Management of Distributed Medical Information Systems

Elena Kukharenko and Alexey Yankevskiy

Abstract The article deals with the problem of managing medical information systems, including the example of quality control of the provision of medical services using isotope-containing medical materials. A digitalization of economics leads to a strong transformation of business routines of companies in wide variety of industry branches. The transition from paper media to electronic document management systems all over the world is associated with a complex of methodological and organizational and technical tasks to ensure the availability and reliability of data, regulatory support for the interactions of all participants in the process of collecting, transferring, processing and storing information, as well as the formation of an archive of data of former periods. The mathematical model allows at the practical level to carry out multi-parameter monitoring and control in the main critical areas. The use of a qualitative assessment in parallel with a quantitative one allows the managing staff of the administration of a medical institution to obtain a more complete assessment of the situation in controlling the circulation of isotope-containing materials in the provision of medical services to the population.

Keywords Medical information system · Information technology · Management

1 Introduction

A digitalization of economics leads to a strong transformation of business routines of companies in wide variety of industry branches [1]. The transition from paper media to electronic document management systems all over the world is associated with a complex of methodological and organizational and technical tasks to ensure the

E. Kukharenko (✉)
Moscow Technical University of Communications and Informatics, Aviamotornaya St. 8A, 111024 Moscow, Russia
e-mail: e.g.kukharenko@mtuci.ru

A. Yankevskiy
Peoples Friendship University of Russia, Miklukho-Maclay St. 6, 117198 Moscow, Russia

E. Zaramenskikh and A. Fedorova (eds.), *Digitalization of Society, Economics and Management*, Lecture Notes in Information Systems and Organisation 53,
https://doi.org/10.1007/978-3-030-94252-6_14

availability and reliability of data, regulatory support for the interactions of all participants in the process of collecting, transferring, processing and storing information. as well as the formation of an archive of data of former periods [2, 3]. For example, collection and storage of large volumes of medical information on a local computer does not make sense or because of the high requirements for reliability and safety imposed by the legislation of the country for this class of information in connection with which cloud storage technologies are used to store access to it. Consider the basic principles of building geographically distributed info-communication medical systems:

- Confidentiality and security of patient data.
- Information service providers.
- Regulatory support, security policy and control.
- Infrastructure for information exchange.
- Construction options.
- Geographic locations of data storage.
- Data access models.
- Ensuring data integrity.
- Geographically distributed multi-user environment.
- Incidents in the system and algorithms for responding to them.
- Data protection (monitoring, encryption, deletion).
- Confidentiality and security of patient data.

2 Regulation

The formation of a systemic approach to the functioning of medical information systems was laid by the laws adopted by the US government in 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act and in 2003 the Health Information Portability and Accountability Act (HIPAA) in 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act. They require organizations involved in the work with health information to implement a set of measures to ensure confidentiality and security, as well as inform patients when the privacy and security of their personal data is at risk. HIPAA covers medical organizations: medical institutions, insurance companies, and medical settlement centers. The HITECH Act has extended the HIPAA Privacy Rule and Security Rule standards to business partners. Business partners provide processing and administration, data analysis and management services. A cloud provider where PHI is considered a business partner. In January 2013, the OCR published the final Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, as well as the Other Modifications to the HIPAA Rules. They are changing the definition of a business partner, improving the security and privacy of PHI, placing direct responsibility on business partners, changing the damage threshold in the Breach Notification Rule, and clarifying the

content of the business partner agreement. An important point−OCR jurisdiction extends to business partners and their subcontractors. The definition of a business partner has been changed in the Omnibus Rules. Business partner subcontractors are considered to be acting on their behalf, i.e. they are persons to whom a business partner has delegated the performance of a function covered by HIPAA.

