Protection of Information in Telecommunication Medical Systems based on a Risk-Oriented Approach

Svitlana Shevchenko[1], Yuliia Zhdanova[1], Yurii Dreis[2], Roman Kyrychok[1], and Diana Tsyrkaniuk[1]

[1]Borys Grinchenko Kyiv University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine
[2]Polissia National University, 7 Staryi ave., Zhytomyr, 10008, Ukraine

Abstract

The changes brought by informatization to society have a qualitative effect on the process of modernization of medical care. At the same time, the digitization of big data in healthcare creates numerous risks from the point of view of ensuring the confidentiality, integrity, and availability of information. Inadequate security is due to both objective and subjective reasons. Among them: are the lack of a sufficient number of qualified specialists in the field of information protection; budget restrictions; software conflict; lack of training in information security rules and skills of medical personnel; non-compliance with traditional cyber security practices; legal and ethical issues related to patient data. Determining the minimum and maximum possible degrees of risk of security breaches in information and telecommunication medical systems is the key to ensuring the protection of medical information. This confirms the significance and timeliness of this research, which is based on a risk-oriented approach. The analysis of the scientific literature, having allowed the designation of the components, is how the information-telecommunication system and the links between them are put together. For each asset, the source of the threat, the threat itself, and the variants of reaction to it are identified. The following violations are most common: theft of the patient's medical information (confidentiality threats); modification of the patient's medical information (threats to integrity); failure of individual components of the medical system (availability threat). A graphic and quantitative approach to the assessment of information security risks and methods and means of processing these risks are proposed. This study can serve cyber security specialists for modeling information protection in medical systems and be used in the educational process of students of 125 Cyber Security specialties.

Keywords

Information risks, risk-oriented approach, risk management, information-telecommunication medical system, telemedicine, threats, vulnerabilities.

1. Introduction

Thanks to automation and programming, artificial intelligence, and machine learning, the modern medical world has received great opportunities to effectively interact with patients in making clinical decisions in both diagnosis and treatment. However, at the same time, there is an increase in cases of information security violations in such systems [1–4]. The main part of the medical information processed in the medical information system, in the process of implementing telemedicine activities, is the personal data of patients. This category of information is the most sensitive and vulnerable to information security threats. Information about the health status of patients is the most valuable information, in the processing of which some individuals are interested, and can use it for criminal purposes [5–11]. First of all, attackers choose small medical institutions, seeing that they have an insufficient level of protection for

CPITS 2023: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2023, Kyiv, Ukraine
EMAIL: s.shevchenko@kubg.edu.ua (S. Shevchenko); y.zhdanova@kubg.edu.ua (Y. Zhdanova); dreisyuri@gmail.com (Y. Dreis); r.kyrychok@kubg.edu.ua (R. Kyrychok); d.tsyrkaniuk.asp@kubg.edu.ua (D. Tsyrkaniuk)
ORCID: 0000-0002-9736-8623 (S. Shevchenko); 0000-0002-9277-4972 (Y. Zhdanova); 0000-0003-2699-1597 (Y. Dreis); 0000-0002-9919-9691 (R. Kyrychok); 0000-0002-9422-8617 (D. Tsyrkaniuk)

confidential information. Healthcare breach report for the 1st and 2nd half of 2022 [5, 6] in the analysis of information security in healthcare determines that 80.3% of violations are hacker attacks, and 14.2% are unauthorized access. Although the number of incidents did not increase, more patients became victims of breaches: in the second half of 2022, 28.5 million medical records were breached and accessed, which is 35% more than in previous years.

Inadequate security is caused by several reasons [5–18]:

- Lack of a sufficient number of qualified specialists in the field of information protection.
- Budget limitations (only 4–7% of IT-budget of a medical establishment is allocated to cyber security).
- Conflict of new software and hardware devices and security software systems.
- Non-compliance with traditional cyber security practices.
- Lack of training in information security rules and skills of medical personnel.
- Legal and ethical issues related to patient data (confidentiality is one of the factors that makes it impossible to access the patient database without their consent. It prevents the machine collection of information to create a suitable base for research [12]).

It is obvious that an organization's security policy is a complex, routine process, but the ways to overcome security controls are becoming increasingly filigree, which urges scientists and practitioners to improve and create the most sustainable countermeasures.

2. Medical Information Systems

With the birth of the Internet in the 1990s, the possibilities of using personal computers and mobile phones determined the rapid digitalization in the medical field. A large database of health-related data needs to be analyzed, stored, and processed in real-time to make effective urgent decisions, which is not possible without powerful information technology. Modern medical information systems are considered in the integration of two directions:

- Information systems are used to store and provide accessible data about services made available by healthcare organizations and other health-related organizations.
- Information systems store and provide access to population data that are important for surveillance, program evaluation, policy development, and public health priority setting [19].

