УДК 614.2
EDN: XPDVDG
https://doi.org/10.15275/ssmj490

Обзор

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ЦИФРОВЫХ ОТНОШЕНИЙ В ЗДРАВООХРАНЕНИИ (ОБЗОР)

З. Э. Кудашева
ФГБОУ ВО «Саратовский ГМУ им. В. И. Разумовского», Саратов, Россия

INFORMATION AND PSYCHOLOGICAL SAFETY OF DIGITAL RELATIONS IN HEALTHCARE (REVIEW)

Z. E. Kudasheva
Saratov State Medical University, Saratov, Russia

Для цитирования: *Кудашева З. Э.* Информационно-психологическая безопасность цифровых отношений в здравоохранении (обзор). Саратовский научно-медицинский журнал. 2024; 20 (4): 490–499. EDN: XPDVDG. https://doi.org/10.15275/ssmj490.

Аннотация. *Цель:* определить специфику информационно-психологической безопасности цифровых отношений в здравоохранении как институционального параметра развития цифрового контура медицины. *Методика написания обзора*. Методом исследования послужил теоретический анализ научной литературы, позволивший проследить интеграцию проблематики информационно-психологической безопасности коммуникационных процессов в осмысление институциональных изменений в сфере здравоохранения. Отбор литературных источников для анализа проведен в современных электронных библиографических базах PubMed, Google Scholar, e-Library, Web of Science, CyberLeninka. Изучено 96 источников, из них в обзор вошло 38 работ, опубликованных в период с 1989 по 2024 г. *Заключение*. Важным этапом в изучении цифровых отношений в здравоохранении стало понимание информационно-психологической безопасности как необходимого условия их институционализации. Концептуальное представление о видах и функциях информационно-психологической безопасности определяет возможности ее проецирования на уровень агентов цифровых отношений. Ключевой характеристикой информационно-психологической безопасности выступает коммуникативная компетентность врачебных кадров и ее формирование как стратегическая задача современной высшей медицинской школы.

Ключевые слова: цифровые технологии, информационно-психологическая безопасность пациента, цифровые коммуникативные компетенции врачей, цифровая компетентность

For citation: *Kudasheva ZE.* Information and psychological safety of digital relations in healthcare (Review). Saratov Journal of Medical Scientific Research. 2024; 20 (4): 490–499. (In Russ.) EDN: XPDVDG. https://doi.org/10.15275/ssmj490.

Abstract. *Objective:* to determine the specifics of information and psychological security of digital relations in healthcare as an institutional parameter for the development of the digital loop in healthcare. *Methodology for writing a review*. The research method was a theoretical analysis of the scientific literature, which made it possible to detect the integration of the problems of information and psychological security in communication processes into the understanding of institutional changes in the field of healthcare. A literary review and analysis of information conducted in modern electronic bibliographic databases PubMed, Google Scholar, e-Library, Web of Science, and CyberLeninka. A total of 96 sources were studied, of which 38 works published between 1989 and 2024 were included in the review. *Conclusion.* An important stage in the study of digital relations in healthcare was the understanding of information and psychological security as a necessary condition for their institutionalization. A conceptual idea of the types and functions of information and psychological security determines the possibilities of its projection to the level of agents of digital relations. The key characteristic of information and psychological security is the communicative competence of medical personnel and its formation as a strategic task of a modern higher medical school.

Keywords: digital technologies, information and psychological safety of the patient, digital communicative competencies of doctors, digital competence

Введение. В отечественной медицине происходит цифровизация работы медицинских учреждений по программе «Единый цифровой контур». Цифровизация создала технические условия для институциональных изменений, связанных с конструированием цифровых отношений в здравоохранении. Последние включают: отношения медицинской организации/врача и пациента; использование электронной системы хранения медицинских карт и историй болезни; медицинское страхование; цифровой режим обращения к аптечной информации и др. Оценка масштабов и качества цифровых отношений в здравоохранении осуществляется через внедрение в повседневную профессиональную практику онлайн-предоставления медицинской информации. По мнению некоторых авторов, развитие профессиональных консультативных сетей может снять «трудности посещения врача» и даже способно гармонизировать отношения между врачом и пациентом [1]. Институционализация консультативных сетей как ключевого сегмента цифровых отношений в здравоохранении активирует проблему информационно-психологической безопасности субъектов данного взаимодействия.

Несмотря на существенные различия национальных систем здравоохранения, угрозы «нарушения границ» информационно-психологической безопасности пациентов имеют общие предпосылки и могут быть преодолены едиными способами [2]. В связи с этим стала еще более очевидной важность дискуссии относительно обеспечения безопасности пациентов. В настоящее время на международном уровне Всемирной организацией здравоохранения (ВОЗ) введен Всемирный день безопасности пациентов, который отмечают 17 сентября ежегодно.

Динамика результатов обсуждения безопасности в общественном пространстве представлена в табл. 1.

Ответственный автор — Зульфия Эиповна Кудашева
Corresponding author — Zulfia E. Kudasheva
E-mail: zulfam05@mail.ru

Таблица 1

Хронология мировой повестки безопасности

Этап	Название мероприятия/документа	Временные параметры, год	Ядерные проблемы	Целевые субъекты
I	55-я сессия Всемирной ассамблеи здравоохранения (далее ВАЗ)	2002	Безопасность пациентов (создание проекта резолюции по этому вопросу)	Делегации 191 страны, представители специализированных агентств и учреждений Организации Объединенных Наций
II	57-я сессия ВАЗ.	2004	Создан Всемирный альянс за безопасность пациентов (Россия вступила в альянс в 2006 г.)	192 страны — члены ВОЗ
III	58-я сессия ВАЗ	2005	Приняты две резолюции: «Безопасность пациентов и качество медицинской помощи» и «Безопасная медицинская помощь для профилактики передачи HBV, HCV и других возбудителей, передающихся с кровью»	194 страны — члены ВОЗ
IV	«Глобальная проблема безопасности пациентов на 2005–2006 гг.» («Чистое лечение — безопасное лечение»)	2005–2006	Основная идея обеспечения стерильности при уходе за больными	194 страны — члены ВОЗ
V	3-я глобальная встреча по проблеме безопасности пациентов в ВОЗ	2017	Безопасность пациентов как ключевой принцип системы здравоохранения	194 страны — члены ВОЗ
VI	3-й глобальный министерский саммит (Токийская декларация)	2018	Формирование стратегии «Глобальных действий» в области безопасности пациентов медицинских организаций	450 участников из 42 стран.
VII	4-я Глобальная встреча по проблеме безопасности пациентов в ВОЗ	2019	Оценка влияния информатизации на безопасность пациентов	194 страны — члены ВОЗ
VIII	72-я сессия ВАЗ	2019	Разработка плана действий по безопасности пациентов	194 страны — члены ВОЗ
IX	74-я сессия ВАЗ	2021	Принят глобальный план действий по обеспечению безопасности пациентов	194 страны — члены ВОЗ
X	76-я сессия ВАЗ: «Вовлечение пациентов в целях обеспечения их безопасности»	2023	Разработка Хартии прав пациентов на безопасность	194 страны — члены ВОЗ

