Этические аспекты использования медицинских изделий с технологией Интернета тела

Хохлов А.Л.[1,2], Белоусов Д.Ю.[3]

[1] — ФГБОУ ВО «Ярославский государственный медицинский университет», Ярославль, Россия

[2] — Совет по этике при Министерстве здравоохранения Российской Федерации

[3] — ООО «Центр фармакоэкономических исследований», Москва, Россия

Аннотация. В данной статье изложены вопросы биоэтики, связанные с применением технологии Интернета тела (Internet of Bodies; IoB) в здравоохранении, т. н. медицинских IoB-изделий. Производители медицинских IoB-изделий обещают обеспечить существенную пользу для здоровья, улучшить результаты лечения и другие преимущества, но такие IoB также несут и серьёзные риски для здоровья и жизни, включая риски взлома (киберхакинга), неисправности, получения ложноположительных результатов измерений, нарушения конфиденциальности, умышленного вторжения в частную жизнь. Кроме того, медицинские IoB-изделия могут напрямую причинить физический вред человеческому телу. По мере того, как человеческая плоть будет переплетаться с оборудованием, программным обеспечением и алгоритмами, IoB будет проверять наши общественные моральные ценности и этические нормы. В частности, IoB бросят вызов представлениям о человеческой автономии и самоуправлении, поскольку они создают определённую угрозу автономии человека. Таким образом, защита автономии человека должна стать основным этическим принципом применения медицинских IoB-изделий.

Ключевые слова: этическая экспертиза; биомедицинские исследования; медицинские изделия; комитет по этике; интернет тела; интернет медицинских вещей

Для цитирования:
Хохлов А.Л., Белоусов Д.Ю. Этические аспекты использования медицинских изделий с технологией Интернета тела. *Качественная клиническая практика*. 2021;(2):89-98. https://doi.org/10.37489/2588-0519-2021-2-89-98

Ethical aspects of the Internet of Bodies

Khokhlov AL[1,2], Belousov DYu[3]

[1] — Yaroslavl State Medical University of the Ministry of Health of Russia, Yaroslavl, Russia

[2] — Ethics Council under the Ministry of Health of the Russian Federation

[3] — LLC "Center for pharmacoeconomics research", Moscow, Russia

Abstract. This article outlines bioethical issues related to the application of the Internet of Body (IoB) technology in health care so-called medical IoB devices. Manufacturers of medical IoB devices promise to provide significant health benefits, improved treatment outcomes and other benefits, but such IoB also carry serious risks to health and life, including the risks of hacking (cyberhacking), malfunctioning, receiving false positive measurements, breaching privacy, deliberate invasion of privacy. In addition, medical IoB products can directly cause physical harm to the human body. As human flesh is intertwined with hardware, software, and algorithms, the IoB will test our social values and ethics. In particular, IoB will challenge notions of human autonomy and self-government as they threaten to undermine the fundamental precondition of human autonomy. Thus, the protection of human autonomy should become the main ethical principle of the use of medical IoB devices.

Keywords: ethical review; biomedical research; medical devices; ethics committee; Internet of Bodies; IoB; Internet of Medical Things; IoMT

For citation:
Khokhlov AL, Belousov DYu. Ethical aspects of the Internet of Bodies. *Kachestvennaya klinicheskaya praktika = Good Clinical Practice.* 2021;(2):89-98. (In Russ). https://doi.org/10.37489/2588-0519-2021-2-89-98

Введение / Introduction

Широкий спектр медицинских «умных» устройств, подключённых к Интернету, так называемый **Интернет медицинских вещей** (*англ.* Internet of Medical Things; IoMT) — *интеллектуальные медицинские сетевые системы со встроенными датчиками, процессорами и исполнительными механизмами, которые предназначены для восприятия и взаимодействия с физическим миром, включая пользователей — людей* [1], растёт с каждым годом. У IoMT есть несколько общепризнанных характеристик:

1) подключение к Интернету напрямую или через локальную сеть;

2) наличие одной из следующих функций:
   — способность вызывать или ощущать некоторые физические изменения,
   — напрямую получать информацию от людей, или предоставлять информацию людям, или извлекать данные, или хранить данные;
3) возможность взаимодействовать, чтобы приносить пользу для здоровья.

Однако рынок IoMT теперь растёт и за счёт появления индустрии устройств, которые контролируют человеческое тело, собирают персональные данные о здоровье и другую личную информацию, и передают эти данные через Интернет. Эти новые технологии и собираемые ими данные в 2016 году Андреа Матвишин (Andrea M. Matwyshyn) назвал **Интернетом тела** (*англ.* Internet of Bodies; IoB) — *сеть человеческих тел, целостность и функциональность которых, по крайней мере частично, зависят от Интернета и связанных с ним технологий, таких как искусственный интеллект* [2]. Любое устройство IoB является устройством IoMT.

Поскольку пока общепринятого определения IoB не существует, в данной статье мы подразумеваем **медицинские IoB-изделия** *вместе с программным обеспечением и данными, которые они собирают и передают их посредством Интернета или через локальную сеть, и которые напрямую связаны с человеческим телом.* Наше определение IoB включает в себя медицинские технологии, которые также называют Интернетом вещей в сфере здравоохранения (*англ.* the health-care Internet of Things) [3], хотя не каждое устройство IoB в сфере здравоохранения можно считать медицинским IoB-изделием.

В данной статье изложены вопросы биоэтики, связанные именно с медицинскими изделиями с IoB-технологиями, которые применяются только в здравоохранении (оборот которых должен соответствующим образом регулироваться на законодательном уровне), а не в личных целях для поддержания здорового образа жизни (соблюдения диеты, оптимального уровня физической активности, режима сна, медитации и прочего).