Examples of Health Information Systems: Electronic Medical Records (EMR); Electronic Health Records (EHR); Practice Management Software; Master Patient Index (MPI); Patient Portals; Remote Patient Monitoring (RPM); Clinical Decision Support (CDS); Telemedicine.

There is no stable defined concept of "telemedicine". We will take as a basis the definition presented by the World Health Organization, Telemedicine—the provision of medical services at a distance using information and telecommunication technologies by all medical workers to exchange reliable information for the diagnosis, treatment, and prevention of diseases and injuries, research and assessment, as well as for the learning process of health care workers, which takes place to improve the health of individuals and communities [20]. "Tele" is a Greek word meaning distance, "mederi" is a Latin word meaning to heal.

The history of telemedicine began in 1964 at the University of Nebraska School of Medicine using a closed television system and continued to be used in psychology [21]. This is the first case of health professionals using the telephone to send and receive medical documents across long distances. The development of telemedicine in the world is presented in studies [22–25].

The analysis of literary sources shows that telemedicine has evolved through different research stages, starting from telemedicine as a simple communication environment that complements traditional services, to automation technologies and decision-making tools that expand the scope and range of medical services [24].

In Ukraine, the direction of telemedicine started in 1935 with the organization of teleelectrocardiography by the doctor and scientist Maryan Franke in the city of Lviv. However, stagnation had been observed for a long time, though point research and clinical centers were formed. In 2007, the State Clinical Scientific and Practical Center of Telemedicine of the Ministry of Health of Ukraine was established—the only specialized healthcare institution created for the implementation and development of telemedicine in Ukraine. The sectoral normative document on the use of telemedicine in Ukraine is the Order of the Ministry of Health of March 26,

2010 No. 261 "On the implementation of telemedicine in health care institutions" alongside the methodological recommendations [26].

At the legislative level, telemedicine was approved in 2015 by the Order of the Ministry of Health of October 19, 2015 No. 681 [7]. It defines telemedicine as a complex of actions, technologies, and measures used in the provision of medical care, using means of remote communication in the form of the exchange of electronic messages. In 2016, the eHealth information and telecommunication system for automating the record keeping of medical services and management of medical information and the Helsi medical service were created to provide patients with access to their medical information and the choice of medical services (medical facilities and doctors).

Analysis of the literature [11, 13, 14, 16, 17, 27–34] made it possible to distinguish six main components of the information and telecommunication medical system (Fig. 1):

1. Patient portal (sub-modules containing personal data, statements, referrals, statuses, and other medical information of the patient, and the patient can view it).
2. Laboratory-diagnostic information system (Ambulatory information system, Clinical information system, Laboratory information system, Radiological information system).
1. Pharmaceutical information system (related to processing, distribution, and monitoring of drug safety).
2. Providers of medical services (government, insurance companies, manufacturers of medical equipment, health care managers, research organizations).
3. Database (management, exchange, search, analytical reports, etc.).
4. Service personnel of the medical system (information protection specialists, programmers, cloud storage services).

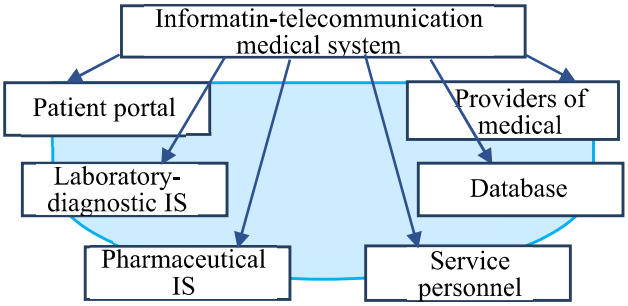


Figure 1: Components of the information and telecommunication medical system

One of the goals of the telemedicine system is to preserve medical secrecy and confidentiality, the integrity of medical information about the patient's health and statistical data, and the possibility of access to information at any time by authorized personnel. In other words, the priority task at the state level is to ensure the protection of information in telecommunication medical systems.

3. Model of Information Protection in Information and Telecommunication Medical Systems

To build a protection system in information and telecommunication medical systems, it is necessary to identify threats and vulnerabilities of system elements, analyze and process information risks with the aim of managing them.

Information security risk is a numerical (verbal) function that describes the probability of the implementation of IS threats and the amount of damage from their implementation due to the use of asset vulnerabilities by these threats in order to harm the organization [35]. In this case, material damage to the patient or reputational damage is possible. IS risk management is understood as a continuous cyclic process that includes the following stages: risk identification (collection of information on assets, sources of threats, classification of threats and vulnerabilities; ranking of risks); risk analysis (qualitative and quantitative approach to risk assessment); risk assessment (the process of comparing the quantified risk with given risk criteria to determine the significance of IS risk); risk processing and acceptance. Fig. 2 presents the IS risk management process algorithm [36].

