Вестник Томского государственного университета. 2021. № 468. С. 243–252. DOI: 10.17223/15617793/468/28

УДК 343.3/.7

Л.Р. Клебанов, С.В. Полубинская

ЦИФРОВОЕ ЗДРАВООХРАНЕНИЕ, ПАНДЕМИЯ COVID-19 И ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Анализируются инструменты цифровых технологий в области здравоохранения, применяемые для оказания медицинской помощи, в том числе в условиях пандемии COVID-19. Рассматривается зарубежный опыт организации медицинской практики с помощью удаленного доступа, мобильной связи и «умных» устройств медицинского назначения. Дается анализ основных угроз кибербезопасности цифрового здравоохранения, определяются направления противодействия этим угрозам.
Ключевые слова: цифровое здравоохранение; пандемия COVID-19; медицинская помощь; телемедицина; устройства медицинского назначения; медицинские данные; конфиденциальность медицинских данных; кибератака; кибербезопасность.

Понятие и цели цифрового здравоохранения

В международных документах – резолюциях, планах действий, руководствах – совокупность различных форм и способов применения информационно-коммуникационных технологий в сфере охраны здоровья граждан именуется электронным здравоохранением (eHealth) или цифровым здравоохранением (digital health). Первый термин используется преимущественно в более ранних по времени принятия документах и раскрывается в одном из них как «использование [информационно-телекоммуникационных технологий] в продуктах, услугах и процессах здравоохранения в сочетании с организационными изменениями в системах здравоохранения и новыми навыками с целью улучшения здоровья граждан, эффективности и производительности при оказании медицинских услуг, а также экономической и социальной ценности здоровья» [1. P. 3].

Среди международных организаций «широчайшими правовыми полномочиями по решению глобальных проблем в области общественного здравоохранения» обладает Всемирная организация здравоохранения (ВОЗ) [2. P. 797]. В документах последнего времени ВОЗ оперирует понятием «цифровое здравоохранение». В содержание этого понятия включается электронное здравоохранение, в том числе использование мобильной беспроводной связи (mHealth), а также другие активно развивающиеся новые области, такие как сбор и обработка «Больших данных» (Big Data), компьютерные технологии в геномике и внедрение искусственного интеллекта [3. P. ix]. При этом надо заметить, что по смыслу термин «электронное здравоохранение» более точен, чем «цифровое здравоохранение», поскольку последний сужает область рассмотрения, оставляя за бортом аналоговые устройства, гибридные (аналогово-цифровые) устройства, а в перспективе предназначенные и для работы с «Большими данными» квантовые компьютеры, которые отнюдь не являются цифровыми. Однако ввиду широкой распространенности термина «цифровое здравоохранение» будем его использовать с оговоркой.

В Глобальной стратегии в области цифрового здравоохранения (2020–2025 гг.) цифровое здравоохранение определяется как «область знаний и практики, связанная с развитием и использованием цифровых технологий для улучшения здоровья», покрывая тем самым весь спектр применения высокотехнологичных устройств в решении задач охраны здоровья граждан. К ранее названным областям добавлены интернет вещей (IoT) (точнее было бы сказать – интернет медицинских вещей или IoMT), перспективные компьютерные технологии и робототехника [4. P. 5–6].

ВОЗ придает особое значение развитию цифрового здравоохранения, определяет его задачи и принципы. Так, 26 мая 2018 г. высший орган ВОЗ (Всемирная ассамблея здравоохранения) одобрила Резолюцию о цифровом здравоохранении, призывающую государства-члены «рассмотреть, при необходимости, как цифровые технологии могут быть интегрированы в существующие инфраструктуры систем здравоохранения и системы регулирования в целях усиления национальных и глобальных приоритетов в области здравоохранения путем оптимизации существующих платформ и услуг для усиления социальной направленности медицинской помощи и мер профилактики болезней, а также для снижения нагрузки на системы здравоохранения» [5].

Как подчеркивается в Глобальной стратегии, цифровое здравоохранение должно стать «неотъемлемой частью приоритетов в сфере охраны здоровья и приносить пользу людям с точки зрения этики и безопасности», а применение информационно-коммуникационных технологий – быть «безопасным, надежным, справедливым и устойчивым». Цифровые инновации в здравоохранении следует развивать на основе таких, среди прочих, принципов, как транспарентность, доступность, функциональная совместимость, конфиденциальность и безопасность [4. P. 5].

Целями цифрового здравоохранения, помимо повышения качества и доступности медицинских услуг, являются «предоставление индивиду центральной роли в заботе о своем здоровье и благополучии», «использование огромного потенциала данных в интересах охраны здоровья», а также содействие переходу «к прогностическим и профилактическим моделям оказания медицинской помощи» [6. С. 1–2].

В отношения в сфере цифрового здравоохранения вовлекается широкий круг субъектов, среди которых: а) пациенты и их законные представители; б) врачи и иные медицинские работники; в) организации, оказывающие медицинскую помощь, вне зависимости от хозяйственно-правовой формы и ведомственной принадлежности; г) уполномоченные органы, осуществ-

ляющие регулирование в сфере здравоохранения (федеральные и региональных); д) научное сообщество (этот сегмент представлен как научно-исследовательскими и образовательными учреждениями медицинского профиля, так и отдельными учеными и научными коллективами; е) аптечные организации; ж) страховые организации [7. С. 17–18].

Государственный контроль эффективности и безопасности цифровых технологий в здравоохранении

На практике цифровые инновации уже служат различным потребностям охраны здоровья граждан и включают, в том числе, организацию электронных сервисов для обращения в медицинские организации, ведение электронной медицинской документации, обеспечение адресной связи с конкретными пациентами и удаленного контроля состояния их здоровья, разработку системы поддержки клинических решений и организацию с помощью телемедицины консультаций специалистов высокой квалификации для пациентов и врачей, контроль производства и поставок изделий медицинского назначения и лекарственных средств, создание медицинских баз данных для совершенствования протоколов диагностики и лечения, проведения клинических испытаний и научных исследований. Перечень основных способов использования цифровых технологий в отрасли содержится в разработанной ВОЗ Классификации цифровых вмешательств в области здравоохранения v 1.0 [8].

В 2019 г. размер глобального рынка цифрового здравоохранения оценивался более чем в 106 млрд долл. По прогнозам до 2026 г., совокупный среднегодовой темп роста этого рынка составит 28,5%, а стоимость совокупных продаж достигнет 639,4 млрд долл. Прогнозируется рост продаж мобильных приложений для здоровья (на 28,9%), медицинского оборудования (на 31%) и услуг телемедицины (26,2%). Значительно меньший рост ожидается в рыночном сегменте медицинской аналитики (9,7%) [9].

Объем реализуемых на глобальном рынке продукции и услуг цифрового здравоохранения требует государственного регулирования отрасли в целях обеспечения качества, эффективности и безопасности внедряемых цифровых технологий. Одним из способов такого регулирования является разработка стандартов, которым такие технологии должны соответствовать. В национальных документах, нередко имеющих рекомендательный характер, но которым следуют на практике, специальное внимание уделяется контролю надежности, эффективности и безопасности устройств, используемых в медицинских целях, их защищенности от киберпосягательств, правилам надлежащей медицинской практики, а также защите медицинской информации [10–13]. Исключительная важность конфиденциальности медицинской информации, требующей «высоких стандартов [обеспечения] безопасности» таких персональных данных, особо отмечается на международном уровне [4. P. 6].