Целесообразно считать медицинским IoB-изделием, если оно:
1) напрямую временно или постоянно связано с телом человека (носится, приклеивается, проглатывается, имплантируется или иным образом прикрепляется к телу или внедряется в тело);
2) содержит программное обеспечение или вычислительные возможности;
3) может связываться с подключённым к Интернету устройством или сетью и удовлетворяет одному или двум условиям:
   — собирает персональные данные о состоянии здоровья, генерируемые человеком,
   — может изменить функции систем органов человека.

Программное обеспечение или вычислительные возможности в медицинском IoB-изделии могут быть такими же простыми, как несколько строк кода, используемых для настройки имплантата микрочипа радиочастотной идентификации (*англ.* radio frequency identification; RFID), или такими же сложными, как компьютер, который обрабатывает алгоритмы искусственного интеллекта и машинного обучения [4].

Для медицинского IoB-изделия требуется подключение к Интернету через сотовую сеть или Wi-Fi, но не обязательно прямое подключение. Например, устройство может быть подключено через Bluetooth к смартфону или USB-устройству, которое обменивается данными с компьютером, подключённым к Интернету. Медицинские изделия, не подключённые к Интернету, такие как обычные кардиомониторы или медицинские идентификационные браслеты, не входят в наше определение медицинских IoB-изделий.

Некоторые устройства IoB могут подпадать под наше определение лишь частично. Например, смартфон с подключением к Wi-Fi сам по себе не будет частью IoB, однако после установки приложения для здоровья, которое требует подключения к телу для отслеживания пользовательской информации, такой как частота сердечных сокращений или количество сделанных шагов, телефон будет считаться IoB, но не медицинским IoB-изделием, а лишь частью экосистемы IoMT. «Умный» холодильник больницы, используемый для хранения вакцин, который может быть подключён к сети Интернет и предупреждать персонал, если запасы кончаются, также не является медицинским IoB-изделием, поскольку не собирает персональные данные о больном и не влияет на функции систем органов человека.

Персональные данные о состоянии здоровья, генерируемые человеком, относятся к данным о здоровье, клинических проявлениях заболеваний или изменений в самочувствии, собираемым медицинскими IoB-изделиями для записи или анализа пользователем, алгоритмом или другим лицом.

Наконец, к *изменению функции систем органов человека* относится оказываемое медицинским IoB-изделием влияние на функции органов человека или их модификация.

Наше определение предназначено для охвата быстро развивающихся медицинских технологий, которые могут привести к различным рискам и преимуществам, обсуждаемым в этой статье, поэтому мы сосредоточимся на анализе существующих именно медицинских IoB-изделий.

Производители медицинских IoB-изделий обещают обеспечить существенную пользу для здоровья, улучшить результаты лечения и другие преимущества, но такие IoB также несут и серьёзные риски для

здоровья и жизни, включая риски взлома (киберхакинга), неисправности, получения ложноположительных результатов измерений, нарушения конфиденциальности, умышленного вторжения в частную жизнь.

Некоторые из медицинских IoB-изделий, такие как искусственная поджелудочная железа, могут значительно улучшить контроль сахарного диабета, в то время как другие просто ведут к повышению расходов на здравоохранение с небольшим положительным влиянием на результаты лечения.

Доступ к огромным потокам персональных данных о состоянии здоровья, генерируемые человеком в режиме реального времени, может спровоцировать прорыв в медицинских знаниях или в понимании поведения пациента. Всё это может привести к увеличению разрыва в сохранении или поддержании здоровья между разными слоями населения, поскольку только люди с большими финансовыми средствами будут иметь доступ к новейшим медицинским IoB-изделиям.

Появление и использование медицинских IoB-изделий будет свидетельствовать о тех же недостатках безопасности, которые преследуют устройства IoMT, однако, в отличие от большинства IoMT, медицинские IoB-изделия могут напрямую причинить физический вред человеческому телу — ряд причин, по которым законодатели и регулирующие органы сочтут заслуживающими внимание организацию правовой защиты их применения. Таким образом, более широкое использование медицинских IoB-изделий индуцирует появление корпоративной ответственности за программное обеспечение, и, кроме того, прецеденты с нанесением вреда здоровью человека послужат стимулом к развитию новой правовой науки — биомедицинского права (так называемого «биоправа»), борющегося за соблюдение целостности человеческого тела и разума.

Тем не менее, проблемы медицинских IoB-изделий не носят чисто юридический характер. Социальная интеграция IoB также не будет гладкой. По мере того, как человеческая плоть будет переплетаться с оборудованием, программным обеспечением и алгоритмами, IoB будет проверять наши общественные моральные ценности и этические нормы. В частности, IoB бросят вызов представлениям о человеческой автономии и самоуправлении, поскольку они угрожают подорвать фундаментальное предварительное условие — автономию человека. Таким образом, защита автономии человека должна стать основным этическим принципом применения медицинских IoB-изделий [2].

Технологии медицинских IoB-изделий / Technologies of the medical IoB

Медицинские IoB-изделия бывают разных видов и функциональной направленности. Некоторые из них уже широко используются, например, электрокардиостимуляторы, кохлеарные имплантаты и искусственная поджелудочная железа. Эти устройства имеют непосредственный доступ к человеческому телу и собирают большое количество персональных данных. На рис. 1 показаны примеры таких медицинских IoB-изделий.

Правовая основа / Legal basis

Основа правовых подходов к регулированию медицинских изделий, в том числе и медицинских IoB-изделий, заложена в Федеральном законе от 21 ноября 2011 г. № 323 «Об основах охраны здоровья граждан в Российской Федерации» [5], в котором в статье 38 определение термина «медицинское изделие» (МИ) соответствует определению медицинского IoB-изделия в целях и предназначении применения.

Государственная регистрация медицинских IoB-изделий и контроль за их обращением на территории Российской Федерации осуществляются Федеральной службой по надзору в сфере здравоохранения (Росздравнадзор). Общие правила государственной регистрации медицинских изделий описаны в постановлении Правительства РФ от 27.12.2012 г. № 1416 [6].