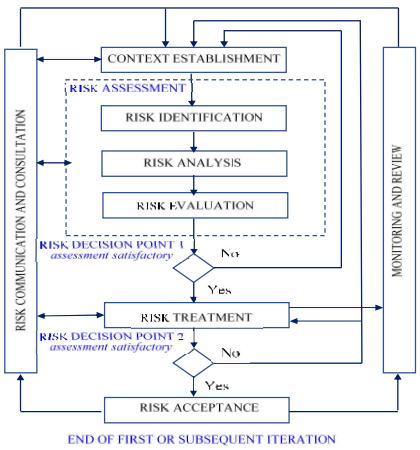


Figure 2: The IS risk management process algorithm

The effectiveness of IS risk management depends significantly on the assessment of these risks. A qualitative and quantitative approach to establishing IS risk values is distinguished. A qualitative approach can be carried out using a SWOT analysis [37], a quantitative result—a statistical method (if a sufficiently large amount of homogeneous data is given), the Monte Carlo method [38], the fuzzy set method [39], an expert method, and others. After a specific IS risk is identified and assessed, a decision must be made regarding its treatment—the selection and implementation of risk minimization measures. Information security risk management includes reducing, accepting (retaining), preventing, or transferring IS risk. This approach to creating an organization's information security system is called risk-oriented.

4. Properties of Protected Information

Information systems are used in virtually all activities inherent in the field of medical services. This is the storage, access, processing, sharing, and transfer of health information; support in case of providing medical assistance to the patient; consultation and training of medical personnel; management of the healthcare system and business processes in it. This information is not static, it changes, and its quantity grows, this information environment needs protection from the point of view of ensuring confidentiality, integrity, and availability in real-time.

Confidentiality is defined as the property of information such that it cannot be accessed by unauthorized users and/or processes. Medical Privacy: All medical records are subject to strict laws governing user access privileges. According to the law, security, and authentication systems are required for those who process and store medical records [40]. Violation of privacy is called theft or disclosure of information. The most typical ways of implementing this threat in distributed systems are listening to communication channels ("sniffing") and changing the authorized entity. Violators can also attack the end nodes of the system - file servers, database servers, as well as user workstations [15].

Information integrity is the property that cannot be modified by users and/or processes that do not have the appropriate authority to do so. The integrity of the medical documentation implies the accuracy of the complete medical record. This category covers information management, patient identification, verification of authorship, making changes and corrections to records, and checking records for documentation validity during reimbursement claims [41]. A violation of this category is called message falsification. It can be implemented as a result of equipment failures and failures, as well as due to careless or intentional actions of users, including due to the action of computer viruses and other malicious software. Purposeful falsification in medical systems is not so likely, but it can have very significant consequences (for example, possible falsification of information about a person's health, changing the prescription or dosage of drugs) [15].

Availability of information is a property that consists of the possibility of its use according to the requirements of a user who has the appropriate authority. Availability of medical documentation is the property that electronic medical information is available and suitable for use at the request of an authorized person [42]. Denial of service (DoS) is very common in distributed information systems and can be implemented through DoS attacks aimed both at end nodes in the telecommunications system and at intermediate nodes (routers). Also, a violation of the availability of information can occur due to equipment failures and malfunctions, which is especially relevant for remote access systems, as well as due to damage to communication channels [15].

A breach of information security in medical systems can cause not only material and reputational damage to the patient. But also to the deterioration of his health or even death in the case of the use of medical products of the Internet of Things. It should also be noted that the number of attacks on groups of doctors increased from 2% of the total number of violations in the first half of 2021 to 12% in the first half of 2022 [5].

5. Identification of Threats and Implementation in the Information and Telecommunication Medical System

The functioning of the information and telecommunication medical system is carried out through the following processes:

- Information.
- Telecommunication.

- Processes of implementing operations using algorithms.

Fig. 3 presents a typical diagram of the network of the information and telecommunication medical system and shows the flow of information through the various components of the system. The source of information security threats in this medical system can be changed in the external environment (natural disasters and accidents, earthquakes, floods, fires, and other random events that are unlikely), failures and failures of software and hardware equipment, the consequences of errors during the design and development of the system, as well as the actions of medical workers, service personnel, medical service as well as the actions of medical professionals, service personnel, medical service providers, patients, and external offenders [15].

