УДК: 663.1:004.056 DOI: 10.24411/2075-4094-2018-16050

# К ВОПРОСУ ВЫБОРА СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В МЕДИЦИНСКИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ПО КРИТЕРИЯМ КАЧЕСТВА

В.П. ГУЛОВ[*], В.П. КОСОЛАПОВ[*], А.В. ХВОСТОВ[**], Г.В. СЫЧ[*]

[*] *ФГБОУ ВО «Воронежский государственный медицинский университет им. Н.Н. Бурденко» Министерства здравоохранения Российской Федерации, ул. Студенческая, д.10, Воронеж, 394000, Россия*
[**] *ФГБОУ ВО «Воронежский государственный технический университет», Московский пр-т., д.14, Воронеж, 394026, Россия*

**Аннотация.** На основе анализа особенностей построения и функционирования систем защиты информации от несанкционированного доступа, используемых в медицинских информационных системах при обработке персональных данных, предложен комплексный критерий для их выбора по многим показателям качества. В основе системы показателей качества использованы отечественные и международные стандарты в области качества программных систем. Российские и международные стандарты в области качества программных систем регламентируют показатели надежности, удобства использования, ресурсоемкости и т.п. При этом, показатели качества зачастую противоречат друг другу. Для обоснованного выбора систем защиты информации разработана методика конструирования комплексного показателя, позволяющего сделать обоснованный выбор по многим показателям качества. Полученный комплексный показатель качества, построенный на основе анализа парных предпочтений показателей качества, таких как надежность, ресурсоемкость, удобство использования позволит на практике осуществить выбор систем защиты информации без применения лексикографических методов и существенно упростить процессы принятия решения должностными лицами. Комплексный показатель качества систем защиты информации мажет быть использован при обосновании выбора варианта системы, как при организации персональных данных, обрабатываемых в медицинских информационных системах, так и при защиты конфиденциальной информации другого вида.

**Ключевые слова:** информационная безопасность, показатель качества, бинарное отношение, сложная программная система.

# TO THE QUESTION OF THE CHOICE OF THE SYSTEM OF PROTECTION OF PERSONAL DATA IN MEDICAL INFORMATION SYSTEMS BY QUALITY CRITERIA

V.P. GULOV[*], V.P. KOSOLAPOV[*], A.V. KHVOSTOV[**], G.V. SYCH[*]

[*] *Federal State Budget Educational Institution of Higher Education «Voronezh State N.N. Burdenko Medical University» of the Russian Federation Ministry of Health, Studencheskaya Str., 10, Voronezh, 394000, Russia*
[**] *Federal State Budget Educational Institution of Higher Education «Voronezh State Technical University», Moscow Av., 14, Voronezh, 394026, Russia*

**Abstract.** Based on the analysis of the features of the construction and operation of information security systems against unauthorized access used in medical information systems for the processing of personal data, a comprehensive criterion for their selection is proposed for many quality indicators. The system of quality indicators is based on domestic and international standards in the field of software system quality. Russian and international standards in the field of quality of software systems are regulated by reliability, ease of use, resource consumption, etc. At the same time, the quality indicators often contradict each other. For a reasonable choice of information security systems, a methodology for constructing a complex indicator has been developed, which makes it possible to make an informed choice in many quality indicators. The obtained complex quality index, built on the basis of the analysis of the pair preferences of quality indicators, such as reliability, resource intensity, ease of use, will allow in practice to select the information security systems without using lexicographic methods and substantially simplify the decision-making processes of officials. The complex quality index of the information security systems can be used to justify the choice of a variant of the system, both in the organization of personal data processed in the in medical information systems, and in the protection of confidential information of a different kind.

**Key words:** information security, quality indicator, binary relation, complex software system.

Все большее внимание в настоящее время уделяется вопросам обеспечения безопасности *персональных данных* (ПДн). Вступивший в силу с 2007 года Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» в 2011-2013 годах был дополнен сразу несколькими подзаконными актами всех основных регуляторов в данной сфере. Гарантия защиты ПДн в учреждениях здравоохранения России также закреплена в ряде Законов [1, 2].