Электрокардиостимулятор | **Кохлеарный имплантат** | **Искусственная поджелудочная железа**

Рис. 1. Примеры медицинских IoB-изделий
Figure 1. Examples of medical IoB

Этическую экспертизу возможности проведения клинических испытаний медицинских изделий с участием человека в качестве субъекта проводит Совет по этике в сфере обращения медицинских изделий Министерства здравоохранения России [28].

Действующее российское законодательство устанавливает, что государственная регистрация медицинских изделий осуществляется на основании технических и клинических испытаний с учётом потенциального риска применения и в соответствии с номенклатурной классификацией МИ, которые определены приказом Министерства здравоохранения России от 06.06.2012 г. № 4н [7].

Медицинские IoB-изделия подразделяются, как и все МИ, в зависимости от потенциального риска применения [8]. Приказом Министерства здравоохранения России от 06.06.2012 г. № 4н предусмотрено 4 класса риска [7]; каждое медицинское IoB-изделие может быть отнесено только к одному классу. При классификации также учитывают длительность применения, инвазивность, наличие контакта с телом человека или взаимосвязь с ним, применение для жизненно важных органов и систем. Например, электрокардиостимуляторы, кохлеарные имплантаты и искусственная поджелудочная железа относятся к 3-му классу с высокой степенью потенциального риска применения.

Уязвимость медицинских IoB-изделий / Vulnerability of medical IoB devices

Технологии IoB страдают от тех же направлений атак хакеров, что и другие IoMT и вычислительные устройства, но устройства IoB имеют повышенные риски в результате слияния нескольких характеристик, включая связь с человеческим телом, вид и объём собираемой информации, а также то, как эта информация может быть использована.

Компьютерное программное обеспечение медицинских IoB-изделий по своей природе уязвимо для непреднамеренных ошибок или злонамеренных действий. Слабые места в коде могут быть использованы для кражи информации, собираемой медицинским IoB-изделием, или манипулирования ею, нарушения его работы или иного поведения, вызывающего непредвиденный вред. Возможности подключения устройств, подключённых к Интернету, постоянно развиваются по своему характеру и качеству, и в дальнейшем они будут обеспечиваться такими коммуникационными технологиями, как 5G, Wi-Fi 6 (802.11ax) и спутниковый Интернет. Но эти системы связи также могут стать и мишенью хакеров-преступников [9].

Кроме того, физическое устройство, имплантированное или прикреплённое к телу, будет подключаться по беспроводной сети к устройству мониторинга, например, к смартфону, которое затем будет передавать информацию в облачный сервис. Затем данные становятся доступными для внешней стороны, такой как производитель устройства или практикующий врач. Это сочетание аппаратного и программного обеспечения, физических и логических каналов связи и организационных границ вводит множество уровней сложности, каждый из которых подвержен сбоям, ухудшению качества, компрометации и хакерским атакам [4].

Большинство уязвимостей медицинских IoB-изделий связаны с ошибками аутентификации пользователя и дефектами кода. Недостатки аутентификации пользователей могут позволить неавторизованным пользователям получать доступ к данным и связывать их (например, нарушать конфиденциальность устройства). Дефекты кода относятся к недостаткам программного обеспечения, которые могут позволить злоумышленнику нарушить конфиденциальность, целостность или доступность системы. Например, хакер может заставить устройство обмениваться данными с неавторизованными пользователями, манипулировать данными так, чтобы устройство работало некорректно, или просто заставить устройство перестать работать [4].

Риски кибербезопасности часто группируются в три категории [4]:

1) конфиденциальность — означает, что данные видны только уполномоченным лицам;
2) целостность — означает, что собранные данные не были умышленно изменены;
3) доступность — гарантирует, что данные будут доступны тогда и там, где они необходимы.

Уязвимость медицинских IoB-изделий может случайно вызвать физический ущерб человеку или использоваться злонамеренно для причинения вреда или смерти. Эта уязвимость может позволить злоумышленнику перехватить обмен данными между имплантированным медицинским изделием и устройством клинического программирования или домашним компьютером для мониторинга таким образом, чтобы можно было манипулировать данными или вводить ложные (вредоносные) команды в имплантированное медицинское изделие. Например, в 2016 году были обнаружены три уязвимости в компьютерном коде инсулиновой помпы, которые могут позволить злоумышленнику вводить вредоносные команды, нанося серьёзный ущерб здоровью человека [10]. В 2019 году уязвимость была обнаружена в программном обеспечении беспроводной связи имплантируемого кардиовертера-дефибриллятора компании Medtronic plc. [11]. Также в 2019 году FDA объявило, что некоторые высокотехнологичные инсулиновые помпы производства компании Medtronic plc. уязвимы для кибервзлома. «*Человек со специальными техническими навыками и оборудованием может потенциально подключиться к чужой инсулиновой помпе*

по беспроводной связи, чтобы изменить настройки и контролировать доставку инсулина», — говорится в письме компании Medtronic plc., которое оно направило пациентам. Компания отмечает, что изменение подачи инсулина может привести к опасно высокому или низкому уровню глюкозы в крови [12].

Привносят проблемы с уязвимостью и биохакеры — энтузиасты любительских исследований, которые в своей деятельности придерживаются хакерских принципов применительно к современным биомедицинским исследованиям, считая, что инновации в медицине должны быть легкодоступными, недорогими и открытыми для всех. При разработке научных приборов биохакеры придерживаются принципов «открытого кода»: оставляют покупателю возможность контролировать, настраивать и автоматизировать приобретённую систему, в том числе путём доработки открытого для изменений программного обеспечения. Цели биохакеров — оптимизация работы организма и различных систем, борьба с заболеваниями (например, с сахарным диабетом), подтверждение собственных оригинальных идей и удовлетворение научного любопытства. Уже есть примеры того, как биохакеры «взламывают» медицинские IoB-изделия для улучшения их функциональности (см. Пример 1) [13, 14].