The main threats to information security in this medical system include:

- Failure of software and hardware (threat of availability).
- Theft, interception, leakage of information (threat to privacy).
- Abuse of privileged access (threat to integrity and confidentiality).
- Introduction of malicious software (threat to confidentiality, integrity, availability).
- Insider activity (threat to privacy).

Identification of threats and assets affected by these threats is presented in Fig. 4.

It is especially necessary to outline the problem of big data security in information and telecommunication medical systems. The storage of the patient's personalized medical information is complicated by its large volume, especially the graphic type, and its heterogeneous structure. In the study [16], the authors propose a life cycle of big data security in health care: the data collection stage, the data transformation stage, the data modeling stage, and the knowledge creation stage. At each stage, an analysis of threats and attacks is carried out, as well as countermeasures and possible methods are proposed in the context of privacy and integrity of big data in the field of healthcare: implementation of authentication, encryption, and access control.

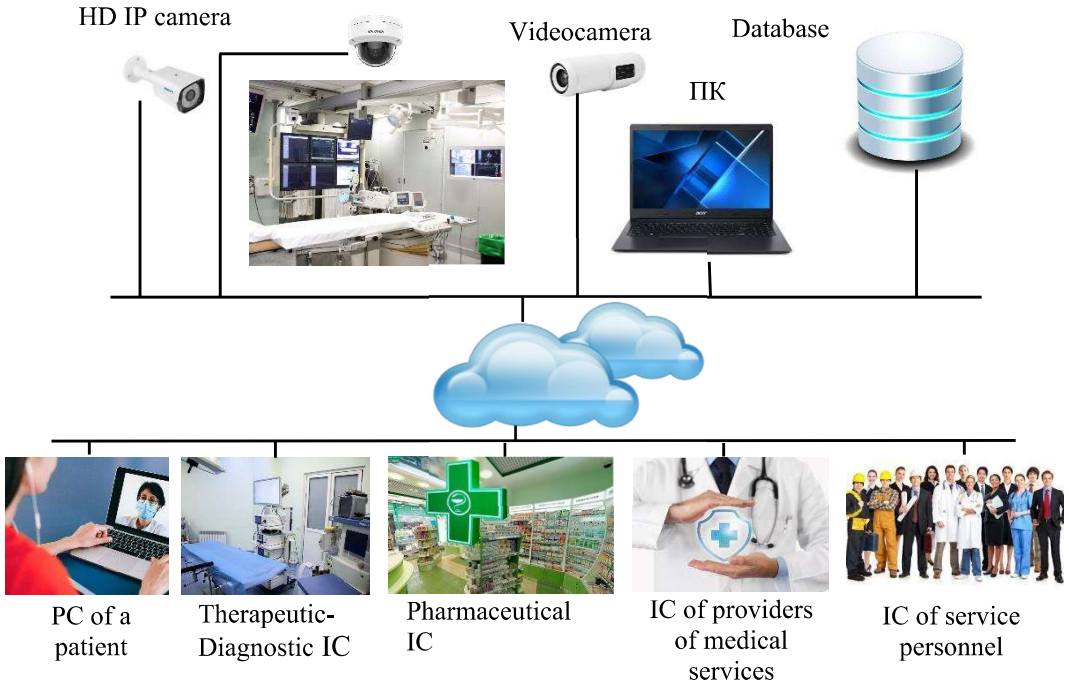


Figure 3: A typical scheme of the information and telecommunication medical system