2.1 Information Service Providers

Cloud service providers are uniquely placed among the business partners trusted by EPHI. When EPHI is stored in the cloud, consumers disclose it to a cloud provider who become a business partner and is HIPAA and HITECH compliant. Organizations are allowed to share EPHI information in the course of treatment, payment, and healthcare operations without patient consent. When exchanging, only the required minimum EPHI should be opened. Medical organizations can share EPHIs with each other and with business partners. When disclosing this information to a business partner, healthcare organizations must ensure that the business partner will adequately protect the information provided by the BAA. BAA is a Service Level Agreement containing HIPAA and HITECH compliance clauses. Medical organizations are required to enter into BAAs with business partners to whom they provide EPHI. Business Partners must enter into a BAA with their subcontractors to whom they share this information. Business partners must enter into BAAs with subcontractors. Healthcare organizations are not required to enter into separate agreements with subcontractors to provide PHI. By clearly defining the roles and responsibilities of the healthcare organization, business partner and subcontractor in the BAA, the responsibility of each party to the agreement can be reduced and the processes for reporting leaks are simplified. Agreements between healthcare organizations and business partners must adhere to the Security Rule when reporting unprotected PHI leaks to the organization, and ensure that their subcontractors comply with business partner level PHI restrictions and conditions. If the healthcare organization is aware of the business partner's activities that violate the BAA, then it must take appropriate action to correct the leak or stop the violation, and otherwise terminate the BAA. The BAA states that a business partner must comply with the Privacy Rule applicable to a healthcare organization. Even without a BAA, business partners and subcontractors are directly responsible for their actions, but agreements help define important commitments.

2.2 Unconditional Commitment

OCR emphasizes that the privacy and security of PHI should be held accountable by all who are trusted with it. Formulating these rules, OCR explains that it wants to "avoid a situation where the privacy and security of PHI is not ensured just because the

work is performed by a subcontractor and not by a business partner directly associated with a healthcare organization." Cloud service providers are directly responsible and must carefully monitor data. To avoid violations, it is necessary to constantly monitor client access to data, to ensure proper authentication procedures. This will reduce the risk of vulnerabilities, increase the chances of detecting and fixing violations before they cause damage, and also facilitate interaction with other business partners, medical organizations and the ministry in the event of a PHI leak.

2.3 Civil Monetary Penalties (CMP)

This new liability can be very costly for business partners, with penalties of up to $1.5 million per year for violation. However, OCR clarifies that this is a ceiling for one type of violation. When imposing fines, the ministry takes into account many factors and can change the amount of the fine if it is inadequate for the violation. Cloud services are specific to each consumer, especially private clouds customized to a specific client. Therefore, the cloud services provided can be an important factor in determining the amount of penalties. For example, some consumers may use software as a service (SaaS), thereby giving the cloud provider control of most of their data, including PHI. Consumers can also use open clouds. In both cases, efficient data management results in cost savings. However, such services can become a source of leaks, damaging many people in a short period of time, while a consumer using infrastructure as a service (IaaS) or a private cloud can better control leaks. Regardless of the cloud service model, the Omnibus Rules change from "history of violations" to "previous noncompliance" allows the ministry to take into account the good faith efforts of the cloud service provider, its business partners, and healthcare organizations to eliminate or mitigate leaks. Cloud providers are unlikely to have a "history of violations," and a proactive approach to compliance can be an effective way to reduce penalties.

2.4 Leaks

HHS defines an EPHI leak as "inappropriate use or disclosure… compromising the security or privacy of protected health information and posing a significant risk of financial, reputational or other harm to an individual." Since 2009, major EPHI leaks affecting medical records of 500 or more people have compromised the data of almost 21 million people. The share of business partners in large leaks was 21%. More and more information is stored electronically (including in the cloud), these statistics will inevitably change. Migration to the cloud spawns new methods of attacking EPHI. These attacks now threaten off-site EPHI, where those to whom it was originally trusted have less control. Regardless of the reason for the leak, violations of HIPAA are subject to criminal and civil penalties at both the state and federal levels.