Однако разработчики не одобряют эти модификации, утверждая, что они могут негативно повлиять на функциональность изделия. Эксперты говорят, что эта практика питает подпольный рынок использованных медицинских IoB-изделий, на котором пользователи покупают устаревшие медицинские устройства с известными уязвимостями безопасности. В этой практике есть определённые опасности: используются медицинские изделия, на которые не распространяются гарантии производителя или их применение не соответствует инструкции по применению, поэтому производители не могут поддержать их в случае возникновения проблемы.

В дополнение к кибербезопасности самих медицинских IoB-изделий, электронные медицинские базы данных, в которых хранятся *интегрированные электронные медицинские карты*[1] (ИЭМК), также должны иметь достаточную защиту, программное обеспечение и средства контроля безопасности. В противном случае пользователи могут также оказаться в опасности в связи со стремительным внедрением ИЭМК в рутинную медицинскую практику.

Дискуссионные аспекты / Discussion aspects

Данные. Медицинские IoB-изделия собирают и обрабатывают сугубо персональные данные, возможно, более личные, чем любой другой тип пользовательской информации, поэтому существует множество рисков для конфиденциальности. Информация о местонахождении пользователей, состояния их здоровья, то, что они видят и слышат, может быть записана и сохранена.

Медицинские данные уязвимы для предвзятости отбора, поскольку типичные пользователи медицинских IoB-изделий представляют собой группу, вы-

Пример 1

Биохакинг инсулиновой помпы [14]

Example 1

Insulin pump biohacking [14]

Дана Льюис (Dana Lewis), уроженка Алабамы (США), является одним из пионеров в области инсулиновой помпы «сделано своими руками». В 2014 году она использовала специальную программу, чтобы разблокировать показания уровня глюкозы в крови в реальном времени со своей инсулиновой помпы, и создала алгоритм, который может предсказать, каким будет её уровень глюкозы в крови в будущем. Затем она встретилась с биохакером Беном Уэстом (Ben West), который придумал, как применить алгоритм к инсулиновым помпам компании Medtronic plc., «*и загорелась лампочка*», — сказала Льюис. Она разместила код в Интернете, назвав его OpenAPS[2], и сделала его широко доступным для всех, кто хотел разблокировать свои инсулиновые помпы. «*Я хотела поделиться своим решением с другими людьми. С самого начала это было движение пациентов, которые говорили: "Я хочу иметь выбор"*, — сказала Льюис. — *Речь шла о том, как восполнить пробел, пока не появится что-то коммерчески доступное*». По словам Льюиса, тысячи людей во всём мире используют данную гибридную стратегию.

В последние годы разрозненная сеть так называемых «агрессивных пациентов» начала использовать бреши в безопасности в некоторых инсулиновых помпах, чтобы заставить их автоматически определять уровень глюкозы в крови и соответствующим образом корректировать уровни инсулина. Взломанные помпы дают пользователям более плавный уровень глюкозы, чем тот, который пользователь может получить прямо сейчас с уже одобренными устройствами. Однако метод «сделано своими руками» требует, чтобы пользователи вводили свои собственные параметры, включая чувствительность к инсулину и базальный режим, который включает форму инсулина длительного действия для поддержания стабильного уровня глюкозы.

[1] **Интегрированная электронная медицинская карта** — это совокупность электронных персональных медицинских записей, относящихся к одному человеку, собираемых и используемых несколькими медицинскими организациями [16].

[2] **OpenAPS** (англ. Open Artificial Pancreas System) — «операционная система» искусственной поджелудочной железы [15]. Выгружает данные из Nightscout, прогнозирует и подстраивает доставку инсулина помпой, подгружает данные в Nightscout для непрерывного отслеживания. **Nightscout** — программа с открытым исходным кодом для хранения и визуализации данных для больных сахарным диабетом I типа.

бирающую такие изделия самостоятельно ввиду их новизны и дороговизны; и мало что известно о тех, кто не пользуется медицинскими IoB-изделиями из-за их высокой стоимости либо других препятствий. Нерепрезентативность данных о состоянии здоровья — это хорошо задокументированная проблема, поскольку большинство клинических данных обычно собираются по молодым мужчинам [17].

Есть много и других нерешённых вопросов, например:

— Кто имеет право использовать данные, собранные медицинскими IoB-изделиями, и каким образом?

Например, возникают вопросы о том, что правоохранительные органы могут делать с информацией, извлечённой из медицинского IoB-изделия? Поскольку медицинская информация, такая как данные из кардиостимулятора, уже использовалась для обвинения людей в преступлениях (см. Пример 2).

Сбор данных может поставить под угрозу конфиденциальность пользователей медицинских IoB-изделий, если не будут приняты меры защиты от неправомерного использования. Сам процесс сбора может представлять риск для конфиденциальности, включая то, какие данные собираются, как часто, было ли получено информированное согласие (особенно у уязвимых групп населения, таких как несовершеннолетние, пожилые с когнитивными нарушениями и другие), и есть ли у пользователя возможность остановить сбор или перепродажу данных в любое время.

Информация, раскрывающая нездоровый образ жизни, может привести к увеличению взносов на медицинское страхование для некоторых людей. Увеличение количества медицинских IoB-изделий, развитие системы анализа медицинских данных с помощью алгоритмов системы искусственного интеллекта может усилить эту тенденцию объединения данных о здоровье с другими персональными данными. Поэтому возникают вопросы о неотъемлемых правах, которыми может быть наделён пользователь:

— Должен ли пользователь иметь право отказаться от определённых типов сбора или хранения персональных данных?

— Должно ли быть указано право отзыва выданного ранее согласия?