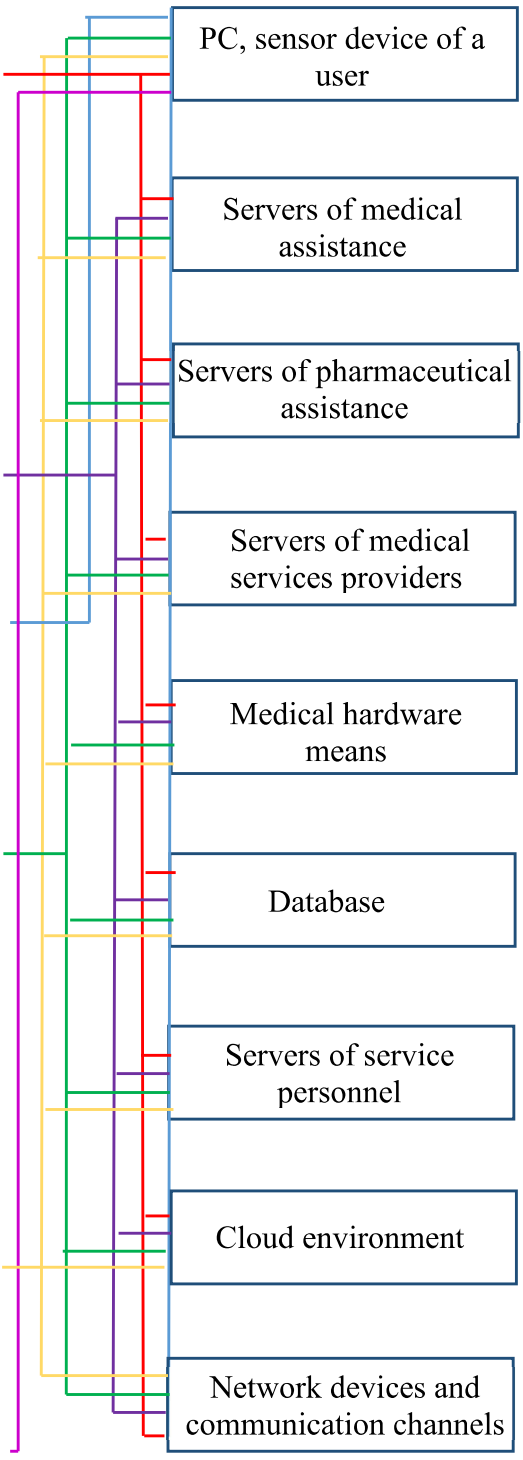
Type of identification Violation	Threat and its source	Assets subject to threats	Consequences
Violation of privacy	Leakage of information through communication channels (hacker attacks, introduction of malicious software, non-compliance with privileged access requirements)B		1) Complete or partial disability of information systems
	Provision of patient information to third parties (insider activity)		
	Theft of media		2) Material damage
Violation of integrity	Modification of medical information, software and hardware (introduction of virus software); non-compliance with privileged access requirements		
Violation of accessibility	Blocking access to medical information (introduction of malicious software); software and hardware errors		3) Moral damage (blackmail, bribery, reputational risks)
	Destruction of media		

Figure 4: Identification of threats and consequences of their implementation in the information and telecommunication medical system

6. Calculation of the Risks of the Information and Telecommunication Medical System

To assess the risks of information security in the information and telecommunication medical system, we will apply a model in the form of a graph of attacks. Attack graphs are a method that can be used to explore the interactions between vulnerabilities in an entire system. On the other hand, the attack graph is a directed graph G = G(V, E), on which a set of scenarios (paths of attacks) simulating the infliction of damage by a malicious agent on the information system to be protected is studied [43].

The following types of attack graphs are distinguished [44]:

- State enumeration graph (state enumeration graph)—in such graphs vertices correspond to triples **(s, d, a)**, where **s** is the source of the attack, d is the target of the attack, and **a** is an elementary attack (or the use of a vulnerability); arcs indicate transitions from one state to another (Fig. 5).
- Condition-oriented dependency graph—vertices correspond to the results of attacks, and arcs correspond to elementary attacks that lead to such results (Fig. 6).
- Exploit dependency graph (graph of the conditions for the implementation of exploit opportunities)— vertices correspond to the results of attacks or elementary attacks, arcs reflect dependencies between vertices—the conditions necessary for the execution of the attack and the consequence of the attack (Fig. 7).

