ГОСУДАРСТВО И ПРАВО, 2023, № 6, с. 149–160
STATE AND LAW, 2023, No. 6, pp. 149–160

BIG DATA В ЗДРАВООХРАНЕНИИ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПРАВОВАЯ ОХРАНА ПЕРСОНАЛЬНЫХ ДАННЫХ

© 2023 г. С. В. Полубинская[1, *], М. И. Галюкова[2, **]

[1]Институт государства и права Российской академии наук, г. Москва
[2]Центральный районный суд города Челябинска

**E-mail: svepol@yandex.ru*
***E-mail: 753825777@mail.ru*

Поступила в редакцию 26.12.2022 г.

Аннотация. Цифровизация российского здравоохранения ведет к увеличению объема оцифрованных медицинских данных, становящихся в итоге Big Data (Большими данными), что требует разработки безопасных способов сбора, обработки, хранения и использования такой информации.
В статье дается анализ действующих нормативных правовых актов, регламентирующих способы защиты медицинской информации в цифровой форме, а также устанавливающих правовой режим персональных данных. Авторы обращают внимание на риски реидентификации обезличенных медицинских данных и сложности соблюдения некоторых требований законодательства о персональных данных при использовании технологий Big Data.
Обсуждая ответственность за правонарушения в сфере компьютерной информации, авторы предлагают рассматривать информационные системы в здравоохранении, содержащие персональные данные, как объекты критической информационной инфраструктуры Российской Федерации. Такой режим позволит квалифицировать неправомерный доступ к содержащейся в них информации и другие преступные деяния по ст. 274[1] УК РФ. Распространенность использования информационно-коммуникационных технологий как способа посягательств на оцифрованные медицинские данные, а в конечном счете – на неприкосновенность частной жизни приводит авторов к выводу о целесообразности дополнения ст. 137 УК РФ соответствующим квалифицирующим признаком.

Ключевые слова: цифровое здравоохранение, Большие данные, персональные данные, врачебная тайна, информированное согласие, оцифрованные медицинские данные, преступления в сфере компьютерной информации, информационная безопасность, критическая информационная инфраструктура, неприкосновенность частной жизни.

Цитирование: *Полубинская С.В., Галюкова М.И.* Big Data в здравоохранении: информационная безопасность и правовая охрана персональных данных // Государство и право. 2023. № 6. С. 149–160.

DOI: 10.31857/S102694520025938-2

BIG DATA IN HEALTHCARE: CYBERSECURITY AND LEGAL PROTECTION OF PERSONAL DATA

© 2023 S. V. Polubinskaya[1, *], M. I. Galyukova[2, **]

[1]Institute of State and Law of the Russian Academy of Sciences, Moscow
[2]The Central District Court of the City of Chelyabins

**E-mail: svepol@yandex.ru*
***E-mail: 753825777@mail.ru*

Received 26.12.2022

Abstract. Digitalization of Russian healthcare leads to an increase of digital medical data, which eventually becomes Big Data and requires secure ways to collect, process, store and use such information.
In this article, the authors analyze legal acts that govern ways to protect medical information in digital form, as well as those that establish the legal regime of personal data. The authors draw attention to the risks of re-identification of anonymized medical data and difficulties to comply with some requirements of the personal data legislation in use of Big Data technologies.
In discussion on liability for offences and crimes in the sphere of computer information, the authors propose to consider healthcare information systems containing personal data as objects of critical information infrastructure of the Russian Federation. Such regime would allow to charge unlawful access to the information contained and other criminal acts under Article 274[1] of the Criminal Code of the Russian Federation. Prevalence of information and communication technologies as a method of encroachments on the digital medical data, and ultimately an intrusion into privacy, leads authors to the conclusion about expediency of addition of Article 137 of the Criminal Code of the Russian Federation with the relevant aggravating circumstance.

Key words: digital health, Big Data, personal data, medical privacy, informed consent, digital medical data, crimes in the field of computer information, information security, critical information infrastructure, privacy.

For citation: *Polubinskaya, S.V., Galyukova, M.I. (2023).* Big Data in healthcare: cybersecurity and legal protection of personal data // Gosudarstvo i pravo=State and Law, No. 6, pp. 149–160.

Введение

Цифровая трансформация здравоохранения является приоритетным направлением развития отрасли в России, как и во многих других государствах. Целью национального цифрового здравоохранения является создание инновационной экосистемы с использованием искусственного интеллекта, отвечающей целям и задачам, обозначенным в Глобальной стратегии в области цифрового здравоохранения на 2020–2025 годы, принятой в 2020 г. на 73-й сессии Всемирной ассамблеи здравоохранения[1].

Цифровизация здравоохранения неизбежно ведет к росту объема оцифрованных медицинских данных, поступающих из различных источников (электронные медицинские карты, устройства удаленного мониторинга, видеозаписи медицинских консультаций, рентгенография, МРТ-сканирование и др.)[2] и приобретающих в конечном счете характер Big Data[3]. Этот процесс требует разработки безопасных способов сбора, обработки, хранения и использования медицинской информации. В Глобальной стратегии в области цифрового здравоохранения подчеркивается, что все данные о здоровье человека следует рассматривать как конфиденциальные персональные данные, требующие самых высоких стандартов защиты. В этой связи помимо эффективных технических решений необходимо и создание правовой базы, обеспечивающей неприкосновенность частной жизни и конфиденциальность медицинской информации, а также безопасность информационных систем и их защиту от неправомерного доступа и ненадлежащего использования[4].

Понятие, параметры и источники Больших данных. Считается, что термин "Big Data" в научный оборот впервые ввел К. Линч (C. Lynch) в 2008 г.[5] Однако этот термин использовался еще в 1997 г. применительно к визуализации с использованием внешней памяти компьютера[6], а в 2001 г. Д. Лэйни (D. Laney) в докладе для META Group определил три параметра Больших данных (т.н. три "V") – объем,

[1] См.: Global Strategy on Digital Health 2020–2025 [Электронный ресурс]. – Режим доступа: URL: https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf (дата обращения: 25.09.2022).

[2] По данным Института статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ, в цифровом здравоохранении и медицине наиболее востребованной на рынке цифровых услуг является телемедицина, получившая ускоренное развитие в связи с пандемией COVID-19 (см. подр.: *Robbins T.*, *Hudson S.*, *Ray P. et al.* COVID-19: A new digital dawn? // Digital Health. 2020. Vol. 6. P. 1–3), на втором месте на том же рынке, но на первом среди исследовательских проектов находятся биосенсоры, служащие для мониторинга различных показателей функционирования организма человека (частота сердечных сокращений, артериальное давление, уровень сахара в крови и т.п.) (см., напр.: *Coravos A.*, *Goldsack J.C.*, *Karlin D.P. et al.* Digital Medicine: A Primer on Measurement // Digital Biomarkers. 2019. Vol. 3. No. 2. P. 31–71), третье место по значимости и на рынке услуг, и в исследовательских интересах занимает электронный документооборот (см.: Топ-10 цифровых решений в медицине и здравоохранении. С. 2 [Электронный ресурс]. – Режим доступа: URL: https://issek.hse.ru/mirror/pubs/share/691544300.pdf (дата обращения: 22.09.2022)).