Согласно ст. ч. 2 ст. 9 и ч. 5 ст. 21 Федерального закона № 152-ФЗ «О персональных данных» [19], после отзыва согласия оператор персональных данных не может обрабатывать персональные данные и должен будет прекратить обработку персональных данных в течение 30 дней с даты поступления отзыва, за исключением случаев, когда обработка может быть продолжена по закону (например, при заключении с оператором договора на оказание услуг и подписанном согласии: после отзыва согласия оператор данных вправе продолжить обработку персональных данных только в том объёме, который необходим для оказания услуг по договору).

— Должно ли быть реализовано «право на забвение» для тех, кто просит удалить свои персональные данные?

В 2016 году в России появился правовой инструмент, который позволяет воспользоваться «правом на забвение». Инструкция к российскому «праву на забвение» изложена в ст. 10.3 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в редакции от 1 января 2016 г.) [20]. Данная норма позволяет пользователю (заявителю) требовать у оператора поисковой системы удаления из результатов поиска ссылок на страницы сайтов, которые содержат информацию о заявителе. Однако убрать из поиска можно далеко не любую информацию о пользователей. Закон допускает делистинг в отношении следующих категорий: информация, распространяемая с нарушением законодательства РФ (например, оскорбления, личные фото, незаконная обработка персональных данных); недостоверная информация; неактуальная информация; информация, которая утратила значение для заявителя в силу последующих событий или действий заявителя.

Пример 2

Использование данных из кардиостимулятора в работе правоохранительных органов

Example 2

Using data from a pacemaker in law enforcement

Росс Комптон (Ross Compton) из штата Огайо (США) сообщил полиции, что увидел, как его дом горит, собрал свои вещи в чемоданы, выкинул их из окна спальни, а потом отнёс в машину. Однако полицейские заподозрили неладное: у Росса ранее были диагностированы серьёзные проблемы с сердцем, и стражи порядка усомнились в его способностях таскать тяжёлые чемоданы. Этот аргумент позволил им добиться от прокурора ордера на скачивание данных с кардиостимулятора подозреваемого. Врач-кардиолог проанализировал данные о сердцебиении и пришёл к выводу, что Росс не мог сделать то, о чём заявил полиции. Этот вывод стал основным доказательством обвинения в умышленном поджоге в целях получения страховки в 400 000 $ США. Росса арестовали по обвинению в предумышленном поджоге и страховом мошенничестве, опираясь на скачанные с его кардиостимулятора данные. Это дело вызвало широкий резонанс среди юристов технологических компаний. По их мнению, необходимо выработать чёткие правила, защищающие данные с кардиостимуляторов и других имплантируемых электронных устройств (по тому же принципу, который защищает личную переписку и другие персональные данные) [18].

— Должны ли персональные данные быть удалены после смерти человека или они могут быть доступны для ближайших родственников? (Так называемое «посмертное право на неприкосновенность частной жизни»).

Кроме того, *интерпретация данных* медицинских IoB-изделий и выходных данных алгоритмов, которые используя эти данные, могут быть предвзятыми, особенно если в этих процессах мало прозрачности — алгоритм работает по принципу **«чёрного ящика»** [21].

Есть также опасения по поводу *долговечности данных*. Например, сопоставление результатов генетического тестирования с данными медицинского IoB-изделия могут идентифицировать человека как носителя генетического заболевания, информация о котором может быть передана его или её детям, что может однажды привести к тому, что этим детям откажут в определённой медицинской страховке или других льготах [22].

Наконец, поскольку ценность данных о состоянии здоровья может достигать миллиардов долларов США, то возникает вопрос:

— Кому принадлежит право собственности (владения) на данные, генерируемые любым медицинским IoB-изделием: пользователю (больному), производителю медицинского изделия, поставщику медицинских услуг?

Неравенство. Одним из обещанных преимуществ медицинских IoB-изделий является уменьшение различий в результатах медицинского обслуживания за счёт уменьшения затрат на профилактику и диагностику, и упрощения доступа к ней, но неясно, *снизят ли эти технологии расходы на здравоохранение?* или *будут ли они доступны для всего населения?* В целом передовые технологии в здравоохранении способствовали увеличению общих прямых медицинских затрат [23].

Большинство новых медицинских IoB-изделий не могут войти в систему возмещения затрат по обязательному медицинскому страхованию до тех пор, пока не проведена оценка технологии здравоохранения [24], в рамках которой необходимо провести анализ «затраты-эффективность» и анализ влияния на бюджет [25]; и пока такие результаты не покажут, что эти медицинские изделия действительно улучшают краткосрочные и долгосрочные клинические исходы соразмерно их затратам. Для этого потребуется наличие релевантных доказательств. Нужно будет знать: проявляются ли эти преимущества во всех слоях населения (например, пожилые пациенты, которые могут быть менее технологически подкованы, группы населения с низким социально-экономическим статусом и так далее).

Кроме того, неравенство из-за барьеров доступа к цифровому здравоохранению и телемедицине может усугубиться для тех, у кого нет надёжного доступа в Интернет.

Свобода от медицинских IoB-изделий. По мере того, как медицинские IoB-изделия становятся всё более распространёнными, может возрастать количество людей, кто хочет жить своей жизнью с минимальной зависимостью от этих устройств или взаимодействием с ними [4].

Некоторые медицинские IoB-изделия могут собирать потенциально конфиденциальную информацию за пределами самого владельца. Например, кохлеарные имплантаты предназначены для записи звука, что может вызвать беспокойство по поводу конфиденциальности у лиц, которые не дали своего согласия на запись их голосов [4].

