МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / METHODS AND SYSTEMS OF INFORMATION PROTECTION, INFORMATION SECURITY

DOI: https://doi.org/10.23670/IRJ.2024.142.38

ORGANIZATIONAL AND LAW ASPECTS OF MEDICAL INFORMATION SYSTEMS

Research article

Gorbunov N.[1], *, Kuleshova V.[2], Korzhuk V.[3]
[1] ORCID : 0009-0004-2973-9594;
[2] ORCID : 0000-0003-1377-6003;
[3] ORCID : 0000-0002-0240-9067;
[1, 2, 3] ITMO University, Saint-Petersburg, Russian Federation

* Corresponding author (gorb-2157[at]mail.ru)

Abstract

The article describes the systematization of the approach to the formation of a list of organizational and distribution documents (ODD) on information security (IS) that need to be developed for medical information systems (MIS) with new goals and objectives. It is proposed a unique list of ORD for MIS, which are created to implement new complex functionality. For the writing of this scientific article, the lists of ODD were taken as a research material, which were created for the MIS of the «Netrika Medicine» company. The necessary and sufficient list of ODD for MIS is presented in the format of a table. The practical result shows that in newly developed MIS, the composition of the ODD can be formed based on the results of an analysis of the IS requirements. There were identified, as theoretical results, classification similarities in the composition of ODD for new MIS. It is concluded that the systematization of formation of a list ORD for MIS, developed for the implementation of digital health, is recommended for use.

Keywords: medical information systems, organizational and distribution documents.

ОРГАНИЗАЦИОННО-ПРАВОВЫЕ АСПЕКТЫ МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Научная статья

Горбунов Н.А.[1], *, Кулешова В.[2], Коржук В.М.[3]
[1] ORCID : 0009-0004-2973-9594;
[2] ORCID : 0000-0003-1377-6003;
[3] ORCID : 0000-0002-0240-9067;
[1, 2, 3] Университет ИТМО, Санкт-Петербург, Российская Федерация

* Корреспондирующий автор (gorb-2157[at]mail.ru)

Аннотация

В статье описана систематизация подхода к формированию перечня организационно-распределительных документов (ОРД) по информационной безопасности, которые необходимо разработать для медицинских информационных систем (МИС) с новыми целями и задачами. Предложен уникальный перечень ОРД для МИС, которые создаются для реализации нового комплексного функционала. Для написания данной научной статьи в качестве исследовательских материалов взяты перечни ОРД, созданные для МИС компании «Нетрика Медицина». Необходимый и достаточный перечень ОРД, используемый в МИС, представлен в виде таблицы. Практический результат показывает, что во вновь разрабатываемых МИС состав ОРД может формироваться по результатам анализа требований информационной безопасности. В качестве теоретических результатов были выявлены классификационные сходства состава ОРД для новых МИС. Сделан вывод, что систематизация подхода к формированию перечня ОРД для новых МИС, целью которых является реализация цифрового здравоохранения, рекомендована к использованию.

Ключевые слова: медицинские информационные системы, организационно распорядительные документы.

Introduction

Public and private medical organizations process a great deal of confidential information on an ongoing basis. Such confidential processing may include personal data (PDt) [1], information from government systems [2], as well as information about critical information infrastructure (CII) [3]. Information, the processing of which in the IMS has a high level of importance, protection class and significance category. It cannot be denied that information transmitted to MIS needs enhanced protection, as it is a tasty morsel for cybercriminals.

In previous publication, which presented for portal of the educational and information-methodological «Evercare.ru» [4], it is demonstrated a detailed story about the protection of PDt, from the point of view of understanding the specifics of IS for MIS, the list of threats, the probability of which is high during theft, modification and uncontrolled leaks into the hands of attackers of information of medical properties. The article about methodology of forming list of PDt processed in MIS, which are developed to perform new functionality, have been confirmed [5]. In this scientific article is supplemented that data processed in MIS is also parts of government IS and CII. In order to understand the need to implement measures to carry out technical and, of course, important organizational manipulations to ensure information security, it is necessary to analyze the IS requirements. It is important to underline the types of IS requirements for MIS. During the discussion, the importance of organizational and law aspects of protecting PDt, government information systems and CII will be described.

