ANALYSIS OF REQUIREMENTS FOR CONFIDENTIALITY AND EXCHANGE OF DIGITAL HEALTH DATA

Alzubaidi AK ✉

Yelets State University named after Bunin IA, Yelets, Russia

The article provides answers to immediate questions associated with the state regulation of confidentiality of information and exchange of data in the era of digital healthcare. The institute of medical confidentiality which originated in the ancient world is still evolving throughout the development of medical law. In the current era of global digitalization, however, the issues related to data confidentiality have become more relevant than ever. With all the modern technologies and digital health care platforms on the rise, new challenges associated with protection of these patients are emerging. To ensure the reliable protection of patient's personal and medical information, doctors and medical institutions have to meet data security standards. It becomes vital to develop effective strategies and mechanisms to prevent unauthorized access and data leakage due to a larger volume of electronic medical records and digital data exchange. Strict rules and standards regulating collection, storage and transfer of medical data belong to a key aspect in this area. The Russian Federation is making great efforts to create the legislation which could protect the rights of patients and made medical establishments to follow the high standards of confidentiality, and to develop technical aids that provide data encryption and protection against hacker attacks.

Keywords: medical secrecy, law, ethics, data disclosure, protection issues, medicine, patient, expert, digital health care, state control, digital rights, personal data protection, digital security, online state services

✉ **Correspondence should be addressed:** Azkhar K. Alzubaidi
Kommunarov Str., 10A, Yelets, Russia; azhrstar90@gmail.com

Received: 14.10.2023 **Accepted:** 25.11.2023 **Published online:** 05.12.2023

DOI: 10.24075/medet.2023.030

АНАЛИЗ ТРЕБОВАНИЙ К КОНФИДЕНЦИАЛЬНОСТИ И ОБМЕНУ ДАННЫМИ ЦИФРОВОГО ЗДРАВООХРАНЕНИЯ

А. К. Алзубаиди ✉

Елецкий государственный университет им. И. А. Бунина, Елец, Россия

Статья отвечает на насущные вопросы, связанные с государственным регулированием конфиденциальности информации и обмена данных в эпоху цифрового здравоохранения. Институт врачебной тайны, зародившийся в Древнем мире, продолжает эволюционировать на протяжении всего развития медицинского права. Однако в наше время, в эпоху глобальной цифровизации, вопросы, связанные с конфиденциальностью информации, стали более актуальными, чем когда-либо. С развитием современных технологий и цифровых платформ здравоохранения возникают новые вызовы в области защиты данных пациентов. Врачи и медицинские учреждения сталкиваются с необходимостью соблюдения стандартов безопасности данных, чтобы обеспечить надежную защиту личной и медицинской информации пациентов. С увеличением объема электронных медицинских записей и цифровых обменов данными становится жизненно важным разработать эффективные стратегии и механизмы для предотвращения несанкционированного доступа и утечек информации. Одним из ключевых аспектов в этой области является установление строгих нормативов и законов, которые регулируют сбор, хранение и передачу медицинских данных. В Российской Федерации активно работают над созданием законодательства, которое защищало бы права пациентов и обязывало медицинские учреждения соблюдать высокие стандарты конфиденциальности, а также разработать технические средства, которые обеспечивают шифрование данных и защиту от хакерских атак.

Ключевые слова: врачебная тайна, закон, этика, раскрытие данных, вопросы защиты, медицина, пациент, эксперт, цифровое здравоохранение, государственный контроль, цифровые права, защита персональных данных, информационная безопасность, электронные госуслуги

✉ **Для корреспонденции:** Азхар Кхудхаир Алзубаиди
ул. Коммунаров, д. 10А, г. Елец, Россия; azhrstar90@gmail.com

Статья поступила: 14.10.2023 **Статья принята к печати:** 25.11.2023 **Опубликована онлайн:** 05.12.2023

DOI: 10.24075/medet.2023.030

At present, digital medical services, which can analyze survey results based on extensive data, have seen rapid growth. So, the issue of medical secrecy and data confidentiality remains highly relevant.