Наиболее вероятно, что насильственное внедрение технологии IoB произойдёт в системе уголовного правосудия. Например, FDA в 2017 году впервые одобрило использование электронной таблетки Abilify MyCite® (таблетки арипипразола с сенсором). Лекарственный препарат предназначен для лечения шизофрении, биполярного расстройства I типа отдельно или в сочетании с литием или вальпроатом для терапии острого маниакального или смешанного эпизода, поддерживающего лечения, большого депрессивного расстройства вместе с другими антидепрессантами [26]. Особенностью разработки является сенсор внутри таблетки, который реагирует на присутствие желудочного сока. После контакта с ним таблетка посылает сигнал на закрепляемый на груди электронный пластырь-датчик, который пересылает данные о времени приёма на его смартфон. Система работает, отправляя сообщение от сенсора внутри таблетки на носимый пластырь-датчик, который передаёт информацию в мобильное приложение, чтобы пациенты могли отслеживать приём лекарственного препарата на своём смартфоне, который, в свою очередь, пересылает данные в панель управления системы в компьютере [27]. Также, при желании пациента, эти данные могут автоматически пересылаться его близким или лечащему врачу (см. рис. 2).

Можно себе представить применение электронной формы таблетки арипипразола для стационарзамещающего лечения шизофрении и других психических расстройств по решению суда. Также медицинские IoB-изделия могут быть применены для тех, кто был арестован или осуждён за преступления, например, для отслеживания употребления наркотиков или других показателей предполагаемого девиантного поведения.

Автономность и целостность тела. Ещё одно этическое соображение касается прав пользователей на технологии, встроенные в их тела. Это право находится в потенциальном противоречии с попытками разработчиков технологий сохранить свои права на программное обеспечение и устройства.

Таблетка арипипразола с сенсором | **Пластырь-датчик** | **Мобильное приложение** | **Панель управления**

Рис. 2. Система Abilify MyCite®
Fig. 2. Abilify MyCite® System

Одним из примеров этого противоречия является *пользовательское соглашение*[3], которое разработчики программного обеспечения используют для ограничения того, что пользователь может делать с программным обеспечением после покупки [4].

Пользовательское соглашение может ограничивать модификацию программного обеспечения или ограничивать его использование для обеспечения предполагаемой производительности или защиты интеллектуальной собственности. Однако после того, как медицинское IoB-изделие имплантировано человеку, постоянный контроль над *проприетарным программным обеспечением*[4] разработчиком и над самим изделием может стать проблематичным. Например, когда разработчик принуждает пользователя подписать согласие на изменение политик использования данных, относящихся к изделию, которое уже было, и возможно навсегда, имплантировано в его тело. Некоторые будут утверждать, что люди имеют фундаментальное моральное право на автономию тела, и это право должно позволить им иметь полный контроль над своими устройствами как продолжением своего тела. Поскольку пользователи видят устройство как часть своего тела, они могут обоснованно полагать, что имеют право сопротивляться изменениям, внесённым разработчиком. Они также могут настаивать на возможности изменять изделие по своему усмотрению, взламывать его [4].

Заключение / Conclusion

Сегодня появляются проекты, разрабатывающие технологии нейроинтерфейса (*англ.* brain-computer interface; BCI) — набора программно-аппаратных комплексов, позволяющих управлять внешними устройствами (компьютером или экзоскелетом) напрямую с помощью электрических сигналов мозга, которые трансформируются в команды управления при помощи технологий искусственного интеллекта. Так, стартап Neuralink Илона Маска разрабатывает нейроинтерфейс подключения мозга к компьютеру. Компания уже успешно вживила обезьяне чип, позволяющий силой мысли играть в видеоигры. Главная цель всего проекта Neuralink — устранение последствий травм головного и спинного мозга и восстановление утраченных из-за них функций [29].

Заместитель председателя синодального отдела по взаимоотношениям церкви с обществом и СМИ Московского патриархата Вахтанг Кипшидзе заявил, что «отвечая на вопрос о возможности вживления в мозг человека микрокомпьютеров, я считаю важным различать случаи, когда любое устройство имплантируется в тело человека с целью исцеления болезни или облегчения состояния больного человека, который требует помощи, — это допустимо. И совершенно другое дело, когда электронные устройства нацелены на то, чтобы превратить человека в кибернетический механизм, интегрированный с другими электронными устройствами, что недопустимо. Мы считаем, что замысел Бога о человеке не предполагает его интеграцию с электронными устройствами. Человек уникален, и он не может стать частью электронной системы: слишком высоко для этого его Богом данное достоинство» [30].

Таким образом, современные реалии быстро развивающихся медицинских технологий, в том числе Интернета тела, требуют повышения осведомлённости об этических последствиях их применения в

[3] **Пользовательское соглашение** (или «лицензионное соглашение с конечным пользователем»; англ. end-user license agreement; EULA) — договор между владельцем компьютерной программы и пользователем её копии. Обычно используется вместе с проприетарным программным обеспечением, а также дистрибутивами свободного программного обеспечения с несвободными элементами.

[4] **Проприетарное программное обеспечение** (несвободное программное обеспечение) — программное обеспечение (ПО), являющееся частной собственностью авторов или правообладателей и не удовлетворяющее критериям свободного ПО. Правообладатель проприетарного ПО сохраняет за собой монополию на его использование, копирование и модификацию, полностью или в существенных моментах. Обычно проприетарным называют любое несвободное ПО, включая полусвободное.

здравоохранении. Члены Комитетов по этике при рассмотрении медицинских IoB-изделий должны сосредоточить своё внимание на то, в какой степени IoB подрывают принцип автономности человека, нарушают принцип анонимности и конфиденциальности данных. Назрела необходимо разработать руководящие принципы этической экспертизы медицинских IoB-изделий. Такие принципы могут помочь выявить пробелы в системе государственного регулирования оборота медицинских изделий, способствовать инновациям в разработке технологий и защитить все заинтересованные стороны.

Даже при отсутствии функции регулятивного принуждения разработчики IoB могут более чётко сообщать потребителям о рисках кибербезопасности и методах обеспечения конфиденциальности данных.