В условиях реализации в России ряда проектов по внедрению в поликлиниках и больницах электронных медицинских карт пациентов, предоставлению услуг «электронной регистратуры», созданию территориальных медицинских регистров и автоматизированных систем в здравоохранении – *медицинских информационных систем* (МИС) – возникает множество новых проблем, связанных с обеспечением конфиденциальности медицинской информации и сохранением врачебной тайны и ПДн при их использовании.

В нормативных документах основных регуляторов по защите ПДн определены следующие основные вопросы:

– организацию работ по защите информации, в том числе при разработке и модернизации объектов информатизации и их систем защиты информации;

– состав и основное содержание организационно-распорядительной, проектной, эксплуатационной и иной документации по защите информации;

– требования и рекомендации по защите речевой информации при ведении переговоров, в том числе с использованием технических средств;

– требования и рекомендации по защите информации при ее автоматизированной обработке и передаче с использованием технических средств;

– порядок обеспечения защиты информации при эксплуатации объектов информатизации;

– особенности защиты информации при разработке и эксплуатации *автоматизированных систем* (АС), использующих различные типы средств вычислительной техники и информационные технологии;

– порядок обеспечения защиты информации при взаимодействии абонентов с Сетями.

*Таблица 1*

**Показатели качества ПС и характеризуемые ими свойства**

| Наименование групп показателей качества | Наименование показателей качества | Характеризуемое свойство |
|---|---|---|
| Показатели надежности | Устойчивость функционирования | Характеризуют способность ПС в конкретных областях применения выполнять заданные функции в соответствии с программными документами в условиях возникновения отклонений в среде функционирования, вызванных сбоями технических средств, ошибками во входных данных, ошибками обслуживания и другими дестабилизирующими воздействиями |
| | Работоспособность | |
| Показатели сопровождения | Структурность | Характеризуют технологические аспекты, обеспечивающие простоту устранения ошибок в программе и программных документах и поддержания ПС в актуальном состоянии |
| | Простота конструкции | |
| | Наглядность | |
| | Повторяемость | |
| Показатели удобства применения | Легкость освоения | Характеризуют свойства ПС, способствующие быстрому освоению, применению и эксплуатации ПС с минимальными трудозатратами с учетом характера решаемых задач и требований к квалификации обслуживающего персонала |
| | Доступность эксплуатационных программных документов | |
| | Удобство эксплуатации и обслуживания | |
| Показатели эффективности | Уровень автоматизации | Характеризуют степень удовлетворения потребности пользователя в обработке данных с учетом экономических, вычислительных и людских ресурсов |
| | Временная эффективность | |
| | Ресурсоемкость | |
| Показатели корректности | Полнота реализации | Характеризуют степень соответствия ПС требованиям, установленным в техническом задании, требованиям к обработке данных и общесистемным требованиям |
| | Согласованность | |
| | Логическая корректность | |
| | Проверенность | |

Однако выбор *систем защиты информации* (СЗИ для защиты ПДн в МИС связан с необходимостью проведения анализа их качества. Руководители различного уровня в здравоохранении, независимо от профиля организации, кроме знаний основных положений, требований и рекомендаций по защите ПДн, основ организации работ по защите конфиденциальной информации, основных обязанности учреждений здравоохранения, эксплуатирующих МИС, существующих угрозах и методах (способах) решения задачи обеспечения *безопасности информации* (БИ) должны иметь четкий и легко используемый критерий, позволяющий оценить качество различных вариантов СЗИ.

При выборе вариантов *программных систем* (ПС) в России (операционных систем, систем управления базами данных, средств разработки и др.) заказчики и разработчики руководствуются стандартами [3, 4]. В стандартах определены термины и определения в области качества ПС, основные группы характеристик качества ПС, системные показатели качества, характеризуемые ими свойства. Структура показателей качества, содержащихся в этих стандартах, представлена в табл. 1.

