УДК 004.056.5
DOI: 10.26102/2310-6018/2024.44.1.030

# Метрики семантической близости запроса пользователя как критерий безопасности в тематической иерархической модели управления доступом

**В.А. Хвостов[1]✉, Г.В. Сыч[2], О.Н. Чопоров[2,3], В.П. Гулов[2]**

*[1]Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация*
*[2]Воронежский государственный медицинский университет имени Н.Н. Бурденко, Воронеж, Российская Федерация*
*[3]Воронежский государственный технический университет, Воронеж, Российская Федерация*

***Резюме.*** Расширение сферы применения мобильных технологий и устройств как элементов распределенных систем для повышения эффективности и удобства доступа к различным информационным системам и цифровым сервисам привело к необходимости совершенствования методов и механизмов защиты информации и информационной безопасности. Одним из основных механизмов защиты является управление доступом. Проведен анализ особенностей использования традиционных (дискреционных и мандатных) моделей управления доступом в распределенных информационных системах (ИС) при использовании мобильных систем (МС) в качестве элементов. В качестве наиболее эффективной модели, отвечающей требуемой политике безопасности, предложена тематическая иерархическая. Для данной модели управления доступом предложен онтологический метод формирования доверительных прав на доступ к объектам, основанный на использовании метрик семантической близости. При использовании традиционных тематически иерархических моделей управления доступа логическая информационная архитектура ресурсов ИС формирует собой тематический иерархический классификатор (рубрикатор). Диаграмма Хассе вводит отношения порядка в тематическом классификаторе на решетке безопасности для формирования доверительно-тематических полномочий пользователей ИС. Построение диаграмм Хассе на решетке безопасности, включающей несколько уровней безопасности, достаточно сложная алгоритмическая задача. При построении доверительно-тематических полномочий пользователей для избегания неопределенности при неполноте построенной диаграммы Хассе и завышения предоставленных полномочий при формировании прав доступа предлагается использовать семантическую близость запроса на доступ пользователя и тематической рубрики иерархического классификатора. Анализ существующих подходов к формированию метрик семантической близости показал, что в качестве наилучшей метрики для задания доверительных полномочий пользователя может использоваться меры близости, основанные на иерархии понятий.

***Ключевые слова:*** мобильная система, управление доступом, иерархическая тематическая классификация, семантическая близость, семантическое расстояние.

***Для цитирования:*** Хвостов В.А., Сыч Г.В., Чопоров О.Н., Гулов В.П. Метрики семантической близости запроса пользователя как критерий безопасности в тематически иерархической модели управления доступом. *Моделирование, оптимизация и информационные технологии.* 2024;12(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1382 DOI: 10.26102/2310-6018/2024.44.1.030

# Metrics of semantic proximity of a user's request as a security criterion in a thematic hierarchical access control model

**V.A. Khvostov[1]✉, G.V. Sych[2], O.N. Choporov[2,3], V.P. Gulov[2]**

*[1]Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation*
*[2]Voronezh State Medical University n.a. N.N. Burdenko, Voronezh, the Russian Federation*
*[3]Voronezh State Technical University, Voronezh, the Russian Federation*

***Abstract.*** The increasing scope of application of mobile technologies and devices as elements of distributed systems to enhance the efficiency and convenience of access to various information systems and digital services has made it necessary to improve methods and mechanisms for information protection and information security. One of the main security mechanisms is access control. Features of traditional (discretionary and mandatory) access control model application in distributed information systems (IS) when using mobile systems (MS) as elements are analyzed. Thematically, hierarchical model is proposed as the most effective model that meets the required security policy. For this access control model, an ontological method for forming trust rights to access objects is proposed based on the use of semantic proximity metrics. When using traditional thematic hierarchical access control models, the logical information architecture of IS resources forms a thematic hierarchical classifier (categorizer). The Hasse diagram introduces order relations in the thematic classifier on the security grid to form trust-thematic powers of IS users. Constructing Hasse diagrams on a security grid that includes several security levels is a rather complex algorithmic task. When constructing trust-thematic powers of users in order to avoid uncertainty due to the incompleteness of the constructed Hasse diagram and overestimation of the granted powers when forming access rights, it is proposed to use the semantic proximity of the user access request and the thematic heading of the hierarchical classifier. An analysis of existing approaches to the formation of semantic proximity metrics has shown that proximity measures based on the hierarchy of concepts can be used as the best metric for setting the user's trust authority.

