и для Национальных институтов здоровья США.

Кристин Соарес

БУДУЩЕЕ – за наукоемкими проектами

Актуальным вопросам внедрения научных достижений в области биотехнологий в производственную практику Подмосковья была посвящена конференция «Биотехнология 2008», которая прошла в г. Пущино Московской области.

Всеобщий интерес вызвал доклад о международных проектах заместителя директора Пущинского филиала Института биоорганической химии им. академиков М.М. Шемякина и Ю.А. Овчинникова РАН С.А. Феофанова. В конференции участвовали с российской стороны — президиум Пущинского научного центра (ПНЦ), консорциум «Биомак», МГУ им. М.В. Ломоносова, с немецкой — Агентство будущего земли Бранденбург, Альянс «Наук о жизни» общества Фраунгофера, Союз германских биотехнологических компаний (*VBU*). Один из главных проектов, который активно обсуждался участниками, — «Лесная биотехнология: плантационное лесоводство, возобновляемые источники энергии и окружающая среда». В частности, говорили о станции искусственного климата «Биотрон», расположенной в Пущине, которая помогает решать проблему восстановления вырубленных и выжженных пожарами лесов. В «Биотроне» выращивают сады растений с различными встроенными генами, создающими полезные свойства: сверхсладкости ягод и фруктов, способности к долгому (до нескольких месяцев) хранению помидоров, устойчивости к инсектицидам. Аналогичным способом создают и быстрорастущие деревья. Если обычная ель вырастает в среднем за 80 лет, то генетически модифицированная — за восемь. Однако сегодня проводится лишь селекция быстрорастущих сортов. Трансгеноз, вызывающий немало споров в мире, — следующий этап. Такие деревья будут выращиваться на специально отведенных, огороженных площадях, и перенос генетического материала будет почти исключен.

Проректор НОУ «Международная академия оценки и консалтинга» В.Б. Железный отметил, что в связи с инновационным развитием науки большинство ученых нуждаются в ликбезе по экономике. Многие до сих пор не совсем представляют, как работают, например, венчурные фонды. Процесс внедрения идеи или технологии в производство — сложный, требующий значительных финансовых вливаний. Другая проблема — выход на рынок, грамотная реклама товара. Каждому автору необходимо владеть азами экономических знаний, он должен представлять стадии инновационного проекта. Немаловажно и правильно поставить задачу перед профессионалами, чтобы впоследствии не оказаться обманутым из-за собственной неграмотности. В.Б. Железный также добавил,

что нынешний мировой кризис благоприятствует инновационному развитию: инвесторы начинают обращать внимание на долговременные наукоемкие проекты.

Многие докладчики отмечали опыт других стран. Если в России строительство и запуск бизнес-инкубаторов, технопарков только начинает набирать обороты, то за рубежом уже переходят к следующим этапам. Россия идет по своему пути инновационного развития, и проведение конференций, подобных той, что прошла в Пущине, способствует активному обмену опытом между различными научно-производственными структурами, учеными, представителями бизнеса, власти.

Фирюза Янчилина

НАУКА XXI ВЕКА

В двенадцатый раз в г. Пущино проходила международная школа-конференция молодых ученых «Биология — наука XXI века».

Участники школы-конференции

Приветствуя в Институте биофизики клетки РАН молодых людей, приехавших из разных городов России и ближнего зарубежья, заместитель председателя Пущинского научного центра РАН Е.А. Пермяков подчеркнул, что в последние годы «наметилась тенденция к улучшению состояния отечественной науки». Увеличились зарплаты научных сотрудников, появились деньги на дорогостоящее оборудование. Однако все еще остается проблема пополнения армии ученых молодыми кадрами. Чтобы молодежь хотела заниматься научной деятельностью, необходимо предоставлять ей хорошие условия работы, обеспечивать жильем. Другая проблема связана с понижением уровня образования выпускников вузов. Конференции, подобные той, что проводятся в Пущине, повышают интерес молодежи к научным исследованиям, помогают наладить новые научные и дружеские контакты.

Среди выступавших на школе-конференции были как маститые ученые, так и только начинающие свой творческий путь. Пленарные заседания проводились во многих научно-исследовательских институтах Пущина. Доклад доктора физико-математических наук Н.Н. Хечинашвили был научным, однако результаты исследований, о которых он рассказал, представляют и прикладной интерес. В частности, в настоящее время идет поиск механизмов функционирования белков при высоких температурах. Большинство белков — это ферменты, активность которых возрастает с повышением температуры вплоть до 60–70° С. Некоторые термофильные организмы продуцируют белки, работающие даже в перегретой воде при температуре до 120° С. Перед учеными стоит проблема стабилизации таких веществ, это необходимо при производстве, например, соков, вакцин.

Профессор, доктор биологических наук С.С. Колесников сделал обзорный доклад по основополагающим работам о сенсорных клетках: обонятельных, вкусовых, фоторецепторах. Всех заинтересовал его рассказ о первичных процессах, запускаемых в таких клетках сенсорными стимулами: светом, запахами, вкусовыми веществами. С.С. Колесников отметил, что в живых организмах сенсорные клетки работают на пределе физических возможностей. Причина в непредсказуемости окружающей среды: внешние стимулы могут изменяться с произвольной скоростью, в произвольном диапазоне интенсивности.

О том, как создавался город биологов, рассказала заместитель директора Пущинского музея экологии и краеведения Т.С. Кубасова. В середине прошлого века возникло новое научное направление — молекулярная биология, и Пущино обязано своим появлением во многом именно этой науке. Создатели небольшого, красивого городка отказались от принципа «забирать все у природы, подчинить ее своим интересам», они выбрали путь взаимодействия с миром и бережно встраивали научный центр в окружающий ландшафт.

Сегодня главная задача ученых — восстановить связь поколений, нарушенную в 1990-х гг. Конференции молодых ученых, несомненно, будут этому способствовать.

Фирюза Янчилина

«ЗЕЛЕНОЕ» СТРОИТЕЛЬСТВО В РОССИИ

В отеле «Мариотт Гранд» состоялась конференция на тему экологической устойчивости и энергоэффективности в строительной отрасли

Carrier, подразделение корпорации *United Technologies Corporation* (*NYSE:UTX*), совместно со своим российским партнером компанией *AHI* провели однодневную *Moscow 2008 Green Buildings Conference*, посвященную современным тенденциям, продукции, стратегиям и нормативно-правовому регулированию в области коммерческого строительства. Среди докладчиков — специалисты, работающие в строительной индустрии, и эксперты по экологической устойчивости. Выступая с докладами перед аудиторией из 120 представителей строительной индустрии, они говорили о новых направлениях в российской энергосберегающей политике и о возможности «зеленого» будущего для России

Экологическая устойчивость и энергоэффективность имеют важнейшее значение для правительства, бизнеса и общества в целом. По данным Всемирного предпринимательского совета по устойчивому развитию, не менее 40% энергопотребления в большинстве стран приходятся на долю зданий. Ответственность за состояние окружающей среды и соблюдение принципов энергоэффективности при строительстве зданий стали частью политики корпорации *Carrier* по охране окружающей среды.

По словам Келли Романо (Kelly Romano), президента корпорации *Carrier* по системам и услугам для строительного сектора, корпорация стремится к разработке новой продукции, технологий и ресурсов. Цель — помощь индустрии систем отопления, вентиляции и кондиционирования воздуха в удовлетворении растущих потребностей рынка в экологически чистых высокоэффективных зданиях.

По данным Американского совета по экологии зданий, экологически чистые или «зеленые» здания в среднем потребляют на 40% меньше энергии и на 50% меньше воды, чем их традиционные аналоги. При строительстве «зеленых» зданий используются экологические устойчивые и возобновляемые материалы. Их эффективность повышается в течение всего жизненного цикла здания благодаря улучшенной конструкции, совершенным методам строительства, эксплуатации, обслуживания и сноса. В результате такие здания выделяют в атмосферу значительно меньше парниковых газов, чем обычные дома, качество воздуха внутри их помещений лучше и к тому же они способствуют сохранению природных ресурсов.

«Экологическая устойчивость и энергоэффективность зданий — сравнительно новые для России понятия, — пояснил Д.А. Портанский, директор по связям с общественностью и органами государственной власти московского представительства *United Technologies International Operations*. — В настоящее время российское правительство разрабатывает нормативно-правовую базу для создания благоприятных условий для внедрения энергоэффективных технологий во многих отраслях промышленности, включая и строительный сектор».

Сегодня в России разрабатываются экологически устойчивые здания, которые будут отвечать мировым экологическим стандартам и жестким требованиям, предъявляемым к охране окружающей среды. Россия участвует в многосторонних соглашениях по решению экологических проблем, среди которых изменение климата, сохранение биологического разнообразия и защита озонового слоя. «Обязанность *Carrier* — помочь представителям промышленности в разработке новых экологически устойчивых решений и продукции для строительства зданий высокой эффективности», — считает Келли Романо, президент корпорации.

Павел Худолей

ДЛЯ ЖЕНЩИН В НАУКЕ

12 ноября в отеле «Балчуг-Кемпински» состоялась торжественная церемония награждения десяти молодых российских женщин-ученых национальными стипендиями «Л'Ореаль-ЮНЕСКО». Выделение стипендий на развитие научной карьеры в России молодым женщинам – часть международного проекта компании «Л'Ореаль»

Международная премия «Для женщин в науке» учреждена в 1998 г. ЮНЕСКО и компанией «Л'Ореаль» с целью поддержать женщин, развивающих свою карьеру в науке. Согласно последним данным Института ЮНЕСКО, в науке и технике по-прежнему доминируют мужчины. Во всем мире только одну четверть ученых составляют представительницы слабого пола, примерно 10% университетских профессоров и менее 5% членов академий наук. Среди нобелевских лауреатов менее 5% женщин-лауреаток из 809 награжденных. Преодоление существующих социальных стереотипов позволяет женщинам более успешно строить свои научные карьеры и добиваться значительных результатов. Развивая программу «Для женщин в науке», компания «Л'Ореаль» и ЮНЕСКО стремятся изменить сложившуюся ситуацию. Всего за девять лет более 350 женщин-ученых со всего мира были награждены в рамках программы.

В нашей стране проект осуществляется с 2007 г., партнером выступает Российская академия наук. Стипендии предназначены для женщин-ученых, кандидатов наук в возрасте до 35 лет, работающих в российских научных институтах и вузах по следующим дисциплинам: физика, химия, медицина и биология. Критерии выбора стипендиаток — научная значимость кандидата, практическая польза и осуществимость предложенного на рассмотрение жюри проекта, а также желание кандидата продолжать научную карьеру в России. На первый же конкурс поступило 189 анкет из более чем 40 городов России.

27 ноября 2007 г. в Москве состоялась торжественная церемония вручения стипендий «Для женщин в науке», где были объявлены пять имен победителей. На этом же мероприятии было предложено продолжить программу выделения стипендий для молодых российских женщин-ученых в 2008 г. Большое количество заявок, а также высокий уровень представляемых на конкурс работ побудили организаторов увеличить количество выделяемых грантов.

В этом году за время проведения конкурса было получено более 320 анкет из 65 городов России. Все анкеты были переданы на рассмотрение жюри в следующем составе: академик РАН А.Р. Хохлов (председатель жюри); профессор, доктор физико-математических наук Т.М. Бирштейн; профессор, доктор биологических наук М.С. Гельфанд; академик РАН И.Л. Еременко; член-корреспондент РАН О.А. Донцова; академик РАН В.Е. Фортов.

Стипендии «Л'Ореаль-ЮНЕСКО» присуждены следующим ученым:

- Ирена Игоревна Артамонова (Москва, Институт общей генетики им. Н.И. Вавилова РАН, старший научный сотрудник);
- Софья Борисовна Артемкина (Новосибирск, Институт неорганической химии им. Николаева СО РАН, младший научный сотрудник);
- Евгения Валентиновна Богомолова (Санкт-Петербург, Ботанический институт им. В.Л. Комарова РАН, старший научный сотрудник);
- Оксана Викторовна Калюжная (Иркутск, Лимнологический институт СО РАН, научный сотрудник);
- Галина Викторовна Лукова (Черноголовка, Московская область, Институт проблем химической физики РАН, старший научный сотрудник);
- Анастасия Михайловна Макарьева (Гатчина, Ленинградская область, Отделение теоретической физики, Петербургский институт ядерной физики им. Б. П. Константинова РАН, старший научный сотрудник);
- Екатерина Марковна Мерзляк (Москва, Московский государственный университет им. М.В. Ломоносова, научный сотрудник);
- Лада Николаевна Пунтус (Москва, Институт радиотехники и электроники РАН, старший научный сотрудник);
- Надежда Евгеньевна Устюжанина (Москва, Институт органической химии им. Н.Д. Зелинского РАН, научный сотрудник);
- Анна Александровна Федорова (Москва, Институт космических исследований РАН, старший научный сотрудник).

Павел Худолей

Пятый Всероссийский Форум-выставка

ГОСЗАКАЗ 2009

Москва, март 2009 года

Ежегодное конгрессно-выставочное мероприятие
в области государственных закупок, имеющее федеральный статус

ФОРУМ-ВЫСТАВКА «ГОСЗАКАЗ-2009» – ЭТО ЭКСПОЗИЦИИ

- Федеральных органов исполнительной власти Российской Федерации
- Субъектов Российской Федерации
- Российских и иностранных поставщиков товаров, работ и услуг для государственных нужд

ФОРУМ

- Пленарные заседания, тематические сессии
- Круглые столы по вопросам контроля, нормативного правового регулирования, информационного и программного обеспечения в системе размещения госзаказа
- Торги в режиме удаленного доступа, электронные аукционы, электронные торговые площадки
- Информационные семинары, ежедневные постоянно действующие консультации на стенде Минэкономразвития России, Комитета по государственному заказу МАП, Правительства Москвы, Института госзакупок РАГС
- Конкурсы «Лучший госзаказчик 2008 года», «Лучший поставщик 2008 года»

Организаторы:

Министерство экономического развития Российской Федерации

Межрегиональная общественная организация «Московская ассоциация предпринимателей» МАП

Под патронатом:

Торгово-промышленной палаты Российской Федерации

При поддержке:

Правительства РФ, ФАС России, Счетной палаты РФ, Минобороны России, Правительства Москвы, Федеральных органов исполнительной и законодательной власти Российской Федерации

ПРИГЛАШАЕМ НА ПЯТЫЙ ЮБИЛЕЙНЫЙ ФОРУМ-ВЫСТАВКУ

Исполнительная дирекция: 119072, Москва, Берсеневская наб., 20/2
тел/факс: (495) 959-06-98, 959-13-82, 959-30-64, 959-39-57, 258-00-26 E-mail: goszakaz@inconnect.ru

Подробная информация о Форуме-выставке на Web-сайте www.goszakaz.inconnect.ru

Адам Хинтертуер

СТРАСТИ ВОКРУГ пластика

Насколько опасны для здоровья пластиковые бутылочки для детского питания, линзы для очков и другие содержащие бисфенол-А изделия? Патриция Хант (Patricia Hunt), обратившая внимание на эту проблему 10 лет назад, до сих пор пытается в ней разобраться

Когда однажды направление исследований Патриции Хант круто изменилось, ее аспиранты из Университета Западного резервного района были крайне недовольны. Им не терпелось опубликовать только что полученные интересные данные и поставить новые эксперименты. Однако Хант быстро охладила их пыл и посоветовала подождать, пока сама не разберется в возникшей ситуации. А состояла она в следующем.

Генетик по профессии, Хант исследовала причины, по которым процесс репродукции человека часто протекает с отклонениями. У нее было подозрение, что хромосомные аномалии в яйцеклетках, осложняющие беременность, каким-то образом связаны с гормонами. Статья, в которой излагались результаты влияния уровня гормонов на протекание беременности у экспериментальных мышей, была почти готова к отправке в печать. Оставалось только убедиться в том, что с контрольной популяцией грызунов, не подвергавшихся никаким манипуляциям, все в порядке. Каково же было удивление Хант, когда она обнаружила, что у 40% мышей из контрольной группы яйцеклетки тоже имеют отклонения!

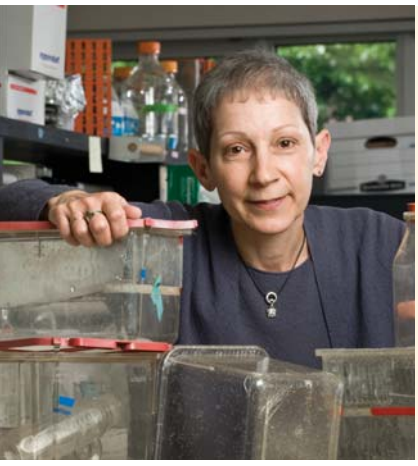
Отправлять статью в печать было нельзя; Хант занялась тщательной проверкой всех методик, оборудования и инструментов, которые использовались в опытах. Через четыре месяца она нашла то, что искала. Это было средство, использовавшееся для мытья полов в лаборатории. Вместо мягкого детергента оно содержало абразивное вещество. Этим же средством мыли клетки, где содержались животные, и бутылочки с водой. При такой жесткой обработке в среду попадало химическое вещество бисфенол-*А* (БФА), виновник аномалий. В результате оказывалось, что подопытные животные находились не в комфортных условиях, а в высокотоксичной среде.

Данное открытие, сделанное в 1999 г., заставило Хант и ее коллегу, Фредерика фом Сааля (Frederick vom Saal) из Миссурийского университета, заявить об опасности БФА не только для животных, но и для людей. Скептики назвали обоих ученых паникерами, ссылаясь на то, что не зафиксировано ни одного случая, когда БФА-содержащие пластики наносили бы ущерб здоровью живых существ.

Бисфенол-*А* был синтезирован еще в 1891 г. и в 1930-х гг. использовался как искусственный эстроген. Позже химики обнаружили, что в соединении с фосгеном (применявшимся во время Первой мировой войны как отравляющее вещество) и некоторыми другими химикатами БФА образует прозрачный твердый пластик: из него стали изготавливать автомобильные фары, линзы для очков, *DVD*-диски, бутылочки для детского питания.

Однако в процессе получения пластика не весь БФА связывается с другими компонентами смеси, часть его остается в свободном состоянии и поступает в окружающую среду; количество свободного БФА увеличивается особенно сильно, когда пластик нагревается — в машине для мытья посуды, в микроволновой печи, в стерилизаторе.

В последние годы из самых разных лабораторий поступали сведения о том, что БФА оказывает вредное воздействие на подопытных животных: с его влиянием связывали развитие у грызунов рака молочной и предстательной железы, аномалии в развитии гениталий у самцов, преждевременное половое созревание



ПАТРИЦИЯ ХАНТ

- **ТОКСИКОЛОГ ПО СОВМЕСТИТЕЛЬСТВУ, ГЕНЕТИК ПО СПЕЦИАЛЬНОСТИ: обнаружила, что бисфенол-А (БФА), имитирующий действие эстрогена, высвобождается из содержащих его пластиковых изделий; это отразилось на здоровье подопытных мышей и свело на нет результаты экспериментов.**
- **ГРАНДИОЗНЫЕ МАСШТАБЫ: в 2004 г. было произведено примерно 3 млн тонн бисфенола-А, пошедшего на изготовление компакт-дисков, линз для очков, бутылочек для детского питания и других товаров. Производство БФА увеличивается ежегодно на 10%.**
- **ЕСТЬ ЛИ ПРИЧИНЫ ДЛЯ БЕСПОКОЙСТВА? Сообщение Хант о возможном вредном воздействии БФА на живые организмы не прошло незамеченным. Одни считают его ошибочным, другие доверяют полученным результатам и выражают обеспокоенность. «Любой, кто знает Патрицию, скажет, что не было случая, когда она оказалась бы неправа», — говорит Фредерик фом Сааль, коллега Хант.**

самок, ожирение и даже изменения в поведении (дефицит внимания, гиперактивность).

Что касается Патриции Хант, которая теперь работает в Университете штата Вашингтон, то она занялась исследованием анеуплоидии — изменения числа хромосом в яйцеклетке, приводящего к рождению неполноценного потомства. В прошлом году она опубликовала в журнале *PLos Genetics* статью, по сравнению с которой результаты, полученные ранее, были, по ее словам, «детской забавой». Хант подвергала беременных мышей воздействию БФА во время формирования яичников у эмбрионов. Когда грызуны достигли половозрелости, у 40% из них яйцеклетки оказались поврежденными, что неизбежно должно было сказаться на их потомстве. По-видимому, однократное действие БФА проявляется у животных вплоть до третьего поколения.

Пока специалисты обсуждали, можно ли использовать мышей в качестве модели для исследования действия БФА на человека, появились указания на то, что результаты экспериментов Хант трудно воспроизвести. В докладе Гарвардского центра по анализу рисков за 2004 г. сообщалось, что «не найдено никаких свидетельств токсичности БФА в малых дозах». По словам Гленна Сайпса (I. Glenn Sipes) из Аризонского университета, одного из авторов упомянутого доклада, такое несоответствие настораживает. Он считает, что полученный ранее на экспериментальных грызунах результат нельзя экстраполировать на человека.

На это Хант возражает, что существует масса дополнительных свидетельств реальности вредного воздействия БФА на человека. В ответ на гарвардский доклад она вместе с другими исследователями подготовила статью для *Reproductive Toxicology*, опубликованную в 2007 г., в которой сообщалось о результатах работы группы из 36 ученых, руководимых ею и фом Саалем. Ими были проанализированы сотни финансируемых правительством исследований, связанных с БФА. В 90% из них говорилось о вредном воздействии данного вещества на здоровье. При этом нашлось немногим более десятка работ, финансируемых промышленными организациями, сообщавших, что эффект отсутствует.

Впрочем, по мнению Хант, важно было другое. На воздействие БФА можно смотреть с точки зрения токсиколога (такой подход свойствен скептикам) и эндокринолога (что и делает Хант). На сайте www.bisphenol-a.org, созданном Американским химическим советом (он объединяет компании, связанные с производством пластиков), можно найти утверждение, что «токсикология БФА изучена достаточно полно» и что «это соединение опасно только при очень высоких концентрациях».

Но, по глубокому убеждению Хант, считать БФА обычным токсином было бы опасным заблуждением, поскольку он «играет не по правилам». В токсикологии принято считать, что чем больше доза вредного вещества, тем оно опаснее. Однако токсичность БФА имеет иную природу: он имитирует действие эстрогена, являющегося гормоном, а гормоны в высоких дозах могут блокировать реакцию на них организма; в то же время низких доз бывает достаточно для проявления эффекта.

Считать бисфенол-А обычным токсином — опасное заблуждение, поскольку, по словам Патриции Хант, он «играет не по правилам»

И в самом деле, в опытах Хант на лабораторных мышах действие БФА наблюдалось при 20 мкг на 1 кг веса животного, аналогичные результаты получены и в других лабораториях. Это соответствует $1/2$–$1/3$ дозы, считающейся безопасной по регламентации *FDA*. При таких дозах концентрация БФА в организме составляет примерно одну часть на миллион, однако, как показывают последние данные, если БФА связывается с рецепторами гормонов на клеточной поверхности, то физиологический ответ отмечается при концентрации одна часть на *триллион*!

Соответственно, любой контакт с БФА может иметь нежелательные последствия. Тревожный вывод, особенно если учесть, что в 2004 г. БФА в неметаболизированной форме был обнаружен в моче 93% из более чем 2,5 тыс. обследованных пациентов. Таков вывод Центра по контролю и предотвращению заболеваний. А по данным Национальной и токсикологической программы, реализуемой Министерством здравоохранения и социальных служб США, БФА присутствует в крови человека и грудном молоке.

При такой распространенности БФА нельзя исключить, что скоро мы столкнемся с множеством непредвиденных проблем. Отсутствие сегодня четких свидетельств подстерегающей нас опасности и придает уверенности скептикам. «Почему мы должны тратить столько времени и средств на попытки доказать, что эффект малых доз БФА действительно существует? — спрашивает Гленн Сайпс. — Почему реакция на БФА то есть, то нет?»

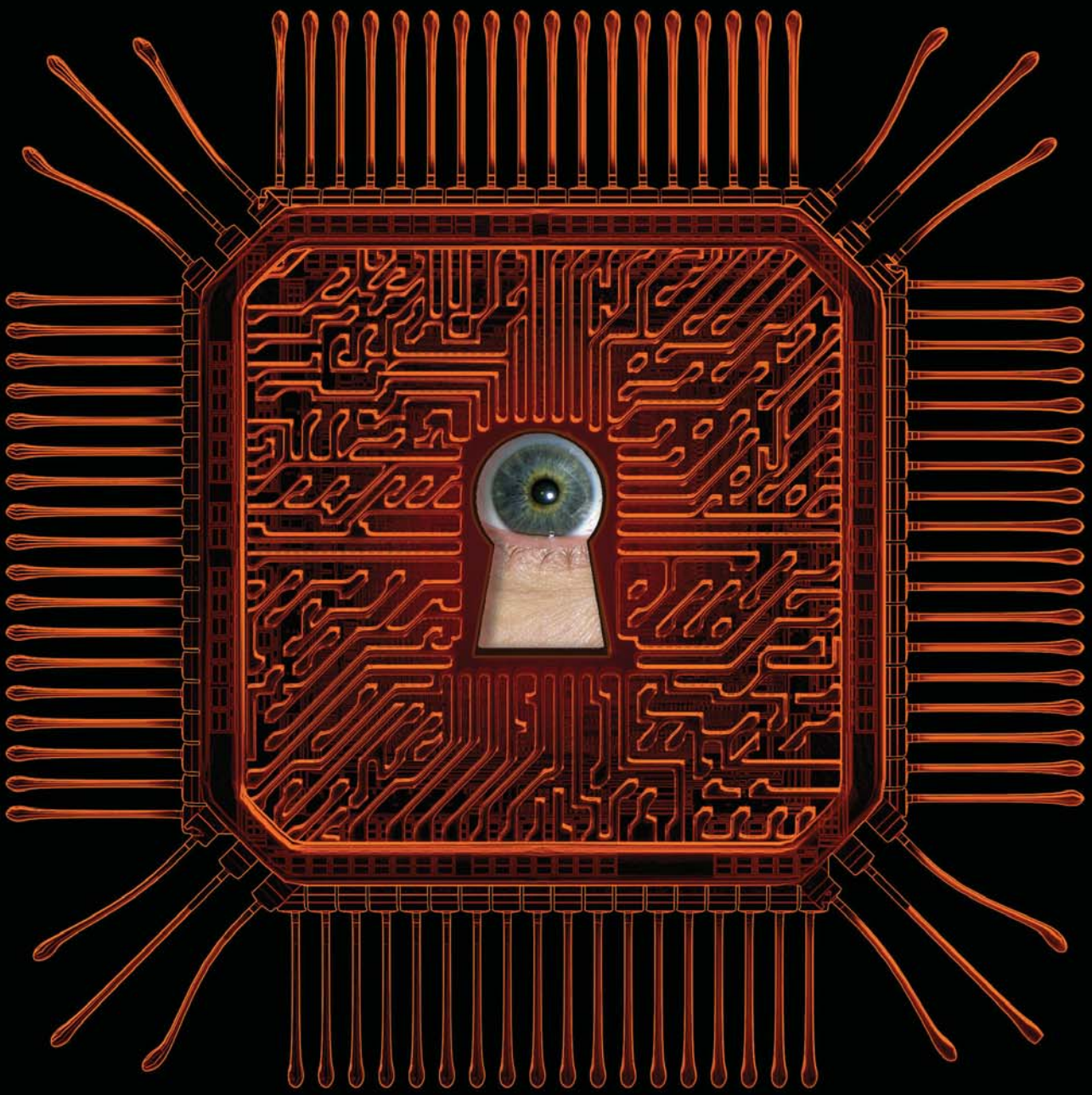
Пока научное сообщество пытается разобраться в сути дела, общественность уже бьет тревогу. 17 апреля 2007 г. Национальные институты здоровья подняли вопрос о том, что считать «безопасным» уровнем БФА, а через несколько дней *Health Canada*, аналог американской *FDA*, запретила применение бутылочек для детского питания, изготовленных из БФА-содержащего поликарбоната. Такие крупные торговые центры, как *Wal-Mart*, вынуждены были прекратить продажу изделий из этого пластика.

Кому-то подобные действия покажутся преждевременными — ведь опасность БФА для здоровья до конца не доказана. Однако Хант напоминает, что с аналогичными ситуациями потребители уже сталкивались — тогда «возмутителями спокойствия» были ртуть и свинец, обнаруженные в некоторых товарах. «Сегодня мы должны проявить настойчивость и решить, следует ли впускать в нашу повседневную жизнь изделия, безопасность которых вызывает сомнения», — говорит исследовательница. ■

Перевод: Н.Н. Шафрановская

приватность в век

ТЕРАБАЙТОВ И ТЕРРОРИЗМА



Питер Браун

Стресс после событий 11 сентября 2001 г. в сочетании с революционными переменами, привнесенными Интернетом, смещает границы между общественными интересами и «правом быть оставленным в покое»

Двойной императив технического прогресса и борьбы с терроризмом привел к радикальным и, возможно, необратимым переменам в том, что может считаться частной сферой. Около 10 лет назад Скотт Макнили (Scott McNealy) из корпорации *Sun Microsystems* произнес свою знаменитую фразу о смерти частной жизни. «Забудьте о ней», — сказал он. Некоторые люди, в основном моложе 25 лет, заявили, что так и сделали, приняв антитезу приватности — полное раскрытие сведений о себе.

Бесспорно, во многих случаях — например при поиске террористов или носителей опасных болезней — интересы общества требуют предоставления огромного количества информации, которая в обычных условиях считается приватной. Однако во многих областях — банковской, коммерческой, дипломатической и медицинской — конфиденциальность связи существенна. «Отцы-основатели» США приложили много усилий, чтобы защитить личную жизнь людей. Воплощение этого стремления — Билль о правах (несмотря на то что определения приватности как такового, о чем мы часто напоминаем, в нем нет). В своей статье «Размышления о приватности 2.0» Эстер Дайсон объясняет смысл данного понятия, указывая нам, что в него не входит: некоторые важные составляющие частной сферы легче понять с точки зрения проблем безопасности, политики в области здравоохранения, страхования или самопрезентации.

Крайнюю актуальность теме неприкосновенности частной сферы придали терроризм и всеохватность сети Интернет, но есть и множество других серьезных причин для того, чтобы присмотреться к будущему приватности.

Одна из них — выборы в США, проходившие в период существенных перемен в правовой и законодательной базах, касающихся прослушивания телефонных разговоров спецслужбами (*см.: Диффи У., Ландау С. Дивный новый мир: контроль сетевой телефонии*).

Вторая — соблазн извлечь выгоду из раскрытия некоторых видов информации, например при введении электронных историй болезней вследствие модернизации медицинского обслуживания (*см.: Ротстейн М. Держите свои гены при себе!*) или, напротив, для лучшей защиты от хищения опознавательных данных личности за счет использования биометрической авторизации (*см.: Джейн А., Панканти Ш. Перспективы биометрии*).

Третья — тот факт, что развитие технологий создает небывалые угрозы частной жизни и личной безопасности как из-за непредвиденных эффектов самораскрытия, так и вследствие быстрого совершенствования средств слежки и разведки (*см.: Эшли С. Средства шпионажа*), радиочастотных меток *RFID* (*см.: Олбрехт К. Радиометка — это вы*) и слияния данных (*см.: Гарфинкель С. Данные всех стран, соединяйтесь!*), не говоря уже о вирусах и других вредоносных программах, заражающих Интернет (*см.: Укрепление безопасности сетей*).

В ответ на все эти угрозы было создано удивительное разнообразие технологий защиты частной жизни, которые практически не используются (*см.: Лисянская А. Чтобы тайное не стало явным*). Многие молодые люди считают все тревоги по поводу приватности пустым шумом: они слишком счастливы, чтобы жертвовать полнотой жизни в аквариуме социальной сети ради того, что их родители называют «конфиденциальной информацией» (*см.: Солоув Д. Конец приватности?*).

По всем вышеперечисленным и ряду других причин редакция журнала *Scientific American* посвящает настоящий номер будущему того, что судья Верховного Суда Луис Брандейс (Louis Brandeis) назвал «правом быть оставленным в покое». ■

Перевод: И.Е. Сацевич

Эстер Дайсон

РАЗМЫШЛЕНИЯ о приватности 2.0

Многие вопросы, которые считают относящимися к защите приватности, могут обернуться вопросами безопасности, политики здравоохранения, страхования или самопрезентации. Поэтому прежде чем обращаться собственно к теме приватности, полезно внести некоторую ясность

Как только вы произнесете где-нибудь вслух слово «приватность», так сразу же спровоцируете массу страстных споров. Одних тревожат злоупотребления властью со стороны правительства; другие стыдятся того, что употребляют наркотики, или своего сексуального опыта; третьих возмущает то, как корпорации собирают личные данные, чтобы вести направленную рекламу, или то, как страховые компании роются в историях болезней своих клиентов, чтобы найти повод отказать в выплате страховки. Кого-то страшит мир вездесущей коммерциализации, в котором информация используется для распределения всех и каждого по «сегментам рынка», чтобы лучше удовлетворять самые потаенные желания или самые несерьезные прихоти людей.

Такие страхи обычно представляются как альтернативы: неприкосновенность частной сферы против медицинского обслуживания, против бесплатного (оплачиваемого рекламодателями) контента или против безопасности. Все эти споры давно затасканы, но сегодня они приобрели новое звучание, не так как тогда, когда тема привлекала только специалистов, людей, имеющих доступ к конфиденци-

MARK CLEMENS (photoillustration); RICHARD NOWITZ National Geographic Collection (crowd scene)

Растущая прозрачность традиционных границ частной жизни в нашем обществе, принесенная Интернетом, ставит перед людьми этические проблемы, которых не могло быть, когда информация была больше разделена на «секторы». Это положение иллюстрируют вымышленные сведения о людях, изображенных на снимке. Если бы они были помещены в Интернет, возникло бы несколько острых этических коллизий

альной информации, и твердолобых защитников права на приватность.

С одной стороны, эрозия частной сферы несомненна. Сегодня услугами Интернета пользуется большинство американцев, и перед нами порой не раз вставал вопрос: «Как они узнали это?». Правительство США нарушает неприкосновенность частной сферы направо и налево, при этом все больше засекречивая свои действия. Если кто-то, особенно правительство, прилагает все усилия, чтобы узнать, кто вы такой, действовать анонимно становится очень трудно.

С другой стороны, у людей возникают все новые основательные причины для раскрытия своей личной информации. Мир стоит на пороге персонализации медицинского подхода. Использование подробной медицинской и генетической информации из историй болезней людей для лечения отдельных больных и анализа эпидемиологической статистики по населению имеет огромный потенциал для улучшения здоровья общества в целом. Многие люди получают удовольствие, делясь личной информацией с другими через социальные сети Интернета. Кроме того, из-за растущей угрозы терроризма некоторые граждане готовы раскрыть личную информацию ради иллюзорных обещаний большей безопасности.

Многое из того, что люди раньше воспринимали само собой разумеющимся в области частной сферы, было побочным продуктом ограниченного доступа и систематизации информации. Сегодня этих трудностей почти не осталось. Жизнь любого члена общества подобна жизни знаменитостей: каждый их шаг можно проследить, их прибавка в весе или проблема с волосами становятся предметами обсуждения.

Границы и условия

В этом номере журнала основное внимание уделяется и тем технологиям, которые вторгаются в частную сферу, и тем, которые, наоборот, оберегают ее. Но для определения рамок обсуждения я хочу изложить три основных положения.

Первое. В определении некоего раскрытия информации как нарушения приватности полезно отличать объективный ущерб, вызванный этим раскрытием, — мошенничество, отказ в обслуживании, ограничение свободы — от субъективного восприятия ущерба, когда таковым видится сам факт, что кому-то стороннему известны частные сведения о тебе. Во многих случаях то, что называют вторжением в частную сферу, на самом деле является нарушением секретности или финансовым ущербом: если некто узнал или злонамеренно использовал ваш номер социального страхования (а я сообщаю свой, вероятно, несколько раз в месяц), то это вопрос нарушения не приватности, а секретности. Что же касается нарушения именно приватности, то «ущерб», получаемый человеком, субъективен и индивидуален. И общество должно не пытаться раз и навсегда определить границы частной сферы, а предоставить людям средства контроля над распространением и использованием их личных данных. Выбор соотношения между секретностью и доступностью определяется личными предпочтениями, но средства и даже законы, позволяющие осуществлять этот выбор, нужны всем.

Второе. В связи с изменением границ между частным и общественным люди должны сохранить право на обнародование имеющейся у них информации. Когда в мире свободного отслеживания информации личная сфера все больше ограничивается, граждане имеют право знать, чем занимается правительство и бизнес, а также должны иметь доступ к средствам массовой информации. В этом случае баланс интересов личности и общества будет сохранен.

Третье дополняет первое. При оценке изменений ожиданий людей в отношении приватности важно помнить о неоднородности личных подходов к контролю распространения данных. Частная сфера не может быть чем-то единым, одинаково подходящим для всех: люди в разные времена имеют свое понимание того, что происходит с их личной информацией, и кому можно позволить знакомиться с ней. Они должны иметь право или возможность строить свои отношения с правительственными организациями, работодателями и страховыми компаниями на равных условиях. Сегодня как раз и закладывается основа такого социального партнерства.

Объективный ущерб

Безопасность — не единственный общественный фактор, определяемый как вопрос приватности. Многие аспекты, касающиеся, например, медицинской и генетической информации о личности, являются, в сущности, проблемами денег и страхования. Должны ли люди с плохим здоровьем больше платить за медицинское обслуживание? Если вы считаете, что

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Эрозию приватности часто воспринимают как один из видов ущерба.
- «Потеря конфиденциальности» на деле часто может быть потерей безопасности.
- Большинство опасений (хотя и не все) в отношении конфиденциальности генетической информации были бы развеяны, будь медицинское обслуживание доступно всем.
- Граждане должны иметь право контролировать всю информацию о деятельности правительства и его чиновников.
- Люди должны получить действенные средства контроля над тем, какую личную информацию они готовы предоставлять, и кому.

нет, вам, возможно, придется прийти к выводу, что им придется лгать. Это заключение часто ошибочно трактуется как защита приватности. Однако дело здесь не в приватности, а в модели страховой системы США. Люди меньше беспокоились бы о конфиденциальности своих медицинских данных, если бы раскрытие сведений об их состоянии здоровья не влекло за собой увеличения платы за медицинское обслуживание и страхование.

Похоже, что особенно тревожным примером информации, которая может быть использована для дискриминации людей, является генетическая информация. Опасаются, в частности, что страховые компании могут вскоре потребовать генетических тестов от страхующихся и отказывать в страховании людям с генетическими рисками. Геном и в самом деле содержит много данных. В частности, он позволяет однозначно идентифицировать личность человека, за исключением случаев однояйцевых близнецов, и обнаруживать скрываемые родственные связи. По определенным генетическим меткам могут быть выявлены некоторые редкие болезни.