On the one hand, medical secrecy is protected by the state through restrictions and defense mechanisms. On the other hand, the issue is influenced by the ethical part. According to Aleksandra Dronova, State Secretary and Deputy Minister of Health of the Russian Federation, it is regulated by special standards of the medical law. 'Now, when information technologies are being developed, it is essential to ensure medical confidentiality during treatment and protection of data collected from patients', says the expert. Data processing is associated with the risks of its disclosure. Thus, the issue of reliable protection has reached a new level [1].

As per Federal Law as of 21 November 2011 No. 323-FZ 'On fundamental health care principles in the Russian Federation' [2], medical secrecy involves various data including the fact of seeking medical aid by a citizen, condition of health, diagnosis and data obtained during a medical survey and treatment [3]. The law strictly prohibits the disclosure of the data to persons who have acquired them, except as required by law [4].

First, in the presence of written consent of the citizen (authorized representative), information classified as medical secrecy can be transferred to other citizens and qualified persons to conduct a medical survey, treatment and associated procedures [5].

Second, in the absence of written consent, the following cases are allowed (part 4, art. 13, Law No. 323-FZ) [2]:

– to perform a medical survey and treatment of a citizen who is unable to express own will because of his/her condition;

- at risk of spreading infectious diseases, mass poisoning and destructions;
- at the request of state bodies only in cases specified by law, for instance, at the request of inquiry, investigation agencies, or court in connection with an investigation or trial;
- to control whether persons recognized as suffering from drug addiction discharge the duties imposed on them by court;
- when medical aid is provided to the minor;
- to inform the law enforcement agencies of certain cases, such as admission to the hospital of a person who most likely suffered as a result of unlawful actions;
- to have a military medical examination;
- to investigate an industrial accident and a professional disease;
- when medical organizations exchange data;
- to exercise accounting and monitoring within the system of compulsory social insurance;
- to control the quality and safety of a medical activity.

The strict limitations are designed for proper protection of medical secrecy and confidentiality of patients in the Russian Federation. The term 'medical secrecy' does not encompass the full range of individuals who should maintain the secrecy; it refers not to doctors only but to the entire personnel of the medical institution where the patient is admitted and any people who obtained access to the data (for instance, pharmacists or lawyers). The medical secrecy includes not only medical data about the patient's health but also other data such as the patient's location, the fact of seeking medical aid, hospitalization, surveys, etc. [6, 7]

It is stressed in the concept that anybody who has access to medical information of the patients should ensure medical confidentiality, and that by doing so, they maintain patient trust in the medical system.

The legislation of the Russian Federation, namely the Federal Law 'On fundamental health care principles in the Russian Federation' as of 22.07.93 No. 5488-1 (Resolution No. 5488-1) states that citizens have the right to keep it confidential that they referred to medical aid, along with other data submitted by them while asking for medical aid. The rights include a requirement for informed and voluntary consent to medical intervention and a right to refuse from it. The rules and standards of handling medical data are also regulated by the Ethical Code of a Russian Physician (Code, 1994) [8].

As per article 30 entitled 'The Patient's Rights' of the law about fundamental principles, a patient who refers for a medical aid has a right to keep the following information confidential: fact of seeking medical aid, condition of health, diagnosis and other data obtained during examination and treatment as per article 61 hereof. The patient can also select who can obtain access to his/her health-related data (par. 6.9 of article 30) [8].

According to article 31 'Citizens' rights to health information', the data contained within the citizen's medical documents constitutes medical secrecy and can be disclosed without a citizen's consent only in cases set in article 61 hereof. It also guarantees the right of everyone to obtain health-related data in any convenient form including data about the survey results, the presence of a disease, prognosis, methods of treatment, related risks, possible interventions and their consequences, and treatment outcomes [8].

According to article 61 'Medical secrecy', data confirming that medical assistance was sought, information about a citizen's health, diagnosis and other data obtained during an examination and therapy are considered as medical secrecy [8].

The right of citizens for confidentiality of transferred data while obtaining medical assistance and other information constituting medical secrecy entails responsibility of medical workers and other persons for disclosure of data. The responsibility can include administrative, disciplinary or criminal measures in accordance with the legislation of the Russian Federation and republics within the Russian Federation.