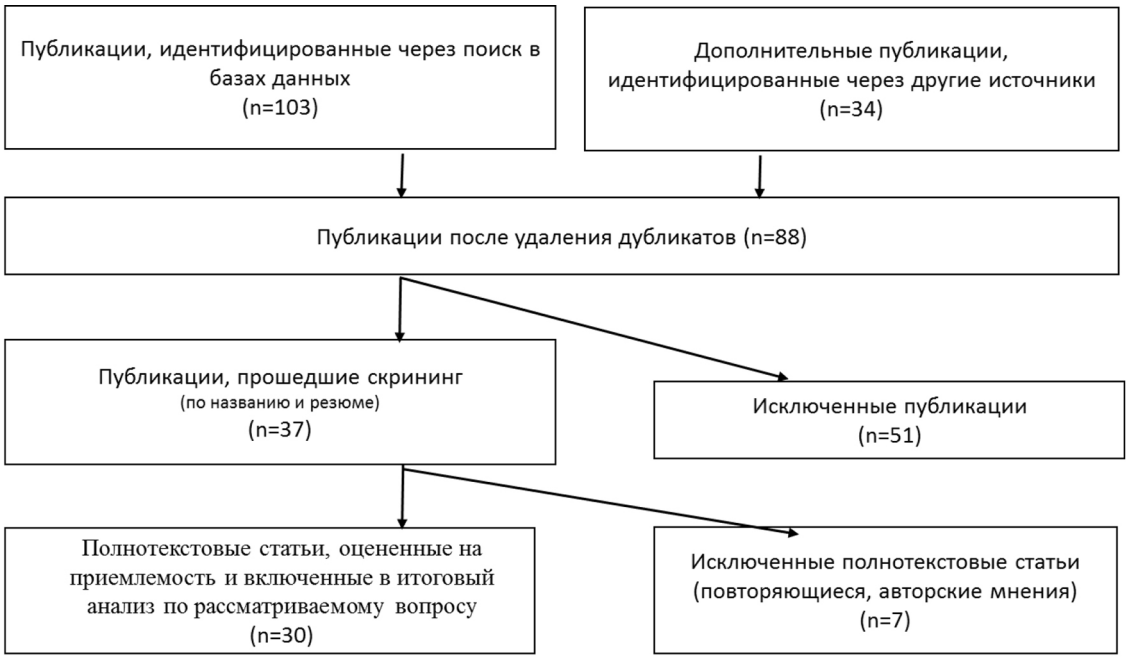
Таким образом, очевидна последовательная работа на глобальном уровне, в которой охватываются различные вопросы. Прослеживается смещение акцентов, постепенное осознание важности не только непосредственной работы врача с пациентом, но и опосредованной — ввиду информатизации и цифровизации нашего общества.

Проблема регламентации коммуникативного поведения агентов взаимодействия в информационном пространстве цифрового здравоохранения обусловлена нормами и принципами информационно-психологической безопасности. А. Н. Лунев, Н. Б. Пугачева, Л. З. Стуколова выделили такие принципы, как принцип центрации, легитимизации, имплицитности, амплификации [3]. Они определяют контур формирования цифровых коммуникативных компетенций обучающихся высшей медицинской школы, несоблюдение которых наносит непоправимый вред лечебно-профилактическому процессу, в связи с чем трудно переоценить значимость задачи, стоящей перед высшей медицинской школой в сфере формирования профессиональных коммуникативных компетенций, позволяющих минимизировать риски оказании консультативной помощи в рамках цифровой медицины.

Цель — определить специфику информационно-психологической безопасности цифровых отношений в здравоохранении как институционального параметра развития цифрового контура медицины.

Методика написания обзора. Систематический обзор выполнен по методологии PRISMA (The Preferred Reporting Items for Systematic reviews and Meta-Analyses) (рисунок). Методом исследования послужил теоретический анализ научной литературы, позволивший проследить интеграцию проблематики информационно-психологической безопасности коммуникационных процессов в осмысление институциональных изменений в сфере здравоохранения. Цифровые технологии формируют новую реальность медицинской практики, модифицируя способы коммуникации как внутри профессионального сообщества, так и вне его. При этом в качестве институционального параметра рассматривается информационно-психологическая безопасность как «защищающая» границы медицинской практики и личные границы пациента.

В силу того, что тема информационной безопасности не так давно начала разрабатываться в науке, требуется закрепление определенных понятий на законодательном уровне из-за интенсификации



Методология отбора литературных источников

развития цифровизации общества и возникновения угроз информационной безопасности как общества в целом, так и личности. Именно поэтому в список литературных источников были включены ссылки на словари ввиду наличия определения понятий «безопасность», «информационная безопасность» и ссылки на нормативно-правовую базу, отражающие сущность информационной безопасности общества и человека.

Таким образом, данная тема находит отражение в изученных нормативно-правовых документа (в том числе и в Конституции РФ), вследствие чего мы находим возможным сравнение юридических и научных источников, обнаруживая понятийное сходство термина «информационная безопасность». Исходя из этого в дальнейшем было выведено определение понятия «информационно-психологическая безопасность».

Критерии приемлемости. В научной статье проведен обзор и анализ современных и актуальных исследовательских данных по теме обеспечения информационно-психологической безопасности пациента в цифровом коммуникативном пространстве медицины.

Критерии включения. Преимущественно в нашем исследовании использовались научные работы за последние 10 лет, в которых изучался вопрос информационно-психологической безопасности пациента в цифровом коммуникативном пространстве.

Источники информации. Литературный обзор и анализ данных проведен с помощью электронных библиографических систем, таких как Google Scholar, PubMed, Web of Science, e-Library, Cyberleninca.

Поиск. Применялись следующие ключевые слова из русскоязычных источников: «цифровизация здравоохранения», «информационно-психологическая безопасность пациента», «информационная безопасность пациента», «конфиденциальность», «врачебная тайна», «цифровые коммуникативные компетенции врачей», «цифровая компетентность врача»; для англоязычных источников: «information and psychological safety of the patient», «confidentiality in medicine», «medical secrecy», «digitalization of medicine», «information technology in medicine», «digital communication competencies of doctors». Анализ проводили без использования специализированных программных средств. Отбор научных работ осуществлен в зависимости от их научной ценности. Особое внимание уделено статьям, опубликованным в рецензируемых научных изданиях.

Проанализировано 96 научных источников по теме информационно-психологической безопасности пациентов. Коммуникацию с авторами исследования не проводили. В работе применялось 38 научных источников, опубликованных в период с 1989 по 2024 г.

Результаты обзора. Рассмотрим цифровые отношения в здравоохранении, дадим определение данного понятия, определим действующие лица данных отношений.