Зарубежный опыт по созданию качественного программного обеспечения был обобщен, и на его основе сформировалась система управления качеством. Основные положения системы управления качеством легли в основу стандартов *ISO* серии 9000 [5]. Основным здесь является утвержденный в 1991 г. международный стандарт *ISO* 9126:1991 – «Информационная технология. Оценка программного продукта. Характеристики качества и руководство по их применению». При выборе минимума стандартизируемых показателей качества ПС стандарты учитывает следующие принципы:

– ясность и измеряемость значений;

– отсутствие перекрытия между используемыми показателями;

– соответствие установившимся понятиям и терминологии;

– возможность последующего уточнения и детализации;

– выделены характеристики, которые позволяют оценивать программные системы с позиции пользователя, разработчика и управляющего проектом.

Стандартом *ISO* 9126 рекомендуется 6 основных характеристик качества ПС, каждая из которых детализируется следующими субхарактеристиками:

– функциональная пригодность детализируется пригодностью для применения, точностью, защищенностью, способностью к взаимодействию и согласованностью со стандартами и правилами проектирования;

– надежность рекомендуется характеризовать уровнем завершенности (отсутствием ошибок), устойчивостью к ошибкам и перезапускаемостью;

– применимость предлагается описывать понятностью, обучаемостью и простотой использования;

– эффективность рекомендуется характеризовать ресурсной и временной экономичностью;

– сопровождаемость – удобством для анализа, изменяемостью, стабильностью и тестируемостью;

– переносимость предлагается отражать адаптируемостью, структурированностью, замещаемостью и внедряемостью.

Использование СЗИ для защиты ПДн в МИС связано с необходимостью выбора варианта СЗИ лучшего одновременно по всем пяти группам показателей качества программных систем. С учетом противоречивости различных показателей качества (показатели качества, характеризующие удобство использования СЗИ противоречат группе показателей качества, характеризующей надежность, группа показателей, характеризующая показатели сопровождения требует принятия компромиссного решения с группой показателей качества, характеризующей эффективность и т.п.) необходимо конструирование комплексного показателя качества, являющегося сверткой отдельных показателей СЗИ [6].

Методика свертки отдельных показателей качества сложных технических систем подробно разработана в [7-10]. Свертка базируется на графе, отражающем бинарные отношения предпочтения между частными показателями качества СЗИ, используемыми при выборе. Граф предпочтений показателей качества СЗИ для дальнейшего конструирования комплексного показателя качества можно формализовать матрицей связности. При этом, собственный вектор матрицы предпочтений, соответствующий максимальному собственному числу матрицы предпочтений позволяет полностью характеризовать важность каждого частного показателя качества в системе показателей качества.

Содержательный анализ показателей качества, представленных в табл. 1 и на основе сравнительного анализа конструктивного и потребительского качества СЗИ [11] можно построить граф, отражающий бинарные отношения предпочтения в виде показанном на рис. 1.