Analyzing the regulation of the legal status of medical secrecy, the head of the department of social legislation of the Institute of Legislation and Comparative Law affiliated to the Government of the Russian Federation Natalia Putilo has noted a growing tendency to exclude something belonging to medical secrecy. Thus, the previous edition of the Legislation of the Russian Federation on the Protection of the Health of Citizens (approved by the Supreme Court of Russia as of 22 July 1993 No. 5487-1, which is no longer in effect) had five positions related to the exclusions of medical secrecy disclosure, whereas the previous and current editions of the current law had 10 and 14 positions respectively. It should be noted that according to the decisions taken by the Constitutional Court, the Russian legislation is imperfect as far as medical secrecy goes. Additional grounds have to be established in relation to disclosure of medical secrecy to relatives of deceased patients in certain cases. According to the expert, the respective legislation is under development now. It means that there is a growing number of exclusions in relation to medical secrecy disclosure[2].

The issue about the legislative regulation of telehealth services deserves separate discussion [2]. Telehealth technologies represent the means of distant interaction between medical professionals and patients, identification of participants and records of medical consultations and observations. In the legal society, there exist two opposite opinions about the subsequent regulation of telehealth technologies. Some experts believe that the existing regulation is not sufficient and needs to be more rigid and detailed. Others believe that the current standards are elaborated enough and that excessive regulation prevents novel information technologies from development[9].

In the light of medical sector digitalization, numerous processes of data treatment have gone to electronic format. Increased information puts more responsibility on its safety. Thus, information safety in medicine requires to observe three principles: integrity, accessibility and confidentiality. It is necessary to protect not just information but also the infrastructure used to process the data. Moreover, the medical sphere is a part of critical informational structure; the subjects of the sphere have to protect the data and correspond to safety requirements [1].

Medical institutions have numerous personal data belonging to employees and patients. Many of the data represent medical secrecy [10, 11]. Due to that, their vulnerability to various cyber-threats, either of which represents unique challenges and risks, is increased even more. Ransomware attacks are of particular concern. Let's consider the WannaCry attack in 2017, which seriously affected the National Health Service (NHS) of Great Britain and showed the vulnerability of medical systems to similar threats [12].

Personal medical information (PMI) is highly valued in the black market. So, data theft also poses significant risks. A good example is the Anthem Data Breach of 2015, when hackers were able to steal 79 million member's records [13].

Phishing attack is another common threat aimed at health care workers. Its goal is to extract confidential information or install malware. This is what happened in 2019 at the University of Washington Medicine when a misconfigured server had resulted in almost million of patient data being exposed online [14].

Internal threats, either intentional or accidental, are also a problem in medicine. The incident in 2018 when a nurse of a New-York hospital Illegally obtained access to patients'

medical records by breaching their confidentiality can serve as an example [15].

A growing use of connected medical devices or Internet of Medical Things (IoMT) brings about new vulnerabilities. For instance, FDA report on pacemaker safety made in 2017 underlines potential IoMT related risks [16].

Supply chain attacks is another vector of cyber-threats when intruders target third-party suppliers associated with medical institutions. In 2020, the security of a large American-based hospital system was breached through a supplier. Millions of patients were affected [17].

DDoS (Distributed Denial of Service) attacks can paralyze IT health care systems as in case of DDoS attack launched in April 2014 on Boston Children's Hospital when the operation of the hospital was seriously disrupted [18].

So, information safety in medicine acquires even more importance. Artificial intelligence (AI) is an important ally here as it offers novel solutions to solidify the security of data and keep them confidential. The ability of AI to rapidly analyze huge amounts of data, detect abnormalities and react to online threats revolutionizes the way data protection is handled. AI-based technologies will reformat the methods used by us to protect and treat the confidential data by ensuring a high safety standard within our interconnected world, starting from predictive threat analysis and ending with complex encryption methods [19, 20]. The AI systems are good at analyzing samples and abnormalities seen in the large sets of data, making them more effective in the field of advanced threat detection than regular software. They can examine normal network behavior and rapidly determine deviations, which can point at a security alert such as unauthorized access or attempts of data exfiltration. Early detection is essentially important to prevent or mitigate the consequences of violation of personal data security [21].