В настоящее время в здравоохранении за счет активной цифровизации и перехода к цифровой медицине появляется понятие «цифровые отношения», и взаимодействие в рамках медицинского обслуживания осуществляется по сложной сети, включающей в себя не только людей, но также и нечеловеческие субъекты (цифровые медицинские карты, базы данных, информационные системы больниц, электронные медицинские карты, онлайн-сообщества пациентов, приложения, связанные со здоровьем, и т. д.) [4].

Цифровые взаимоотношения в здравоохранении формируют новую реальность медицинской практики, модифицируя способы коммуникации как внутри профессионального сообщества, так и вне его. Соответственно между субъектами цифрового здравоохранения формируются совершенно новая система взаимодействия: субъектами выступают виртуальные «личности», осуществляющие взаимодействие с идентификацией личности в виртуальном пространстве; также будут реализовываться права человека в виртуальном пространстве. Соответственно, основным условием вступления в цифровые отношения будет являться обеспечение безопасности всех субъектов данного взаимодействия, в частности, особое внимание необходимо уделить

информационно-психологической безопасности пациентов [5].

Если пациенты не будут уверены, что их данные будут безопасными, прозрачными и доступными для них, то это может привести к нарушению доверия к конкретному медицинскому работнику и системе здравоохранения в целом.

Исходя из сказанного следует выделить: первостепенное значение для пациентов в рамках цифровых отношений приобретает необходимость сохранения конфиденциальности и прозрачности данных с их полного разрешения [6].

Рассмотрим задачи цифровых отношений и технологическую среду, в которой реализуются данные отношения (понятие цифрового контура, то, как он создан, и средства, которыми он пользуется).

Потребность в изучении цифровых отношений в здравоохранении появляется в связи с переходом к цифровой медицине. В России нормативными основаниями перехода к цифровой медицине послужили следующие документы:

Федеральный закон №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации №152-ФЗ от 27.07.2006 «О персональных данных»;

Постановление Правительства РФ от 09.02.2022 № 140 (ред. от 04.03.2024) «О единой государственной информационной системе в сфере здравоохранения» (вместе с «Положением о единой государственной информационной системе в сфере здравоохранения»);

приказ Минздрава России №1159н от 31.12.2013 «Об утверждении Порядка ведения персонифицированного учета при осуществлении медицинской деятельности лиц, участвующих в оказании медицинских услуг»;

приказ Минздрава России №965н от 30.11.2017 «Об утверждении порядка организации и оказания медицинской помощи с применением телемедицинских технологий»;

приказ Минздрава России №341н от 14.06.2018 «Об утверждении Порядка обезличивания сведений о лицах, которым оказывается медицинская помощь, а также о лицах, в отношении которых проводятся медицинские экспертизы, медицинские осмотры и медицинские освидетельствования»;

Указ Президента РФ от 06.06.2019 №254 «О стратегии развития здравоохранения в Российской Федерации на период до 2025 года»;

Распоряжение Правительства РФ от 29.12.2021 №3980-р «Об утверждении стратегического направления в области цифровой трансформации здравоохранения» [7].

В настоящий момент активно развивающийся в России проект «Единый цифровой контур» направлен на повышение эффективности функционирования российской системы здравоохранения за счет активной ее цифровизации.

Внедрение цифрового контура в систему здравоохранения создает условия для институциональных изменений, которые связаны с проектированием цифровых отношений в медицине. Это, в свою очередь, привело к актуализации проблемы информационно-психологической безопасности субъектов данного взаимодействия.

Таким образом, для эффективной реализации проекта «Единый цифровой контур» необходимо обеспечение информационной безопасности граждан Российской Федерации. Для предоставления информационно-психологической безопасности потребителям медицинских услуг необходимо следующее: ведéние перечня информационных ресурсов и сведений об уровне их конфиденциальности, ведéние единого каталога пользователей, обезличивание персональных данных.

Рассмотрим информационно-психологическую безопасность личности пациентов через содержательное наполнение, структуру, ее нормативно-правовое измерение.

В Кэмбриджском словаре (Cambridge Dictionary) «безопасность» (safety) определяется, как состояние или место, в котором вы не подвергаетесь опасности или риску. В словаре Чэмберса (The Chambers dictionary) «безопасность» описывается как «состояние, чувство или средства пребывания в безопасности». В данном определении акцент делается на эмоциональной составляющей и средствах, которые обеспечивают эту безопасность. В этом определении также отсутствие «*тревожности и озабоченности*» рассматривается как условие «*стабильности*» и «*уверенности*» [8]. В Оксфордском словаре (Oxford English Dictionary) [9] безопасность рассматривается как состояние, которое обладает более приоритетным и более высоким уровнем значимости для личности, чем уверенность. В словаре современного американского языка Гарнера (Garner's Modern American Usage) понятие безопасности трактуется в «освободительном» ключе — в ключе «*преодоления*» [10]. Безопасность представляется как свобода от опасности и риска, от озабоченности и сомнений. В большом французском словаре «Ларусс» (Grand Larousse encyclopédique) также имеется указание на безопасность как состояние «*уверенности*» и «*отсутствие беспокойства*» [11]. В свою очередь, немецкая культурная традиция описывает безопасность как «*надежность и уверенность*».

В отечественной традиции понятие «безопасность» включает три компонента: отсутствие опасности, угрозы, а также безвредность. В «Толковом словаре русского языка» (С.И. Ожегова, Н.Ю. Шведовой) понятие «безопасность» определяется как «состояние, при котором не угрожает опасность и есть *защита от опасности*». В «Толковом словаре живого великорусского языка» (В.И. Даля) безопасность описывается как «состояние *сохранности и надежности*».

Проведенный нами анализ позволяет констатировать, что в разных культурах представления о безопасности являются схожими. Таким образом, безопасность может трактоваться как *чувство защищенности от различного рода рисков и опасности* [12]. Далее изучим то, как можно интерпретировать понятие «информационная безопасность».

В 1980 г. впервые появляется термин «безопасность информации», или «информационная безопасность», «безопасность IT». Одним из базовых условий формирования информационной безопасности является защита информации от несанкционированного доступа, а также искажения или от утраты данных.

Под информационной безопасностью Российской Федерации понимается «состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства» [13, 14].

В Указе Президента РФ №646 от 05.12.2016 «Об утверждении Доктрины информационной

безопасности Российской Федерации» понятие «информационной безопасности» представлено схожим образом [15].

В зарубежной литературе подчеркивается, что подход к информационной безопасности должен носить многоуровневый и превентивный характер [16]. Сам термин связывается с такими понятиями, как конфиденциальность, целостность и доступность [17]. Конфиденциальность создает уверенность в том, что информация будет закрыта от неподходящих лиц. Целостность — в том, что данные будут точными и полными. Доступность — в том, что информацию смогут получить те, для кого она была создана [18].

Таким образом, термин «информационная безопасность» раскрывает схожее с термином «безопасность» содержание, его определение ведется в ключе доступа к информации, а также работы любого рода с ней (изменения, распространения и пр.).