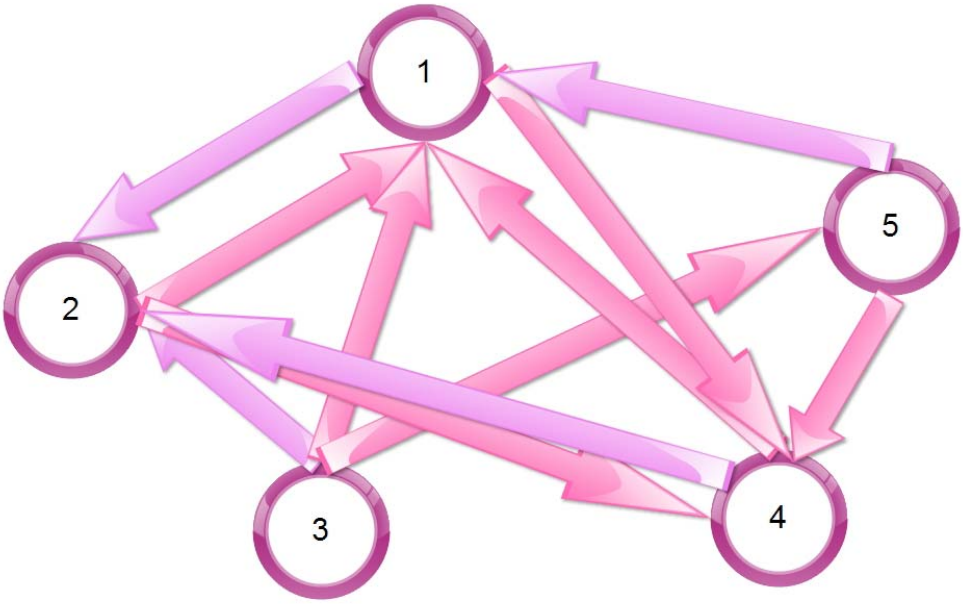


*Рис. 1*. Граф предпочтений показателей качества СЗИ при защите ПДн в МИС.

На рисунке показаны следующие обозначения:

1. сопровождаемость;
2. удобство применения;
3. надежность;
4. эффективность;
5. корректность.

Граф предпочтений, показанный на рис. 1 формализуется матрицей связности вершин графа (матрицей предпочтений критериев качества), имеющей следующий вид:

$$\begin{vmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{vmatrix}$$

Собственные числа матрицы определяются характеристическим уравнением вида:

$$\begin{vmatrix} 0-\lambda & 1 & 0 & 1 & 0 \\ 1 & 0-\lambda & 0 & 1 & 0 \\ 1 & 1 & 0-\lambda & 0 & 1 \\ 1 & 1 & 0 & 0-\lambda & 0 \\ 1 & 0 & 0 & 1 & 0-\lambda \end{vmatrix} =$$

$$= -\lambda^5 + 3\lambda^3 + 2\lambda^2 = (-1)(\lambda)(\lambda)(\lambda+1)(\lambda+1)(\lambda-2)$$

Решение алгебраического выражения дает следующие собственные числа матрицы предпочтений показателей качества СЗИ:

$$\lambda_1 = 0$$
$$\lambda_2 = 0$$
$$\lambda_3 = -1$$
$$\lambda_4 = -1$$
$$\lambda_5 = 2$$

Для наибольшего собственного числа матрицы предпочтений показателей качества СЗИ $\lambda_5 = 2$ можно записать систему однородных линейных уравнений для определения собственного вектора матрицы:

$$A - \lambda * E = \begin{vmatrix} -2 & 1 & 0 & 1 & 0 \\ 1 & -2 & 0 & 1 & 0 \\ 1 & 1 & -2 & 0 & 1 \\ 1 & 1 & 0 & -2 & 0 \\ 1 & 0 & 0 & 1 & -2 \end{vmatrix} = 0$$

Решение системы однородных линейных уравнений для определения собственного вектора матрицы предпочтений показателей качества СЗИ решается методом Гаусса.

Результирующая система однородных линейных уравнений после эквивалентных преобразований (1) в соответствии с методом Гаусса имеет следующий вид:

$$\begin{aligned} x_1 - x_5 &= 0 \\ x_2 - x_5 &= 0 \\ x_3 - \frac{2}{3}x_5 &= 0 \\ x_4 - x_5 &= 0 \end{aligned} \qquad (2)$$

Из уравнения 4 системы (2) найдем переменную $x_4$:

$$x_4 = x_5$$

Из уравнения 3 системы (2) найдем переменную $x_3$:

$$x_3 = \frac{3}{2}x_5$$

Из уравнения 2 системы (2) найдем переменную $x_2$:

$$x_2 = x_5$$

Из уравнения 1 системы (2) найдем переменную $x_1$:

$$x_1 = x_5$$

Собственный вектор матрицы предпочтений показателей качества СЗИ, таким образом, будет иметь следующий вид:

$$X = \begin{vmatrix} x_5 \\ x_5 \\ \frac{3}{2}x_5 \\ x_5 \\ x_5 \end{vmatrix}$$

При $x_5 = 1$, собственный вектор матрицы предпочтений показателей качества СЗИ, соответствующий максимальному собственному числу, будет иметь вид:

$$\Psi = \begin{vmatrix} 1 \\ 1 \\ \frac{3}{2} \\ 1 \\ 1 \end{vmatrix}$$

Проведя процедуру нормализации показателей качества СЗИ в соответствии с правилом [7-10]:

$$f_j^*(x) = f_j(x) / \max_{x \in X} f_j(x)$$

можно получить нормализованный вектор матрицы предпочтений показателей качества СЗИ следующего вида:

$$\Psi^* = \begin{vmatrix} 0{,}6 \\ 0{,}6 \\ 1 \\ 0{,}6 \\ 0{,}6 \end{vmatrix}$$

Свертку показателей качества СЗИ можно представить в виде:

$$F = \sum_{i-1\ldots6} \psi_i^* * x_i = x_3 + \sum_{i-1\ldots6, i \neq 3} 0{,}6 * x_i$$

где $\psi_i^*$ — значения коэффициентов значимости частных критериев качества СЗИ в комплексном показателе качества.

Таким образом, сконструированный в статье комплексный показатель качества СЗИ решает практическую проблему их выбора при решении задачи обеспечения безопасности информации в МИС при обработке ПДн и другой конфиденциальной информации. Основой комплексного показателя качества СЗИ является граф отражающий частные предпочтения отдельных показателей качества программных систем, регламентированных Российскими и международными стандартами.

**Литература**

1. ГОСТ 28195 – 89. Оценка качества программных средств. Общие положения. М: Госстандарт СССР, 1990. 15 с.

2. ГОСТ 28806 – 90. Качество программных средств. Термины и определения. М: Госстандарт СССР, 1991. 18 с.

3. ГОСТ РИСО/МЭК 9126 – 93. Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению. М.: Госстандарт России, 1993. 10 с.

4. Ломазов В.А., Прокушев Я.Е. Решение задачи экономичного многокритериального выбора на основе метода анализа иерархий // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2010. №7-1(78).

5. Лубенцова Е.В., Лубенцов В.Ф. Многокритериальный выбор алгоритмов систем управления // Наука. Инновации. Технологии. 2014. №1.

6. Юдин Д.Б. Математические методы управления в условиях неполной информации: задачи и методы стохастического программирования. М.: Советское радио, 1974. 400 с.

7. Ларичев О.И., Браун Р.В. Количественный и вербальный анализ решений: сравнительное исследование возможностей и ограничений // Экономика и математические методы. 1998. Т. 34, № 4. С. 97–107.

8. Ногин В.Д. Принятие решений в многокритериальной среде: количественный подход. М.: Физматлит, 2002. 144 с.

9. Макаров О.Ю., Рогозин Е.А., Хвостов В.А. Система показателей для оценки качества программных систем защиты информации // Информация и безопасность. 2004. Вып. 1. С. 107–110.

10. Гулов В.П., Хвостов В.А., Попов А.С. Метод нормирования требований к информационной безопасности основных элементов медицинской информационной системы при заданном общем уровне безопасности // Вестник новых медицинских технологий. 2015. Т. 22, №2. С. 7–11.

11. Гулов В.П., Хвостов В.А., Чесноков П.Е. Детальный алгоритм множества реализаций угроз информационной безопасности в медицинской информационной системе // Вестник новых медицинских технологий. Электронное издание. 2015. №2. Публикация 1-4. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf (дата обращения: 30.06.2015). DOI: 10.12737/11910.

12. Федеральный закон от 27 июля 2006 г. №152 ФЗ «О персональных данных» // Российская газета от 29 июня 2006. №165.

13. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Парламентская газета от 3 августа 2006. №126-127.

**References**

1. GOST 28195-89. Ocenka kachestva programmnyh sredstv. Obshchie polozheniya [Evaluation of the quality of software. Generalities]. Moscow: Gosstandart of the USSR; 1990. Russian.

2. GOST 28806-90. Kachestvo programmnyh sredstv. Terminy i opredeleniya. [The quality of the software. Terms and definitions]. Moscow: Gosstandart of the USSR; 1991. Russian.

