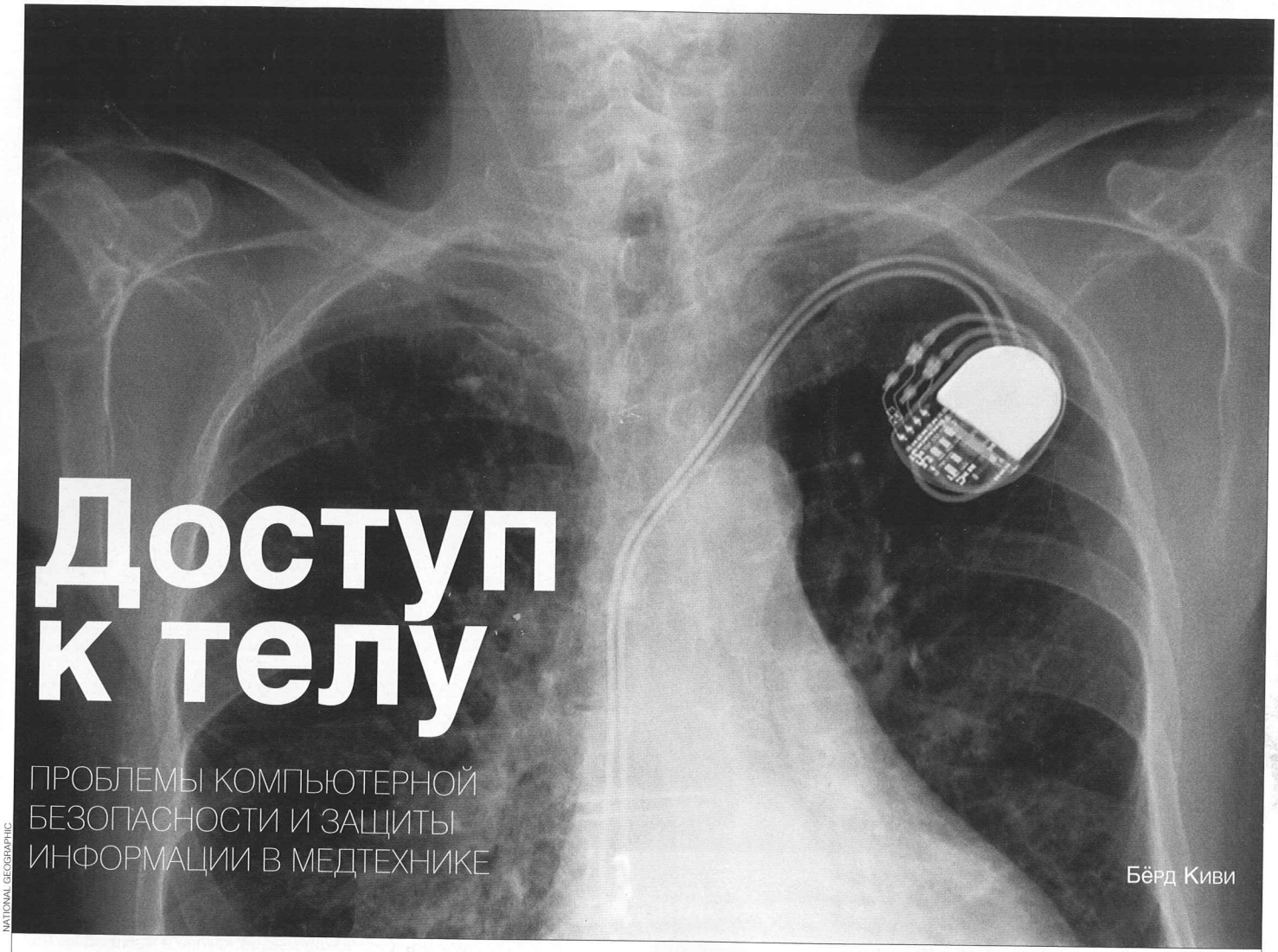


Доступ к телу

ПРОБЛЕМЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ В МЕДТЕХНИКЕ

Бёрд Киви

NATIONAL GEOGRAPHIC

Вряд ли надо доказывать, что в области медицины и охраны здоровья очень важны вопросы защиты информации. Однако инфобезопасность в здравоохранении часто сводят к защите баз данных с историями болезней, результатами анализов и прочими весьма чувствительными к компрометации персональными сведениями. Меж тем инфотехнологическое развитие современной медицины идет по множеству направлений, и с некоторых пор разработчики и пользователи медицинской техники начали сталкиваться с совсем иными компьютерными угрозами.