[3] См. подр.: *Bahri S.*, *Zoghlami N.*, *Abed M. et al.* BIG DATA for Healthcare: A Survey // IEEE Access. 2019. Vol. 7. P. 7397, 7398.

[4] См.: Global Strategy on Digital Health 2020–2025. P. 11, 12.

[5] См.: *Lynch C.* How do your data grow? // Nature. 2088. Vol. 455. Iss. 7209. P. 28, 29.

[6] См.: *Cox M.*, *Ellsworth D.* Application-Controlled Demand Paging for Out-of-Core Visualization. P. 1 [Электронный ресурс]. – Режим доступа: URL: https://ntrs.nasa.gov/api/citations/20020046803/downloads/20020046803.pdf (дата обращения: 25.09.2022).

скорость накопления и разнообразие (Volume, Velocity, Variety)[7].

В справочных и научных источниках содержание понятия "Big Data" раскрывается по-разному[8], и общепринятое определение, в том числе применительно к здравоохранению[9], отсутствует. Интересен в этой связи подход, отраженный в докладе Глобального института Маккинси (McKinsey Global Institute), где Big Data понимаются как «огромные массивы данных, которые могут быть собраны, переданы, накоплены, сохранены и проанализированы»[10]. Подчеркивается, что их размер превышает возможности стандартных программных средств по сбору, хранению и анализу баз данных. Авторы доклада не предлагают содержательное определение и количественные характеристики Больших данных, вполне резонно полагая, что по мере развития технологий и в зависимости от доступности программных инструментов и потребностей той или иной отрасли, где востребованы Big Data, их объем, как и определение самого понятия, могут различаться[11].

От содержательного определения Больших данных уходит и введенный в действие с 1 ноября 2021 г. национальный стандарт ГОСТ Р ИСО/МЭК 20546-2021[12]. В п. 3.1.2 Большие данные характеризуются как «большие массивы данных[13], отличающиеся главным образом такими характеристиками, как объем, разнообразие, скорость обработки и / или вариативность, которые требуют использования технологии масштабирования для эффективного хранения, обработки, управления и анализа». В примечании к пункту указано, что «термин "большие данные" широко применяется в различных значениях, например в качестве наименования технологии масштабирования, используемой для обработки больших массивов данных».

Отказавшись от выработки понятия "Big Data", исследователи сосредоточились на их параметрах, справедливо полагая, что именно в этом состоит их принципиальное отличие от любой другой информационной базы. К первоначально выделенным трем "V" добавились еще Veracity – правдивость, качество данных и их источников, Value – ценность и Variability – переменчивость, связанная с форматом или способом сбора данных. В литературе можно найти и другие, дополнительные параметры Больших данных, например: Validity – достоверность, точность, Viability – актуальность, Volatility – непостоянство, изменяемость, Vulnerability – уязвимость, Visualization – отражение в удобной для использования форме, визуализация[14].

Отечественные ученые приступили к изучению Больших данных позднее зарубежных коллег и в отличие от них включают в это понятие не только информацию, но и инструменты по ее сбору, структурированию и анализу[15].

Жизненный цикл Big Data до их использования складывается из ряда последовательных этапов, каждый из которых имеет правовое значение и требует технической и правовой защиты информации.

Первый этап – сбор данных – включает в себя получение сведений различных форматов из разных источников. Среди источников, прежде всего, электронные медицинские карты, создаваемые со специальной целью – диагностики и лечения конкретного пациента, но которые могут использоваться и для оценки деятельности медицинской организации, и для научных исследований. Как отмечают Н. Пик (N. Peek) с соавторами, «медицинские карты содержат обширный массив данных, от демографической информации, результатов лабораторных

[7] См.: *Корнев М.С.* История понятия «большие данные» (Big Data): словари, научная и деловая периодика // Вестник РГГУ. Серия: История. Филология. Культурология. Востоковедение. 2018. № 1 (34). С. 83; *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал ВШЭ. 2015. № 1. С. 46, 47.

[8] См. подр.: *Корнев М.С.* Указ. соч. С. 82, 83.

[9] См.: *Baro E.*, *Degoul S.*, *Beuscart R. et al.* Toward a Literature-Driven Definition of Big Data in Healthcare // BioMed Research International. 2015. Vol. 2015. Art. 639021. P. 1–9.

[10] *Manyika J.*, *Chui M.*, *Brown B. et al.* Big Data: The next frontier for innovation, competition and productivity // McKinsey Global Institute. May 2011. Preface [Электронный ресурс]. – Режим доступа: URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx (дата обращения: 22.09.2022).

[11] См.: ibid. P. 1.

[12] См.: ГОСТ Р ИСО/МЭК 20546-2021. Национальный стандарт Российской Федерации. Информационные технологии. Большие данные. Обзор и словарь (утв. и введен в действие Приказом Росстандарта от 13.07.2021 г. № 632-ст) // В официальных источниках опубликован не был.

[13] «Идентифицируемая совокупность данных, к которой можно получить доступ или скачать в одном или нескольких форматах» (п. 3.1.11 ГОСТа). Данные – «представление информации в формальном виде, пригодном для передачи, интерпретации или обработки» (п. 3.1.5 ГОСТа). В примечании к этому пункту отмечается, что «данные могут быть обработаны автоматически или вручную».

[14] См. подр.: *Paamanik P.K.*, *Pal S.*, *Mukhopadhyay M.* Healthcare Big Data: A Comprehensive Overview // In: Intellegent Systems for Healthcare Management and Delivery / ed. Nardjes Bouchmal. USA: IGI Global, 2018. P. 73–75 [Электронный ресурс]. – Режим доступа: URL: https://www.researchgate.net/publication/327845528_Healthcare_Big_Data_A_Comprehensive_Overview (дата обращения: 04.10.2022); см. также: *Bahri S.*, *Zoghlami N.*, *Abed M. et al.* Op. cit. P. 7398, 7399; *Dicuonzo G.*, *Galeone G.*, *Shini M. et al.* Towards the Use of Big Data in Healthcare: A Literature Review // Healthcare. 2022. Vol. 10. Iss. 7. Art. 1232. P. 2.

[15] См., напр.: *Могилюк А.А.*, *Палис Я.В.* Управление большими данными в здравоохранении // Журнал «Московская Медицина». 2022. № 1 (47). С. 6–11.

исследований, выписанных лекарств, снимков и других диагностических обследований, медицинских интервенций до клинических заметок в свободной форме. Они [ведутся] длительное время, с повторяющимися наблюдениями за пациентами, и... отражают объемы [деятельности] организаций здравоохранения, из которых они поступают»[16].