***Keywords:*** mobile station, access control, hierarchical thematic classification, semantic proximity, semantic distance.

***For citation:*** Khvostov V.A., Sych G.V., Choporov O.N., Gulov V.P. Metrics of semantic proximity of a user's request as a security criterion in a thematically hierarchical access control model. *Modeling, Optimization and Information Technology*. 2024;12(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1382 DOI: 10.26102/2310-6018/2024.44.1.030 (In Russ.).

## Введение

В последние годы все больше расширяется сфера применения мобильных технологий и устройств как элементов распределенных систем для повышения эффективности и удобства доступа к различным информационным системам и цифровым сервисам. Как средства доступа к ИС мобильные технологии сделали актуальными новые угрозы безопасности информации (БИ). Появились угрозы БИ, обусловленные уязвимостями аппаратной составляющей МС, уязвимостями ее операционной системы, уязвимостями мобильных приложений, уязвимостями сервисов мобильного доступа ИС, уязвимостями беспроводных технологий, обеспечивающих доступ в интернет МС и других компонентов мобильных технологий [1, 2].

При организации защиты информации (ЗИ) от угроз БИ, направленных на уязвимости сервисов мобильного доступа ИС, применяются средства идентификации и управление доступом. Также этот класс средств защиты известен как Identity Access Management (IAM) [3]. Средства защиты IAM используются для интеграции услуг, таких как аутентификация и авторизация, в мобильное решение для формирования единого профиля безопасности для каждого пользователя. Управление доступом обеспечивает

согласованное применение политики безопасности для всех мобильных сервисов и позволяет интегрировать системы аутентификации и авторизации ИС с мобильной станцией.

Функция защиты управления доступом реализуется в процессе функционирования пользователей в системе и обеспечивает конфиденциальность данных от нарушителей, имеющих доступ к системе в соответствии с установленными правилами распределения доступа. Реализация управления доступом осуществляется специальным программным компонентом системы защиты – монитором безопасности. Монитор безопасности реализует функции управления доступом в соответствии с известными моделями управления доступом.

Возможности применения существующих моделей управления доступа в ИС с использованием МС, таких как модель Харрисона, Руззо и Ульмана [4], модель Белла-ЛаПадулы (мандатного доступа), модель Лендвера-МакЛина (ролевого управления доступом) [5], были проанализированы в [6]. Как показал анализ, предпочтительной моделью управления доступом в ИС с использованием мобильных технологий является тематическо-иерархический.

Использование тематическо-иерархического управления доступом обусловлено сложившейся практикой при разграничении доступа к документам. Тематическая стратификация информационных ресурсов осуществляется по организационно-технологическим процессам и профилям деятельности. В существующих моделях тематическо-иерархического управления доступом [7], формирование доверительно-тематических полномочий пользователей представляет собой достаточно сложную математическую задачу.

Пользователь, как правило, не в полной мере владеет терминологией используемого иерархического классификатора, что приводит к тому, что запросы к информационному ресурсу не в полной мере удовлетворяют информационные потребности пользователя. Для устранения этой проблемы требуется разработка метрик семантической близости запроса и рубрики классификатора. При этом, перспективным является использование теории нечетких множеств онтологического подхода.

В связи с этим, целью настоящей работы является разработка метрик семантической близости запроса пользователя и тематической рубрики иерархического классификатора для формирования доверительных прав доступа пользователей к информационному ресурсу на основе онтологического подхода.