АТАКА ПО РАДИОКАНАЛУ

Недавно группа исследователей «хакнула» имплантируемое медицинское устройство — а именно, сердечный дефибриллятор — через его канал беспроводной связи. В результате была похищена персональная информация о пациенте и история болезни, после чего были дистанционно изменены терапевтические настройки дефибриллятора. Итогом столь серьезной атаки вполне могла бы стать смерть пациента — если бы тот был настоящий, конечно. К счастью, все обошлось без жертв, поскольку демонстрация проводилась лишь на приборе, помещенном в условия, имитирующие реальные.

Описание и анализ этой атаки являются главной темой доклада[1] на майской конференции IEEE Symposium on Security and Privacy. Авторы работы — большой коллектив ученых-исследователей из междисциплинарного научного проекта «Центр безопасности медицинских устройств» (www.secure-medicine.org), в котором участвуют сотрудники Гарвардской медицинской школы, Массачусетского университета в Амхерсте и Вашингтонского университета.

РЕНТГЕНОВСКИЙ СНИМОК ИМПЛАНТИРОВАННОГО В ТЕЛО ДЕФИБРИЛЛЯТОРА

Насколько известно авторам работы, они первыми продемонстрировали подобный хакинг биомедицинского устройства. По словам Кевина Фу (Kevin Fu), профессора-компьютерщика из Массачусетского университета и одного из лидеров проекта, важнейший итог этого исследования в том, что наглядно продемонстрировано, каким образом можно скрытно от пациентов не только извлекать информацию из вживленного в них устройства, но и перепрограммировать его. Спектр проблем, порождаемых этим открытием, оказался столь широким, что в Центре всерьез занялись их систематическим изучением и поисками путей решения.

Суть дела — в продвинутых коммуникационных возможностях современных имплантируемых устройств. Беспроводная связь была добавлена в дефибриллятор для того, чтобы доктора могли проверять и перепрограммировать аппарат, не прибегая к хирур-

1 «Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses», by Daniel Halperin et al.

гическому вмешательству для извлечения вживленного контейнера из тела. Но теперь стало ясно, что оборотной стороной этой бесспорно удобной возможности оказываются дополнительные риски для жизни пациента, исходящие от вредоносных хакерских атак.

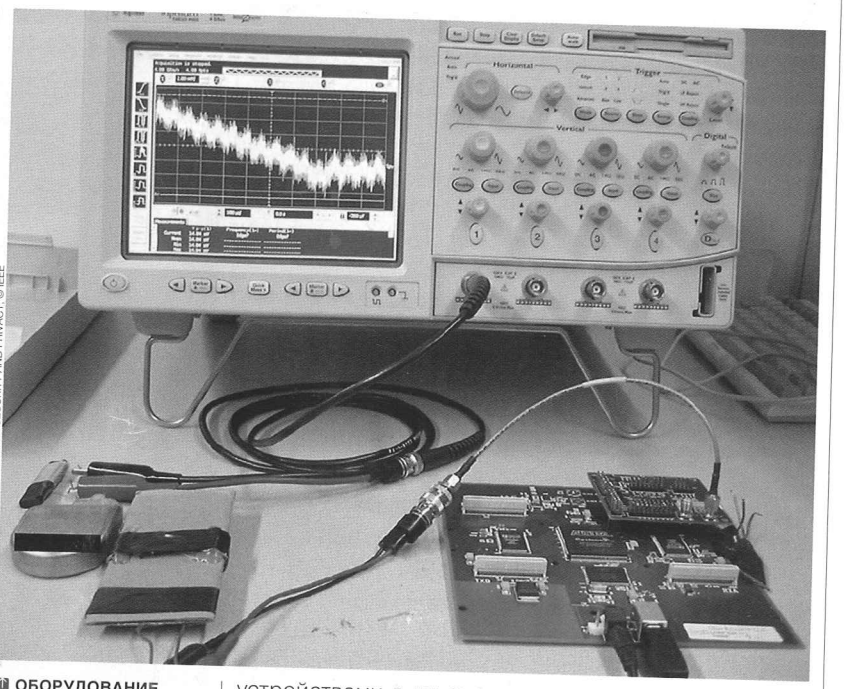
Для экспериментов выбрали дефибриллятор-кардиостимулятор Maximo фирмы Medtronic как типичный по конструкции и распространенный на рынке аппарат. Демонстрация была проведена именно на типовом, серийном устройстве, однако исследователи подчеркивают, что обладателям медицинских имплантатов пока рано опасаться коварных преступников, замышляющих их изощренное убийство через канал беспроводной связи. Для реализации этой идеи ученым потребовалось около года работ и электронное оборудование на сумму около 30 тысяч долларов. По мнению Фу, крайне маловероятно, чтобы сегодня кто-нибудь сумел применить для перепрограммирования биомедицинских устройств общедоступные средства беспроводной связи. Как показали эксперименты, чтобы изменить рабочие параметры, нужно не только приблизиться к пациенту на расстояние около нескольких сантиметров, но и обеспечить сильное магнитное поле. На больших расстояниях создать поле достаточной интенсивности без специального оборудования крайне затруднительно.

