ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ МЕДИЦИНЫ И АКТУАЛЬНОСТИ ЕЕ ИЗУЧЕНИЯ В ВЕДОМСТВЕННЫХ ВУЗАХ

DOI: 10.25629/HC.2021.04.07

Демаков В.И.[1], Рерке В.И.[2], Портная Я.А.[1], Ракитский В.В.[3]

[1]Иркутский государственный медицинский университет

[2]Иркутский государственный университет. Педагогический институт

[3]Восточно-Сибирский институт МВД России

Аннотация. В статье показаны роль и актуальность использования средств и методов соблюдения информационной безопасности в сфере медицины, в особенности в условиях глобальной цифровизации врачебной деятельности. Быстро увеличивающиеся в объемах массивы данных о различных медицинских параметрах требуют не только обеспечения качества информации, выражающегося в достоверности, релевантности, актуальности, доступности, но и постоянного мониторинга выполнения требований их защищенности. Создание единого информационного медицинского пространства сначала на национальном уровне, а затем и на международном, разработка стандартизированных автоматизированных рабочих мест для специалистов, с соблюдением всех требований защиты конфиденциальных данных, позволит существенно повысить эффективность работы медицинских организаций, а также может способствовать повышению доверия пациентов к врачебной деятельности.

Ключевые слова: информационная безопасность, образовательный процесс, конфиденциальность персональных данных, автоматизированные рабочие места, цифровая медицина.

Введение

Внезапно возникшие сложности, с которыми мы столкнулись в ушедшем году в ходе противостояния распространению нового вируса, показали, насколько важнó объединение усилий всего общества для повышения эффективности любых противоэпидемиологических мероприятий. Широкий спектр проводимых внутри медицинских организаций работ по раннему выявлению больных с COVID-19, а также межведомственное взаимодействие с медицинскими организациями, все это связано с обменом разнообразной информацией о количестве заболевших, клиническими характеристиками нозологических групп, а также с профилактическими и лечебными методами воздействия и т.д. Внедрение в медицинскую отрасль передовых направлений математической и программной инженерии, способствует накоплению, обработке и анализу значительных объемов данных. Кроме того, масштаб распространения вирусной инфекции сразу поставил профессиональное медицинское сообщество перед необходимостью не ограничиваться национальными рамками, а выстраивать полноценное международное сотрудничество по всем направлениям – от клинических до научно-исследовательских. Активная разработка и внедрение дистанционных методов профилактики, диагностики, лечения и реабилитации с применением телемедицины, быстрое развитие смежных отраслей, обеспечивающих эффективность работы медицинских организаций, существенно расширяют экономические ресурсы. Это касается, например, фармацевтической отрасли, логистических компаний и т.п. Существенно возросшие, в условиях пандемии, объёмы научно-исследовательских работ в области иммунологии, генетики и молекулярной биологии, приводят к созданию глобальных баз данных, которыми активно пользуется все мировое сообщество. Кроме того, весь мировой экономический уклад неизбежно перестраивается на цифровой мотив, что влечет переход на массовое использование электронных ресурсов. Глобализация автоматизации обработки данных подводит российское общество к реализации идеи, которая была заложена авторами федерального закона «О персональных данных» [1] еще в 2006 году – к созданию единого федерального реестра персональной информации с целью его использования всеми государственными структурами.

Все эти процессы приводят к активной и широкой цифровизации медицины, созданию единого информационного пространства.

Гипотеза

Переход на электронную обработку информации в этой области должен сопровождаться качественными решениями по обеспечению информационной безопасности, а также исследованиями в области кибербезопасности на уровне федеральных центров обработки данных (ЦОДов), которые объединены квантовыми коммуникациями. Действительно, данные, находящиеся в медицинских массивах, требуют повышенной защиты. Помимо персональной информации [1, 2], необходимо соблюдать и врачебную тайну [3, 4], а в некоторых обстоятельствах речь идет о национальной безопасности, в том случае, когда утечка сведений может повлечь массовые панические настроения.

Обсуждение

Однако, насколько эффективны меры, направленные на обеспечение информационной безопасности, насколько подготовлены в этой сфере медицинские работники, насколько готовы к обучению в данном направлении ведомственные образовательные организации?