Исследование областей применения цифровых технологий в здравоохранении и требований к ним, уже ставших предметом регламентации в разных странах (США, Великобритания, Испания, Франция, Германия, Канада), показало, что число используемых для оценки технологий и устройств критериев варьируется от двух до десяти. Наиболее проверяемыми являются такие их качества, как безопасность, включая защищенность данных, клиническая эффективность, удобство использования и функциональная совместимость.

Внимание авторов руководящих принципов обращается и на экономические вопросы, в частности на стоимость внедрения технологии, однако ни в одном из изученных авторами исследования источников при принятии решения о применении не предлагались ни разработка технико-экономического обоснования такого решения, ни количественный анализ потенциальных убытков и прибыли.

В итоге авторы исследования установили, что более половины критериев, которые рекомендуются для оценки цифровых инноваций при их внедрении в практику здравоохранения, касаются преимущественно организационных последствий принятого решения, безопасности данных и технических характеристик. Такие критерии, как наличие остающихся без удовлетворения медицинских потребностей, а также учет правовых и этических аспектов использования технологии, встречались существенно реже (в трех, двух и одном из одиннадцати источников соответственно) [14].

Всего авторы исследования содержательно проанализировали одиннадцать руководств, содержащих рекомендуемые критерии оценки, три из которых относились к телемедицине, четыре – устанавливали требования к мобильным медицинским устройствам, и оставшиеся носили общий характер. Публикации для анализа, изданные за период с сентября 1998 г. по декабрь 2019 г., были отобраны в международных информационных базах Pubmed, Scopus, and Science Direct по ключевым словам «digital health interventions», «mhealth», «mobile health», «telemedicine», «health app» и «wearables» в сочетании с терминами «assessment», «guidelines», «checklist», «framework» и «consensus».

Сами авторы отмечают его определенную ограниченность. В частности, изученные ими рекомендации касались главным образом телемедицины и мобильных медицинских устройств и не относились к иным способам использования цифровых технологий, например, для поддержки клинических решений [14. P. 4]. Вместе с тем полученные результаты позволяют наметить пути развития и совершенствования государственного контроля в сфере цифрового здравоохранения.

Цифровое здравоохранение в условиях пандемии COVID-19

Пандемия новой коронавирусной инфекции (COVID-19) – острого респираторного заболевания, вызванного коронавирусом SARS-CoV-2, – послужила катализатором для более широкого использования цифровых технологий в здравоохранении. Не имеющая прецедентов нагрузка на национальные системы здравоохранения, введение карантинных и иных ограничений для граждан, которым на длительное

время запрещается покидать их дома, за исключением строго определенных случаев, серьезно снизили доступность для них медицинских услуг и сократили возможности решения имеющихся проблем со здоровьем. В этих условиях службам здравоохранения многих стран приходится искать новые способы как наблюдения за состоянием здоровья пациентов и оказания медицинской помощи, так и выполнения иных задач общественного здравоохранения. И здесь на помощь медицинским работникам приходят цифровые технологии, среди которых наиболее часто называются мобильные приложения и телемедицина.

Так, применительно к COVID-19 мобильные приложения предлагается использовать для самостоятельного контроля симптомов заболевания, отслеживания контактов инфицированных пациентов и подтверждения их выздоровления. В значительной степени эффективность этой технологии зависит от ее распространенности и согласия пациентов на использование, возможности подключения к мобильным сетям, организации системы обработки получаемых данных и безопасности их передачи. Телемедицина, в свою очередь, позволяет осуществлять дистанционное консультирование по широкому кругу медицинских проблем пациентов [15. P. 4].

Несколько уже получивших распространение в британской системе здравоохранения направлений и способов применения цифровых технологий в условиях пандемии получили отражение в научной литературе [16].

Во-первых, это использование мессенджеров и социальных сетей для организации предоставления медицинских услуг, ротации персонала в случаях заболевания либо самоизоляции, а также профессионального общения медицинских работников и обмена опытом диагностики и лечения заболевших COVID-19.

Во-вторых, цифровые технологии служат образовательным целям, когда требуется быстрое обучение медицинских работников уже подтвердившим свою результативность методам лечения и ухода за пациентами либо получение необходимых профессиональных знаний представителями непрофильных медицинских специальностей, участвующими в оказании помощи больным COVID-19.

И, наконец, такие технологии позволяют разработать и внедрить новые модели ухода и медицинской помощи, включая удаленный контроль состояния здоровья пациента и проведение врачебных консультаций. Эти модели позволяют существенно сократить риск заражения COVID-19 для пациентов и предотвратить дальнейшее распространение инфекции. Отмечается, что «подавляющее большинство посещений клиник заменено методами дистанционного консультирования, начиная от базовых консультаций по телефону до более сложных видеоконференций на основе телемедицины или мобильных приложений» [16. P. 2]. В формате видеоконференций теперь проводятся и собрания мультидисциплинарных медицинских бригад, что, в свою очередь, снижает риски распространения вируса среди медицинского персонала.

По тому же пути идет и американское здравоохранение. В более чем 50 медицинских системах, объединяющих больницы и другие медицинские организации, к весне 2020 г. были созданы и работали программы телемедицины. Для лечебных учреждений, где такие программы отсутствовали, имелась возможность прибегнуть в порядке аутсорсинга к помощи других организаций, оказывающих подобные услуги (например, Teladoc Health, American Well, к примеру) [17. P. 1679].

Примером медицинской практики при удаленном доступе является деятельность медицинской системы Partners Healthcare в Новой Англии – регионе на северо-востоке США. Входящие в систему медицинские организации еще до появления COVID-19 предоставляли дистанционную медицинскую помощь в следующих формах: виртуальные визиты, предполагающие контакт между пациентом и специалистом в режиме реального времени; виртуальные консультации, представляющие собой видеоконтакты в реальном времени между специалистом, направившим пациента на консультацию, и телеконсультантом-экспертом; электронные визиты, заключающиеся в безопасном (по защищенным каналам связи) обмене информацией между специалистом и пациентом; электронные консультации с получением мнения второго профессионала, когда информацией обмениваются медицинские специалисты. Мнение второго эксперта запрашивается в сложных случаях, при наличии комплекса медицинских проблем и обширной медицинской документации пациента [18. P. 2].

В перспективе, связанной с продолжением пандемии COVID-19, предполагается обеспечивать удаленное наблюдение за пациентами на дому, включая находящихся на карантине с угрозой ухудшения их состояния, ввести структурированные клинические опросники на портале организации и расширить дистанционную специализированную медицинскую поддержку с помощью электронных консультаций. В медицинской системе считают, что «инструменты виртуальной медицинской помощи, если они внедряются быстро и надежно, могут помочь снизить показатели распространения COVID-19 и позволить… здравоохранению обеспечивать [такую] помощь в течении более длительного времени без превышения своих возможностей» [18. P. 3].