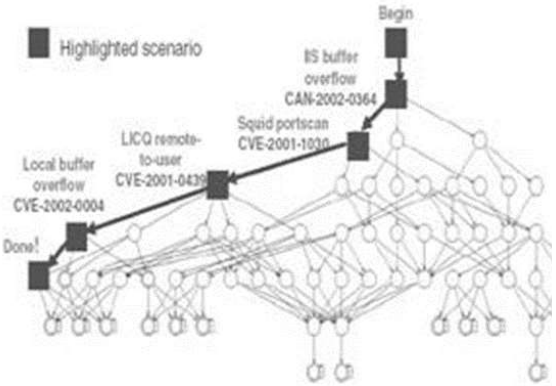


Figure 5: State enumeration graph

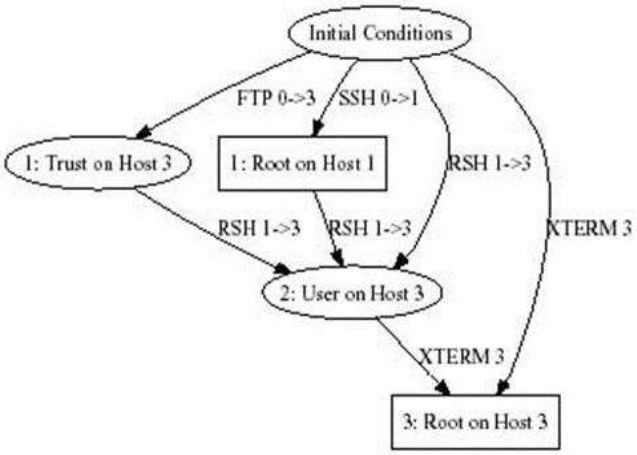


Figure 6: Condition-oriented dependency graph

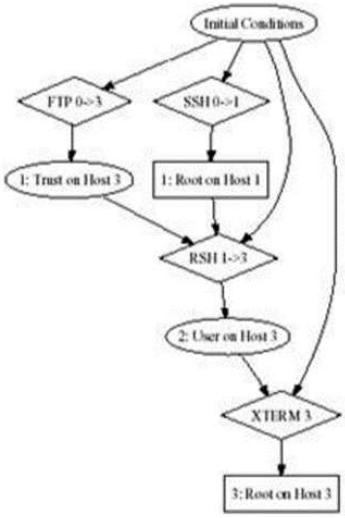


Figure 7: Exploit dependency graph

Next, we present a risk-oriented model based on the theory of graph attacks. Information and telecommunication medical systems will be presented in the form of an oriented graph $\vec{G}(V, \vec{E})$, where $V = \{v_i\}, i = \overline{1,n}$, are threats to the assets, $\vec{E}$ is the connection between them. Arc (v_i, v_j) corresponds to the connection of the threat v_i with the threat v_j, the probability of which is the result of the realization of the threat v_j.

For each threat $v_i, i = \overline{1,n}$, let us determine the following parameters:

- w_i is the frequency of the threat v_i.
- p_i is the probability of the threat being realized v_i.
- l_i is the coefficient of damage from the realization of the threat v_i.
- $r(A_i)$ is the value of the asset A_i, $A_i \subset A$, where A is the set of assets targeted by the threat v_i.

- p_{ij} is the probability of choosing the implementation path of the threat v_j, connected to the threat v_i.

Then the quantitative indicator of risk is calculated according to the formulas:

$$R_i = \sum_i w_i p_i l_i r(A_i), \quad (1)$$

$$R_{ij} = R_i + \sum_{i,j} p_{ij} R_j \quad (2)$$

For example, Fig. 8 presents a part of the information system,

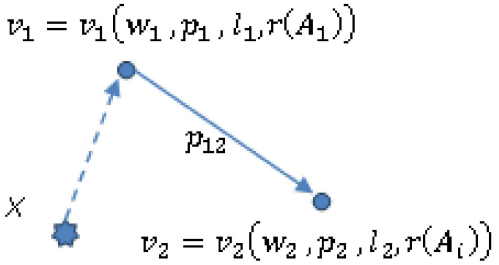


Figure 8: Sample application of the graph attack method

where X is the violator; v_1 is a threat to the PC of a patient, so $v_1 = v_1(w_1, p_1, l_1, r(A_1))$, where A_1 is personal data of a patientпер; v_2 is a threat to the databaseз, therefore $v_2 = v_2(w_2, p_2, l_2, r(A_i))$, where A_i is personal data i-number of patients.

Using the formula (1), we get the degree of risk for the PC of a patient

$$R_1 = w_1 p_1 l_1 r(A_1);$$

The degree of risk for the database

$$R_2 = w_2 p_2 l_2 \sum_i r(A_i).$$

Thus, according to formula (2), the degree of risk to the database through the patient's PC is equal to

$$R_{12} = R_1 + p_{12} R_2.$$

Statistical methods or expert evaluations are used to determine the value of assets, the probability of threat realization, and their frequency. It is also possible to prioritize threats using the CVSS system. It is an open industry standard for assessing computer system security vulnerabilities. This toolkit assesses vulnerability on a ten-point scale (low: 0.1–2.0; medium: 2.1–5.0; high: 5.1–8.0; critical: 8.1–10). As a result, a ranked list is formed, starting with the highest risk indicator;

800-30, BSI-Standard 100-3, Standard ISO/IEC 27005, and DSTU ISO/IEC 27005:2019. software methods and tools for assessing and managing information risks.

The direction of further research will be aimed at the step-by-step implementation of this model with the presentation of calculations and methods at each stage.

Ensuring the protection of information in medical systems is offered by various methods (cryptographic, hardware, software). Neglecting information security means denying all the advantages of information and telecommunication medical technologies since citizens' trust in new technologies depends on the degree of information security, their willingness to hand over an extremely important area of their lives to the "hands" of computers, communication networks, and information systems and algorithms.