Отметим, что по данным отчета InfoWatch [5] за 9 месяцев 2020 в мире зафиксировано на 7,4% меньше утечек персональных данных, чем за аналогичный период предыдущего года. При этом, в России этот же показатель возрос на 5,7%.

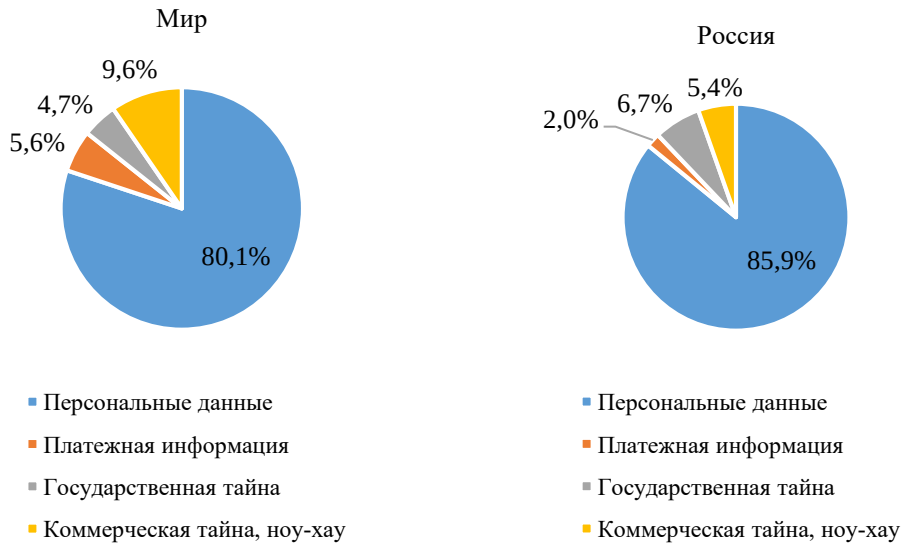

Рисунок 1 – Распределение утечек по типам данных за 1 полугодие 2020 года [5]

На круговых диаграммах рисунка 1 видно, что в первом полугодии 2020 года были выявлены факты утечки информации, составляющей коммерческий интерес, а также государственную тайну. Однако, подавляющее большинство компрометации допущено в отношении персональных данных. Напомним, что государственной тайной [6] считается такая информация, разглашение которой может нанести ущерб государственной безопасности. Так, например, в Италии на один день раньше была допущена утечка данных о планах правительства закрыть север страны на карантин с 9 марта. В итоге, начиная с 8 марта население не только Милана, но и других северных городов в состоянии паники хлынуло на юг страны.

В Китае неизвестный под псевдонимом THE0TIME выставил на продажу данные китайской компании Huiying Medical Technology, которая на основе искусственного интеллекта разрабатывает технологии выявления коронавирусной инфекции [7]. Помимо пользовательских данных, хакер украл исходный код технологии обнаружения COVID-19, а также данные экспериментальных работ. За всю информацию злоумышленник просит 4 биткойна (примерно

$31 тыс.). Разработанная Huiying технология, позволяет по снимкам компьютерного томографа диагностировать формы пневмонии и определить симптомы заболевания коронавирусом у пациента. По собственным данным компании, ее решение позволяет выявить COVID-19 с точностью до 96% [7]. Перечисленные утечки стали возможны из-за случаев краж телефонов, содержащих секретные сведения и персональные данные.

Данные примеры иллюстрируют значимость решения проблемы информационной безопасности населения. Подчеркнем, что любая информация – персональная, а в особенности связанная с медицинской сферой, весьма дорого стоит на черном рынке [8].

Из отчета Hi-Tech Crime Trends 2020-2021 [9] следует, что, если в мире 52,6% случаев утечек спровоцированы внешними воздействиями, то в России более 79% утечек случились в результате внутренних нарушений (рис. 2).