Иначе говоря, подобная атака чересчур сложна, если рассматривать ее как способ изощренного убийства больного. Но ведь и цель исследовательской работы была отнюдь не в том, чтобы создать такой способ.

С ПРИЦЕЛОМ НА БУДУЩЕЕ

Технологии, лежащие в основе имплантируемых медицинских устройств, развиваются очень быстро. Поэтому практически невозможно предсказать, что будут представлять собой эти аппараты даже лет через пять-десять. Но специалисты уверены, что в будущем этим устройствам предстоит все больше опираться на беспроводную связь, Интернет и вычислительные способности новых процессоров. Электронные имплантаты смогут вести сложное общение с другими устройствами в их окружении, что, в свою очередь, обеспечит более эффективное лечение средствами телемедицины и дистанционное наблюдение врачей за состоянием здоровья пациентов. Также вполне возможно, что в тело пациентов будут вживлять сразу несколько взаимодействующих устройств-имплантатов.

Принимая во внимание все эти тенденции, эксперты по безопасности считают, что сейчас самое время озаботиться вопросами защиты информации и приватности, которые бесспорно важны для больных, использующих медицинские имплантаты. Ведь несмотря на очень быстрый и впечатляющий прогресс в технологиях, у создателей медимплантатов по сию пору имеется лишь смутное представление о том, как сочетать информационную безопасность и приватность с медицинской безопасностью и эффективностью лечения. Весьма продвинутые методы обеспечения охраны здоровья и недопущения случайных несчастий совсем не обязательно предотвращают преднамеренные сбои в работе и другие проблемы,



ИЗОТОЧНИК: PROC. 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY. © IEEE

ОБОРУДОВАНИЕ, ПРИМЕНЯВШЕЕСЯ ДЛЯ ХАКИНГА ДЕФИБРИЛЛЯТОРА. Контейнер имплантата в левом нижнем углу
(Daniel Halperin, et al, «Pacemakers and Implantable Cardiac Defibrillators»)

РОЗЫГРЫШ

Один из знаменитых интернет-розыгрышей последнего времени сделал мишенью бурно цветущую индустрию медицинских устройств-имплантатов. Группа шутников сфабриковала «документальный» видеофильм, рассказывающий о новой опасной болезни «злокачественный металлоз», постепенно превращающей человека в киборга.

МЕДИЦИНСКИЕ ИМПЛАНТАТЫ

Имплантируемые медицинские устройства отслеживают и поддерживают определенные физиологические условия в организме, помогая пациентам вести нормальную жизнь. Сегодня применяются имплантаты множества разных типов, включая кардиостимуляторы и сердечные дефибрилляторы, системы подачи лекарств, нейростимуляторы, заглатываемые камеры-капсулы. Такого рода техника помогает лечить многие недуги — от сердечной аритмии, диабета и потери слуха до болезни Паркинсона, хронических болей, навязчивых неврозов, депрессии, эпилепсии и недержания. Количество людей с медицинскими имплантатами исчисляется десятками миллионов.