## Основные положения модели тематико-иерархического разграничения доступа

Модель тематико-иерархического разграничения доступа (Multilevel thematic-hierarchical access control (MLTHS)) можно представить в следующем виде [7]. Информационная система формирует собой тематический иерархический классификатор (рубрикатор), включающий конечное множество тематических рубрик $T_u = \{t_1, t_2, \ldots t_M\}$, отражающий логическую информационную архитектуру всех информационных ресурсов.

При построении доверительных прав доступа пользователей должен быть установлен частичный порядок на сформированном классификаторе, определяемый как корневое дерево.

Тематическая классификация на основе отображения множества мультирубрик $T^M$ на множестве субъектов и объектов ИС ($S \cup O$) определяется на корневом дереве иерархического рубрикатора. Назначим функцию тематического окрашивания $f_M$. В составе мультирубрицированного отображения субъектов и объектов ИС на иерархический рубрикатор $F_{u2}[x]$ функция тематического окрашивания определяет для

любого субъекта и объекта доступа ИС в каждый момент времени соответствующую ей мультирубрику: $f_M[x] = t^M$, где $x \in S \cup O$, $t_i^M \in T^M$.

Работа тематическо-иерархического управления доступом состоит из переходов состояний в момент времени $t_k$ в состояния в момент времени $t_{k+1}$.

Переходы в модели тематическо-иерархического управления доступом приводят к новым отношениям доступа (новым потокам) между существующими сущностями ИС $X = S \cup O$, либо создают (удаляют) новые субъекты и объекты доступа.

При управлении доступом реализуется принятие решения о правомочности доступа $S$ к $O$, обеспечивающего транзитивность потоков при реализации требуемого подмножества безопасных по определенному критерию потоков.

Принцип формирования иерархического классификатора представлен на Рисунке 1.

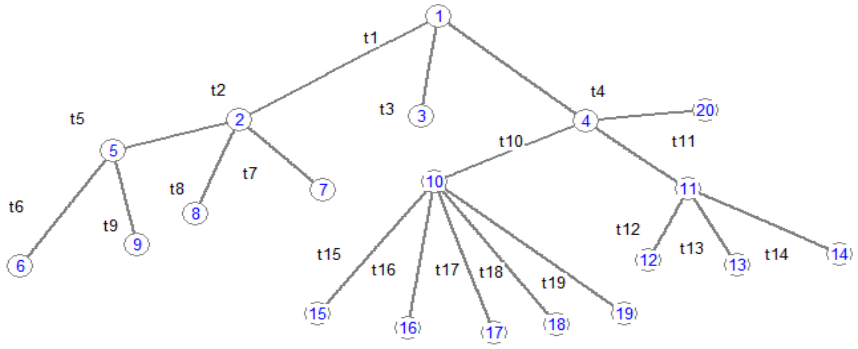


Рисунок 1 – Пример корневого графа, формализующего иерархический тематический классификатор информационных объектов ИС

Figure 1 – Example of a root graph formalizing a hierarchical thematic classifier of IS information objects

Как показал анализ использования моделей тематическо-иерархического управления доступом, формирование доверительно-тематических полномочий пользователей $F_{\text{LTH}}(s) = \{L_S, T_S^M\}$ реализуется в соответствии с установленными политиками безопасности с использованием диаграммы Хассе, вводящей отношения порядка в тематический классификатор на решетке безопасности в соответствии с методами, изложенными в [7], и представляет собой достаточно сложную математическую задачу.

## Анализ возможности применения мер семантического расстояния для задания доверительно-тематических полномочий

Вместо сложной задачи построения диаграммы Хассе, вводящего отношения порядка для корневого графа, формализующего иерархический тематический классификатор информационных объектов ИС, предлагается формирование доверительных прав доступа пользователей на основе метрик семантической близости запроса пользователя и тематической рубрики иерархического классификатора информационного ресурса ИС.