Специалисты отмечают, что до пандемии телемедицина в США не получила должного развития. Проведенный в 2019 г. опрос руководителей медицинских организаций, входящих в систему здравоохранения США, показал, что 38% из них не включали внедрение цифровых технологий в стратегический план развития организации. В качестве факторов, ограничивающих распространение цифровых технологий в здравоохранении, 94% опрошенных указали установленные правила защиты данных и конфиденциальности медицинской информации и предписания федерального закона о мобильной передаче данных и ответственности в области медицинского страхования (Health Insurance Portability and Accountability Act или HIPAA) 1996 г. Положения этого закона распространены на цифровые технологии в здравоохранении в соответствии с федеральным Законом о медицинских информационных технологиях для экономического и

клинического здоровья (Health Information Technology for Economic and Clinical Health Act или HITECH) 2009 г. [19. P. e82(1)].

С целью снижения нагрузки на национальную систему здравоохранения, порожденную пандемией COVID-19, в литературе высказывались предложения о смягчении установленных законодательством требований, затрагивающих цифровые технологии. Такое решение позволило бы обеспечить их более широкое применение, например, для организации «стационаров на дому», медицинской поддержки больных COVID-19 и других пациентов, требующих постоянного контроля за состоянием здоровья, а также мониторинга соблюдения карантинных ограничений [19. P. e82(2)].

В этой связи надо отметить, что в соответствии с принятым 6 марта 2020 г. федеральным законом о дополнительных ассигнованиях на обеспечение готовности к коронавирусу и реагирования на него (Coronavirus Prepardness and Response Supplemental Appropriations Act) действие ряда требований HIPAA было временно приостановлено, а число случаев, допускающих обращение в медицинские учреждения с помощью телемедицины, расширено [20; 21. P. e470].

Европейская комиссия, в свою очередь, сообщила о поддержке тринадцати проектов по использованию цифровых технологий в здравоохранении, направленных на борьбу с пандемией, которые «обеспечат новые решения для защиты медицинских работников, быстрого обнаружения и предотвращения распространения COVID-19, а также для улучшения интенсивной терапии». Проекты с общим объемом финансирования 55,2 млн евро рассчитаны на два года с появлением первых результатов в течение ближайших 6-12 месяцев [22].

Криминальные риски для кибербезопасности цифрового здравоохранения

На основе анализа многочисленных сообщений о кибератаках в сфере организации и оказания медицинской помощи, зафиксированных в разных странах, можно выделить их основные типы, по сути, раскрывающие криминальные риски цифрового здравоохранения:

– нападения на организации системы здравоохранения (лечебные, диагностические, научные и образовательные медицинские структуры, фармацевтические лаборатории, учреждения управления здравоохранением и т.д.);

– атаки на устройства, относящиеся к интернету медицинских вещей, гаджеты, приборы и девайсы, подключенные, в том числе, и к локальным сетям организаций здравоохранения, а также медицинские цифровые платформы;

– похищение и разглашение конфиденциальной медицинской информации, существующей в цифровом формате, сотрудниками медицинских организаций, имеющими доступ к такой информации.

Рост использования цифровых технологий, особенно в условиях пандемии, увеличивает число объектов для посягательств. Надо заметить, что национальные системы здравоохранения и организации, обладающие персональными медицинскими данными, страдали от кибератак и ранее.

Применительно к организациям здравоохранения специалистами выделяются три основных типа нападений – цифровое вымогательство, DDoS-атаки и взлом информационных систем, где хранится конфиденциальная информация (data breaches). Как показывает практика, вне зависимости от вида атаки для совершения любого из них, как правило, используются вредоносные бот-системы (The Big Bad Bot) [23].

Цифровое вымогательство является одним из наиболее часто встречающихся киберпреступлений, вне зависимости от его объекта. Преступление совершается с помощью специального вредоносного программного обеспечения (ransomware). Исследования показывают, что цифровое вымогательство имеет тенденцию к росту и угрожает любым организациям, независимо от сферы их деятельности и географической локации. Так, по оценкам IBM Security X-Force, в сентябре 2020 г. каждая из четырех кибератак совершалась с помощью ransomware. Всплеск преступной активности пришелся на июнь – именно тогда была совершена одна треть всех подобных преступлений от общего числа киберпосягательств, зарегистрированных в 2020 г. Наибольшее число цифровых вымогательств было зафиксировано в Азии, Северной Америке и Европе – соответственно 33, 30 и 27%. Опасность такого преступления определяется его кумулятивными преступными последствиями. Преступники сначала похищают важную информацию у компаний-«потерпевших» перед тем, как подвергнуть эту информацию шифрованию, а потом, если вымогатели не добиваются выкупа за дешифровку данных, то они предают эту информацию огласке [24]. Вымогательские атаки сопровождаются не только похищением информации, но и выводом из строя сервисов медицинских услуг.

Только за 2016 г. 7/8 от общего числа случаев цифрового вымогательства в США совершалось в отношении организаций здравоохранения [25]. В 2017 г. в результате распространения вредоносного вируса-вымогателя WannaCry была нарушена работа государственной Национальной службы здравоохранения в Англии. Ее ключевые системы оказались заблокированы, не позволяя медицинскому персоналу получить доступ к данным о пациентах и важным медицинским сервисам [26]. В 2019 г. в США подобным атакам подверглись 764 организации, предоставляющие медицинскую помощь, – пациентов, нуждающихся в срочной помощи (emergency patients), пришлось переводить в другие больницы, медицинские карты стали недоступны, а некоторые были просто утеряны, хирургические операции отменены, медицинские обследования перенесены, сервисы служб спасения недоступны [27].

Прошлый год ознаменовался тяжким резонансным киберпреступлением: была зарегистрирована первая смерть в результате цифрового вымогательства, которому подвергся университетский госпиталь в Дюссельдорфе (Германия). Преступники осуществили атаку с помощью вируса, поразившего 30 серверов

госпиталя. Системы обеспечения его деятельности были выведены из строя, и пациентов, нуждающихся в срочной помощи, пришлось отправлять в другие больницы. Одна из пациенток, находящаяся в крайне тяжелом состоянии, была перевезена в Вупперталь – за 20 миль от Дюссельдорфа. Женщина скончалась, не получив своевременно необходимую помощь [27].

Еще одним трендом преступной деятельности цифровых вымогателей стал выбор школ, университетов и академических институтов в качестве целей своих атак, что неудивительно, поскольку школы и иные учебные заведения из-за пандемии COVID-19 перешли на дистанционный либо смешанный формат обучения [24]. В группе риска (universities-targets, schools-targets) оказались и медицинские образовательные учреждения.

Второй вид нападений на организации здравоохранения – DDoS-атаки – также делает невозможным предоставление медицинских услуг. Так, DDoS-атака на детский госпиталь в Бостоне, когда многие больничные сервисы, в том числе электронная запись пациентов, вышли из строя, продолжалась неделю [23].

Что касается взлома информационных систем организаций здравоохранения с целью хищения значимой информации (sensitive information), то «популярность» таких преступлений вполне объяснима – больницы, поликлиники, медицинские центры, фармацевтические компании аккумулируют огромные объемы информации (персональные данные пациентов, истории их болезней, номера медицинских страховок, номера кредитных карт). Хакеры, получив эти данные, могут использовать их для совершения других преступлений либо просто продать информацию в Даркнете [23].