Нормативно-правовой подход к информационной безопасности как термина цифрового контура здравоохранения берет начало в статье 41 Конституции РФ [19]. Устанавливается, что медицинская информация про пациента должна быть конфиденциальной, это и будет определять сохранность информационной безопасности личности пациента. В законодательстве это требование закреплено в Федеральном законе Российской Федерации №323 от 21.11.2011 «Об основах охраны здоровья граждан в Российской Федерации» [20]. Все подобные сведения, используемые в информационных системах, являются врачебной тайной [21].

Персональные данные пациента, хранящиеся в медицинских информационных системах, также подлежат защите. К информационной безопасности в системе здравоохранения предъявляется ряд следующих требований: честность, конфиденциальность, целостность, доступность, подотчетность [22, 23]. Отметим, что это является расширенной номенклатурой требований, предъявляемых к информационной безопасности, которые описаны нами ранее (при анализе зарубежной литературы).

Потребность выделения информационно-психологической безопасности как отдельного направления исследования обусловлено следующими факторами: информатизацией общества; появления понятия «цифровые отношения», неоспоримым влиянием цифровизации на состояние человека, его физическое и психическое здоровье [24].

Если анализировать данный термин с социально-философских позиций, то будет раскрываться следующее его содержание: осознание личностью уровня защищенности значимых для него интересов от внутренних и внешних угроз или опасностей, а также как социальные практики, способствующие формированию безопасного поведения [25].

В коммуникативном ключе данное понятие значит состояние защищенности социальных субъектов различных уровней общности, масштаба, системно-структурной и функциональной организации от воздействия негативных информационных факторов. Отсутствие или недостаток требуемой информации, нарушение прав в сфере ее получения также служат маркером для описания информационно-психологической безопасности личности [26].

Информационно-психологическая безопасность может быть описана и как состояние целостности активного социального субъекта в условиях информационного взаимодействия с окружающей средой [27].

Таким образом, многоаспектность и полисемантичность понятия «информационно-психологическая безопасность личности» объясняется его этимологией, историей развития, однако центральным звеном данного понятия остается личность человека, вокруг которой вырастают все смыслы.

Рассмотрим классификацию рисков информационно-психологической безопасности пациента.

В рискогенном ключе информационно-психологическая безопасность пациента включает две основные группы источников угроз: внешние и внутренние.

Основной источник — неадекватное содержание информации, а также непроверенная информация [28]. Она вводит пациента в заблуждение относительно его здоровья, дестабилизирует его и не позволяет адекватно воспринимать окружающий мир и самого себя. Информационная среда приобретает для пациента характер «второй субъективной реальности». Поскольку Интернет становится повсеместной частью информационной жизни людей, большинство людей имеют доступ к нему, им становится комфортно использовать Всемирную сеть для своих информационных нужд. В сфере здравоохранения быстрое распространение медицинской информации в Интернете привело к тому, что все больше пациентов обращаются к поисковым системам как к первому источнику медицинской информации и получают знания о возможных причинах своего текущего состояния здоровья, прежде чем обращаться за профессиональным диагнозом. Между тем это вовсе не значит, что найденные данные будут корректны [29]. В результате неправильно принятой и отраженной информации у пациента формируется та ее часть, которую условно можно обозначить как «иллюзорная реальность» [30]. Данная «реальность», сформированная на основе искаженного видения индивидом болезни и ее последствий, напрямую влияет на эффективность терапевтического процесса.

Действия субъектов, представленные в информационной среде, или алгоритм действий, который предлагается информационной средой, также являются внешним фактором угрозы информационной безопасности пациентов. Они могут сформировать у пациента систему ошибочных действий. Известно, как прочитав множество недостоверных малонаучных источников, пациент может самостоятельно поставить себе диагноз и начать лечение, что может пагубно сказаться на его здоровье. К таким источникам мы можем отнести результаты деятельности различных представителей нетрадиционной медицины, фармацевтических компаний, шаманов-целителей и других, которые активно репрезентируют в медиасреде непроверенную медицинскую информацию.

В качестве еще одного источника внешних угроз информационно-психологической безопасности личности пациента выступают сами медицинские работники. Опасность возникает, когда они, преследуя личные интересы, а иногда и просто реализуя свои амбиции, пропагандируют собственные методы лечения. Недобросовестные врачи часто используют собственный статус и маскируют свои истинные цели с целью оказания информационно-психологического воздействия на пациентов.

Безусловно, к источникам риска для личности мы можем отнести и людей, с которыми осуществляется коммуникация: родственники больного, другие пациенты, люди, выкладывающие медицинскую информацию в социальных сетях, блогах, на сайтах, форумах и др. Социально-психологические качества

субъектов, включенных в коммуникацию с пациентом, часто оказывают негативное влияние на реципиента медицинской информации. Внешними проявлениями угроз в данном случае выступают информационные грубость, невнимательность, поспешность, неполнота, недостоверность, неоконченность и т. д.

Угрозы содержатся и в самой информационной среде: недостаток нужных данных, ограничение прав личности к источникам информации [31].

К внутренним источникам угроз можно отнести особенности психики человека, ее биосоциальную природу, личностные и социально-психологические характеристики пациента. В силу этих особенностей люди по-разному могут реагировать на информационные воздействия, различным образом способны анализировать и оценивать поступающую к ним информацию. Есть некоторые шаблонные ошибки мышления, так называемые когнитивные искажения, происхождение которых обусловлено характеристиками и закономерностями функционирования психики. Их наличие делает каждого из нас обусловливаемым и поддающимся манипулятивным тактикам и стратегиям информационного характера. Кроме того, пациенты могут не обладать необходимыми навыками для оценки медицинской информации и соотнесения ее со своими потребностями.

В кризисных ситуациях повышается внушаемость людей, их восприимчивость к информационно-психологическим воздействиям. Так, в ситуации эпидемиологических рисков возрастает скорость распространения и воздействия негативной информации (посредством информационных технологий) на большие массы людей. Человек подвергается своеобразному психическому заражению определенным негативным психоэмоциональным состоянием, что отрицательным образом сказывается на формировании общественного мнения относительно всей системы здравоохранения [32].

Для обеспечения информационной безопасности следует создать надлежащую систему противодействия внутренним и внешним угрозам, такая система должна состоять из нормативно-правового, организационного и технологического компонентов [33]. Следует отметить, что, помимо выделенных компонентов, ведущим для реализации информационно-психологической безопасности выступает коммуникативный компонент.

Таким образом, важным условием и механизмом формирования цифрового коммуникативного пространства медицины и обеспечения информационно-психологической безопасности в системе здравоохранения является коммуникативная компетентность агентов взаимодействия в системе здравоохранения.

Рассмотрим, какие цифровые коммуникативные компетенции должны быть у врача для обеспечения безопасной информационной среды пациента.