Следует указать также и административные данные, которые не являются в строгом смысле клиническими, но могут содержать личные сведения, включая связанные с диагностикой и лечением пациента, например информация страховых организаций[17].

К иным источникам Big Data относятся в том числе зарегистрированные сведения с биосенсоров, записи телемедицинских консультаций, данные неотложной и скорой помощи, фармацевтических организаций, социальные сети, медицинские запросы в сети Интернет, результаты научных исследований, прежде всего, публикации в профессиональных периодических изданиях[18].

После того, как данные получены, следующим шагом является создание внутренней архитектоники Больших данных для их дальнейшего системного анализа – этап преобразования данных. На этом этапе данные еще не обезличены и содержат конфиденциальную информацию, поэтому для обеспечения их безопасности все каталоги, списки и информационные базы должны быть защищены. Распространенной точкой зрения считается, что надежно хранить данные в облачном хранилище, однако это мнение неверно. Облачные инфраструктуры уязвимы, подвержены несанкционированным доступам и злонамеренным кибератакам, и основной угрозой для них является утечка данных[19]. Безопасность облачных хранилищ требует усложненного входа в систему, криптографического шифрования данных, включая передачу пакетов данных с облака, создания систем-ловушек для хакеров, а также определенной архитектуры таких хранилищ[20].

На следующем этапе – моделирования – происходит непосредственное формирование Больших данных. Уровень безопасности на данном этапе должен быть максимальным, поскольку работа идет одновременно как с уже имеющимися данными, так и с качественно новым результатом их обработки. В этих случаях специалисты рекомендуют использовать методы криптографии[21].

Логическим продолжением этапа моделирования является этап создания Больших данных, которые должны иметь определенную ценность для пользователя и давать ему новые знания. В зависимости от целей использования и субъектов, имеющих право на доступ к данным, могут устанавливаться различные способы такого доступа. При наличии в базах персональной медицинской информации требуются меры и технической, и правовой защиты от утечек и неправомерного использования, включая установление юридической ответственности.

Информационные системы в российском здравоохранении и защита персональных данных. Информационные системы включают в себя государственные информационные системы в сфере здравоохранения федерального и регионального уровней, а также информационные системы медицинских и фармацевтических организаций, включая частную систему здравоохранения. Кроме того, в них входят информационные системы в сфере здравоохранения Федерального фонда обязательного медицинского страхования и аналогичных территориальных фондов (ч. 1, 2 ст. 91 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации»[22]) (далее – Федеральный закон № 323-ФЗ).

Операторами информационных систем являются уполномоченный федеральный орган исполнительной власти, иные федеральные органы исполнительной власти в сфере охраны здоровья и их территориальные органы, уполномоченные органы исполнительной власти субъекта Российской Федерации, организации, назначенные указанными органами, органы управления Федерального фонда обязательного медицинского страхования

[16] *Peek N.*, *Holmes J.H.*, *Sun J.* Technical challenges for big data in biomedicine and health: data sources, infrastructure, and analytics // Yearbook of Medical Informatics. 2014. Vol. 9. Iss. 1. P. 43.

[17] См. подр.: ibid.

[18] См.: ibid. P. 43, 44; *Bahri S.*, *Zoghlami N.*, *Abed M. et al.* Op. cit. P. 7397, 7398; *Цветкова Л.А.*, *Черченко О.В.* Технология Больших данных в медицине и здравоохранении России и мира // Врач и информационные технологии. 2016. № 3. С. 61.

[19] См. подр.: *Krishna H.B.*, *Kiran S.*, *Murali G. et al.* Security Issues in Service Model of Cloud Computing Environment // Procedia Computer Science. 2016. Vol. 87. P. 248; *Hersiba L.C.*, *Sathiaseelan J.G.R.* Security Issues in Service Models of Cloud Computing // International Journal of Computer Science and Mobile Computing. 2016. Vol. 5. Iss. 3. P. 611.

[20] См., напр.: *Shahzad F.* State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions // Procedia Computer Science. 2014. Vol. 37. P. 360, 361; *Manogaran G.*, *Thota C.*, *Kumar M.V.* MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing // Procedia Computer Science. 2016. Vol. 87. P. 128–133.

[21] См.: *Запечников С.В.*, *Казарин О.В.*, *Тарасов А.А.* Криптографические методы защиты информации: учеб. пособие для академического бакалавриата. М., 2019. С. 209–218.

[22] См.: СЗ РФ. 2011. № 48, ст. 6724.

и территориальных фондов в части, касающейся персонифицированного учета в системе обязательного медицинского страхования, медицинские и фармацевтические организации (ч. 3 ст. 91 Федерального закона № 323-ФЗ).

Федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы здравоохранения (ЕГИСЗ)», являющийся частью национального проекта «Здравоохранение», предполагает, что в 2023 г. не менее 80% медицинских организаций субъектов Российской Федерации обеспечат юридически значимый электронный документооборот. В том же году планируется завершить внедрение государственных информационных систем в сфере здравоохранения. К концу 2024 г. после подключения к ЕГИСЗ информационных систем медицинских организаций и государственных информационных систем в личном кабинете пациента «Мое здоровье» на едином портале государственных и муниципальных услуг (ЕПГУ) гражданам станут доступны разнообразные услуги и сервисы в сфере здравоохранения, включая доступ к своим электронным медицинским документам[23]. Предоставление пациенту доступа к медицинской документации в форме электронных документов, в том числе с использованием единого портала государственных и муниципальных услуг, обеспечивает Федеральный реестр электронных медицинских документов – подсистема ЕГИСЗ (п. 15, п/п. «в» п. 16 Положения о единой государственной информационной системе в сфере здравоохранения)[24].

Сбор и обработка медицинских данных происходят на Единой платформе регистров на основе ЕГИСЗ в соответствии с национальным проектом «Здравоохранение» и вертикальной интегрированной медицинской информационной системы (ВИМИС). ВИМИС предназначена для оперативного ведения пациентов и будет осуществлять взаимосвязь между региональным здравоохранением и национальными медицинскими исследовательскими центрами (НМИЦ). В разработке на 2022 г. находились четыре направления, которые влияют на показатели смертности: сердечно-сосудистые заболевания, онкология, профилактика, а также акушерство и неонатология[25].

Интерес представляет также подключенная к ЕГИСЗ платформа предиктивной аналитики и управления рисками в здравоохранении на основе машинного обучения Webiomed. Программное обеспечение «Система поддержки принятия врачебных решений “Webiomed”» зарегистрирована Росздравнадзором в качестве медицинского изделия и получила разрешение на применение в российской медицине[26]. Система поддерживает оценку рисков развития либо ухудшения для 14 заболеваний и 40 подозрений на наличие заболеваний.