Кардиостимуляторы и дефибрилляторы созданы для лечения отклонений в работе сердца. Кардиостимулятор автоматически подает в сердечную мышцу слабые электрические импульсы, задавая нормальный ритм в те моменты, когда собственный ритм сердца замедляется. Современные дефибрилляторы тоже включают в себя функции кардиостимулятора, однако главная их задача состоит в ином. Дефибрилляторы — это устройства, подающие резкие электрические разряды в сердечную мышцу, если сердцебиение становится опасно быстрым или хаотическим. Такие разряды могут восстанавливать сердечный ритм, не доводя дело до приступа, то есть до остановки сердца, влекущей смерть человека в течение нескольких минут.

После того как клинические испытания показали, что подобные устройства могут ежегодно спасать жизнь многим тысячам людей с больным сердцем, имплантируемые дефибрилляторы превратились в очень прибыльный, многомиллиардный бизнес. Конструктивно аппарат представляет собой небольшой контейнер со встроенной батарейкой, который имплантируется в мышцу ниже ключицы (у пациентов-правшей обычно с левой стороны, у левшей справа), а к сердцу подключается изолированными проводами. Эти провода используются для работы сенсора, следящего за ритмом сердца, а также для подачи электроразряда при наступлении опасной для жизни ситуации. Когда заряд батарейки иссякает — сейчас этот срок составляет от 4 до 7 лет, — коробочку дефибриллятора приходится заменять, однако провода остаются на месте. ■

относящиеся к сфере информационной безопасности. Отыскание оптимального баланса этих факторов со временем будет становиться все более важной задачей при обеспечении дальнейшего развития медицинских имплантатов.

До появления вышеупомянутой работы о хакинге дефибриллятора, по-видимому, не было ни одного строгого в научном смысле исследования, посвященного анализу инфозащиты в коммерческих устройствах-имплантатах. Авторы исследования считали одной из главных целей выяснение вопроса о том, могут ли злоумышленники создать свое собственное оборудование, способное осуществлять беспроводные коммуникации с вживленным в тело имплантатом. Используя доступные компоненты — антенну, радиоаппаратуру и персональный компьютер, — ученые обнаружили, что в принципе это возможно: посторонние могут подключаться к радиоканалу, передающему чувствительную информацию о пациенте и медицинские телеметрические данные о работе устройства.

Главная причина в том, что имплантаты передают информацию о больных и телеметрию без какого-либо шифрования. Благодаря этому перехватчик получает доступ к имени пациента, медицинской истории больного, дате рождения и тому подобным данным. С помощью созданного ими оборудования ученые смогли полностью отключать или перенастраивать терапевтические установки, хранящиеся в памяти имплантата. Это означает, что злоумышленник может сделать устройство неспособным к надлежащей реакции в случае опасных признаков сердечной активности. Более того, можно даже заставить устройство подавать электроразряды, способные вызвать желудочковую фибрилляцию, то есть аритмию сердца с потенциально смертельным исходом.

ЧТОБЫ НЕ ДОПУСТИТЬ ИСПОЛЬЗОВАНИЯ РАБОТЫ О ХАКИНГЕ МЕДИЦИНСКИХ ИМПЛАНТАТОВ ВО ЗЛО, АВТОРЫ ИЗЪЯЛИ ИЗ СТАТЬИ ЛЮБЫЕ МЕТОДОЛОГИЧЕСКИЕ ПОДРОБНОСТИ

Исследованию было подвергнуто лишь одно конкретное устройство — сердечный дефибриллятор. Однако имеющаяся у исследователей информация не дает никаких оснований полагать, будто другие имплантаты защищены более надежно.

(Daniel Halperin, et al, «Security and Privacy for Implantable Medical Devices»)

Одна из важных целей исследований — разработка технологических механизмов для обеспечения оптимального баланса между инфозащитой и медицинской безопасностью/эффективностью. Авторы предложили три подхода для уравновешивания этих конфликтующих друг с другом факторов. Сейчас проводятся эксперименты с устройством-прототипом, реализующим эти предложения на практике.