AI can respond to threats faster than humans. As soon as a threat is detected, AI can take actions immediately such as isolation of involved systems, block of suspicious network traffic or activation of other security protocols to prevent subsequent damage. Moreover, AI can conduct a predictive analysis based on historical data, which allows to predict and prevent potential safety threats [22].

AI increases data safety by improving encryption methods. By optimizing encryption, AI makes it difficult for unauthorized users to access confidential data. These AI-based encryption methods are constantly evolving and outpace intuder's attempts to crack the security code [23].

The biometric authentication systems represent another area with a significant contribution from AI. AI improves facial recognition, fingerprint scanning and voice recognition by ensuring a better security access to confidential information as compared to traditional passwords [24].

As far as maintenance of confidentiality during data analysis goes, AI can extract valuable data from big data with simultaneous protection of single data points. Some methods such as differential confidentiality prevent data analysis results from breaching individual confidentiality. Moreover, AI tools are crucial to ensure compliance with data protection laws such as Federal Law No. 152-FZ 'Concerning Personal Data' as they automatically evaluate whether the data handling practices within a company correspond to the required legal standards [25].

AI also improves security information and event management (SIEM) systems by correlating and analyzing security signals originating from various sources. This ensures better understanding of potential security threats. Finally, AI is invaluable while assessing templates indicative of a fraudulent activity in critical sectors such as finances and health care protecting institutions and their clients from potential fraud [26].

CONCLUSION

One of the main system requirements of the system is to ensure the confidentiality of a large amount of data accumulated at medical institutions. Due to low protection of confidential data of the existing medical information systems, there are risks that hackers will attack data systems and use personal data of patients and medical professionals for unacceptable purposes.

AI integration into medical information systems makes analysis and solution of common issues, confidentiality and safety, much more effective. AI is essential to reduce the problems by offering complex solutions, which is impossible to do with traditional methods.

AI algorithms can monitor and detect any unusual actions or potential threats within medical information systems. By analyzing patterns and detecting abnormalities, AI can present an early warning system against hacker attacks, which pose a significant risk due to low protection within the existing medical information systems.

Moreover, AI can reduce load on IT personnel at medical institutions by automating routine tasks such as data backup, encryption and disaster recovery. The automation allows to cut expenses and minimize human errors, which can be costly and harmful in sensitive medical data processing.

Finally, AI can increase the total reliability of medical information systems. Use of AI along with advanced algorithms for threat detection and response can result in a higher safety and security, which is crucial in the processing of sensitive medical information.

References

1. Sazonova M. Vrachebnaya tayna i tsifrovizatsiya: kak zashchitit' informatsiyu o patsiyente. Available from URL: https://www.garant.ru/news/1465292/ (data obrashcheniya: 30.03.2023). Russian.
2. Federal'nyy zakon ot 21 noyabrya 2011 g. № 323-FZ «Ob osnovakh okhrany zdorov'ya grazhdan v Rossiyskoy Federatsii» Available from URL: https://base.garant.ru/12191967/ (data obrashcheniya 31.03.2023). Russian.
3. Ivanov AV, Petrov VS. Osobennosti vrachebnoy tayny v kontekste meditsinskogo prava. Zhurnal meditsinskogo prava. 2016; 2: 35–40. Russian.
4. Smirnov Ye P. Zashchita personal'nykh meditsinskikh dannykh v Rossii. Zhurnal prava i interneta. 2018; 10(1): 45–60. Russian.
5. Petrova LL. Pravovyye aspekty peredachi meditsinskoy informatsii. Zhurnal meditsinskogo prava. 2017; 4: 120–135. Russian.
6. Vasil'yev DI. Raskrytiye meditsinskoy informatsii bez soglasiya patsiyenta: zakonodatel'stvo i praktika. Zhurnal zdravookhraneniya i meditsinskogo prava. 2019; 15(2): 200–210. Russian.
7. Federal'nyy zakon ot 27 iyulya 2006 g. № 152-FZ «O personal'nykh dannykh» Rezhim dostupa: [Elektronnyy resurs] URL: https://base.garant.ru/12148567/ (data obrashcheniya 31.03.2023). Russian.
8. Nazarenko GI, Guliyev YaI, Yermakov DYe. Meditsinkiye Informatsionnyye sistemy: teoriya i praktika. Pod red. G. I. Nazarenko, G. S. Osipova. M.: FIZMATLIT. 2005; 320 s. Russian.
9. Sazonova M. Zdorov'ye i tekhnologii: pravovyye problemy vzaimodeystviya. Available from URL: https://www.garant.ru/article/1453970/ (data obrashcheniya 30.03.2023). Russian.
10. Federal'nyy zakon ot 26 iyulya 2017 g. № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii

Available from URL: https://base.garant.ru/71730198/ (data obrashcheniya 31.03.2023). Russian.
11. Ivanov A, Petrova M. Povysheniye bezopasnosti dannykh v meditsine s pomoshch'yu resheniy na osnove iskusstvennogo intellekta. Zhurnal meditsinskoy informatiki. 2022; 33(4): 207–219. https://doi.org/10.1080/medinf.2022.207219 Russian.
12. CBS News. Massive ransomware attack hits 74 countries. 2017, May 14.
13. Husted ET, Jaffe M. Big Health Care Data Breaches Like Anthem's Are Common. NPR. 2015, February 6.
14. Clarridge C. Data breach at UW Medicine exposes information of nearly 1 million patients. The Seattle Times. 2019, February 20.
15. United States Department of Health and Human Services. Conduent Community Health Solutions of New York. OCR Breach Portal. 2018.
16. U. S. Food and Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. 2017, August 29.
17. Whittaker Z. Millions of Americans' medical images and data are left 'unprotected' online. TechCrunch. 2019, September 18.
18. Heimes J. The 10 Biggest Healthcare Data Breaches of 2020, So Far. HealthITSecurity. 2020, June 24.
19. Ellement JR. At first, a hacker was convicted of RICO charges for using a 'botnet.' Boston Globe. 2018, October 1.
20. Smit Dzh., Dzhonson K. Il i setevaya bezopasnost': obnaruzheniye ugroz s pomoshch'yu mashinnogo obucheniya. Zhurnal kiberbezopasnosti. 2022; 18(2):123–135. https://doi.org/10.1080/12345678.2022.1234567. Russian.
21. Li M., Kim YU. Bystryy otklik i ustraneniye kiberugroz s pomoshch'yu sistem na baze Il. Mezhdunarodnyy zhurnal informatsionnoy bezopasnosti. 2023; 22(1): 67–79. https://doi.org/10.1007/s10207-022-00555-4. Russian.
22. Patel' R, Gupta S. Uluchsheniye metodov shifrovaniya dannykh s pomoshch'yu tekhnik Il. Zhurnal prikladnoy kriptografii. 2022; 9(4): 301–317. https://doi.org/10.1016/j.jappcry.2022.03.001. Russian.
23. Tompson A, Chzhan B. Il v biometricheskoy autentifikatsii: novaya era bezopasnosti. Segodnyashniye biometricheskiye tekhnologii. 2023; (1): 14–22. https://doi.org/10.1016/j.btt.2023.01.003. Russian.
24. Devis Ye, Kumar V. Sokhraneniye konfidentsial'nosti dannykh v epokhu Il. Zhurnal zashchity dannykh i konfidentsial'nosti. 2022; 5(2): 210–225. https://doi.org/10.1016/j.jdpp.2022.04.002. Russian.
25. Grin F, Braun L. Il v sistemakh SIYEM: usileniye upravleniya bezopasnost'yu sobytiy. Zhurnal setevoy bezopasnosti. 2022; 17(3): 134–147. https://doi.org/10.1080/15733021.2022.1189072. Russian.
26. Nguyen KH, Chang Dzh. Obnaruzheniye finansovogo i meditsinskogo moshennichestva s pomoshch'yu Il. Zhurnal upravleniya moshennichestvom. 2022; 11(4): 32–45. https://doi.org/10.1080/jfm.2022.11223344. Russian.