2.5 Leak Notification

Business partners are directly responsible for leaks of PHI under their control and must report them to healthcare providers (as well as subcontractors with an agreement with business partners). Business partners who have access to, use, or disclose PHI must notify the healthcare organization if this information is leaked. After receiving the notification of the leak, the medical organization is fully responsible for notifying the affected persons, the ministry, the media and other organizations. However, OCR permits BAA parties to determine who will be responsible for the notification. OCR provides healthcare organizations and business partners with the ability to determine who will take responsibility for the notification, as well as set requirements for how, when and to whom the notification should be sent. A healthcare organization is more suited to this role than cloud providers, who may be subcontractors and located far from affected individuals. However, the cloud provider may be more able to collect information that the healthcare organization needs to include in the notification because it stores the EPHI. Therefore, the business partner must provide the healthcare organization with all available information that the organization must include in the notification. If this information cannot be provided at the time the leak is discovered, the business partner can first notify their business partner or healthcare organization of the leak and then send additional information. In addition, the regulations require the medical organization to be informed of all the facts regarding the leak, so the business partner must provide this information, even if it becomes available after sending the notification to the victims.

2.6 HIPAA Compliance: Cloud Specific Issues

Moving data to the cloud poses a number of challenges that complicate HIPAA compliance for healthcare organizations, business partners, and cloud providers themselves. These are control, access, availability, shared multi-tenant environments, incident preparedness and response, and data protection, all of which are covered in the remainder of this article. While there are many benefits to storing EPHI in the cloud, customers and cloud service providers should be aware of how each of these issues impacts HIPAA and HITECH compliance.

2.7 Control Over Data

By entrusting cloud providers with storing their data, consumers are relinquishing direct control over that data from the application layer. Due to the change in control when moving EPHI to the cloud, the consumer and supplier must clearly define in the BAA who takes responsibility for the privacy and security of the data.

3 Customer Control

The cloud service provider offers processing, storage, networking, and other resources to enable the consumer to deploy and run any software. The consumer controls the operating systems, storage systems, deployed applications, and possibly some of the networking components, and therefore must take on more responsibility.

3.1 Application and Infrastructure

Cloud computing service level models provide consumers with different levels of control, often offering appropriate security tradeoffs. Consumers and suppliers must balance their organizations and determine the risk they are willing to take in losing control of their data.

3.2 Deployment Models

Cloud deployment models themselves affect data control regardless of the application or infrastructure tier. In the open cloud model, infrastructure is publicly available, and control is lost when data is deployed. At the other end, there is a private cloud infrastructure available to only one consumer. A public cloud is available to a specific community, and a hybrid cloud combines open and private cloud models. To provide the highest level of control, and therefore the greatest confidentiality and security of EPHI, it is necessary to use a private cloud model. However, open clouds can also be used to store EPHI. The open cloud makes EPHI more vulnerable. A number of vendors specifically separate a portion of their cloud services to host EPHI-related data. However, many vendors do not, so such services can be costly to consumers. Consumers must choose the degree of risk they are willing to take when hosting data in open, private or hybrid clouds. Regardless of where consumers host their data, cloud service providers must ensure the privacy and security of EPHI in accordance with HIPAA and HITECH requirements, given the level of control they have over that data.

3.3 Geographic Location of the Data

Cloud services allow you to store data in multiple locations, which is useful in emergency situations. Storing data off-site or in multiple locations ensures that critical business operations are not interrupted. However, consumers who don't know where their data is located lose control of EPHI at a different level. They need to know

where the data is in order to understand which laws, rules and regulations must be followed. In some cases, the geographic location of EPHI may lead to problems with international legislation that is contrary to HIPAA and HITECH.

4 Access to Data

Given that the consumer loses control over the data at several levels, the question arises who has access to it and how to control access. The growing number of actors involved means more people are able to access EPHI in the cloud, increasing the risks of data security breaches. Cloud service providers and consumers must work together to ensure security by managing the granting and modification of access rights. It all starts with determining the right of a user or a computer system to carry out a certain activity.

4.1 Granting Access Rights for Personnel

It is the user's responsibility to determine who should have access to the data stored in the cloud, and the cloud provider enforces the user's decisions. All employees who may have access to EPHI must go through the clearance process. Customers, cloud providers, and those the providers work with should create job descriptions that clearly describe the responsibilities assigned to each employee and oversee compliance with them. All employees with access to EPHI must receive unique usernames and receive training to maintain the confidentiality of their registration information. Each user is granted access in accordance with his assigned role, and if necessary, the access rights must be immediately changed or revoked.