С точки зрения медицинской безопасности весьма критично, чтобы жизнь батареи в устройстве была максимально долгой. Поэтому все три подхода к укреплению инфобезопасности основаны на концепции «нулевой энергии». Реализация этих защитных мер позволит вообще отказаться от встроенной батареи. Необходимую энергию будут давать внешние радиочастотные коммуникационные сигналы.

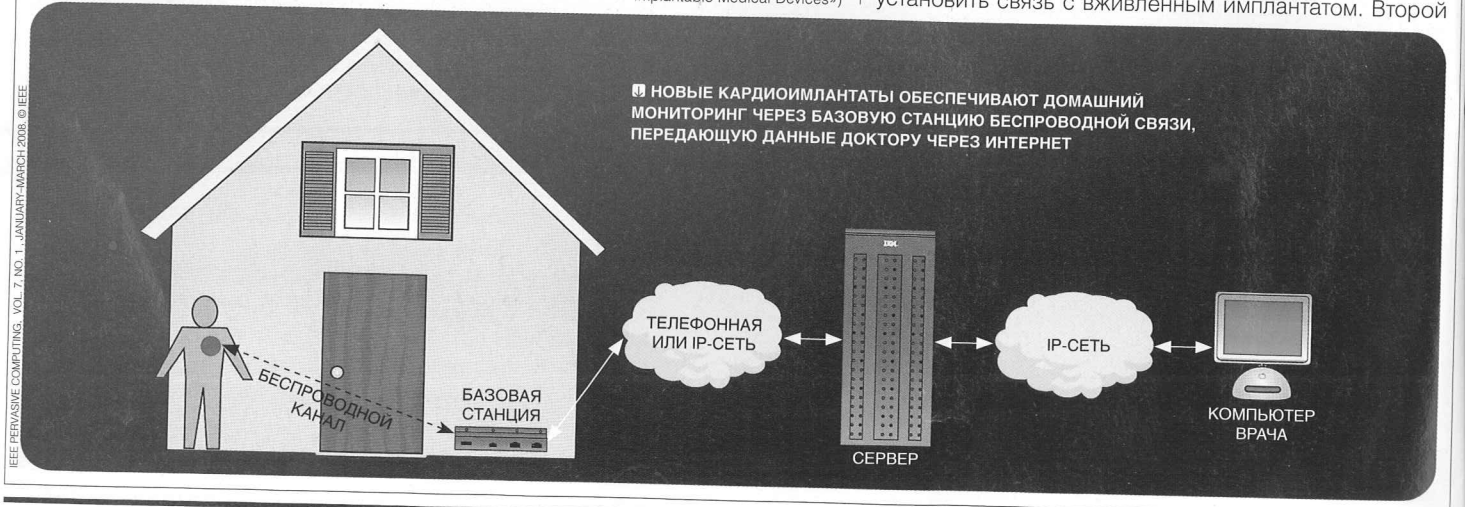
Первый метод защиты основан на подаче слышимого для пациентов звукового сигнала, предупреждающего о том, что неавторизованная сторона пытается установить связь с вживленным имплантатом. Второй

ОПАСНЫЕ ИГРЫ ПРИДУРКОВ

В марте нынешнего года был зафиксирован первый, как считается, в Интернете случай умышленной хакерской атаки на людей с медицинскими проблемами. Сайт благотворительной организации Epilepsy Foundation, занятой поддержкой больных, страдающих эпилепсией, имеет веб-форум, где посетители могут неформально общаться, делиться опытом лечения и получать консультации. Именно этот форум выбрала по какой-то — ведомой лишь им самим — причине анонимная группа хакеров-придурков в качестве стартовой площадки для физических атак на эпилептиков.

Сначала дискуссионные ветви форума стали наводнять сотни посланий со встроенными картинками GIF-анимации, которые мерцающей сменой красок способны вызывать у больных эпилептический припадок или сильнейший приступ мигрени. Администрация сайта сработала быстро и после первых же сообщений о происходящем заблокировала сообщения с опасными картинками. Однако на следующий день атакующая сторона прибегла к более изощренной тактике — в послания встраивался код, отправляющий читателей на другой веб-сайт. На нем окно браузера автоматически переводилось в полноэкранный вид, после чего начиналась демонстрация быстро меняющихся изображений, провоцирующих приступы у эпилептиков.