Как правило, в случае совершения DDoS-атак вредоносные бот-сети отправляют массовые скоординированные запросы на сайты медучреждений, что в итоге приводит к обрушению компьютерной сети организации. Если организация не сможет отфильтровать атакующий трафик, то сбой в работе продлится ровно столько, сколько захотят сами преступники. В тех случаях, когда замышляется цифровое вымогательство либо взлом компьютерных систем медицинских организаций с целью хищения конфиденциальной информации, преступники осуществляют предварительную разведку на предмет выявления уязвимостей (vulnerability scans). С этой целью хакеры тоже используют бот-сети – они позволяют производить автоматическое сканирование через интернет для поиска уязвимых систем, а когда они будут найдены, хакеры начинают прямые атаки тем или иным способом [23].

Так, в 2015 г. преступники похитили 80 млн учетных документов из американской медицинской страховой компании Anthem. В 2018 г. были украдены медицинские данные 1,5 млн жителей Сингапура, включая премьер-министра страны [26]. В июне 2019 г. от крупной утечки персональных данных почти 20 млн пациентов пострадало Американское медицинское агентство по медицинским счетам и взысканию долгов (AMCA). В открытый доступ попали имена, даты рождения, адреса, телефоны, даты обращения за медицинской помощью и лечебные учреждения, ее оказавшие, а также сведения о кредитных картах и банковских счетах клиентов. В результате финансовых потерь и последствий юридического характера агентство стало банкротом. В октябре того же года после четырех хакерских атак на компьютерную систему организации Tu Oka Compass Health в Новой Зеландии были похищены медицинские данные почти миллиона человек [28. P. 9, 11]. В том же году 95% организаций здравоохранения в США сообщили о том, что они стали мишенью различных кибератак. Злоумышленники пытались не только получить неправомерный доступ к конфиденциальной медицинской информации пациентов, но и нарушить систему поставок медицинского оборудования и вмешаться в медицинскую деятельность [29. P. 3].

С началом пандемии число киберпосягательств на медицинские организации выросло. Так, в апреле 2020 г. Google сообщил о примерно 18 миллионах вредоносных программ и фишинговых электронных писем в связи с COVID-19. Осенью того же года Агентство кибербезопасности и защиты инфраструктуры (CISA), Департамент здравоохранения и социальных служб (NSS) США и ФБР опубликовали совместный документ по вопросам кибербезопасности, в котором предупреждали о распространении вредоносных программ-вымогателей. В дальнейшем стало известно о десятках американских больниц, подвергшихся атаке требующего выкуп вируса-вымогателя Ryuk, сходного с уже известным WannaCry [29. P. 3].

Рост числа угроз кибербезопасности системы здравоохранения США подтверждается и результатами опроса 168 специалистов по кибербезопасности в этой сфере, который в 2020 г. провела американская неправительственная организация Healthcare Information and Management Systems Society (HIMSS).

Выяснилось, что большинство подобных организаций уже сталкивались с серьезными посягательствами, совершенными путем удаленного доступа. Основными способами атак был фишинг, в том числе по электронной почте, вымогательство (требования выкупа) и попытки получить доступ к информации с использованием средств социальной инженерии – злоупотребления доверием либо обмана, когда, например, мошенник выдает себя за другое лицо. Злоумышленники направляли свои действия по преимуществу на финансовую информацию, персональные данные сотрудников организации и на медицинскую информацию о пациентах. Типичными последствиями подобных действий стали сбои в работе информационных систем пострадавших организаций и нарушения в предоставлении медицинских услуг, нередко из-за повреждения соответствующих компьютерных систем и устройств [30. P. 2].

Если говорить о наиболее резонансных цифровых нападениях, которым в год пандемии подверглись организации здравоохранения по всему миру, то необходимо упомянуть атаки хакеров-вымогателей на госпиталь в Брно (Чехия), парижскую госпитальную систему, больницы в Испании и Таиланде, клиники в различных штатах США, в частности в Техасе. Атакам подверглись и регуляторы в рассматриваемой

сфере – департамент здравоохранения штата Иллинойс. Не избежала такой участи даже ВОЗ, но самым трагичным стало уже упомянутое хакерское нападение на госпиталь в Дюссельдорфе, повлекшее смерть пациентки, – первый в мире зарегистрированный случай человеческой жертвы компьютерного преступления [31].

Еще одной тенденцией того же года были нападения хакеров на медицинские и фармацевтические организации (научные центры и лаборатории), которые целенаправленно работали над созданием вакцины от COVID-19. Как отмечают специалисты IBM, семь ведущих компаний и ученых-исследователей в разных странах мира (Канада, Франция, Индия, Южная Корея, США), создающих вакцину и проводящих клинические испытания, стали мишенями для цифровых атак [31].

Актуальной угрозой цифровому здравоохранению также являются кибератаки (реальные или потенциальные) на различные медицинские гаджеты, девайсы, электронные устройства, многие из которых относятся к интернету медицинских вещей, либо на специализированные цифровые платформы.

В медицинской литературе предлагаются различные классификации подобных устройств. По одной из них к ним относятся: 1) измерительные приборы (measurement products); 2) инвазивные приборы (intervention products); 3) комбинированные измерительно-инвазивные приборы. Первый тип включает приборы, фиксирующие медицинские показатели, например, исследующие голос больных, страдающих болезнью Паркинсона, с тем, чтобы выявить изменения тремора, либо переносные устройства, позволяющие измерять частоту сердечных сокращений во время занятий бегом; второй тип охватывает инсулиновые помпы, вшитые кардиостимуляторы и т.п.; третий – глюкометры, которые осуществляют постоянный мониторинг состояния лиц, больных диабетом, и через специальные приложения отправляют данные их лечащим врачам [32. P. 34–35].

Для более ясного понимания объектов киберпосягательств предлагается следующая классификация устройств медицинского назначения:

1. Соединенные с интернетом устройств (connected devices), которые могут быть двух видов – носимые (переносные) устройства (wearable devices) и устройства, которые не являются носимыми (nonwearable devices). В специальной литературе к первому виду относят те из них, которые работают по принципу «пассивного сбора данных». Речь идет о находящихся на теле пациента приборах для измерения кровяного давления, температуры тела, частоты дыхания, количества пройденных шагов и т.д.

Второй вид представлен «умными» медицинскими приборами (smart medical devices), которые непригодны к ношению и работают по принципу «активного сбора данных». Таким является, например, CYCORE – устройство, состоящее из сенсоров и мобильных приложений, предназначенное для удаленного сбора информации и оценки состояния здоровья пациентов, страдающих от раковых образований головы и шеи и подверженных риску обезвоживания во время курса радиотерапии. Комплект датчиков состоит из подключенных весов и манжеты для измерения кровяного давления и пульса, отправляющих показатели в общую базу данных. При тестировании устройства пациенты использовали его два раза с интервалом в пять дней в период лечения, при этом они заполняли и отправляли с помощью смартфона электронную анкету, описывая имеющиеся у них признаки обезвоживания. Было установлено, что CYCORE эффективно фиксировал симптомы дегидратации во время обоих периодов исследования [33. P. 2–4].

