

Научная статья

УДК 331.54

DOI: <https://doi.org/10.63973/2949-1258/2025-3/095-105>

EDN: <https://elibrary.ru/ZIFOJG>

## **Нормативное регулирование деятельности управленческих кадров по информационной безопасности в сфере здравоохранения**

**Гавришев Алексей Андреевич**

Московский государственный лингвистический университет

Москва, Россия

***Аннотация.** На основании проведенных исследований и данных из различных источников предложены возможные меры по совершенствованию нормативной базы, регулирующей работу управленческих кадров по информационной безопасности (ИБ) в сфере здравоохранения. Анализ выявил, что текущая нормативно-правовая база, регулирующая деятельность управленческих кадров по ИБ в отечественном здравоохранении, опирается на федеральные законы, указы Президента РФ и постановления Правительства РФ. Однако существующие нормативные правовые акты (НПА) в указанной области не содержат конкретных положений, учитывающих специфику сферы здравоохранения. Подчеркивается необходимость детализации этих вопросов в НПА Министерства здравоохранения РФ и иных отраслевых подзаконных документах. С учетом требований законодательства и анализа различных источников предложены упрощенные варианты внесения изменений в некоторые отраслевые НПА, касающиеся регулирования деятельности управленческих кадров по ИБ в здравоохранении. Несомненно, что представленный перечень возможных улучшений нормативной базы, регулирующей работу управленческих кадров по ИБ в здравоохранении, не является до конца исчерпывающим. Однако авторы полагают, что комплексное применение предложенных мер может способствовать улучшению ситуации в данной области в будущем. Полученные выводы и рекомендации могут быть полезны экспертам, занимающимся разработкой квалификационных требований к управленческим кадрам по ИБ в системе здравоохранения, а также руководителям медицинских организаций и профильным специалистам, работающим в этих учреждениях.*

***Ключевые слова:** управленческие кадры, информационная безопасность, здравоохранение, нормативное регулирование, совершенствование.*

***Для цитирования:** Гавришев А.А. Нормативное регулирование деятельности управленческих кадров по информационной безопасности в сфере здравоохранения // Территория новых возможностей. Вестник Владивостокского государственного университета. 2025. Т. 17, № 3. С. 95–105. DOI: <https://doi.org/10.63973/2949-1258/2025-3/095-105>. EDN: <https://elibrary.ru/ZIFOJG>*

Original article

## **Normative regulation of the activities of management personnel on information security in the healthcare sector**

**Alexey A. Gavrishev**

Moscow State Linguistic University

Moscow, Russia

---

© Гавришев А.А., 2025

**Abstract.** Based on the conducted research and data from various sources, this article suggests possible measures to improve the regulatory framework governing the work of management personnel on information security (IS) in the healthcare sector. The analysis revealed that the current regulatory framework governing the activities of management personnel on IS in domestic healthcare is based on federal laws, decrees of the President of the Russian Federation and resolutions of the Government of the Russian Federation. However, the existing legal acts in this area do not contain specific provisions that take into account the specifics of the healthcare sector. It emphasizes the need to detail these issues in the legal acts of the Ministry of Health of the Russian Federation and other sectoral bylaws. Taking into account the requirements of legislation and the analysis of various sources, simplified options for making changes to some sectoral regulations concerning the regulation of management personnel on IS in healthcare are proposed. Undoubtedly, the presented list of possible improvements to the regulatory framework governing the work of management personnel on IS in healthcare is not completely exhaustive. However, the authors believe that the integrated application of the proposed measures may contribute to improving the situation in this area in the future. The conclusions and recommendations obtained can be useful to experts involved in the development of qualification requirements for management personnel on IS in the healthcare system, as well as to heads of medical organizations and specialists on IS working in these institutions.

**Keywords:** management personnel, information security, healthcare, normative regulation, improvement.

**For citation:** Gavrishev A.A. Normative regulation of the activities of management personnel on information security in the healthcare sector // *The Territory of New Opportunities. The Herald of Vladivostok State University*. 2025. Vol. 17, № 3. P. 95–105. DOI: <https://doi.org/10.63973/2949-1258/2025-3/095-105>. EDN: <https://elibrary.ru/BZIFOJG>