4.2 Authentication

According to HIPAA, procedures must be in place to ensure that only registered individuals have access to EPHI. This could be an authorization system using a unique username and password or other data. A number of cloud service providers offer integration with consumer authentication systems using LDAP mechanisms or single sign-on (SSO) technologies. However, these methods can themselves become a source of security threats.

4.3 Audit of Access

The Security Rule requires regular review of information system activity reports to identify any inappropriate EPHI disclosure. In addition, hardware, software, and/or procedural mechanisms must be used to record and study activity in information systems containing or using EPHI. The HITECH Act requires additional EPHI leak monitoring. Audit is a particular concern of HIPAA and HITECH because it is dependent on incident response, reporting procedures and ultimately the ability to stop and mitigate leaks.4) Integrity. The integrity of EPHI depends on who has access to the data. Suppliers and consumers have a responsibility not only to determine who has access to the EPHI stored in the cloud, but also to maintain the integrity of the data and protect it from tampering.

4.4 Common Multi-User Environment

Open cloud services are cost-effective because such infrastructure often includes shared multi-tenant environments, whereby consumers share components and resources with other consumers that they do not know.

4.5 Data Availability

One of the Security Rule is the availability of EPHI, especially in case of emergency or other incidents. One of the benefits of moving EPHI to the cloud is the ability to improve data availability in a variety of ways. Cloud services that store redundant data in multiple locations are better at handling disasters.

5 Preparedness and Response to Incidents

Incident response is a key issue in HIPAA and HITECH compliance. Regardless of the number of actions taken, not all incidents can be prevented.

5.1 Preparedness for Incidents

Before an incident occurs, customers and suppliers must develop specific policies and procedures, such as an emergency plan. They must perform proactive monitoring of

threats and vulnerabilities. Cloud service providers must communicate these vulnerabilities to customers so that they can determine the acceptability of risks or fix vulnerabilities. In addition to locating EPHI and assessing risk, consumers must back up their data. A backup EPHI must be created and maintained. Cloud services provide the ability to back up data externally. Consumers and cloud providers must control access to EPHI and ensure that only authenticated authorized users get it. Cloud service providers and consumers must continually test for vulnerabilities and adjust their policies and procedures accordingly.

5.2 Incident Response

The cloud provider must respond to incidents and is responsible for verifying and analyzing incidents, isolating consequences, collecting data, storing, resolving problems and restoring normal operations. Based on the results of the investigation, he must isolate the consequences of the incident to ensure the confidentiality, integrity and availability of EPHI. Customers should determine how an incident will be verified and how information will be collected to analyze it.

6 Data Protection

Transferred data and backups must be protected in different ways. Security measures must be taken by cloud service providers and include: monitoring, encryption, key management, and data deletion.

6.1 Monitoring Data Leaks

By handing over control of data to a cloud provider, consumers are forced to rely on the processes that the provider uses to monitor data leaks on their systems. Such as firewalls, network intrusion detection, monitoring server logs and end user access. Cloud service providers must perform regular checks to ensure that they are operational. If a leak or vulnerability is discovered, the cloud provider must inform the consumer.

6.2 Encryption

Organizations can encrypt data to make it unusable, unreadable, or indecipherable by unauthorized persons.

6.3 Key Management

Encryption key management schemes are another way to protect data. Consumers can use this tool on their own or through a cloud service provider. Those who already use key management schemes must address the issues of securing key vaults, limiting access to vaults, and their backup and recovery.

6.4 Data Deletion

The Security Rule requires healthcare organizations and business partners to "implement policies and procedures for the permanent disposal of electronic health information and/or the hardware or electronic media on which it is stored." Therefore, cloud service providers must ensure that the EPHI is correctly deleted and cannot be re-created at the request of consumers, including from backups.

The use of geographically distributed medical information systems of electronic document management using cloud technologies of various types allows doctors to collect more information to study patient histories. Various systems for the exchange of information about the patient's health constantly perform operations to exchange information, which creates risks and vulnerabilities for such systems.