По итогам 2021 г. платформа обработала более 200 млн медицинских документов, оценку риска получили более 3 млн пациентов, реализовано более 20 проектов в 20 субъектах Российской Федерации[27]. В 2021 г. сервисы Webiomed были включены в цифровую платформу Медицинского цифрового диагностического центра (MDDC), входящую в экосистему Сбербанка[28], и интегрированы с Единой цифровой платформой ЕЦП.МИС «РТ Медицинские информационные системы», входящей в группу компаний «Ростелеком»[29].

В литературе справедливо указывается на то, что «на современном этапе защита той или иной информации зачастую связана с безопасностью именно информационной инфраструктуры, а не с компетенцией отдельных лиц»[30], осуществляю-

[23] См.: Паспорт национального проекта «Здравоохранение» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 24.12.2018 г. № 16) // В официальных источниках опубликован не был.

[24] См.: постановление Правительства РФ от 09.02.2022 г. № 140 «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения») // СЗ РФ. 2022. № 8, ст. 1152.

[25] См.: Национальный проект «Здравоохранение». Федеральный проект «Создание единого цифрового контура в здравоохранении на основе единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ)». Методические рекомендации по организации информационного взаимодействия медицинских информационных систем медицинских организаций частной системы здравоохранения с единой государственной информационной системой в сфере здравоохранения (Версия 1.0) (утв. Минздравом России 14.08.2020 г.) // В официальных источниках опубликован не был.

[26] См.: Система Webiomed стала первой российской разработкой в области искусственного интеллекта для здравоохранения, зарегистрированной как медицинское изделие. 23.04.2020 [Электронный ресурс]. – Режим доступа: URL: https://webiomed.ru/novosti/sistema-webiomed-stala-pervoi-rossiiskoi-razrabotkoi-v-oblasti-iskusstvennogo-intellekta/ (дата обращения: 25.09.2022).

[27] См.: В Webiomed подвели итоги 2021 года [Электронный ресурс]. – Режим доступа: URL: https://webiomed.ru/novosti/v-webiomed-podveli-itogi-2021-goda/ (дата обращения: 25.09.2022).

[28] См.: Медицинский цифровой диагностический центр [Электронный ресурс]. – Режим доступа: URL: https://sbermed.ai/diagnostic-center/about-the-mddc/ (дата обращения: 25.09.2022).

[29] «РТ-МИС» и «К-скай» запускают умную платформу для здравоохранения. 19.04.2021 [Электронный ресурс]. – Режим доступа: URL: https://www.company.rt.ru/press/news/d458832/ (дата обращения: 25.09.2022).

[30] *Акулин И.М., Чеснокова Е.А., Смирнова К.М., Пресняков Р.А.* Трансформация института врачебной тайны в эпоху электронного здравоохранения // Закон. 2019. № 9. С. 184.

щих деятельность по созданию, развитию и эксплуатации информационных систем. В ЕГИСЗ защита информации «обеспечивается оператором единой системы посредством применения организационных и технических мер защиты информации, а также осуществления контроля за эксплуатацией единой системы» (п. 64 Положения о единой государственной информационной системе в сфере здравоохранения). С этой целью в Положении предусмотрены порядок доступа в единую систему, а также требования к ее программно-техническим средствам и защите содержащейся в ней информации (разд. VI, VII, IX соответственно).

Так, персональные данные о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования, хранятся в ЕГИСЗ (подсистема «Федеральная интегрированная электронная медицинская карта») в обезличенном виде (п. 4 ч. 3 ст. 91[1] Федерального закона № 323-ФЗ, п. 13, 14 Положения). Порядок обезличивания сведений с целью защиты от несанкционированного использования устанавливается Минздравом России[31]. В соответствии с п. 13 Порядка обезличивание осуществляется методом введения идентификаторов, в которых часть сведений заменяется идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным, и методом изменения состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений.

В ходе обезличивания преобразованию подлежат сведения, перечисленные в ст. 94 Федерального закона № 323-ФЗ, в том числе фамилия, имя, отчество лица, дата его рождения, данные документа, удостоверяющего личность, место жительства и место регистрации, страховой номер индивидуального лицевого счета в системе обязательного пенсионного страхования, номер полиса обязательного медицинского страхования застрахованного лица. При этом должно быть обеспечено сопоставление результатов обезличивания со сведениями о поле и гражданстве лица, а также анамнезе, диагнозе, виде оказанной медицинской помощи, ее сроках, объеме, результате и некоторых других (п. 5 Порядка). Полученные в результате данные должны быть полными, структурированными и релевантными, а также обладать такими качествами, как семантическая целостность, применимость и анонимность, т.е. не содержать возможность однозначной идентификации субъектов данных, полученных в результате обезличивания (п. 7 Порядка).

Угрозы безопасности медицинских персональных данных и правовые средства противодействия им. Несмотря на используемые при работе медицинских информационных систем способы защиты, полностью гарантировать их безопасность невозможно. Основными угрозами являются неправомерный доступ к информации, ее сбор и использование в неправомерных целях, что чревато причинением вреда человеку, обществу и государству[32]. В этой связи важно изначально определить, какие информационные системы могут относиться к общедоступным, а какие – к информации ограниченного доступа, установить способы и уровни доступа и механизмы защиты данных, включая ответственность за правонарушения.

Под информацией ограниченного доступа, как следует из п. 2 ст. 3 и ч. 2 ст. 5 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации»[33], понимается информация, доступ к которой ограничен федеральными законами (далее – Федеральный закон № 149-ФЗ). Ограничения устанавливаются «в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны

[31] См.: приказ Минздрава России от 14.06.2018 г. № 341н «Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования» // В официальных источниках опубликован не был.

[32] Так, только в первой половине 2022 г. в сфере здравоохранения США произошло 337 нарушений компьютерной безопасности медицинских и страховых организаций, приведших к утечке более чем 19 млн единиц информации (records), допускающих раскрытие данных о пациентах. Крупнейшим нарушением стала кибератака в марте на Shields Health Care Group, затронувшая 2 млн человек. Неизвестный субъект завладел их конфиденциальными данными, включая полные имена, номера социального страхования, номера медицинских карт, идентификаторы пациентов, диагнозы, даты рождения, адреса, а также информацию о лечении, лечащих врачах и выставленных счетах (см.: Biggest Healthcare Data Breaches Reported This Year, So Far [Электронный ресурс]. – Режим доступа: URL: https://healthitsecurity.com/features/biggest-healthcare-data-breaches-reported-this-year-so-far (дата обращения: 11.11.2022)). В России в декабре 2020 г. стало известно об утечке в Интернет персональных данных около 100 тыс. пациентов московских больниц, переболевших коронавирусом, в том числе их имен, номеров телефонов, паспортных данных, домашних адресов, диагнозов и иной информации, составляющей врачебную тайну (см.: Больных COVID-19 выписали в интернет // Коммерсантъ. 2020. 10 дек. [Электронный ресурс]. – Режим доступа: URL: https://www.kommersant.ru/doc/4605346 (дата обращения: 11.11.2022)). Весной 2022 г. в даркнете были выставлены на продажу данные 30 млн клиентов сети лабораторий «Гемотест» (имена, даты рождения, паспортные данные, адреса, телефоны, электронная почта, номера медицинской страховки и СНИЛС, результаты анализов) (см.: В сеть утекла база данных клиентов «Гемотеста» // Forbes. 2022. 4 мая [Электронный ресурс]. – Режим доступа: URL: https://www.forbes.ru/tekhnologii/464697-v-set-utekla-baza-dannyh-klientov-gemotesta (дата обращения: 11.11.2022)).