Но гены — только один из факторов в жизни человека. Они очень мало могут сказать о динамике рода и ничего не говорят о том, что сделал человек с унаследованными способностями. Гены обычно проявляют себя через сложные взаимодействия с воспитанием, поведением, средой и случайностями.

Дискриминация по генетическим признакам в любом случае может вскоре стать незаконной. В мае 2007 г. Джордж Буш подписал Закон о запрете дискриминационного использования генетической информации (*Genetic Information Nondiscrimination Act, GINA*) при страховании и трудоустройстве.

Тем не менее нарастающий поток медицинской и генетической информации может изменить саму природу медицинского страхования. С увеличением доступности сведений о здоровье широких масс населения совершенствуется система прогнозирования на основе статистического анализа. Но если отдельные граждане могут быть с приемлемой точностью отнесены к той или иной так называемой стоимостной корзине, страхование людей, отнесенных к группе риска, потеряет свою общественную значимость. Встает вопрос о направлении средств, вносимых обществом, на доступное страхование лиц, находящихся а группе риска.

Таким образом, обществу предстоит ясно и открыто решить, какие виды дискриминации допустимы, а какие нет. Всем нам предстоит напрямую столкнуться с нравственным выбором.

Если от страховых компаний требуют управления денежными поступлениями, то они, со своей стороны, должны получить четкие установки, какие затраты на здоровье отдельных лиц и в какой доле готово оплачивать общество. (Трудность заключается в том, чтобы заставить страховые компании и органы здравоохранения снижать затраты путем предоставления качественного медицинского обслуживания, а не его ограничения. Как я уже отметила выше, увеличение объема информации о рисках для здоровья и результатах лечения поможет оценить эффективность лечения и позволит достичь названной цели.)

Право на частную информацию

Если одна сторона может требовать данных от другой, людям нужны гарантии защиты частной сферы. Самый яркий пример — возможность правительства собирать и использовать (в том числе, в своих интересах) личные данные. Эту возможность необходимо контролировать.

Как лучше всего ограничить власть государства? Законы о защите частной информации граж-

RICK SMOLAN (Dyson); SOURCE FOR TIMELINE: BEN FRANKLIN'S WEB SITE, BY ROBERT ELLIS SMITH. PRIVACY JOURNAL, 2000 (WWW.PRIVACYJOURNAL.NET); MPI/GETTY IMAGES (Puritans); IMAGEZOO/IMAGES.COM/CORBIS (envelope); TODD GIPSTEIN Corbis (Preamble to U.S. Constitution)

ХРОНОЛОГИЯ

ОБЩЕСТВЕННАЯ ЖИЗНЬ И ТЕХНОЛОГИИ

1600-е гг.: священник, который регистрировал рождения, браки и смерти, забрасывал все более широкие сети для вылавливания информации о гражданских делах. В Массачусетсе правительственные чиновники обходили дома, проверяя степень нравственности поведения жителей

1700-е гг.: приватности почти не было: все члены семьи, а иногда и гости порой ночевали в одном помещении

1700-е гг.: письма регулярно вскрывались на почте

1800-е гг.: «грошовые газеты» под защитой 1-й Поправки к Конституции США без стеснения публикуют любые слухи о знаменитостях

1838 г.: появился телеграф, начались перехваты телеграфных сообщений

Около 1900 г.: отпечатки пальцев признаны уникальным и неизменным идентификатором личности

1600 | 1700 | 1800 | 1900

Приватность в Америке, 1600-2008 гг.

В американцах парадоксально сочетаются неиссякаемое любопытство и упорное желание, чтобы их оставили в покое

1600-е гг.: пуританская мораль считала слежку за соседями гражданской обязанностью. Во многих городах людям запрещалось жить в одиночестве

1700-е гг.: в частной сфере видится убежище от общественных волнений. Колонисты согласны с англичанами и христианами древнего Рима в том, что «дом человека – его крепость»

1787 г.: Конституция предусматривает проведение переписи каждые 10 лет. Многие относятся к переписям с недоверием

1791 г.: Билль о правах гарантирует свободу слова и защищает от необоснованных обысков и арестов

1890 г.: Сэмюель Уоррен-младший (Samuel D. Warren Jr.) и Луис Брандейс (Louis D. Brandeis) выступили в *Harvard Law Review* в защиту права на приватность

ЗАКОНЫ И ПОЛИТИКА

дан здесь мало помогут, т.к. правительство может не выполнять или не защищать их. Информация о работе правительства должна быть доступна гражданам.

Ранее главным гарантом этого права были СМИ, но сегодня Интернет предоставил людям возможность взять это дело в свои руки. Любая фото- или видеокамера может сохранять свидетельства притеснений, как, например, драматическая видеозапись событий 1991 г. Родни Кинга (Rodney King), или снимки из тюрьмы Абу-Грейд, опубликованные в 2004 г. Интернет открывает каждому человеку мгновенный доступ к всемирной аудитории. Сообщения неправительственных организаций и граждан со всего мира распространяются через социальные сети, сайты обмена файлами и в виде текстовых сообщений по сотовым телефонам.

Как ни парадоксально, лучшей моделью может оказаться предоставление обществу той информации, которой правительство требует от бизнеса.

Требования к открытости бизнеса в сфере трудовых отношений, финансовых показателей все время ужесточаются. Инвесторы получают информацию о финансовом состоянии компании, а потребители имеют право знать, из чего и каким способом производятся товары, которые они покупают.

На том же основании граждане имеют право контролировать избираемых и оплачиваемых ими чиновников. Граждане должны иметь в отношении правительства те же права, какие существуют у акционеров и потребителей (и, в данном случае, у служб госбезопасности и у Комиссии США по биржам и ценным бумагам) в отношении публично работающих компаний. Я бы сказала, что граждане имеют особые права в отношении правительства именно потому, что оно вынуждает нас предоставлять ему так много информации. Фонд *Sunlight Foundation* (www.sunlightfoundation.com), чьим доверенным лицом я являюсь, побуждает людей искать и обнародовать информацию о своих представителях в Конгрессе и вообще обо всех чиновниках.

Дневной свет для бизнеса

Что касается прав бизнеса в отношении приватности, у него их немного (и не должно быть много). Правда, компании могут регистрировать собственные транзакции с потребителями, причем в случае кредитных транзакций от клиентов требуют подтверждения кредитоспособности путем предоставления личных сведений. Но как компания может не согласиться продавать в кредит, так и потребитель может отказаться иметь с ней дело, если она требует слишком много данных. Чего должны требовать законы от компаний, так это соблюдения ими же установленных правил.

Что касается сведений, раскрываемых правительством (и особенно политиками, претендующими на должность), они идут гораздо дальше того, что требует закон. Рейтинги, дискуссии и другой создаваемый пользователями контент, касающийся услуг (отелей, врачей и др.) и товаров, размещается на всех видах веб-сайтов. Правда, многие обзоры отелей готовятся самими отелями или их конкурентами. (Для борьбы с такой практикой некоторые сайты требуют от пользователей регистрации и поощряют их давать оценки репутации других пользователей и обозревателей.) Пациенты могут получать сведения о своих врачах и лечебных учреждениях на различных сайтах — от *HealthGrades.com* (услуга платная) до ряда сайтов, финансируемых рекламодателями.

Новая услуга *Barcode Wikipedia* (www.sicamp.org/?page_id=21) позволяет пользователям размещать ин-

ARCHIVEHOLDINGS, INC. (computer technician); BETTMANN/CORBIS (Social Security card and man with listening device); G. RKAN SENG N http://livecd.gnustep.org (Web page); FACEBOOK (logo)

1973 г.: «Возникли и растут опасения, что компьютеры уже являются или вскоре станут опасной угрозой частной сфере» — Хорст Фейстел (Horst Feistel), *Cryptography and Computer Privacy; Scientific American, май 1973 г.*

1976 г: Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin E. Hellman) изобрели шифрование с открытыми ключами

1980-е гг.: широкое распространение получили идентификация по ДНК и сотовые телефоны.

1989 г.: Интернет дополнен Всемирной Паутиной (*World Wide Web*)

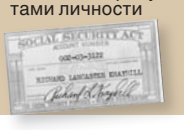
1995 г.: Впервые употреблен термин *spyware* — «шпионское ПО»

2004 г.: Появился популярный социальный веб-сайт *Facebook*

1950 | 1975 | 2000

1928 г.: Верховный Суд США признал законным прослушивание телефонных переговоров

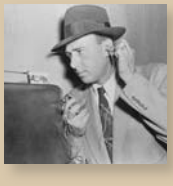
1936 г.: большинству взрослых граждан США присвоены номера социального страхования, ставшие пожизненными атрибутами личности



1966 г.: принят Закон о свободе информации (*Freedom of Information Act, FOIA*)

1968 г.: принят 3-й вариант Всеобщего Закона о борьбе с преступностью и обеспечении безопасности на улицах (*Omnibus Crime Control and Safe Streets Act, Title III*), часто определяемый как «конец приватности», который регламентировал, в каких случаях для прослушивания требуется санкция

1978–1994 гг.: Конгресс принимает поправки к законам о контроле телефонных разговоров, сначала в ответ на возмущение по поводу Уотергейта, а позднее - чтобы потребовать от телекоммуникационных компаний «быть готовыми к подключению прослушивающих устройств»



2001 г: Закон *USA Patriot Act* предоставил властям широкие права бесконтрольного просмотра баз данных и слежки

2008 г.: Конгресс внес поправки в закон о прослушивании, расширив полномочия исполнительной власти в деле слежки

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ электронного ведения историй болезней наглядно иллюстрируются доступностью этой информации через Сеть. С одной стороны, эти данные могут помочь спасти жизнь пострадавшему от несчастного случая, если он находится без сознания (*снимок слева*), а с другой, если в них содержатся сведения о болезнях, требующих дорогостоящего лечения, они могут стать основанием для отказа в медицинском страховании (*снимок вверху*)

формацию о товарах — их ингредиентах или компонентах, месте изготовления или сборки этих изделий, трудовых отношениях в компании-производителе, воздействии на окружающую среду, побочных эффектах и т.п. Компании также имеют право публиковать на сайтах свою точку зрения по этим вопросам. Разумеется, при такой свободе мнений вполне вероятны преувеличения и ложь. Однако со временем, как продемонстрировала сама *Wikipedia*, пользователи начинают сдерживать друг друга, и правда в большей или меньшей степени выявляется.

Жизнь на миру

До недавнего времени приватность в какой-то мере была обеспечена ограниченностью доступа к информационным ресурсам. Сведения о том, что вы делаете в частной жизни, не были столь доступны, если только вы не были слишком знамениты или сами широко не рекламировали свои действия. Сегодня меняется само понятие частной сферы. Многих взрослых людей ужасает то, что они находят на таких сайтах, как *Facebook* или *MySpace*. Некоторые молодые люди знают об опасности социальных сетей, но не относятся к ней серьезно. Юности не хватает памяти о прошлом. И возможно, что со временем появятся законодательные ограничения в отношении неразумного поведения: большинство работодателей (которые, как и все другие люди, могут просматривать веб-страницы в поисках кандидатов на работу), просто снизят свои требования к принимаемым на работу, хотя некоторые и останутся более строгими. Вспомните о татуировках: 20 лет назад родители предостерегали детей от них, а сегодня они есть почти у половины женщин, которых я вижу в раздевалке своего спортивного клуба, и я думаю, что таков же, и даже больше, будет процент мужчин, украшающих себя подобным образом.

У молодежи еще сохранилось чувство неприкосновенности частной сферы, и молодых людей могут ранить чужие мнения о них. Дело в том, что большинство из них проводят среди сверстников больше времени, чем их родители. Но и XX в. отличался от XIX в., когда лишь немногие люди могли позволить иметь отдельную спальню: дети обычно спали в одной комнате друг с другом, а то и с родителями.

У некоторых обеспеченных людей были свои отдельные комнаты, но у них были слуги, выносившие ночные горшки, помогавшие им одеваться и заботившиеся об их самых интимных потребностях. В XX в. представления о приватности стали совершенно иными.

В предшествующих столетиях многие сельские жители знали друг о друге очень много. Но явным было немногое. Разница в том, что в прошлом Хуан не мог узнать, что говорила Алиса, из Интернета. Первый мог лишь предполагать, что именно известно второй, но он не мог проверить это. Точно так же молодой человек легко мог избегать общения с девушкой. Но сегодня, если Хуан был любовником Алисы, он может мучить себя, следя за ее очередным флиртом через Интернет. Существует ли такая концепция приватности, которая отвечала бы собственным желаниям человека?

ОБ АВТОРЕ

Эстер Дайсон (Esther Dyson) — дочь известного физика-ядерщика Фримена Дайсона, одного из создателей квантовой электродинамики, американская предпринимательница, писательница и публицистка, филантроп и общественный деятель, инвестор ряда новых сайтов, включая *23andMe* (информация о геноме потребителей), *PatientsLikeMe* (обмен медицинской информацией через Сеть) и *Boxby* (пользовательские предпочтения в отношении электронной почты). Она предоставила для проекта *Personal Genome Project* все данные о своем геноме и сопровождающие их медицинские сведения. Еще в 1997 г. писательница издала книгу *Release 2.0*, в которой рассматриваются вопросы защиты приватности в сетевом мире. Эстер Дайсон много раз бывала в России и способствовала развитию отечественного ИТ-рынка. Ее статьи и интервью часто публикуются в российских журналах, посвященных экономике, рынку высоких технологий и интеллектуальной собственности.

Сведения обо мне и я сам

Второе важное изменение в области частной сферы состоит в том, что люди учатся в какой-то мере управлять открытой информацией о своей личной жизни. В 2007 г. *Facebook* ввел службу *Beacon*, которая возмутила многих его пользователей, т.к. она регистрировала покупки, совершаемые пользователем через Интернет, и передавала информацию в Сеть. О введении этой службы было объявлено, но недостаточно внятно, и многие обнаружили возможности охраны своей приватности только спустя некоторое время. (Позднее *Facebook* перестроил службу, применив более продуманный подход.) Сегодня многие клиенты изменили свои установки охраны приватности как в отношении входящих новостей от друзей (нужно ли вам знать о каждом свидании друга?), так и в отношении исходящих сообщений друзьям (хотите ли вы извещать всех о своей деловой поездке?). Пользователи могут как обмениваться фотоснимками в пределах определенной группы, так и выставлять их на всеобщее обозрение.

Веб-сайт для обмена фотоснимками *Flickr* позволяет пользователям определять, кому могут быть показаны те или иные снимки, хотя и в ограниченной степени. (Раскрою карты: я была инвестором этого сайта.) Однако этот контроль, вероятно, станет более прицельным. Сегодня вы можете при желании создать замкнутую группу, но не можете избирательно показывать снимки отдельным людям. Например, вы может создать две перекрывающиеся семейные группы: в одну включить родных братьев и сестер и мать, а в другую — не только родных, но и единокровных и единоутробных братьев и сестер, отца и мачеху, но не мать. Другие люди могут создать иные подгруппы, например из отца и его детей, но без его новой жены, само наличие которой может сохраняться в тайне.

Блоггер и специалист по социальным сетям дана бойд (*danah boyd*; да, так и пишется — все строчными буквами), член ученого совета Беркмановского центра общества и Интернета при Гарвардском университете, недавно красноречиво высказалась о желании пользователей полностью определять, кому могут быть показаны выставляемые ими материалы, и какие рекламные объявления могут их сопровождать. Для бойд (и многих других) это не столько вопрос приватности, сколько способ самопрезентации (включая в случае бойд и ее собственное имя). Люди знают, что не могут контролировать все, что говорится в их адрес другими пользователями, но они могут выбирать те службы сетевого сообщества, которые позволяют им контролировать, как они презентуют себя в Сети, и то, кто может видеть каждую из этих презентаций.

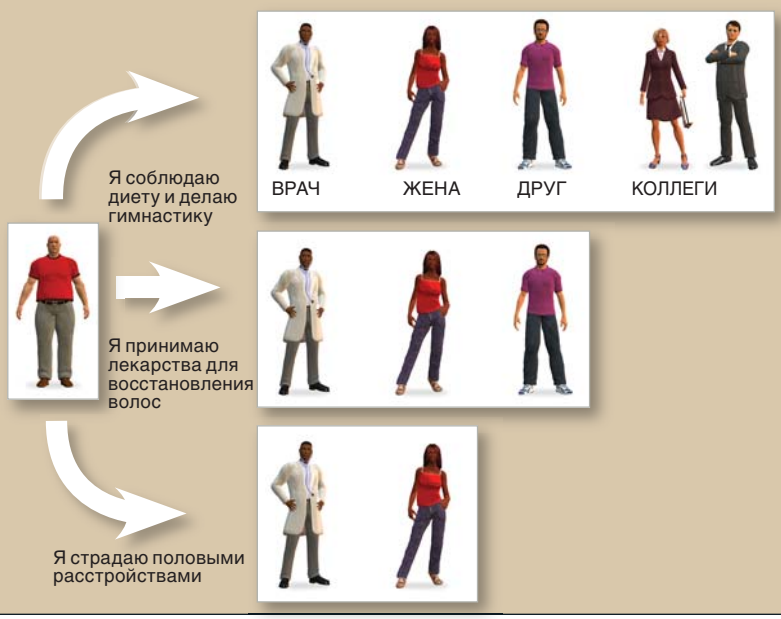
Как мне кажется, этот вид контроля распространится на категорию «дружественных» поставщиков. Алиса хотела бы, чтобы человек, продавший ей красный свитер 42-го размера, знал о ее потребительских пристрастиях, но не желает, чтобы к этой информации имели доступ ее друзья, ее нынешний бойфренд или другие продавцы. Естественно, Алиса не может управлять тем, что другие люди говорят или знают о ней. Если Хуан продолжает носить красный свитер и после их разрыва, кто-то может это заметить. И они могут комбинировать эти сведения, используя множество способов.

Тем не менее прозрачность не упрощает нашу жизнь. А реальность заключается в том, что не существует единой истины — или единственного перечня того, кому что разрешается знать. Неопределенность — неотъемлемое свойство истории и романов, политических кампаний и переговоров о заключении сделок, партий товара, благодарственных писем и поздравлений, не говоря уже о разводах, пакетах законов, увольнениях с работы и приглашениях на обед. Усложнение аппаратных и программных средств не устранит этой неопределенности. ■

Перевод: И.Е. Сацевич

СТЕПЕНИ РАСКРЫТИЯ

Лысый человек с избыточным весом желает контролировать распространение различных сведений из своей истории болезни, ограничивая его все более сужающимся кругом людей. Его лысина и полнота очевидны (даже если вес не известен точно), но он не видит надобности в том, чтобы сведения о его участии в программе диеты, проводимой его работодателем, распространялись дальше его врача, жены, друзей и коллег по работе. Сообщать о том, что он принимает средства для выращивания волос, он считает возможным врачу, жене и близким друзьям, а о половых расстройствах — только врачу и жене



дивный новый мир: контроль сетевой телефонии

Уитфилд Диффи и Сьюзан Ландау

По Интернету ведется все больше телефонных разговоров, и не удивительно, что желающие их подслушать тоже переместились во Всемирную паутину. Развитие подобных технологий прослушивания может повлечь за собой усиление государственного контроля

Чужие тайны были интересны посторонним всегда. Когда важные дела обсуждались за закрытыми дверями, любопытные подглядывали сквозь замочные скважины. Как только люди начали пользоваться телефоном, их разговоры стали прослушивать. В наши дни огромные объемы информации проходят через киберпространство, и шпионы освоили его тоже.

Виртуальное пространство, в отличие от физического, создают сами люди. Одни придумывают его законы и форму, обеспечивают сохранность и безопасность данных, а другие работают над предоставлением доступа к чужой информации. Службы безопасности разных государств, борясь с преступностью и терроризмом, уделяют все больше внимания киберпространству. Преимущества такого подхода очевидны.

Однако есть у него и неприятные последствия. Использование специального оборудования для контроля трафика повлияет на скорость передачи данных и может привести к уходу с рынка мелких провайдеров, т.к. не каждый сможет себе позволить дополнительные траты на его установку. Тотальное слежение может сказаться и на положении страны на информационном рынке в целом, привести к нарушению гражданских прав, подвергнуть риску все сетевое пространство и, в конечном итоге, национальную безопасность.

Если США создадут мощную систему перехвата интернет-сообщений, то как гарантировать простым гражданам, что она будет использована надлежащим образом? Коррумпированные полицейские могут воспользоваться частной информацией в корыстных целях, а преступники, террористы, сотрудники разведок других стран — применить ее против американских граждан. Решения, необходимые для защиты от таких возможных проблем, могут быть разными. Они требуют широкого обсуждения, но завеса секретности, окружающая деятельность спецслужб, не позволяет предать их гласности.

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Переход на электронную систему телефонных коммуникаций и развитие интернет-сервисов существенно осложнили работу спецслужб. Теперь для контроля телефонных переговоров требуется сложная электронная техника.
- Федеральные службы заставляют интернет-провайдеров устанавливать оборудование для контроля сообщений в Сети, аналогичное тому, которое используется телефонными компаниями. Такие действия могут существенно сдерживать развитие телекоммуникационных технологий.
- Нет гарантии, что информация будет использована сотрудниками спецслужб должным образом и не попадет в руки шпионов или террористов.

Краткая история прослушивания телефонов

Чтобы понять, как осуществляется контроль телефонных сообщений сегодня, нужно заглянуть в прошлое и разобраться в технологиях передачи сигнала. С момента изобретения телефона и до середины 1990-х гг. для обеспечения телефонной связи использовалась сеть с коммутацией каналов. Абонент набирал нужный номер, и из проводов, реле и коммутаторов выстраивался канал доступа, который обеспечивал передачу голосовых сообщений и был занят на протяжении всего разговора. Основной задачей телефонных станций было предоставление канала связи, а организацией соединения и передачей данных занимались операторы-телефонисты.

Прослушивание телефонных переговоров в США имеет свою историю. Вначале было достаточно, не выходя за пределы телефонной станции, подключить пару проводов к линии абонента, надеть наушники и включить магнитофон для записи разговора. Со временем спецслужбы создали особые подразделения, которые базировались в отдельных помещениях, соединенных с телефонными станциями каналами связи.

Суды не рассматривали материалы, полученные путем прослушивания телефонов, как составную часть расследования, но в 1967 г. в ходе процесса «Катц против Соединенных Штатов» Верховный суд признал, что перехват телефонных разговоров граждан является частью расследования, и в таком случае их права должны быть защищены. Прецедент привел к тому, что в 1968 г. Конгресс принял закон о соблюдении прав граждан в ходе следствия. Под его действие не попадала разведывательная деятельность за пределами США и в отношении иностранных граждан.

Уже в 1972 г. Конгрессу пришлось вернуться к данному вопросу. Расследование Уотергейтского скандала показало, что сотрудники администрации президента прослушивали телефонные разговоры. В числе пострадавших оказались члены американских и иностранных политических организаций. Кризис разрешился в 1978 г., когда был принят закон о разведывательной деятельности и на его основании учрежден Секретный федеральный суд, ответственный за выдачу санкций на прослушивание телефонных переговоров.

Перехват разведывательной информации в основном не попадает под действие закона, поскольку разведке в первую очередь интересна не телефонная сеть, а радиосообщения. К тому же за границей возможности спецслужб ограничены. Если прослушивать телефонные разговоры граждан США можно только при наличии серьезных подозрений в противоправной деятельности, то за пределами Соединенных Штатов такая деятельность превращается в большой бизнес. На контроль информационных потоков агентство национальной безопасности ежегодно тратит миллиарды долларов. Наземные, воздушные, морские и спутниковые станции слежения занимаются перехватом информации по всему миру.

Наиболее существенные различия лежат в области законодательства. В соответствии с Четвертой поправкой к Конституции гражданам США гарантируется право защиты от «необоснованного расследования и ареста». «Обоснованное» понимается таким образом, что сотрудник спецслужб в ходе предварительного расследования должен получить доказательства противоправной и общественно опасной деятельности гражданина и обратиться с ними в суд для получения санкции на прослушивание телефонных переговоров подозреваемого. На территории США совершенно не допустимо следствие с применением средств контроля и использование его в качестве доказательной базы преступления. Сотрудники разведки не обязаны следовать таким процедурам. В своей работе они полагаются на профессиональную интуицию и на основании имеющейся информации принимают решение, какой объект стоит взять под наблюдение.

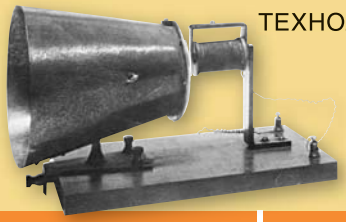
Закон о разведывательной деятельности США выделяет три основ-

Можем ли мы быть уверены в том, что система контроля телефонных переговоров и интернет-сообщений будет использоваться в интересах государства и граждан?

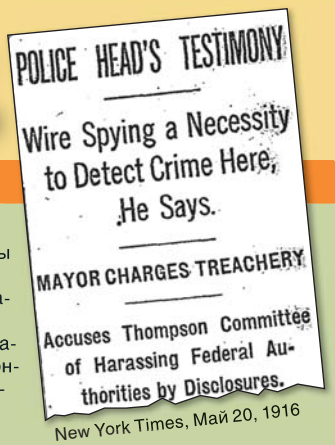
BETTMAN/CORBIS (telephone receiver); NEW YORK TIMES, PAGE 1, MAY 20, 1916 (newspaper); ANGEL FRANCO AP Photo (Bell Labs sign)

ОСНОВНЫЕ ДАТЫ

1876 г.: Александр Белл подал заявку на изобретение телефона



ТЕХНОЛОГИИ



New York Times, Май 20, 1916

1875 — 1900

ИСТОРИЯ СИСТЕМЫ ПРОСЛУШИВАНИЯ ТЕЛЕФОННЫХ ПЕРЕГОВОРОВ

По мере развития технологий совершенствовалось законодательство

1890-е гг.: спецслужбы впервые использовали систему прослушивания телефонных переговоров

ЗАКОН И ПОЛИТИКА

ные категории объектов контроля: коммуникации между резидентами США (граждане, лица имеющие вид на жительство, американские компании) и иностранцами; между системами передачи данных на территории США и за ее пределами; между проводными и беспроводными системами связи. Для контроля проводных систем на территории США необходимо получать ордер, а радиокоммуникации защищены законом, если сигнал перехвачен на территории США и сообщение передается конкретному гражданину США, находящемуся на территории страны.

До недавнего времени процедура получения ордера сотрудниками разведывательных служб была такой же, как и у полицейских. Разведчик должен был предоставить суду данные об объекте, его местонахождении, сведения о техническом устройстве и обосновать необходимость проведения мероприятия. Не допускалось получать таким способом улики и использовать их в качестве доказательной базы преступления. В качестве временной меры принятый Конгрессом закон предусматривал возможность перехвата радиосообщений на территории США без получения ордера, если они исходили от нерезидентов США, что оказалось весьма полезным для разведслужб.

Спутниковые системы связи, появившиеся в конце 1960-х — начале 1970-х гг., коренным образом изменили телефонный трафик в США. Теперь станции слежения *NASA*, расположенные в штатах Вашингтон и Виргиния, могли на законных основаниях контролировать весь проходящий по ним информационный поток.

В 1970-х гг. появился принципиально новый носитель, предназначенный для передачи данных на большое расстояние, — оптико-волоконные кабели с лазерной модуляцией сигнала. По таким сетям можно было мгновенно, без задержки, в отличие от систем спутниковой связи, передавать огромные объемы информации: они были в большей степени защищены от перехвата, нежели радиосигналы, но главным их преимуществом стала относительно низкая стоимость. С 1990-х гг. основной информационный поток между фиксированными операторами связи пошел по оптико-волоконным сетям, которые по американскому законодательству относятся к проводным, поэтому передаваемая по ним информация подлежит защите. Разведка не может перехватить ее без получения санкции суда, что осложняет задачу контроля транзитного трафика (более 20% трафика, проходящего по американским коммуникационным сетям, генерируется и передается европейскими, азиатскими и латиноамериканскими пользователями).

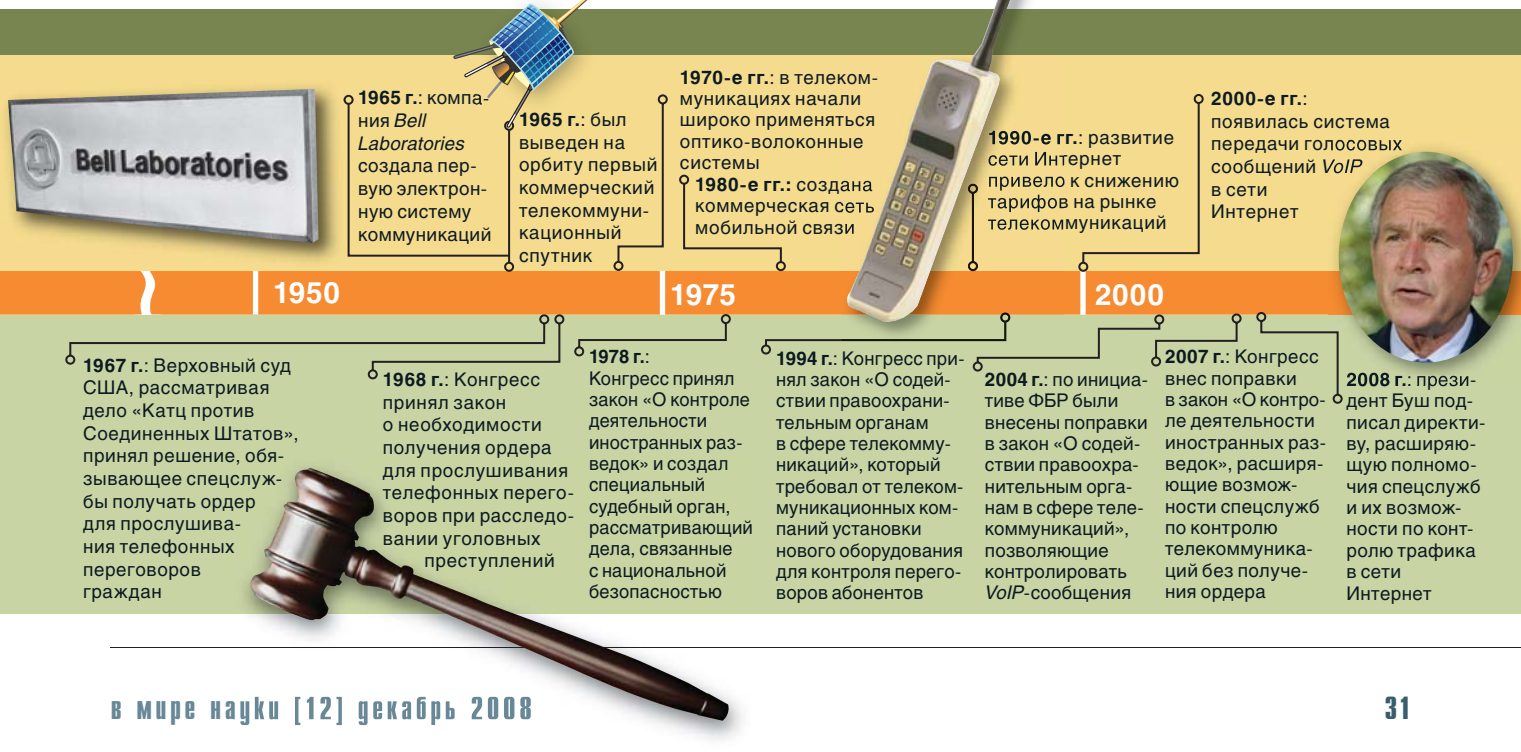
Примерно в то же время начали использоваться электронные системы. Они открыли дорогу новым услугам телефонной связи, таким как голосовые сообщения и автоответчики, и существенно осложнили работу спецслужб. Теперь абонент мог оставлять сообщения на голосовой почте телефонной компании, и даже при наличии санкции спецслужбы не имел доступа к информации, за исключением тех случаев, когда выход на голосовой почтовый ящик осуществлялся с контролируемого телефона.

В 1994 г. Конгресс принял закон «О содействии правоохранительным органам в сфере телекоммуникаций» (*Communication Assistance for Law Enforcement, CALEA*), который обязывал телекоммуникационные компании предоставлять информацию вне зависимости от того, какими услугами пользовался абонент. Он существенно увеличил количество и качество информации, доступной сотрудникам спецслужб при проведении расследований.

Контроль Сети

В середине 1990-х гг. все больше пользователей получили до-

DAVID MUIR (gavel); JEN CHRISTIANSEN (satellite); LAWRENCE MANNING Corbis (cell phone); ROGER L. WOLLENBERG Pool/CNP/Corbis (Bush)



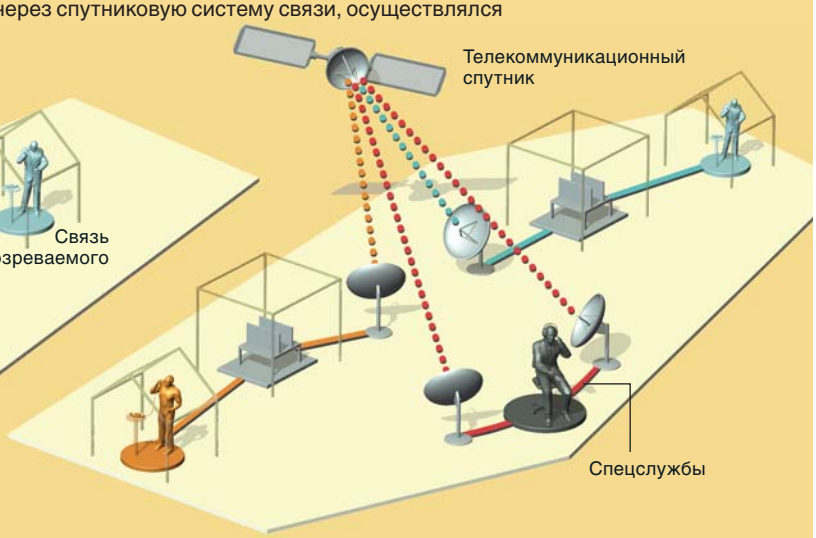
ТОГДА И ТЕПЕРЬ: СИСТЕМЫ КОНТРОЛЯ СТАНОВЯТСЯ СЛОЖНЕЕ

Развитие телекоммуникационных технологий вынуждает спецслужбы совершенствовать технологии

КОНТРОЛЬ СТАЦИОНАРНОЙ СЕТИ

В прежние времена сотрудники спецслужб, получив ордер, могли контролировать телефонную линию от дома подозреваемого до коммутатора. Контроль сообщений, идущих через спутниковую систему связи, осуществлялся без получения ордера

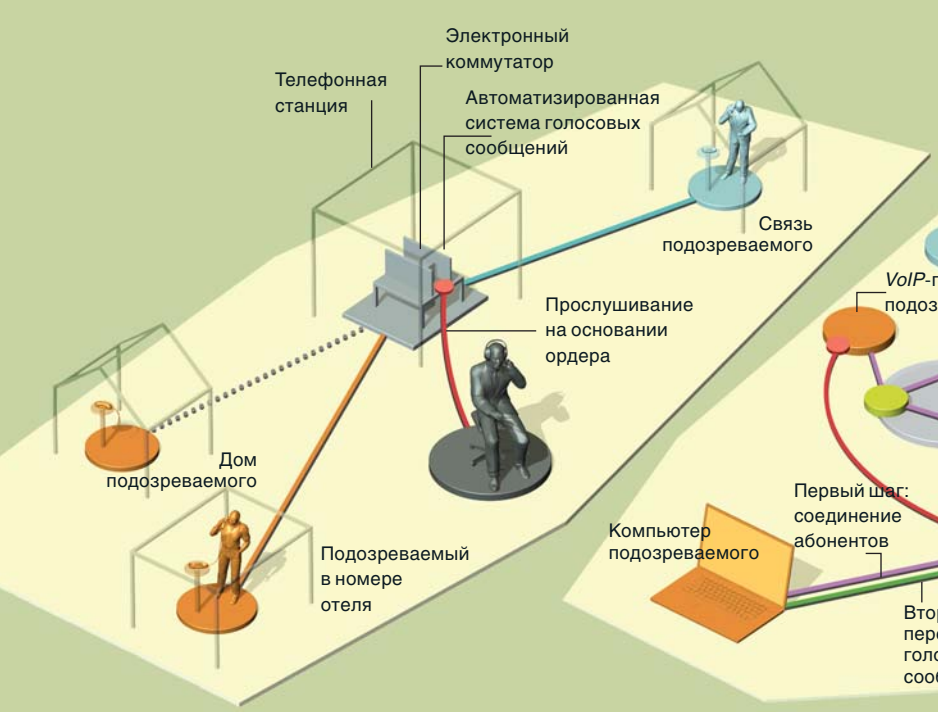
1 Стационарная связь



2 Беспроводная связь

НОВЫЕ МЕТОДЫ

С появлением электронных систем соединения абонентов и передачи сигналов спецслужбы перешли на новые методы контроля сообщений. Развитие технологий передачи голосовых сообщений через Интернет существенно осложнит систему контроля



3 Электронная сеть

4 Контроль сообщений в сети Интернет

ступ в Интернет, и на смену долгим телефонным разговорам пришли короткие сообщения, имеющие адрес отправителя и получателя. Если в телефонной сети стоимость соединения относительно высока, и короткие сообщения для телекоммуникационных компаний экономически не выгодны, то в Интернете чем они короче, тем дешевле. Просматривая сайты, пользователь каждый раз создает коммуникационную цепочку, которая рассыпается при переходе на другой сайт.

В эру телефонной связи прослушивание телефонов было возможно потому, что абонент был связан с конкретной линией и номером. С переходом на электронные станции и интернет-телефонию ситуация коренным образом изменилась. Сегодня без проблем можно получить новый номер или электронный адрес. Еще большую неразбериху внесло изобретение протокола передачи голосовых сообщений *VoIP*. Например, популярная *VoIP*-система *Skype* устанавливает соединение между абонентами и передает трафик разными каналами.

В соответствии с законом *CALEA* провайдер *VoIP* при получении вызова с контролируемого телефона должен передать сообщение спецслужбам, но он не может этого сделать. Допустим, что связь через Интернет устанавливают два человека, путешествующие по США. Алиса, находясь в аэропорту Чикаго, со своего компьютера звонит Бобу, который сидит в баре отеля в Сан-Франциско. Задача *VoIP*-провайдера состоит в том, чтобы с помощью *IT*-протокола соединить два компьютера, далее голосовые сообщения передаются *ISP*-провайдером с использованием его протоколов.