### Введение

В динамичной обстановке последствия решений, принимаемых управленческими кадрами, становятся все более значимыми. В начале XXI в. исследователями было установлено, что итоговое качество любого продукта или сервиса, предоставляемого любой организацией, практически на 100 % обусловлено эффективностью управления ключевыми процессами [1]. При этом известно, что организация любой формы собственности по своей сути является в некотором роде системой [1–3]. Обычно под системой понимается множество (совокупность) элементов (объектов) любой природы, взаимодействующих между собой для достижения общей цели и обладающих системным свойством / свойствами. Одно из центральных мест в достижении общих целей отводится процессам управления. Под управлением будем понимать функцию организованных систем различной природы, обеспечивающую сохранение их определенной структуры, поддержание режима деятельности, реализацию программ, цели деятельности [2]. Важной характеристикой для процесса управления является управляющее воздействие, под которым понимается воздействие субъекта управления, например компетентного должностного лица, на объект управления, направленное на достижение цели управления. Обычно управляющее воздействие реализуется через управленческое решение, под которым понимается акт волеизъявления субъекта управления, адресованный объекту управления, о необходимости выполнения последним конкретных действий [2, 3], в то время как управленческое решение всегда представляется в виде указания, приказа или распоряжения.

Вместе с тем в условиях масштабной цифровизации экономики, расширения использования информационных технологий и иных технологических новшеств неперенным условием эффективного управления любыми системами, например социальными, является наличие нормативно-правового обеспечения процессов управления. Известно, что главенствующее место в нормативно-право-

вом обеспечении любых процессов занимает государство, которое с помощью государственного регулирования той или иной деятельности может прямо или косвенно устанавливать требования к соответствующим видам деятельности посредством издания различных нормативных правовых актов (НПА), имеющих обязательную юридическую силу [2, 3].

В настоящее время одной из самых важных социальных сфер, от которой зависит благополучие современного общества, является здравоохранение. Исходя из вышесказанного результативность системы здравоохранения, уровень и доступность медицинской помощи для населения, скорость технологического прогресса в отрасли, а также успех в реализации утвержденных программ в значительной степени зависят от квалификации и мотивированности руководящего состава медицинских учреждений [4–6]. В отечественном здравоохранении одним из сравнительно недавно появившихся и еще не получивших повсеместного распространения направлений развития управленческих кадров является деятельность по управлению обеспечением информационной безопасностью (ИБ) в медицинских учреждениях. В соответствии с НПА по ИБ организации здравоохранения [7–9], выступая в качестве субъектов критической информационной инфраструктуры (КИИ), должны делегировать полномочия в области обеспечения ИБ заместителю руководителя.

В настоящее время обеспечение ИБ объектов КИИ, владельцами которых являются субъекты КИИ, в том числе медицинские учреждения, является одним из приоритетных направлений развития цифровой экономики РФ [7–9]. Логичным объяснением данного факта, с одной стороны, является бурное развитие информационных технологий и их внедрение во все сферы жизни общества, включая здравоохранение, а с другой – порождаемые новыми технологиями угрозы безопасности [2, 10–12]. Так, только за первые полгода 2024 г. количество компьютерных атак на российские учреждения здравоохранения выросло на треть по сравнению с аналогичным периодом 2023 г. [13]. При этом почти половина успешных компьютерных атак за этот период привела к тому, что пострадавшие медицинские учреждения временно не могли оказать некоторые виды медицинской помощи или теряли доступ к данным. В указанных условиях, помимо совершенствования нормативного регулирования в указанной области, регуляторы в области ИБ также проводят проверки соответствующих организаций, в том числе и из сферы здравоохранения. В частности, по результатам мониторинга, проведенного ФСТЭК России, выяснилось, что практически 90 % объектов КИИ не имеют минимального уровня защищенности, установленного соответствующими НПА [14].

На основании этого в целях соблюдения законодательных требований по ИБ Министерство здравоохранения РФ выпустило информационное письмо, подчеркивающее необходимость возложения ответственности за ИБ на заместителей руководителей медицинских учреждений, а также определяющее требования к их образованию и опыту работы [15].

Таким образом, на сегодняшний день управленческие кадры по ИБ стали неотъемлемой частью организационной структуры учреждений здравоохранения.

Однако ввиду новизны и недостаточной разработанности этой области исследование информационной безопасности остается актуальным и требует дальнейшей проработки [16].

*Цель статьи* – разработка предложений по совершенствованию нормативной базы, регулирующей деятельность управленческих кадров по ИБ в системе здравоохранения РФ.