По данным медицинской статистики, в мире насчитывается около 50 млн. человек, страдающих теми или иными формами эпилепсии. Хотя всего лишь несколько процентов из них подвержены приступам из-за мерцающего света, это все равно огромное количество людей, которым безответственные и нравственно недоразвитые «умельцы» способны с помощью инфотехнологий наносить физический ущерб просто так, забавы ради. Более наглядного и убедительного примера серьезности проблем инфобезопасности, встающих ныне перед медициной, наверное, и не придумать. ■



НОВЫЕ КАРДИОИМПЛАНТАТЫ ОБЕСПЕЧИВАЮТ ДОМАШНИЙ МОНИТОРИНГ ЧЕРЕЗ БАЗОВУЮ СТАНЦИЮ БЕСПРОВОДНОЙ СВЯЗИ, ПЕРЕДАЮЩУЮ ДАННЫЕ ДОКТОРУ ЧЕРЕЗ ИНТЕРНЕТ

подход реализует криптографически защищенные схемы аутентификации, используя только энергию внешних радиосигналов. Третий подход использует передачу криптографических ключей (усложненных паролей) таким образом, чтобы люди физически ощущали этот процесс, например, через слух или осязание.

РЕАКЦИЯ ИНДУСТРИИ

Исследователи Центра безопасности медустройств подчеркивают, что вовсе не пытаются выдать свои разработки за окончательное решение проблем с инфозащитой имплантатов. Эти исследования — лишь шаг к созданию потенциального фундамента, на котором могли бы разрабатываться новые защитные механизмы для будущих конструкций подобных устройств.

Один из непосредственных участников хакинг-проекта, кардиобиолог Уильям Мэйсел (William H. Maisel) из Бостонского медицинского центра, уточняет, что выявленные проблемы имеют общий характер для всей индустрии устройств-имплантатов. Посему исследователи не сочли нужным выходить на изготовителя конкретного аппарата, фирму Medtronic, а передали свои результаты в FDA, правительственное Управление по контролю за продуктами и лекарствами, ведающее, среди прочего, и безопасностью медицинской техники.

В американском FDA, надо отметить, незадолго до этого уже озаботились проблемой радиопередатчиков в медицинских имплантатах. Но главное внимание пока сосредоточено на вопросах непреднамеренной интерференции. В частности, на том, сколь серьезные помехи в работе медицинских радиоустройств могут вызвать посторонние электромагнитные сигналы и насколько это опасно для жизни пациентов.

Компания Medtronic, нынешний лидер по части продаж кардиоимплантатов, в сдержанном комментарии для прессы сообщила, что может только приветствовать возможность более тщательного изучения проблем безопасности вместе с врачами, исследователями и регулирующими органами. Добавив, что за тридцать лет работы она ни разу не сталкивалась с попытками нелегального или неавторизованного хакинга своих устройств, обладающих возможностями телеметрии или беспроводного управления.

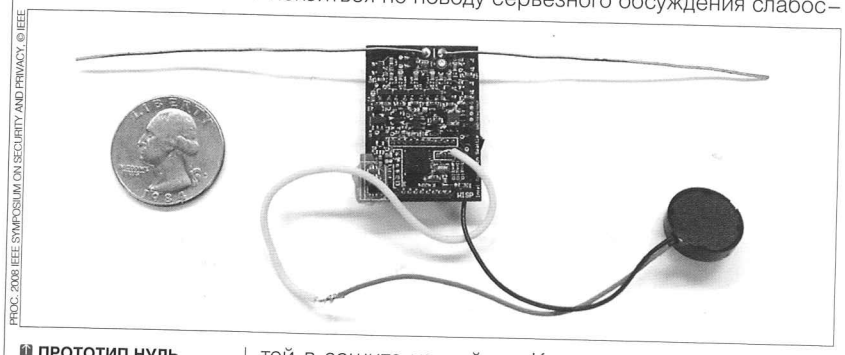
МЕШОК

При экспериментах с хакингом медимплантатов для воссоздания в условиях компьютерной лаборатории максимально реалистичной обстановки контейнер-имплантат помещался внутрь мешка с сырым мясом и беконом. Использовались только фиктивные симуляционные данные о виртуальном пациенте.