Чтобы контролировать сообщения абонента в Сети, государственным органам необходимо одновременно работать с большим количеством компаний, предоставляющих телекоммуникационные услуги. В случае с Алисой и Бобом, получив сообщение от *VoIP*-провайдера, представители спецслужб должны связаться с несколькими провайдерами и предоставить ордер на право контроля абонентов. Трудность заключается и в том, что ордер имеет силу только для провайдеров, зарегистрированных в США и ряде других стран, с которыми имеются соответствующие соглашения.

Большую проблему представляет обеспечение безопасности в сети Интернет. Недобросовестный сотрудник всегда может найти доступ к данным клиента и использовать их в корыстных целях.

CALEA разделил понятие традиционной телефонии и Интернета, определив последний как информационные услуги. Но уже в 2004 г. Министерство юстиции, ФБР и Департамент по борьбе с наркотиками, обеспокоившись ростом популярности *VoIP*, распространили действие закона на операторов широкополосного доступа. Федеральная комиссия связи США содействовала принятию новых правил «прослушивания» Интернета. Новые поправки могут создать опасный прецедент в сфере контроля коммуникаций.

Такие меры со стороны правительства способны существенно ограничить развитие передовых информационных технологий. В отличие от традиционных систем телефонной коммуникации Интернет не имеет централизованной и управляемой системы развития. Развитие новых услуг у телефонных компаний планируется на несколько лет вперед, а в Интернете сервисы могут появляться совершенно непредсказуемо. Для их создания не требуется мощная производственная база, и умельцы, имея широкополосный доступ в Сеть, могут разрабатывать программы, сидя дома или в гараже. Тотальный контроль сообщений в Сети может привести к тому, что мир вернется к старым добрым телефонам. Развитие технологий будет сдерживаться государственным регулированием, и вместо того, чтобы развивать информационный бизнес, американцы будут плестись в хвосте прогресса. Если другие страны пойдут по пути меньших ограничений, то они вырвутся вперед, и в таком случае появится реальная угроза национальной безопасности США.

С распадом Советского Союза с театра разведывательной деятельности ушел очень сильный игрок. Еще не так давно русские корабли патрулировали берега, в крупных городах Америки находились дипломатические миссии, спутники и разведывательные базы контролировали информационные потоки. Сегодня к главным противникам можно отнести «Аль-Каиду» и Китай, но их возможности гораздо скромнее. Они пытаются проникнуть в Интернет и через Сеть получить доступ к компьютерам и закрытым базам данных. Правительству необходимо адекватно реагировать на новые вызовы.

МИНИМИЗАЦИЯ

Разница в системе наблюдения за преступниками и сотрудниками иностранных разведок заключается в том, что в рамках уголовного расследования прослушивают и записывают только те переговоры, которые относятся к противоправной деятельности. Когда дело касается иностранных спецслужб, слежение ведется в более широких масштабах

ОБ АВТОРЕ

Уитфилд Диффи (Whitfield Diffie) начинал свою карьеру как эксперт по вопросам криптографии. В 1990-х гг. выступал против попыток правительства продавать третьим странам криптографические технологии. В настоящее время Диффи работает в компании *Sun Microsystems* и занимается вопросами влияния интернет-технологий на безопасность. **Сьюзан Ландау** (Susan Landau) — ведущий специалист компании *Sun Microsystems*, где она занимается изучением проблем безопасности. Ранее работала в нескольких крупных университетах США.

HARRY CAMPBELL

В августе прошлого года Конгресс под давлением Белого дома проголосовал за законопроект, вносящий необходимые поправки в документ «О контроле деятельности иностранных разведок», принятый еще в 1978 г. Речь идет о новом варианте Закона о защите Америки, срок действия которого истек 16 февраля. Белый дом уже давно добивался, чтобы спецслужбам было дано право без санкции суда прослушивать телефонные разговоры и просматривать электронную переписку между иностранцами, находящимися за пределами США, но использующими американские спутниковые каналы, узлы связи или интернет-серверы.

В начале 2008 г. представители спецслужб выступили с рядом инициатив по усилению контроля в сети Интернет. Нужно признать, что проблема безопасности существует. Пользователи постоянно находятся под угрозой проникновения вирусов или иных программ, способных изменять алгоритм работы и управления системой. Такие компьютеры, объединенные в группы, могут использоваться злоумышленниками для решения своих задач.

В январе 2008 г. президент Буш подписал директиву о создании национальной системы мониторинга государственных и частных компьютерных сетей *Cyber Initiative*. Основной задачей системы является контроль информации, поступающей и исходящей из государственных учреждений. В рамках данной программы предполагается сократить количество компьютеров, находящихся в государственных учреждениях и подключенных к сети Интернет, с нескольких тысяч до сотни. Контролю подлежат практически все информационные потоки, как подозрительные, так и простые обращения граждан в официальные ведомства.

ГЕОГРАФИЯ ПРОСЛУШИВАНИЯ

Закон «О контроле деятельности иностранных разведок» с внесенными в него поправками определяет, какие линии связи можно контролировать, имея лишь судебный ордер, а где он не требуется

Администрация стремится использовать те же методы, которыми боролись с разведывательными службами других государств: не идти получать ордер, а просто контролировать. Противники таких планов заявляют, что Интернет за последние годы стал особой информационной средой, в которой присутствуют официальные структуры государства и бизнеса, а также частные лица. Ее можно сравнить с автотрассами. Здесь тоже должны быть своя полиция и служба безопасности.

Система контроля в Интернете существенно отличается от той, которую широко используют для защиты отдельных компьютеров. Принесет ли пользу такой план, и сможет ли предложенная правительством программа укрепить безопасность?

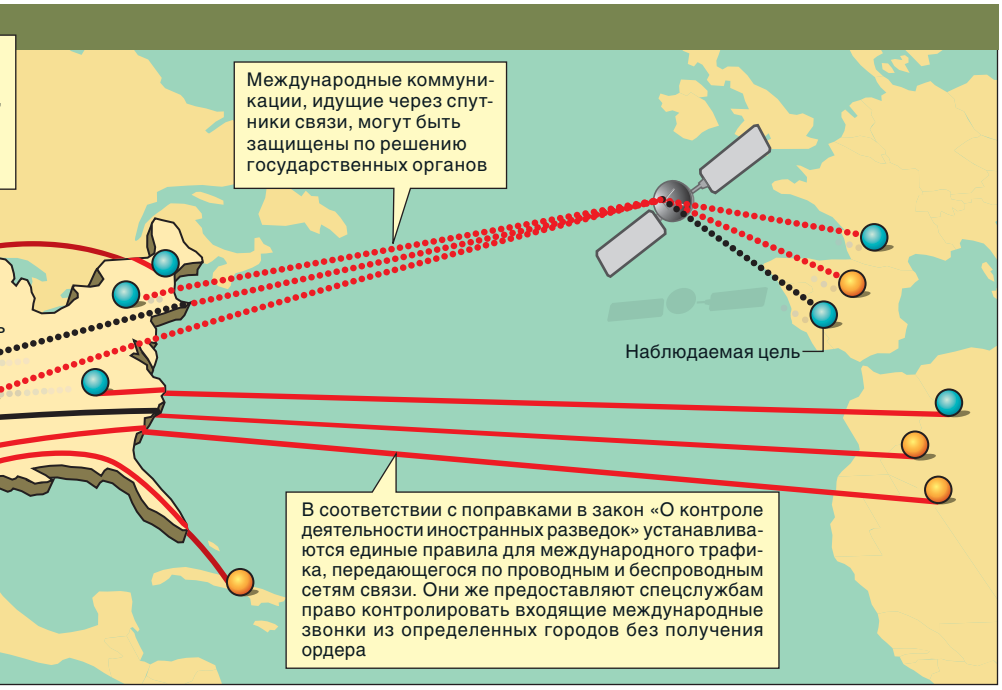
Осуществление подобных задач нельзя отдавать в одни руки. Государство уже имеет опыт в такой критической сфере, как ядерная безопасность, где самые ответственные шаги предпринимаются несколькими структурами или людьми. До последнего времени решение вопроса о контроле телефонных и электронных сообщений принималось государственным органом и исполнялось телекоммуникационными компаниями. Теперь последние поставлены в такие условия, что любой отказ от сотрудничества со спецслужбами может рассматриваться как признак нелояльности. Такие действия могут привести к тому, что государство потеряет контроль над процессом.

Мы стоим в начале пути создания информационного общества — этап столь же значимый, как начало строительства городов в 5 тыс. до н.э. Общение — краеугольный камень человечества, а его защищенность — основа нашей национальной безопасности и демократии. Главное — соблюсти баланс между интересами граждан и государства и не замедлить (или даже остановить) научно-технический прогресс. Иначе все надежды на создание свободного общества тщетны. ■

Коммуникации играют огромную роль в жизни общества, а права граждан неотъемлемы от демократии и национальной безопасности

Перевод: А.П. Худолей

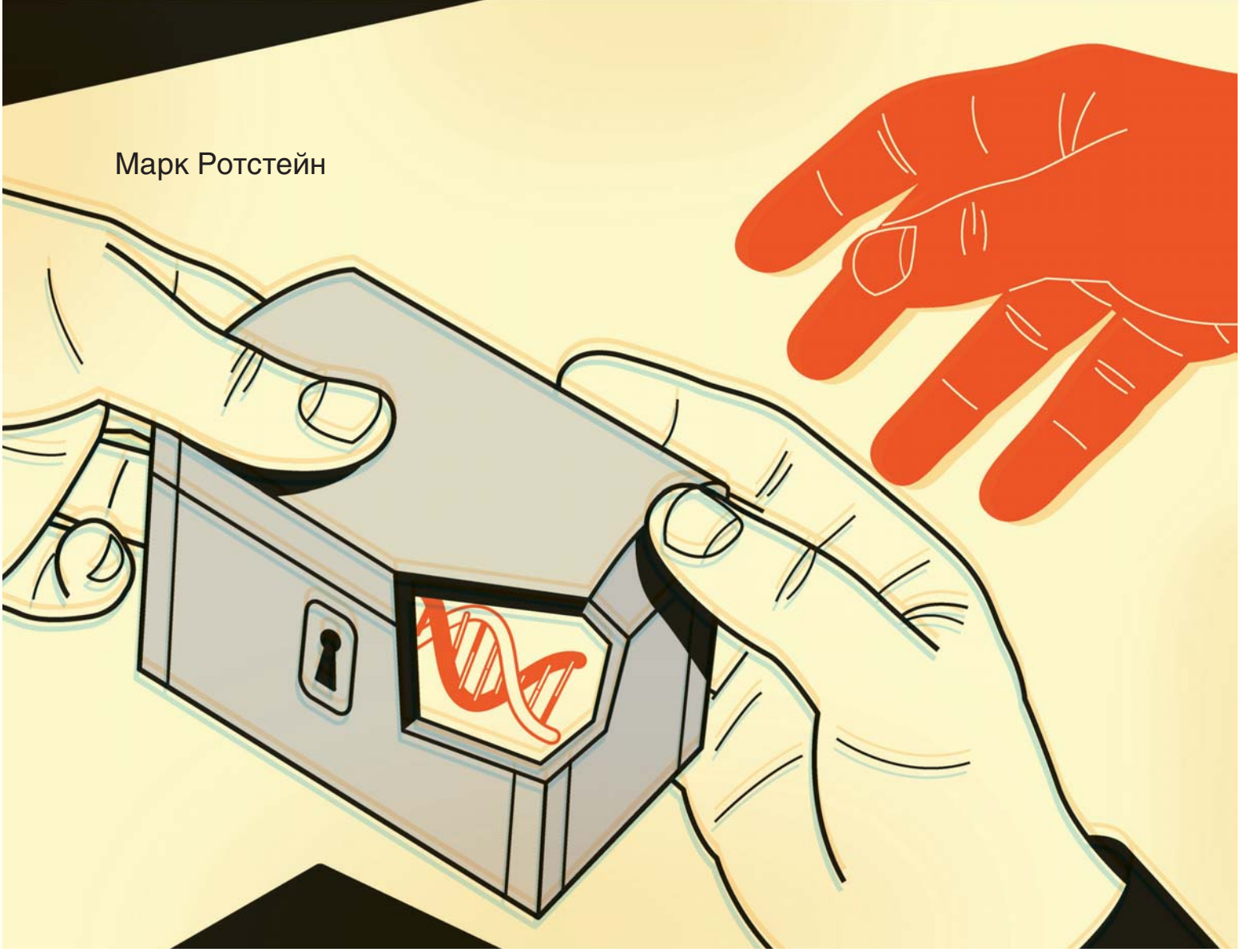
JEN CHRISTIANSEN



ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

- Information Privacy Law: Cases and Materials. Second edition. Daniel J. Solove, Marc Rotenberg and Paul Schwartz. Aspen, 2005.
- Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. Steven M. Bellovin, Matt Blaze, Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Diffie, Susan Landau, Jon Peterson and John Treichler. Information Technology Association of America, 2006. Available at www.itaa.org/news/docs/CALEAVOIPreport.pdf
- Privacy on the Line: The Politics of Wiretapping and Encryption. Updated and expanded edition. Whitfield Diffie and Susan Landau. MIT Press, 2007.
- More information on communications surveillance issues is available at the Web sites of the Center for Democracy and Technology: www.cdt.org; the Electronic Frontier Foundation: www.eff.org; and the Electronic Privacy Information Center: www.epic.org

Марк Ротстейн



ДЕРЖИТЕ СВОИ ГЕНЫ при себе!

Принятые недавно законы, которые запрещают работодателям и страховым агентствам использовать во взаимоотношениях с клиентами информацию об их генетическом статусе, нуждаются в ужесточении

Предположим, что у одного из ваших родственников обнаружен рак прямой кишки (мы от всей души желаем, чтобы этого не произошло). В былые времена вам не оставалось ничего, кроме как ждать и надеяться, что лично вас эта беда минует. Сегодня вы можете пройти генетическое тестирование и узнать, превышает ли для вас риск развития данного заболевания среднестатистическую величину, и в случае необходимости принять превентивные меры. Чем больше узнает лечащий врач о вашем генетическом статусе, тем адекватнее будет лечение.

Эти ожидания еще больше подогрели энтузиазм, с которым в 1990 г.

HARRY CAMPBELL

было встречено известие о начале работ над проектом «Геном человека». Однако вскоре оптимизма поубавилось: стало ясно, что персональные генетические данные — обоюдоострое оружие. Результат простого теста, выявившего какой-либо генетический дефект, легко становился «черной меткой» для его носителя. На этом основании страховые компании могли отказать ему в медицинской страховке или урезать ее стоимость, а кадровые менеджеры — не принять на работу. И ученые, и сотрудники органов здравоохранения осознали, что весь потенциал генетического тестирования никогда не удастся реализовать, если люди будут в массовом порядке отказываться от него из опасений, что результаты будут использованы ненадлежащим образом.

Страхи по поводу дискриминации на основе генетической информации о человеке не оправдались — но только пока. Несмотря на то что со времени окончания работы над проектом прошло пять лет, генетическое тестирование не получило широкого распространения. Во-первых, это очень дорогостоящая процедура — секвенирование генома одного человека обходится в несколько тысяч долларов. Во-вторых, отсутствуют стандартные методы извлечения полезной информации из результатов масштабного сканирования, что ограничивает его применение в медицине.

Тем не менее в развитых странах с хорошо организованной системой здравоохранения генетическое тестирование при многофакторных заболеваниях вскоре приобретет рутинный характер. Благодаря разработке новых технологий и массовой компьютеризации медицинских учреждений тесты становятся более информативными и доступными. Однако сохранение генетической информации в тайне — задача гораздо более сложная, чем может показаться, и принятые законодательные акты, в числе которых Закон о запрете дискриминационного использования генетической информации (*GINA*) от 2008 г., мало что решают. Прежде чем генетическое тестирование действительно получит широкое распространение (а вместе с этим возрастет и число злоупотреблений), необходимо усовершенствовать законодательство.

Под натиском новых данных

Найти способ защиты генетической информации было бы проще, если бы само понятие имело четкое определение. Эксперты в области биомедицины считают, что почти все заболевания в той или иной степени генетически обусловлены, и разграничить чисто генетическую компоненту и компоненты, не являющиеся таковыми, бывает чрезвычайно трудно. Тем не менее законодатели склонны уделять больше внимания защите именно генетических данных. Распространено представление, что к таковым относятся результаты генетического тестирования самого индивида и членов его (или ее) семьи, а также истории болезни их всех (поскольку болезни, встречающиеся в семьях, имеют общие генетические корни).

Данные такого рода становятся все более обширными. В прошедшее десятилетие в генетических исследованиях и их клинических применениях произошло смещение акцента с заболеваний, ассоциированных с одним геном (муковисцидоз или мышечная дистрофия), к более сложным, определяющимся взаимодействиями между многими генами и влиянием окружающей среды (астма, рак, сердечно-сосудистые заболевания, диабет). Сегодня в арсенале клиницистов — более 1,5 тыс. генетических тестов, на стадии разработки находятся еще сотни. Как только они станут частью обычной процедуры обследования больного, большинство, если не все показатели состояния здоровья будут содержать значимую генетическую компоненту.

В дальнейшем такая тенденция будет только усиливаться. Тесты могут заключаться в идентификации однонуклеотидных замен среди сотен тысяч азотистых оснований — всем известных «букв» *A*, *T*, *G* и *C* генетического алфавита, составляющих молекулу ДНК. Такие замены часто ассоциируются с конкретными заболеваниями. Несмотря на мнение большинства ученых о преждевременности рутинного применения подобных технологий, некоторые компании (в их числе *23andMe* в Калифорнии, *deCODE* в Рейкьявике) ведут агрессивную политику продвижения геномного сканирования, даже не имея лицензии на деятельность, связанную с медициной. Через какие-нибудь десять лет каждый сможет получить расшифровку своего генома, заплатив менее $1 тыс.

Следует учитывать еще два важных момента. От развития методологии исчерпывающего сканирования генома будет зависеть распространение персонифицированной медицины — подбора оптимальной для данного больного схемы лечения. Фармакогеномное тестирование уже становится обычной процедурой при выборе лекарственных препаратов и их доз для терапии некоторых онкологических больных, и эта практика будет только расширяться. Развитие получает и так называемая токсикогеномика — применение генетических инструментов для исследования реакции организма на токсины. Это важно,

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Генетическое тестирование получает все большее распространение, и теперь в медицинской карте пациента могут содержаться сведения, которые он не хотел бы разглашать. С переводом всех записей в карте в электронную форму доступ к данным посторонних лиц упрощается.
- Обладая возможностью узнать о состоянии здоровья клиента, страховые компании могут отказать ему в выплате компенсации, а кадровые агентства — в приеме на работу.
- Существующие законы практически не защищают права граждан в этой сфере. Необходимо предоставлять пациентам больше возможностей контроля доступа к их персональным данным, раскрывать последние только с письменного разрешения владельца, наказывать нарушителей.

ЗАИНТЕРЕСОВАНЫ, НО НЕ БЕЗОГЛЯДНО

Согласно оценкам, полученным в мае 2008 г. службой *Knowledge Networks*:

- 47% американцев хотели бы стать пользователями служб, обеспечивающих доступ к их персональным сведениям медицинского характера в режиме реального времени (в числе таких служб — *Google Health* или *Microsoft HealthVault*)
- 19% респондентов, однако, ответили, что их беспокоит, смогут ли соответствующие компании обеспечить конфиденциальность информации
- *Markle Foundation* выработала ряд рекомендаций, обеспечивающих максимальную защиту медицинской информации. Гражданин имеет право проследить, кто запрашивал его данные, и оспорить правомочность действий ответственного лица

в частности, в ситуации, когда предполагается работа человека во вредных условиях, или если изучается влияние на его здоровье веществ, загрязняющих окружающую среду.

Проблема защиты медицинской информации усугубляется с переходом на компьютерные способы ее хранения и обработки, хотя на первый взгляд это кажется странным. Медицинские данные любого рода все чаще не записывают на бумаге, а заносят в компьютер, что должно повысить качество медицинского обслуживания и снизить его стоимость. В США создается «сеть сетей» — Общенациональная информационная сеть в системе здравоохранения (*Nationwide Health Information Network, NHIN*). Ее основной задачей станет разработка электронных форматов хранения данных, что позволит сопоставлять результаты самых разных обследований и без труда передавать их по Сети. В конечном счете электронная история болезни будет содержать исчерпывающую информацию о состоянии здоровья пациента на протяжении всей его жизни — от рождения до смерти.

Однако отношение к созданию *NHIN* двоякое. Когда информация хранится в рукописном виде, ее защиту обеспечивает сама неупорядоченность данных. Именно потому, что записи носят фрагментарный характер, их бывает трудно не только сопоставить, но даже просто найти — они разбросаны по различным медицинским учреждениям и относятся к самым разным временным периодам. Другое дело — информация, упорядоченная во времени и собранная в одном месте. Теперь диагноз «депрессия», поставленный вам во время учебы в колледже, или результат генетического тестирования, проведенного в связи с болезнью кого-то из родственников, навсегда останется в вашей электронной медицинской карте. Многие люди, страдающие недугом, порочным с точки зрения обывателя (например, пристрастием к спиртному), уже сейчас отказываются от лечения, опасаясь огласки, а это наносит большой ущерб и самому человеку, и здоровью нации в целом. Между тем для эффективного лечения не всегда нужна исчерпывающая информация о пациенте. Например, для назначения физиотерапевтических процедур по поводу растяжения связок лодыжки совсем не нужно знать о предрасположенности пострадавшей к раку молочной железы, а зубному врачу не важно, были среди родственников пациента больные хореей Гентингтона или нет.

Для того чтобы предотвратить нежелательный для пациента доступ к его медицинским данным, в таких странах, как Канада, Нидерланды и Великобритания, изыскиваются возможности ограничения объема разрешенной к просмотру информации. Среди предлагаемых мер — полный контроль пациента над своими медицинскими данными,

Многие люди боятся, что не получат работу, если не впишутся в рамки медицинских требований, предъявляемых компанией

HARRY CAMPBELL

вплоть до изъятия из истории болезни некоторой устаревшей информации или предоставления только тех сведений, которые необходимы для постановки диагноза. Для этого предполагается создавать базы данных, открытые для всех имеющих отношение к делу лиц, и независимые файлы, которые можно открывать только по указанию пациента. В сети электронных историй болезней, созданной в Дании — стране, более других преуспевшей на этом поприще, — пациент может блокировать любую информацию в своей истории болезни. Такая возможность используется редко, но само ее наличие чрезвычайно важно с психологической точки зрения.

В США подобные разработки пока не ведутся. Остается неясным, как соблюсти баланс между необходимостью для лечащего врача иметь как можно более полную информацию и желанием пациента сохранить какие-то факты в тайне. Если он волен полностью контролировать доступ к своей истории болезни, то как лечащий врач получит необходимые данные? Ему придется проводить повторные обследования, что неизбежно приведет к удорожанию лечения. С другой стороны, если возможности контроля со стороны пациента над своей историей болезни кажутся ему недостаточными, он может принять ответные меры — например изъять какую-то личную информацию из базы данных или вообще отказаться от определенных обследований.

Этим проблемы, связанные с компьютеризацией системы медицинского обслуживания, не исчерпываются. Должны ли распространяться запреты на службы, занимающиеся сканированием электронных данных для выявления возможных взаимодействий между лекарственными веществами, если они гарантируют неразглашение информации? Нужно ли снабжать электронную историю болезни примечанием, что доступ к каким-то сведениям возможен только с разрешения пациента? И что делать в экстренных ситуациях?

СТОИТ ЛИ НАРУШАТЬ ПОКОЙ БЛИЗКИХ?

Сара, сорокалетняя женщина, мать троих детей, проанализировала результаты своих тестов и пришла к выводу, что в будущем ей грозят болезнь Альцгеймера, а также рак молочной железы. Стоит ли ей сообщать своим детям и родственникам, что риск развития этих недугов у них тоже повышен?

С юридической точки зрения ответ однозначен: ни один суд не скажет вам, что вы не имеете права сообщить близким результаты пройденного вами генетического тестирования. С моральной стороной дела все обстоит гораздо сложнее. Решение зависит от того, насколько серьезно предполагаемое заболевание, как долго болезнь будет протекать бессимптомно, излечима ли она. Имеют значение и взаимоотношения между вами и родственниками, их эмоциональность, возраст, заинтересованность в тех сведениях, которые вы хотите им сообщить, и многое другое.

Основную роль в принятии решения играет то, насколько опасно для жизни ваше заболевание. Бывают случаи, когда при определенных стрессовых воздействиях оно оказывается смертельным. Например, носитель мутации, ассоциированной со злокачественной гипертермией, может умереть во время хирургического вмешательства, если применен неподходящий наркоз. Человеку с гипертрофированной кардиомиопатией грозит внезапная смерть при чрезмерных физических нагрузках. В подобных случаях оповещение родных об опасностях, которые им грозят, вполне оправдано и даже необходимо.

Но бывают случаи, когда генетической информацией лучше не делиться. Допустим, что в результате тестирования выяснилось, что человек, считавшийся отцом ребенка, таковым не является. Вся семья в шоке. Прежде чем проходить тестирование, а уж тем более сообщать кому-либо о его результатах, вам следует обратиться в генетическую консультацию. К сожалению, сегодня в США таких консультаций всего 2,5 тыс. Самая распространенная ошибка состоит в том, чтобы пассивно дожидаться результатов анализа, не обдумывая дальнейшие шаги. Всякий, решившийся на тестирование, должен заранее продумать, как он поступит с близкими. Простого решения здесь не существует, поэтому лучше всего обратиться за советом к профессионалам.

Слабые законы

Поскольку мы стоим на пороге всеобщей компьютеризации системы учета персональных генетических данных, решение вопроса юридической защиты частной информации не терпит отлагательств. К сожалению, в США соответствующие законы отсутствуют. Последние законодательные акты по этому поводу были приняты в 1996 г. (Закон о страховании здоровья и медицинской ответственности, *HIPAA*) и в 2003 г. (Правило конфиденциальности, *Privacy Rule*).

ОБ АВТОРЕ

Марк Ротстейн (Mark A. Rothstein) — заведующий кафедрой юриспруденции и медицины, а также директор Института биоэтики, здравоохранения и законодательства в Медицинской школе Луисвиллского университета. С 2001 по 2008 гг. возглавлял подкомитет по защите конфиденциальных данных в Национальном комитете по статистике в области здравоохранения, который давал рекомендации по соответствующим вопросам правительству США.

ГЕНЕТИКА НАСТУПАЕТ

В 2008 г. дан старт проекту 1000 *Genome*, который разработан международным исследовательским консорциумом. Его задача — построение карты генома человека в пять раз более детальной, чем та, что получена в рамках проекта *HapMap*.

Открытия, сделанные во время реализации последнего проекта, послужили стимулом к масштабным исследованиям геномов в целом, что позволило идентифицировать более 130 генетических отклонений, связанных с различными заболеваниями (среди них диабет II-го типа, коронарная болезнь, рак предстательной железы, рак молочной железы, ревматоидный артрит, психические расстройства).

Участники проекта 1000 *Genome* надеются в ближайшие три года секвенировать геномы по крайней мере 1 тыс. жителей Земли. Более детальную информацию можно найти на сайте www.genomes.org

Однако акт 2003 г. касается только информации, зафиксированной в электронном виде. Это делают далеко не все медицинские учреждения, спортивные организации и фитнес-клубы. Не урегулированы и вопросы компенсации ущерба, понесенного в связи с утечкой данных. На сегодня известен лишь один случай выплаты штрафа, так что правонарушители чувствуют себя спокойно.

Далее, *HIPAA* затрагивает только учреждения системы здравоохранения, однако общественность волнуют прежде всего страховые и кредитные организации, а также кадровые службы. Обычной практикой в работе администрации предприятий считается требование личной подписи работника под запросом в соответствующие медицинские учреждения, чтобы те сообщили, каково состояние его здоровья. По некоторым оценкам, в США ежегодно посылается более 25 млн таких запросов.

Компании, требующие раскрытия медицинской информации, действуют в рамках закона; все дело в ее объеме. Например, какой-нибудь энергетической компании совсем не нужно знать, имеется ли у претендента на рабочее место мутация, способствующая возникновению сердечно-сосудистого заболевания в далеком будущем. В то же время большинство законодательных актов, касающихся доступа к информации личного свойства, настолько расплывчаты, что фактически не указывают никаких ограничений.

Данную проблему поможет решить система электронных историй болезни. Можно сканировать все данные и выбрать из них только те, которые имеют отношение к делу. Однако необходимо создать алгоритм, определяющий, что считать «имеющим отношение к делу». Например, можно включить в него требование, чтобы раскрывалась только информация, которая касается предполагаемой продолжительности жизни человека, желающего застраховать свою жизнь. Но поскольку коммерческие организации вряд ли проявят инициативу в создании соответствующих алгоритмов, нужны законодательные акты, побуждающие их к этому.

Частные инициативы

Ввиду слабости федерального законодательства в сфере регуляции обращения с персональными генетическими данными каждый штат решает возникающие проблемы по-своему. Так, в некоторых из них принят акт об «эксклюзивности генетической информации», согласно которому правила работы с ней отличаются от правил для других, тоже имеющих отношение к состоянию здоровья данных. Оправдан ли такой подход, пока не ясно, но он соответствует правилам, действующим при работе с информацией о таких состояниях, как токсикомания, психические расстройства и СПИД.

Законодательные акты, принятые в разных штатах, не идентичны. Так, в 12 штатах от граждан требуют письменного согласия на генетическое тестирование, предварительно проинформировав их обо всех плюсах и минусах, а в других 27 штатах результаты тестов могут быть раскрыты только с согласия пациента. Однако страховые и кадровые агентства по-прежнему вправе требовать от клиента разрешения на доступ к его истории болезни. Чтобы снять противоречие, в 47 штатах запрещено обосновывать отказ в выдаче страховки или ограничении ее размеров генетической информацией о клиенте. В 35 штатах введен запрет на генетическое тестирование как необходимое условие приема на работу, однако работодатель вправе потребовать письменного согласия кандидата на доступ к информации о состоянии его здоровья.

Разноголосица в законодательстве вынудила Конгресс принять дополнительные меры по защите информации частного характера и в конце концов одобрить Закон о запрете дискриминационного использования генетической информации (*Genetic Information Nondiscrimination Act, GINA*), который находился на рассмотрении с середины 1990-х гг. К сожалению, этот закон немногим лучше тех, что приняты в различных штатах, и не касается страхования жизни и любых долговременных мероприятий по медицинской помощи.

Универсальное решение

Недостатки систем регулирования актов *GINA* и *HIPAA*, как и федеральных законов, связаны не с тем, что кому-то было выгодно оставить лазейки в законодательстве, или что кто-то что-то недосмотрел. Они стали следствием несовершенства самой системы здравоохранения (*см. в этом номере: Дайсон Э. Размышления о приватности 2.0*). Граждане США могут получить страховку одним из трех способов: по месту работы (большинство предприятий и организаций страхует своих сотрудников), в индивидуальном порядке и в рамках федеральных программ, таких как *Medicare* и *Medicaid*. В первых двух случаях страховщики оценивают индивидуальные и коллективные риски, а также размеры соответствующих выплат. Конечно, их первоочередная задача — защитить финансовые интересы страховой компании. Ее работники хотят знать, чем болел

HARRY CAMPBELL

их клиент в прошлом, и какова вероятность, что его настигнет тот или иной недуг в будущем: это позволит точнее оценить сумму выплат.

Ни один из упомянутых выше законов по защите частной информации не касается *Medicare* или *Medicaid*, поскольку технически данные программы обеспечивают лишь некое вспомоществование, а не страховку. Для защиты информации в их рамках не раз пытались разработать соответствующие акты, но на правительственном уровне никто не занимался конкретно генетической информацией по причине отсутствия каких-либо нормативов.

Несомненно, защита информации частного характера — обязанность государства; именно так обстоит дело в Канаде. В этом случае разрабатываются некие универсальные программы, риск распределяется между всеми гражданами, и расходы оплачиваются населением в целом. Какова вероятность заболеть любого отдельного индивида, не важно с точки зрения страховки, а потому нет нужды «охотиться» за закрытой информацией. Это сразу решает две проблемы: люди не боятся, что не получат страховку или получат ее в урезанном виде, и не опасаются, что им откажут в приеме на работу, если состояние здоровья не впишется в рамки, установленные работодателем. Конечно, система не безупречна, но предпосылок к дискриминации гораздо меньше.

В США такая тактика вряд ли будет принята в ближайшее время, хотя сама тема активно обсуждается в ходе предвыборной президентской компании. Следовательно, необходимо выработать более совершенные законы, касающиеся неприкосновенности медицинской информации. В настоящее время известно лишь о нескольких официально документированных случаях затруднений с устройством на работу или страхованием, связанных с генетическими данными, однако медицинские генетики часто сталкиваются с отказом пациентов пройти генетическое тестирование из боязни, что в дальнейшем они подвергнутся дискриминации. И в самом деле: в ближайшие 10 лет число доступных генетических тестов существенно возрастет, а электронные базы медицинских данных слабо защищены от несанкционированного проникновения.

В ходе дискуссий о поисках надежных способов защиты приватных данных становится все более очевидно, что сделать это будет сложно и затратно. Жесткие защитные меры могут обеспечить закрытость информации для тех, у кого нет официально оформленного разрешения, но важно еще четко определить круг лиц и учреждений, имеющих право его выдавать, и указать перечень причин, по которым получить такой документ необходимо.

Эффективное законодательство обязано удовлетворять как минимум четырем требованиям. Во-первых, оно должно соблюдать баланс между правами нанимателя и работника и учитывать трудности с получением страховки. Во-вторых, оно должно ограничить использование информации о вероятности того или иного заболевания в будущем в немедицинских целях, в том числе при страховании жизни и долгосрочном медицинском страховании. В-третьих, любое законодательство обязано очерчивать круг лиц, имеющих право доступа к частной информации, наказывать нарушителей и обеспечивать защиту людей, пострадавших от неправильных действий тех, кто получил доступ к их персональным данным. И наконец, электронная система хранения данных должна быть организована таким образом, чтобы проникнуть в нее было очень трудно. Выполнение всех этих условий станет лишь первым шагом к созданию действительно надежной системы защиты. ■

В Канаде и Нидерландах контроль над сведениями, касающимися состояния здоровья, может быть передан в руки самих пациентов

Перевод: Н.Н. Шафрановская

Стивен Эшли

СРЕДСТВА шпионажа

Камеры ночного видения, биометрические датчики и многие другие устройства уже сегодня позволяют шпионам проникать в личное пространство людей. А скоро могут появиться и миниатюрные автономные разведчики с дистанционным управлением

СРЕДСТВА ПОДСМАТРИВАНИЯ

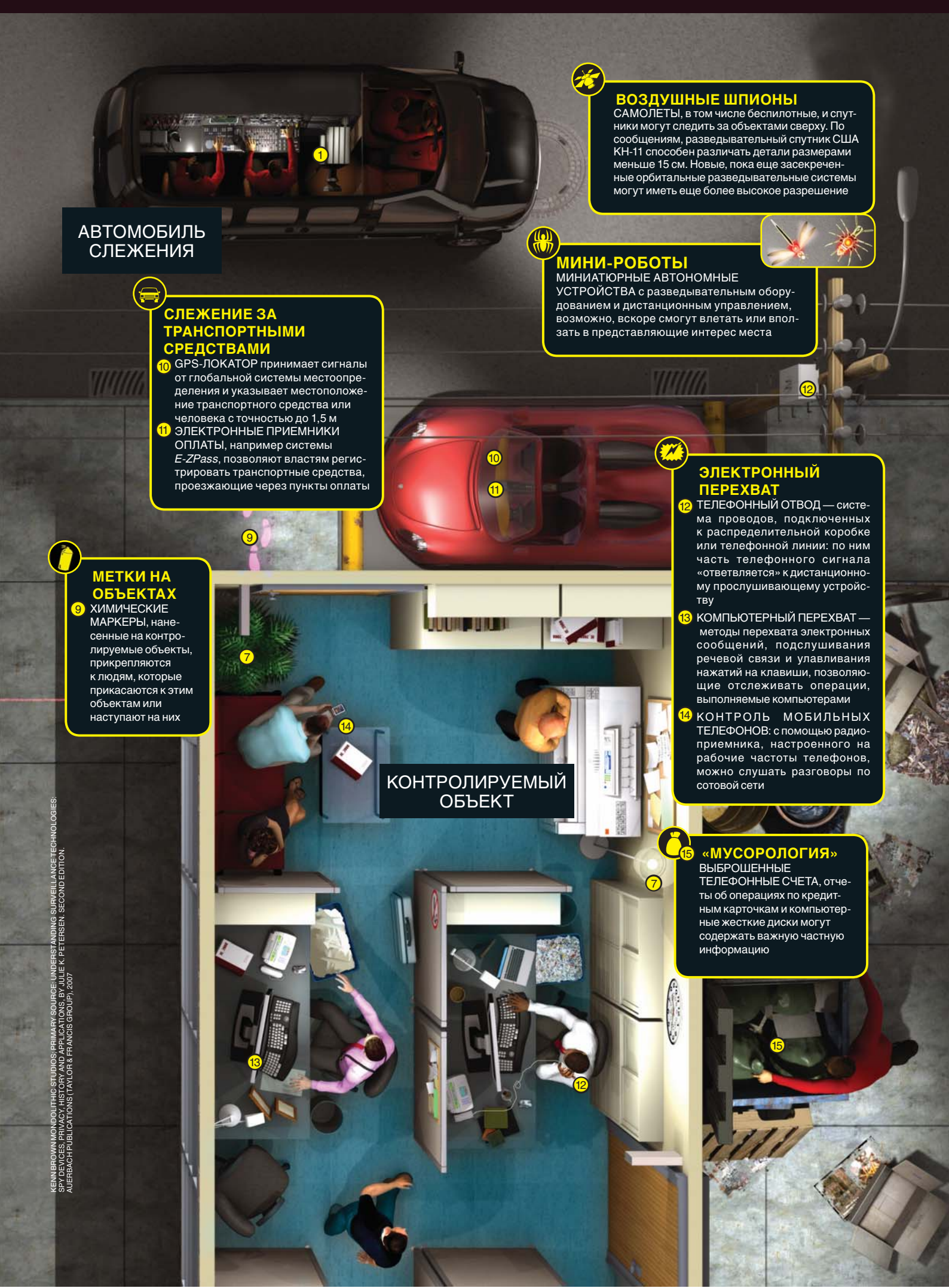
1. ЦИФРОВЫЕ ФОТО- И ВИДЕОКАМЕРЫ с длиннофокусными объективами позволяют агентам различать детали объектов с больших расстояний. Агент с телефотокамерой может читать газетные заголовки (а, возможно, и подзаголовки) с расстояния, равного длине футбольного поля
2. ОЧКИ И ТЕЛЕСКОПЫ НОЧНОГО ВИДЕНИЯ с фотоумножителями способны во много раз увеличивать доступную освещенность, а тепловые датчики позволяют обнаруживать живых существ и нагретые от работы механизмы в полной темноте

БИОМЕТРИЧЕСКИЕ ИДЕНТИФИКАТОРЫ

3. ГОЛОС, черты лица, походка и другие особенности позволяют идентифицировать личности, чьи физические или поведенческие признаки зарегистрированы в базах данных
4. ДАТЧИК ДНК, одно из последних биометрических устройств, берет пробы ДНК, оставленной, например, на стекле или дверной ручке, и сравнивает их с генетической информацией, содержащейся в файле
5. ИСКУССТВЕННЫЙ НОС обнаруживает запах тела человека и сравнивает его с записанными

ПОДСЛУШИВАЮЩИЕ УСТРОЙСТВА

6. НАПРАВЛЕННЫЙ МИКРОФОН с параболическим отражателем или «ружьем» (линейным приемником) позволяет подслушивать разговоры на открытом воздухе с расстояния в сотню метров
7. «ЖУЧОК» — маленький потайной микрофон с радиопередатчиком малого радиуса действия (например, на растении в горшке, как изображено на странице напротив) — передает разговоры на радиоприемник, а тот пересылает их на записывающее устройство или наушники агента (*показан сидящим ниже*)
8. ЛАЗЕРНЫЙ ЛУЧ, отраженный от стекла, позволяет улавливать его вибрации, вызванные звуками разговоров в помещении. Оптический приемник преобразует структуру отраженного луча в звук



KENN BROWN MONOLITHIC STUDIOS; PRIMARY SOURCE: UNDERSTANDING SURVEILLANCE TECHNOLOGIES: SPY DEVICES, PRIVACY, HISTORY AND APPLICATIONS, BY JULIE K. PETERSEN. SECOND EDITION. AUERBACH PUBLICATIONS (TAYLOR & FRANCIS GROUP), 2007

радиометка — это вы

Катрин Олбрехт

Миниатюрные радиочастотные идентификационные метки (Radio-Frequency Identification Tags, RFID), давно используемые для отслеживания движения поставок и запасов, в последнее время стали все шире применяться для маркировки потребительских товаров. Защитники частной информации утверждают, что устройства представляют угрозу для тех, кто «носит» их, часто не подозревая об этом

HARRY CAMPBELL

Средний потребитель может не подозревать, как много *RFID*-меток он имеет при себе. Они интегрированы в личные вещи и даже в некоторые предметы одежды

Американцы, проживающие в приграничных с Канадой или Мексикой штатах, уже получают водительское удостоверение, допускающее дистанционное считывание. За внедрение таких документов, предназначенных для идентификации граждан США, пересекающих границу страны, ратует Министерство внутренней безопасности. Но тем, кто обеспокоен безопасностью и неприкосновенностью личной сферы, стоит дважды подумать, прежде чем получать такой идентификатор.