Medical staff are no longer the only owners and custodians of confidential information about a patient's health, medical history and prescribed procedures and drugs and treatment plan. For example, employees of telecommunications companies or system integrators who manage the storage of data also have access to this information and, thus, are responsible for its safety.

Analysis of statistical data and the practice of operating the currently geographically distributed information and communication systems in the field of treatment of cancer patients in cities with a population of one million allows us to formulate the management task for this class of systems—the level of a metropolis—in a balanced way.

From the point of view of management of complexes of systems, it is most clearly and more convenient from the point of view of information presentation, when the features describing control objects have a qualitative characteristic.

This is due to the fact that the quality parameter is more stable and unchanged over time.

It is not characterized by the uncertainties inherent in quantitative parameters, possible incompleteness of information about the object, various subjective quantitative inaccuracies, etc.

In the case of a study of multidimensional control systems of the scale of a megalopolis, it becomes necessary to compare (compare) the systems and objects from them according to several common features.

In particular, in some cases, some of the parameters of objects lend themselves to quantitative assessment, and some cannot be expressed numerically.

7 Formulation of the Control Problem

Based on the above data and a balanced analysis of the parameters affecting the system in the use of medical information systems for the provision of medical services to cancer patients, the following management task is formulated: multi-parameter control of the quality of services provided to the population in the field of health care using isotope-containing radioactive materials.

Construction and analysis of a mathematical model for the development of medical information systems for the treatment of cancer patients.

Based on the formulated problem, we will construct a mathematical model using the optimized quantitative parameters. Limitations imposed on the system:

External:

- Federal Legislation (Constitution).
- Regional level legislation.
- City legislation.

Internal:

- The current level of development of technologies in medicine.
- The patient's health status.

Using the "black box" principle, we will graphically represent the economic and mathematical model of the control problem with corrective feedback (Fig. 1).

$$N' = F[N] = F[H;\ T;\ G], \tag{1}$$

where:

H—A set of parameters describing the availability of employees with the proper qualifications for the process of providing services.

T —A set of parameters describing the logistics of the service delivery process.

G —A set of parameters describing the environmental component of the service delivery process.

Figure 2 shows a graphical representation of the mathematical model with detailing from the general view (Formula 1) to detailing by parameters.

where:

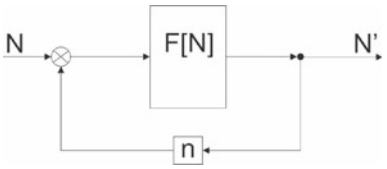

Fig. 1 General mathematical model of the system. Where N is a set of input parameters, N 'is a set of output parameters, n—corrective action. In general, the functional is as follows:

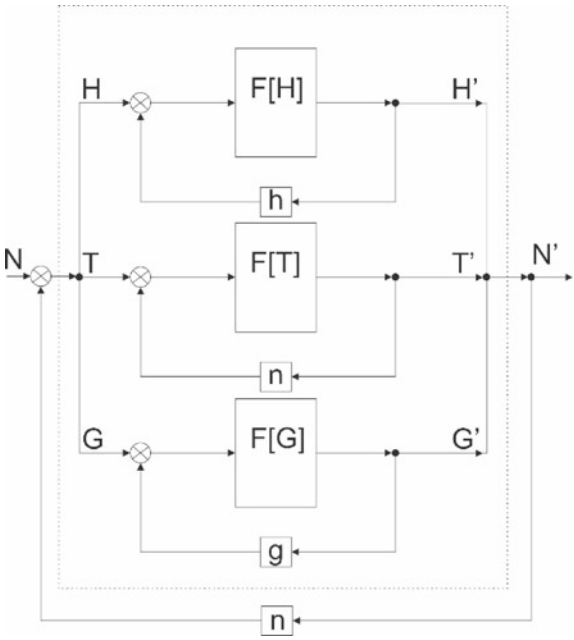

Fig. 2 A mathematical model with a representation by parameters

H is a set of input parameters according to the level of training of human resources (Formula 2).