Кибератаки на подобные устройства способны привести к самым тяжелым последствиям, что требует особого внимания к их защищенности. Так, в 2017 г. Управление по контролю качества пищевых продуктов и лекарственных препаратов США (FDA) отозвало полмиллиона кардиостимуляторов из-за их уязвимости к цифровым атакам [34. P. e61].

2. Цифровые платформы для сбора данных о пациентах. Одной из таких платформ является Distress Assessment and Response Tool platform (DART), которая представляет собой действующую в режиме самоотчета скрининговую систему, собирающую данные по формам Patient Health Questionnaire-9, Patient Depression Questionnaire-9 и Social Difficulties Inventory-21 [33. P. 4–5].

3. Устройства, используемые в телемедицине, объединяющей аудио- и видео технологии в целях дистанционного взаимодействия с пациентом и двустороннего обмена информацией [33. P. 5–6].

4. Чатботы (chatbots) и «умные помощники» (intelligent assistants). Chatbot – это основанная на системе искусственного интеллекта компьютерная программа, созданная для общения с людьми в режиме диалога (in a conversational manner). «Умные помощники» – это технологии на основе искусственного интеллекта и нейросетей, дающие ответы на голосовой запрос (Amazon's Alexa, Google's Assistant, Microsoft's Cortana, Apple's Siri). Кроме того, цифровые помощники способны передавать информацию с помощью текстовых сообщений: СМС, через мессенджеры, мобильные приложения, Web-страницы и т.д. [33. P. 6–7].

5. Медицинские девайсы, не имеющие доступа в интернет, но подключенные к локальным сетям медицинских организаций. Уязвимость таких устройств продемонстрировало исследование израильских специалистов по кибербезопасности в сфере здравоохранения.

Как известно, компьютерная томография (КТ) и магнитно-резонансная томография (МРТ) служат эффективными диагностическими методами, и каждый год по всему миру проводятся миллионы таких исследований. Томографы (сканеры) подключены к внутренним локальным сетям, а центральный сервер медицинской организации получает и хранит соответствующие снимки с тем, чтобы предоставить их потом врачам. Сегодня уже существуют вредоносные программные технологии, созданные на основе искусственного интеллекта, которые позволяют искажать изображения снимков, сделанных при томографии. Например, фальсифицируется изображение легких онкологического больного так, что на снимке ни-

каких следов рака легких не остается. И наоборот, здоровому человеку снимок может выдать «ложную» картину заболевания. Исследование показало, что, изучая фальсифицированные снимки, комиссия из трех специалистов-рентгенологов «приняла за чистую монету» изображения и мнимого здоровья (94% случаев) и мнимой болезни (99% случаев). Но даже после того, как врачей предупредили о фальсификации снимков, при повторном их изучении удельный вес ошибок составил 60 и 87% соответственно. Сотрудник Университета имени Бен-Гуриона (Бэер-Шева, Израиль) И. Мирский провел эксперимент – с согласия руководства медицинских учреждений он незаметно проникал в отделения томографии и подключал специальное устройство для перехвата данных с томографов, передаваемые по локальной сети. Вся «миссия» заняла у него 30 секунд. Эксперимент касался томографии онкобольных, но такая технология может быть использована для искажения снимков при любом заболевании. Использовать ее можно при совершении цифровых вымогательств, страхового мошенничества и в иных преступных целях [34, 35].

Криминальную угрозу цифровому здравоохранению представляет и разглашение конфиденциальной медицинской информации, существующей в цифровом формате. Источниками таких угроз могут быть не только внешние вмешательства, к примеру хакерские атаки, но и внутренние, неправомерные действия, совершаемые сотрудниками медицинских организаций (медицинскими работниками, техническими специалистами, обслуживающими компьютерные системы, и т.п.). Среди случаев, когда простая невнимательность медицинского персонала приводила к утечке конфиденциальных данных, – телефонный пранк (розыгрыш) в отношении медицинской сестры лондонского госпиталя короля Эдуарда VII, где находилась Кейт Миддлтон – супруга принца Уильяма. Два диджея австралийской радиостанции позвонили в регистратуру госпиталя и, имитируя британский акцент, представились королевой Елизаветой II и принцем Чарльзом, после чего спросили о состоянии здоровья герцогини Кембриджской. Медицинская сестра в регистратуре, не распознав обмана, соединила их со старшей медицинской сестрой. Старшая медсестра тоже не увидела подвоха и сообщила мнимым членам монаршего дома конфиденциальную медицинскую информацию, после чего радиостанция выдала в эфир запись разговоров с медиками [36. P. 977].

Не так давно скандал случился в российском здравоохранении – в интернете оказались персональные данные около 100 тысяч пациентов московских больниц, переболевших коронавирусом (имена, номера телефонов, паспортные данные, номера полисов медицинского страхования, домашние адреса, а также информация, составляющая медицинскую тайну). В мэрии Москвы заявили, что в утечке виноват «человеческий» фактор – сотрудники, которые занимались обработкой служебных документов, передали их третьим лицам. Всего «ушло» данных общим объемом в 1 Гб (362 файла в формате Word, Excel, PDF, JPG). Некоторые файлы формата PDF и JPG содержали данные медицинского осмотра пациентов. Было установлено, что организация, создавшая эти файлы, – департамент информационных технологий Москвы, руководитель которого Э. Лысенко заявил, что взломов и другого несанкционированного вмешательства в работы IT-систем не было, а следовательно, причина утечки – человеческий фактор [37].

Противодействие киберугрозам для цифрового здравоохранения

Реально наступающие и отдаленные тяжкие последствия кибератак на организации здравоохранения, все шире использующие цифровые технологии, делают противодействие таким преступным посягательствам первоочередной и жизненно важной задачей в буквальном смысле слова. Не исключая других сфер разработки и осуществления мер противодействия подобным преступлениям, полагаем, что приоритетными являются право, техника и образование.

К *правовым мерам* необходимо отнести, прежде всего, регламентацию правового режима цифрового здравоохранения, а также совершенствование уголовного законодательства как на национальном, так и на международном уровне, включая заключение соответствующих соглашений. Адаптация национального уголовного права может осуществляться через институты как Общей, так и Особенной части, в том числе с помощью введения в закон новых обстоятельств, отягчающих наказание, и конструирования специальных норм об ответственности за компьютерные преступления в сфере здравоохранения. Крайне важное значение имеют локальные нормативные акты, принятые в конкретной медицинской или иной организации, с правилами, среди прочего, «цифровой гигиены» для сотрудников. *Технические меры* играют решающую роль в обеспечении кибербезопасности системы здравоохранения. Такие меры должны включать в себя программные, аппаратные, программно-аппаратные средства противодействия. С учетом того, какие угрозы (внутренние или внешние) необходимо нейтрализовать, конкретные технологии и средства предупреждения могут варьироваться. К техническим мерам относятся также процедуры стандартизации и контроля перед получением разрешения на применение цифровых устройств медицинского назначения и использование технологии «блокчейн» для защиты медицинской информации. *Образовательные меры* должны включать регулярные мероприятия информационно-образовательного характера с медицинским персоналом и иными сотрудниками медицинских организаций, использующими в своей деятельности цифровые технологии. Необходимо разрабатывать соответствующие руководства по кибербезопасности для организаций здравоохранения.