Новое удостоверение содержит радиочастотную идентификационную метку *RFID*, которая считывается через бумажник, кошелек или карман с расстояния до 10 м. Каждая такая метка представляет собой микросхему с уникальным идентификационным номером. Когда ее носитель приближается к пункту пограничного контроля, радиоволны, излучаемые считывающим устройством (*RFID*-ридером) и принимаемые антенной метки, активизируют микросхему, и она передает свой идентификационный номер. К тому моменту, когда владелец метки доберется до пограничника, этот номер уже поступит в базу данных, и на экране компьютера появятся фотография владельца и сведения о нем.

Несмотря на то что получение такого «усовершенствованного» водительского удостоверения в приграничных штатах является делом добровольным, специалисты по безопасности опасаются, что желающие получить такие права не знают о риске, которому они подвергаются. Доступ к личным данным сможет получить любой человек, у которого есть *RFID*-ридер (а достать его несложно), — недобросовестный торговец, правительственный агент, вор или просто любопытный. Более того, когда владелец такого удостоверения совершает транзакцию по кредитной карточке, радиометка может быть использована в качестве идентификатора наряду с проездными билетами и пропусками, кредитными карточками, одеждой, телефонами и даже продовольственными товарами.

RFID-метки — это активный штрихкод, который ранее использовали в основном для идентификации товаров. Вместо того чтобы сканировать универсальный код продукта (*Universal Product Code, UPC*), работник склада может регистрировать содержимое каждого контейнера, например с бумажными полотенцами, просто считывая уникальный порядковый номер прикрепленной к нему *RFID*-метки. В центральной базе данных этому номеру соответствует полный перечень содержимого контейнера. Но люди — не бумажные изделия. За последнее десятилетие инсталляция микросхем в потребительские товары и в документы вызвала новый виток дебатов в отношении безопасности и защиты частной информации именно потому, что технология *RFID* — очень эффективное средство слежения. Степень кодирования информации в радиометках не высока, а существующие законы не защищают граждан от недобросовестного слежения и получения сведений о личности в условиях растущей «помеченности» жизни.

Кроме штрихкодов

Первые радиометки использовались во время Второй мировой войны для распознавания своих и чужих самолетов. С конца 1980-х гг. эти технологии стали применяться для оплаты проезда в общественном транспорте, а в 1999 г. были предприняты первые попытки учитывать и контролировать движение товаров с помощью радиометок. В частности, компании *Procter & Gamble* и *Gillette* (которые впоследствии объединились, став крупнейшим мировым производителем потребительских товаров) совместно с инженерами Массачусетсского технологического института создали консорциум *Auto-ID Center* для разработки компактных, эффективных и дешевых *RFID*-меток, способных со временем заменить на потребительских товарах штрихкоды стандарта *UPC*.

Консорциум привлек инвесторов более чем из 100 компаний и правительственных учреждений и к 2003 г. представил рабочий прототип. Сторонники меток предрекали, что микрочипы будут революционным новшеством в управлении товаропотоками и для защиты от подделок (*см.: Уонт Р. Тотальная автоматизация // ВМН, 2004, № 4*).

Законодательное принятие правительством новой технологии потребовало, чтобы Главное управление обслуживания (*GSA*), федеральная организация, занимающаяся закупками для государственных учреждений, подготовило в 2004 г. меморандум, рекомендующий руководителям всех федеральных ведомств внедрение технологии *RFID*. Сразу после этого практически все учреждения, от Управления общественной безопасности до Управления по пищевым продуктам и медикаментам разработали программы внедрения *RFID*-технологии.

В те же годы подобные планы реализовывались и в других странах. В 2003 г. Международная организация гражданской авиации ИКАО (агентство ООН, занимающееся, в частности, разработкой мировых стандартов на паспорта) поддержа-

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Радиочастотные идентификационные метки (*RFID*-метки) все чаще маркируют личные вещи и документы, удостоверяющие личность.
- Поскольку метки задумывались как эффективные средства слежения, но надежными средствами защиты не оснащены, человек, имеющий при себе *RFID*, уязвим для тайной слежки и получения сведений о нем.
- Законодатели во всем мире не сделали почти ничего для снижения этих рисков для граждан.

КАК РАБОТАЕТ RFID

Обычно RFID-система работает на основе взаимодействия считывающего устройства (*RFID*-ридера) с *RFID*-меткой и с базой данных, содержащей информацию о считываемой метке. Метка состоит как минимум из интегральной схемы, содержащей уникальный опознавательный номер, и катушки или антенны, способной передавать энергию, получаемую от *RFID*-ридера

ла идею использования *RFID*-меток в паспортах. Сегодня ИКАО рекомендует использование этих радиометок во всех поддающихся сканированию электронных паспортах.

С момента своего появления это нововведение вызывает споры в отношении безопасности и возможного риска вмешательства в личную сферу. В отчете ИКАО за 2006 г. один ее представитель обещал, что меры шифрования обеспечат «такой уровень защиты, который убедит самых обеспокоенных владельцев паспортов в том, что их личные данные не смогут считываться без их ведома».

Специалисты по безопасности быстро доказали обратное. В 2007 г. британский специалист Адам Лори (Adam Laurie) взломал защитный код британского паспорта и дистанционно считал содержащуюся в нем личную информацию, хотя сам документ находился в запечатанном почтовом конверте. Примерно в то же время немецкий консультант по безопасности Лукас Грюнвальд (Lukas Grunwald) скопировал данные с чипа германского паспорта и ввел их в другую *RFID*-метку для фальшивого паспорта. Исследователи из Карлова университета в Праге нашли такие же слабые места в чешских электронных паспортах.

Несанкционированные факты доступа к частной информации не послужили препятствием для использования *RFID*-меток. Напротив, данная технология стала внедряться во многих странах. Малайзия выпустила около 25 млн бесконтактных внутренних паспортов. В Катаре появились электронные документы, в которых кроме информации о личности владельца хранится его отпечаток пальца. А в рамках *RFID*-проекта, который обозреватели считают самым крупным в мире, китайское правительство выделяет $6 млрд на национальные удостоверения личности с *RFID*-метками для миллиарда граждан и резидентов.

Однако между удостоверениями личности с *RFID*-метками и новыми водительскими удостоверениями есть существенное отличие. В большинстве стран *RFID*-метки бесконтактных внутренних удостоверений личности и электронных паспортов отвечают нормам отраслевого стандарта *ISO* 14443, разработанного специально для идентификационных и платежных карт и предусматривающего некоторые средства защиты информации, а в американских «пограничных» водительских удостоверениях используются микрочипы *RFID*-стандарта *EPCglobal Gen 2*, который был разработан для отслеживания движения запасов на складах.

Если стандарт *ISO* 14443 предусматривает наличие хотя бы простейших средств шифрования и требует, чтобы считывание производилось только с малых расстояний (порядка дюймов, а не футов), то в стандарте *Gen 2* шифрование обычно отсутствует, а меры защиты информации минимальны. Считывание информации стандарта *ISO* 14443 требует взломать шифр, в то время как для стандарта *Gen 2* особого искусства не требуется, нужен только любой подходящий *RFID*-ридер. Хакер или преступник с *RFID*-ридером может считывать «пограничные» карточки через кошелек с другого конца комнаты или даже через стену.

В МАГАЗИНЕ

Розничная торговля изучает возможности использования *RFID*-меток не только для контроля над движением товаров. Это «волшебное зеркало» может считывать метки на одежде и выдавать на дисплей сведения об изделии, о его цвете или об аксессуарах

LILA RUBENSTEIN AND TOMMY MOORMAN (illustration); COURTESY OF AVERY DENNISON AND THEBIGSPACE (magic mirror)

К апрелю 2008 г. водительские удостоверения с *RFID*-метками получили более 35 тыс. водителей из штата Вашингтон. Участвовать в программе согласились и другие пограничные штаты, включая Аризону, Мичиган и Вермонт, а скоро к ним присоединится и Нью-Йорк.

Однако возможность взлома защиты карточек злоумышленниками — не единственная причина для беспокойства. Многие защитники частной сферы опасаются, что документы, допускающие дистанционное считывание, могут быть незаконно использованы правительствами для слежения за своими гражданами.

Китайские национальные идентификационные карточки содержат массу личной информации: сведения о здоровье, репродуктивной истории, работе, вероисповедании, национальности и даже имя и номер телефона владельца. Но больше опасений вызывает то, что карточки составляют часть большого проекта покрытия китайских городов сетью современных технологий слежения. Майкл Линь (Michael Lin), вице-президент частной компании *China Public Security Technology*, поставляющей карточки для этой программы, не стесняясь, представляет их газете *New York Times* как «средство правительственного контроля над населением в будущем».

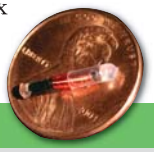
Жизнь с меткой

Если предположение о возможности использования *RFID*-меток компаниями для получения данных о людях кажется вам надуманным, то стоит посмотреть патент *IBM*, представленный компанией в 2006 г. (заявка на него была подана в 2001 г.). В нем прямо говорится об использовании радиометки для слежения за гражданами и получения информации о них даже при условии, что официальный доступ к базам данных строго ограничен. Документ под названием «Идентификация лиц и слежение за ними с помощью предметов, оборудованных *RFID*-метками, в условиях магазина» подробно описывает возможности *RFID*-меток в плане глобального контроля. Объединенные сети *RFID*-ридеров, называемые «блоками слежения за людьми» (*Personal Tracking Units, PTU*) будут размещаться практически везде — в торговых залах, в аэропортах, на железнодорожных и автовокзалах, в лифтах, в поездах, на самолетах, в туалетах, на стадионах, в библиотеках, театрах и музеях, — чтобы тщательно отслеживать перемещения людей.

Согласно данному патенту, система будет работать следующим образом: сканер отслеживает *RFID*-метку покупателя и при его перемещении по магазину регистрирует радиосигналы меток, которые тот имеет при себе. Системы *PTU* способны хранить записи о местах, в которых побывал посетитель, и о времени посещения.

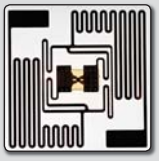
Отсутствие сведений о личности в *RFID*-метке не вызывает затруднений при идентификации, поскольку их можно получить, когда покупатель использует свою кредитную или дисконтную карту. Достаточно один раз определить связь между уникальным номером *RFID*-метки и личностью человека, чтобы карточка стала идентификатором человека. Новые водительские удостоверения штата Вашингтон идеально подходят для отслеживания людей в магазинах, т.к. их уже сегодня можно считывать с помощью существующих сканеров стандарта *Gen 2*, применяемых в магазинах сетей *Wal-Mart*, *Dillard's* и *American Apparel*.

По мере увеличения числа граждан, имеющих при себе предметы с *RFID*-метками (включая одежду и обувь), инфраструктура слежения будет становиться все более полезной для владельцев магазинов. Сегодня в обращении находятся десятки миллионов бесконтактных кредитных и банкоматных карточек с *RFID*-метками



ТИПЫ МЕТОК

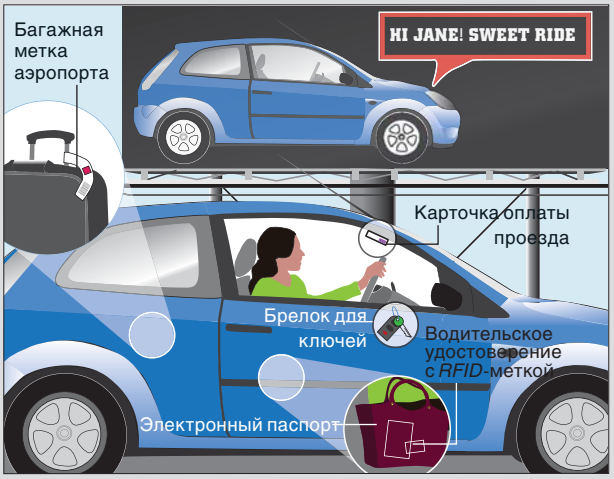
Технические стандарты, устанавливаемые компанией *EPCglobal*, позволяют классифицировать *RFID*-метки в соответствии с их возможностями. Каждый следующий класс добавляет функции к тем, что имеются у предшествующего. Класс I является «пассивным», т.е. требует *RFID*-ридера для запуска сеанса активации. Пассивные метки могут считываться с расстояния до 10 м, активные — с расстояния до 100 м и более



	Функциональные возможности	Примеры применения
КЛАСС I (пассивные)	• Уникальный идентификационный номер • Функция блокировки метки • ПЗУ • Новые версии *Gen 2* могут быть перезаписываемыми и защищены паролем	• Товары и запасы • Новое водительское удостоверение США • Карточка-ключ
КЛАСС II (пассивные)	• Номер с увеличенным числом разрядов • Дополнительная перезаписываемая память • Доступ с помощью пароля	• Электронный паспорт • Кредитная карточка • Национальное удостоверение личности
КЛАСС III (полуактивные	• Один или несколько датчиков и источник питания	• Контейнеры и складские датчики
КЛАСС IV (активные)	• Передатчик и источник питания • Может инициировать связь с ридером и другими метками	• Брелок для ключей от автомобиля • Метка для животного • Карточка оплаты проезда по платным дорогам

RFID КАЖДЫЙ ДЕНЬ

RFID-метки инсталлируются в большое число объектов, используемых людьми повседневно. Они создают удобство для потребителей и помогают бизнесу управлять запасами. Кроме того, они предоставляют все больше возможностей для маркетинговых исследований



В поездке человека может сопровождать множество меток, включая карту оплаты проезда и брелок для ключей, считываемые с большого расстояния, электронный паспорт, «усовершенствованное» водительское удостоверение и багажные метки аэропортов

Сотрудникам организаций обычно выдают карточки-ключи и удостоверения личности. В больницах метки позволяют регулировать и контролировать доступ к медикаментам и отслеживать истории болезней пациентов

В школах и публичных библиотеках метки инсталлируются в ученические, студенческие и читательские билеты и книги. В Федеральном округе Колумбия новая единая карточка служит ученическим, читательским билетом и проездным документом

Товары в розничных магазинах оснащаются метками для мониторинга, а некоторые магазины выдают покупателям *RFID*-ридеры, позволяющие им получать информацию или скидки. Магазины должны блокировать метки на купленных товарах, но не всегда делают это

и миллионы электронных пропусков. Проездные билеты с *RFID*-метками широко используются в Европе и Японии, в меньшей степени в США. Комплекс *PTU* компании *IBM* пока еще только запатентован, но английский парк чудес *Alton Towers* предоставляет наглядную иллюстрацию возможностей *RFID*-меток в отношении слежения. На входе в парк всем посетителям предлагают браслет с меткой, имеющей уникальный номер. Когда посетители пользуются аттракционами, размещенные в парке ридеры фиксируют эти метки и включают видеокамеры. Перемещения каждого посетителя сохраняются в файле, именем которого служит номер *RFID*-метки на браслете, и на выходе посетитель может получить сувенирный *DVD* фильм о пребывании на аттракционах.

Как защитить общество

Если *RFID*-метки позволяют в парке чудес снимать на видео тысячи людей, представьте себе, что сможет сделать не стесняющее себя ограничениями правительство, не говоря уже об администрации супермаркетов или преступниках. Именно поэтому мы столь решительно выступаем против использования *RFID*-меток

KARL SIMONS; MAKEUP: SCOTT BARNES (Albrecht)

в удостоверениях личности и на индивидуальных потребительских товарах. Еще в 2003 г. организация *CASPIAN* (*Consumers Against Supermarket Privacy Invasion and Numbering* — Потребители против вмешательства супермаркетов в личную сферу и нумерования) вместе с Информационной службой по праву на неприкосновенность личной сферы, Информационным центром по защите электронной личной сферы, Фондом электронной границы, Американским союзом гражданских свобод и 40 другими ведущими организациями по защите личной приватности и гражданских свобод опубликовали статью с выражением своего осуждения слежения за людьми с использованием *RFID*-меток.

Десятки штатов США внесли законопроекты в защиту потребителей, но все они были отвергнуты сильнейшей оппозицией со стороны лобби *RFID*-отрасли. Когда в 2006 г. сенат штата Нью-Гемпшир обсуждал законопроект, который предусматривал строгую регламентацию *RFID*, внесенная в последнюю минуту поправка заменила его двухлетним обсуждением. В том же году обе палаты законодательного собрания Калифорнии одобрили законопроект, запрещающий использование *RFID*-меток в государственных документах, но губернатор Арнольд Шварценеггер наложил на это решение вето.

Ни один законопроект по защите потребителей от рисков использования *RFID*-меток не прошел и на федеральном уровне. Более того, в 2005 г. организация «Специальные силы республиканцев в сенате в защиту высоких технологий» назвала *RFID*-приложения новыми перспективными технологиями для экономики и поклялась защищать *RFID* от законодательных ограничений.

В Европейском Союзе законодатели хотя бы изучают ситуацию. Европейская Комиссия (исполнительный орган Европейского Союза) признала серьезную угрозу приватности со стороны *RFID* и в начале 2008 г. открыла общественные обсуждения. К июлю, когда полемика вышла на страницы прессы, было решено, что к концу лета должны быть опубликованы рекомендации, выработанные на основе данного обсуждения, однако надежды на принятие каких-либо законов в отношении защиты личной сферы потребителей мало. В марте 2007 г. представитель Комиссии Европейского Союза по информационному сообществу и СМИ Вивиан Рединг (Vivian Reding) заявила, что комиссия не будет регламентировать *RFID*, но позволит бизнесу самому регулировать эту сферу.

К сожалению, там, где дело касается защиты общества от рисков, связанных с использованием *RFID*-технологий, на самоограничение бизнеса надежды мало. Отраслевая организация *EPCglobal*, вырабатывающая сегодня технические стандарты на *RFID*-метки, также подготовила ряд рекомендаций относительно их использования в розничной торговле. Требуется, в частности, уведомлять покупателей о том, что продукт имеет подобную метку, с помощью специального логотипа, однако когда компания *Checkpoint Systems*, член *EPCglobal*, разработала идентификаторы для обуви в явном противоречии с указаниями этой организации, президент *EPCglobal* Майк Меранда (Mike Meranda) признался, что в этой ситуации он бессилен.

Управление лицензирования штата Вашингтон уверяет граждан, что их личной информации ничто не угрожает. Некоторых людей такие официальные заявления могут обнадежить. Группа «Национальная сеть против домашнего насилия», открыто протестующая против использования *RFID*-меток в документах, удостоверяющих личность, и потребительских товарах, представила отчет о том, как злоумышленники могут использовать эту технологию для слежения за своими жертвами.

Однако поезд *RFID* не останавливается. Представитель Управления лицензирования штата Вашингтон Джиджи Зенк (Gigi Zenk) подтвердила недавно, что водительские удостоверения с *RFID*-метками имеют при себе больше 10 тыс. американцев, что уже само по себе обладает огромным потенциалом для злоупотреблений. Недавно в США был принят закон, определяющий несанкционированное считывание информации с *RFID*-метки «с целью мошенничества, получения информации о личности или иной незаконной целью» как тяжкое преступление класса *C*, караемое тюремным заключением на пять лет и штрафом в $10 тыс., однако в законе не сказано, что сканирование данных для других целей, например маркетинговых или «контроля населения», также является правонарушением. ■

Перевод: : И.Е. Сацевич

ОБ АВТОРЕ

Катрин Олбрехт (Katherine Albrecht) получила докторскую степень в Гарвардском университете и является директором 15-тысячной организации потребителей *CASPIAN* по защите личной сферы, борющейся против слежения в розничной торговле за потребителями. С 2003 г. она занимается выявлением и предотвращением неэтичного использования *RFID*-меток. Она регулярно выступает перед законодателями и издает обращения по ключевым вопросам к семинару по *RFID* и защите личной сферы, работающему при Массачусетсском технологическом институте.

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

■ Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID. Katherine Albrecht and Liz McIntyre. Thomas Nelson, 2005.

■ Radio-frequency Identification (RFID): Addressing Concerns over Information Collection and Usage. Видео и обсуждение за круглым столом в Школе юриспруденции Университета штата Вашингтон 19 июля 2007 г. Доступно на www.law.washington.edu/lct/Events/rfid

СЕЗАМ, ОТКРОЙСЯ! Для повышения эффективности в системах безопасности предполагается одновременно использовать несколько биометрических характеристик человека

Анил Джайн
и Шарат Панканти

Системы безопасности, основанные на анатомических и психологических особенностях человека, могут оказаться более эффективными, чем привычные пароли и идентификационные документы

ПЕРСПЕКТИВЫ биометрии

В последнее время людям все чаще требуется подтверждать свою личность при помощи паролей, идентификационных карт или других документов. Все эти средства гарантируют безопасность и обеспечивают защиту личной информации, денег и т.д. Однако стоит потерять пластиковую карту или забыть пароль, и вы не сможете с прежней легкостью снимать деньги с личного счета или лиши-

тесь доступа к своему компьютеру. Если же хотя бы один из таких документов попадет в чужие руки, то средство идентификации вашей личности может превратиться в оружие, направленное против вас.

Биометрия — автоматизированное распознавание личности человека с помощью характерных анатомических и поведенческих особенностей — основа для решения подобных проблем. Растущая популярность биометрических систем связана с тем, что по сравнению с конкретным физическим объектом (пластиковой картой или документом, удостоверяющим вашу личность) биометрические характеристики гораздо труднее подделать или скопировать, а украсть просто невозможно. Портативные компьютеры и мобильные телефоны, способные распознавать отпечатки пальцев, уже появились в продаже. В некоторых странах биометрические системы применяются для защиты кредитных карт или паспортов, контроля над посетителями государственных учреждений или при снятии денег с личного счета. Изобретение новых сенсоров и микропроцессоров отразилось и на биометрических технологиях, сделав их использование более привлекательным.

Измерения человека

Биометрия — наука не новая. В 1879 г. писарь полицейской префектуры Парижа Альфонс Бертильон (Alphonse Bertillon), производя различные измерения человеческого тела, создал новую науку — антропометрию. Его метод успешно применялся для установления личности повторно судимых преступников. В течение следующего десятилетия британские ученые показали, что отпечатки пальцев каждого человека уникальны и не меняются в течение всей жизни. Это послужило поводом для дальнейших исследований и создания в 1896 г. первой дактилоскопической классификации. Вскоре Скотланд-Ярд начал собирать отпечатки пальцев на месте преступления. Сегодня методы дактилоскопии используются в различных областях, начиная от идентификации людей, подозреваемых в различных преступлениях, и заканчивая проверкой кандидатов на ответственные должности. Требования различных охранных предприятий определяют основное направление развития биометрии сегодня — разработку полностью автоматических систем, удобных в управлении и дающих возможность быстро и точно проводить идентификацию.

За последние 30 лет ученые разработали системы, в основе которых лежит работа с изображениями лица, радужной оболочки глаза или записью голоса. При идентификации могут использоваться практически любые параметры человека, соответствующие двум основным требованиям: они должны быть уникальными для каждого человека и не должны меняться с течением времени. К сожалению, идентификационных систем, лишенных недостатков, не существует: если одни обладают высокой эффективностью в распознавании личности человека, то другие более удобны в применении или дешевле в эксплуатации. Три наиболее популярные системы основаны на сканировании отпечатков пальцев, лица и радужной оболочки.

В судебной практике многих стран определение личности человека проводится по отпечаткам пальцев. Только в Министерстве национальной безопасности США с момента запуска системы *US-VISIT* в 2004 г. с ее помощью были обработаны дактилоскопические данные более 75 млн посетителей. С коммерческой точки зрения, основное преимущество идентификации по отпечаткам пальцев заключается в том, что стоимость соответствующих сенсоров за последнее время снизилась до $5. Кроме того, используя новейшие технологии, ученым удалось значительно уменьшить размер соответствующих приборов, что в свою очередь позволяет внедрить их в портативные компьютеры, мобильные телефоны и даже во флеш-карты. Однако такие сенсоры дают большую погрешность, поскольку, в отличие от более дорогостоящих аппаратов, использующихся в правоохранительных органах, они сканируют лишь небольшой участок пальца и обеспечивают низкое разрешение получаемой картинки.

Идентификационные системы, основанные на сканировании лица, в последнее время также становятся все более популярными, поскольку их можно использовать в устройствах, оснащенных встроенными камерами, таких как мобильные телефоны, компьютеры, и т.д. Такие системы обеспечивают приемлемую точность лишь в том случае, когда регистрация изображения происходит в определенных условиях: при хорошем освещении, с естественным выражением лица и т.д. Все подобные системы очень чувствительны, и ошибки могут происходить даже в том случае, когда исходное и полученное в процессе идентификации изображения отличаются друг от друга незначительным изменением позиции, возрастом или такими особенностями, как очки или борода. Возможно, в ближайшее десятилетие совершенствование технологий позволит полностью автоматизировать процесс идентификации личности человека по его лицу, снизив ошибки до приемлемого уровня.

Радужная оболочка человеческого глаза обладает очень сложной структурой, что позволяет использовать ее как индивидуальную характеристику личности человека в соответствующих биометрических сис-

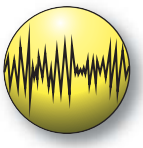
ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Биометрические идентификационные системы во многом удобнее привычных методов, кроме того, их сложнее обмануть.
- Развитие технологий и изобретение мощных экономичных микропроцессоров открывают новые возможности для биометрии
- Прежде чем новейшие биометрические системы окончательно войдут в обиход, исследователям необходимо максимально увеличить их точность.

КАКАЯ ИЗ ПРОЦЕДУР ОПОЗНАНИЯ НАИБОЛЕЕ ЭФФЕКТИВНА?

Выбор одной или нескольких биометрических характеристик для соответствующей охранной системы зависит от специфики системы. Сильные и слабые стороны каждой из четырех основных характеристик отражены в таблице. Например, по сравнению с опознанием человека по отпечаткам пальцев идентификация по радужной оболочке более надежна, хотя и требует более громоздкой и дорогостоящей аппаратуры, которую невозможно встроить в портативный компьютер или мобильный телефон. Эксперты сходятся на том, что уровень ошибок (как при положительном, так и при отрицательном результате идентификации) не должен превышать 0,1%. Однако в ходе тестирования, проведенного Национальным институтом стандартов и технологий, ни одна из представленных систем не продемонстрировала соответствия этому требованию

Биометрические характеристики

Свойства	 Отпечатки пальцев	 Лицо	 Радужная оболочка глаза	 Голос
Различающая способность	Высокая	Низкая	Высокая	Низкая
Долговечность	Высокая	Средняя	Высокая	Низкая
Качество сканирования	Среднее	Высокое	Среднее	Среднее
Скорость, эффективность и стоимость соответствующей аппаратуры	Высокая	Низкая	Высокая	Низкая
Готовность человека пройти идентификацию	Средняя	Высокая	Средняя	Высокая
Сложность соответствующей аппаратуры	Высокая	Низкая	Высокая	Низкая
Процент ошибок при положительном результате идентификации	0,4	1,0–2,5	1,1–1,4	5–10
Процент ошибок при отрицательном результате идентификации	0,1	0,1	0,1	2–5

темах. Однако такие системы требуют высокой точности и скорости измерений: необходимо получить со сканера качественное изображение радужной оболочки глаза исследуемого объекта, а затем обработать его, за считанные секунды сравнив с образцами, хранящимися в базе данных. В последние несколько лет разрешение получаемых при таком подходе изображений и скорость процесса существенно возросли, что позволило повысить эффективность распознавания личности человека. Примером тому может служить разработка британской идентификационной системы сканирования радужной оболочки глаза *IRIS*. Многие британцы по достоинству оценили ее преимущества, позволяющие людям, информация о которых была включена в базу данных *IRIS*, упростить обычную процедуру проверки в аэропортах. Несмотря на все

ОБ АВТОРАХ

Анил Джайн (Anil K. Jain) — профессор факультетов компьютерных наук и машиностроения, электронного и компьютерного машиностроения, вероятности и статистики в Мичиганском государственном университете, автор нескольких книг по биометрии. **Шарат Панканти** (Sharat Pankanti) — глава исследовательской группы в Исследовательском центре Томаса Уотсона в Йорктауне, занимается разработкой универсальных идентификационных систем. Этим двум ученым принадлежит множество патентов на идентификационные устройства, использующие отпечатки пальцев человека.

LUCY READING-IKKANDA

достоинства, у данного метода есть и свои минусы: он зависит от алгоритмов цифрового кодирования, а чрезмерная сложность полученных при сканировании изображений затрудняет процесс сравнения с оригиналом.

Неполные совпадения

В отличие от систем безопасности, основанных на использовании электронных паролей, пластиковых карт и других уже привычных для нас изобретений, в биометрических системах защиты существуют так называемые «неполные совпадения». По сути, любая система, функционирующая по принципу сравнения, допускает два типа ошибок: утверждение о совпадении сканируемого объекта с контрольным образцом в том случае, когда реально объект и образец различаются, и наоборот. Эксперты сходятся на том, что доля обоих типов ошибок не должна превышать 0,1% (т.е. не более одной ошибки на 1000 экспериментов с совпадением результатов и не более одной на 1000 опытов с несовпадением). Вычисления, проведенные Национальным институтом стандартов и технологий в период с 2003 по 2006 г., показали, что для систем, основанных на отпечатках пальцев, сканировании лица, радужной оболочки глаза или анализе голоса уровень ошибок превосходит указанный процент (*врезка*).

Увеличение числа совпадений может снизить количество ошибок только одного типа. Если пытаться повысить общий уровень надежности системы, то придется разрабатывать биометрическую систему, оперирующую снимками очень высокого разрешения и обладающую способностью к их обработке. Несмотря на то что биометрические характеристики очень сложно подделать, разработчики также должны быть уверены, что системы надежно защищены от взлома. Злонамеренные действия такого рода — обычное дело для всех идентификационных систем, включая и те, которые оперируют с паролями и физическими носителями информации. Такие атаки могут быть отражены при помощи повышения надежности защитных систем, например средствами криптографии.

Гораздо более многообещающе выглядит разработка биометрических систем безопасности, поддерживающих только допустимое представление об особенностях человека и исключающих попытки обмана при помощи хирургических средств или, например, пластиковой имитации человеческого пальца. В связи с этим биометрические датчики, регистрирующие тепло человеческого тела и другие признаки жизнедеятельности, могут помочь отличить сканируемые характеристики живого человека от искусственных подделок.

Тем не менее наиболее эффективный путь, увеличивающий точность, достоверность и защиту биометрии, — измерение нескольких параметров объекта одновременно. Подвергая объект исследования комбинации таких измерений, можно с большей уверенностью утверждать, что биометрическая информация принадлежит именно конкретному человеку, исключая возможность фальсификации. На данный момент многие паспортные системы уже функционируют подобным образом. Изначально в процессе идентификации с применением программы *US-VISIT* использовались отпечатки всего двух пальцев. В настоящее время она позволяет оперировать отпечатками уже всех десяти пальцев, а в перспективе дополнительно осуществлять сканирование лица.

Загадка личности

Использование биометрии порождает важную проблему хранения личной информации. Кто имеет право доступа ко всем хранящимся данным — отдельные лица или целые компании? Где гарантия того, что такая важная информация будет использоваться только во благо (для заключения о человеческом здоровье, например)? Отвечая на такие вопросы, стоит учесть, что биометрические системы в ближайшем будущем станут неотъемлемой частью нашей жизни, осуществляя свои измерения все более незаметно и не требуя практически никакого участия со стороны человека. Подобное развитие технологий серьезно изменит наши понятия о тайне личности.

Страны – участницы Евросоюза должны начать выдавать паспорта, включающие биометрические показатели, уже в 2009 г.

В настоящее время не существует эффективного решения данной проблемы. Тем не менее остается надежда, что это лишь одно из преодолимых препятствий на пути развития биометрии — перспективного направления, которое уже сейчас позволяет повышать уровень безопасности и обеспечивать оптимальную защиту информации. ■

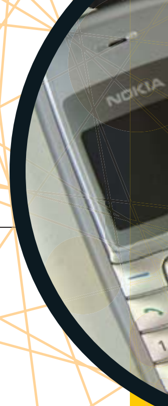
Перевод: Д.С. Хованский

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

- Biometric Recognition: Security and Privacy Concerns. Salil Prabhakar, Sharath Pankanti and Anil K. Jain in IEEE Security & Privacy, Vol. 1, No. 2, pages 33-42; March/April 2003.
- Biometric Systems: Technology, Design and Performance Evaluation. Edited by James Wayman, Anil Jain, Davide Maltoni and Dario Maio. Springer, 2005.
- Handbook of Multibiometrics. Arun A. Ross, Karthik Nandakumar and Anil K. Jain. Springer, 2006.
- Probing the Uniqueness and Randomness of IrisCodes: Results from 200 Billion Iris Pair Comparisons. John Daugman in Proceedings of the IEEE, Vol. 94, No. 11, pages 1927-1935; November 2006.
- Handbook of Biometrics. Edited by Anil K. Jain, Patrick Flynn and Arun A. Ross. Springer, 2008.

Симсон Гарфинкель

ДАННЫЕ ВСЕХ СТРАН, соединяйтесь!



Сведение всех личных данных каждого человека, от счетов, оплаченных кредитной картой, до записи телефонных разговоров, в единое цифровое досье — кошмар в духе Оруэлла, преследующий современного человека. Но сделать это не так просто, как представляют себе многие

Несколько лет назад я ездил в Англию. По дороге в аэропорт в кофейне выпил кофе и, поставив машину на стоянку, улетел. Через восемь часов я, выйдя из самолета в аэропорту Хитроу, купил карту оплаты для своего сотового телефона и отправился приобретать билет на поезд в Лондон. Однако моя кредитная карточка отказалась работать. И только вернувшись в США, я понял, в чем дело. Очевидно, небольшая покупка в кафе и последующее приобретение телефонной карточки по другую сторону океана запустили какой-то алгоритм защиты от мошенничества в компьютере компании, чью кредитную карточку я имел. Сотрудники компании пытались связаться со мной, но, получив сообщение автоответчика, внесли мою кредитку в черный список.

Во всем этом меня раздосадовало то, что компьютер должен был знать, что человеком, который пользовался моей карточкой в Англии, был я сам. В итоге мне удалось приобрести билет на обратный рейс с помощью той же карточки и улететь домой на самолете американской авиакомпании. Может быть, все эти базы следовало бы связать между собой?

Вероятно, большинство людей полагает, что так оно и есть. Из голливудских фильмов, таких как «Враг государства» и трилогия о Джейсоне Борне, мы вынесли уверенность, что тайные организации имеют мгновенный доступ ко всем базам данных, от которых мы зависим, и с помощью нескольких клавиш могут шпионить за каждым нашим шагом. Предполагается, что процесс сбора информации из различных источников создает информационный ресурс гораздо более мощный, гибкий и точный, чем любой из оригинальных источников. Поборники интеграции баз данных утверждают, что их системы позволяют организациям более эффективно использовать уже имеющиеся у них данные, а противники говорят, что данный процесс угрожает гражданским свободам, т.к. позволяет использовать информацию способом, не предусматривавшимся, когда эти данные собирались. И те, и другие считают, что системы слияния данных действительно работают. Истина же в том, что они отнюдь не так всеведущи, надежны и хорошо разработаны, как полагает большинство людей.

Как искать террористов

История технологии объединения баз данных начинается с компьютерных программ поиска совпадений 1970-х гг. Когда конгресс США принял Закон о защите частных интересов от 1974 г., он распорядился также создать Федеральную службу розыска родителей, ведущую сегодня досье на лиц, уклоняющихся от исполнения своих обязанностей, которым отказано во многих федеральных привилегиях, в час-

ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Идея объединения баз данных, известного под названием слияния данных, — кошмарный сон защитников приватности. Однако до сих пор дело, похоже, ограничивалось особыми случаями вроде казино и обеспечения поддержки детей.
- Интеграция баз данных — очень трудная задача, поскольку в них много ошибок и бессмысленных совпадений. Новые алгоритмы позволяют преодолеть некоторые трудности, но изменяют ли они общее соотношение между затратами и выигрышем?