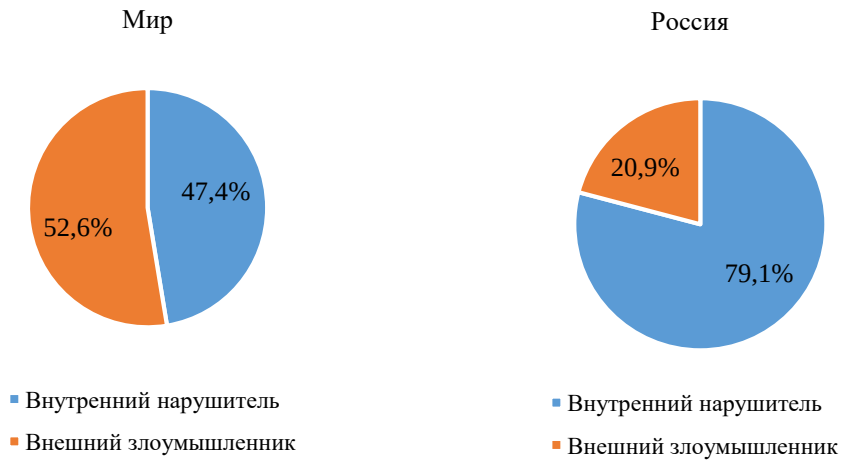

Рисунок 2 – Распределение утечек по вектору воздействия (январь-сентябрь 2020 г.)

Так, из рисунка 2 видно, что в России доля распространения компрометации данных по вине внутренних работников почти вдвое выше, чем в мире. В глобальном распределении по различным отраслям наибольшее количество зафиксированных утечек приходится на сектор высоких технологий – 19,4%, а на втором месте здравоохранение – 16,4%.

Здесь уместно отметить, что около 16% выявленных фактов компрометации конфиденциальных данных в Российской Федерации происходит через мессенджеры [9]. Можно предположить, что данная ситуация возникает в следствие того, что в настоящее время у сотрудников нет другой удобной технической возможности для оперативного обмена информацией с коллегами. Кроме того, наблюдается отсутствие специализированных программных средств или автоматизированных рабочих мест, а также защищённых каналов связи для обработки и передачи служебной информации. В свою очередь использование привычных для персонала мобильных приложений и социальных сетей [10], при отсутствии навыков обеспечения информационной безопасности, создает для пользователей иллюзию безопасного обмена данными.

Несмотря на вышеперечисленные проблемы, требования к обеспечению мер информационной безопасности непрерывно повышаются. Министерством цифрового развития, связи и массовых коммуникаций подготовлен федеральный проект «Информационная безопасность», направленный на обеспечение устойчивости и безопасности информационной инфраструктуры, конкурентоспособности отечественных разработок и технологий информационной безопасности и формирования эффективной системы защиты прав и законных интересов личности, бизнеса и государства от угроз информационной безопасности [10]. Создан российский центр Государственной системы обнаружения, предупреждения и ликвидации последствий

компьютерных атак (ГосСОПКА) [11], перед которым поставлены задачи инвентаризации информационных ресурсов, выявления уязвимостей и анализа угроз, реагирования на инциденты и ликвидацию последствий фактов утечек охраняемой законом информации, а также повышение квалификации персонала, работающего с конфиденциальными данными.

В настоящее время ведется активная разработка автоматизированных медицинских информационных систем (МИС). Можно отметить такие разработки как: МИС «МедАнгел» компании «Angels IT» [12], МИС «Medesk» компании «Medesk», МИС «Medods» компании «СофтСервис», МИС «Renovatio» компании «Реновацио Софт», МИС «Инфоклиника» компании «Смарт Дельта Системс» и другие. Создана Ассоциация Развития Медицинских Информационных Технологий (АРМИТ) [13], которая своей целью отмечает – создание рынка медицинских информационных технологий и единого информационного пространства в сфере цифрового здравоохранения. Благодаря деятельности Ассоциации в регионах России создаются медицинские информационно-аналитические центры (МИАЦ). Сегодня усилиями региональных МИАЦ выполняется функция интерактивной связи с населением по проблемам противодействия распространению короновирусной инфекции.

Тем не менее, на данный момент подобные системы не поддерживают четкого единообразия и стандартизации в интерфейсах, в процессах и форматах обработки и передачи данных, и поэтому не могут рассматриваться как единое программное решение федерального уровня, а, следовательно, проблема выстраивания единого медицинского профессионального электронного пространства по-прежнему актуальна.