Запрос пользователя к информационному ресурсу ИС не в полной мере отражает его информационные потребности. Пользователь не в полной мере владеет терминологией иерархического классификатора ИС. С другой стороны, не всегда пользователь в состоянии сформулировать, что он ищет. Использование семантической близости запроса и рубрики классификатора позволит при предоставлении доступа дать

достаточные права, ранжированные в зависимости от потребностей пользователя. При этом монитор безопасности будет рассматривать $S$ субъекта доступа как нечеткое множество, получающее доступ к запрашиваемому объекту $O$ и семантически близкими объектами $\{O_1, O_2, ...O_n\}$ не ниже определенного порога безопасности $L$.

При построении доверительных прав доступа в мониторе безопасности подразумевается сходство запроса и тематической рубрики иерархического классификатора информационного ресурса ИС, а не их семантическая связность (компьютер – программа). Семантическая близость запроса и рубрики иерархического классификатора может содержать множество аспектов близости (расстояния). В этой связи проблема выработки критерия и назначения порога безопасности достаточно сложна, и в каждой отдельной ИС требует индивидуального решения.

Онтологический подход формирования мер семантической близости запроса и рубрики иерархического классификатора позволит формировать доверительные права на доступ не просто на основе простых слов (sicut verbum), а на основе их смыслового значения (index verborum). В этом случае содержание запроса определяется смыслом слов, который определен онтологией.

Под онтологией, в соответствии с [8-12], понимается кортеж вида:

$$< L =: L^c \cup L^P \cup L^A \cup L^{VA}, C, P, A, F, G, H^c, J, H^p, I >,$$

где $L$ – лексикон; $L^c$ – множество терминов понятий; $L^P$ – отношений между понятиями; $L^A$ – атрибутов понятий; $L^{VA}$ – значений атрибутов; $C$ – множество понятий; $P: C \times C$ – множество отношений между понятиями; $A: C \times L^{VA}$ – множество атрибутов понятий; $F: L^C \to C$ – функция связи лексикона с понятиями; $G: L^P \to P$ – функция связи лексикона с отношениями; $H^C: C \times C$ – таксономическая иерархия классов; $H^P: P \times P$ – иерархия отношений; $I$ – множество экземпляров (экземпляр – понятие единичного объема).

В качестве семантической близости онтологических термов $x$ и $y$ будем использовать функцию $S(x, y) \in [1,0]$.

Подробный обзор и классификация существующих мер семантической близости онтологических термов (понятий, отношений и экземпляров) и онтологий представлен в [13]. Выделены следующие категории мер семантической близости онтологических термов: меры, основанные на иерархических структурах; меры, основанные на неиерархических отношениях; гибридные меры; меры, учитывающие значения атрибутов.

Иерархический тематический классификатор информационных объектов ИС (пример на Рисунке 1) обусловил выбор в качестве меры семантической близости запроса пользователя и рубрики иерархического классификатора при формировании прав доверительного доступа меры, основанные на иерархических структурах.

Близость двух понятий в мерах, основанных на иерархических структурах, определяется положением вершин, соответствующих этим понятиям в иерархических онтологических структурах. Простейшая мера близости в случае формирования доверительных прав доступа в ИС может быть определена как длина кратчайшего пути, измеряемого числом вершин (ребер) между таксономиями запроса и тематической рубрики иерархического классификатора информационного ресурса ИС.

Мера семантической близости с учетом глубины таксономической иерархии в наиболее простом виде определяется в следующем виде [13, 14]:

$$S(c_1, c_2) = \log \frac{2N}{d(c_1, c_2)}, \quad (1)$$

где $c_1, c_2$ – таксономии запроса пользователя и тематической рубрики иерархического классификатора информационного ресурса ИС; $N$ – глубина дерева тематического классификатора информационного ресурса ИС; $d(c_1, c_2)$ – длина кратчайшего пути между вершинами.