Поскольку разработчики IoB собирают огромные объёмы конфиденциальных данных, то им необходимо:

- чётко изложить политику конфиденциальности;
- получить от пользователя согласие на цели и методы сбора данных;
- указать срок, на который выдано согласие;
- предусмотреть и описать возможность отказа от определённых типов сбора или хранения данных;
- описать права на использование данные;
- привести информацию о праве собственности (владения) на полученные данные;
- описать, кому может или не может оператор персональных данных передать полученные данные (если да, то каким третьим лицам или сторонней организации, и требуется ли повторное получение согласия на обработку данных);
- предоставить (если уместно) информацию о трансграничной передаче данных;
- проинформировать о способе отзыва ранее выданного согласия;
- описать право на забвение.

Эти политики конфиденциальности должны прямо объяснять, как данные будут защищены, как эти данные будут использоваться и кому они могут быть предоставлены, принадлежать или быть проданы. Разработчики также должны информировать общественность о возможных рисках, связанных с медицинскими IoB-изделиями. Наконец, пациенты и потребители должны осознавать риски применения медицинских IoB-изделий и учитывать их при принятии решения об использовании таких устройств.

В отсутствии чётких российских нормативно-правовых актов потребителям следует проявлять осторожность и исходить из предположения, что после того, как данные будут собраны медицинским IoB-изделием, у потребителя вряд ли будет полный контроль над тем, как эти данные хранятся и используются, и потребитель должен быть готов к потенциальному нарушению конфиденциальности. В конечном счёте, потребители должны знать, что их персональные данные собираются организациями, которые не обязательно учитывают интересы потребителей. Повышение осведомлённости потребителей о медицинских IoB-изделиях и их рисках в такой ситуации имеет решающее значение.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ / ADDITIONAL INFORMATION

Конфликт интересов. Авторы заявляет об отсутствии конфликта интересов в отношении данной статьи. Авторы заявляют об отсутствии финансирования подготовки и написания данной статьи.

Conflict of interest. The authors declares that there is no conflict of interest in relation to this article. The author claims that there is no for preparing and writing this article.

СВЕДЕНИЯ ОБ АВТОРАХ ABOUT THE AUTORS

Хохлов Александр Леонидович
e-mail: al460935@yandex.ru
ORCID ID: 0000-0002-0032-0341
SPIN-код: 9389-8926
д. м. н., член-корр. РАН, зав. кафедрой клинической фармакологии и этики применения лекарств ЮНЕСКО ФГБОУ ВО «Ярославский государственный медицинский университет» Минздрава России, Россия, Ярославль

Белоусов Дмитрий Юрьевич
Автор, ответственный за переписку
e-mail: clinvest@mail.ru
ORCID ID: 0000-0002-2164-8290
SPIN-код: 6067-9067
Ведущий специалист ООО «Центр фармакоэкономических исследований», Россия, Москва

Khokhlov Alexander L.
e-mail: al460935@yandex.ru
ORCID ID: 0000-0002-0032-0341
SPIN code: 9389-8926
MD, Corresponding Member of the Russian Academy of Sciences, Professor, Head of the Department of the Clinical Pharmacology and ethical drugs utilization UNESCO, Yaroslavl State Medical University of the Ministry of Health of Russia, Russia, Yaroslavl

Belousov Dmitry Yu.
Corresponding author
e-mail: clinvest@mail.ru
ORCID ID: 0000-0002-2164-8290
SPIN code: 6067-9067
Leading specialist LLC «Center for Pharmacoeconomics Research», Russia, Moscow

Литература / References

1. Networking and Information Technology Research and Development, "Cyber-Physical System Interagency Working Group (2015) CPS Vision Statement," June 3, 2015. Режим доступа: https://clck.ru/U6Qe4

2. Andrea M. Matwyshyn, The Internet of Bodies, 61 Wm. & Mary L. Rev. 77 (2019). Режим доступа: https://clck.ru/U6Qev

3. Healey, Jason, Neal Pollard, and Beau Woods, "The Healthcare Internet of Things: Risks and Rewards," Atlantic Council, March 2015. Режим доступа: https://clck.ru/U6QfM

4. Lee Mary, Benjamin Boudreaux, Ritika Chaturvedi, Sasha Romanosky, and Bryce Downing. The Internet of Bodies: Opportunities, Risks, and Governance. Santa Monica, CA: RAND Corporation, 2020. Режим доступа: https://clck.ru/U6Qfo.

5. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 г. № 323-ФЗ (с изменениями на 22 декабря 2020 года) (редакция, действующая с 1 января 2021 года). [Federal Law "Ob osnovakh okhrany zdorov'ya grazhdan v Rossiyskoy Federatsii" dated November 21, 2011 No. 323-FZ (as amended on December 22, 2020) (as amended on January 1, 2021). (In Russ).] Режим доступа: https://clck.ru/U6fkm

6. Постановление Правительства РФ от 27 декабря 2012 года № 1416 Об утверждении Правил государственной регистрации медицинских изделий (с изменениями на 24 ноября 2020 года). [Resolution of the Government of the Russian Federation of December 27, 2012 No. 1416 On approval of the Rules for state registration of medical devices (as amended on November 24, 2020). (In Russ).] Режим доступа: https://clck.ru/UCDaq

7. Приказ Министерства здравоохранения России от 06.06.2012 № 4н (ред. от 07.07.2020) «Об утверждении номенклатурной классификации медицинских изделий» (вместе с «Номенклатурной классификацией медицинских изделий по видам», «Номенклатурной классификацией медицинских изделий по классам в зависимости от потенциального риска их применения») (Зарегистрировано в Минюсте России 09.07.2012 N 24852). [Order of the Ministry of Health of Russia dated 06.06.2012 No. 4n (as amended on 07.07.2020) "On approval of the nomenclature classification of medical devices" (together with the "Nomenclature classification medical devices by type "," Nomenclature classification of medical devices by classes depending on the potential risk of their use ") (Registered in the Ministry of Justice of Russia on 09.07.2012 N 24852). (In Russ).] Режим доступа: https://clck.ru/MHfdL