### **Основная часть**

В работе [17] проведено исследование ситуации на рынке труда в области управленческих кадров, отвечающих за ИБ в медицинских учреждениях РФ. В результате проведенных исследований установлено, что в большинстве случаев в литературе анализируется либо рынок труда управленческих кадров в здравоохранении в целом, без учета специфики работы по ИБ, либо рынок труда управленческих кадров по ИБ, не ориентированных на работу в медицинской отрасли. Итогом проведенного анализа стал вывод о том, что вопреки наличию четких законодательных требований для рассматриваемых специалистов в РФ пока не наблюдается ни устоявшейся организационной структуры, ни развитого рынка труда в этой области [17]. Кроме этого указано, что нехватка квалифицированных кадров по ИБ на рынке труда также осложняет процесс подбора соответствующих сотрудников. Установлено, что рынок труда в области управленческих кадров по ИБ для учреждений здравоохранения находится в стадии формирования. Следовательно, необходимы дальнейшие исследования по совершенствованию информационной безопасности.

В связи с вышесказанным одним из важных направлений в исследуемой области является нормативно-правовое регулирование деятельности управленческих кадров по ИБ в системе здравоохранения. Известно, что в РФ законодательство имеет вертикальную (по видам правовых актов) и горизонтальную структуру (по отраслям законодательства) [18].

Согласно первой классификации структура российского законодательства включает в себя [2, 3, 18]:

- Конституцию РФ;
- федеральные законы и кодексы;
- указы Президента РФ и постановления Правительства РФ;
- НПА федеральных органов исполнительной власти;
- другие законодательные акты (НПА субъектов РФ и пр.).

Непосредственно, касаясь исследуемой тематики, отметим, что в настоящее время в РФ нормативно-правовое регулирование деятельности управленческих кадров по ИБ в системе здравоохранения основывается на Федеральном законе [7], Указе Президента РФ [8] и Постановлении Правительства РФ [9]. Вместе с тем указанные НПА не уточняют отдельные вопросы, специфические для отрасли здравоохранения; они должны уточняться в НПА Министерства здравоохранения РФ и иных отраслевых подзаконных актах. При этом единственным отраслевым НПА, регулирующим в настоящее время деятельность управленческих кадров по ИБ в системе здравоохранения, является НПА, представленный в работе [15].

Среди нераскрытых вопросов в области деятельности управленческих кадров по ИБ в системе здравоохранения отметим следующие [17]:

- в сфере здравоохранения нет общепринятого названия для должности заместителя руководителя, ответственного за обеспечение ИБ;

- для государственных и муниципальных организаций здравоохранения не определены нормы штатной численности для должности заместителя руководителя, ответственного за обеспечение ИБ.

Различные нераскрытые вопросы в исследуемой области, в том числе описанные выше, способны в будущем осложнить процесс применения требований соответствующих НПА, что может привести к неблагоприятным последствиям различного характера.

В таблице 1 приведены отдельные НПА, которые непосредственно соприкасаются с указанными вопросами. Анализ НПА (см. табл. 1) показывает, что представленные выше вопросы в области деятельности управленческих кадров по ИБ в системе здравоохранения не раскрыты [17].

Таблица 1

**Отдельные НПА, регулирующие деятельность кадров в системе здравоохранения**

№ п/п	Наименование НПА	Номер источника
1	Квалификационный справочник должностей руководителей, специалистов и других служащих (утв. Постановлением Минтруда России от 21.08.1998 № 37)	[19]
2	Приказ Минздравсоцразвития РФ от 22.04.2009 № 205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации»	[20]
3	Приказ Минздрава РФ от 09.06.2003 № 230 «Об утверждении штатных нормативов служащих и рабочих государственных и муниципальных учреждений здравоохранения и служащих централизованных бухгалтерий при государственных и муниципальных учреждениях здравоохранения» (далее – приказ Минздрава РФ от 09.06.2003 № 230)	[21]
4	Методические рекомендации по формированию службы информационных технологий в медицинских организациях (утв. ФГБУ «ЦНИИОИЗ» Минздрава России 04.03.2022) (далее – Методические рекомендации)	[22]

*Примечание:* сост. автором.

С учетом вышесказанного предлагается усовершенствовать нормативную базу, регулирующую деятельность управленческих кадров по ИБ в системе здравоохранения, с помощью следующих предложений [17]:

– с учетом требований законодательства рекомендуется внести дополнения в отдельные профессиональные стандарты в сфере ИБ, добавив положение о должности заместителя руководителя, ответственного за обеспечение ИБ. Необходимо указать наименование должности, круг обязанностей, требования к образованию и опыту, а также другие характеристики;

– с учетом требований законодательства в соответствующие справочник и приказ [19, 20] рекомендуется внести дополнение о заместителе руководителя организации, ответственного за обеспечение ИБ, вне зависимости от направления деятельности организации. Необходимо определить название должности, функциональные обязанности, квалификационные требования и пр.;

– рекомендуется официально утвердить типовое название должности заместителя руководителя медицинской организации, ответственного за обеспечение ИБ;

– в целях соблюдения требований НПА предлагается включить в документ [21] пункт, касающийся позиции заместителя руководителя медицинского учреждения, ответственного за обеспечение ИБ. Следует указать общепринятое название должности и число требуемых ставок;

– с учетом требований законодательства рекомендуется внести изменения в документ [22], добавив в него информацию о должности заместителя руководителя медицинской организации, ответственного за обеспечение ИБ. Необходимо указать общепринятое обозначение должности, круг обязанностей, квалификационные требования и пр.