Выводы

Результаты проведенного исследования приводят к следующим выводам:

– цифровое здравоохранение получает все большее распространение в мире и в России, и, учитывая скорость развития и внедрения цифровых технологий,

недалеко время, когда такие технологии станут общепринятым, вполне обыденным инструментом охраны здоровья граждан;

– организации здравоохранения подвергаются и будут подвергаться кибератакам, зачастую посягающим одновременно на несколько объектов уголовно-правовой охраны: общественную безопасность, собственность, жизни и здоровье, а также конституционные права граждан, безопасность сбора, хранения и обращения компьютерной информации;

– пандемия COVID-19 послужила катализатором роста киберпосягательств на организации здравоохранения;

– кибервойны с участием государств перестали быть фантастикой, что не исключает возможные кибердиверсии в отношении национальных систем здравоохранения в целом, как и отдельных ее структурных единиц, например, нападения на объекты военной медицины;

– корыстные мотивы лежат в основе всей массы зарегистрированных сегодня киберпосягательств в сфере здравоохранения (вымогательства, кражи персональных данных), что объясняется повышающейся капитализацией здравоохранения;

– уголовное право (как на международном, так и на национальном уровне) должно немедленно отреагировать на криминальные угрозы кибербезопасности здравоохранения (спектр возможных средств широк от заключения соответствующих международных соглашений до включения способа совершения преступлений в число отягчающих ответственность обстоятельств);

– происходит оформление отдельного направления в теории и практике кибербезопасности – кибербезопасность здравоохранения, что требует развития соответствующей индустрии, продукция которой (техническая, программная, информационная, образовательная) была бы направлена на снижение рисков цифровых угроз именно для этой деятельности;

– необходимо сотрудничество ученых различных специальностей с тем, чтобы противодействие криминальным цифровым угрозам в сфере здравоохранения имело основательный научный фундамент.

ЛИТЕРАТУРА

1. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century. COM (2012) 736 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0736&from=EN (дата обращения: 17.12.2020).
2. Meier B.M., Taylor A. Eccleston-Turner M. et al. The World Health Organization in Global Health Law // The Journal of Law, Medicine & Ethics. 2020. Vol. 48, Is. 4. P. 796–799. DOI: 10.1177/1073110520979392
3. WHO guideline: recommendations on digital interventions for health system strengthening. Geneva : World Health Organization, 2019. URL: https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1 (дата обращения: 17.12.2020).
4. WHO. Global strategy on digital health 2020–2025. URL: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf (дата обращения: 17.12.2020).
5. Digital health. Resolution WHA71.7. May 2018. URL: https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf?ua=1 (дата обращения: 17.12.2020).
6. Report of the WHO Symposium on the Future of Digital Health Systems in the European Region. Copenhagen, Denmark, 6–8 February 2019. URL: https://apps.who.int/iris/bitstream/handle/10665/329032/9789289059992-eng.pdf (дата обращения: 19.12.2020).
7. Карпов О.Э., Субботин С.А., Шишканов Д.В., Замятин М.Н. Цифровое здравоохранение. Необходимость и предпосылки // Врач и информационные технологии. 2017. № 3. С. 6–22.
8. Classification of digital health interventions v 1.0. A shared language to describe the uses of digital technology for health. URL: https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06-eng.pdf (дата обращения: 17.12.2020).
9. Digital Health Market Share Trends 2020-2026 Growth Report. Global Market Insights. Insights to Innovation. URL: https://www.gminsights.com/industry-analysis/digital-health-market (дата обращения: 11.01.2021).
10. FDA Guidances with Digital Health content. URL: https://www.fda.gov/medical-devices/digital-health-center-excellence/guidances-digital-health-content (дата обращения: 9.01.2021).
11. Criteria for health app assessment. URL: https://www.gov.uk/government/publications/health-app-assessment-criteria/criteria-for-health-app-assessment (дата обращения: 9.01.2020).
12. A guide to good practice for the use of digital technology in health and care. URL: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (дата обращения: 09.01.2021).
13. Information Security Management: NHS Code of Practice. URL: https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice (дата обращения: 9.01.2021).
14. Kolasa K., Kozinski G. How to Value Digital Health Interventions? A Systematic Literature Review // International Journal of Environmental and Public Health. 2020. Vol. 17, Is. 6. Art. 2119. DOI: 10.3390/ijerph17062119
15. Maedar A.J., Bidargaddi N.P., Williams P.A.H. Contextualising Digital Health to Fighting the COVID-19 Pandemic // Journal of International Society for Telemedicine and EHealth. 2020. Vol. 8. Art. e3. DOI: 10.29086/JISfTeH.8.e3
16. Robbins T., Hudson S., Ray P. et al. COVID-19: A new digital dawn? // Digital Health. 2020. Vol. 6. P. 1–3. DOI: 10.1177/2055207620920083.
17. Hollander J.E., Carr B.G. Virtually Perfect? Telemedicine for Covid-19 // New England Journal of Medicine. 2020. Vol. 382, № 18. P. 1679–1681. DOI: 10.1056/NEJMp2003539
18. Schwamm L.H., Erskine A., Licurse A. A digital embrace to blunt the curve of COVID19 pandemic // NPJ Digital Medicine. 2020. Vol. 3. Art. № 64. DOI: 10.1038/s41746-020-0279-6.
19. Keesara S., Jonas A., Schulman K. Covid-19 and Health Care's Digital Revolution // New England Journal of Medicine. 2020. Vol. 382, № 23. P. e82(1)-e82(3). DOI: 10.1056/NEJMp2005835
20. Coronavirus Prepardness and Response Supplemental Appropriations Act. H.R. 6074. URL: https://www.congress.gov/bill/116th-congress/house-bill/6074/text?q=%7B%22search%22%3A%5B%22coronavirus+preparedness+and+response+supplemental+appropriations+act%22%5D%7D&r=1&s=2 (дата обращения: 11.01.2021).
21. Loeb A.E., Rao S.S., Ficke J.R. et al. Departmental Experience and Lessons Learned With Accelerated Introduction of Telemedicine During the COVID-19 Crisis // Journal of American Academy of Orthopaedic Surgeons. 2020. Vol. 28, № 11. P. e469-e476. DOI: DOI: 10.5435/JAAOS-D-20-00380
22. European Commission. Shaping Europe's digital future. Digital health technologies addressing the pandemic. URL: https://ec.europa.eu/digital-single-market/en/digital-health-technologies-addressing-pandemic (дата обращения: 11.01.2021).
23. Hayardeny E. Protecting healthcare organizations from cyberattacks // Security. 2020. Dec. 4. URL: https://www.securitymagazine.com/articles/94087-protecting-healthcare-organizations-from-cyberattacks (дата обращения: 11.01.2021).