[33] См.: СЗ РФ. 2006. № 31 (ч. I), ст. 3448.

страны и безопасности государства» (ч. 1 ст. 9 Федерального закона № 149-ФЗ).

На практике термин «информация ограниченного доступа» зачастую подменяется термином «конфиденциальная информация». При этом игнорируется то обстоятельство, что в Федеральном законе говорится о конфиденциальности информации как требовании, обязательном для выполнения лицом, получившим доступ к определенной информации, не передавать такую информацию третьим лицам без согласия ее обладателя (п. 7 ст. 2 Федерального закона № 149-ФЗ). В ч. 2 ст. 9 подчеркивается обязательность соблюдения конфиденциальности информации, доступ к которой ограничен федеральными законами.

Информация ограниченного доступа зачастую совпадает с охраняемой законом тайной (государственной, коммерческой, банковской, адвокатской и др.)[34]. Условия отнесения информации к сведениям, составляющим тайну, обязательность соблюдения ее конфиденциальности и ответственность за разглашение устанавливаются федеральными законами (ч. 4 ст. 9 Федерального закона № 149-ФЗ).

А.В. Морозов, анализировавший правовое регулирование банковской тайны, отмечает, что «правовой режим информации ограниченного доступа в банковской деятельности дополняется правовым режимом персональных данных»[35]. Это наблюдение в полной мере относится и к деятельности в сфере здравоохранения, поскольку значительный объем собираемой, хранящейся и используемой в такой деятельности информации составляют персональные данные.

Так, врачебную тайну составляют сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ч. 1 ст. 13 Федерального закона № 323-ФЗ). Запрет разглашать сведения, составляющие врачебную тайну, в том числе и после смерти человека, содержится в ч. 2 ст. 13. Однако с письменного согласия гражданина или его законного представителя, а также в случаях, закрытый перечень которых содержатся в ч. 4 той же статьи, подобные сведения могут стать достоянием третьих лиц. Среди таких случаев – обмен информацией между медицинскими организациями в целях оказания медицинской помощи и с соблюдением требований законодательства о персональных данных (п. 8 ч. 4 ст. 13). Это законодательное предписание относится и к информации, размещенной в медицинских информационных системах, где обработка персональных данных осуществляется как с соблюдением законодательства о персональных данных, так и с соблюдением врачебной тайны (ч. 2 ст. 91 Федерального закона № 323-ФЗ).

В свою очередь, Федеральный закон «О персональных данных»[36] (далее – Федеральный закон № 152-ФЗ) рассматривает сведения о состоянии здоровья гражданина как одну из специальных категорий таких данных (ч. 1 ст. 10). По общему правилу обработка персональных данных допускается с согласия лица, к которому они относятся (ст. 9), но для рассматриваемой категории требуется согласие субъекта данных в письменной форме (п. 1 ч. 2 ст. 10). Такое согласие должно быть конкретным, предметным, информированным, сознательным и однозначным и может быть давшим его лицом отозвано (ч. 1, 2 ст. 9)[37].

Согласие субъекта данных не требуется, если их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну, в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг (п. 4 ч. 2 ст. 10 Федерального закона № 152-ФЗ). Кроме того, данные о состоянии здоровья, полученные в результате обезличивания персональных данных, могут обрабатываться в целях повышения эффективности государственного или муниципального управления, а также в иных целях, предусмотренных двумя Федеральными законами, посвященными внедрению в Российской Федерации цифровых инноваций и технологий искусственного интеллекта[38] (ч. 2^1 ст. 10).

---

[34] См. подр.: *Сизоненко А.Б.* Классификация информации ограниченного доступа в соответствии с законодательством Российской Федерации // Вестник Краснодарского ун-та МВД России. 2010. № 4. С. 91–96; см. также: Справочная информация «Перечень нормативных актов, относящих сведения к категории ограниченного доступа» (материал подготовлен специалистами «КонсультантПлюс») [Электронный ресурс]. – Режим доступа: URL: https://online11.consultant.ru/cgi/online.cgi?req=doc&ts=7HwwxMTOnqSuZ1Rp&cacheid=9DA369E61FA637C0ECFAD35303300738&mode=splus&rnd=rvtVog&base=LAW&n=93980&dst=100000001#gxDZyMTgR3JvLkLV1 (дата обращения: 11.11.2022).

[35] *Морозов А.В.* Информационное общество, цифровая экономика и информационная безопасность. М., 2019. С. 115.

[36] См.: СЗ РФ. 2006. № 31 (ч. I), ст. 3451.

[37] См. подр.: *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд., перераб. и доп. М., 2021.

[38] См.: Федеральный закон от 24.04.2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных"» // СЗ РФ. 2020. № 17, ст. 2701; Федеральный закон от 31.07.2020 г. № 258-ФЗ (ред. от 02.07.2021) «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // СЗ РФ. 2020. № 31 (ч. I), ст. 5017.

Помимо законного основания обработки на эту специальную категорию персональных данных распространяются принципы, установленные Федеральным законом № 152-ФЗ в ст. 5. Не допускается обработка данных, несовместимая с целями их сбора (ч. 2), содержание и объем таких сведений должны соответствовать заявленным целям обработки, а обрабатываемые данные по отношению к упомянутым целям не должны быть избыточными (ч. 5).

За неправомерные действия в отношении персональных данных установлена административная и уголовная ответственность. К административным правонарушениям относится, в частности, обработка персональных данных в случаях, не предусмотренных законодательством в области персональных данных, либо несовместимая с целями сбора персональных данных, а также без согласия в письменной форме субъекта персональных данных на обработку сведений о нем в случаях, когда по закону требуется такое согласие (ч. 1, 3 ст. 13.11 КоАП РФ). По ч. 4 той же статьи наказываются операторы, обрабатывающие персональные данные, за невыполнение обязанности по предоставлению субъекту персональных данных информации, касающейся такой обработки, а по ч. 7 – за невыполнение обязанности по обезличиванию персональных данных либо несоблюдение установленных требований или методов обезличивания.

В ст. 13.14 КоАП РФ предусмотрена ответственность за разглашение информации с ограниченным доступом лицом, которому она стала известна в связи с исполнением служебных и профессиональных обязанностей, по ст. 13.14.1 – незаконное получение информации с ограниченным доступом. Эти нормы являются общими в данной области и применяются к правонарушениям, не содержащим признаков деяний, за которые установлена уголовная ответственность.