H' is a set of output parameters by the level of training of human resources,

h —Corrective action on the level of training of human resources,

T is a set of parameters for the provision of services (Formula 3).

T' is a set of output parameters for the provision of services, t is the corrective action for the provision of services.

G is a set of parameters associated with the circulation of isotopic materials (Formula 4).

G 'is a set of output parameters associated with the circulation of isotopic materials.

g is the corrective action associated with the circulation of isotopic materials.

Let us write the set for each of the parameters in the form of functionals:

$$H' = F[H] = F[E, S, P, O], \tag{2}$$

where:

E —personnel training;

S —personnel certification;

P —practical experience;

O —staffing with proper qualifications.

$$T' = F[T] = F\left[Eqm,\ Eqit,\ Est,\ Sec\right], \tag{3}$$

where:

Eqm is a set of measures for the software and hardware of the process of providing medical services;

Eqit is a set of measures for software and hardware exchange of information between participants in the process;

Est —a set of measures for archiving and data storage hardware and software;

Sec is a set of measures for information security software and hardware and information protection.

$$G' = F[G] = F[M,\ St,\ U,\ Ut], \tag{4}$$

where:

M —a set of measures for the transportation of isotopic materials;

St —a set of measures for the storage of isotopic materials;

U —a set of measures to ensure the normal use of isotopic materials;

Ut —a set of measures to ensure the utilization and disposal of isotopic materials.

Final functional is as follows:

$$N' = F[N] = F[H; T; G] = F\left[E,\ S,\ P,\ O; Eqm,\ Eqit,\ Est,\ Sec; M,\ St,\ U,\ Ut\right] \tag{5}$$

Thus, the final functional is a set of vector matrices for each of the optimized parameters. The area where the optimal values are found is graphically represented as a three-dimensional figure. The volume of this figure is calculated using a double integral. In the absence and/or loss of a part of the statistical values of previous periods, genetic algorithms for multicriteria optimization (GAMO) with Cauchy and Pareto optimization are used to find the missing parameter values. Analysis of the proposed mathematical model makes it possible to provide the following control functions: in terms of the time of the event, from the point of view of the object of control.

Control functions in terms of the time of the event (point of time, PoT) can be illustrated at high level as it is presented in Fig. 3.

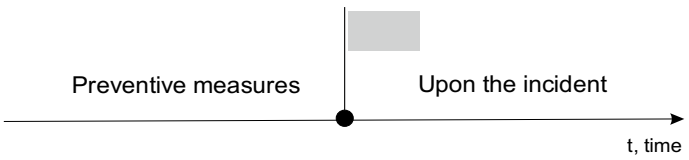

Fig. 3 Control function in terms of the time of the event

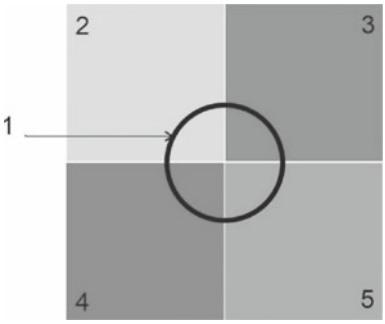

Fig. 4 Control function from the prospective of the controlled object. Here 1 —is Patient (ID); 2 —Medical and scientific staff; 3 —Clinic; 4 —Equipment; and 5—Interaction

The Flag sign in Fig. 3 denotes the time of the incident (events outside the controlled parameters). All functions can be split into two groups: Preventive measures such as monitoring of the current activities of organization and checking the current activities of organizations for compliance with regulations and upon the incident actions such as investigation of incidents and the development of recommendations for the prevention of incidents.

Control functions from the point of object (PoO) prospective are represented by the diagram in Fig. 4.

Patient (ID is a unique patient number in the electronic medical document management system):

- Electronic medical history,
- Survey results,
- Treatment plan,
- Results of stages of treatment.

Medical and scientific staff:

- Training,
- Personnel certification,
- Control over the planning and execution of works,
- Provision of institutions with personnel with proper qualifications.

Clinic:

- Which clinic examined,
- Who conducted the survey,
- Who prepared the treatment plan,
- Who reviewed and approved the treatment plan,
- Who performed the treatment,
- Results at each stage of treatment,
- Compliance with treatment regulations.