При использовании онтологических метрик семантической близости, правила формирования прав на доступ к иерархическим информационным ресурсам ИС будут по аналогии с моделями управления доступом MLTHS иметь следующий вид.

Пользователи ИС, формируя запрос к системе, посредством сервисов мобильного доступа инициализируют свои первичные рубрики, которым монитор безопасности присваивает метки безопасности и назначает действия по аудиту.

Правилом (основным критерием) безопасности в MLTHS системе с онтологическим принципом назначения доверительных прав доступа является отсутствие информационных потоков от тематической рубрики наиболее точно соответствующих семантически запросу пользователя к тематическим рубрикам, имеющим меньшее некоторого априори заданного значения семантической близости. Под семантической близостью понимается мера, определяемая по формуле (1). Для информационных потоков тематической рубрики, наиболее точно соответствующих семантически запросу пользователя к тематическим рубрикам, имеющим большее значение семантической близости, разрешен полный доступ.

Для монитора безопасности, реализующего MLTHS с онтологическим принципом назначения доверительных прав доступа целесообразно определить следующие правила, определяемые основным критерием безопасности.

Правило 1. Доступ субъекта $S$ к объекту $O$, вызывающий поток по чтению (r), разрешается монитором безопасности в случае, когда метка семантической близости запроса пользователя ИС меньше установленного значения:

$$S(c_1, c_2) < S_{kr}(c_1, c_2). \quad (2)$$

Переходы системы из одного состояния $E_k$ в другое состояние $E_{k+1}$, требующие создания новых объектов, разрешаются монитором безопасности, когда метка семантической близости запроса пользователя ИС меньше установленного значения, при этом монитор безопасности присваивает новому объекту $O^*$ мультирубрику, с значением меры семантической близости меньше возможного значения для установления прав на доступ по записи и чтению.

Инициализация нового субъекта доступа $S^*$ допускается монитором безопасности свободно с присвоением ему допустимого значения семантической близости.

## Назначение меры семантической близости для запроса пользователя ИС при использовании мобильных систем

В качестве примера задания меры семантической близости для запроса пользователя с применением онтологического принципа управления доступом используем тематический классификатор иерархической структуры ИС, представленный на Рисунке 1.

Дерево тематического классификатора, представленное на Рисунке 1, имеет глубину, равную 4. Зададим ограничение права доступа пользователю соседними

вершинами ( $d(c_1,c_2)=2$ ). К примеру, запрос пользователя к рубрике $t_{12}$ должен одновременно обеспечить доступ к рубрикам $t_{13}$, $t_{14}$, $t_{11}$, $t_4$.

Расчет по формуле (1) показывает, что для этого требуется назначить пользователю пороговое значение меры семантической близости $S_{kr}(c_1,c_2)=0{,}6$.

Таким образом, пользователь ИС с использованием МС при получении доступа получает априорную пороговую меру семантической близости 0,6.

## Заключение

Требование обеспечения безопасности конфиденциальной информации при применении мобильных технологий в качестве элементов ИС потребовало реализации технических мероприятий по их защите. Основной технической мерой ЗИ является управление доступом. Существующие моделей управления доступом (дискреционная, мандатная, ролевая) имеют ряд проблем при их реализации. Для реализации управления доступом в ИС предложен онтологический метод, являющийся модернизацией тематико-иерархического. Основным направлением совершенствования тематически-иерархического метода является замена алгоритмически сложных процедур построения диаграмм Хассе достаточно простой процедурой назначения мер семантической близости запроса пользователя и рубрики иерархического классификатора информационного ресурса ИС. Мерой семантической близости целесообразно использовать длину кратчайшего пути, измеряемого числом вершин (ребер) между таксономиями запроса и тематической рубрики иерархического классификатора информационного ресурса ИС с учетом глубины таксономической иерархии дерева.