Уголовная ответственность установлена за преступления в сфере компьютерной информации, в том числе за неправомерный доступ к охраняемой законом компьютерной информации, если это повлекло ее уничтожение, блокирование, модификацию либо копирование (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (ст. 274 УК РФ).

Принятие Федерального закона от 26 июля 2017 г. № 187-ФЗ[39] стало причиной введения в Уголовный кодекс РФ в том же году ст. 274[1], предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (далее – КИИ)[40].

По ч. 1 этой статьи наказывается создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ, в том числе с использованием вредоносных компьютерных программ либо иной компьютерной информации, если он повлек причинение вреда критической информационной инфраструктуре, влечет ответственность по ч. 2 той же статьи. Уголовно наказуемым является и нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре, а также правил доступа к указанным информации и объектам, если оно повлекло причинение вреда КИИ (ч. 3 ст. 274[1] УК РФ).

Е.А. Русскевич и И.Г. Чекунов указывают на предмет преступного посягательства как главный признак, позволяющий отграничить преступления, ответственность за которые предусмотрена в ст. 274[1] УК РФ, от других уголовно наказуемых деяний в сфере компьютерной информации[41]. Информационная система, информационно-коммуникационная сеть или автоматизированная система управления должны не только

[39] См.: СЗ РФ. 2017. № 31 (ч. I), ст. 4736.

[40] См.: Федеральный закон от 26.07.2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» // СЗ РФ. 2017. № 31 (ч. I), ст. 4743.

[41] См.: *Русскевич Е.А.*, *Чекунов И.Г.* Квалификация неправомерного воздействия на критическую информационную структуру Российской Федерации // Уголовное право. 2022. № 5 (141). С. 27–29.

функционально относиться к критически значимой для государства сфере, но и приобрести юридический статус объекта КИИ путем присвоения определенной категории значимости и включения в реестр значимых объектов КИИ (ст. 7, 8 Федерального закона от 26.07.2017 г. № 187-ФЗ)[42]. В этой связи «для применения ст. 274[1] УК РФ вопрос о моменте получения соответствующей информационной системой статуса объекта КИИ имеет принципиальное значение»[43].

По нашему мнению, все информационные системы в области здравоохранения, содержащие как обезличенные, так и идентифицируемые персональные данные, начиная от медицинских и иных организаций и заканчивая ЕГИСЗ, следует относить к объектам КИИ. После введения в отношении информационной системы режима КИИ неправомерный доступ к содержащейся в ней информации и другие преступные посягательства подлежат квалификации по ст. 274[1] УК РФ.

Охраняет уголовный закон и неприкосновенность частной жизни. В соответствии со ст. 137 УК РФ наказывается, среди прочих деяний, незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия. Конституционный Суд РФ указал, что «собирание или распространение информации о частной жизни лица допускается лишь в предусмотренном законом порядке и лишь в отношении тех сведений, которые уже официально кому-либо доверены самим лицом и в законном порядке собраны, хранятся, используются и могут распространяться»[44]. Это положение в полной мере относится к информации о состоянии здоровья человека и иным данным, составляющим врачебную тайну, независимо от формы их представления.

Заметим, что ст. 137 УК РФ нечасто встречается на практике, хотя за последние пять лет заметен рост подобных уголовных дел. Так, в 2017 г. было осуждено 84 лица по ч. 1 и 2 – по ч. 2, а также 57 человек по ч. 1 с дополнительной квалификацией по другим статьям Уголовного кодекса РФ. В 2021 г. приговоры были вынесены в отношении 218 лиц по ч. 1, 17 – по ч. 2 с добавлением 94 и 4 человек соответственно с дополнительной квалификацией. Приговоры по ч. 3 ст. 137 УК РФ отсутствовали[45].

По оценке Е.А. Русскевича, подробно изучавшего преступления, совершаемые с использованием информационно-коммуникационных технологий, «состояние правоприменения объективно указывает на то, что именно такой способ [совершения преступления] является преобладающим по данной категории дел»[46]. При отсутствии в ст. 137 УК РФ квалифицирующего обстоятельства, указывающего на использование названных технологий, содеянное должно квалифицироваться по совокупности этой статьи Кодекса с соответствующими статьями из гл. 28. Такая правовая позиция зафиксирована в п. 16 Постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37[47]. При этом получение доступа к информации, составляющей охраняемую законом тайну, либо предоставление к ней доступа неограниченному кругу лиц рассматриваются Пленумом Верховного Суда РФ как тяжкие последствия, предусмотренные в качестве квалифицирующего признака в ч. 4 ст. 272, ч. 3 ст. 273, ч. 2 ст. 274 и ч. 5 ст. 274[1] УК РФ (п. 14 Постановления).

Заключение

Существуют большие ожидания от внедрения технологий Big Data в здравоохранение. Аналитика таких данных способна принести большие выгоды в повышении качества управления здравоохранением, включая распределение ресурсов, в частности, дорогостоящего медицинского оборудования, а также улучшения медицинского обслуживания. Клинические рекомендации, разработанные на основе Больших данных, станут более полными и точными, а анализ демографических и клинических данных пациентов послужит развитию персонализированного характера медицинской помощи. Использующие анализ Больших данных фармацевтические компании смогут их учитывать при разработке приоритетных маркетинговых стратегий и в конечном счете получат преимущества на рынке. Новый импульс получат и научные биомедицинские исследования[48].

---

[42] См. также: постановление Правительства РФ от 08.02.2018 г. № 127 (ред. от 19.08.2022) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» // СЗ РФ. 2018. № 8, ст. 1204.

[43] *Русскевич Е.А.*, *Чекунов И.Г.* Указ. соч. С. 27.

[44] См.: пункт 2 Определения Конституционного Суда РФ от 28.06.2012 г. № 1253-О «Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации» // В официальных источниках опубликовано не было.

[45] См.: Форма № 10-а «Отчет о числе осужденных по всем составам преступлений Уголовного кодекса Российской Федерации и иных лиц, в отношении которых вынесены судебные акты по уголовным делам» [Электронный ресурс]. – Режим доступа: URL: http://www.cdep.ru/?id=79 (дата обращения: 12.11.2022).

[46] *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения. М., 2022. С. 30.

[47] См.: Росс. газ. 2022. 28 дек.

[48] См. подр.: *Bahri S.*, *Zoghlami N.*, *Abed M. et al.* Op. cit. P. 7403–7405; Applications of Big Data in Healthcare. Theory and Practice / eds. Ashish Khanna, Deepak Gupta, Nilanjan Dey. UK, USA: Academic Press, 2021 [Электронный ресурс]. – Режим доступа: URL: https://www.researchgate.net/publication/350808920_Application_of_BigData_in_Healthcare-Theory_and_Practices (дата обращения: 18.11.2022).