7. Conclusions

In the future, they compare the risk indicators with the standard adopted in the organization. For those indicators that have exceeded the standard, the methods of risk processing (reduction, prevention, transmission, such as insurance) are used. The current stage is characterized by a sufficient number of international standards on which the information security management process in the world is based, in particular, NIST 800-30, BSI-Standard 100-3, ISO/IEC 27005, and DSTU ISO/IEC 27005: 2019. Different software techniques and tools are also used in practice to evaluate and manage information risks. The direction of further research will be aimed at the gradual implementation of this model with the presentation of calculations and methods at each stage. The provision of information protection in medical systems is offered by different methods (cryptographic, hardware, software). Neglecting information safety-means to refute all the benefits of information and telecommunication medical technologies, since the degree of information security depends on citizens' trust in new technologies, their willingness to transfer an extremely important sphere of their life in the "hands" of computers, communication networks, information systems, and algorithms.

8. References

[1] V. Zhebka, et al., Optimization of Machine Learning Method to Improve the Management Efficiency of Heterogeneous Telecommunication Network, in: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 149–155.

[2] P. Anakhov, et al., Evaluation Method of the Physical Compatibility of Equipment in a Hybrid Information Transmission Network, Journal of Theoretical and Applied Information Technology 100(22) (2022) 6635–6644.

[3] O. Kopiika, P. Skladannyi, Use of Service-Oriented Information Technology to Solve Problems of Sustainable Environmental Management. Information Technology and Mathematical Modeling for Environmental Safety 3021 (2021) 66-75.

[4] M. Kalimoldayev, et al., The Device for Multiplying Polynomials Modulo an Irreducible Polynomial, News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences 2(434) (2019) 199–205.

[5] Healthcare breach report 2022, H1. Security Research and Data Analysis URL:https://www.criticalinsight.com/

[6] 2022 H2 Healthcare Data Breach Report URL:https://cybersecurity.criticalinsight.com/healthcare-breach-report-h2-2022

[7] On the Approval of Regulatory Documents Regarding the Use of Telemedicine in the Field of Health Care. Ministry of Health of Ukraine; Order from 19.10.2015 No. 681. URL:https://zakon.rada.gov.ua/laws/show/z1400-15#top

[8] Information security strategy (Ukraine), 28.12.2021, No 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (in Ukrainian)

[9] On the Protection of Information in Communication Systems (Ukraine), 05.07.1994, No. 80/94-BP. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text

[10] G. Pawlowski, et. al., Legal Aspects of Information Security in Telemedicine in Ukraine, Path of Sci. 8 (2022) 1011–1017. doi:10.22178/pos.87-2

[11] V. Martsenyuk, N. Klymuk, I. Gvozdetska, On Problem of Telemedical Information Protection: Regulatory and Organizational Aspects From the Experience of the Republic of Poland, Med. Informs. Eng. 3 (2016) 44–55. doi:10.11603/mie.1996-1960.2016.3.6753

[12] J. Yoon, L. Drumright, M. Van der Schaar, Anonymization Through Data Synthesis Using Generative Adversarial Networks (ADS-GAN), IEEE J. of Biomedical and Health Informs. 24(8) (2020) 2378–2388. doi:10.1109/JBHI.2020.2980262

[13] O. Yudin, et. al., Protection of Critical Medical Information in GSM-type Telecommunication Networks Based on Elliptic Curves, Probls. Inf. Manag. 4(52) (2015) 125–131. doi:10.18372/2073-4751.4.10351

[14] A. Kulyk, et. al., Telemedicine. Computer Systems and Information Technologies, VNMU, Vinnytsia, 2020.

[15] M. Graivoronsky, Protection of Confidential Information in Telemedicine Systems. Legal, Regulatory and Metrological Support of the Information Protection System in Ukraine, 11 (2005) 191–195.

[16] K. Abouelmehdi, A. Beni-Hessane, M. Saadi, Security Model for Big Healthcare Data Lifecycle, Proced. Comput. Sci. 141 (2018) 294–301.

[17] Dw. Kim, J. Choi, Kh. Han, Risk Management-Based Security Evaluation Model For Telemedicine Systems, BMC Med. Inf. Decis. Mak. 20(106) (2020). Doi:10.1186/s12911-020-01145-7

[18] K. Abouelmehdi, A. Beni-Hessane, H. Khaloufi, Big Healthcare Data: Preserving Security and Privacy, J. Big Data. 5(1) (2018). doi:10.1186/s40537-017-0110-7

[19] C. Magruder, et. al., Using Information Technology to Improve the Public Health System, J. Public Health Manag. and Pract.: JPHMP. 11(2) (2005) 123–130. doi:10.1097/00124784-200503000-00005

[20] A Health Telematics Policy in Support of WHO's Health-For-All Strategy for Global Health Development: Report of the WHO Group Consultation on Health Telematics, 11–16 December, Geneva, 1997, Geneva, World Health Organization, 1998.