3. GOST RISO/IEC 9126-93. Informacionnaya tekhnologiya. Ocenka programmnoj produkcii. Harakteristiki kachestva i rukovodstva po ih primeneniyu [Information technology. Evaluation of software products. Quality characteristics and guidelines for their application]. Moscow: Gosstandart Of Russia; 1993. Russian.

4. Lomazov VA. Reshenie zadachi ehkonomichnogo mnogokriterial'nogo vybora na osnove metoda analiza ierarhij [Economical Solution to the problem of multicriteria choice based on the method of analysis of hierarchies]. Bulletin of Belgorod state University. Series: Economics. Informatics. 2010;7-1(78). Russian.

5. Lubentsova EV. Mnogokriterial'nyj vybor algoritmov sistem upravleniya [Multi-Criteria choice of algorithms of control systems]. Nauka. Innovations. Technologies. 2014;1. Russian.

6. Yudin DB. Matematicheskie metody upravleniya v usloviyah nepolnoj informacii: zadachi i metody stohasticheskogo programmirovaniya [Mathematical methods of control in conditions of incomplete information: problems and methods of stochastic programming]. Moscow: Soviet radio; 1974. Russian.

7. Larichev OI. Kolichestvennyj i verbal'nyj analiz reshenij: sravnitel'noe is-sledovanie vozmozhnostej i ogranichenij [Quantitative and verbal decision analysis: a comparative study of opportunities and constraints]. Economics and mathematical methods. 1998;34(4):97-107. Russian.

8. Nogin VD. Prinyatie reshenij v mnogokriterial'noj srede: kolichestvennyj podhod [Decision Making in multicriteria environment: a quantitative approach]. Moscow: Fizmatlit; 2002. Russian.

9. Makarov OYu. Sistema pokazatelej dlya ocenki kachestva pro-grammnyh sistem zashchity informacii [A system of indicators to assess the quality of software information security systems]. Information and security. 2004;1:107-10. Russian.

10. Gulov VP. Metod normirovaniya trebovanij k informacionnoj bezopasnosti osnovnyh ehlementov medicinskoj informacionnoj sistemy pri zadannom obshchem urovne bezopasnosti [Method of normalizing the information security requirements of the basic elements of the medical information system at a given General level of security]. Bulletin of new medical technologies. 2015;22(2):7-11. Russian.

11. Gulov V.P. Detal'nyj algoritm mnozhestva realizacij ugroz informacionnoj bezopasnosti v medicinskoj informacionnoj sisteme [The Detailed algorithm many implementations of information security in the medical information system]. Bulletin of new medical technologies. Electronic edition. 2015[cited 2015 Jun30];2 [about 7 p.]. Russian. Available from: http://www.medtsu.tula.ru/VNMT/Bulletin/E2015-2/5191.pdf. DOI: 10.12737/ 11910.

12. Federal'nyj zakon ot 27 iyulya 2006 g. №152 FZ «O personal'nyh dannyh» // Rossijskaya gazeta [Federal law of July 27, 2006 №152 FZ «On personal data»]. Rossiyskaya Gazeta ot June 29, 2006;165. Russian.

13. Federal'nyj zakon ot 27 iyulya 2006 g. N 149-FZ «Ob informacii, informacionnyh tekhnologiyah i o zashchite informacii» [The Federal law of July 27, 2006 N 149-FZ «About information, information technologies and about information protection»]. Parliamentary newspaper of August 3, 2006;126-127. Russian.

**Библиографическая ссылка:**
Гулов В.П., Косолапов В.П., Хвостов А.В., Сыч Г.В. К вопросу выбора системы защиты персональных данных в медицинских информационных системах по критериям качества // Вестник новых медицинских технологий. Электронное издание. 2018. №3. Публикация 2-7. URL: http://www.medtsu.tula.ru/VNMT/Bulletin/E2018-3/2-7.pdf (дата обращения: 14.06.2018). DOI: 10.24411/2075-4094-2018-16050.*
* номера страниц смотреть после выхода полной версии журнала: URL: http://medtsu.tula.ru/VNMT/Bulletin/E2018-3/e2018-3.pdf