В силу ограниченного объема статьи в качестве примера приведем упрощенные варианты внесения дополнений и изменений в соответствующие приказ и Методические рекомендации [21, 22] согласно представленным выше рекомендациям и требованиям законодательства. Условимся считать, что в НПА, которые регулируют основные положения о должности заместителя руководителя, ответственного за обеспечение ИБ, вне зависимости от направления деятельности организации уже внесены соответствующие дополнения и изменения [19], а в отраслевые НПА – пока еще нет.

С учетом требований [7–9] и отдельных результатов [10, 16, 17] представим упрощенный вариант внесения дополнений в приказ Министерства здравоохранения РФ от 09.06.2003 № 230. Для оптимизации вопросов совершенствования указанного НПА изменения предлагается внести в виде приложения № 4 к приказу Министерства здравоохранения РФ от 09.06.2003 № 230. Полученные результаты приведены в табл. 2.

Как видно из табл. 2, с учетом требований законодательства любое медицинское учреждение, являющееся субъектом КИИ, должно предусмотреть в своем штатном расписании должность заместителя руководителя по обеспечению ИБ. При этом количество должностей специалистов по ИБ, которые подчиняются заместителю руководителя по обеспечению ИБ, определяется в соответствии с [22].

Таблица 2

**Упрощенный вариант внесения дополнений в приказ Министерства здравоохранения РФ от 09.06.2003 № 230 в виде приложения к нему № 4**

Штатные нормативы структурных подразделений (работников), уполномоченных на решение задач в области обеспечения информационной безопасности государственных и муниципальных учреждений здравоохранения		
№ п/п	Тип учреждения	Наименование должностей
1	Любой тип медицинского учреждения, являющегося субъектом КИИ	1. Одна должность заместителя главного врача (директора, заведующего, начальника) по ИБ. 2. Количество должностей специалистов по ИБ, определяемое в соответствии с [22]

*Примечание:* сост. автором по [7–10, 16, 17].

С учетом требований [7–9] и отдельных результатов [10, 16, 17] представим упрощенный вариант внесения дополнений и изменений в Методические рекомендации [22]. Полученные результаты приведены в табл. 3.

Таблица 3

**Упрощенный вариант внесения дополнений и изменений в Методические рекомендации**

№ п/п	Название раздела	Вносимые дополнения и изменения
1	4. Цели, задачи и функции ИТ-службы медицинской организации	Уточнение целей, задач и функций в области ИБ с учетом требований [7–9]
2	5. Направления деятельности ИТ-службы	Уточнение направлений деятельности в области ИБ с учетом требований [7–9]
3	6. Структура ИТ-службы и рекомендуемое количество ставок	1. Ввести должность заместителя главного врача (директора, заведующего, начальника) по ИБ (описать требования к уровню образования и обучению, опыту практической работы, трудовым функциям, количеству ставок и т.д. согласно [7–9]). 2. Для специалистов службы обеспечения ИБ в п. 6.5 уточнить требования к уровню образования, опыту практической работы, трудовым функциям и количеству ставок согласно [7–9]. 3. Отобразить, что служба обеспечения ИБ подчиняется заместителю главного врача (директора, заведующего, начальника) по ИБ. 4. Пересмотреть типовые нормы времени на техническое и сервисное обслуживание информационных ресурсов в государственных (муниципальных) учреждениях для сотрудников, обеспечивающих ИБ, с учетом требований [7–9]

*Примечание:* сост. автором по [7–10, 16, 17].

Как видно из табл. 3, с учетом требований законодательства любое медицинское учреждение, являющееся субъектом КИИ, помимо назначения заместителя руководителя, ответственного за обеспечение ИБ, должно сформировать у себя службу обеспечения ИБ, которая должна подчиняться такому заместителю руководителя. Требования к уровню образования данных кадров, их опыту практической работы и трудовым функциям определяются соответствующим законодательством.