MELISSA THOMAS (photoillustration); PATRIK STOLLARZ Getty Images (cell phone); THINKSTOCK/CORBIS (checkout card in back);

ИНТЕГРАЦИЯ БАЗ ДАННЫХ позволит создать единый информационный центр

MELISSA THOMAS (photoillustration); PATRIK STOLLARZ Getty Images (cell phone); THINKSTOCK/CORBIS (checkout card in book); JIM CRAIGMYLE Corbis (wand in laptop); ELISE AMENDOLA AP Photo (driver's licenses); PURESTOCK (passport); DAVID MACK Photo Researchers, Inc. (DNA); PHILIP JAMES CORWIN Corbis (bank statement); SHEILA TERRY Photo Researchers, Inc. (computer hard disk)

тности, в получении паспорта. Эта база объединена с данными Национального справочника по трудоустройству с целью выявления недавно поступивших на работу родителей, задерживающих выплаты алиментов, чтобы на их зарплату можно было наложить арест.

Термин «объединение баз данных» вошел в технический язык в 1984 г., когда исследователи из Центра передовых технологий компании *Lockheed Martin* опубликовали две статьи о системе «тактической интеграции данных», которая должна в реальном времени объединять данные с поля боя от датчиков и других источников, чтобы представлять их аналитикам. С тех пор дело продвинулось еще дальше. Специалисты по биоинформатике говорят о создании интегральной базы данных о геномах. Министерство внутренней безопасности потратило больше $2,5 млн на создание 58 центров интеграции баз данных — местных или в масштабах отдельных штатов. Маркетинговая компания *Nielsen* разрабатывает программы обработки различных баз данных для выявления потенциальных потребителей.

Объединение информационных ресурсов вызывает больше всего споров в обществе в связи с использованием этого механизма для борьбы с преступностью. «Ключ к выявлению террористов — анализ характера их деятельности, которая может свидетельствовать о подготовке террористических планов. При этом используются сведения о прежних террористических атаках», — писали в 2006 г. контр-адмирал Джон Пойндекстер (John Poindexter) и Роберт Попп (Robert L. Popp) из Агентства передовых оборонных исследований (*DARPA*). Они утверждали, что взрывы бомб в Центре мировой торговли в 1993 г. и в Оклахома-Сити в 1995 г. можно было бы предотвратить, если бы правительство имело возможность сканировать базы данных торговых организаций с целью выявления крупных покупок удобрений лицами, не имеющими отношения к сельскому хозяйству. Однако получение сведений о таких приобретениях и объединение их с базой данных о владельцах и работниках ферм потребовало бы свободного доступа правительства к частным компьютерным системам. Это позволило бы правительству контролировать каждую транзакцию — а, следовательно, и каждую личность, — не имея на то серьезных оснований. Именно эта причина стала основанием, по которому конгресс США в 2003 г. закрыл исследовательскую программу Пойндекстера и Поппа «Полная осведомленность об информации» (*Total Information Awareness*).

Насколько полезны совпадения

Однако имеется достаточно сведений, говорящих о том, что интеграция баз данных сталкивается не только с этическими и юридическими, но и с техническими проблемами.

Одна из них — качество данных. Большая часть информации, содержащейся в базах данных, собиралась первоначально в статистических целях и может быть недостаточно точной. В 1994 г. Роджер Кларк (Roger Clarke) из Австралийского национального университета в Канберре изучал компьютерные программы поиска совпадений, используемые федеральным правительством и правительствами штатов в США и Австралии. Эти систе-

ИГРЫ, В КОТОРЫЕ ИГРАЮТ ЛЮДИ

Казино Лас-Вегаса первыми занялись интеграцией баз данных из разных источников, поскольку столкнулись с многочисленными фактами мошенничества. Вот несколько примеров, основанных на подлинных случаях

мы сканировали миллионы записей и отмечали тысячи потенциальных «попаданий». Но большинство совпадений оказывались случайными. Например, одна из программ поиска случаев мошенничества в сфере социального обеспечения сопоставляла данные о работниках Министерства здравоохранения и социального обеспечения с досье социального обеспечения. Было выявлено около 1000 совпадений, но дальнейшие исследования показали, что три четверти выявленных людей ни в чем не замешаны. Результаты такого поиска не оправдывают затрат на сбор данных, обучение персонала и выявление случайных совпадений.

Многие люди думают, что программы интеграции баз данных позволят предвидеть и предотвратить крупные теракты, и на такие проекты можно потратить любые средства. Пойндекстер, успешный морской офицер, сравнил технические проблемы с поиском вражеской подводной лодки на обширных водных просторах. На самом деле обнаружить признаки подготовки теракта в океане данных гораздо сложнее. Мировой океан огромен, но любая точка в нем однозначно определяется широтой, долготой и глубиной. Океаны данных характеризовать не так легко. Кроме того, размеры земных морей, в отличие от океанов данных, не удваиваются каждые несколько лет. Данные разбросаны по миллионам локальных компьютерных систем, и многие из них скрыты от властей или не известны им. Истинная трудность не в получении данных, а в их осмыслении.

Что есть на вашем жестком диске?

Чтобы понять проблемы интеграции баз данных, хорошо начать с информации, хранящейся на жестком диске вашего компьютера. С 1998 по 2005 гг. я занимался именно этим: на сетевом аукционе *eBay*, в маленьких компьютерных магазинах и по обмену мной были приобретены более 1000 бывших в употреблении жестких дисков. Я даже извлекал диски из компьютеров, брошенных на улицах. В январе 2003 г. мы с Аби Шелатом (Abhi Shelat), специ-

KENN BROWN Mondolithic Studios

ОБ АВТОРЕ

Симсон Гарфинкель (Simson L. Garfinkel) занимается наукой, журналистикой и бизнесом. Он — специалист по информатике в Школе повышения квалификации офицеров ВМС США в Монтерее (штат Калифорния), где в число его научных интересов входят криминалистика, защита информации, приватность и тактика террористов. Написанный им учебник по защите компьютеров «Безопасность сетей и бизнес» (*Web Security & Commerce*) разошелся тиражом более 250 тыс. экземпляров и был переведен более чем на десяток языков. Гарфинкель основал фирму, занимающуюся защитой компьютеров, и владеет несколькими патентами в этой области. В свободное время он проводит эксперимент по воспитанию сыновей-двойняшек. Взгляды, изложенные в настоящей статье, — его личное мнение, а не позиция правительства США.

алистом по информатике в Виргинском университете, опубликовали статью с подробным описанием наших результатов.

Около трети дисков оказались негодными, еще треть была тщательно очищена прежними владельцами, но оставшаяся часть оказалась кладезем личной информации: электронные сообщения, памятные заметки, финансовые записи. Один из дисков использовался в банкомате, и на нем были записаны тысячи номеров кредитных карточек, другой в супермаркете для предъявления банку счетов по платежам. Оба не были очищены перед выставлением на продажу на аукционе.

Средства, позволившие изучать эти диски, широко доступны и не особенно сложны. Подобные же средства применяют для извлечения файлов из компьютерных дисков и сотовых телефонов полицейские управления всего мира. Пользователи часто не имеют представления о том, какие обрывки информации они оставляют. Рассмотрим случай Денниса Рейдера, серийного убийцы *BTK* (прозвище, которое он себе придумал сам, от *bind — torture — kill*, «связать — мучить — убить»), совершившего в 1970-х — 1980-х гг. восемь убийств в Уичите (штат Канзас), а затем залегшего на дно. В марте 2004 г. он объявился, послав в газету *Wichita Eagle* письмо с подробным описанием своих преступлений, а на местную телевизионную станцию — дискету с файлом в формате *Microsoft Word*. Этот файл содержал «метаданные», которые связывали его с компьютером местной церкви. Полиция установила, что человеком, который пользовался компьютером, был президент совета церковной общины — он же был и убийцей.

Как сделать винегрет из файлов

Однако определить, какой документ важен, а какой бесполезен, трудно, и для этого нужно комбинировать информацию с диска с другой, полученной из внешних источников. Так, когда я в 1990-х гг. начал анализировать жесткие диски, на многих из них оказались копии *Island Hopper News*, что выглядело очень подозрительно. Позже мне удалось узнать, что на деле эта электронная газета была демонстрационным файлом, который компания *Microsoft* распространяла со своим программным пакетом *Visual Studio 6.0*. Не получив эту информацию, я мог бы сделать неправильные выводы о прежних владельцах дисков.

Единственный путь отсеивания безобидных файлов состоит в том, чтобы сделать выборку из мира цифровых документов и сформировать перечень тех из них, которые широко доступны. Быстрый способ сделать это — создание так называемого хеш-набора. Криптографические алгоритмы хеширования могут присваивать любому цифровому файлу уникальный «электронный отпечаток пальца». Из этих алгоритмов наиболее популярны два: *MD5*, генерирующий отпечатки пальца длиной в 128 битов, и *SHA-1*, создающий 160-битные отпечатки. Они могут вместо побайтового сравнения файлов изучать их отпечатки пальцев.

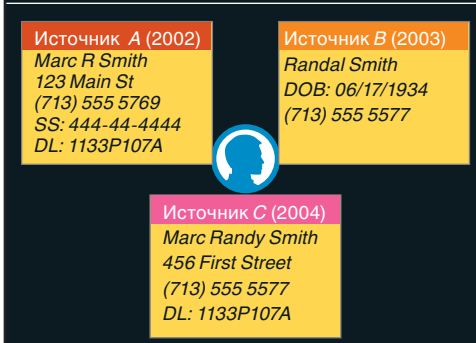
На средства гранта от Министерства юстиции Национальная библиотека справочной информации по программному обеспечению Национального института стандартов и технологий (*NIST*) приобретает программы от сотен издателей и превращает каждый файл в криптографический хеш. После этого *NIST* распространяет базу данных, которая содержит сегодня больше 46 млн позиций, что дает правоохранительным органам быстрый и надежный способ выделить файлы, распространяемые разработчиками ПО (аналогичных файлу *Island Hopper News*), которыми, следовательно, вполне можно пренебречь. Базы данных других федеральных учреждений содержат электронные отпечатки пальцев хакерских инструментов и детской порнографии.

Однако хешированные базы данных, несмотря на их полезность, представляют собой лишь небольшие выборки существующих документов. Чтобы дополнить их, я разработал программу перекрест-

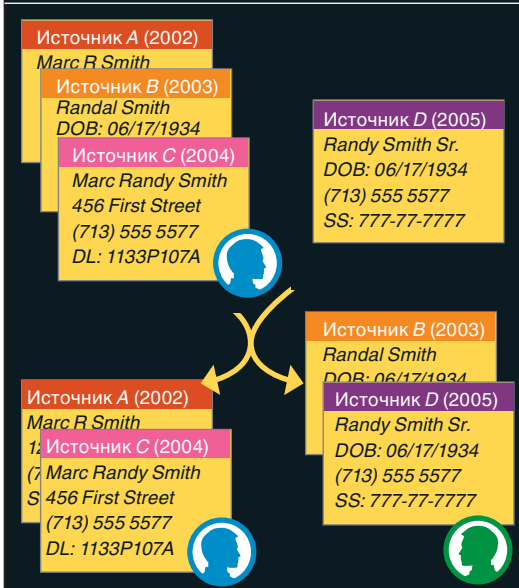
КАК ЭТО РАБОТАЕТ

Работу с неполной и противоречивой информацией иллюстрирует алгоритм, созданный первоначально для казино

Запись *A* с номером водительского удостоверения (*DL*) и запись *B* с датой рождения (*DOB*) содержат разную информацию, поэтому система первоначально предположила, что эти записи относятся к разным людям

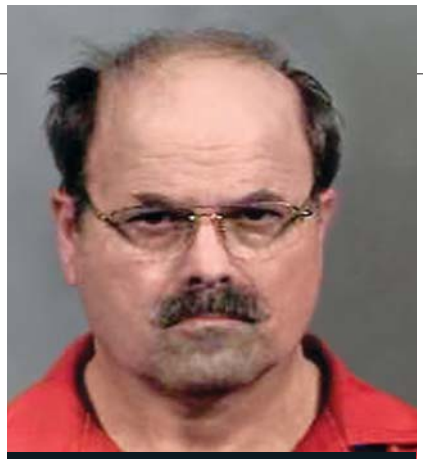


Третья запись (*C*) содержит информацию, общую с записями *A* и *B*: номер водительского удостоверения из *A* и номер телефона из *B*, поэтому система отнесла все три записи к одному человеку



Однако четвертая запись (*D*) содержит дату рождения, совпадающую с датой в записи *B*, но с номером карточки социального страхования (*SS*), отличным от номера в записи *A*, из чего следует, что четыре рассмотренные записи представляют двух человек с общей фамилией и одинаковым номером телефона. Система сделала вывод, что это могут быть отец и сын

COURTESY OF SIMSON L. GARFINKEL (author); MELISSA THOMAS (illustration)



Деннис Рейдер, он же убийца *BTK*, выдал себя метаданными, скрытыми в электронном документе, который он послал на телевизионную станцию

Эвакуированные вследствие урагана «Катрина» находили своих родственников с помощью простой системы сравнения данных

ного анализа дисков. Эта технология позволяет систематизировать информацию, разбросанную на тысячах жестких дисков, флеш-устройствах и других носителях. Программа выделяет такие идентификаторы, как электронные адреса, номера кредитных карточек, и определяет степень важности в соответствии с тем, как часто они встречаются: предполагается, что чем более распространен некий идентификатор, тем менее он важен. После этого программа ищет корреляции между идентификаторами на всех отдельных дисках: если электронный адрес или номер кредитной карточки обнаруживаются всего на двух дисках из тысяч, то существует большая вероятность, что эти два диска связаны между собой.

Кто есть кто?

Еще одна проблема интеграции данных — идентификация личности. В электронном мире могут быть десятки людей с одинаковыми именами, а один и тот же человек может использовать десятки имен. В одних базах данных контр-адмирал Пойндекстер может фигурировать как Джон Марлан Пойндекстер, в других — как Дж. М. Пойндекстер, а в некоторых его фамилия может быть вообще написана неправильно. Личное имя человека в одной базе данных может быть записано как Роберт, в другой — как Роб, а в третьей — как Боб. Человек с арабским именем, которое в Западной Африке транслитерируется как *Haj Imhemed Otmane Abderaqib*, в Ираке может быть известен как *Hajj Mohamed Uthman Abd Al Ragib*.

Сопоставление разных имен и номеров счетов, существующих в электронном мире, с реальными лицами называется идентификацией личности. Любопытно, что многие новшества в системах установления личности были внедрены по инициативе администраций казино в Лас-Вегасе. По закону штата Невада в казино не должны допускаться к игре неадекватные личности. Эти игроки добровольно вносят себя в список, говоря этим: «Больше не допускайте меня к игре». Но игромания может быть болезнью, и некоторые из них потом все же пытаются вернуться к игре под другим именем или изменив несколько цифр в дате своего рождения. В казино стараются не допускать к игре людей, заподозренных в мошенничестве или осужденных за него, а если человек выигрывает крупную сумму в джекпот, то хотят быть уверенным, что крупье и игрок — не соседи по комнате.

В связи с этим разработана методика анализа неочевидных связей (*nonobvious relationship analysis, NORA*), сочетающая идентификацию личности с анализом баз данных кредитных компаний, записями актов гражданского состояния и регистрации постояльцев в отелях. Система *NORA* может определить, например, что жена крупье жила когда-то в одном доме с человеком, только что выигравшим $100 тыс. В 1990-х гг. программист Джефф Джонас (Jeff Jonas) разработал систему, позволяющую сопоставлять имена, хранящиеся в компьютерах казино, с другими источниками информации. Система генерирует гипотезы на основе данных и последующего пересмотра их в случае появления новой информации.

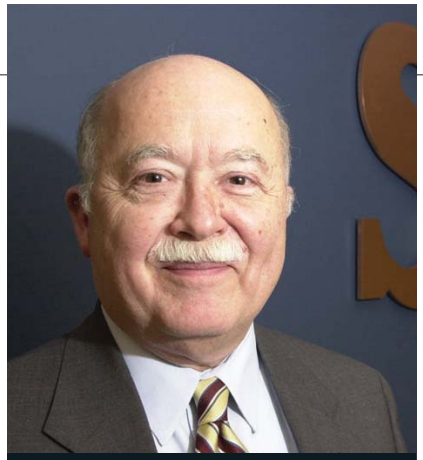
Например, программа может получать исходные данные водительского удостоверения на имя Марка Р. Смита, кредитную информацию о Рэндале Смите и заявку на кредит от Марка Рэнди Смита. На основании анализа можно предположить, что все эти имена принадлежат одному человеку, особенно если номер водительского удостоверения у Марка Р. Смита и Марка Рэнди Смита один и тот же, а Рэндал Смит и Марк Рэнди Смит имеют один и тот же номер телефона. Но предположим, что, согласно новым данным, даты рождения Рэнди Смита-старшего и Рэндала Смита совпадают, но номер его карточки социального страхования отличается от номера карточки Марка Р. Смита. Теперь система может пересмотреть свое прежнее предположение и заключить, что Марк Р. Смит — это Рэндал Смит-младший, а Рэнди Смит — это Рэндал Смит-старший.

Ключ к выполнению всей этой работы — программирование систе-

СЛИЯНИЕ И СМЕШЕНИЕ

Чтобы понять реальное состояние информационного потока, редактор журнала *Scientific American* заказал за $80 у сетевого консолидатора, собирающего персональные данные, включая записи об уголовных делах, недвижимости и банкротстве, свое досье. В нем оказалось масса ошибок: от неправильного написания его фамилии до путаницы с однофамильцами по всей стране, у многих из которых наложен арест на имущество. К счастью, ничего криминального не обнаружилось. Признаков хищения личных данных не зафиксировано. Так везет не всем

Автор изучает данные с выброшенных жестких дисков, чтобы понять, как может интеграция баз данных помочь полиции в уголовных расследованиях



Джон Пойндекстер, бывший советник президента США по национальной безопасности, пытался в 2002 г. создать правительственную базу данных для поиска террористов

мы таким образом, чтобы она никогда не смешивала исходные данные с выводами, сделанными на их основе.

В 2005 г. Джонас продал свою поисковую систему и компанию корпорации *IBM*. С тех пор *IBM* добавила к ней функцию анонимного разрешения, которая позволяет двум организациям определить, что в их базах данных есть имя некоего человека, не обмениваясь именами всех других сотрудников, не совпадающих с этим именем. Функция работает путем сопоставления криптографических хешей.

Защитники частной сферы продолжают настаивать, что хеши, перекрестный анализ, анонимное разрешение и другие подобные вещи не содержат почти ничего, что могло бы снять их принципиальные возражения. Наконец, все эти системы используют частные сведения для целей, отличных от тех, для которых эти сведения первоначально собирались. Кроме того, они превращают вылавливание таким «неводом» частных данных вне зависимости от того, подозреваются ли люди, чьи данные просматриваются, в преступных намерениях, в рутинную процедуру. Однако эти системы выдают намного меньше ложных совпадений, чем системы, созданные в 1980-х гг. В некоторых обстоятельствах общественная польза может перевесить ущерб личной сфере.

Как же собрать все это вместе?

Итак, насколько же хорошо работают системы интеграции баз данных на деле? Серьезной проблемой остается их качество. Например, получите свои кредитные отчеты от каждого из трех крупнейших кредитных агентств США, — и вполне вероятно, что в любом из них обнаружатся ошибки и противоречия. Эти данные могут «дремать» годами, не причиняя никому особого беспокойства. Опасность возникает, когда некий новый алгоритм начинает слишком глубоко копаться в этих противоречиях.

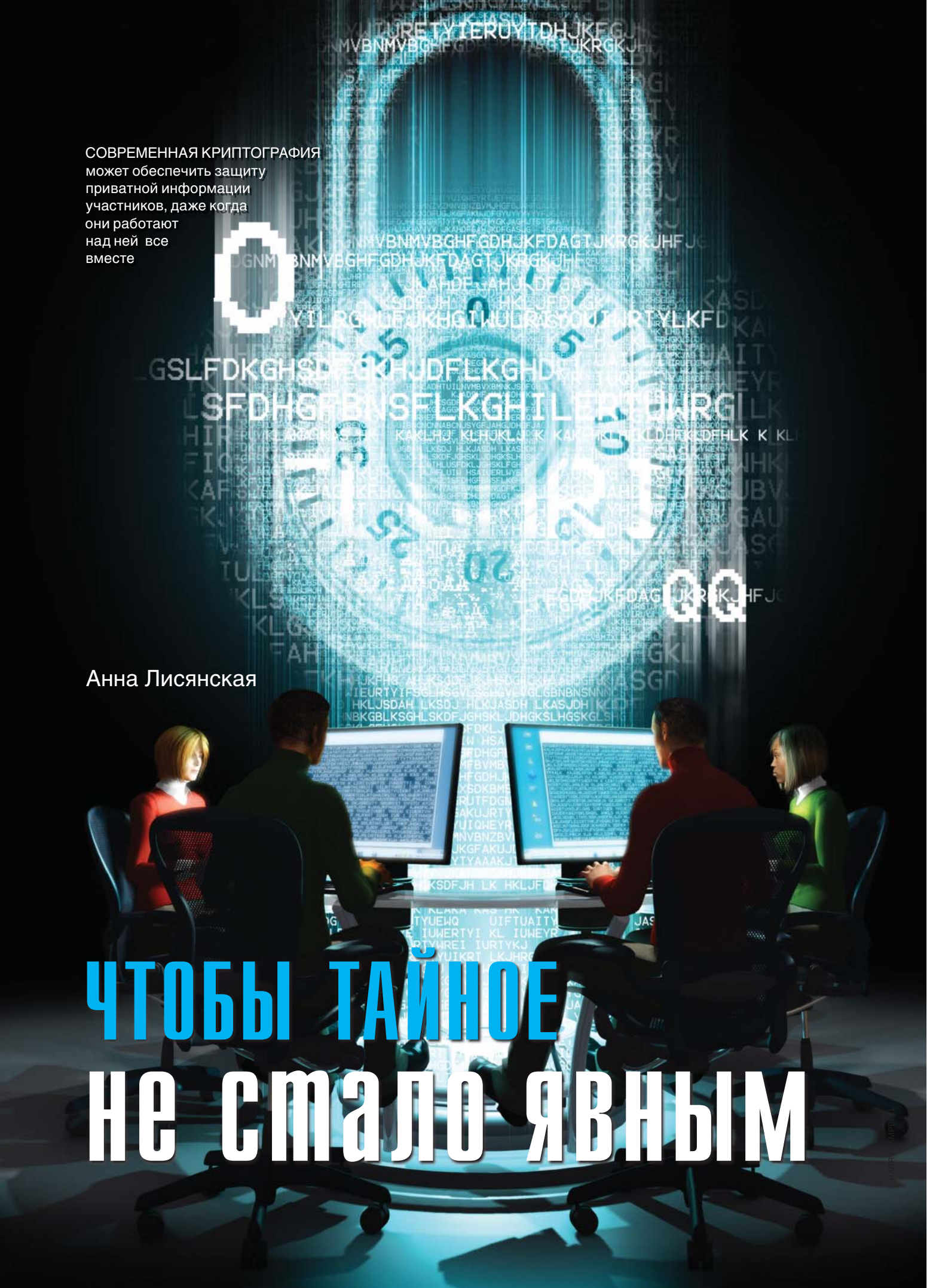
Даже если сведения точны, то соотношения, выявляемые в результате сравнения баз данных, могут быть как значимыми, так и чисто случайными, столь же неизбежными, как возможность нахождения в комнате двух лиц, родившихся в один и тот же день. Возможно, что четыре человека, которые встречаются каждую неделю для длительной совместной поездки, планируют преступление, но может быть, они входят в одну софтбольную команду и ездят вместе на игру, которая проводится раз в неделю.

Надежды общества на эффективность интегральных баз данных могут быть неоправданно завышенными. Если террористы смешались с населением, общество будет в равной мере ждать результатов и от аналитиков, и от компьютеров. Большинство систем поиска имеют те или иные средства регулировки чувствительности. Сместите индикатор влево, и система не сможет выявлять реальные совпадения. Сместите его вправо, и она будет выдавать слишком много ложных прогнозов. Где установить индикатор? Если система будет указывать на каждого третьего авиапассажира, она с большей вероятностью выявит истинного террориста, но при этом воздушное сообщение вообще остановится.

Если система не работает так, как хотелось бы, дело может быть как в принципиальной порочности ее алгоритмов, так и в недостатке данных. Если же система функционирует хорошо передача ей большего количества данных может только улучшить ее характеристики. Таким образом, проекты интеграции баз данных имеют естественную тенденцию к расширению задач, пугая не только защитников гражданских свобод, но и тех, кто платит по счетам. В своей статье 1994 г. Кларк писал, что «противоречия между стремлением государства контролировать общество и желанием отдельных граждан оградить себя от неоправданного вмешательства решаются, как правило, в пользу государства».

В спорах общественности по поводу интеграции баз данных меня как ученого очень разочаровывает тот факт, что обществу предоставляется крайне мало сведений о данном процессе. Это напоминает мне споры по поводу криптографии в 1990-х гг., когда правительство США утверждало, что есть серьезные причины для законодательного ограничения использования криптографии, но они настолько связаны с государственной тайной, что их публичное обсуждение будет угрозой для национальной безопасности. Я подозреваю, что подобные дебаты назревают и в отношении баз данных, не говоря уже о применении этой мощной технологии в бизнесе и в политической деятельности. А дебаты должны проходить в открытой форме. ■

Перевод: И.Е. Сацевич



СОВРЕМЕННАЯ КРИПТОГРАФИЯ может обеспечить защиту приватной информации участников, даже когда они работают над ней все вместе

Анна Лисянская

ЧТОБЫ ТАЙНОЕ НЕ СТАЛО ЯВНЫМ

Широкий спектр вычислительных методов может обеспечить необходимый уровень защиты частной информации даже при работе онлайн

Зак решил обратиться в сетевую службу знакомств *Chix-n-Studz.com*. Он создал на сайте учетную запись и заполнил несколько форм, детализирующих его личные данные и ожидания от потенциального партнера. Служба мгновенно предложила Заку список возможных претенденток, в котором его заинтриговало имя Венди. Он сообщил ей свой адрес электронной почты (*e-mail*) и отправил сообщение. Венди ответила, и у них завязался бурный виртуальный роман.

Бедный Зак! Вскоре на его телефон обрушился шквал звонков от активных политических групп и комми-вояжеров, которые, похоже, знают о нем все. А его страховая компания оказалась осведомлена о его экстремальных приключениях во время отпуска. Очевидно, недобросовестные владельцы *Chix-n-Studz* продали информацию о клиенте. Но это еще не все. Зак показал одно из электронных писем Венди своему сослуживцу Джону, не отягощенному моральными принципами. Зак не подозревает о том, что несколько последних сообщений от его дамы сердца, возможно, фальшивки, присланные Джоном.

Алиса, напротив, счастлива, как и ее новый друг Боб. Эти двое познакомились с помощью службы *SophistiCats.com*, которая использует все последние достижения криптографии. Веб-страница, на которую входит Алиса, защищена с помощью анонимной авторизации, гарантирующей, что никто из обслуживающего персонала не может проследить, кто она такая и когда обращается к сайту. *SophistiCats* использует программное обеспечение, которое гарантирует безопасное вычисление функции (*SFE*), обеспечившее совпадение ее характеристик и требований к партнеру с данными Боба таким образом, что никто в службе не имеет информации даже о том, что Алиса и Боб подошли друг другу. Вообразите себе эффективно работающую службу знакомств, которая фактически ничего не знает о своих клиентах!

Алиса связывается с Бобом с помощью так называемого анонимного канала, а он отвечает таким образом, что даже ее поставщик интернет-услуг (провайдер) не знает ни о том, что они общаются, ни о содержании сообщений. Провайдер Боба так же мало осведомлен. Однако соседка Алисы по комнате, Ева, *знает все*, но лишь потому, что Алиса рассказала ей о Бобе и прикрепила распечатку некоторых его сообщений над компьютером. Ева могла бы вмешаться, поскольку она любитель розыгрышей и способна подменить входящие и исходящие электронные сообщения Алисы (фактически, она контролирует сеть, через которую обе выходят в Интернет). Однако шифрование данных гарантирует, что Ева не сможет узнать ничего, кроме того, что Алиса ей показала, а цифровые подписи на электронных письмах Алисы и Боба обеспечивают выявление и игнорирование фальшивых сообщений Евы.

Все зашифровано

Подобно Алисе и Заку, множество людей пользуется электронными средствами коммуникации в повседневной жизни — от общения с друзьями и совершения покупок до составления правительственных документов. При этом получить всестороннюю информацию о большинстве из нас столь же просто, как отследить наши перемещения в течении дня. По различным причинам не только поставщики интернет-услуг регистрируют действия пользователей — например, когда и на каких сайтах они побывали. Многие объекты, с которыми мы взаимодействуем онлайн, — интернет-магазины, газеты, места свиданий на сайтах, и тому подобное — также сохраняют заметки о наших адресах. Таким образом, если для нас важна конфиденциальность, мы оказываемся перед задачей, как использовать в своих интересах все, что Интернет может предложить, сохранив приватность персональных данных.

Удивительное открытие современной криптографии — то, что фактически любая задача с использованием электронных средств связи может быть выполнена конфиденциально. Многие люди, включая редакторов большинства словарей, ошибаются, думая, что «криптография» — синоним кодирования. Современная криптография включает в себя намного больше. Она создает математические методы для защиты связи и вычислений от всех видов злонамеренных действий.

Предположим, например, что все члены группы, подключенные к Интернету, хотят вычислить что-то, зависящее от данных, поступающих от каждого из них — но при условии, что каждый хочет сохранить свою

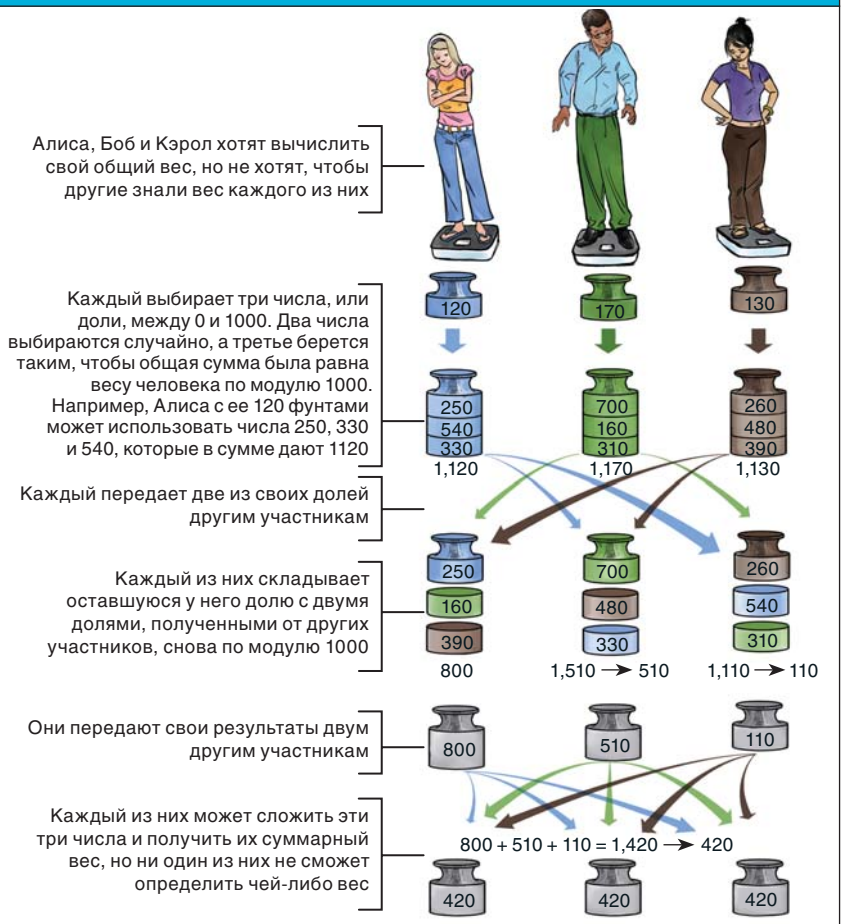
ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Современная криптография владеет разнообразными математическими средствами защиты приватности и секретности, которые выходят далеко за рамки возможностей древнего искусства шифрования сообщений.
- Вы можете помешать злоумышленникам узнать, что и кому вы сообщаете.
- Вы можете оставаться анонимным даже при работе онлайн, когда требуется ваша подпись и приходится сообщать факты непосредственно о себе.
- По коллективным данным своих членов группы могут вычислять что-либо (например, победителя на выборах, в которых они участвуют) без разглашения чьих-либо личных данных.

KENN BROWN Mondolithic Studios

ВЫЧИСЛЕНИЯ В ГРУППЕ

Вычисление функции в условиях секретности дает возможность группе людей вычислять что-либо, используя персональные данные членов группы, но не предавая гласности личные данные в процессе вычислений



Более сложная процедура дает возможность группам умножать числа их персональных данных. Добавляя и умножая биты, они могут вычислять что-нибудь из того, что можно определить по их данным с помощью компьютера. Полная система также защищена от людей, нарушающих правила

информацию в тайне. Данные, например, могут быть результатами голосования на выборах, а кто-то хочет знать общий результат голосования, не показывая свой индивидуальный выбор. Процедура, известная как безопасное вычисление в группе, или вычисление функции при соблюдении секретности (*SFE*), дает возможность объединить голоса таким образом, что каждый участник получает правильный результат, но никто не может получить чьи-то индивидуальные результаты — даже группа злонамеренных лиц, способных перехватывать сообщения в Сети и подменять их собственными тщательно построенными поддельными данными. Протокол *SFE* может также предоставлять каждому человеку личные данные, как это делает служба знакомств *SophistiCats*.

Идея, лежащая в основе *SFE*, состоит в том, что данные, вводимые каждым участником, разбиваются на части, или доли, и распределяются среди других членов группы. Далее каждый участник работает с долями, находящимися под его управлением (он может складывать их, перераспределять доли результатов и т.д.). Наконец, группа снова объединяет доли, чтобы получить окончательный результат. И никогда в чье-либо распоряжение не попадают данные, позволяющие восстановить входные данные другого члена группы (*простой пример — на врезке на слева*).

Возможно, не вызовет удивления то, что может быть безопасно вычислена такая простая функция, как сложение числа голосов. Более сложна выборка, предоставленная *SophistiCats* Алисе: поиск среди тысяч клиентов тех, кто наиболее полно соответствует ее требованиям, и сообщение ей некоторого объема ограниченной информации о выбранных кандидатах без изучения чьего бы то ни было досье. Отслеживание сетевого трафика «Большим Братом» или «прочесывание» данных на жестких дисках фирмы *SophistiCats* также не позволило бы что-либо выяснить.

SophistiCats в данном случае — вымышленная служба, но исследователи-криптографы показали, как можно воплотить подобный проект. Действительно, в январе 2008 г. алгоритм *SFE* был использован для решения реальной задачи (в Дании) — установки цены за контракты на поставку сахарной свеклы, которые будут проданы среди приблизительно 1200 датских фермеров на основе конфиденциально внесенных ими предложений. С помощью *SFE* мы можем сделать лучший выбор для обеих сторон: функциональные возможности, которые обеспечивает использование Интернета, и полное сохранение секретности.

Несмотря на то что протокол *SFE* предоставляет широкий диапазон возможностей, за них приходится платить: он требует большого объема вычислений и связи. Протокол достаточно эффективен для специальных задач, таких как выборы, и все же слишком обременительно подключаться к соответствующей службе каждый раз, когда вы связываетесь с защищенной веб-страницей. Вместо этого программисты разработали специализированные протоколы, которые для конкретных, часто встречающихся задач намного более эффективны, чем *SFE*. В их число входят следующие.

Шифрование. Ни провайдер Алисы, ни Ева не могут расшифровать сообщения, которые Алиса посылает Бобу. Обмен между компьютером Алисы и фирмой *SophistiCats* также надежно защищен.

Аутентификация. Алиса может быть уверена, что сообщения поступают от Боба, а не от Евы.

Анонимные каналы. Провайдер Алисы не знает, ни кому она посылала сообщения, ни о ее посещениях сайта *SophistiCats*.

Доказательство с нулевым разглашением (доказательство обладания какой-либо информацией без разглашения самой этой информации). Алиса может доказать кому-либо, что нечто истинно, не раскрывая своего доказательства.

Анонимная авторизация. Когда Алиса обращается к сайту *SophistiCats*, они узнают, что она их клиент, но они не могут сказать, кто она. Этот протокол — частный случай доказательства с нулевым разглашением.

Секретные сообщения

Самая старая и одна из самых фундаментальных проблем криптографии — шифрование, т.е. обеспечение безопасности связи по ненадежному каналу (по такому, который противник может подслушать). Алиса хочет послать сообщение Бобу, но часть канала, которым она пользуется, находится в распоряжении Евы (локальная сеть их квартиры). Алиса хочет, чтобы читать ее сообщения мог только Боб.

Первое, что обращает на себя внимание при анализе данной проблемы — Боб должен знать нечто, что не известно Еве, иначе она могла бы делать то же, что и он. Личное знание Боба называют его секретным ключом (СК). Во-вторых, Алиса тоже должна знать кое-что о СК Боба, чтобы она могла зашифровать текст сообщения, предназначенного для Боба. Если Алиса знает СК, протокол называют шифрованием с секретным ключом — это вид шифрования, который был известен и использовался в течение многих столетий.

В 1976 г. Уитфилд Диффи (Whitfield Diffie) и Мартин Хеллман (Martin E. Hellman), работавшие тогда в Стэнфордском университете, предложили другую возможность, названную шифрованием с открытым ключом, при котором Алисе не требуется знать СК. Все, что ей нужно, — это знание общеизвестной величины, родственной СК и называемой открытым ключом Боба (ОК). Алиса использует его ОК, чтобы зашифровать свое сообщение, и только Боб с его СК может расшифровать получившийся зашифрованный текст (*врезка внизу*). Причем не имеет значения, что Ева тоже знает ОК Боба, потому что она не может с его помощью расшифровать зашифрованный текст. Диффи и Хеллман выдвинули идею открытого ключа, но не знали, как ее реализовать. Решение появилось год спустя, когда Рональд Ривест (Ronald L. Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard M. Adleman), работавшие тогда в Массачусетсском технологическом институте, предложили первую криптосистему с открытым ключом — алгоритм *RSA*. За эту работу в 2002 г. они получили премию Тьюринга — аналог Нобелевской премии в области информатики.