## СПИСОК ИСТОЧНИКОВ

1. Аристов М.С., Шишин О. И., Рапетов А. М., Крымов А. С., Егоров А. Д. Обзор и краткий анализ текущего состояния мобильной связи на примере сетей GSM. *Спецтехника и связь*. 2014;1:2–6.
2. Рапетов А.М., Шишин О.И., Аристов М.С., Холявин В.Б., Савчук А.В., Жорин Ф.В. Методы получения доступа к данным, хранимым на мобильном устройстве и обрабатываемым им. *Спецтехника и связь*. 2014;1:7–12.
3. Баркалов Ю.М., Нестеров А.Д. Особенности обеспечения информационной безопасности в мобильных устройствах под управлением операционной системы Android. *Вестник Дагестанского государственного технического университета. Технические науки*. 2019;46(2):71–80. DOI: 10.21822/2073-6185-2019-46-2-71-80.
4. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in Operating Systems. *Communications of the ACM*. 1976;19(8):461–471.
5. Landwehr C.E. Formal models for computer security. *ACM Computing Surveys*. 1981;13(3):247–278.
6. Гулов В.П., Косолапов В.П., Сыч Г.В., Хвостов В.А. Организация управления доступом к медицинским информационным системам с использованием методов семантической близости. *Системный анализ и управление в биомедицинских системах*. 2021;20(2):79–87. DOI: 10.36622/VSTU.2021.20.2.010.
7. Skiena S. *Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica.* Reading, MA: Addison-Wesley; 1990. 362 с.
8. Guarino N. Formal Ontology and Information Systems. *Proceedings of FOIS'98*. Trento, Italy; 1998. p. 3–15.
9. Palagin O.V., Petrenko M.G. Architectural and ontological principles of building intellectual information systems. *Mathematical machines and systems*. 2006;4:15–20.

10. Resnik P. Using information content to evaluate semantic similarity in ontology. *Proc. of the 14th Int'l Joint Conference on Artificial Intelligence*, 1995. p. 448–453.
11. Palagin O.V., Petrenko M.G. A model of the categorical level of the linguistic and ontological picture of the world. *Mathematical machines and systems*. 2006;3:91–104.
12. Крюков К.В., Панкова Л.А., Пронина В.А., Суховеров В.С., Шипилина Л.Б. Меры семантической близости в онтологии. *Проблемы управления*. 2010;5:1–14.
13. Rada R., et al. Development and Application of a Metric on Semantic Net. *IEEE Trans. on Systems, Man and Cybernetics*. 1989;19(1):17–30.
14. Leacock C., Chodorow M. Combining local context and WordNet similarity for word sense identification. *WordNet: An electronic lexical database*. Cambridge, MA: MIT press, 1998. p. 265–283.