Цифровизация обеспечивает расширение возможностей в медицине: от научных исследований до вопросов ухода за пациентами. Каждая область медицины находится под влиянием цифровой трансформации, что предопределяет важность формирования соответствующих навыков для каждого медицинского работника. При этом исследователи констатируют их нехватку у современных врачей [34]. Отсутствие цифровой компетентности у врача может привести к медицинским ошибкам и ослабить его желание использовать и внедрять новые цифровые инструменты, а также будет влиять на формирование адекватных цифровых отношений между врачом и пациентом [35]. В том числе это требуется для соблюдения информационной безопасности пациентов, которых следует обучать способам самозащиты в информационной среде. Пациент как объект информационно-психологического воздействия, для которого ситуация болезни является стрессовой, не может защитить себя от различного рода негативных влияний (непроверенной информации, грубых слов со стороны врача, случайно услышанных фраз о диагнозе и неправильной их трактовке и т. д.). Первостепенной задачей в этой сфере является разработка и формирование способов обучения цифровым коммуникативным компетенциям медицинских работников всех уровней.

Учеными из Калифорнийского государственного университета и из Городского университета Гонконга применительно к условиям цифровой экономики были предложены следующие компетенции, необходимые для «электронного лидера»: социально-коммуникативные и социально-технологические. На наш взгляд, данные компетенции актуальны и для специалистов, работающих в сфере медицины, так как система здравоохранения является отраслью экономики.

Социально-коммуникативные компетенции включают следующие навыки: коммуникации, социальные навыки, командообразования, создания доверия. Вместе с тем в цифровом контуре здравоохранения все эти характеристики приобретают дополнительную размерность: так, создание доверия возможно не только в живом общении врача и пациента, но и в их виртуальной коммуникации, например на форумах, где медицинские работники дают рекомендации людям по их запросу.

Социально-технологические компетенции охватывают навыки преобразования, то есть способность применять те инновации, которые возникают в цифровой среде, а также технологические навыки, предполагающие, что врач может оставаться в курсе всех разработок, а также осознает те проблемы, которые связаны с безопасностью в цифровом контуре [36], в том числе это способность применять телемедицинские технологии, знать приложения для отслеживания состояния здоровья, которые можно рекомендовать пациенту как часть его лечения, умение применять искусственный интеллект для решения медицинских задач, использовать программы для поддержки принятия медицинских решений, анализировать данные [37].

Безусловно, в условиях цифровизации традиционных социальных навыков врачу будет недостаточно. Такие навыки, как активное слушание, эмпатию необходимо объединять с навыками использования различных методов виртуального взаимодействия. При этом врачам нужно владеть различными инструментами коммуникации: способами речевого воздействия — убеждением, внушением, побуждением, стратегиями и тактиками коммуникации, навыками бесконфликтного общения, нормами речевого поведения — языковыми, коммуникативными и этическими и т. д.

Особую значимость в рамках электронного общения в диаде «врач — пациент» приобретает доверие, которое возникает у потребителей медицинских услуг как к системе в целом, так и к его агентам. При доверии пациент становится более комплаентным, уменьшается количество противоречий между ним и врачом, между ними формируется гармоничное взаимодействие. Категория «доверия» является индикатором успешности и эффективности внедрения цифровых технологий в сферу здравоохранения [38].

Важность доверия как одного из ключевых видов социального восприятия в условиях виртуального взаимодействия определяется отсутствием личных контактов между участниками лечебно-профилактического процесса, а также зависимостью от технических средств, позволяющих осуществлять коммуникацию. Одна из наиболее значительных задач в условиях цифрового взаимодействия — корректировка и расширение существующих норм и принципов общения для успешной работы в цифровом формате. Четко закрепленные нормы и правила общения в рамках виртуального взаимодействия в системе здравоохранения помогут установить доверительные отношения в диаде «врач — пациент», которые обеспечат ясность ролей каждого участника коммуникации, улучшат обратную связь и повысят удовлетворенность всех участников лечебно-профилактического процесса.

Следует отметить, что информационная безопасность пациента формирует ситуацию доверия к цифровым технологиям. Высокая степень доверия способствует координации и сотрудничеству субъектов медицинского взаимодействия, снижению опасений пациентов относительно конфиденциальности персональных данных и обеспечивает эффективное достижение поставленных целей.

Можем заключить, что функциональное благополучие личности пациента возможно в случае обеспечения его информационно-психологической безопасности в рамках цифровых отношений. Это определяет потребность разработки междисциплинарной методологии и диагностического инструментария для решения масштабных задач подготовки высококвалифицированных кадров для работы в условиях цифровой медицины и обеспечения информационно-психологической безопасности пациентов как институционального условия развития цифрового будущего медицины.

В табл. 2 представлены краткие выводы систематизированного обзора подходов к определению понятий «цифровые отношения» и «информационная безопасность».

Заключение. Цифровые технологии в здравоохранении меняют способы оказания медицинской

Таблица 2

Систематизация подходов к определению понятий «цифровые отношения» и «информационная безопасность»

Статья, год, ссылка	Основная мысль	Событие (факт)
Fu Y., Tang T., Long J., et al. Factors associated with using the internet for medical information based on the doctor-patient trust model: A cross-sectional study. 2021 [1]	Использование цифровых технологий для улучшения медицинских услуг	Цифровые отношения
Костюк А.В., Примакин А.И. Информационно-психологическая безопасность личности: проблемы и подходы. 2018 [2]	Способы преодоления угроз нарушения информационно-психологической безопасности	Информационная безопасность
Лунев А.Н., Пугачева Н.Б., Стуколова Л.З. Информационно-психологическая безопасность личности: сущностная характеристика. 2014 [3]	Основные принципы формирования информационно-психологической безопасности личности	Цифровые отношения
Belliger A., Krieger D.J. The digital transformation of healthcare. 2018 [4]	Влияние норм цифровой трансформации на изменение управления знаниями в сетях здравоохранения	
Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности. 2018 [5]	Обеспечение информационно-безопасности как условие вступления в цифровые отношения	
Warraich H.J., Califf R.M., Krumholz H.M. The digital transformation of medicine can revitalize the patient-clinician relationship. 2018 [6]	Цифровая трансформация здравоохранения может сделать оказание медицинских услуг более гуманным и персонализированным	
Åhlfeldt R.M., Söderström E. Patient safety and patient privacy in information security from the patient s view: A case study 19. 2010 [22]	Условием эффективного оказание медицинских услуг является обеспечение безопасности и конфиденциальности пациента. Основные требования к информационной безопасности в системе здравоохранения	Информационная безопасность
Брумштейн Ю.М., Кузнецова Е.О., Захаров А.Д. Медицинские данные организаций и пациентов: системный анализ категорий информации, угроз информационной безопасности, подходов к защите. 2017 [28]	Основные угрозы информационной безопасности	
Tan S.S., Goonawardene N. Internet health information seeking and the patient-physician relationship: A systematic review. 2017 [29]	Влияние онлайн-информации о здоровье на отношения пациента и врача	
Грачев Г., Мельник И. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. 1999 [30]	Проблема манипулирования людьми с использованием различных технологий и способов информационно-психологического воздействия	
Хмелевская Е. Информационная безопасность в клинике: как организовать, чтобы свести риски утечки переданных пациентов к нулю. 2020 [31]	Угрозы информационной безопасности, содержащиеся в самой информационной среде	
Курбанова З.Х., Исмаилова Н.П. Информационно-психологическая безопасность личности в условиях пандемии. 2021 [32]	Источники внутренних угроз информационной безопасности пациента	