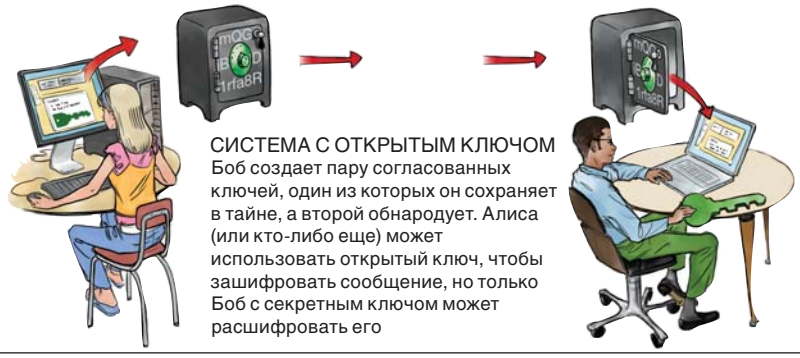
Их алгоритм используется для шифрования с открытым ключом, потому что в него включена так называемая «функция лазейки». Вычисления по алгоритму *RSA* при создании зашифрованного текста производятся легко, однако его трудно инвертировать, чтобы восстановить исходный текст, если не используется специальная функция — «лазейка». Данная функция и служит секретным ключом. Алгоритм *RSA* был первым ее примером.

Появление *RSA*, провозглашенное как фундаментальное достижение, обеспечило годы исследований в области шифрования и — более широко — кодирования. В области кодирования все еще остается много сложной работы от поисков новых функций лазейки до изучения математических предположений, которые лежат в основе защитных свойств определенной функции, и до точного определения требований

СОКРЫТИЕ СОДЕРЖАНИЯ

Современные методы шифрования информации относятся к одному из двух типов: с секретным ключом и с открытым ключом

СИСТЕМА С СЕКРЕТНЫМ КЛЮЧОМ
Алиса и Боб совместно используют ключ, который они сохраняют в тайне. С его помощью Алиса зашифровала свое сообщение. Она отправила его Бобу, который использует тот же самый ключ, чтобы расшифровать текст



СИСТЕМА С ОТКРЫТЫМ КЛЮЧОМ
Боб создает пару согласованных ключей, один из которых он сохраняет в тайне, а второй обнародует. Алиса (или кто-либо еще) может использовать открытый ключ, чтобы зашифровать сообщение, но только Боб с секретным ключом может расшифровать его

ПОДПИСЬ СООБЩЕНИЯ

Цифровая подпись гарантирует, что сообщение поступило от определенного человека и что оно не было изменено

к системе кодирования, чтобы ее можно было считать надежной.

Кодирование с открытым ключом позволяет совершать покупки онлайн, не посылая открыто через Интернет конфиденциальную информацию, такую как номер кредитной карты. Веб-браузер клиента выступает в роли Алисы, а веб-сайт — Боба. Более широко — в протоколе *HTTPS*, который поддерживает большинство браузеров, — используется шифрование с открытым ключом, чтобы обеспечить просмотр сети по зашифрованному каналу: ищите отметку «https://» в адресе сайта (*URL*) и значок изображение закрытого замка в строке состояния браузера.

Многие также используют кодирование с открытым ключом для обеспечения безопасной связи через электронную почту. Существует большое количество бесплатного программного обеспечения, позволяющего осуществлять безопасные соединения и шифровать данные, в том числе и пакет программ *GNU Privacy Guard* (его можно найти на www.gnupg.org), впервые выпущенный Фондом бесплатного программного обеспечения еще десять лет назад. Если вы не шифруете сообщения, отправляемые по электронной почте, то их можно запросто прочесть, так как они некоторое время хранятся на серверах по пути следования.

Привет, это я!

С проблемой кодирования тесно связана задача аутентификации (подтверждения подлинности). Предположим, что Алиса получает сообщение «Алиса, пожалуйста, пошли Еве $100. Люблю, Боб». Как ей узнать, что письмо действительно пришло от Боба, а не было сфабриковано Евой?

Так же, как в сценарии шифрования, для того, чтобы создавать сообщения для Алисы, Боб должен знать нечто такое, что не известно Еве. Таким образом, Бобу вновь необходим секретный ключ. Кроме того, Алиса должна кое-что знать о его СК, чтобы проверить, действительно ли сообщение пришло от Боба. И снова существуют два варианта протокола: аутентификация по секретному ключу, шире известная как код аутентификации сообщения, и аутентификация по открытому ключу, часто называемая схемой с цифровой подписью. Диффи и Хеллман первыми рассмотрели схемы с цифровой подписью — тогда же, когда они предложили шифрование с открытым ключом. Первой была построена схема, использующая алгоритм *RSA*.

Главная идея состоит в том, что Боб с помощью своего СК вычисляет «сигнатуру» (подпись), которую он добавляет к своему сообщению, а Алиса или кто-то еще используют его ОК, чтобы проверить, что подпись соответствует самому сообщению (*врезка слева*). Алиса знает, что сообщение должно быть от Боба, потому что никто больше не имеет СК, необходимого для создания правильной сигнатуры.

В настоящее время клиента электронной почты легко можно заставить думать, что сообщение прибыло от Боба, когда фактически оно прибыло от Евы. Фальшивые сообщения могут содержать подложную информацию, например неверные биржевые цены, провоцируя людей действовать вопреки их интересам. Но если бы вся электронная почтовая связь сопровождалась аутентификацией, то такое вмешательство стало бы невозможным: ваш почтовый клиент должен был бы сопровождать все отправляемые сообщения цифровой подписью и проверять цифровые сигнатуры всех поступающих сообщений. Аутентификация могла бы стать барьером на пути нежелательной почты, заставляя серверы отклонять поступающие сообщения, не заверенные отправите-

лем. В 1970-е гг., когда электронная почта только появилась, протоколов опознавания еще не существовало, и многие пользователи до сих пор действуют по старинке.

Маршрутизация методом «луковицы»

Зашифровав сообщения, вы можете скрыть от провайдера (или любого другого соглядатая) содержание корреспонденции, но не то, с кем вы общаетесь. Например, компания, предоставляющая Алисе услуги доступа в Интернет, будет знать, посещает ли она сайт Общества анонимных алкоголиков. Представьте себе, что могло бы произойти, если бы провайдер продавал такую информацию автомобильным страховым компаниям. Люди реже бы обращались за помощью в режиме онлайн, опасаясь увеличения страховых взносов.

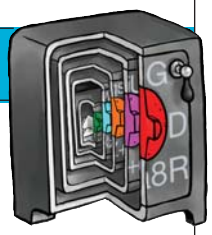
Проблему можно было бы решить с помощью *SFE*, используя который, Алиса может набрать *URL*-адрес страницы и посетить нужный ей сайт таким образом, что никто об этом не узнает. Однако безопасное вычисление функции в данном случае было бы очень неэффективным. В 1981 г. Дэвид Чом (David Chaum), работавший тогда в Калифорнийском университете в Беркли, предложил более простое решение, названное анонимными каналами, известное теперь как маршрутизация методом «луковицы».

Как следует из самого названия, Алиса «обертывает» свое сообщение рядом слоев. Она зашифровывает каждый слой (и все внутри него) с помощью открытых ключей различных людей, индивидуальных для каждого слоя, и затем вне каждого слоя добавляет адрес. Сообщение от Алисы до Боба могло бы дойти следующим образом: Алиса посылает «луковицу» Марку, который, удалив самый внешний слой, расшифровывает «луковицу» с помощью своего секретного ключа. Внутри он находит меньшую «луковицу» и адрес Лайзы. Он посылает ее Лайзе, которая расшифровывает «луковицу» своим ключом, и так далее. Наконец, Боб получает от кого-то ядро «луковицы», и расшифровывает его своим ключом, чтобы получить сообщение Алисы.

На практике в качестве посредников выступает сеть компьютеров (так называемых *Tor*-серверов), настроенных так, чтобы автоматически производить расшифровку и дальнейшую пересылку данных. В идеальном случае каждый промежуточный компьютер (*Tor*-сервер) непрерывно в случайном порядке получает и отправляет дальше множество «луковиц». Даже если провайдер все время следит за всеми посредниками, при достаточном уровне трафика «луковиц» в Сети он не сможет сказать, куда направлено

СОКРЫТИЕ СОЕДИНЕНИЙ

Данные можно послать анонимно с помощью протоколов маршрутизации по схеме «луковицы», в которой данные и нужный маршрут заключены в многослойную оболочку с множеством уровней шифрования



ОТПРАВКА «ЛУКОВИЦЫ»

Алиса сначала шифрует свое сообщение с помощью нескольких открытых ключей, принадлежащих случайно выбранным посредникам, создавая «луковицу» со многими слоями кодирования. Она также помещает в каждый слой команду маршрутизации

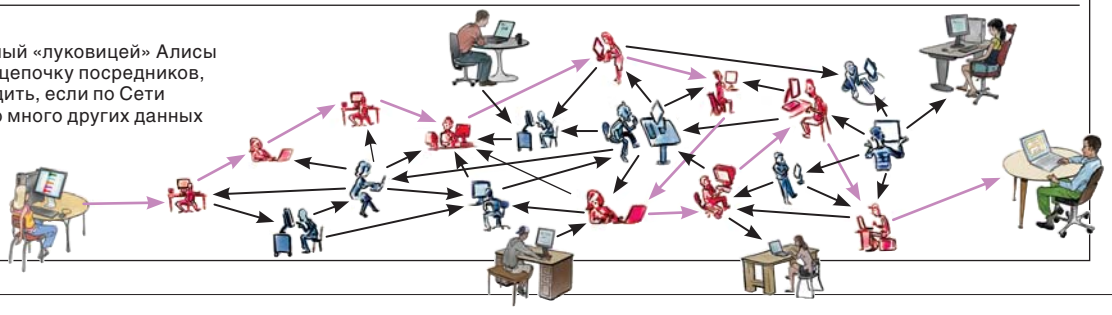
Она посылает «луковицу» Марку, секретный ключ которого расшифровывает самый верхний слой кодирования. Внутри он находит «луковицу», адресованную Лайзе, которую он ей и посылает

Секретный ключ Лайзы удаляет следующий слой «луковицы», и внутри она находит другую «луковицу» с адресом, которую она пересылает дальше, и т.д.

Наконец, Том добирается до ядра «луковицы» и посылает его Бобу, который открывает ядро своим секретным ключом и читает сообщение. Никто, кроме Алисы, не знает полного маршрута, проделанного «луковицей»

СЕТЬ

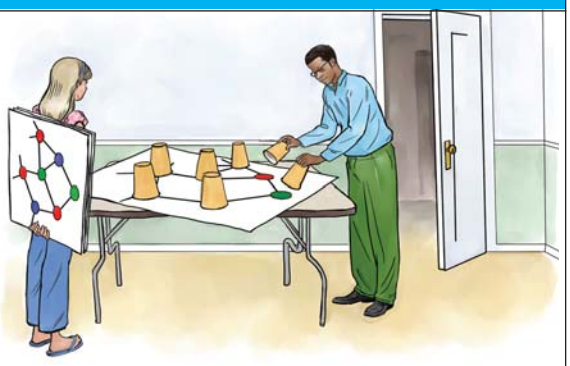
Маршрут, проделанный «луковицей» Алисы (*фиолетовый*) через цепочку посредников, невозможно проследить, если по Сети проходит достаточно много других данных



ПОДТВЕРЖДЕНИЕ ПОЛНОМОЧИЙ БЕЗ РАСКРЫТИЯ, КТО ВЫ ЕСТЬ

При использовании анонимной авторизации зарегистрированный пользователь может войти на сайт, не показывая никакой идентифицирующей его информации. Веб-сайт даже не был бы в состоянии связать пользователя с его предыдущими посещениями. Такой протокол — пример доказательства с нулевым разглашением, в котором одна сторона доказывает факт, не сообщая ничего о доказательстве, кроме утверждения о его правильности

Представьте себе, что Алиса и Боб играют в игру с графом, тремя цветными карандашами и пачкой бумажных стаканчиков. Граф представляет собой набор точек, или вершин, связанных линиями. Две вершины, соединенные линией, называют смежными. Только некоторые графы можно раскрасить тремя цветами, т.е., трех карандашей достаточно для закрашивания всех вершин таким образом, чтобы никакие две смежные вершины не были окрашены в один цвет. Алиса заявляет Бобу, что она раскрасила свой граф тремя цветами, не сообщая ему ничего о том, как это сделать.



Игра начинается с того, что Боб выходит из комнаты. Алиса рисует шесть отдельных копий графа. Поскольку она знает, как раскрасить граф тремя цветами, она делает это с первой копией. Для других пяти она использует все шесть возможных перестановок цветов. Таким образом, шесть копий являются трехцветными тривиально различными графами. Она выбирает одну из шести копий наугад, кладет ее на стол и накрывает каждую вершину бумажным стаканчиком. Теперь Боб возвращается, выбирает любые две смежные вершины и снимает с них стаканчики. Если две вершины оказываются одного цвета, то он узнает, что Алиса обманула его и не построила правильный трехцветный граф.

Они повторяют цикл: каждый раз Боб покидает комнату, а Алиса случайным образом выбирает одну из шести копий графа и накрывает ее стаканчиками. С точки зрения Боба, если Алиса обманывает его, то она могла бы показывать ему много различных недопустимых раскрасок, и предательское соответствие смежных вершин не обязано быть в одном и том же месте на каждом графе. Но поскольку он повторяет проверку достаточно много раз, вероятность, что он поймает обман, приближается к 100%. И все же после всего этого он не будет знать, как Алиса раскрасила граф. В каждом цикле два цвета, которые он видит на выбранных вершинах, случайны; он мог бы сам выбирать эти цвета.

Для любого утверждения, которое имеет разумно короткое доказательство (например, «Я имею документ, подтверждающий, что я зарегистрированный пользователь, и мне больше 18 лет»), можно придумать версию этой игры, которая доказывала бы данное утверждение, не раскрывая никакой дополнительной информации (такой как: «Меня зовут Алиса» или «Я пользователь № 4790561»).

сообщение Алисы или откуда пришло письмо для Боба.

Самому Бобу не известно, кто послал сообщение, если Алиса не включила в него свое имя. Но он все же может ответить, если она добавила «луковицу ответа», содержащую слои адресов и открытые ключи, которые должны направить сообщение отправителю.

Сообщения Алисы и Боба невозможно отследить, даже если некоторые из посредников допускают утечку информации о том, что они делают. Поскольку большинство участников системы предоставляют свои компьютеры в качестве промежуточных пунктов, то становится все более трудным выяснить, кто с кем связывается.

Как и в случае с шифрованием и цифровыми подписями для электронной почты, бесплатное программное обеспечение для общения по анонимным каналам или участия в Сети в качестве посредника доступно для всех. Проект «Маршрутизатор-луковица» (*TOR*), например, можно найти по адресу *www.torproject.org*.

Конфиденциальные входы в систему

Предположим, что Алиса — подписчик онлайн-журнала *SophistiCat American*. Она соединяется с сайтом журнала через анонимный канал, регистрируется под своим именем пользователя, при помощи своего пароля и заботится о том, чтобы все ее входящие и исходящие сообщения были зашифрованы. Означает ли это, что она может быть уверена: никто не узнает о том, что она делает онлайн? Конечно, нет — в журнале точно знают, что делает Алиса.

Она могла бы попробовать «замести следы» с помощью псевдонима, но читательские предпочтения такого пользователя могут указать на личность Алисы. Она может ввести свой почтовый индекс, чтобы узнать прогноз погоды, напечатать свою дату рождения, чтобы посмотреть гороскоп, и фактически сообщить свой пол, просматривая статьи по таким темам, как рак молочной железы. Трех блоков информации — почтовый индекс, дата рождения и пол — достаточно, чтобы однозначно идентифицировать 87% населения США (*см. в этом номере Гарфинкель С. «Данные всех стран, соединяйтесь!»*).

Удивительно то, что проблема Алисы имеет криптографическое решение, называемое анонимной авторизацией. Алиса может при каждом обращении к веб-странице журнала доказывать, что она — зарегистрированный пользователь. И все же это доказательство не позволяет узнать ничего о том, кем именно из подписчиков она является, и даже, скажем, что она тот самый человек,

который обращался к журналу несколькими часами ранее. Такой протокол — частный случай более общего протокола доказательства с нулевым разглашением информации.

При помощи доказательства с нулевым разглашением Алиса может убедить Боба, что ее утверждение является истинным, не показывая, почему оно истинно или фактически не давая никакой дополнительной информации вообще. Для доказательства утверждения «Я зарегистрированный пользователь журнала *SophistiCat American*» журнал или сторонняя служба при подписке могли бы выдать Алисе уникальный мандат — что-то похожее на секретный ключ. Каждый раз, когда журнал впоследствии будет запрашивать ее, она сможет использовать этот ключ, чтобы доказать, что она имеет действующую подписку, не предъявляя мандат непосредственно. Имея мандаты от различных организаций, Алиса могла бы обеспечить доказательство с нулевым разглашением и более сложных утверждений типа: «я зарегистрированный пользователь, и мне больше 18 лет».

Основная идея того, как работает доказательство с нулевым разглашением, иллюстрируется сценарием, описанным во врезке на противоположной странице, в котором Алиса доказывает Бобу, что она раскрасила диаграмму специальным способом (задача «раскрашивания графа тремя цветами»), не показывая Бобу, как она это сделала. Задача является так называемой *NP*-полной проблемой. Для данного обсуждения важным в *NP*-полноте является то, что вы можете выбрать любое утверждение, для которого имеется разумно короткое доказательство, и придумываете версию игры Алисы и Боба, чтобы дать доказательство вашего утверждения без раскрытия данных.

Протокол раскраски тремя цветами демонстрирует принципы, которые делают возможными доказательства с нулевым разглашением, но это не очень эффективно на практике — подобно тому, как неэффективно общее вычисление функции с соблюдением секретности. К счастью, исследователи-криптографы разработали подобные протоколы для частных видов мандатов, которые можно использовать для эффективной анонимной авторизации.

Взламывание кодов

Насколько надежны данные алгоритмы? Когда Алиса зашифровывает сообщение для Боба, насколько трудно Еве расшифровать его? И что, если Ева имеет какие-то дополнительные знания или возможности, чтобы попробовать играть с системой? Например, у нее может быть кое-какая информация о содержании зашифрованного сообщения — скажем, ей известно название местного кафе, где Алиса и Боб собираются впервые встретиться лично. Или, если «Боб» — особо защищенный веб-сервер, то Ева могла бы послать ему вместо зашифрованного текста тщательно подобранную тарабарщину и по его ответам получить данные о его секретном ключе. Общепринятое определение секретности при шифровании с открытым ключом охватывает все эти вопросы и требует, чтобы Ева не могла получить никакой сколько-нибудь пригодной для использования информации.

Анализ надежности криптосистемы — весьма разработанная область знаний. Вопреки обычному восприятию, шифрование — не игра в кошки-мышки, в которой система считается безопасной просто потому, что никто не показал, как ее можно взломать. Многие составные части криптографии основаны на хорошо изученных проблемах математики. Криптографы не могут с абсолютной уверенностью доказать, что такую-то криптосистему невозможно взломать, но они доказывают, что любой алгоритм взлома позволил бы ответить на один из фундаментальных вопросов, который уже загнал в угол лучших математиков и программистов.

Некоторые протоколы зависят только от существования определенного вида математической функции. Например, криптографы знают, как из любой функции-лазейки создать криптосистему с открытым ключом. Таким образом, если кто-то взломает функции, используемые в алгоритме *RSA*, то их можно заменить другими, которые еще сохранили стойкость.

Схема очень редко считается надежной на особых основаниях, и только после того, как сотни ведущих исследователей во всем мире изучали алгоритм в течение нескольких лет. Сообщество криптографов может позволить себе провести такую работу для нескольких критичных составляющих блоков. Затем они доказывают надежность больших систем исходя из надежности базовых блоков. Дополнительный материал по предположениям, лежащим в основе безопасности криптосистем, — на *www.SciAm.com/sep2008*.

Криптографические протоколы могут обеспечить удивительное разнообразие решений, казалось бы, неразрешимых проблем конфиденциальности информации (например, анонимной авторизации). Но многие из проблем секретности, с которыми приходится сталкиваться, не представляются криптографическими по самой своей природе. Если Алиса находится под постоянным наблюдением в физическом мире, то для нее слабым утешением будет то, что ее действия онлайн безопасны. Так, в Лондоне в интересах правоохранительной деятельности в общественных местах размещены камеры наблюдения. Возможно, чтобы защитить частную жизнь граждан, владельцы здания могли бы управлять данными от камер, установленных на их собственности, таким образом, чтобы *SFE* (вычисление функции с соблюдением секретности), позволяло проследить за подозреваемыми, покидающими место преступления, не сохраняя в центральной базе данных действия других лиц. В более широком смысле, когда частной сфере угрожает, например, видеонаблюдение в общественных местах, мы должны спросить себя, какие проблемы данная система пытается решить? И можем ли мы сохранить нашу приватность с помощью криптографии? ■

Перевод: Б.А. Квасов

ПРОБЛЕМЫ ОНЛАЙН-БЕЗОПАСНОСТИ

По мнению специалистов по защите информации, для эффективного противостояния растущему числу все более сложных атак хакеров необходимо уделять внимание не только усовершенствованию технологий, но и человеческому фактору, а также юридической стороне проблемы

Участники круглого стола

Рахул Абхьянкар (Rahul Abhyankar)
Старший директор по управлению продуктами, *McAfee Avert Labs, McAfee*

Уитфилд Диффи (Whitfield Diffie)
Вице-президент и глава отдела безопасности, *Sun Microsystems*

Арт Гиллилэнд (Art Gilliland)
Вице-президент по управлению продуктами, информационными рисками и соответствию законодательным требованиям, *Symantec*

Патрик Хейм (Patrick Heim)
Глава отдела защиты информации, *Kaiser Permanente*

Джон Лэндвер (John Landwehr)
Директор по решениям по безопасности и стратегии, *Adobe Systems*

Стивен Липнер (Steven Lipner)
Старший директор по технической стратегии защиты, *Microsoft*

Мартин Сэдлер (Martin Sadler)
Директор лаборатории безопасности систем, *HP Labs, Hewlett-Packard*

Райан Шерстобитов (Ryan Sherstbitoff)
Главный корпоративный специалист по продвижению, *Panda Security US, Panda Security*

Quis custodiet ipsos custodes? («Кто будет охранять охраняющих?») — гласит классическая римская максима. Однако поставщики средств защиты, стоящие на страже безопасности современных сетевых информационных систем, находятся под пристальным вниманием своих конкурентов, клиентов, хакеров, а все чаще — и правительств, заботящихся о национальной безопасности. В мае 2008 г. главный редактор журнала *Scientific American* Джон Ренни (John Rennie) встретился в Пало-Альто (штат Калифорния) с представителями отрасли защиты информации и некоторых смежных отраслей, чтобы обсудить трудности, с которыми все они сталкиваются. Ниже приводятся некоторые выдержки из беседы. Полную версию обсуждения можно найти на *www.SciAm.com/sep2008*.

На ком лежит ответственность?

Участники обсуждения пришли к общему мнению в определении приоритетных направлений в области поддержания и повышения уровня безопасности информации. Большое внимание уделялось не только развитию технологий, но законодательным и юридическим аспектам.

Диффи: В следующем десятилетии веб-услуги и то, что я называю цифровым аутсорсингом, будут оказывать огромное влияние на общество. Мы стоим на пороге мира, в котором существенно расширится спектр информационных услуг. Через десять лет, оглянувшись вокруг, вы увидите: того, что сегодня называют безопасной информатикой, больше не существует. Поэтому понадобится законодательная база, которая обяжет участников соглашений обеспечивать защиту своей информации. Однако для этого должны быть созданы надлежащие технические средства защиты.

Гиллилэнд: Да, но сегодня пользователи реализуют предоставляемые технологиями возможности в гораздо меньшем объеме, чем могли бы. Возможно, пока это и не создает проблем. Речь идет о необходимости сделать технологии настолько удобными, чтобы клиенты могли решать конкретные задачи: самостоятельно проводить проверки и управлять защитой данных в соответствии с действующими стандартами. Сегодня большинству это недоступно.

Липнер: Для корпоративных клиентов необходимо то, о чем говорили Диффи и Гиллилэнд: гарантии того, что с данными можно произвести

определенный объем операций, способы описания ограничений в отношении их использования и т.д. Пользователям нужна среда, которой они могли бы доверять и которая на деле работала бы, поскольку развитие Интернета и интернет-бизнеса во многом зависит от доверия клиентов. Мы обязаны укреплять это доверие и добиваться того, чтобы оно было оправдано.

Гиллилэнд: Мы должны достичь своеобразного баланса: с одной стороны, дать предпринимателям возможность совместно пользоваться информацией с наибольшей быстротой, чтобы они могли принимать правильные решения, а с другой стороны — сделать такое совместное пользование простым.

Коварный человеческий фактор

Ахиллесовой пятой систем безопасности могут быть сами пользователи, которые склонны ошибаться и, пусть и неосознанно, жертвовать безопасностью ради простоты в работе. Именно технологии должны компенсировать возможные слабости пользователей.

Хейм: Человеческий фактор нельзя недооценивать. Здесь можно провести параллель с вождением автомобиля. Мы требуем наличия водительского удостоверения, чтобы автомобилисты понимали хотя бы основы правил дорожного движения и знали, как управлять транспортным средством, т.к. это сводит к минимуму его потенциальную опасность. Не думаю, что конечные пользователи в достаточной мере осведомлены о правилах безопасного пользования их системами. Я не настаиваю на необходимости «информационного водительского удостоверения», но, знаете, это неплохая идея. Очевидно, что многие наблюдаемые проблемы — по своей природе поведенческие.

Диффи: Это чудовищная идея. Киберпространство — мир будущего. Ограничение доступа — покушение на свободное общество.

Абхьянкар: Пренебрегать человеческим фактором нельзя. Недавно мы отмечали тридцатилетие спама. Электронная почта, которой все

Рахул Абхьянкар
McAfee

Райан Шерстобитов
Panda Security

Джон Лэндвер
Adobe Systems

Арт Гиллилэнд
Symantec

Патрик Хейм
Kaiser Permanente

Мартин Сэдлер
Hewlett-Packard

Стивен Липнер
Microsoft

Уитфилд Диффи
Sun Microsystems

пользуются — уязвимое место технологии. Средства хищения информации, находящиеся в распоряжении «плохих парней», совершенствуются намного быстрее, чем те, которыми располагают «хорошие парни» для ее защиты. Это проблема, которую при помощи одних только технологий решить невозможно.

Гиллилэнд: Наши исследования показывают, что около 98% потерь данных обусловлены ошибками людей и нарушениями технологических процессов. В отрасли защиты информации мы постоянно боремся со злоумышленниками. Но не они являются главной проблемой в вопросе утери данных. Хищение информации всегда дает возможность кому-то заработать, и мы никогда не сможем искоренить такого рода деятельность. Однако можно существенно сократить утерю данных, обусловленную человеческим фактором.

Хейм: Мы каждый день видим, что если служба технической поддержки не может предвосхитить нужды отдельных лиц, то они во многих случаях позволяют себе выполнять свою работу с помощью технологий потребительского уровня.

Шерстобитов: Верно. Невозможно обеспечить безопасность информации, если, чтобы поработать дома, вы пересылаете ее себе самому через *Gmail*.

Хейм: Несомненно, что если людям не предоставлены безопасные технологии, то они будут пользоваться потребительскими, например маршрутизатором с беспроводным доступом или съемным *USB*-накопителем. Таким образом, кроме технических трудностей существуют и экономические. Сколько нужно потратить денег, чтобы сделать информационные технологии удобными и безопасными, такими, чтобы людям не нужно было проникать через черный ход, чтобы делать свою работу?

Диффи: Короче говоря, нехватка функций часто оборачивается угрозой безопасности. Если система не позволяет вам безопасно делать то, что вам нужно, вы в любом случае будете делать это, но так, как сможете.

Экономика современного хакерства

Хакерство перестало быть уделом любопытных или скучающих программистов. Сегодня создание вредоносных программ превратилось в бизнес, что радикально меняет рамки задачи.

Абхьянкар: Экономическая модель хакерства разработана настолько хорошо, что, будь это дело законным и будь вы предприимчивым капиталистом, ищущим приложение своим деньгам, вы могли бы получить хорошую прибыль. Верно? Стоимость отправки сообщения по электронной почте все время снижается. А анонимность в Сети затрудняет поиск «плохих парней» с целью привлечения их к ответственности.

Шерстобитов: Большую часть работы хакеры делают чужими руками. Они используют посредников. В результате расследования вы выходите на людей — их называют мулами, — которые не имеют представления, что стали жертвами определенной схемы. В результате мы видим, как с некоего веб-сайта распространяется послание, где говорится: «Есть прекрасная работа для вас! Заработок — $1000 в неделю!» Правоохранительные органы не могут добраться до создателя вредоносной программы. Хакера или того, кто организовал атаку, давно уже нет. Хакеры не проводят атак сами, они продают свои программы. На их продаже держится целая подпольная экономика. Сегодня вы можете купить что-то, скажем, за $1200 и стать киберпреступником.

Сэдлер: Итак, раз мы все понимаем, какими изощренными стали методы «плохих парней», то какой степени сотрудничества должны мы придерживаться? Ведь мы все фактически конкурируем между собой. Мы разобщены, а злоумышленники сплочены. И есть множество свидетельств тому, что разные организованные криминальные группы торгуют друг с другом. У нас нет такого уровня кооперации.

Шерстобитов: Именно поэтому я и ратую за использование подхода, обеспечивающего независимость от поставщика. Для преодоления угрозы необходимы не только технические средства, но и совместное противодействие: исследовательские лаборатории должны обмениваться получаемыми сведениями. Уже сегодня часть образцов вредоносных программ наши лаборатории получают не от клиентов, а от коллег по отрасли. На высшем уровне мы не ведем себя как жесткие конкуренты. Это общая проблема, которую мы должны решать объединенными усилиями.

Лучшее просвещение или лучшее проектирование?

Участники круглого стола пришли к парадоксальному выводу: в долгосрочной перспективе защита данных не зависит от уровня знаний пользователей: слишком быстро меняется природа угроз.

Липнер: Мы должны избавить конечных пользователей от необходимости сложного обучения и добиться того, чтобы технология сама помогала им обеспечивать свою безопасность, а не заставляла мучаться с всплывающими окнами. Очень многое в построении систем безопасности зависит от опытности пользователя. И я считаю, что это дело срочное для всей отрасли: времени у нее мало.

Сэдлер: Я вообще не думаю, что мы должны делать упор на обучение пользователей. Я уверен, что лишь просвещение в самом общем смысле может быть полезным дольше шести месяцев. Посмотрите на множество образовательных программ во всем мире: все, чему они учат пользователя, имеет очень короткий срок действия. Нужно устанавливать новейшие версии антивирусных программ.

Хейм: Если бы люди осознавали реальные последствия установки, например, бесплатного скринсейвера (программы, выводящей анимированную заставку на экран монитора), говоря себе: «Я доверяю разработчику этой маленькой штучки, обеспечивающей полный доступ к моей системе и всем моим данным», — то это могло бы изменить их поведение в Сети.

Сэдлер: Я думаю, что выход есть. Вы учите своих детей, когда они выходят из дома, быть внимательными к окружению, объясняете, что опасно,

а что нет. Происходящее в Интернете можно описать так: вы продемонстрировали свой банковский счет в самой подозрительной компании и удивляетесь, что вас ограбили. Нужно разделить цели, чтобы люди могли устанавливать новейшие версии скринсейверов, но в ту часть своей среды, которая не влияет на банковский счет.

Хейм: Однако когда мы имеем дело с крупномасштабными инфраструктурами, нам нужно иметь возможность делать вставки в программы и сохранять устойчивость среды. И не всегда можно быть уверенным, что вносимые изменения не разрушат систему полностью.

Гиллилэнд: Я согласен, что не нужно никакого водительского удостоверения или сертификата на право пользования Интернетом. Но почему бы не создать что-то вроде ликбеза по безопасности для конечных пользователей? Такой инструктаж, когда вы приходите в компанию: «Вот ваш ноутбук, вот ваш КПК. Я хочу научить вас принципам безопасности при работе с *Symantec*».

Сэдлер: И как долго, по-вашему, эта информация будет актуальна?

Гиллилэнд: Достаточно долго.

Диффи: Это зависит от самих принципов.

Гиллилэнд: «Не открывайте электронные сообщения от неизвестных адресатов или вложения в эти сообщения».

Диффи: Это безнадежное правило.

Липнер: Единственный путь здесь — использование инфраструктуры обеспечения безопасности и аутентификации (опознавания). Вы предоставляете пользователям возможность выбора, но они должны знать, что есть классы вещей безопасных, будь то веб-сайты, вложения или исполняемые программы. Когда вы говорите пользователю: «Вы должны прочесть код или интерпретировать диалоговые *SSL*-окна», это слишком сложно для него. Необходимо предоставить пользователю инфраструктуру аутентификации, которая позволяла бы ему знать, с кем он имеет дело.

Гиллилэнд: Если конечным пользователям предоставить возможность, но не обучить должным образом, то они будут пренебрегать правилами доверительного поведения. Даже если на экран выскочит окно с предупреждением об опасности данного сайта, а на сайте будет заманчивый призыв: «Кликните здесь, и вы увидите обнаженную Бритни Спирс», пользователи будут кликать. Самый эффективный способ распространения вирусов — психологическая атака. Всегда.

Лэндвер: Нет ли другого пути? Вместо того чтобы уделять так много внимания тому, как ознакомить пользователей с вредоносными программами, мы можем таким образом изменить правила игры, чтобы снизить заинтересованность хакеров в атаках на наши компьютеры, улучшив уровень защиты информации. Тогда кто-то, похитив файлы с чужого жесткого диска, обнаружит, что они зашифрованы. Ошибочно отправленное по почте сообщение также будет невозможно прочесть. Если информация попадет куда-то, куда она не должна была попадать, то у получателя не будет ключа, чтобы расшифровать ее.

Шерстобитов: Согласен. В финансовом сообществе уже начинается переход на опознавание по внешнему каналу (взаимное опознавание двух независимых систем, например подключенного к сети компьютера и сотового телефона). Некоторые разъездные торговцы получают аутентификационные устройства — интеллектуальные ключи или *RSA*-маркеры. Некоторые финансовые организации включают системы обнаружения аномалий в серверную часть, чтобы выявлять подозрительные структуры данных и локализации. Наконец, финансовые организации видоизменяют свои технологии и механизмы аутентификации таким образом, чтобы они не привлекали хакеров.

Лэндвер: Существует множество работ, посвященных смарт-картам (со встроенным микропроцессором и ОС). Получив такую карту — электронный пропуск здесь, я смогу воспользоваться ею, чтобы войти в здания нашей компании, расположенные по всему миру. Но в нее заложены также мои опознавательные данные на основе инфраструктуры открытых ключей (*PKI*), которые я могу использовать для входа в прикладные программы, шифрования деловых документов и цифровой подписи *PDF*-файлов. Кроме того, она защищена *PIN*-кодом как банковские пластиковые карточки. Тот, кто похитит у меня карточку, получит лишь возможность несколько раз ввести *PIN*-код, после чего она перестанет работать.

Международные планы

Национальные планы в отношении защиты информации и частной жизни сильно различаются. США во многих отношениях опаздывают с реакцией на возникающие угрозы.

Сэдлер: Мне представляется, что во Франции, Германии и Великобритании просвещению малого бизнеса уделяется гораздо больше внимания, чем в США. Поэтому, несмотря на свои доводы против просвещения, я полагаю, что Соединенные Штаты, вероятно, должны предложить малому бизнесу некие основы. Диалог между наукой, властью и бизнесом в Европе также идет гораздо лучше, чем в Америке.

Шерстобитов: В Европе создаются специальные группы по борьбе с киберпреступностью. Они принимают меры заблаговременно. Но из бесед с ФБР видно, что в нашей стране ничего подобного пока нет.

Липнер: Поскольку и в Европе, и в США есть свои особенности и цели, потребуются дополнительные стандарты. И я считаю, что они должны быть международными.

Гиллилэнд: Несомненно, что нормы защиты частной сферы в разных странах Европы несколько различаются. Компании стараются понять, как им вписаться в некоторые процессы или в политические рамки, чтобы выполнять как можно больше правил. Это задача, которой мы не уделили здесь достаточного внимания. Как люди и компании, которые стараются удовлетворять законодательным требованиям в отношении приватности, могут доказать, что они действительно делают это? ■

Перевод: И.Е. Сацевич

Дэниел Солоув

КОНЕЦ приватности?

Молодые люди выносят на сайты социальных сетей самые интимные подробности своей личной жизни, что предвещает пересмотр соотношения общественного и личного

У него есть имя, но большинство людей знают его как *Star Wars Kid* (мальчик из «Звездных войн»). Он действительно известен десяткам миллионов человек во всем мире. К сожалению, эта популярность стала одним из самых досадных моментов его жизни.

В 2002 г. он снял себя на видео размахивающим уловителем мячей для гольфа как световым мечом. Ему было 15 лет, он постоянно спотыкался и без квалифицированной помощи специалистов-хореографов, работавших на съемках «Звездных войн», выглядел комично. Эту запись нашел один из мучителей мальчика и выложил на известный видеоресурс в Интернете. Она мгновенно стала хитом для множества фанатов. Обитатели блогосферы стали дразнить парня, насмехаясь над его малым ростом, неуклюжестью и непривлекательностью. Появилось несколько ремиксов ролика с добавлением спецэффектов. Блоггеры заставляли уловитель мячей светиться подобно световому мечу, накладывали музыку из «Звездных войн» или микшировали запись с другими. Были созданы десятки версий. *Star Wars Kid* появился в видеоигре и в телевизионных шоу *Family Guy* («Семейное посмешище») и *South Park* («Южный Парк»). Одно дело, когда тебя дразнят одноклассники, и совсем другое, когда тебя высмеивает весь мир. Подросток ушел из школы и вынужден был прибегнуть к помощи психологов.

То, что случилось с ним, может произойти с каждым из нас — и в любой момент. Сегодня фиксирование личной информации стало второй натурой человека. У все большего числа людей появляются сотовые телефоны с фотокамерами, цифровые аудиорекордеры, веб-камеры и другие устройства, легко регистрирующие детали их частной жизни. Впервые в истории человечества возможность распространять информацию по всему миру появилась почти у каждого. Теперь не нужно быть знаменитостью, чтобы СМИ взяли у тебя интервью. С помощью Интернета любой человек может получить всемирную аудиторию.

Появление новых технологий привело к разрыву между поколениями. По одну сторону баррикад оказались школьники и студенты, чья жизнь значительной частью проходит в социальных сетях и блогах, а по другую — их родители, чье прошлое часто остается погребенным в их слабеющей памяти или в лучшем случае запечатленными в книгах, на фотографиях и видеозаписях. История жизни нынешнего поколения сохраняется в Интернете потенциально навечно. Данная тенденция позволяет поднять вопрос о том, какой степени приватности люди могут ожидать (или желать) в век вездесущности социальных сетей.