24. Singleton C., Kiefer C., Villadsen O. Ransomware 2020: Attack Trends Affecting Organizations Worldwide // Security Intelligence. 2020. Sept. 28. URL: https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/ (дата обращения: 21.01.2021).
25. Blinder A., Perlroth N. Hard Choice for Cities Under Cyberattack: Whether to Pay Ransom // New York Times. URL: https://www.nytimes.com/2018/03/29/us/atlanta-cyberattack-ransom.html (дата обращения: 15.01.2021).
26. Ghafur S., Grass E., Jennings N.R., Darzi A. The challenges of cybersecurity in health care: the UK National Health Service as a case study // The Lancet Digital Health. 2019. Vol. 1, № 1. P. e10–e12. DOI: 10.1016/S2589-7500(19)30005-6
27. Eddy M., Perloth N. Cyber Attack Suspected in German Woman's Death // The New York Times. 2020. Sept. 18. URL: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (дата обращения: 22.01.2021).
28. Cyber Security Report. 2020. Check Point Software Technologies LTD. URL: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf (дата обращения: 14.01.2021).
29. BD 2020 Cybersecurity Report. Improving cybersecurity collaboration across the industry. URL: https://cybersecurity.bd.com/ documents/Cybersecurity/BD_BD-2020-Cybersecurity-Report_EN.pdf (дата обращения: 14.01.2021).
30. 2020 HIMSS Cybersecurity Survey. Healthcare Information and Management Systems Society. URL: https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf (дата обращения: 14.01.2021).
31. Burt T. Cyberattacks targeting health care must stop. 2020. Nov. 13. URL: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (дата обращения: 22.01.2021).
32. Coravos A., Goldsack J.C., Karlin D.P. et al. Digital Medicine: A Primer on Measurement // Digital Biomarkers. 2019. Vol. 3, № 2. P. 31–71. DOI: 10.1159/000500413
33. Garg S., Williams N.L., Ip A., Dicker A.P. Clinical Integration of Digital Solutions in Health Care: An Overview of the Current landscape of Digital technologies in Cancer Care // JCO Clinical Cancer Informatics. 2018. Vol. 2. P. 1–9. DOI: 10.1200/CCI.17.00159
34. Burki T. The dangers of the digital age // The Lancet Digital Health. 2019. Vol. 1, № 2. P. e61–e62. DOI: 10.1016/S2589-7500(19)30032-9
35. Zetter K. Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists // The Washington Post. 2019. April 3. URL: https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?fbclid=IwAR2sE8kdnrlVW-YxPI2F3S0jFe7nzujxZq5-QNDSbrYBsOJ4idTlESFORa4&noredirect=on (дата обращения: 15.01.2021).
36. Taitsman J.K., Grimm C.M., Agrawal S. Protecting Patient Privacy and Data Security // The New England Journal of Medicine. 2013. Vol. 368, № 11. P. 977–979. DOI: 10.1056/NEJMp1215258
37. В сети оказались личные данные 100 тыс. московских пациентов // Новости Mail.ru. URL: https://news.mail.ru/society/44491151/ (дата обращения: 22.01.2021).

Статья представлена научной редакцией «Право» 13 мая 2021 г.

Digital Health, COVID-19 Pandemic, and Cybersecurity Issues

Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal, 2021, 468, 243–252.
DOI: 10.17223/15617793/468/28

Lev R. Klebanov, Peoples' Friendship University of Russia (Moscow, Russian Federation). E-mail: solomon70@bk.ru
Svetlana V. Polubinskaya, Institute of State and Law of the Russian Academy of Sciences (Moscow, Russian Federation). E-mail: svepol@yandex.ru

Keywords: digital health; COVID-19 pandemic; medical care; telemedicine; medical devices; medical data; medical data confidentiality; cyberattack; cybersecurity.

The article focuses on a wide range of cybersecurity issues related to the use of digital technologies in healthcare. Many countries are increasingly adopting digital innovations into their national health systems and therefore raise their cybersecurity risks. The number of cyberattacks on health care organizations is steadily increasing; and the COVID-19 pandemic, which has required more frequent use of digital technologies to address public health challenges, has also influenced the proliferation of criminal cyberattacks. The aim of the study was to describe the main types of criminal, mostly digital, risks for digital health and identify the most important ways to counteract them. The article includes an analysis of international and national regulatory documents, foreign scientific literature, reports of organizations dealing with cybersecurity issues. In preparing it, the authors used general and specific scientific methods including analysis, synthesis, formal and legal analysis, historical method, interdisciplinary research, and expert assessment. The authors conclude that the increasing use of digital technologies in health care, especially in the context of the COVID-19 pandemic, expands the number of targets for cybercriminals. Three main types of digital health criminal risks are identified: attacks on health care organizations, attacks on devices used for medical purposes, including those associated with the Internet of Medical Things, and the theft and disclosure of digitally stored confidential medical information. The latter group of acts is committed by both outsiders and employees of healthcare organizations. The vast majority of registered cybercrimes are profit motivated ones, and the most common cybercrime is extortion with the use of malicious software (ransomware). To counter criminal risks for digital health, the authors propose a set of actions divided into three groups such as legal, technical, and educational. According to the authors, international and national criminal law should immediately respond to digital criminal threats to healthcare systems, in particular by making relevant international agreements and by including the manner in which such crimes are committed into criminal laws as an aggravating circumstance. In addition, the authors note the formation of a special direction in cybersecurity research and practice – healthcare cybersecurity – which requires the development of an appropriate industry, with respective hardware, software, informational and educational products that would be aimed at eliminating and reducing the risks for digital health.

REFERENCES

1. European Commission. (2012) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century. COM (2012) 736 final*. [Online] Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0736&from=EN (Accessed: 17.12.2020).
2. Meier, B.M. et al. (2020) The World Health Organization in Global Health Law. *The Journal of Law, Medicine & Ethics.* 48 (4). pp. 796–799. DOI: 10.1177/1073110520979392
3. WHO. (2019) *WHO guideline: recommendations on digital interventions for health system strengthening*. Geneva: World Health Organization. [Online] Available from: https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1 (Accessed: 17.12.2020).