Компания Boston Scientific, чье подразделение Guidant по цифрам продаж уступает лишь Medtronic, тут же воспользовалась удачной пиар-ситуацией. В своем комментарии эта фирма сообщила, что в ее имплантатах уже имеются «встроенное шифрование и технологии безопасности, разработанные для уменьшения отмеченных рисков». Поскольку дефибрилляторы Guidant никто из хакеров пока не исследовал, утверждение изготовителя остается принять на веру.

Третья по значимости из выпускающих кардиоимплантаты компаний, St. Jude Medical, выступила примерно в том же ключе, сообщив, что и в ее дефибрилляторах для защиты информации используются некие «проприетарные технологии». И коль скоро никаких известий о нелегальных манипуляциях конкретно с этими устройствами не поступало, надежность защиты здесь подразумевается адекватной.

Короче говоря, известие об успешном хакинге имплантатов с радиопередатчиком индустрия восприняла спокойно. Есть даже явные признаки того, что криптозащитой информации во вживляемых медустройствах там уже занимаются. Сами же исследователи, привлекшие внимание общества к проблеме, всячески подчеркивают, что больным не следует беспокоиться по поводу серьезного обсуждения слабостей в защите устройств. Как говорит уже упоминавшийся кардиолог Уильям Мэйсел, «для пациентов, имеющих такие устройства, гораздо лучше быть с ними, нежели без них; если бы мне самому требовался дефибриллятор, я попросил бы тот, что оснащен беспроводной связью». Однако, тут же добавляет его коллега-компьютерщик Кевин Фу, «необходимо уже сегодня планировать, каким образом эти устройства будут использоваться в ближайшие пятнадцать-двадцать лет». ■



PROC. 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY, © IEEE

ПРОТОТИП НУЛЬ-ЭНЕРГЕТИЧЕСКОГО УСТРОЙСТВА ОПОВЕЩЕНИЯ ПАЦИЕНТА НА ОСНОВЕ ПЬЕЗОЭЛЕМЕНТА
(Daniel Halperin, et al, «Pacemakers and Implantable Cardiac Defibrillators»)

АУДИОПЛЕЕРЫ ПРОТИВ КАРДИОСТИМУЛЯТОРОВ

В июне 2007 года медицинский журнал Heart Rhythm опубликовал статью, вызвавшую как заметный резонанс среди специалистов-кардиологов, так и сильнейшие сомнения в достоверности полученных результатов («Pacemaker interference with an iPod», by M.B. Patel et al.). Суть работы, как можно понять из названия, в том, сколь серьезно излучение от аудиоплееров, используемых пациентами, может воздействовать на работу их имплантатов-кардиостимуляторов. Получалось, что для возникновения опасной интерференции достаточно разместить плеер iPod на расстоянии 5 см от груди пациента. Более того, в некоторых случаях iPod порождал интерференционные помехи на расстояниях до полуметра.

Столь серьезная угроза у многих ученых с самого начала вызвала сомнения. Как показали дальнейшие исследования, для скепсиса были все основания. Было показано, что аудиоплееры очень слабо влияют на работу кардиостимуляторов. В одной из последних работ, выполненной в Гарвардской медицинской школе, было протестировано четыре распространенных типа музыкальных плееров на пациентах от 6 до 60 лет, имеющих вживленные кардиостимуляторы и дефибрилляторы. Многие сотни тестов доказали, что аудиоплееры не оказывают ни малейшего воздействия на функционирование кардиостимуляторов. Единственное, что было отмечено, это небольшие помехи, появлявшиеся в процессе перепрограммирования устройств, «но не до такой степени, чтобы нарушить их функциональность». Таким образом, делается вывод в этой работе, пациентам следует обращать внимание на плеер лишь в тех случаях, когда доктор перепрограммирует вживленное устройство. ■