Equipment:

- What equipment was used,

- What materials were used,
- Who is the supplier of the equipment,
- Who is the supplier of the materials,
- How the materials were disposed of.

Interaction:

- Organizations, participants in the treatment process,
- Organizations for the material support of the medical process,
- Organizations participating in the electronic exchange of information,
- Organizations, participants in the process of archiving and storing information.

8 Methodology of Conversion of Quantitative Indicators into Qualitative Indicators and Their Following Assessment

The result of building a mathematical model by quantitative parameters is the final functional (Formula 5). On the basis of which it is necessary to translate quantitative values into their qualitative analogs of quality gradations. The mathematical apparatus considered below allows you to convert quantitative values into precise fractional numbers, in some cases, in order to level errors and distortions associated with incomplete information, they can be rounded to the nearest integer. Since we use a relative system for assessing the quality of the services provided and statistical data from 2017 were chosen as zero, the total number of quality levels (Q) varies in the range from –10 to + 10 a total of 20. Let's find the length of the quality interval:

$$Dq = Q --1 \tag{6}$$

Using the linear dependence of the translation of the quantitative value of the attribute Xj of the final function (Formula 7) into its qualitative analog Qj:

$$Qj = (Xj - Xmin) / (Xmax + Xmin/Dq) + 1 \tag{7}$$

The qualitative parameters obtained as a result of translation are relative analogs of the quantitative data preceding them. Thus, Fig. 3 obtained as a result of the calculations should be considered quality level 3. From the point of view of the control function for monitoring and analyzing the interaction of a set of different systems, it is necessary to determine an integral qualitative assessment of their functioning across the entire set of the above-mentioned features.

Consider three options for determining this integral quality indicator:

Method 1. Determination of the reference quality (if possible), as is done for measuring physical quantities. Subsequently, the comparison of the obtained quality parameter with the reference one.

Method 2. The quality of the object at the current stage in comparison with its state at the previous stages.

Method 3. Determination of the quality level in comparison with other objects of the same class.

If objects are compared only on one basis, then it is easy to assign a rating – who is the best, that has a higher rating.

However, in the case of managing infocommunication systems of the megalopolis level, it is more difficult to determine the ratings, since they are characterized by several features of a different nature. In this case, for each feature that characterizes the object, it is proposed to establish the upper and lower limit of the quantitative values of each feature or index. One of the simplest indices is economic indicators or the number of patients served.

For example, to integrate a new entity (enterprise or organization) into the existing system for each indicator involved in assessing the "suitability" of the organization set objective upper and lower quantitative boundaries. The method proposed above is at the testing stage in the structures for the provision of medical services to cancer patients in Moscow to determine the integral quality indicator, the suitability of the structure's components for effective functioning and integration.

9 Development of a Roadmap for the Management and Development of Territorial Distributed Medical Information Systems

From the point of view of the current functioning and development of medical information systems used in the treatment of cancer patients, we distinguish the following levels:

- operational;
- knowledge level;
- tactical level;
- strategic level.

A feature of the functioning of this class of systems is that it is not a separate legally formalized enterprise or organization, but combines parts of municipal, commercial and state structures with a bidirectional exchange of information.

From the point of view of the municipality, the roadmap for maintenance and development should have the following subsystems.

At the operational level:
executive management support systems.

– Executive Support Systems (ESS).

At the strategic level:
management information systems.

– Management Information Systems (MIS).

  decision support systems.

– Decision Support Systems (DSS).

  At the tactical (managerial) level:
  knowledge management systems.

– Knowledge Work System (KWS).

  office automation systems.

– Office Automation Systems (OAS).

  At the level of knowledge:

– Transaction Processing Systems (TPS).

10 Operational Grade Systems Support Accounting and Control

For example, sales accounting, personnel accounting, accounting, material flow control. Systems at this level are data processing systems. An example of an element of a roadmap at an operational level is a recommended set of measures to improve the operation of a medical institution. However, at the current moment in time, this set of measures is not mandatory, but after 3–5 years it becomes mandatory, and subsequently it is included in the law of the subject of the federation or municipality as part of the mandatory requirements.