Окончание табл. 2

Статья, год, ссылка	Основная мысль	Событие (факт)
Чегурова М.М. Руководители в условиях цифровой экономики: новые вызовы и компетенции. 2021 [33]	Навыки необходимые медицинским работникам для противодействия внутренним и внешним угрозам информационно-психологической безопасности пациента	Цифровые отношения
Roda S. Digital skills for doctors — explaining European doctors' position. 2021 [34]	Цифровые навыки врачей в трех основных областях: общие, технические и связанные с отношениями между пациентом и врачом	
Foadi N., Varghese J. Digital competence — A key competence for todays and future physicians. 2022 [35]	Необходимость включения цифровых компетенций в подготовку будущих медицинских кадров	
Roman A.V., Van Wart M., Wang X., et al. Defining e-leadership as competence in ICT-mediated communications: An exploratory. 2019 [36]	Электронное лидерство как необходимая компетенция в области коммуникации	
Slawomirski L., Auraaen A., Klazinga N. The economics of patient safety: Strengthening a value-based approach to reducing patient harm at national level. 2017 [37]	Экономика безопасности пациентов. Эффективные методы минимизации вреда, причиненного пациентам в рамках оказания медицинских помощи	Информационная безопасность
Клейменова Е.Б., Яшина Л.П. Роль медицинских информационных технологий в обеспечении безопасности пациентов. 2020 [38]	Медицинские информационные системы как важнейший фактор повышения качества, эффективности и доступности медицинской помощи. Роль МИС в обеспечении безопасности пациентов	

помощи, меняют медицинскую практику и отношения между пациентом и врачом. Пациент перемещается в цифровые отношения при получении медицинской помощи, в которых одним из главных условий выступает его информационно-психологическая безопасность. Следует отметить, что эффективность всех лечебно-профилактических процедур напрямую зависит от информационной безопасности личности пациента. Услуги, предоставляемые в рамках цифрового контура здравоохранения, должны соответствовать требованиям информационной безопасности потребителей медицинских услуг: честности, конфиденциальности, целостности, доступности, подотчетности. Формирование информационно-психологической безопасности в сфере здравоохранения требует создания надлежащей системы противодействия различного рода угрозам. Условием обеспечения информационной безопасности пациента является создание эффективных механизмов подготовки квалифицированных медицинских кадров к цифровому будущему и формирование у врачей новых цифровых коммуникативных компетенций как одной из стратегических задача современной высшей медицинской школы. Об этом свидетельствует проведенный анализ отечественных и зарубежных литературных источников.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

References (Список источников)

1. Fu Y, Tang T, Long J, et al. Factors associated with using the internet for medical information based on the doctor-patient trust model: A cross-sectional study. BMC Health Serv Res. 2021; 21 (1): 1268. DOI: 10.1186/s12913-021-07283-6

1. Kostyuk AV, Primakin AI. Information and psychological security of a person: Problems and approaches. Bulletin of the Saint Petersburg University of the Ministry of Internal Affairs of Russia. 2018; 3 (79): 227–30. (In Russ.) Костюк А.В., Примакин А.И. Информационно-психологическая безопасность личности: проблемы и подходы. Вестник Санкт-Петербургского университета МВД России. 2018; 3 (79): 227–30.

2. Lunev AN, Pugacheva NB, Stokolova LZ. Informational and psychological security of a person: essential characteristic. Modern Problems of Science and Education. 2014; 1. (In Russ.) Лунев А.Н., Пугачева Н.Б., Стуколова Л.З. Информационно-психологическая безопасность личности: сущностная характеристика. Современные проблемы науки и образования. 2014; 1.

3. Belliger A, Krieger DJ. The digital transformation of healthcare. In: North K, Maier R, Haas O, eds. Knowledge Management in Digital Change. Progress in IS. Springer, Cham. 2018; 311–26. DOI: 10.1007/978-3-319-73546-7_19

4. Khabrieva TYa, Chernogor NN. Law in a digital reality. Journal of Russian Rights. 2018; 1: 85–102. (In Russ.) Хабриева Т.Я., Черногор Н.Н. Право в условиях цифровой реальности. Журнал российского права. 2018; 1: 85–102.

5. Warraich HJ, Califf RM, Krumholz HM. The digital transformation of medicine can revitalize the patient-clinician relationship. NPJ Digit Med. 2018; 1: 49. DOI: 10.1038/s41746-018-0060-2

6. Voshed DV. Digital evolution in the field of healthcare: trends and legal regulation of digitalization of primary health care in the Russian Federation (analytical review). Health Care Manager. 2023; 11: 71–83 (In Russ.) Вошед Д.В. Цифровая эволюция в сфере здравоохранения: тенденции и правовое регулирование цифровизации первичной медико-санитарной помощи в Российской Федерации (аналитический обзор). Менеджер здравоохранения. 2023; 11: 71–83. DOI: 10.21045/1811-0185-2023-11-71-83

7. The Chambers dictionary. 13th edition. London: Chambers Harrap Publishers Ltd., 2014. URL: http://0-search.credoreference.com.brum.beds.ac.uk/content/title/chambdict (19 April 2024).

8. Simpson JA, Weiner ESC. Oxford English Dictionary. 2nd ed. Oxford: Oxford University Press, 1989.

9. Garner BA. Garner's Modern American Usage. 4th ed. Oxford: Oxford University Press, 2016.

10. Larousse. fr: encyclopedie et dictionnaires gratuits en ligne. URL: https://www.larousse.fr/(18 April 2024).

11. Roshchin SK, Sosinin VA. Psychological security: New approach to human, society and state security. Rossiiskii Monitor. 1995; 6: 28–35. (In Russ.) Рощин С.К., Соснин В.А. Психологическая безопасность: новый подход к безопасности человека, общества и государства. Российский монитор. 1995; 6: 28–35.

12. Markov AA. Characteristics of information security at the present stage of society development. Management consulting. Current Problems of State and Municipal Management. 2011; 3 (43): 67–76. (In Russ.) Марков А.А. Характеристики информационной безопасности на современном этапе развития общества. Управление консультирование. Актуальные проблемы государственного и муниципального управления. 2011; 3 (43): 67–76.

13. Kurilo AP, Miloslavskaya NG, Senatorov MYu, Tolstoy AI. Fundamentals of information security management. Textbook for universities. Moscow: Hot Line — Telecom, 2012; 202 p.

(In Russ.) Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Основы управления информационной безопасностью: учеб. пособие для вузов. М.: Горячая линия — Телеком, 2012; 202 с.