4. WHO. (2021) *Global strategy on digital health 2020–2025.* [Online] Available from: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf (Accessed: 17.12.2020).
5. WHO. (2018) *Digital health. Resolution WHA71.7. May 2018*. [Online] Available from: https://apps.who.int/gb/ebwha/pdf_files/WHA71/A71_R7-en.pdf?ua=1 (Accessed: 17.12.2020).
6. WHO. (2019) *Report of the WHO Symposium on the Future of Digital Health Systems in the European Region*. Copenhagen, Denmark, 6–8 February 2019. [Online] Available from: https://apps.who.int/iris/bitstream/handle/10665/329032/9789289059992-eng.pdf (Accessed: 19.12.2020).
7. Karpov, O.E. et al. (2017) Digital Public Health. Necessity and Background. *Vrach i informatsionnye tekhnologii – Information Technologies for the Physician.* 3. pp. 6–22. (In Russian).
8. WHO. (2018) *Classification of digital health interventions v 1.0. A shared language to describe the uses of digital technology for health.* [Online] Available from: https://apps.who.int/iris/bitstream/handle/10665/260480/WHO-RHR-18.06-eng.pdf (Accessed: 17.12.2020).
9. Global Market Insights. Insights to Innovation. (2021) *Digital Health Market Share Trends 2020–2026 Growth Report.* [Online] Available from: https://www.gminsights.com/industry-analysis/digital-health-market (Accessed: 11.01.2021).
10. FDA. (2021) *FDA Guidances with Digital Health content.* [Online] Available from: https://www.fda.gov/medical-devices/digital-health-center-excellence/guidances-digital-health-content (Accessed: 09.01.2021).
11. GOV.UK. (2017) *Criteria for health app assessment*. [Online] Available from: https://www.gov.uk/government/publications/health-app-assessment-criteria/criteria-for-health-app-assessment (Accessed: 9.01.2020).
12. GOV.UK. (2021) *A guide to good practice for the use of digital technology in health and care.* [Online] Available from: https://www.gov.uk/government/publications/code-of-conduct-for-data-driven-health-and-care-technology/initial-code-of-conduct-for-data-driven-health-and-care-technology (Accessed: 09.01.2021).
13. GOV.UK. (2007) *Information Security Management: NHS Code of Practice*. [Online] Available from: https://www.gov.uk/government/publications/information-security-management-nhs-code-of-practice (Accessed: 9.01.2021).
14. Kolasa, K. & Kozinski, G. (2020) How to Value Digital Health Interventions? A Systematic Literature Review. *International Journal of Environmental and Public Health.* 17 (6). Art. 2119. DOI: 10.3390/ijerph17062119
15. Maedar, A.J., Bidargaddi, N.P. & Williams, P.A.H. (2020) Contextualising Digital Health to Fighting the COVID-19 Pandemic. *Journal of International Society for Telemedicine and EHealth.* 8. Art. e3. DOI: 10.29086/JISfTeH.8.e3
16. Robbins, T. et al. (2020) COVID-19: A new digital dawn? *Digital Health.* 6. pp. 1–3. DOI: 10.1177/2055207620920083.
17. Hollander, J.E. & Carr, B.G. (2020) Virtually Perfect? Telemedicine for Covid-19. *New England Journal of Medicine*. 382 (18). pp. 1679–1681. DOI: 10.1056/NEJMp2003539
18. Schwamm, L.H., Erskine, A. & Licurse, A. (2020) A digital embrace to blunt the curve of COVID19 pandemic. *NPJ Digital Medicine.* 3 (64). DOI: 10.1038/s41746-020-0279-6
19. Keesara, S., Jonas, A. & Schulman, K. (2020) Covid-19 and Health Care's Digital Revolution. *New England Journal of Medicine.* 382 (23). pp. e82(1)–e82(3). DOI: 10.1056/NEJMp2005835
20. 116th Congress. (2020) *Coronavirus Prepardness and Response Supplemental Appropriations Act. H.R. 6074*. [Online] Available from: https://www.congress.gov/bill/116th-congress/house-bill/6074/text?q=%7B%22search%22%3A%5B%22coronavirus+preparedness+and+response+supplemental+appropriations+act%22%5D%7D&r=1&s=2 (Accessed: 11.01.2021).
21. Loeb, A.E. et al. (2020) Departmental Experience and Lessons Learned With Accelerated Introduction of Telemedicine During the COVID-19 Crisis. *Journal of American Academy of Orthopaedic Surgeons.* 28 (11). pp. e469–e476. DOI: DOI: 10.5435/JAAOS-D-20-00380
22. European Commission. (2020) *Shaping Europe's digital future. Digital health technologies addressing the pandemic*. [Online] Available from: https://ec.europa.eu/digital-single-market/en/digital-health-technologies-addressing-pandemic (Accessed: 11.01.2021).
23. Hayardeny, E. (2020) Protecting healthcare organizations from cyberattacks. *Security*. Dec. 4. [Online] Available from: https://www.securitymagazine.com/articles/94087-protecting-healthcare-organizations-from-cyberattacks (Accessed: 11.01.2021).
24. Singleton, C., Kiefer, C. & Villadsen, O. (2020) Ransomware 2020: Attack Trends Affecting Organizations Worldwide. *Security Intelligence*. Sept. 28. [Online] Available from: https://securityintelligence.com/posts/ransomware-2020-attack-trends-new-techniques-affecting-organizations-worldwide/ (Accessed: 21.01.2021).
25. Blinder, A. & Perlroth, N. (2018) Hard Choice for Cities Under Cyberattack: Whether to Pay Ransom. *New York Times.* [Online] Available from: https://www.nytimes.com/2018/03/29/us/atlanta-cyberattack-ransom.html (Accessed: 15.01.2021).
26. Ghafur, S. et al. (2019) The challenges of cybersecurity in health care: the UK National Health Service as a case study. *The Lancet Digital Health.* 1 (1). pp. e10–e12. DOI: 10.1016/S2589-7500(19)30005-6
27. Eddy, M. & Perloth, N. (2020) Cyber Attack Suspected in German Woman's Death. *The New York Times.* Sept. 18. [Online] Available from: https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (Accessed: 22.01.2021).
28. Check Point Software Technologies LT D. (2020) *Cyber Security Report.* [Online] Available from: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf (Accessed: 14.01.2021).
29. BD. (2020) *Cybersecurity Report. Improving cybersecurity collaboration across the industry.* [Online] Available from: https://cybersecurity.bd.com/documents/Cybersecurity/BD_BD-2020-Cybersecurity-Report_EN.pdf (Accessed: 14.01.2021).
30. Healthcare Information and Management Systems Society. (2020) *2020 HIMSS Cybersecurity Survey*. [Online] Available from: https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf (Accessed: 14.01.2021).
31. Burt, T. (2020) *Cyberattacks targeting health care must stop.* Nov. 13. [Online] Available from: https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/ (Accessed: 22.01.2021).
32. Coravos, A. et al. (2019) Digital Medicine: A Primer on Measurement. *Digital Biomarkers*. 3 (2). pp. 31–71. DOI: 10.1159/000500413
33. Garg, S. et al. (2018) Clinical Integration of Digital Solutions in Health Care: An Overview of the Current landscape of Digital technologies in Cancer Care. *JCO Clinical Cancer Informatics.* 2. pp. 1–9. DOI: 10.1200/CCI.17.00159
34. Burki, T. (2019) The dangers of the digital age. *The Lancet Digital Health*. 1 (2). pp. e61–e62. DOI: 10.1016/S2589-7500(19)30032-9
35. Zetter, K. (2019) Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists. *The Washington Post.* April 3. [Online] Available from: https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?fbclid=IwAR2sE8kdnrlVW-YxPI2F3S0jFe7nzujxZq5-QNDSbrYBsOJ4idTlESFORa4&noredirect=on (Accessed: 15.01.2021).
36. Taitsman, J.K., Grimm, C.M. & Agrawal, S. (2013) Protecting Patient Privacy and Data Security. *The New England Journal of Medicine.* 368 (11). pp. 977–979. DOI: 10.1056/NEJMp1215258
37. Novosti Mail.ru. (2020) *V seti okazalis' lichnye dannye 100 tys. moskovskikh patsientov* [The personal data of 100 thousand Moscow patients leaked to the web]. [Online] Available from: https://news.mail.ru/society/44491151/ (Accessed: 22.01.2021).

Received: 13 May 2021