Вместе с тем, несмотря на достаточно подробный правовой режим персональных данных, связанных с Big Data, обеспечить их полную защиту невозможно. Так, эксперты отмечают, что имеющееся правовое регулирование в этой области «не исключает риски реидентификации, лежащие на стороне получателя такой обезличенной информации, в полной мере. Вследствие поступательного роста производительности и доступности вычислительных мощностей можно осуществить реидентификацию лица путем совмещения баз данных, содержащих даже обезличенную информацию»[49].

Что касается уголовной ответственности за неправомерные доступ и использование персональных медицинских данных, то, с учетом тенденции «сращивания» посягательств на неприкосновенность частной жизни с преступлениями в сфере компьютерной информации, целесообразно дополнить ст. 137 УК РФ квалифицирующим признаком, указывающим на использование информационно-телекоммуникационных технологий при их совершении.

СПИСОК ЛИТЕРАТУРЫ

1. *Акулин И.М.*, *Чеснокова Е.А.*, *Смирнова К.М., Пресняков Р.А.* Трансформация института врачебной тайны в эпоху электронного здравоохранения // Закон. 2019. № 9. С. 184, 185.
2. *Запечников С.В.*, *Казарин О.В.*, *Тарасов А.А.* Криптографические методы защиты информации: учеб. пособие для академического бакалавриата. М., 2019. С. 209–218.
3. *Корнев М.С.* История понятия «большие данные» (Big Data): словари, научная и деловая периодика // Вестник РГГУ. Серия: История. Филология. Культурология. Востоковедение. 2018. № 1 (34). С. 82, 83.
4. *Могилюк А.А.*, *Палис Я.В.* Управление большими данными в здравоохранении // Журнал «Московская Медицина». 2022. № 1 (47). С. 6–11.
5. *Морозов А.В.* Информационное общество, цифровая экономика и информационная безопасность. М., 2019. С. 115.
6. *Русскевич Е.А.* Уголовное право и «цифровая преступность»: проблемы и решения. М., 2022. С. 30.
7. *Русскевич Е.А.*, *Чекунов И.Г.* Квалификация неправомерного воздействия на критическую информационную структуру Российской Федерации // Уголовное право. 2022. № 5 (141). С. 27–29.
8. *Савельев А.И.* Научно-практический постатейный комментарий к Федеральному закону «О персональных данных». 2-е изд., перераб. и доп. М., 2021.
9. *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал ВШЭ. 2015. № 1. С. 46, 47.
10. *Сизоненко А.Б.* Классификация информации ограниченного доступа в соответствии с законодательством Российской Федерации // Вестник Краснодарского ун-та МВД России. 2010. № 4. С. 91–96.
11. Топ-10 цифровых решений в медицине и здравоохранении. С. 2 [Электронный ресурс]. – Режим доступа: URL: https://issek.hse.ru/mirror/pubs/share/691544300.pdf (дата обращения: 22.09.2022).
12. *Цветкова Л.А.*, *Черченко О.В.* Технология Больших данных в медицине и здравоохранении России и мира // Врач и информационные технологии. 2016. № 3. С. 61.
13. Applications of Big Data in Healthcare. Theory and Practice / eds. Ashish Khanna, Deepak Gupta, Nilanjan Dey. UK, USA: Academic Press, 2021 [Электронный ресурс]. – Режим доступа: URL: https://www.researchgate.net/publication/350808920_Application_of_BigData_in_Healthcare-Theory_and_Practices (дата обращения: 18.11.2022).
14. *Bahri S.*, *Zoghlami N.*, *Abed M. et al.* BIG DATA for Healthcare: A Survey // IEEE Access. 2019. Vol. 7. P. 7397–7399, 7403–7405.
15. *Baro E.*, *Degoul S.*, *Beuscart R. et al.* Toward a Literature-Driven Definition of Big Data in Healthcare // BioMed Research International. 2015. Vol. 2015. Art. 639021. P. 1–9.
16. *Coravos A.*, *Goldsack J.C.*, *Karlin D.P. et al.* Digital Medicine: A Primer on Measurement // Digital Biomarkers. 2019. Vol. 3. No. 2. P. 31–71.
17. *Cox M.*, *Ellsworth D.* Application-Controlled Demand Paging for Out-of-Core Visualization. P. 1 [Электронный ресурс]. – Режим доступа: URL: https://ntrs.nasa.gov/api/citations/20020046803/downloads/20020046803.pdf (дата обращения: 25.09.2022).
18. *Dicuonzo G.*, *Galeone G.*, *Shini M. et al.* Towards the Use of Big Data in Healthcare: A Literature Review // Healthcare. 2022. Vol. 10. Iss. 7. Art. 1232. P. 2.
19. *Hersiba L.C.*, *Sathiaseelan J.G.R.* Security Issues in Service Models of Cloud Computing // International Journal of Computer Science and Mobile Computing. 2016. Vol. 5. Iss. 3. P. 611.
20. *Krishna H.B.*, *Kiran S.*, *Murali G. et al.* Security Issues in Service Model of Cloud Computing Environment // Procedia Computer Science. 2016. Vol. 87. P. 248.
21. *Lynch C.* How do your data grow? // Nature. 2088. Vol. 455. Iss. 7209. P. 28, 29.
22. *Manogaran G.*, *Thota C.*, *Kumar M.V.* MetaCloudDataStorage Architecture for Big Data Security in Cloud Computing // Procedia Computer Science. 2016. Vol. 87. P. 128–133.
23. *Manyika J.*, *Chui M.*, *Brown B. et al.* Big Data: The next frontier for innovation, competition and productivity // McKinsey Global Institute. May 2011. Preface. P. 1 [Электронный ресурс]. – Режим доступа: URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx (дата обращения: 22.09.2022).
24. *Paamanik P.K.*, *Pal S.*, *Mukhopadhyay M.* Healthcare Big Data: A Comprehensive Overview // In: Intellegent Systems for Healthcare Management and Delivery / ed. Nardjes Bouchmal. USA: IGI Global, 2018. P. 73–75 [Электронный ресурс]. –

[49] *Акулин И.М.*, *Чеснокова Е.А.*, *Смирнова К.М., Пресняков Р.А.* Указ. соч. С. 185.

Режим доступа: URL: https://www.researchgate.net/publication/327845528_Healthcare_Big_Data_A_Comprehensive_Overview (дата обращения: 04.10.2022).

25. *Peek N.*, *Holmes J.H.*, *Sun J.* Technical challenges for big data in biomedicine and health: data sources, infrastructure, and analytics // Yearbook of Medical Informatics. 2014. Vol. 9. Iss. 1. P. 43, 44.
26. *Robbins T.*, *Hudson S.*, *Ray P. et al.* COVID-19: A new digital dawn? // Digital Health. 2020. Vol. 6. P. 1–3.
27. *Shahzad F.* State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions // Procedia Computer Science. 2014. Vol. 37. P. 360, 361.