Поколение *Google*

Число молодых людей, пользующихся такими социальными сетями, как *Facebook* или *MySpace*, ошеломляет. В большинстве кампусов более 90% студентов поддерживают собственные сайты. Я называю современную молодежь «поколением *Google*». Многие фрагменты их частной информации останутся в Интернете навсегда и будут доступны для нынешнего и будущего поколений путем простого поиска с помощью системы *Google*.

У этой открытости есть и позитивные, и негативные аспекты. Сегодня люди могут распространять свои идеи повсюду, не завися от издателей, радиовещания и других традиционных цензоров. Но эта возможность таит огромную угрозу для частной сферы и репутаций. Газета «Нью-Йорк Таймс» вряд ли обратит внимание на слухи, циркулирующие в школе старшей ступени г. Дубьюк или в Орегонском университете, а вот блоггеры и другие люди, общающиеся через Сеть, очень даже обратят. Для них рассказы и слухи о друзьях, врагах, членах семьи, боссах, сослуживцах и других — главный материал для размещения в Интернете.

До появления Интернета слухи распространялись из уст в уста и оставались в пределах местного общества. Подробности личной жизни фиксировались в дневниках, которые хранились под замком в тайном ящике письменного стола. Сайты социальных сетей, порожденные Интернетом, позволили человечеству вернуться к культуре тесных связей доиндустриального общества, где почти каждый член племени или житель деревушки знал о своих соседях все. Только «деревушка» теперь охватывает весь мир. Студенты колледжей стали распространять непристойные подробности из жизни своих коллег. Веб-сайт *JuicyCampus* играет роль доски объявлений, на которой студенты всей страны могут анонимно «вешать» непроверенные пикантные сведения о сексе, употреблении наркотиков и пьянстве в жизни учащихся в колледжах. Другой сайт, *Don't Date Him Girl*, призывает женщин помещать жалобы на мужчин, с которыми они встречались, с указанием имен и предоставлением фотографий.

Социальные сети и блоги — не единственные угрозы приватности. В нескольких статьях настоящего номера говорится о том, что компании постоянно собирают и используют частную информацию о людях. Компания, которая выдала вам кредитную карточку, регистрирует все ваши покупки. Если вы покупаете что-то через Интернет, то торговцы ведут список всех купленных вами вещей. Ваш интернет-провайдер отслеживает ваши перемещения

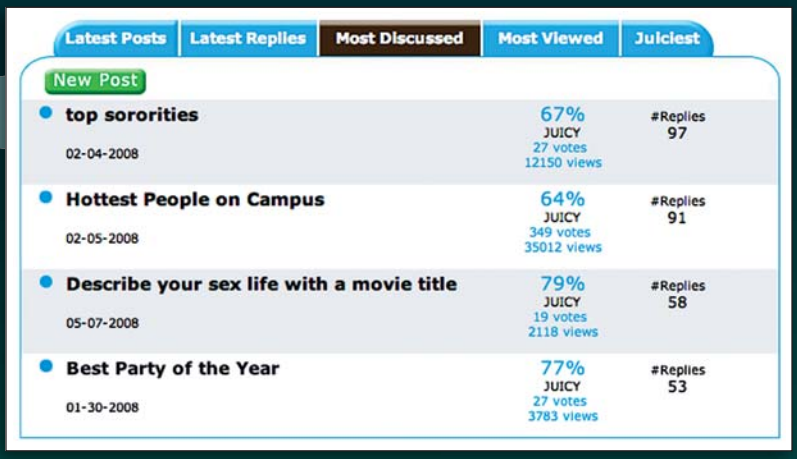
ОСНОВНЫЕ ПОЛОЖЕНИЯ

- Сайты социальных сетей позволяют тривиальным, казалось бы, сплетням распространяться по всему миру, иногда делая людей объектами кривотолков, известных миллионам пользователей Интернета.
- Публичное распространение сведений о личной жизни привело к переосмыслению сегодняшней концепции приватности.
- Существующие законы следует дополнить, чтобы обеспечить некоторую защиту частной сферы в отношении того, что говорят и делают люди в среде, раньше считавшейся общественной.

HARRY CAMPBELL

ПО СЕКРЕТУ ВСЕМУ СВЕТУ

Для сайтов, выносящих на свет божий ошибки, сексуальные подвиги и другие сплетни о жизни колледжа, не бывает слишком сокровенных подробностей



JUICYCAMPUS — популярная электронная доска объявлений, на которую студенты могут анонимно «вывешивать» сплетни и слухи о других студентах. На сайте сообщается, что он был создан «с простой целью дать возможность анонимного свободного разговора в Сети о жизни кампуса». Темы сплетен — секс, наркотики, пьянство, болезни и другие, позволяющие осветить темные стороны жизни колледжа

DON'T DATE HIM GIRL — сайт, на котором женщины размещают сведения о мужчинах, с которыми они встречались. В их рассказах называются их реальные имена и приводятся фотопортреты. Непроверенные сведения могут включать утверждения, что мужчина инфицировал женщину половым путем или был жестоким

по Сети, а ваша компания кабельного телевидения знает, какие шоу вы смотрите.

Нарушает приватность и правительство, собирая обширные базы данных, которые можно использовать для выявления подозрительного поведения. Управление национальной безопасности США прослушивает и изучает записи миллионов телефонных разговоров. Другие организации анализируют финансовые операции. Тысячи государственных институтов на федеральном уровне и на уровне штатов имеют реестры личных сведений, хроники рождений и вступлений в брак, записи сведений о работе, собственности и др. Информация часто хранится открыто, будучи легко доступной кому угодно, и с увеличением числа электронных записей тенденция к большей незащищенности личных данных продолжает расти.

Будущее репутаций

Широкая доступность частных сведений ограничивает возможности защиты репутации путем формирования образа, представляемого людям. Репутация играет очень важную роль в обществе, и разглашение подробностей о личной жизни может сильно повредить ей. Мы учитываем репутацию человека, когда решаем, дружить ли с ним, встречаться, принимать ли его на работу или заключать перспективную сделку.

Можно предположить, что сужение частной сферы сделает людей менее замкнутыми и более честными. Но если проступки каждого выставляются на всеобщее обозрение, то это вовсе не означает, что люди станут судить других менее жестко. Осведомленность в ваших личных делах может и не улучшить мнения о вас — она скорее увеличит вероятность того, что вас станут опрометчиво осуждать. Более того, редукция приватности может подавить свободу. Необходимость жизни на виду в сетевом мире может привести к тому, что вам никогда не удастся избавиться от груза ошибок прошлого.

Люди хотят всегда иметь шанс начинать с чистого листа. Как отме-

TOMMY MOORMAN; SOURCES: JUICYCAMPUS AND DON'T DATE HIM GIRL (screen shots)

тил американский философ Джон Дьюи (John Dewey), человек не есть «нечто полное, совершенное или законченное». Он есть «нечто движущееся, меняющееся, состоящее из отдельных частей и, наконец, формирующееся, а не окончательное». Раньше юношеские эксперименты и глупости постепенно забывались, что позволяло людям меняться и расти. Но при нынешнем обилии информации в Сети избавиться от напоминаний о грехах молодости становится все труднее. Людям приходится жить под грузом цифрового багажа своего прошлого.

Эта открытость означает, что возможности людей поколения *Google* могут сужаться из-за чего-то сделанного много лет назад. Их секреты могут быть раскрыты их знакомыми, или же они могут стать ничего не подозревающими жертвами ложных слухов. Однако нравится вам это или нет, но многие люди начинают привыкать к тому, что в Сети хранится великое множество сведений о них.

Что делать?

Можем ли мы предотвратить грозящую в будущем опасность, когда колоссальные объемы информации о личной жизни людей будут свободно циркулировать по миру без их ведома? Некоторые технические специалисты и юристы категорически утверждают, что не можем. Приватность, говорят они, просто несовместима с миром, в котором данные обращаются так свободно. Известно высказывание Скотта Макнили (Scott McNealy) из компании *Sun Microsystems*: «У вас уже нет приватности. Забудьте о ней». Бесчисленные книги и статьи провозвестили «конец», «смерть» и «разрушение» приватности.

Такие заявления в лучшем случае ошибочны. Защитить частную сферу еще можно, но это потребует переосмысления ее устаревшей концепции. Существует точка зрения, что приватность требует полной секретности: как только информация становится известной другим, она перестает быть частной. Такое определение не годится для сетевого мира. Современная молодежь понимает приватность более тонко. Она уже принимает как данность то, что частными сведениями пользуется бесчетное количество людей, и что любой из нас оставляет след везде, куда бы ни пошел. Нюанс трактовки поколения *Google* — осознание необходимости того, что человек должен сохранять какую-то степень контроля над личной информацией, которая становится широко доступной. Представители этой генерации хотят говорить о том, как распространяются сведения об их частной жизни.

Вопрос контроля над личной информацией вышел на передний план в 2006 г., когда сайт *Facebook* ввел службу *News Feeds*, назначением которой было оповещение друзей пользователя, подписавшихся на эту службу, об изменении или обновлении странички с его данными. К большому удивлению владельцев сайта, многие из его пользователей выразили возмущение. Жалобы предъявили более 700 тыс. человек. На первый взгляд гневные протесты против *News Feeds* выглядят непонятными: ведь сведения на этих страничках и так находились в свободном доступе. Почему же недовольные сочли оповещение друзей об изменениях этих сведений нарушением приватности?

А вот почему. Они и не считали, что частная сфера — это секреты, хранящиеся в темном чулане. Все дело в доступности. Протестующие пользователи указывали, что большинство людей не проявляют такого интереса к их личным данным, чтобы обращать внимание на небольшие изменения и обновления, которые, соответственно, могли оставаться незаметными. Но *Facebook* акцентировал эту информацию. Таким обра-

ИНТЕРНЕТ ПОМНИТ ВСЕ

Сегодня обречь на всемирное осмеяние можно одним нажатием клавиши ввода. Когда некий молодой человек хотел поступить на работу в инвестиционную компанию, вместе со своим резюме он послал видеоклип под заголовком «Невозможного нет», где показал себя занимающимся разными физическими упражнениями — от жима лежа, где он поднимает 224 кг, до прыжков на лыжах и разбивания кирпичей ребром ладони. На протяжении всего ролика он превозносит свои спортивные достижения и успешность в жизни.

Нет нужды говорить, что этот клип имел мало отношения к работе, которую он хотел получить, а самомнение юноши было столь завышенным, что клип выглядел очень смешно. Видимо, кто-то в инвестиционной компании допустил утечку информации, и видеоролик попал в *YouTube*. Он мгновенно стал хитом, его просмотрели сотни тысяч раз. Героя высмеивали и пародировали. Его шансы получить работу существенно снизились. Молодой человек несомненно сделал глупость и мог извлечь из нее урок, но его ошибка, его детское хвастовство остались в Интернете навсегда

SOURCE: VEOH (video clips); GEORGE WASHINGTON UNIVERSITY LAW SCHOOL (Solove)

ОБ АВТОРЕ

Дэниел Солоув (Daniel J. Solove) — профессор права в Школе права Университета Джорджа Вашингтона и автор книг *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* («Будущее репутаций: слухи, сплетни и приватность в Интернете», 2007) и *Understanding privacy* («Осмысливая приватность», 2008).

СТРАТЕГИИ ЗАЩИТЫ ЧАСТНОЙ СФЕРЫ

Законы о защите частной сферы в США менее строги, чем во многих других странах. Желание защитить личную жизнь людей в Интернете породило новые мысли о том, как сочетать открытость с необходимостью ограничить обнародование подробностей личной жизни

ДЕЛИКТ присвоения

Имя или образ — например, лицо Анджелины Джоли — не могут без ее согласия использоваться в рекламе для получения финансовой выгоды. Для борьбы со злоупотреблениями в Сети эту норму общего права необходимо расширить, запретив помещение фотографий в Интернете без согласия изображенного лица

ДЕЛИКТ НАРУШЕНИЯ КОНФИДЕНЦИАЛЬНОСТИ

Частная информация, предоставляемая определенным категориям лиц, например врачам, адвокатам и священникам, защищена законом. Эту правовую норму можно ужесточить, чтобы охватить другие виды взаимоотношений, например отвергнутых любовников, бывших супругов или друзей

ПУБЛИЧНАЯ ПРИВАТНОСТЬ

По законам США человек теряет все права на защиту частной информации, если она была обнародована. В Канаде и многих европейских странах такое обнародование не означает потери всех прав на охрану этой информации. Необходимо осознать, что при появлении на публике человек не должен терять всех прав на защиту своей приватности

зом, протесты касались не секретности, а степени доступности.

В 2007 г., когда *Facebook* ввел рекламную систему, состоящую из двух частей, *Social Ads* и *Beacon*, это вызвало новую волну возмущений. *Social Ads* позволяла сайту каждый раз, когда кто-то положительно отзывался о товаре или фильме, использовать имя, снимок и слова этого человека в рекламных объявлениях, рассылаемых его друзьям, в надежде, что такое одобрение будет действеннее обычной рекламы. А *Beacon* обеспечивала обмен данными с разными другими коммерческими сайтами. Если человек покупал билет на фильм на сайте *Fandango* или товар на каком-то другом сайте, сведения об этом сразу же отражались на страничке с его данными. *Facebook* развернул упомянутые программы без надлежащего уведомления пользователей. Люди случайно обнаруживали себя на страничках своих друзей рекламирующими новое приобретение. А другие были шокированы, увидев, что их частные покупки на других сайтах выставлялись на всеобщее обозрение. Протесты и соответствующие электронные требования изменения этой практики, быстро собравшие десятки тысяч подписей, привели к внесению некоторых коррективов.

Как видно из приведенных выше случаев, приватность не всегда касается только разглашения секретных сведений. Пользователи сайта *Facebook* не хотели, чтобы при помощи программы *Social Ads* товары рекламировались с использованием их имени. Одно дело — написать, сколько радости доставили вам фильм или музыка, и совсем другое — когда ваше имя используют для того, чтобы всучить товар другим.

Изменения законодательства

В Канаде и большинстве европейских стран законодательное обеспечение приватности гораздо строже, чем в США, которые противились введению всеобъемлющего законодательства. Законы о частной сфере в других странах оговаривают, что предоставление информации другим не ограничивает права человека на приватность. Однако растущая доступность личной информации требует, чтобы и США поняли необходимость определенной степени охраны приватности в мире открытости.

В некоторых областях законодательства США располагают хорошо разработанной системой контроля информации. Система авторского права строго регламентирует права пользования информацией, обеспечивая защиту широкого круга произведений — от кинофильмов до программного обеспечения. Защита права на интеллектуальную собственность не означает, что результаты умственного труда необходимо держать под замком. Вы можете читать журнал, авторские права на который охраняются, можете копировать материалы из него для личного пользования и одалживать эти копии другим. Но вы не имеете права делать с ними все, что вам заблагорассудится, например фотокопировать от корки до корки или продавать нелегальные копии на улице. Закон об авторском праве нацелен на обеспечение баланса свободы и контроля, хотя пока ему еще приходится бороться с противоречиями цифрового века.

Ближе всего к строгой системе наподобие регламентации охраны авторских прав законодательство США в отношении защиты приватности подходит в формулировке понятия «деликта присвоения» — запрета на использование имени или образа другого человека для извлечения финансовой выгоды. К сожалению, этот закон сформулирован таким образом, что часто оказывается неэффективным против того типа угроз приватности, число которых нарастает сегодня. Закон об охране авторских прав касается в основном защиты прав собственности на продукты творческой деятельности человека, например песни или картины. В целях борьбы с растущим риском угрозы приват-

ТОЛЬКО ФАКТЫ

Каждый день люди выкладывают на сайт *YouTube* больше 65 тыс. видеозаписей

В 2006 г. число пользователей сайта *MySpace* превысило 100 млн

С 1999 г. число блогов выросло с 50 до 50 млн

Больше 50% блогов ведутся людьми младше 19 лет

МОЯ ЖИЗНЬ — ТВОЯ ЖИЗНЬ

После того как три службы сайта *Facebook* самовольно послали информацию друзьям пользователей, последние потребовали более строгой защиты частной сферы

TOMMY MOORMAN; SOURCE: FACEBOOK (screen shot)

ности понятие деликта присвоения следует расширить, возможно, включив в него исходную интерпретацию этого принципа общего права в начале XX в., где защита частной сферы рассматривается шире, чем защита собственности: «Право изъятия из открытого обозрения в тех случаях, когда человек может считать это подобающим, входит в право на личную свободу», — говорится в декларации Верховного суда штата Джорджия 1905 г. Однако сегодня деликт присвоения не вменяется, когда имя или изображение человека появляются в новостях, произведениях искусства или на сайтах социальных сетей, в то же время защищая от использования имени или образа человека без его согласия в рекламных целях. Это ограничение весьма существенно. Оно означает, что деликт присвоения будет редко применяться по отношению к сведениям в Интернете.

Любое расширение рамок деликта присвоения должно быть согласовано с конкурирующей потребностью в разрешении законного сбора новостей и распространения информации. Деликт должен применяться только тогда, когда фотографии или иная личная информация используются каким-либо способом, не связанным с общественными интересами, но этот критерий неизбежно станет предметом затяжных юридических дискуссий.

Присвоение — не единственное нарушение приватности, относящееся к общему праву, которое требует пересмотра в целях приведения в большее соответствие с реалиями сетевых коммуникаций. У нас уже есть много правовых инструментов для защиты частной сферы, но сегодня они «стреножены» концепциями приватности, которые не позволяют им работать эффективно. Расширение формулировки закона требует учета случаев сомнительного использования личной информации — как в случае со *Star Wars Kid* или службой *Beacon* сайта *Facebook*.

Было бы лучше, если такие споры разрешались бы без обращения в суд, но широкое распространение электронных сетей может потребовать изменений в общем праве. Угроза частной сфере огромна, и люди начинают понимать, насколько сильно они ценят охрану приватности как свое фундаментальное право. В связи с этим общество должно разработать новое и более тонкое понимание общественной и частной жизни, понимание, учитывающее тот факт, что доступным становится все большее количество личной информации, но подразумевающее защиту возможности некоторого выбора в вопросе о том, как эта информация распространяется и коллективно используется. ■

Перевод: И.Е. Сацевич

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

- Privacy and Freedom. Alan Westin. Atheneum, 1967.
- Philosophical Dimensions of Privacy: An Anthology. Ferdinand Schoeman. Cambridge University Press, 1984.
- The future of Reputation: Gossip, Rumor, and Privacy on the Internet. Daniel J. Solove. Yale University Press, 2007.

Сухие краски

Марк Фишетти

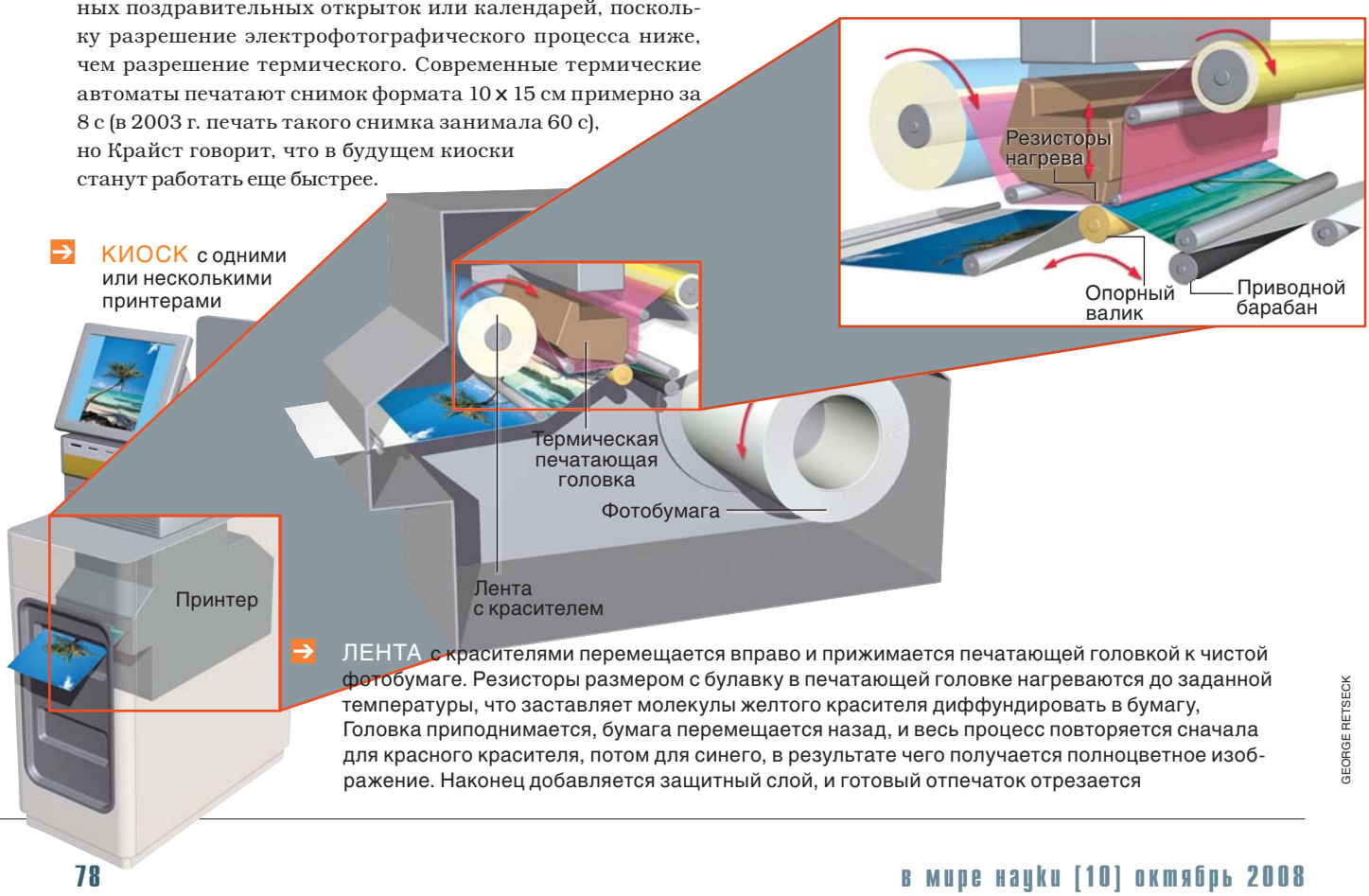
Все более широкое распространение цифровых фотоаппаратов вызвало к жизни целую новую отрасль: моментальной печати фотоснимков. Фотограф-любитель приносит карту памяти своей камеры в магазин, вставляет в гнездо киоска, отмечает нужные снимки, и через несколько секунд отпечатки выпадают в лоток. Такие автоматы можно найти повсюду. «За пять лет число цифровых киосков в мире возросло до 85 тыс., — говорит директор по термическим системам компании *Eastman Kodak* Чарлз Крайст-младший (Charles S. Christ Jr.).

В основе работы принтеров лежит «сухой» процесс, называемый термическим переносом красителей (в отличие от традиционного «мокрого» процесса с погружением экспонированных фотоматериалов в водные растворы химикатов). Когда фотобумага проходит мимо печатающей головки, выстроенные в ряд миниатюрные резисторы, независимо нагреваемые до определенных температур, переносят на нее с ленты малые количества желтого, красного и синего красителей. Сочетания точек этих цветов образуют элементы цветного изображения — пиксели (*илл. внизу*).

Более крупные автоматы в универмагах работают и на основе процессов электрофотографии, но используются в основном для двусторонней печати, например заказных поздравительных открыток или календарей, поскольку разрешение электрофотографического процесса ниже, чем разрешение термического. Современные термические автоматы печатают снимок формата 10 x 15 см примерно за 8 с (в 2003 г. печать такого снимка занимала 60 с), но Крайст говорит, что в будущем киоски станут работать еще быстрее.

Использование «сухого» процесса способствует возвращению моды на моментальное фотографирование. В июле 2008 г. компания *Polaroid* выпустила карманный моментальный принтер *PoGo*, позволяющий печатать снимки, сделанные цифровым фотоаппаратом, в формате 51 x 76 мм, используя для этого канал *Bluetooth* или *USB*-кабель. А новая компания *Zink Imaging* разработала технологию на основе химического процесса, изобретенного Стивеном Телфером (Stephen Telfer), сегодня занимающим в компании должность старшего исследователя.

В этой системе в фотобумагу заделываются бесцветные кристаллы. При нагреве резисторами до определенной температуры они становятся желтыми, красными или синими (*илл. на стр. напротив*). *PoGo* делает отпечаток за 60 с, питается от батареек и может использоваться во всех тех ситуациях, в которых использовались фотоаппараты *Polaroid*: на вечеринках, в отпуске, на мероприятиях компании и др. Первые образцы *PoGo* стоят около $150, а комплект из 30 листов бумаги — около $10. Телфер говорит, что уже существуют опытные образцы, печатающие снимки большего формата, и поскольку чернил в них нет, их можно встраивать, например, в телевизоры, чтобы получать снимки изображений с экрана. ■

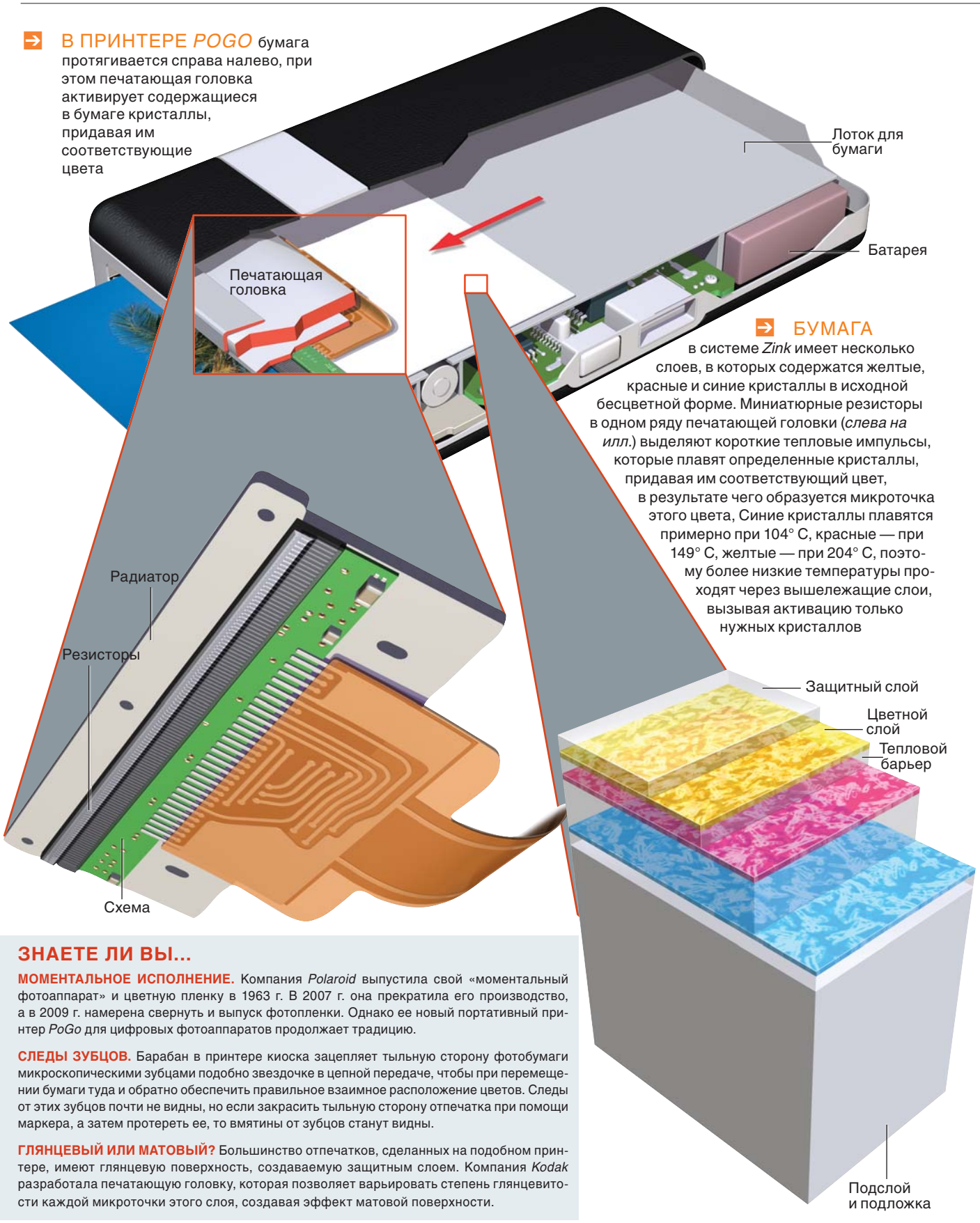


КИОСК с одними или несколькими принтерами

ЛЕНТА с красителями перемещается вправо и прижимается печатающей головкой к чистой фотобумаге. Резисторы размером с булавку в печатающей головке нагреваются до заданной температуры, что заставляет молекулы желтого красителя диффундировать в бумагу, Головка приподнимается, бумага перемещается назад, и весь процесс повторяется сначала для красного красителя, потом для синего, в результате чего получается полноцветное изображение. Наконец добавляется защитный слой, и готовый отпечаток отрезается

GEORGE RETSECK

В ПРИНТЕРЕ *POGO* бумага протягивается справа налево, при этом печатающая головка активирует содержащиеся в бумаге кристаллы, придавая им соответствующие цвета



БУМАГА в системе *Zink* имеет несколько слоев, в которых содержатся желтые, красные и синие кристаллы в исходной бесцветной форме. Миниатюрные резисторы в одном ряду печатающей головки (*слева на илл.*) выделяют короткие тепловые импульсы, которые плавят определенные кристаллы, придавая им соответствующий цвет, в результате чего образуется микроточка этого цвета, Синие кристаллы плавятся примерно при 104° С, красные — при 149° С, желтые — при 204° С, поэтому более низкие температуры проходят через вышележащие слои, вызывая активацию только нужных кристаллов

ЗНАЕТЕ ЛИ ВЫ...

МОМЕНТАЛЬНОЕ ИСПОЛНЕНИЕ. Компания *Polaroid* выпустила свой «моментальный фотоаппарат» и цветную пленку в 1963 г. В 2007 г. она прекратила его производство, а в 2009 г. намерена свернуть и выпуск фотопленки. Однако ее новый портативный принтер *PoGo* для цифровых фотоаппаратов продолжает традицию.

СЛЕДЫ ЗУБЦОВ. Барабан в принтере киоска зацепляет тыльную сторону фотобумаги микроскопическими зубцами подобно звездочке в цепной передаче, чтобы при перемещении бумаги туда и обратно обеспечить правильное взаимное расположение цветов. Следы от этих зубцов почти не видны, но если закрасить тыльную сторону отпечатка при помощи маркера, а затем протереть ее, то вмятины от зубцов станут видны.

ГЛЯНЦЕВЫЙ ИЛИ МАТОВЫЙ? Большинство отпечатков, сделанных на подобном принтере, имеют глянцевую поверхность, создаваемую защитным слоем. Компания *Kodak* разработала печатающую головку, которая позволяет варьировать степень глянцевитости каждой микроточки этого слоя, создавая эффект матовой поверхности.

Геннадий Аветов, Александр Аствацатуров,
Григорий Двоскин и Алексей Старостин

УТИЛИЗАЦИЯ ОТХОДОВ, СОДЕРЖАЩИХ радиоактивные компоненты

Проблема утилизации содержащих радиоактивные компоненты отходов, образующихся в ходе технологических процессов, связанных с расщепляющимися материалами (спецодежда, респираторы, ткань ПХВ, фильтры Петрянова, обтирочный материал, перчатки, пластикат, резина и т.п.), является весьма актуальной. Дело в том, что утилизация таких отходов возможна только на специализированных предприятиях. Но даже на крупных производствах ядерной энергетики количество ежедневно образующихся опасных отходов не превышает нескольких сотен килограммов, а поскольку обращение с этими материалами требует соблюдения особых условий, их транспортировка малыми партиями нецелесообразна. Отходы приходится накапливать, что требует оборудования и содержания специальных хранилищ. Все это в совокупности с высокой стоимостью утилизации предполагает большие материальные затраты. Поэтому уже сейчас оптимальным решением проблемы должно стать наличие устройств, позволяющих экологически безопасно утилизировать подобные материалы непосредственно в местах их образования.

Сегодня наиболее распространенным методом утилизации твердых радиоактивных отходов (ТРАО) является их термическое уничтожение. Но сжигание даже обычных отходов требует особой организации процессов горения и последующей очистки дымовых газов, т.к. в противном случае в атмосферу выбрасывается целая гамма вредных веществ, что совершенно недопустимо при обращении с радиоактивными материалами. Для уменьшения или даже предотвращения возможности образования таких продуктов необходима соответствующая организация технологического процесса.

В общем случае для достижения полноты сгорания вредных компонентов необходимо обеспечить следующие основные условия:

- избыток окислителя (> 1,2);
- качественное смешение парогазовой смеси с горячим окислителем;
- высокую температуру процесса горения (> 1200° С);
- достаточно продолжительное время нахождения продуктов в зоне высоких температур (> 2 с).

Проблема решается при использовании технологии ЭЧУТО (экологически чистое уничтожение твердых отходов), предусматривающей непрямое, двухступенчатое сжигание отходов, включающее их предварительное бескислородное термическое разложение (среднетемпературный пиролиз с максимально возможным переводом органической составляющей исходного материала в газообразное состояние), последующее квалифицированное сжигание газообразных продуктов в оптимальных условиях (с использованием выделяющегося тепла на поддержание процесса) и дожиг коксового остатка.

Принципиальные положительные особенности применения ЭЧУТО для уничтожения органических материалов, в том числе и хлорсодержащих:

- управляемое сжигание при высокой температуре концентрированной неразбавленной парогазовой смеси (теплота сгорания — 6680–10450 кДж/м^3), что позволяет обеспечить высокую (1200–1300° С) температуру факела;
- выделяющийся при пиролизе хлорсодержащих материалов активный хлор уже в камере термического разложения реагирует с водородом, образуя стойкое соединение *HCl*, которое далее легко нейтрализуется на стадии доочистки: тем самым предотвращается образование диоксинов и фуранов;
- обеспечивается обязательное огневое обезвреживание продуктов, что в сочетании с дополнительны-

ОБ АВТОРАХ

Геннадий Артемович Аветов — сотрудник ООО «ВП-Сервис».
Александр Георгиевич Аствацатуров — кандидат технических наук.
Григорий Исакович Двоскин — кандидат технических наук, старший научный сотрудник.
Алексей Дмитриевич Старостин — кандидат технических наук, старший научный сотрудник.

ми очистными устройствами гарантирует экологически чистое уничтожение отходов.

На предприятии МСЗ «Элемаш» с августа 2003 г. находится в эксплуатации типовая установка ЭЧУТО-150.03, выпускаемая ООО «ВП-Сервис» и модернизированная под условия предприятия.

Установка включает термореактор, фильтр каталитического дожига, теплообменник, циклон, скруббер, узел выгрузки коксозольного остатка.

В результате эксплуатации установки были сделаны следующие выводы:

- термическое разложение (пиролиз) отходов в бескислородной атмосфере позволяет перевести основную массу содержащейся в отходах органики в газообразное состояние, оставляя тем самым основное количество радиоактивных компонентов в коксозольном остатке;
- работа всей технологической цепочки под разрежением, создаваемым дымососом, расположенным на выходе из установки, обеспечивает невозможность выхода радиоактивных компонентов в атмосферу в ходе технологического процесса;
- повторный пиролиз шлама и дожиг коксового остатка позволяют сконцентрировать в коксозольном остатке основную часть исходной радиоактивности отходов.

Одним из существенных эксплуатационных недостатков установки оказалась ее небольшая производительность (~ 5–12 кг/ч). Это объясняется тем, что данная типовая установка ЭЧУТО рассчитана на переработку бытовых отходов с низкой калорийностью (~2500 ккал/кг), а вышеперечисленные отходы предприятия значительно более калорийны — (8–10 тыс. ккал/кг).

Установка ЭЧУТО-150.03

После того как в ходе многолетней эксплуатации пилотной установки была подтверждена пригодность предложенной технологии для эффективной утилизации ТРАО и ее экологическая безопасность, ООО «ВП-Сервис» и ОАО «Элемаш» совместно осуществили разработку, изготовление, пуско-наладочные работы и освоение аналогичной установки большей производительности.

Установка, получившая название «ПИТОН» (Печь-Инсинератор для утилизации Твердых Отходов Непрерывного действия), предназначена для утилизации технологических оборотов уранового производства обогащением менее 5% по урану $U235$.

При проектировании установки были учтены конструктивные и технологические недостатки, выявленные в ходе эксплуатации пилотной установки. В частности:

- предусмотрена непрерывная выгрузка шнеком зольного остатка из камеры дожига, что особенно важно при сжигании ТРАО;
- в конструкции установки использованы коррозионно- и жаростойкие материалы (титан вместо обычной низкоуглеродистой стали), что увеличивает срок эксплуатации печи;
- предусмотрена принудительная подача воздуха в циклонную топку;
- установлена дополнительная горелка для сокращения времени разогрева при пуске из холодного состояния.

В настоящее время установка находится в опытной эксплуатации. ■

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ УСТАНОВКИ «ПИТОН»

Режим загрузки установки — цикличный.
Продолжительность цикла — 15–20 минут.
Производительность (в зависимости от калорийности отходов) — 10–20 кг/ч.
Разовая загрузка — 3–8 кг оборотов.
Выход коксозольного остатка — 1–2 кг/ч.
Обслуживающий персонал, оператор — 1 чел. в смену.
Класс безопасности по ОПБ ОЯТЦ-НП-01620 — 4.
Первичный источник тепловой энергии — сжигание дизельного топлива.
Расход дизельного топлива — 2–5 кг/ч.
Габаритные размеры установки: — длина — 6,95 м, ширина — 4,35 м, высота — 7,00 м.
Установленная мощность — 5 кВт.

Это будет интересно всем

Вниманию читателей предлагается учебник по истории искусствознания. В нем рассматривается развитие теории изобразительного искусства, архитектуры, музыки и драмы от античности до XX в. Книга содержит списки рекомендованной литературы и темы для письменных занятий. Это единственное в отечественной литературе пособие для тех, кто изучает историю искусства и культуры.

Издание предназначено в первую очередь для студентов и преподавателей художественных и гуманитарных вузов. Оно будет также полезно широкому кругу читателей, интересующихся историей искусства.

Шестаков В.П. История истории искусства: От Плиния до наших дней. М.: Издательство ЛКИ, 2008.

Неожиданно просто

Книга раскрывает существо многих математических идей и представляет собой новый шаг в области популяризации науки. Неожиданно просто и коротко передается смысл фундаментальных результатов, сложные факты изложены понятно для широкого круга читателей.

Рекомендуется в первую очередь студентам и преподавателям, инженерам и научным работникам, а также старшеклассникам.

Босс В. Интуиция и математика. 3-е изд., испр. и доп. Серия: Лекции по математике В. Босса. М.: Издательство ЛКИ, 2008.