Также остро стоит вопрос о создании защищенного ресурса для внутриведомственного обмена медицинской информацией. Как пример подобного решения, можно привести опыт министерства внутренних дел, где с 2005 года велась работа над созданием единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, а позднее, с марта 2012 года – федеральной системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Важнейшим компонентом этого комплекса является телекоммуникационная структура, обеспечивающая информационное взаимодействие всех подразделений правоохранительной системы на территории России. Передача служебной информации по каналам связи внутри ИСОД МВД России осуществляется в зашифрованном виде, обеспечивая на должном уровне информационную безопасность ресурсов. Единый формат обработки данных позволяет надстроить ИСОД многочисленными прикладными сервисами, едиными для всех подразделений. Возможность изучения данных программных решений в образовательной системе МВД России позволяет выпускать специалистов, подготовленных к эффективной работе с подобными автоматизированными системами. Кроме этого, во всех образовательных программах подготовки сотрудников для правоохранительной системы уже около 20 лет содержится дисциплина «Основы информационной безопасности», что позволяет рассчитывать на пополнение российских силовых структур кадрами, обладающими навыками информационной культуры.

В тоже время в рамках подготовки медицинских специалистов данная тематика не находит должного отражения в учебных программах обучения. Так, в подавляющем большинстве медицинских университетов России в образовательных программах присутствуют лишь дисциплины: «Медицинская информатика» – для специальностей 31.05.01 «Лечебное дело», 31.05.02 «Педиатрия», 31.05.03 «Стоматология»; «Информатика» – для специальности 33.05.01 «Фармация». В рамках данных учебных дисциплин тематика зашиты защиты информации практически не раскрыта. Таким образом, основная масса выпускников с медицинским образованием не имеют представления о проблеме обеспечения информационной безопасности. С недавнего времени в образовательной программе всех специальностей появилась дисциплина «Информационно-образовательные технологии в специальности», которая, по-нашему, мнению будет способна реализовать новых подход к проблеме защиты о персональных данных.

Нельзя не отметить, что в отдельных медицинских университетах в учебных планах некоторых специальностей заявлены такие дисциплины как «Информатика, современные информационные технологии» (ФГБОУ ВО «Волгоградский государственный медицинский университет»

Минздрава России). В рамках данной дисциплины студенты знакомятся с вопросами обеспечения сетевой безопасности, принципами выстраивания комплексных систем безопасности, криптографии, формирования и использования электронной подписи. ФГАОУ ВО Первый МГМУ имени И.М. Сеченова Минздрава России знакомит студентов с проблемами обеспечения информационной безопасности в рамках дисциплины «Информатика». В ФГБОУ ВО «Новосибирский государственный медицинский университет» Минздрава России для специальности 30.05.01 «Медицинская биохимия» преподается дисциплина «Основы информационной безопасности».

Таким образом, сегодня можно сформулировать следующие причины, приводящие к большому количеству утечек конфиденциальной информации в области здравоохранения:

– отсутствие единых специализированных программных продуктов федерального уровня для обеспечения работы медицинских работников;

– отсутствие защищенных каналов передачи информации ограниченного распространения;

– недостаточный уровень информационной культуры медицинских работников и отсутствие достаточных навыков в области информационной безопасности.

Без решения данных проблем сложно рассчитывать на эффективное взаимодействие с международным сообществом в области науки и здравоохранения, а также на внедрение передовых достижений, безусловно использующих методы моделирования и обработки больших массивов данных.

Неслучайно, на базе Первого московского МГМУ им. И.М. Сеченова, совместно с Институтом системного программирования имени В.П. Иванникова, Институтом конструкторско-технологической информатики РАН, Научно-исследовательским институтом биомедицинской химии имени В.Н. Ореховича и Новгородским государственным университетом имени Ярослава Мудрого создается научный центр мирового уровня (НЦМУ) «Цифровой биодизайн и персонализированное здравоохранение», который будет в период с 2020 по 2025 годы реализовывать проект, направленный на цифровизацию здравоохранения и-управление здоровьем населения. Активное участие медицинских вузов всей страны в работе подобных центров позволит вовлекать студентов в решение проблем информатизации медицинской деятельности.