## REFERENCES

1. Aristov M.S., Shishin O.I., Rapetov A.M., Krymov A.S., Egorov A.D. Review and brief analysis of the current state of mobile communications using the example of GSM networks. *Spectekhnika i svyaz'*. 2014;1:2–6. (In Russ.).
2. Rapetov A.M., Shishin O.I., Aristov M.S., Kholyavin V.B., Savchuk A.V., Zhorin F.V. Methods for gaining access to data stored on a mobile device and processed by it. *Spectekhnika i svyaz'*. 2014;1:7–12. (In Russ.).
3. Barkalov Yu.M., Nesterov A.D. Peculiarities of information security in mobile devices running the Android operating system. Herald of Daghestan State Technical University. Technical Sciences. 2019;46(2):71–80. DOI: 10.21822/2073-6185-2019-46-2-71-80. (In Russ.).
4. Harrison M.A., Ruzzo W.L., Ullman J.D. Protection in Operating Systems. *Communications of the ACM*. 1976;19(8):461–471.
5. Landwehr C.E. Formal models for computer security. *ACM Computing Surveys*. 1981;13(3):247–278.
6. Gulov V.P., Kosolapov V.P., Sych G.V., Khvostov V.A. Management organization access to medical information systems using the methods semantic proximity. *System analysis and management in biomedical systems*. 2021;20(2):79–87. DOI 10.36622/VSTU.2021.20.2.010. (In Russ.).
7. Skiena S. *Implementing Discrete Mathematics: Combinatorics and Graph Theory with Mathematica*. Reading, MA: Addison-Wesley, 1990. 362 p.
8. Guarino N. Formal Ontology and Information Systems. *Proceedings of FOIS'98*. Trento, Italy; 1998. p. 3–15.
9. Palagin O.V., Petrenko M.G. Architectural and ontological principles of building intellectual information systems. *Mathematical machines and systems*. 2006;4:15–20.
10. Resnik P. Using information content to evaluate semantic similarity in ontology. *Proc. of the 14th Int'l Joint Conference on Artificial Intelligence*, 1995. p. 448–453.
11. Palagin O.V., Petrenko M.G. A model of the categorical level of the linguistic and ontological picture of the world. *Mathematical machines and systems*. 2006;3:91–104.
12. Kryukov K.V., Pankova L.A., Pronina V.A., Sukhoverov V.S., Shipilina L.B. Measures of semantic proximity in ontology. *Management problems*. 2010;5:1–14.
13. Rada R., et al. Development and Application of a Metric on Semantic Net. *IEEE Trans. on Systems, Man and Cybernetics*. 1989;19(1):17–30.
14. Leacock C., Chodorow M. Combining local context and WordNet similarity for word sense identification. *WordNet: An electronic lexical database*. Cambridge, MA: MIT press, 1998. p. 265–283.

## ИНФОРМАЦИЯОБАВТОРАХ / INFORMATION ABOUT THE AUTHORS

**Хвостов Виктор Анатольевич,** кандидат технических наук, доцент кафедры Информационной безопасности, Воронежский государственный университет инженерных технологий, Воронеж, Российская Федерация.
*e-mail*: hvahva1@mail.ru
ORCID: 0000-0002-9324-5415

**Victor A. Khvostov**, Candidate of Engineering Sciences, Associate Professor at the Department of Information Security, Voronezh State University of Engineering Technologies, Voronezh, the Russian Federation.

**Сыч Галина Владимировна,** кандидат медицинских наук, доцент, доцент кафедры управления в здравоохранении Воронежский государственный медицинский университет имени Н.Н. Бурденко, Воронеж, Российская Федерация.
*e-mail*: sichgala@gmail.com

**Galina V. Sych**, Candidate of Medical Sciences, Associate Professor at the Department Management in Healthcare Voronezh State Medical University named after N.N. Burdenko, Voronezh, the Russian Federation.

**Чопоров Олег Николаевич**, доктор технических наук, профессор, проректор по цифровой трансформации, Воронежский государственный университет им. Н.Н. Бурденко Минздрава России, Воронеж, Российская Федерация.
*e-mail*: choporov_oleg@mail.ru
ORCID: 0000-0002-3176-499X

**Oleg N. Choporov**, Doctor of Engineering Sciences, Professor, Vice-Principal for Digital Transformation, Voronezh State Medical University named after N.N. Burdenko, Voronezh, the Russian Federation.

**Гулов Владимир Павлович,** доктор биологических наук, профессор, профессор кафедры управления в здравоохранении, Воронежский государственный медицинский университет имени Н.Н. Бурденко, Воронеж, Российская Федерация.
*e-mail*: voldemar1908@mail.ru

**Vladimir P. Gulov**, Doctor of Biological Sciences, Professor, Professor of the Department management in healthcare, Voronezh State Medical University named after N.N. Burdenko, Voronezh, the Russian Federation.

*Статья поступила в редакцию 23.05.2023; одобрена после рецензирования 21.03.2024; принята к публикации 28.03.2024.*

*The article was submitted 23.05.2023; approved after reviewing 21.03.2024; accepted for publication 28.03.2024.*