8. ГОСТ 31508-2012 Изделия медицинские. Классификация в зависимости от потенциального риска применения. Общие требования. Дата введения 2015-01-01. [GOST 31508-2012 Izdeliya medicinskie. Klassifikaciya v zavisimosti ot potencial'nogo riska primeneniya. Obshchie trebovaniya. Data vvedeniya 2015-01-01. (In Russ).] Режим доступа: https://clck.ru/UCDXp

9. Manadhata, Pratyusa K., and Jeannette M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software Engineering*, Vol. 37, No. 3, 2010, pp. 371—386. Режим доступа: https://clck.ru/UCRyJ

10. Beardsley, Tod, "R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump," Rapid7 blog, 2016. Режим доступа: https://clck.ru/U6Qhu

11. Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication," webpage, March 21, 2019b. Режим доступа: https://clck.ru/U6PXr

12. Serena Gordon. Healthday Reporter in MedicalXpress. Medtronic recalls some insulin pumps as FDA warns they could be hacked. June 28, 2019. Режим доступа: https://clck.ru/U6QiJ

13. Разработчик-диабетик собрал искусственную поджелудочную железу, работающую на JavaScript. 30 сен 2019. [A diabetic developer has built an artificial pancreas powered by JavaScript. 30 Sep 2019. (In Russ).] Режим доступа: https://clck.ru/U6Qii

14. Brown Dalvin. "Hacking Diabetes: People Break into Insulin Pumps as an Alternative to Delayed Innovations," USA Today, June 5, 2019. Режим доступа: https://clck.ru/U6QjF

15. The Open Artificial Pancreas System project (#OpenAPS). Режим доступа: https://openaps.org/

16. ГОСТ Р 52636-2006 Электронная история болезни. Общие положения (с поправкой). [GOST R 52636-2006 Elektronnaya istoriya bolezni. Obshchie polozheniya (s popravkoj). (In Russ).] Дата введения: 01.01.2008 г. Режим доступа: https://clck.ru/UCRyp

17. Caplan A, Friesen P (2017) Health disparities and clinical trial recruitment: Is there a duty to tweet? *PLoS Biol* 15(3): e2002040. https://clck.ru/UCRzV

18. Middletown homeowner facing felonies for house fire. The Journal-News. Jan 26, 2017. Режим доступа: https://clck.ru/U6Qjy

19. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ. [Federal Law "O personal'nyh dannyh" dated July 27, 2006 No. 152-FZ. (In Russ).] Режим доступа: https://clck.ru/DWym4

20. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в редакции от 1 января 2016 г.). [Federal Law "Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii" dated July 27, 2006 No. 149-FZ (as amended on January 1, 2016). (In Russ).] Режим доступа: https://clck.ru/U6XUT

21. Osoba, Osonde A., and William Welser IV, An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence, Santa Monica, Calif.: RAND Corporation, RR-1744-RC, 2017. Режим доступа: https://clck.ru/U6QkQ

22. Klitzman, Robert, Am I My Genes?: Confronting Fate and Family Secrets in the Age of Genetic Testing, Oxford, UK: Oxford University Press, 2012.

23. Callahan Daniel. Bioethics Briefing Book for Journalists, Policymakers, and Campaigns: Health Care Costs and Medical Technology, Garrison, N.Y.: The Hastings Center, 2008. Режим доступа: https://clck.ru/U6Quw

24. Оценка медицинских технологий, 2013 г. под общ. редакцией Белоусова Ю.Б. М: Издательство ОКИ, 40 стр. [Ocenka medicinskih tekhnologij. Ed by Belousov YuB. Moscow: Izdatel'stvo OKI. 2013. (In Russ).] Режим доступа: https://clck.ru/U6KXG

25. Включение лекарственных препаратов в ограничительные перечни: пошаговый алгоритм / под общ. ред. Белоусова Д. Ю., Зырянова С. К., Колбина А. С. — М.: Издательство ОКИ: Буки Веди, 2019. — 252 с.: ил. ISBN 978-5-4465-2555-3. [Vklyuchenie lekarstvennyh preparatov v ogranichitel'nye perechni: poshagovyj algoritm / Ed by. Belousov DYu, Zyryanov SK, Kolbin AS Moscow: Izdatel'stvo OKI: Buki Vedi, 2019. (In Russ).] Режим доступа: https://clck.ru/SRtoe

26. FDA approves pill with sensor that digitally tracks if patients have ingested their medication. November 13, 2017. Режим доступа: https://clck.ru/U6Qvc

27. How the ABILIFY MYCITE® System works. Режим доступа: https://clck.ru/U6Qvr

28. Приказ № 58н от 8 февраля 2013 г. Министерства здравоохранения Российской Федерации «Об утверждении положения о Совете по этике в сфере обращения медицинских изделий». Режим доступа: https://clck.ru/U6fm6

29. Reed Stevenson and River Davis. Elon Musk Says He Wired Up a Monkey's Brain to Play Video Games. *Bloomberg*. 1 февраля 2021 г. Режим доступа: https://clck.ru/VsAL7

30. В РПЦ с опасением отнеслись к идее вживлять микрочипы в мозг. *РИА НОВОСТИ*. 22.06.2021. [V RPTS s opaseniyem otneslis' k ideye vzhivlyat' mikrochipy v mozg. RIA NOVOSTI. 22.06.2021. (In Russ).] Режим доступа: https://clck.ru/Vs9sh

Поступила: 01.06.2021
Принята к публикации: 18.06.2021