14. On Approval of the Doctrine of Information Security of the Russian Federation: Decree of the President of the Russian Federation from 05.12.2016 №646. (13 April 2024) (In Russ.) Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 №646. URL: https://base.garant.ru/71556224/?ysclid=m4pscrysn3870204036 (дата обращения: 13.04.2024).

15. Syed RSh, Shah S, Aqsa A. Information Security. In: Information Security. Scientific Knowledge Publisher (SciKnowPub), 2024. DOI: 10.5281/zenodo. 10399564. URL: https://www.researchgate.net/publication/377416697_Information_Security (13 April 2024).

16. Nieles M, Dempsey K, Pillitteri VY. An Introduction to Information Security. 2017. DOI: 10.6028/NIST. SP. 800-12r1. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf (13 April 2024).

17. Lundgren B, Möller N. Defining information security. Sci Eng Ethics. 2019; 25 (2): 419–441. DOI: 10.1007/s11948-017-9992-1

18. The Constitution of the Russian Federation. URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (13 April 2024) (In Russ.) Конституция Российской Федерации. URL: http://www.consultant.ru/document/cons_doc_LAW_28399/(дата обращения: 13.04.2024).

19. On the Basics of Public Health protection in the Russian Federation: Federal Law dated 21.11.2011 No. 323-FZ. URL: http://www.consultant.ru/document/cons_doc_LAW_121895/ (13 April 2024) (In Russ.) Об основах охраны здоровья граждан в Российской Федерации: Федер. закон от 21.11.2011 №323-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_121895/(дата обращения: 13.04.2024).

20. Tegza VYu, Chernikov AA, Bigunets VD. On the issue of modern strategies and new risk factors in public health. In: Modern scientific and educational strategies in public health. Russian scientific and practical conference. Saint Petersburg: Kirov Military medical academy, 2018; p. 216–24. (In Russ.) Тегза В.Ю., Черников А.А., Бигунец В.Д. К вопросу о современных стратегиях и новых факторах риска в общественном здоровье. В кн.: Современные научные и образовательные стратегии в общественном здоровье: материалы Рос. науч.-практ. конференции. Saint Petersburg: Kirov Military Medical Academy, 2018; p. 216–24.

21. Åhlfeldt RM, Söderström E. Patient safety and patient privacy in information security from the patient s view: A Case Study19. Information Security in Distributed Healthcare. 2010; 450: 230–9.

22. On Information, Information Technologies and Information Protection: Federal Law No. 149-FZ of 27.07.2006. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/(13 April 2024) (In Russ.) Об информации, информационных технологиях и о защите информации: Федер. закон от 27.07.2006 №149-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/(дата обращения: 13.04.2024).

23. Mantsurova OV, Soluyanov IO, Katishin DA. Modern problems of patient safety related to information technology in the field of health care. In: Science in modern society: Patterns and trends of development. Collection of articles of the International Scientific and Practical Conference. Ufa, 2022; p. 33–35. (In Russ.) Манцурова О.В., Солуянов И.О., Катишин Д.А. Современные проблемы безопасности пациентов, связанные с информационными технологиями в области здравоохранения. В кн.: Наука в современном обществе: закономерности и тенденции развития: сб. ст. Междунар. науч.-практ. конференции. Уфа, 2022; с. 33–35.

24. Lunev AN, Pugacheva NB. Social practice as a philosophical basis of pedagogical strategizing in a technical university. Society: Philosophy, History, Culture. 2013; 4. URL: http://dom-hors.ru/issue/fik/2013-4/lunev-pugacheva.pdf (13 April 2024) (In Russ.) Лунев А.Н., Пугачева Н.Б. Социальная практика как философское основание педагогического стратегирования в техническом вузе. Общество: философия, история, культура. 2013; 4. URL: http://dom-hors.ru/issue/fik/2013-4/lunev-pugacheva.pdf (дата обращения: 13.04.2024).

25. Grachev GV. Informational and psychological security of a person: the state and possibilities of psychological protection. URL: htpp://bookap.by.ru/psywar/grachev (13 April 2024) (In Russ.) Грачёв Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты. URL: htpp://bookap.by.ru/psywar/grachev (дата обращения: 13.04.2024).

26. Dmitrieva LG, Bulayev MO. On the question of information and psychological security of the person. In: Innovative development: The potential of science and modern education. Collection of articles II of the International Scientific and Practical Conference. Penza: Nauka i Prosveschenie (IP Gulyaev G.Yu.), 2018; p. 347–51. (In Russ.) Дмитриева Л.Г., Булаев М.О. К вопросу об информационно-психологической безопасности личности. В кн.: Инновационное развитие: потенциал науки и современного образования: сб. ст. II Междунар. науч.-практ. конференции. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2018; с. 347–51.

27. Brumshtein YuM, Kuznetsova EO, Zakharov AD. Medical data of organizations and patients: System analysis of categories of information, threats to information security, approaches to protection. In: Methods of computer diagnostics in biology and medicine — 2017. Materials of the All-Russian school-seminar. Ed. D. A. Usanov. Saratov: Saratov Source, 2017; p. 65–9. (In Russ.) Брумштейн Ю.М., Кузнецова Е.О., Захаров А.Д. Медицинские данные организаций и пациентов: системный анализ категорий информации, угроз информационной безопасности, подходов к защите. В кн.: Методы компьютерной диагностики в биологии и медицине — 2017: материалы Всерос. школы-семинара. Саратов: Саратовский источник, 2017; с. 65–9.

28. Tan SS, Goonawardene N. Internet health information seeking and the patient-physician relationship: A systematic review. J Med Internet Res. 2017; 19 (1): e9. DOI: 10.2196/jmir.5729

29. Grachev G, Melnik I. Personal manipulation: organization, methods and technologies of information and psychological impact. Moscow: IFRAS, 1999; 230 p. (In Russ.) Грачев Г., Мельник И. Манипулирование личностью: организация, способы и технологии информационно-психологического воздействия. М.: ИФРАН, 1999; 230 с.

30. Khmelevskaya E. Information security in the clinic: how to organize to reduce the risks of leakage of transferred patients to zero. Pravovye Voprosy v Zdravookhranenii. 2020; 3: 54–65. (In Russ.) Хмелевская Е. Информационная безопасность в клинике: как организовать, чтобы свести риски утечки переданных пациентов к нулю. Правовые вопросы в здравоохранении. 2020; 3: 54–65.

31. Kurbanova ZH, Ismailova NP. Informational and psychological security of the person in the conditions of a pandemic. Mir nauki, kul'tury, obrazovaniya. 2021; 4 (89): 147–8. (In Russ.) Курбанова З.Х., Исмаилова Н.П. Информационно-психологическая безопасность личности в условиях пандемии. Мир науки, культуры, образования. 2021; 4 (89): 147–8. DOI: 10.24412/1991-5497-2021-489-147-148

32. Chegurova MM. Leaders in the digital economy: New challenges and competencies. Bulletin of Saint Petersburg University. Sociology. 2021; 14 (3): 208–23. (In Russ.) Чегурова М.М. Руководители в условиях цифровой экономики: новые вызовы и компетенции. Вестник Санкт-Петербургского университета. Социология. 2021; 14 (3): 208–23.