Another example of the operational level was the fulfillment of the UN and IAEA requirements for the decommissioning of equipment that uses Cesium-137, For example, in the United States, this requirement was supported by financial grants for organizations to replace equipment and was carried out with the participation of representatives of the New York City administration [4].

Knowledge-level systems ensure the automation of the development of new types of products, the creation and support of electronic archives, the extraction of information, new knowledge from electronic data storages (CAD, DataWarehousing, OLAP, Data Mining).

Tactical-level systems are designed to provide control, analysis, management, decision-making, and administrative actions for middle managers.

This level includes systems aimed at solving problems for which information requirements are not always clear. Answers to these questions often require new data, both external and internal, that cannot be obtained from existing operational level systems.

As an example of a roadmap element at a tactical level, registration and verification of mini X-ray machines in dental offices is mandatory since 2018. This is due to the fact that as a result of the accumulated statistics, the amount of such equipment in

medical institutions began to make up a tangible value in% of the total amount of isotope-containing materials turnover and required the administration of the region's subject to introduce these requirements step by step (within 3 years).

Strategic-level systems are a tool to help top-level leaders and prepare strategic studies and long-term forecasts, both for city structures and for various external economic processes. An example of an element of a roadmap at a strategic level is the decision to mandate the use of electronic only X-ray images by 2021.

Thus, the conditions for the formation of a roadmap for the development of a geographically distributed medical information system is the analysis of quantitative and qualitative indicators of the ecosystem of infocommunication interaction in the field of medical services using isotope-containing materials.

The impulses for the inclusion of a particular series of measures in the Roadmap can be both the requirements of the Federal and regional levels, and the analysis of statistical indicators on the turnover of isotopic materials. Analysis of practice shows that the most optimal from the point of view of effectiveness are complexes of measures with short-term (up to 1 year) or medium-term planning (3–5 years).

When technological solutions are introduced with a period of more than 5 years, their efficiency indicator drops sharply, due to the fact that every three years Intel and AMD manufacturers release new processors, which is associated with the introduction of new technologies to the market. However, in the case of the operation of mass-use systems, the use of systems and software and hardware complexes created more than 15 years is observed.

11 Conclusions

The mathematical modeling allows at the practical level to carry out multi-parameter monitoring and control in the main critical areas. Graphically, the result of the work of the mathematical model is a volumetric landscape, which makes it possible to comprehensively assess the situation both in each of the city's districts and throughout the metropolis as a whole. The use of a qualitative assessment in parallel with a quantitative one allows the managing staff of the administration of a medical institution to obtain a more complete assessment of the situation in controlling the circulation of isotope-containing materials in the provision of medical services to the population. Requirements and recommendations for building a Roadmap for the development of geographically distributed medical information systems in the field of treatment of cancer patients are formulated.

References

1. Kuzovkova, T. A., Saliutina, T. Y., Kukharenko, E. G., & Sharavova, O.I. (2020). Mechanism of interconnected management of development of networks and platforms of the internet of things on the basis of evaluation of synergetic efficiency. In Wave Electronics and its Application in Information and Telecommunication Systems, WECONF 2020, 9131158. RU.
2. Gorodnichev, M. G., Kukharenko, E. G., Salutina, T. U., Moseva, M. S., & Kukharenko, A.M. (2019). Features of the development of information systems for working with blockchain technology. *Journal of Physics: Conference Series*. In *International Scientific Conference "Conference on Applied Physics, Information Technologies and Engineering - APITECH-2019"*. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations; Polytechnical Institute of Siberian Federal University, 33039. RU.
3. Kukharenko, E. G., Korkunov, I. A., Gorodnichev, M. G., & Salutina, T. U. (2019). On the introduction of digital economics in the transport industry. In *Systems of Signals Generating and Processing in the Field of on Board Communications, SOSG 2019*, 8706797. RU.
4. Pecorella, R. F., & Stonecash, J. M. (2006). *Governing New York State* (5th ed.). SUNY Press.