REFERENCES

1. *Akulin I.M., Chesnokova E.A., Smirnova K.M., Presnyakov R.A.* Transformation of medical privacy in the era of digital health // Zakon. 2019. No. 9. P. 184, 185 (in Russ.).
2. *Zapechnikov S.V., Kazarin O.V., Tarasov A.A.* Cryptographic methods of information protection: textbook for academic baccalaureate. M., 2019. P. 209–218 (in Russ.).
3. *Kornev M.S.* History of the notion "Big Data": dictionaries, scientific and business periodicals. Series: History. Philology. Culturology. Orientalism. 2018. No. 1 (34). P. 83 (in Russ.).
4. *Mogilyuk A.A., Palis J.V.* Management of Big Data in health care // Journal of Moscow Medicine. 2022. No. 1 (47). P. 6–11 (in Russ.).
5. *Morozov A.V.* Information society, digital economy and information security. M., 2019. P. 115 (in Russ.).
6. *Russkevich E.A.* Criminal law and "digital criminality": problems and solutions. M., 2022. P. 30 (in Russ.).
7. *Russkevich E.A., Chekunov I.G.* Qualification of illegal influence on critical information structure of the Russian Federation // Criminal Law. 2022. No. 5 (141). P. 27–29 (in Russ.).
8. *Savelyev A.I.* Scientific and practical article-by-article commentary on the Federal Law "On Personal Data". 2nd ed., rev. and enlarged. M., 2021 (in Russ.).
9. *Savelyev A.I.* The Issues of Implementing Legislation on Personal Data in the Era of Big Data // Law. Journal of VSE. 2015. No. 1. P. 46, 47 (in Russ.)
10. *Sisonenko A.B.* Classification of restricted access information in accordance with the Russian Federation legislation // Herald of Krasnodar University of Ministry of Internal Affairs of Russia. 2010. No. 4. P. 91–96 (in Russ.)
11. Top 10 digital solutions in medicine and healthcare. P. 2 [Electronic resource]. – Access mode: URL: https://issek.hse.ru/mirror/pubs/share/691544300.pdf (accessed: 22.09.2022) (in Russ.).
12. *Tsvetkova L.A., Cherchenko O.V.* Big Data technology in medicine and healthcare in Russia and in the world // Physician and Information Technology. 2016. No. 3. P. 61 (in Russ.).
13. Applications of Big Data in Healthcare. Theory and Practice / eds. Ashish Khanna, Deepak Gupta, Nilanjan Dey. UK, USA: Academic Press, 2021 [Electronic resource]. – Access mode: URL: https://www.researchgate.net/publication/350808920_Application_of_BigData_in_Healthcare-Theory_and_Practices (accessed: 18.11.2022).
14. *Bahri S.*, *Zoghlami N.*, *Abed M. et al.* BIG DATA for Healthcare: A Survey // IEEE Access. 2019. Vol. 7. P. 7397–7399, 7403–7405.
15. *Baro E.*, *Degoul S.*, *Beuscart R. et al.* Toward a Literature-Driven Definition of Big Data in Healthcare // BioMed Research International. 2015. Vol. 2015. Art. 639021. P. 1–9.
16. *Coravos A.*, *Goldsack J.C.*, *Karlin D.P. et al.* Digital Medicine: A Primer on Measurement // Digital Biomarkers. 2019. Vol. 3. No. 2. P. 31–71.
17. *Cox M.*, *Ellsworth D.* Application-Controlled Demand Paging for Out-of-Core Visualization. P. 1 [Electronic resource]. – Access mode: URL: https://ntrs.nasa.gov/api/citations/20020046803/downloads/20020046803.pdf (accessed: 25.09.2022).
18. *Dicuonzo G.*, *Galeone G.*, *Shini M. et al.* Towards the Use of Big Data in Healthcare: A Literature Review // Healthcare. 2022. Vol. 10. Iss. 7. Art. 1232. P. 2.
19. *Hersiba L.C.*, *Sathiaseelan J.G.R.* Security Issues in Service Models of Cloud Computing // International Journal of Computer Science and Mobile Computing. 2016. Vol. 5. Iss. 3. P. 611.
20. *Krishna H.B.*, *Kiran S.*, *Murali G. et al.* Security Issues in Service Model of Cloud Computing Environment // Procedia Computer Science. 2016. Vol. 87. P. 248.
21. *Lynch C.* How do your data grow? // Nature. 2088. Vol. 455. Iss. 7209. P. 28, 29.
22. *Manogaran G.*, *Thota C.*, *Kumar M.V.* MetaCloudData-Storage Architecture for Big Data Security in Cloud Computing // Procedia Computer Science. 2016. Vol. 87. P. 128–133.
23. *Manyika J.*, *Chui M.*, *Brown B. et al.* Big Data: The next frontier for innovation, competition and productivity // McKinsey Global Institute. May 2011. Preface. P. 1 [Electronic resource]. – Access mode: URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx (accessed: 22.09.2022).
24. *Paamanik P.K.*, *Pal S.*, *Mukhopadhyay M.* Healthcare Big Data: A Comprehensive Overview // In: Intellegent Systems for Healthcare Management and Delivery / ed. Nardjes Bouchmal. USA: IGI Global, 2018. P. 73–75 [Electronic resource]. – Access mode: URL: https://www.researchgate.net/publication/327845528_Healthcare_Big_Data_A_Comprehensive_Overview (accessed: 04.10.2022).
25. *Peek N.*, *Holmes J.H.*, *Sun J.* Technical challenges for big data in biomedicine and health: data sources, infrastructure, and analytics // Yearbook of Medical Informatics. 2014. Vol. 9. Iss. 1. P. 43, 44.
26. *Robbins T.*, *Hudson S.*, *Ray P. et al.* COVID-19: A new digital dawn? // Digital Health. 2020. Vol. 6. P. 1–3.
27. *Shahzad F.* State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions // Procedia Computer Science. 2014. Vol. 37. P. 360, 361.

Сведения об авторах

ПОЛУБИНСКАЯ Светлана Вениаминовна – кандидат юридических наук, доцент, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права РАН; 119019 г. Москва, ул. Знаменка, д. 10

ГАЛЮКОВА Мария Игоревна – кандидат юридических наук, доцент, судья Центрального районного суда города Челябинска; 454091 г. Челябинск, ул. Коммуны, д. 87

Authors' information

POLUBINSKAYA Svetlana V. – PhD in Law, Associate Professor, Leading Researcher, Department of Criminal Law, Criminal Procedure and Criminology, Institute of State and Law of the Russian Academy of Sciences; 10 Znamenka str., 119019 Moscow, Russia

GALYUKOVA Mariya I. – PhD in Law, Associate Professor, Judge of the Central District Court of the City of Chelyabinsk; 87 Kommuny str., 454091 Chelyabinsk, Russia