Analyzing the existing challenges and threats to IS in healthcare, it is important to underline that the proposed list of ODD satisfies the IS requirements for the protection of PDt, government systems and CII. This versatility of the ODD set can significantly reduce the cyber threats described above that are characteristic of MIS.

The purpose of this article is to systematize the approach to creating a list of ODD for the digitalization of healthcare by means of using MIS.

Based on the methods used in the development of MIS, created by «Netrika Medicine» company [6], in order to achieve goals, the task was formulated to present a list of ODD for MIS, which are developed to perform new possibilities.

There were used methods of search and cognition, logical inference, methodological design, as well as system analysis at the moment of preparation materials for writing this scientific article.

The novelty of the scientific research is in the fact that a universal list of ODD for MIS with new functionality was developed. The versatility noted above is due to the fact that ODD for MIS have to satisfy the IS requirements for protecting PDt, government information systems and CII. The list of ODD was compiled based on the results of a study of various information systems, however, it was identified unique features of the composition of ODD that are applicable specifically in MIS.

The relevance of the study is in the points that identified the dependence of the types of ODD for MIS on the species, qualitative and quantitative indicators of MIS located in various data processing centers. It is known that most of these data centers have a certificate of compliance [7] with IS requirements for the protection of PDt, government information systems and CII. The resulting indicators were systematically achieved in the form of a tabular presentation (Table 1), which certainly has practical originality at the moment when developing a list of ODD for MIS with new functionality. The most originality composition of ODD for MIS could be described as a situation that this list is satisfied the IS requirements for protecting PDt, government information systems and CII.

For the creating this scientific article, the composition of ODD for the MIS of the «Netrika Medicine» company was analyzed as a research data. It is becoming possible because limited liability company «Netrika Medicine» specializes in the secure integration and creation MIS for regional services, doctors, patients and healthcare organizers. The IS system is a subsystem and is developed on the functions, goals, threat modeling and objectives for medical organizations.

It is obvious that IS systems have two most important clusters: technical equipment and organizational measures. Many information technology companies often do not pay due attention to ODD concentrating on the technical components of protection. It is understanding, because IS specialists are associated with real hardware and often organizational measures are given to technical documentation department. However, representatives of IS department «Netrika Medicine» company are convinced, that for achieving long-term goals for the digitalization of healthcare it is constantly necessary to renovate ODD for MIS.

The methodological value of the research described in this scientific article lies in the systematization of practices for forming a list of ODD, which are important to consider as potential when it is necessary to develop new MIS.

Research methods and principles

Guided by the principle of the inalienability of the organizational component, according to production needs ODD were created for MIS deployed in different data processing centers, certified according to various IS requirements.

There were needed certified data processing centers according to IS requirements of protecting PDt, first of all. That is why using manuals about PDt protecting, in particular government decree about the protection of PDt processed in PDt information systems [8], representatives of IS department developed necessary ODD for MIS, which were created in period decade of tenths of years.

To the second type of certified data processing centers it possible to describe according to IS requirements of protecting government information systems. Due to these needs using manuals about protecting state networks, namely order of the FSTEC of Russia № 17 about IS in government information systems [9], representatives of IS department developed necessary ODD for MIS, which were created in period of the late tenth years.

During the current period of difficult situation, when most CII facilities are constantly being attacked by intruders, medical information and analytical centers in various regions of our country are gradually acquiring the category of CII. Representatives of IS department «Netrika Medicine» directly take part in format of consultation in this labour-intensive process. The main management document in this movement is methodology about categorization of CII subjects [10].