Лекции по математике

Книга посвящена теории сложности алгоритмов в той ее части, где речь идет о противостоянии *P*- и *NP*-задач. В резонанс с проблемой «*P* против *NP*» входит обширная тематика: комбинаторные задачи на графах, неразрешимые проблемы теории алгоритмов, криптография, целочисленное программирование, вероятностные методы, квантовые вычисления, алгоритмы Хачияна и Кармаркара для линейного программирования, а также полиномиальный алгоритм *AKS* для выяснения простоты числа.

Издание рекомендуется студентам, преподавателям, инженерам и научным работникам.

Босс В. Лекции по математике: Перебор и эффективные алгоритмы. Т.10. Серия: Лекции по математике В. Босса. М.: Издательство ЛКИ, 2008.

Лечимся от алкоголизма и табакокурения

В настоящей книге приводится описание лекарственных растений и грибов, применяемых в научной и традиционной (народной) медицине для терапии алкоголизма и табакокурения, а также растений, входящих в состав применяемых в наркологии лекарственных средств, биологически активных добавок к пище и специализированных продуктов питания.

В издании рассмотрены результаты экспериментальных и клинических исследований лекарственных растений и извлекаемых из них соединений, дается описание содержащих лекарственные растения или их экстракты аллопатических и гомеопатических лекарственных средств, которые предназначены для лечения алкоголизма, табакокурения и опийной наркомании.

Книга может быть рекомендована врачам — психиатрам, наркологам, фитотерапевтам, фармакологам, фармакогностам, преподавателям и студентам медицинских вузов.

Нужный В.П., Рожанец В.В., Ефремов А.П. Лекарственные растения и фитокомпозиции в наркологии. М.: КомКнига, 2006.

Когнитивный подход к метафоре

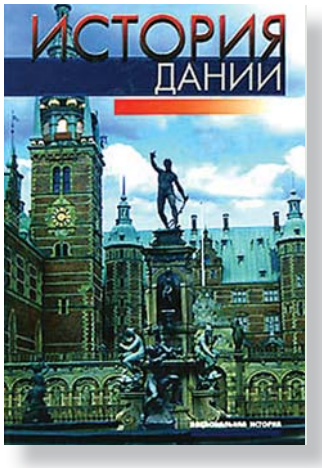
В книге Дж. Лакоффа и М. Джонсона «Метафоры, которыми мы живем» излагаются основы когнитивного подхода к метафоре как феномену языка, сознания и культуры. Обсуждаются как научные аспекты изучения этого явления в лингвистике и философии, так и роль метафоры в современном обществе, в повседневном общении между людьми. Особое внимание обращается на возможности использования метафоры как средства познания действительности, инструмента организации опыта человека, структурирования его знаний о действительности.

Книга, впервые вышедшая на языке оригинала в 1980 г., стала бестселлером в англоязычных странах и получила широкий отклик в научной периодике и публицистике.

Издание почти не содержит специальной терминологии и будет интересно как специалистам в области лингвистики и литературоведения, так и широким кругам читателей, интересующихся функционированием языка в современном обществе, проблемами речевого воздействия и связью между языком, мышлением и сознанием.

Лакофф Дж., Джонсон М. Метафоры, которыми мы живем. Пер. с англ. 2-е изд. М.: Издательство ЛКИ, 2008 (George Lakoff, Mark Johnson. Metaphors We Live By).

Материалы предоставлены интернет-магазином научной книги www.URSS.ru



История Дании / Палудан Х. и др. М.: Весь мир, 2007.

Первая книга в России об истории Дании

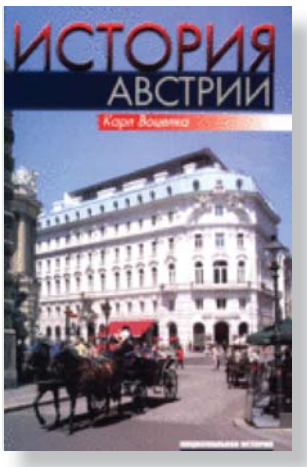
История Дании, написанная датскими исследователями и изданная в переводе, появилась в России впервые. Книга представляет собой коллективный труд ведущих датских историков. Здесь рассмотрены основные этапы становления государственности, конфликты церковной власти и монархии, вопросы социально-экономического развития и различные аспекты внешней политики страны.

История изложена от времен Великого переселения народов, через Реформацию и абсолютизм к индустриализации и развитию капиталистических отношений, к новым задачам наступившего тысячелетия. Обсуждается тенденция неолиберализма, проявившаяся в стимулировании частной предпринимательской деятельности. Рассмотрена современная ситуация сотрудничества в рамках Европейского Союза, проблемы интеграции и усиливающегося внешнего давления на страну. Особое внимание уделено культуре датского народа и формированию его национальной идентичности, интерес к сохранению которой возрос в связи с притоком беженцев и мигрантов в конце прошлого века. Эта книга будет полезна как профессионалам — тем, кто занимается историей и международной политикой, так и широкому кругу читателей — тем, кто, отправляясь в зарубежную поездку, хочет больше узнать о новой для себя стране.

История Австрии с древнейших времен

Эта книга продолжает серию «Национальная история», написанную исследователями тех стран, для которых это их собственная, отечественная история. Данное издание появилось в результате работы автора со студентами Венского университета и его преподавательской деятельности в рамках ряда образовательных программ и курсов по подготовке экскурсоводов. В книге изложена история австрийских земель с древнейших времен до наших дней. Их развитие рассматривается в сложном контексте исторических судеб средневековой Германии, Священной Римской империи и Европы в целом. В поле зрения автора — становление комплекса наследных земель династии Габсбургов на немецком Юго-Востоке, их место в Европе Средних веков и раннего Нового времени, образование и крушение Австро-Венгрии, трагическая судьба Первой республики и политическая жизнь Второй республики. Особое внимание уделено вопросам социальной и гендерной истории, рассмотрены индустриализация и ее последствия для страны, роль женщины в индустриальном обществе. Автор прослеживает основные тенденции в области культуры, упоминая такие имена, как Гайдн, Моцарт, Штраус, Малер. Именно в Австрии, где вальс развился как самобытный музыкальный жанр, ставший символом австрийской музыкальной культуры, особенно ценились выразительность и мелодичность.

В конце обзора изложен взгляд автора на место истории страны в сегодняшнем мире и сценарии будущего развития, отражено скептическое отношение автора к современной модели прогресса, включающей противостояние богатства и бедности, радикализацию правых с их враждебностью ко всему чужому, мощное влияние телевидения, противоречивое влияние туризма на экономику и культурное равновесие.



Воцелка К. История Австрии. Культура, общество, политика. М.: Весь мир, 2007.

Актуальность биобезопасности

Проблема биобезопасности с каждым годом становится все острее. Во многом это следствие развития науки и техники, имеющее не только позитивные стороны. Все новшества, внедряемые в любую сферу человеческой деятельности, должны проходить всесторонний контроль, не наносить ущерба окружающей среде и здоровью человека. Остро стоит и проблема биотерроризма. Эти вопросы поднимались на международной конференции «Наука и образование для целей безопасности», которая прошла в начале октября в Биологическом центре РАН г. Пущино.

Идея проведения подобного мероприятия возникла еще год назад на конференции, посвященной нанобиотехнологиям, и воплотилась благодаря усилиям организаторов: Исследовательского центра «БиоРесурсы и экология», Института биохимии и физиологии микроорганизмов им. Г.К. Скрябина РАН, Пущинского государственного университета и ряда других научных организаций и ведомств России при поддержке международных организаций и фондов.

Тематика докладов, представленных на конференции, отличалась большим разнообразием: от биотерроризма как такового до вопросов защиты здоровья, продуктов питания и окружающей среды, этических проблем, образования в сфере биобезопасности.

Большой интерес вызвало выступление директора Института теоретической и экспериментальной биофизики РАН, члена-корреспондента РАН Г.Р. Иваницкого, который рассказал об использовании нанотехнологий в биомедицине. Сегодня во всем мире, в том числе и в России, развитию таких технологий уделяют большое внимание, но не всегда разработки в области малых величин безобидны. И прежде чем внедрять ставшие модными изобретения в медицину, нужно тщательно изучить все риски вмешательства в организм на наноуровне.

Доклад генерального директора НПО «Поток-Интер» А.В. Наголкина был посвящен созданной в его компании установке по обеззараживанию воздуха в закрытых помещениях (самолетах, купе вагонов дальнего следования), а также там, где имеются особые требования к стерильности (например, в хирургических боксах). Аппараты компании были установлены на международной космической станции «Мир», «Шаттлах», в российских и зарубежных медицинских учреждениях. Установка по обеззараживанию не имеет аналогов в мире: болезнетворные микроорганизмы в ней не фильтруются, а уничтожаются за счет особых физических воздействий.

Ряд докладов был посвящен проблеме борьбы с биотерроризмом. Эта проблема подразумевает не только биологическое оружие. Например, директор Всероссийского научно-исследовательского института биологической защиты растений доктор В.Д. Надыкта рассказал о превентивных мерах противодействия агро- и фитотерроризму. Старший научный сотрудник Института клинической иммунологии СО РАМН А.А. Чепурнов говорил о том, возможно ли изготовить препараты для актов биотерроризма в бытовых условиях и как этому противодей-ствовать.

Как сообщила В.А. Дмитриева, руководитель Исследовательского центра «БиоРесурсы и экология» (некоммерческой организации, грантополучателя и инициатора проведенного мероприятия), одним из главных результатов конференции станет одобренная участниками программа по созданию на базе центра «БиоРесурсы и экология», Пущинского университета и Калифорнийского университета в Риверсайде онлайн-школы по биобезопасности. Кстати, выпускники первой школы уже в 2009 г. получат дипломы о дополнительном образовании, выданные этими тремя организациями. ■

Фирюза Янчилина
Фото автора

Школьные библиотеки — на повестке дня

В Московском Доме Журналиста состоялась пресс-конференция, посвященная открытию месячника школьных библиотек в России. Участниками события стали Т.В. Бокова, заместитель исполнительного директора фонда «Русский мир», В.А. Александров, начальник Департамента полномочного представителя Президента РФ в Центральном федеральном округе, Т.Д. Жукова, президент Русской школьной библиотечной ассоциации, и И.А. Панкеев, профессор МГУ.

По инициативе Международной ассоциации школьных библиотек (*International Association of School Librarianship, IASL*) с 1 по 30 октября во многих странах мира прошли такие съезды. Задача российских съездов состояла в освещении деятельности школьных библиотек, их проектов и ресурсов.

В некоторых регионах России школьная библиотека — по сути единственный культурный центр, поэтому необходимо поддержать библиотечных работников, которые оказывают существенное воздействие на формирование личности ученика. Особенно актуально эта проблема стоит в связи с распространением Интернета и ускорением темпа жизни. Однако ошибочно считать интернет-ресурсы негативным фактором развития современного школьника. По словам И.А. Панкеева, книгой сейчас можно считать любые способ и средство приобретения знаний. Гораздо более серьезная проблема — то, что сейчас все реже читают само литературное произведение, предпочитая краткий пересказ. Особенно печально, что данные международных исследований *PISA* по интересу к чтению показывают лишь 40-е место наших школьников.

Правительство РФ старается делать все возможное для того, чтобы поддержать интерес детей к литературе в целом и русской литературе в частности. Так, в 2007 г. по указу Президента РФ была создана некоммерческая организация «Русский мир», в задачу которой входит поддержание русскоязычной литературы.

С созданием этой организации поступило много запросов из самых разных уголков планеты. Сейчас уже помимо России создано 10 таких центров в странах СНГ, среди которых Армения, Киргизия, Казахстан; планируется создать их в Америке и даже в Гватемале. Такой мощный отклик еще больше вдохновляет руководителей этой организации участвовать в Месячнике школьных библиотек, предоставляя растущему количеству детей из разных стран возможность не забывать русский язык, быть грамотными и больше читать как современную, так и классическую литературу и, следовательно, вернуть должность библиотекаря в ранг уважаемых профессий. ■

Анна Кадырова
Фото автора

Будущее российской кардиологии

В ИА ИТАР-ТАСС прошла пресс-конференция, посвященная учреждению в России национальной премии в области кардиологии «Пурпурное сердце». Главными участниками события стали президент Всероссийского научного общества кардиологов Р.Г. Оганов, президент Российского медицинского общества по артериальной гипертонии И.Е. Чазова, генеральный директор российского представительства ОАО «Фармацевтический завод ЭГИС» (Венгрия) Л. Почайи (L. Pocsaji), а также координатор премии от Национального агентства маркетинговых информационных технологий (НАМИТ) О.Г. Жигунова.

По данным Всероссийского научного общества кардиологов, статистика смертности от инфарктов и инсультов в России в три раза превышает среднеевропейские показатели. Как подчеркнул Р.Г. Оганов, если заболеваемость будет оставаться на прежнем уровне, лишь половина из рожденных сегодня мальчиков доживет до 60 лет. Поэтому для государственных органов здравоохранения решение проблемы заболеваемости и лечения сердечно-сосудистых заболеваний сегодня является одной из главных задач.

В этой связи появление в России премии, направленной на поддержку специалистов в области сердечно-сосудистых заболеваний, представляется особенно своевременным. В ходе ее организации и проведения молодые специалисты получат возможность общаться внутри своего сообщества, а также наладить контакты с выдающимися специалистами в области кардиологии. В процессе реализации проекта будут реализованы информационно-образовательные мероприятия, благодаря которым участники смогут первыми получать информацию о новейших исследованиях, технологиях и методах лечения сердечно-сосудистых заболеваний. Им будет предоставлена возможность участвовать в ведущих научных форумах и конгрессах наряду с мэтрами российской кардиологии.

Учредителем премии стало агентство НАМИТ, реализующее социальные проекты в сотрудничестве с широким кругом как государственных и общественных, так и коммерческих организаций.

Премия «Пурпурное сердце» будет вручаться в следующих номинациях: «Гордость российской кардиологии» (подноминации: «Лучший врач-терапевт года», «Лучший врач-кардиолог года»), «Будущее российской кардиологии», «Лучший кардиологический проект года» (подноминации: «Социальный проект года», «Образовательный проект года», «Научный проект года»), «Медицинское учреждение года» (подноминации: «Лучшее лечебно-профилактическое учреждение России», «Лучшее образовательное учреждение России»), а также «Мэтр кардиологии». По-следняя вручается претенденту, который выдвигается экспертным советом премии (ознакомиться с более подробной информацией, а также подать заявку на участие можно на официальном сайте премии www.purpleheart.ru)

Участником премии может стать любое физическое или юридическое лицо, специализирующееся на профессиональной деятельности в области кардиологии, независимо от формы собственности, специфики деятельности и географического местоположения.

Президиум экспертного совета премии представлен такими значимыми фигурами отечественной кардиологии, как Р.Г. Оганов (председатель экспертного совета) и И.Е. Чазова (главный эксперт). Кроме того, в совет войдут ведущие специалисты в области сердечно-сосудистых заболеваний, представители государственных образовательных и здравоохранительных систем.

Председателем попечительского совета премии стал доктор Л. Почайи, генеральный директор компании «Эгис», менеджер, вошедший в 2007 г. в топ-1000 самых профессиональных менеджеров РФ. В ходе стартовой пресс-конференции он подчеркнул, что главная задача организаторов — работа с претендентами, поскольку для каждого из них участие в проекте может быть единственной и потому уникальной возможностью продемонстрировать свои знания, опыт, наработки перед ведущими специалистами в области кардиологии. В арсенале организаторов премии — обширная региональная сеть, состоящая из более чем 300 представителей: специалистов, научных и лечебных учреждений. Налажена связь между медиками из центра и самых отдаленных субъектов Российской Фе-

дерации. Поэтому возможности, которые дает участникам премия, — это прежде всего шанс проявить себя, получить полезную информацию и наладить контакт с коллегами. Участники пресс-конференции выразили единое мнение, что появление новой премии «Пурпурное сердце» привлечет внимание к профессии врача-кардиолога, ускорит развитие передовых методов диагностики, профилактики и лечения сердечно-сосудистых заболеваний. Все эти меры должны приблизить главную цель организаторов — повышение продолжительности и качества жизни россиян. ■

Анна Кадырова

Социология и политика в России

В Москве прошел III Всероссийский социологический конгресс «Социология и общество: проблемы и пути взаимодействия». Директор Института социально-политических исследований РАН, академик Г.В. Осипов сообщил, что на конгресс подали более 2 тыс. тезисов, а участниками стали более тысячи социологов. Основные проблемы, обсуждавшиеся российскими социологами и иностранными участниками: «Проблемы теории в мировой и российской социологии», «Россия в глобализационных процессах», «Россия и страны европейского сообщества», «Методология социологических исследований: вечные проблемы и новые подходы», «Инновации в социологическом образовании» и многие другие. Важным было участие в конгрессе студентов и молодых ученых, состоялся обмен мнениями между представителями различных регионов и научных школ. Показательны с точки зрения синтеза теории и практики темы круглых столов: «Социологические журналы: главные редакторы, авторы и читатели», «Использование времени и повседневная деятельность», «Реформация трудовых отношений: проблемы и перспективы действий», «Цивилизация в точке бифуркации: социология трансформирующегося общества», «Социология и литература», и т.д. В организации мероприятия приняли участие Институт социологии РАН и Институт социально-политических исследований РАН. Соорганизаторами конгресса выступили Государственный университет — Высшая школа экономики (ГУ ВШЭ), Российское общество социологов (РОС), а также Российский государственный социальный университет, МГУ, Сообщество профессиональных социологов и многие другие сообщества. Принципиальной проблемой для социологии остается выбор стратегии развития — сосредоточенность лишь на объективном отражении социальной действительности или активное влияние на различные стороны жизни общества. Президент Международной социологической ассоциации Мишель Вивьерка считает, что социолог может быть полезен, когда занимается политикой, и исторические примеры это подтверждают, но образ социолога и социологии должен дополняться специалистом вне политики. Руководитель Администрации Президента РФ С.Е. Нарышкин, вспомнив события в Южной Осетии и противоречивую реакцию на них, настоящую борьбу в СМИ, подчеркнул, что социально-политические знания способны не только диагностировать, но и влиять на социальное и политико-информационное пространство, а готовность к информационному противостоянию, к отстаиванию российских позиций в международном идейном пространстве зависит от развития социологической науки и практики.

Социологическое сообщество в России в 2008 г. отмечает две значимые юбилейные даты: 50-летие создания первой в стране социологической ассоциации — Советской социологической ассоциации (ССА) и 40-летие учреждения первого в стране социологического института — Института конкретных социальных исследований (ИКСИ АН СССР, сейчас Институт социологии РАН). Организаторы конференции отмечают, что данные ключевые для отечественной социологии события знаменовали возрождение в стране социологической науки после нескольких десятилетий запрета. Приветствие участникам конгресса направил Президент РФ Д.А. Медведев: «Сегодня социологическая наука динамично развивается и оказывает заметное влияние на общественно-политическую жизнь России, содействует решению ключевых социально-экономических проблем. Отрадно, что год от года растет число специалистов в этой области знания, идут плодотворные профессиональные дискуссии и обмен накопленным опытом. Вам предстоит всесторонне обсудить актуальные задачи, стоящие перед современной социологией. В их числе новые методы исследований, пути повышения качества социологического образования, более эффективный мониторинг общественного мнения».

В то же время многие социологи обращали особое внимание на важность независимой от власти социологической экспертизы, на совершенствование оценок протестных выступлений, методик проведения опросов общественного мнения и т.д. Попытки отделить социологию от политики были не всегда успешными, тем более в России, где социальному развитию мешают проблемы бедности и социального неравенства. Судя по итогам конгресса, социология становится все более междисциплинарной и объективно все более связанной с политикой и идеологией. ■

Дмитрий Мисюров

В № 9 нашего журнала была допущена ошибка. В материале «Нано на НТТМ» (автор — Леонид Раткин) неверно указаны инициалы одного из участников творческого коллектива с кафедры химии и технологии биологически активных соединений им. Н.А. Преображенского Московской государственной академии тонкой химической технологии им. М.В. Ломоносова — Д.И. Бриттала. Кроме того, недостаточно корректно сформулирована суть проблемы, которой занимается творческий коллектив. Исследователи разрабатывают и синтезируют соединения, которые впоследствии могут быть использованы для применения в качестве агентов комбинированного действия для фотодинамической и борнейтронозахватной терапии. Редакция приносит свои извинения Д.И. Бриттalu и читателям.

Анатолий Гендин

С наступающим!

КАК ПРАВИЛЬНО ВЫПИТЬ И ГРАМОТНО ЗАКУСИТЬ

Радостная череда зимних праздников ежегодно скрашивает наши трудовые будни: католическое Рождество плавно переходит в Новый год, а там и православное Рождество со Старым Новым годом. Люди начитанные открывают сезон еще 6 декабря, когда вся Европа отмечает день св. Николауса, он же фактически Дед Мороз. А особо нетерпеливые начинают праздновать аж с 24 ноября: в этот день ровно за месяц до католического сочельника в пунктуальном немецкоязычном мире открываются предрождественские ярмарки

В странах с привычной для нас сезонной ориентацией в это время года снежно и морозно, так что первая забота радушного хозяина — дать гостям согреться с учетом национальных традиций. Скажем, в Ирландии популярен несложный рецепт рождественского горячего виски. Заранее нужно приготовить лимон — нарезать его кружочками, в каждую половинку воткнуть пару-тройку гвоздичек — и нагреть стаканы, сполоснув их горячей водой. Затем налить в них кипяток (объем — по вкусу), растворить в нем две чайные ложки сахара, добавить кусочек лимона с гвоздиками и долить виски до желаемой крепости. Подавать стакан в салфетке — должно быть горячо.

Способ приготовления старинного шотландского напитка «атолл броуз» также несложен и вполне демократичен. Для этого понадобятся всего три составные части: три столовые ложки овсяной муки, две столовые ложки верескового меда и произвольный объем виски. Нужно замесить на воде жидкое тесто и дать ему постоять полчаса, затем процедить и тщательно отжать гущу. В полученную жидкость добавить мед и хорошенько перемешать до однородного состояния, перелить в бутылку желаемой емкости, добавить виски по вкусу и плотно закрыть пробкой. Перед употреблением обязательно хорошо взболтать. С бутылкой этого замечательного напитка шотландские мужчины в новогоднюю ночь отправляются к соседям — поздравить и выпить за удачу в наступающем году. Кстати, об удаче: первым в новом году порог каждого шотландского дома должен пересечь брюнет, это как раз и гарантирует всяческое благополучие на ближайшие 12 месяцев. Если рыжий или (не дай бог!) женщина — хорошего не жди.

Консервативные англичане очень уважают свой традиционный новогодний коктейль «эгног» (*egg-nog*): на дюжину яиц нужно взять литров пять жирного молока, два килограмма жирных сливок, два стакана сахара, стакан виски и стакан коньяка — как раз на небольшую компанию, в случае нужды все легко повторить. Эгног хорош тем, что каждый может легко довести его до нужных консистенции и вкуса, просто добавляя в свой стакан немного алкоголя. Любопытно, что этот же основательный напиток употребляют и в американской Луизиане, но под традиционную местную закуску — устрицы, которые как раз к зиме становятся особенно мясистыми и вкусными.

На любом рождественском базаре в Германии или Австрии обязательно будет «горячее вино» — глювайн (*Gluhwein*). Вот его классический рецепт: три стакана красного вина, одна столовая ложка рома, две столовые ложки сахара, немного корицы, три гвоздички, несколько кружочков апельсина или просто апельсиновых корок. Все смешать, сильно разогреть (но не кипятить!), процедить. Иногда вино разбавляют водой — до половины по объему. Употреблять глювайн следует горячим из кера-

Похож этот кубок на большой и приземистый заварочный чайник с несколькими носиками, через которые все собравшиеся и пьют по очереди фирменный региональный напиток под уклончивым названием «кофе по-вальдостански» (*caffe alla valdostana*). Очень горячий кофе в состав этого напитка действительно входит — наравне с граппой и красным вином, сахар и лимонную цедру добавляют по вкусу.

Похоже, что и традиционного новогоднего шампанского вам не из-

мической кружки, которая заодно согревает руки. Тем, кому удалось попробовать рождественский глювайн, смешанный аромат корицы и гвоздики всегда будет напоминать о новогодних радостях.

Еще один классический новогодний напиток — австрийский «ягате» (*Jaga-tee*), т.е. «охотничий чай». В состав этого легендарного коктейля действительно входит очень горячий черный чай, это половина объема, в оставшейся половине — три части рома, две части шнапса и одна часть красного вина. Еще нужно добавить лимон. Пьют «яга-те» также кружками. Этот, с позволения сказать, чай стал настолько популярен, что одним из лучших сувениров из Австрии считается бутылочка концентрата «ягате», которую можно купить в любом супермаркете. Достаточно к одной части концентрата добавить четыре части обычного кипятка и получается очень похоже на оригинал.

А североитальянский регион Валле д'Аоста славится своим согревающим средством, которое употребляют из особой деревянной посуды под названием «кубок дружбы».

бежать, хотя его и принято употреблять сильно охлажденным. Впрочем, это обстоятельство не останавливает даже любителей горнолыжного досуга: на модных альпийских курортах частокол пустых бутылок из-под самых дорогих марок шампанского вокруг высокогорных ресторанчиков — обычное дело.

Зарубежное рождественское застолье ассоциируется у нас в первую очередь с традиционным гусем с яблоками. Действительно, 25 декабря, на католическое Рождество, миллионы семей на всех континентах собираются на «гусиный ужин». Довольно часто гуся заменяет индейка; мясо у нее и нежное, и нежирное, что очень правильно с точки зрения диетологов.

ОБ АВТОРЕ

Анатолий Александрович Гендин — кандидат исторических наук, гастрономический журналист, писатель, автор серии гастрономических путеводителей «АТЛАС ГУРМАНА», директор информационного агентства «Локатор».

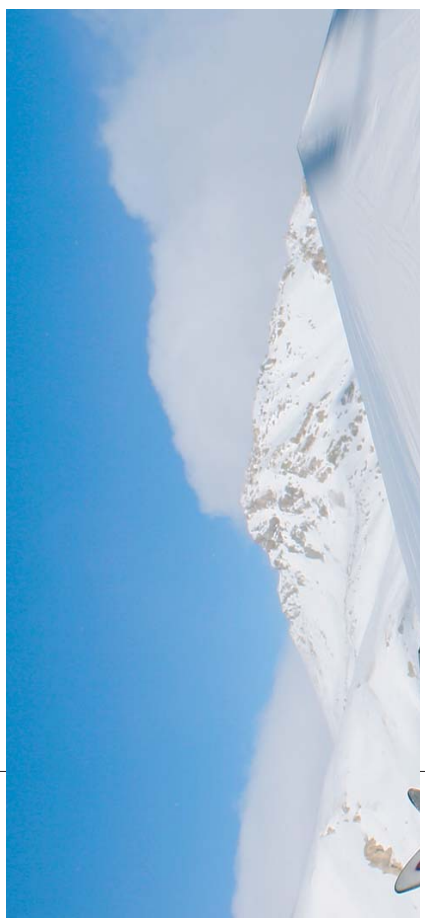
В разных странах эту птицу и готовят по-разному: фаршируют грибами, яйцами, рисом с луком-пореем, рубленой печенью птицы, черносливом, каштанами с беконом, орехами и много чем еще. Только неизменные яблоки не кладут внутрь, а запекают в мясном соке самой индейки и подают затем в качестве гарнира.

Ирландцы с англичанами подают индейку под клюквенным соусом, который готовится очень просто: на три части ягод нужно взять две части сахара и немного воды, довести смесь до кипения и подержать на слабом огне 5–10 минут. Хрустящий зажаренный картофель четвертушками или картофельное пюре и зеленая фасоль с беконом придадут вашему столу отчетливый британский акцент.

Французы готовят свою индейку в белом вине, что тоже вкусно. Они же рекомендуют в качестве новогодней закуски свою любимую фуа-гра — гусиную или утиную печень, особенно с сотерном, белым сладким вином. Впрочем, и во многих других странах белое вино добавляют в фарш для рождественской птицы, чтобы добиться более тонкого и изысканного вкуса. Греки обязательно добавляют белое вино в рисовую начинку с орехами, которой фаршируют индейку. А испанцы предпочитают перед готовкой подержать мясо в маринаде на основе сухого хереса с оливковым маслом и лимонным соком.

31 декабря в Европе отмечают как день св. Сильвестра, так что Новый год многие так и называют — Сильвестр. В этот день к ужину многие австрийцы готовят особое блюдо — «новогоднее» (Neujahrsessen). Это свиная голова с овощами, которая подается с хреном и чечевицей, причем все ингредиенты этого блюда имеют свое символическое значение: свиная голова обещает в новом году удачу, хрен — здоровье, а чечевица — денежное изобилие. А в Баварии в первый день Нового года принято есть свинину с кислой капустой как гарантию финансового процветания в предстоящем году. В центральноевропейской деревне к Рождеству традиционно закалывали специально откормленных свиней, так что и свежие колбасы, и прочие мясные деликатесы как раз поспевали к праздничному столу.

Есть у рождественского меню и еще один популярный раздел — рыбный. Считается, что именно рождественский карп приносит в семью счастье. Во многих европейских странах эту рыбу готовят в особой панировке на манер венского шницеля: сначала крупные куски карпа сбрызгивают лимонным соком и обваливают в муке, затем окунают в слегка взбитые яйца и снова обваливают, но на этот раз уже в сухарной крошке, после чего обжаривают во фритюре и подают с картофельным салатом и лимоном. Рождественского карпа можно и нафаршировать (например, шампиньонами), а потом потушить в пиве, в которое иногда еще добавляют немного меда. Независимо от способа приготовления голова карпа всегда достается главе семьи — в знак признания и уважения. А вот рыбная чешуя, положенная на Рождество в карман или бумажник, обещает финансовое благополучие на весь предстоящий год.



Некоторые популярные во всем мире кондитерские изделия тоже имеют очевидные рождественские корни. Скажем, распространенный в разных странах бисквитно-шоколадный рулет не зря делают в форме полена, а иногда «поленом» и называют: он символизирует реальное полено, которое медленно прогорает в очаге всю рождественскую ночь. Зола от него считалась когда-то лучшим лекарством от многих болезней. Для Германии характерна обильная и разнообразная праздничная выпечка: печенье с орешками или вставками из разноцветных засахаренных ягод и фруктов, живописные пряничные домики или съедобные сувениры вроде марципановых поросят в виде копилки, символизирующих будущее процветание. На сицилийском столе обязательно будут хрустящие трубочки-канноли с кремовой начинкой. А вот ближе к арабскому Востоку свои праздничные символы и приметы — например, гранат, многочисленными зернышками обещающий долголетие. ■

Почему органическое молоко хранится гораздо дольше обычного?

Отвечает профессор Пенсильванского университета, специалист по питанию животных Крейг Баумрукер (Craig Baumrucker)

Данное различие определяется не тем, является молоко органическим или нет; все дело в способе его обработки, направленной на увеличение срока хранения. Согласно требованиям Северо-Восточного альянса производителей органических продуктов (*NODPA*), органическое молоко должно оставаться свежим достаточно долго, поскольку его получают на ограниченном числе ферм, и проходит немало времени, пока оно попадает в магазин.

Молоко нагревают до 138° С и выдерживают в течение двух-четырех секунд. Такой процесс, называемый стерилизацией, отличается от пастеризации, которой подвергают обычное молоко. Существуют два способа пастеризации: в первом случае продукт выдерживают при относительно низкой (63° С) температуре в течение 30 минут, во втором — при относительно высокой (70° С) в течение 15 секунд.

Разницей в температуре обработки и объясняется более долгий срок хранения органического молока. При пастеризации, в отличие от стерилизации, уничтожаются не все бактерии, и вы рискуете получить желудочно-кишечное расстройство.

Обычный срок хранения пастеризованного молока после его доставки в магазин — четыре-шесть дней. Однако следует учесть, что до шести дней уходит на обработку и транспортировку, так что время от получения продукта до покупки может достигать двух недель. В отличие от пастеризованного молоко, прошедшее высокотемпературную обработку, хранится в упакованном виде при комнатной температуре до шести месяцев.

Обычное молоко, как и органическое, тоже можно стерилизовать. Почему же это делают не всегда? Дело в том, что при стерилизации разрушается часть содержащихся в молоке витаминов и повреждаются некоторые белки, отчего оно становится непригодным для изготовления сыров. Еще более существенным является изменение вкуса молока. У него появляется сладковатый привкус из-за карамелизации молочного сахара, а это нравится не всем. ■

Как долго после смерти человека в клетках продолжаются метаболические процессы?

Разобраться в этой таинственной истории пытается Арпад Васс (Arpad Vass), судебный антрополог из Ок-Риджской национальной лаборатории

По самым оптимистическим оценкам, клеточный метаболизм продолжается от четырех до десяти минут после смерти в зависимости от температуры среды, при которой находится тело.

Все это время никакой циркуляции богатой кислородом крови, которая отдает его тканям в обмен на диоксид углерода, не происходит. Диоксид углерода, высвобождаемый клетками, снижает *pH* межклеточной среды (т.е. она становится более кислой). В таких условиях клеточные мембраны разрушаются. Это происходит и с мембранами лизосом, которые содержат ферменты, расщепляющие биологические молекулы — белки, жиры, нуклеиновые кислоты. Ферменты высвобождаются в цитоплазму и разрушают клетку изнутри — происходит так называемое самопереваривание (аутолизис).

Клетки печени

Скорость, с которой распространяется данный процесс, зависит от концентрации ферментов. В печени, богатой ими, аутолизис протекает быстрее, чем в легких. Велика его скорость и в тканях, содержащих относительно много воды, например в тканях головного мозга.

Еще больше влияет на скорость аутолизиса температура окружающей среды: чем она выше, тем быстрее развивается процесс. По этой причине людей, утонувших в очень холодной воде, иногда удается вернуть к жизни даже спустя довольно длительное время после клинической смерти. ■

Читайте в следующем выпуске журнала

В ПОГОНЕ ЗА СКАЧУЩЕЙ ВСЕЛЕННОЙ

Возможно, Большой взрыв не был началом нашей Вселенной. Она могла образоваться в результате управляемого сложными гравитационно-квантовыми эффектами Большого отскока — стремительного сжатия, породившего взрыв

ШТРИХКОД ЖИЗНИ

Точно так же, как штрихкод на промышленных товарах позволяет быстро получить всю необходимую информацию о них, небольшие сегменты ДНК со специфической нуклеотидной последовательностью помогают идентифицировать организмы, от которых они получены

РОЖДЕНИЕ ОКЕАНА

Уникальный фоторепортаж из одного из самых жарких уголков планеты, где сейчас можно наблюдать такое редкое явление, как образование океана

ИСКУСНЫЕ РУКИ

Онлайн-сообщество инженеров, дизайнеров, изобретателей, один из которых лишился руки в Ираке, разрабатывает улучшенную конструкцию протеза

В ПОИСКАХ ИНТЕЛЛЕКТА

Исследователи продолжают искать среди наших генов факторы, отвечающие за интеллект. Однако объект оказался гораздо более неуловимым, чем представлялось

КАК ОФОРМИТЬ ПОДПИСКУ/ЗАКАЗ НА ЖУРНАЛ «В МИРЕ НАУКИ»

1. Указать в бланке заказа/подписки те номера журналов, которые вы хотите получить, а также ваш полный почтовый адрес. Подписка оформляется со следующего номера журнала.
2. Оплатить заказ/подписку в отделении Сбербанка (для удобства оплаты используйте квитанцию, опубликованную ниже). Оплату можно произвести также при помощи любой другой платежной системы по указанным в этой квитанции реквизитам.
3. Выслать заполненный бланк заказа/подписки вместе с копией квитанции об оплате:

- по адресу 105005, г. Москва, ул. Радио, д. 22, редакция журнала «В мире науки»;
- по электронной почте m_biruykova@sciam.ru, info@sciam.ru;
- по факсу: +7(495) 925-03-72, 727-35-30, 727-35-39

Стоимость подписки с 1 января 2009 г. составит:

Для физических лиц: **900 руб. 00 коп.** — на полгода; **1800 руб. 00 коп.** — на год;
Для юридических лиц: **1200 руб. 00 коп**. — на полгода, **2400 руб. 00 коп.** — на год;
Стоимость одного номера журнала: за 2003-2006 гг. — **80 руб. 00 коп.**, за 2007 г. — **90 руб. 00 коп.**, за 2008 г. — **100 руб. 00 коп.**; за 2009 г. — **110 руб. 00 коп.**; стоимость почтовой доставки по России — **50 руб**.
Бланк подписки на журнал размещен на сайте **www.sciam.ru**; также направляем бланк по факсу или e-mail.

Уважаемые подписчики! Доставка журнала осуществляется по почте заказным письмом.

БЛАНК ЗАКАЗА НОМЕРОВ ЖУРНАЛА

Я заказываю следующие номера журнала «В мире науки» (отметить галочкой):

	1	2	3	4	5	6	7	8	9	10	11	12
2008 г.												
2007 г.	■											
2006 г.		■										
2005 г.												
2004 г.							■					
2003 г.	■	■		■						■	■	■

Ф.И.О. _____

Индекс _____

Область _____

Город _____

Улица _____

Дом _____ Корп._____ Кв._____

Телефон _____

E-mail:_____

ЗАО «В мире науки»
Расчетный счет 40702810100120000141
в ОАО «ВТБ» г. Москва БИК 044525187
Корреспондентский счет 30101810700000000187
ИНН 7709536556; КПП 770901001

_____

_____

Фамилия, И.О., адрес плательщика

Вид платежа	Дата	Сумма
Подписка на журнал «В мире науки» на _____ номеров		

Плательщик

ЗАО «В мире науки»
Расчетный счет 40702810100120000141
в ОАО «ВТБ» г. Москва БИК 044525187
Корреспондентский счет 30101810700000000187
ИНН 7709536556; КПП 770901001

_____

_____

Фамилия, И.О., адрес плательщика

Вид платежа	Дата	Сумма
Подписка на журнал «В мире науки» на _____ номеров		

Плательщик

ПОМИМО ЭТОГО ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ «В МИРЕ НАУКИ» ВОЗМОЖНО:

- **в интернет-магазинах www.subscribe.ru, www.russische-presse.de.**
- **в книжных магазинах научного центра «ФИЗМАТКНИГА», тел.: 409-93-28.**
- **по каталогам:**

  «Пресса России», подписной индекс 45724 – для физ. лиц; 39869 – для юр. лиц;

  «Роспечать», подписной индекс 81736 – для физ. лиц; 19559 – для юр. лиц;

  «Почта России», подписной индекс 16575 – для физ.лиц.; 11406 — для юр. лиц.

- **Подписка на Украине по каталогу подписных изданий агентства KSS, подписной индекс 69970.**