Считаем, что реализация учебных дисциплин, основанных на изучении передовых информационных технологий, в частности, проблем обеспечения информационной безопасности в образовательном процессе медицинских вузов, позволит отечественному здравоохранению обеспечивать качественную защиту персональных данных пациентов на высоком уровне и реализовывать сетевое взаимодействие между медицинскими организациями как внутри региона, так и на уровне РФ.

Библиография

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 20.02.2021).

2. Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 г. № 1119 [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения 20.02.2021).

3. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21 ноября 2011 года № 323-ФЗ» (в ред. от 31.07.2020 № 303-ФЗ) // Российская газета, № 263(5639), 23 ноября 2011 г.

4. Лопаткина, Н.В. Правовое регулирование врачебной тайны и защиты персональных данных как фактор обеспечения безопасности личности, общества, государства / Н.В. Лопаткина // Право. Безопасность. Чрезвычайные ситуации. – 2015. – № 2 (27). – С. 19.

5. Ресурс ИТ-решений для анализа информационных потоков и предотвращения утечек корпоративных данных, обеспечения кибербезопасности автоматизированных промышленных систем и защиты бизнес-приложений от уязвимостей и кибератак: [Электронный ресурс]. URL: https://www.infowatch.ru/ (дата обращения 20.02.2021).

6. Федеральный закон «О государственной тайне» от 21.07.1993 № 5485-1 (ред. от 30.12.2020) // Собрание законодательства Российской Федерации, № 41.

7. Портал компании Huiying Medical: [Электронный ресурс]. URL: https://www.intel.ru/content/www/ru/ru/artificial-intelligence/posts/huiying-medical-covid19.html (дата обращения 20.02.2021).

8. Цены «Чёрного рынка» на российские персональные данные [Электронный ресурс]. – Режим доступа: https://www.devicelock.com/ (Дата обращения: 20.02.2021).

9. Ресурс для детектирования и предотвращения кибератак, выявления фрода и защиты интеллектуальной собственности в сети. Система сбора данных о киберугрозах Group-IB: [Электронный ресурс]. URL: https://www.group-ib.ru/ (дата обращения 20.02.2021).

10. Рерке, В. И. Критерии и показатели информационной социализации студентов посредством социальных сетей / В. И. Рерке, В. И. Демаков, Я. А. Портная // Социальная реальность виртуального пространства: материалы I Международной научно-практической конференции. ФГБОУ ВО ИГУ. – Иркутск, 2019. – С. 169-176.

11. Постановление Правительства РФ от 7 октября 2019 г. № 1285 "Об утверждении Правил предоставления субсидий из федерального бюджета на создание отраслевого центра Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА) и включение его в систему автоматизированного обмена информацией об актуальных киберугрозах".

12. Медицинская информационная система «МедАнгел»: [Электронный ресурс]. URL: https://medangel.angelsit.ru/ (дата обращения 20.02.2021).

13. Ассоциация развития медицинских информационных технологий: [Электронный ресурс]. URL: http:// https://armit.ru/ (дата обращения 20.02.2021).

ON ENSURING INFORMATION SECURITY IN THE SPHERE OF MEDICINE AND THE RELEVANCE OF ITS STUDY IN DEPARTMENTAL UNIVERSITIES

DOI: 10.25629/HC.2021.04.07

Demakov V.I.[1], Rerke V.I.[2], Portnaia I.A.[1], Rakitskiy V.V.[3]

[1]Irkutsk State Medical University

[2]Irkutsk State University. Pedagogical Institute

[3]East-Siberian Institute of the Ministry of Internal Affairs of Russia

Abstract. The article shows the role and relevance of the use a means and methods of information security in the field of medicine, especially in the context of the global digitization of medical activity. The rapidly growing arrays of data on various health parameters requires not only quality assurance in terms of reliability, relevance, relevance and accessibility, but also continuous monitoring of compliance with their security requirements. A creation of a single medical information space and standardized automated workstations for specialists, with all the requirements for the protection of confidential data, will make it possible to increase the efficiency of medical organizations, and can also help to increase patients' trust in medical activities.