The hardest moment to date, part of the MIS software has been implemented for the Microsoft SQL server database management system. In view of the fact that in the near future many customers will be subjects of CII or already are, and also plan to carry out certification work, the software for MIS have to be implemented under the special-purpose operating system «Astra Linux Special Edition» (Voronezh release) [11]. Also, CII subjects are starting to use the secure database management system «PostgreSQL», which is also certified as part of the above operating system in the certification systems of the Russian Ministry of Defense, FSTEC of Russia and the FSB of Russia for compliance with IS requirements. The task of switching to Linux-like OS is also complicated by the need to develop a database converter from «SQL Server» to «PostgreSQL». As part of import substitution, developers are working on the transition to a Linux-like operating system and database management systems. At the same time, the development of new software components for MIS have to be carried out for Linux-like systems. The pilot region where the software for the MIS of limited liability company «Netrika Medicine» has been deployed is the Rostov region. Certification work is tentatively scheduled for November 2024.

Studying scientific articles of the IS specifics for healthcare, the advantages of the ODD set described in this article were confirmed in review materials MIS as objects of evaluation [12]. It is identified a constant development of the IS subsystem for MIS, including the renovating of the list of ODD. At different periods of time, MIS first became the PDt information system, the government system and CII. Considering that at these stages of development, financial for the modernization of ODD, and a single study was carried out for each MIS, systematization for the development of ODD set described in this article looks like a clear advantage. Possible disadvantages of the systematization compared to other methods include the fact that the list of ODD described in this article is not relevant for the Ministry of Defense.

An innovation in the field of IS for MIS could be artificial intelligence, which would generate a list of ODD. Thus, as in the MIS itself, where artificial intelligence is currently not applicable, so in the IS subsystem this is still unlikely.

A real-life example of the use of ODD list is MIS developed Netrika Medicine company, which deployed in more than 10 regions of our country. In particular, these are such software products [6] as «Telemedicine», «Patient Flow Management», «Patient Portal», «Access Management System» and «Integrated Electronic Medical Record».

It is generally analyzed the different requirements of regulators for ensuring IS in various information systems [3], [8], [9]. It would seem that each of these guidance documents includes its own set of specific requirements. One gets the feeling that ensuring IS for different MIS will be carried out in parallel, and not together. In fact, any IS specialist will say that most of the requirements are partially repeated. In this case, it is clearly that 85-95% of requirements are repeated at least once. In this regard, there are only 5-15% of the requirements are unique. In conclusion analysis of regulatory documents, it is clear that the MIS consist of requirements for CII, government systems and information systems of PDt.

At the same time, the contract for the development of MIS in the Rostov region was successfully completed and agreed upon by the receiving authorities, including acceptance tests of the IS subsystem. To complete the stages of work, it was necessary to develop ODD for the protection of PDt, state information systems, as well as CII subjects. In this regard, it was decided to develop complex operational ODD that satisfy the above properties. That is why, when it is necessary to form technical specifications and projects for newly developed MIS, it is recommended taking as a basis the list of ODD for IS given in Table 1.

Table 1 - Composition of ODD for MIS

DOI: https://doi.org/10.23670/IRJ.2024.142.38.1

№	Name
1	IS policy
2	Order, instruction about localization of information
3	Order, instruction, magazine of computer storage media
4	Order, regulation about control
5	Order about the list of protected information
6	Order approving the assessment of harm
7	Order and instructions on access procedures
8	Order and magazine about storage locations of protected information
9	Order on the procedure for considering appeals
10	Order and instructions about storage periods
11	Order about instructions for users and personnel in case of emergency situations, organization of password protection, anti-virus control, backup

Main results

Using the example of the MIS of the «Netrika Medicine» company, the results of implementation of the developed ORD for MIS in the following regions were identified: St. Petersburg, Leningrad Region, Rostov Region, Stavropol Territory. Other regions of coverage have not yet completed the stage of categorizing CII, but there is one certainty that for their needs the also developed ORD will be in demand and relevant.