Литература

1. Сазонова М. Врачебная тайна и цифровизация: как защитить информацию о пациенте. Режим доступа: [Электронный ресурс] URL: https://www.garant.ru/news/1465292/ (дата обращения: 30.03.2023).
2. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» Режим доступа: [Электронный ресурс] URL: https://base.garant.ru/12191967/(дата обращения 31.03.2023).
3. Иванов А. В., Петров В. С. Особенности врачебной тайны в контексте медицинского права. Журнал медицинского права. 2016; 2: 35–40.
4. Смирнов Е. П. Защита персональных медицинских данных в России. Журнал права и интернета. 2018; 10(1): 45–60.
5. Петрова Л. Л. Правовые аспекты передачи медицинской информации. Журнал медицинского права. 2017; 4: 120–135.
6. Васильев Д. И. Раскрытие медицинской информации без согласия пациента: законодательство и практика. Журнал здравоохранения и медицинского права. 2019; 15(2): 200–210.
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» Режим доступа: [Электронный ресурс] URL: https://base.garant.ru/12148567/ (дата обращения 31.03.2023).
8. Назаренко Г. И., Гулиев Я. И., Ермаков Д. Е. Медицинкие Информационные системы: теория и практика. Под ред. Г. И. Назаренко, Г. С. Осипова. М.: ФИЗМАТЛИТ. 2005; 320 с.
9. Сазонова М. Здоровье и технологии: правовые проблемы взаимодействия. Режим доступа: [Электронный ресурс] URL: https://www.garant.ru/article/1453970/ (дата обращения 30.03.2023).
10. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» Режим доступа: [Электронный ресурс] URL: https://base.garant.ru/71730198/ (дата обращения 31.03.2023).
11. Иванов А., Петрова М. Повышение безопасности данных в медицине с помощью решений на основе искусственного интеллекта. Журнал медицинской информатики. 2022; 33(4): 207–219. https://doi.org/10.1080/medinf.2022.207219
12. CBS News. Massive ransomware attack hits 74 countries. 2017, May 14.
13. Husted E. T., Jaffe M. Big Health Care Data Breaches Like Anthem's Are Common. NPR. 2015, February 6.
14. Clarridge C. Data breach at UW Medicine exposes information of nearly 1 million patients. The Seattle Times. 2019, February 20.
15. United States Department of Health and Human Services. Conduent Community Health Solutions of New York. OCR Breach Portal. 2018.
16. U. S. Food and Drug Administration. Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. 2017, August 29.
17. Whittaker Z. Millions of Americans' medical images and data are left 'unprotected' online. TechCrunch. 2019, September 18.
18. Heimes J. The 10 Biggest Healthcare Data Breaches of 2020, So Far. HealthITSecurity. 2020, June 24.
19. Ellement JR. At first, a hacker was convicted of RICO charges for using a 'botnet.' Boston Globe. 2018, October 1.
20. Смит Дж., Джонсон К. ИИ и сетевая безопасность: обнаружение угроз с помощью машинного обучения. Журнал кибербезопасности. 2022; 18(2):123–135. https://doi.org/10.1080/12345678.2022.1234567.
21. Ли М., Ким Ю. Быстрый отклик и устранение киберугроз с помощью систем на базе ИИ. Международный журнал информационной безопасности. 2023; 22(1): 67–79. https://doi.org/10.1007/s10207-022-00555-4.
22. Патель Р., Гупта С. Улучшение методов шифрования данных с помощью техник ИИ. Журнал прикладной криптографии. 2022; 9(4): 301–317. https://doi.org/10.1016/j.jappcry.2022.03.001.
23. Томпсон А., Чжан Б. ИИ в биометрической аутентификации: новая эра безопасности. Сегодняшние биометрические технологии. 2023; (1): 14–22. https://doi.org/10.1016/j.btt.2023.01.003.
24. Дэвис Е., Кумар В. Сохранение конфиденциальности данных в эпоху ИИ. Журнал защиты данных и конфиденциальности. 2022; 5(2): 210–225. https://doi.org/10.1016/j.jdpp.2022.04.002.
25. Грин Ф., Браун Л. ИИ в системах СИЕМ: усиление управления безопасностью событий. Журнал сетевой безопасности. 2022; 17(3): 134–147. https://doi.org/10.1080/15733021.2022.1189072.
26. Нгуен Х., Чанг Дж. Обнаружение финансового и медицинского мошенничества с помощью ИИ. Журнал управления мошенничеством. 2022; 11(4): 32–45. https://doi.org/10.1080/jfm.2022.11223344.