33. Roda S. Digital skills for doctors — explaining European doctors' position. J Eur CME. 2021; 10 (1): 2014097. DOI: 10.1080/21614083.2021.2014097

34. Foadi N, Varghese J. Digital competence — A key competence for todays and future physicians. J Eur CME. 2022; 11 (1): 2015200. DOI: 10.1080/21614083.2021.2015200

35. Roman AV, Van Wart M, Wang X, et al. Defining e-leadership as competence in ICT-mediated communications: An exploratory. Pub Admin Assessment Revue. 2019; 79: 853–66.

36. Slawomirski L, Auraaen A, Klazinga N. The economics of patient safety: Strengthening a value-based approach to reducing patient harm at national level: OECD Health Working Papers, 96. Paris: OECD Publ., 2017; 63 p. DOI: 10.1787/5a9858cd-en

37. Kleymenova EB, Yashina LP. The role of medical information technology in ensuring the safety of patients. Vrach i Informatsionnye Tekhnologii. 2020. 3: 13–24. (In Russ.) Клейменова Е.Б., Яшина Л.П. Роль медицинских информационных технологий в обеспечении безопасности пациентов. Врач и информационные технологии. 2020. 3: 13–24. DOI: 10.37690/1811-0193-2020-3-13-24

Статья поступила в редакцию 12.03.2024; одобрена после рецензирования 25.10.2024; принята к публикации 22.11.2024.
The article was submitted 12.03.2024; approved after reviewing 25.10.2024; accepted for publication 22.11.2024.

Информация об авторе:

Зульфия Эиповна Кудашева *— аспирант кафедры философии, гуманитарных наук и психологии, zulfam05@mail.ru, ORCID 0000-0001-6662-8106.*

Information about the author:

Zulfia E. Kudasheva *— Post-graduate Student of the Department of Philosophy, Humanities and Psychology, zulfam05@mail.ru, ORCID 0000-0001-6662-8106.*

УДК 614.2
EDN: XQLDDH
https://doi.org/10.15275/ssmj499

Оригинальная статья

УПРАВЛЕНИЕ ЗАПАСАМИ ИНТРАОКУЛЯРНЫХ ЛИНЗ В УСЛОВИЯХ ГЕОПОЛИТИЧЕСКОЙ НЕСТАБИЛЬНОСТИ

С.Н. Светозарский *[1, 2], **А.Н. Андреев*** *[1], **О.П. Абаева*** *[3], **С.В. Романов*** *[1]*

[1]ФБУЗ «Приволжский окружной медицинский центр» ФМБА России, Нижний Новгород, Россия
[2]ФГБОУ ВО «Приволжский исследовательский медицинский университет» Минздрава России, Нижний Новгород, Россия
[3]ФГАОУ ВО «Первый Московский государственный медицинский университет им. И.М. Сеченова» Минздрава России (Сеченовский Университет), Москва, Россия

INVENTORY MANAGEMENT OF INTRAOCULAR LENSES UNDER GEOPOLITICAL INSTABILITY

S.N. Svetozarskiy *[1, 2], **A.N. Andreev*** *[1], **O.P. Abaeva*** *[3], **S.V. Romanov*** *[1]*

[1]Volga District Medical Center under the Federal Medical and Biological Agency, Nizhny Novgorod, Russia
[2]Privolzhsky Research Medical University, Nizhny Novgorod, Russia
[3]I. M. Sechenov First Moscow State Medical University (Sechenov University), Moscow, Russia

Для цитирования: ***Светозарский С.Н., Андреев А.Н., Абаева О.П., Романов С.В.*** **Управление запасами интраокулярных линз в условиях геополитической нестабильности. Саратовский научно-медицинский журнал. 2024; 20 (4): 499–504. EDN: XQLDDH. https://doi.org/10.15275/ssmj499.**

Аннотация. *Цель:* разработка и научное обоснование целесообразности применения бережливой системы управления запасами интраокулярных линз (ИОЛ) в условиях геополитической нестабильности. *Материал и методы*. Исследование состояло из этапов анализа распределения оптической силы ИОЛ, создания математической модели потребности учреждения в ИОЛ, внедрения разработанной системы и оценки ее эффективности в условиях геополитической нестабильности в период с января 2022 по декабрь 2023 г. *Результаты.* В результате внедрения предложенного подхода объем закупок ИОЛ, осуществляемый дополнительно к плановым заказам, снизился с 4,5% заявок в 2014–2015 гг. до 0,2% в 2022–2023 гг. (p<0,001). Система управления запасами стабильно обеспечивала наличие ИОЛ необходимой оптической силы, облегчала принятие организационных решений, исключала необходимость заказов на срочную поставку и обмен ИОЛ с поставщиком, высвобождала трудовые ресурсы и способствовала обеспечению доступности специализированной медицинской помощи пациентам с катарактой в период нарушения функционирования ранее сложившихся логистических цепочек. *Заключение.* Разработанная бережливая система управления запасами ИОЛ продемонстрировала высокую целесообразность применения, позволив противостоять рискам, связанным с геополитической нестабильностью в мире, сэкономить трудовые и материальные ресурсы медицинской организации, обеспечить непрерывность лечебного процесса.

Ключевые слова: управление запасами медицинских изделий, интраокулярные линзы, катаракта, логистика

For citation: ***Svetozarskiy SN, Andreev AN, Abaeva OP, Romanov SV.*** **Inventory management of intraocular lenses under geopolitical instability. Saratov Journal of Medical Scientific Research. 2024; 20 (4): 499–504. (In Russ.) EDN: XQLDDH. https://doi.org/10.15275/ssmj499.**

Abstract. *Objective:* to develop and scientifically validate the feasibility of applying a lean intraocular lens (IOL) inventory management system under conditions of geopolitical instability. *Material and methods.* The study consisted of the steps of analyzing the distribution of IOL optical power, creating a mathematical model of the institution's need for IOLs, implementing the developed system, and evaluating its effectiveness under geopolitical instability from January 2022 to December 2023. *Results*. As a result of implementing the proposed approach, the volume of IOL purchases made in addition to planned orders decreased from 4.5% of requests in 2014–2015 to 0.2% in 2022–2023 (p<0.001). The inventory management system steadily ensured the availability of IOLs of the required optical power, facilitated organizational decision-making, eliminated the need for orders for urgent delivery and exchange of IOLs with the supplier, freed up labor resources and contributed to the availability of specialized medical care for cataract patients during the period of disruption of previously established logistics chains. *Conclusion*. The developed lean system of IOL inventory management demonstrated high efficiency, saving labor and material resources of the medical organization, ensuring the continuity of the treatment process and resisting the risks associated with geopolitical instability in the world.

Keywords: medical device inventory management, intraocular lenses, cataract, logistics