The practical recommendations for using the ODD list include work on designing a secure MIS. That is why, at the stage of forming IS threat model for the above-mentioned MIS, developed by the «Netrika Medicine» company, attention is focused on the procedure for forming configuration of ODD. Additionally, the types of ODDs being created were identified and the need for additional information security measures when processing sensitive data was processed.

Conclusion

Summing up the results of the research, it is important to underline that the relevance, scientific nature, methodological and practical value of the materials describing a systematic approach to the formation of a list of ODD for information security for new MIS have been confirmed. Thus, when developing the ODD composition for MIS, it is necessary to use the method of their formation described in this scientific article.

Конфликт интересов

Не указан.

Рецензия

Сообщество рецензентов Международного научно-исследовательского журнала
DOI: https://doi.org/10.23670/IRJ.2024.142.38.2

Conflict of Interest

None declared.

Review

International Research Journal Reviewers Community
DOI: https://doi.org/10.23670/IRJ.2024.142.38.2

Список литературы / References

1. Российская Федерация. О персональных данных : Федеральный закон No 152: [принят Государственной Думой 2024-04-17 :одобр. Советом Федерации2024-04-17]. 2006. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (дата обращения: 12.03.2024)

2. Российская Федерация. Об информации, информационных технологиях и о защите информации : Федеральный закон. — 2006. — URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (дата обращения: 12.03.2024)

3. Российская Федерация. О безопасности критической информационной инфраструктуры : Федеральный закон No 187: [2024-03-13 :2024-03-13]. 2017. — URL: https://www.consultant.ru/document/cons_doc_LAW_220885 (дата обращения: 12.03.2024)

4. Горбунов Н.А. Информационная безопасность в здравоохранении: основные аспекты / Н.А. Горбунов // Портал "EverCare.ru". — 2022 — URL: https://clck.ru/3A8LEC (дата обращения: 29.02.2024)

5. Горбунов Н.А. Персональные данные, обрабатываемые в медицинских информационных системах / Н.А. Горбунов // Международный научно-исследовательский журнал. — 2023. — № 9(135). — URL: https://research-journal.org/archive/9-135-2023-september/10.23670/IRJ.2023.135.3 (дата обращения: 12.03.2024)

6. Программные продукты компании «Нетрика Медицина» // Сайт ООО "Нетрика Медицина". — 2024 — URL: https://n3med.ru/ (дата обращения: 29.02.2024)

7. ГОСТ Р 58189-2018. Защита информации. Требования к органам по аттестации объектов информатизации — Введ. 2018-08-02. — Москва: Стандартинформ, 2018.— 3 с.

8. Российская Федерация. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : Федеральный закон No 1119. — 2012. — URL: http://government.ru/docs/all/84743/ (дата обращения: 12.03.2024)

9. Приказ ФСТЭК России от 11.02.2013 № 17. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. — 2013. — URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (дата обращения: 29.02.2024).

10. Российская Федерация. 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: Постановление Правительства РФ от 8 февраля 2018 г. № 127. — URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102460750 (дата обращения: 29.02.2024).

11. Программные продукты группы «Астра» // Сайт группы «Астра». — 2024 — URL: https://astralinux.ru/os/ (дата обращения: 29.02.2024)

12. Ваганова Е.В. Медицинские информационные системы как объект оценки: факторы и тенденции развития / Е.В. Ваганова // Вестник Томского государственного университета. — 2017. — 37. — с. 113-130. — URL: https://journals.tsu.ru/economy/&journal_page=archive&id=1544&article_id=34216 DOI: 10.17223/19988648/37/9.