[21] R. Bashshur, T. Reardon, G. Shannon, Telemedicine: A New Health Care Delivery

System, Annu. Rev. Public. Health, 21 (2000) 613–637. doi: 10.1146/annurev.publhealth.21.1.613
[22] N. Brown, A Brief History of Telemedicine, Telemed. Inf. Exch. 105 (1995) 833–5.
[23] K. Kravets, Development and Application of Telemedicine in the World and in Ukraine, Dermatol. Venereol. 4 (2017) 94–98.
[24] O. Escobar, et. al., The Effect of Telemedicine on Patients' Wellbeing: A Systematic Review, J. Innov. Economs. Manag. 35 (2021) 9–31. doi:10.3917/jie.pr1.0098
[25] O. Ikumapayi, et. al., Telehealth and Telemedicine—An Overview, International Conference on Industrial Engineering and Operations Management Nsukka, Nigeria, 5–7 April, 2022, 1347–1358.
[26] Order of the Ministry of Health of March 26, 2010 № 261 "On the Introduction of Telemedicine in Health Care Institutions" URL:https://zakononline.com.ua/documents/show/70816___70816
[27] J. Tummers, et. al., Designing a Reference Architecture for Health Information Systems, BMC Med. Inf. Decis. Mak. 21(210) (2021). doi:10.1186/s12911-021-01570-2
[28] A. Appari, M. Johnson, Information Security and Privacy in Healthcare: Current State of Research1, Int. J. Internet Enterp. Manag. 6 (2010) 279–314. doi: 10.1504/IJIEM.2010.035624
[29] A. Rajput, et. al. EACMS: Emergency Access Control Management System for Personal Health Record Based on Blockchain, IEEE Access. 7 (2019) 84304–84317. doi: 10.1109/ACCESS.2019.2917976
[30] J. Biskup, G. Bleumer, Cryptographic Protection of Health Information: Cost and Benefit, Int. J. Bio-Medical Comput. 43(1–2) (1996) 61–67, doi: 10.1016/S0020-7101(96)01228-7
[31] S. Pirbhulal, et. al., A Joint Resource-Aware and Medical Data Security Framework for Wearable Healthcare Systems, Future Gener. Comput. Syst. 95 (2019) 382–391, doi: 10.1016/j.future.2019.01.008
[32] S. Hoffman, Cybersecurity Threats in Healthcare Organizations: Exposing Vulnerabilities in the Healthcare Information Infrastructure, World Libraries, 24(1) 2020.
[33] B. Murdoch, Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era, BMC Med. Ethics. 22(122) (2021). doi: 10.1186/s12910-021-00687-3
[34] J. Rodrigues, et. al., Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems, J. Med. Internet Research. 15(8):e186 (2013). doi:10.2196/jmir.2494
[35] S. Shevchenko, et. al., Conducting a SWOT-analysis of Information Risk Assessment as a Means of Formation of Practical Skills of Students Specialty 125 Cyber Security, Cybersecur. Educ. Sci. Technol. 2(10) (2020) 158–168. doi:10.28925/2663-4023.2020.10
[36] DSTU ISO/IEC 27005:2019 (ISO/IEC 27005:2018, IDT) "Information Technologies. Protection Methods. Information Security Risk Management", 2019, URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=85797
[37] H. Shevchenko, et. al., Information Security Risk Analysis SWOT, vol. 2923 (2021) 309–317.
[38] S. Shevchenko, Y. Zhdanova, K. Kravchuk, Information Protection Model Based on Information Security Risk Assessment for Small and Medium-Sized Business, Cybersecur. Educ. Sci. Technol. 2(14) (2021) 158–175. doi:110.28925/2663-4023.2021.13.158157
[39] L. Dubchak, Fuzzy Information Protection System in Telemedicine, Inf. Process. Systs. 8(133) (2015) 97–101. doi:10.13140/RG.2.1.2242.7361
[40] B. Anas, Data privacy (Information privacy) URL:https://www.techopedia.com/definition/10380/information-privacy
[41] Integrity of the Healthcare Record: Best Practices for EHR Documentation. URL:https://library.ahima.org/doc?oid=300257#.Y_p2XHZBxPY
[42] Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices, URL: https://www.coursehero.com/file/76902828/small-practice-security-guide-11-1pdf/
[43] S. Shevchenko, et. al., Mathematical Methods in Cibernetic Security: Graphs and Their Application in Information and Cybernetic Security, Cybersecur. Educ. Sci. Technol. 1(13) (2021) 133–144. doi: 10.28925/2663-4023.2021.13.133144
[44] M. Danforth, Models for Threat Assessment in Networks, Comput. Sci. (2006).