Keywords: information security, educational process, privacy of personal data, automated workplaces, digital medicine.

References

1. Federal Law "On Personal Data" dated July 27, 2006 No. 152-FZ (as amended on December 31, 2017) [Electronic resource]. Access mode: http://www.consultant.ru/document/cons_doc_LAW_61801/ (date of access 20.02.2021). In Rus.

2. Decree of the Government of the Russian Federation "On approval of requirements for the protection of personal data during their processing in personal data information systems" dated 01.11.2012, No. 1119 [Electronic resource]. Access mode: http://www.consultant.ru/document/cons_doc_LAW_137356/ (date of access 20.02.2021). In Rus.

3. Federal Law "On the Basics of Health Protection of Citizens in the Russian Federation" dated November 21, 2011 No. 323-FZ "(as amended on July 31, 2020 No. 303-FZ) // *Rossiyskaya Gazeta*, No. 263 (5639), November 23 2011 r. In Rus.

4. Lopatkina N.V. [Legal regulation of medical secrecy and personal data protection as a factor in ensuring the safety of an individual, society, and the state]. *Law. Security. Emergencies*. 2015. No. 2 (27). P. 19. In Rus.

5. *Resurs IT-reshenii dlya analiza informatsionnykh potokov i predotvrashcheniya utechek korporativnykh dannykh, obespecheniya kiberbezopasnosti avtomatizirovannykh promyshlennykh sistem i zashchity biznes-prilozhenii ot uyazvimostei i kiberatak* [Resource of IT solutions for analyzing information flows and preventing corporate data leaks, ensuring cybersecurity of automated industrial systems and protecting business applications from vulnerabilities and cyber attacks]. URL: https://www.infowatch.ru/ (date of treatment 02.20.2021). In Rus.

6. Federal Law "On State Secrets" dated 21.07.1993 No. 5485-1 (as amended on 30.12.2020) // *Collected Legislation of the Russian Federation*, No. 41. In Rus.

7. Portal of Huiying Medical: [Electronic resource]. URL: https://www.intel.ru/content/www/ru/ru/artificial-intelligence/posts/huiying-medical-covid19.html (date of access 20.02.2021). In Rus.

8. *Tseny "Chernogo rynka" na rossiiskie personal'nye dannye* [Prices of the "Black Market" for Russian personal data] [Electronic resource]. Access mode: https://www.devicelock.com/ (Date of access: 20.02.2021).

9. *Resurs dlya detektirovaniya i predotvrashcheniya kiberatak, vyyavleniya froda i zashchity intellektual'noi sobstvennosti v seti. Sistema sbora dannykh o kiberugrozakh Group-IB* [A resource for detecting and preventing cyberattacks, detecting fraud and protecting intellectual property on the network. Group-IB cyber threat data collection system]. [Electronic resource]. URL: https://www.group-ib.ru/ (date of treatment 02/20/2021).

10. Rerke V.I., Demakov V.I., Portnaya Ya.A. *Kriterii i pokazateli informatsionnoi sotsializatsii studentov posredstvom sotsial'nykh setei. Sotsial'naya real'nost' virtual'nogo prostranstva: materialy I Mezhdunarodnoi nauchno-prakticheskoi konferentsii* [Criteria and indicators of informational socialization of students through social networks. Social reality of virtual space: materials of the I International scientific and practical conference]. FGBOU VO IGU. – Irkutsk, 2019. – P. 169-176.

11. Decree of the Government of the Russian Federation of October 7, 2019 No. 1285 "On approval of the Rules for the provision of subsidies from the federal budget for the creation of an industry center of the State System for Detection, Prevention and Elimination of the Consequences of Computer Attacks (GosSOPKA) and its inclusion in the system of automated exchange of information on current cyber threats". In Rus.

12. Medical information system "MedAngel". [Electronic resource]. URL: https://medangel.angelsit.ru/ (accessed 02.20.2021). In Rus.

13. Association for the Development of Medical Information Technologies: [Electronic resource]. URL: http: // https://armit.ru/ (accessed 02/20/2021).