Список литературы на английском языке / References in English

1. Russian Federation. O personal'nyh dannyh [About perspnal data] : Federal Law No 152: [accepted by Gosudarstvennoj Dumoj 2024-04-17 :approved by Sovetom Federatsii2024-04-17]. 2006. — URL: https://www.consultant.ru/document/cons_doc_LAW_61801 (accessed: 12.03.2024) [in Russian]

2. Russian Federation. Ob informatsii, informatsionnyh tehnologijah i o zaschite informatsii [About information, information technologies and information protection] : Federal Law. — 2006. — URL: https://www.consultant.ru/document/cons_doc_LAW_61798 (accessed: 12.03.2024) [in Russian]

3. Russian Federation. O bezopasnosti kriticheskoj informatsionnoj infrastruktury [About security of critical information infrastructure] : Federal Law No 187: [2024-03-13 :2024-03-13]. 2017. — URL: https://www.consultant.ru/document/cons_doc_LAW_220885 (accessed: 12.03.2024) [in Russian]

4. Gorbunov N.A. Informatsionnaja bezopasnost' v zdravoohranenii: osnovnye aspekty [Information security in healthcare: main aspects] / N.A. Gorbunov // Portal "EverCare.ru". — 2022 — URL: https://clck.ru/3A8LEC (accessed: 29.02.2024) [in Russian]

5. Gorbunov N.A. Personal'nye dannye, obrabatyvaemye v meditsinskih informatsionnyh sistemah [Personal data processed in medical information systems] / N.A. Gorbunov // International Research Journal. — 2023. — № 9(135). — URL: https://research-journal.org/archive/9-135-2023-september/10.23670/IRJ.2023.135.3 (accessed: 12.03.2024) [in Russian]

6. Programmnye produkty kompanii «Netrika Meditsina» [Software products of the company "Netrika Medicine"] // Website of LLC "Netrika Medicine". — 2024 — URL: https://n3med.ru/ (accessed: 29.02.2024) [in Russian]

7. GOST R 58189-2018. Zaschita informatsii. Trebovanija k organam po attestatsii ob'ektov informatizatsii [GOST R 58189-2018. Data protection. Requirements for bodies for certification of informatization objects] — Introduced 2018-08-02. — Moskva: Standartinform, 2018.— 3 p. [in Russian]

8. Russian Federation. Ob utverzhdenii trebovanij k zaschite personal'nyh dannyh pri ih obrabotke v informatsionnyh sistemah personal'nyh dannyh [About approval of requirements for the protection of personal data during their processing in personal data information systems] : Federal Law No 1119. — 2012. — URL: http://government.ru/docs/all/84743/ (accessed: 12.03.2024) [in Russian]

9. Prikaz FSTEK Rossii ot 11.02.2013 № 17. Ob utverzhdenii Trebovanij o zashchite informacii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennyh informacionnyh sistemah [Order of the FSTEC of Russia dated February 11, 2013 No. 17 On approval of Requirements for the protection of information that does not contain state secrets, is taken into account in the state information system]. — 2013. — URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702-prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17 (accessed: 29.02.2024). [in Russian]

10. Rossijskaya Federaciya. Ob utverzhdenii pravil kategorirovaniya ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii, a takzhe perechnya pokazatelej kriteriev znachimosti ob"ektov kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i ih znachenij: Postanovlenie Pravitel'stva RF ot 8 fevralya 2018g. № 127 [Russian Federation. On approval of the rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values]: Decree of the Government of the Russian Federation of February 8, 2018. No. 127. — URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102460750 (accessed: 29.02.2024). [in Russian]

11. Programmnye produkty gruppy «Astra» [Software products of the "Astra" group] // "Astra" group website. — 2024 — URL: https://astralinux.ru/os/ (accessed: 29.02.2024) [in Russian]

12. Vaganova E.V. Meditsinskie informatsionnye sistemy kak ob'ekt otsenki: faktory i tendentsii razvitija [Hospital information systems as the object of evaluation: factors and development tendencies] / E.V. Vaganova // Bulletin of Tomsk State University. — 2017. — 37. — p. 113-130. — URL: https://journals.tsu.ru/economy/&journal_page=archive&id=1544&article_id=34216 DOI: 10.17223/19988648/37/9. [in Russian]