### **Заключение**

Таким образом, на основании проведенных исследований и данных из различных источников предложены возможные меры по совершенствованию нормативной базы, регулирующей работу управленческих кадров по ИБ в сфере здравоохранения РФ.

Проведен анализ нормативно-правового регулирования деятельности управленческих кадров по ИБ в системе здравоохранения. Приведены примеры НПА (федеральные законы, указы Президента РФ, постановления Правительства РФ и пр.), регулирующих информационную безопасность. Отмечено, что в настоящее время в РФ отсутствуют отраслевые НПА, регулирующие указанную область деятельности. Указаны некоторые нераскрытые вопросы в области деятельности управленческих кадров по ИБ в системе здравоохранения [17]. С учетом требований законодательства [7–9] и отдельных результатов [10, 16, 17] представлены упрощенные варианты внесения дополнений о нормативном регулировании деятельности управленческих кадров по ИБ в сфере здравоохранения в некоторые существующие отраслевые НПА [21, 22].

Разумеется, перечень потенциальных решений по оптимизации НПА, регулирующих деятельность управленческих кадров по ИБ в здравоохранении, не исчерпывается предложенным. Тем не менее комплексное внедрение вышеупомянутых мероприятий, по мнению авторов, сможет в будущем положительно повлиять на текущее положение дел в рассматриваемой сфере.

### **Список источников**

1. Деминг У.Э. Новая экономика. Москва: Эксмо, 2006. 208 с.
2. Капгер И.В., Шабуров А.С. Управление информационной безопасностью. Пермь: Изд-во Пермского нац. исслед. политехн. ун-та, 2023. 91 с.
3. Мазеин А.В. Правовое регулирование управленческой деятельности. Москва: Юрайт, 2025. 189 с.
4. Михайлова Ю.В., Мирошникова Ю.В., Князев А.А. Руководящие кадры органов и учреждений здравоохранения (социологическое исследование) // Вестник Росздравнадзора. 2014. № 6. С. 71–77.
5. Найговзина Н.Б., Сон И.М., Зимина Э.В. Подходы к оценке численности управленческих кадров здравоохранения // Современные проблемы здравоохранения и медицинской статистики. 2022. № 4. С. 537–558. DOI: 10.24412/2312-2935-2022-4-537-558
6. Модель компетенций руководителя в сфере охраны здоровья / О.В. Кунгурцев, Д.С. Тюфилин, О.Б. Павленко [и др.] // Социальные аспекты здоровья населения. 2024. № S5. С. 1–8. DOI: 10.21045/2071-5021-2024-70-5S-7

7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).
8. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).
9. Постановление Правительства РФ от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)». URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).
10. Максимова Е.А. Модели и методы оценки информационной безопасности субъекта критической информационной инфраструктуры при деструктивных воздействиях инфраструктурного генеза: дис. ... д-ра техн. наук. Санкт-Петербург, 2023. 448 с.
11. Influence of Human Factors on Cyber Security within Healthcare Organizations: A Systematic Review / S. Nifakos, K. Chandramouli, C.K. Nikolaou [et al.] // Sensors. 2021. No. 21. P. 1–25. DOI: 10.3390/s21155119
12. What happens to rural hospitals during a ransomware attack? Evidence from Medicare data / Hannah T. Neprash, Claire C. McGlave, Katie Rydberg, Carrie Henning-Smith // The Journal of Rural Health. 2024. I. 4. P. 728–737. DOI: 10.1111/jrh.12834
13. Зона заражения: киберпреступники стали чаще атаковать больницы. URL: <https://iz.ru/1734712/dmitrii-bulgakov/zona-zarazheniia-kiberprestupniki-stali-chashche-atakovat-bolnitsy> (дата обращения: 14.04.2025).
14. Тревожный сигнал. URL: <https://www.connect-wit.ru/trevozhnyj-signal.html> (дата обращения: 14.04.2025).
15. Письмо Министерства здравоохранения РФ от 04.06.2022 № 18-4/И/2-9129 «О повышении устойчивости и безопасности функционирования информационных ресурсов Российской Федерации». URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).
16. Гавришев А.А. Исследование отдельных вопросов управления кадрами по информационной безопасности в медицинских учреждениях // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2024. № 1. С. 31–41. DOI: 10.17586/2310-1172-2024-17-1-31-41
17. Гавришев А.А. Состояние рынка труда в сегменте управленческих кадров по информационной безопасности учреждений здравоохранения // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. 2025. № 1. С. 123–133. DOI: 10.17586/2310-1172-2025-18-1-123-133
18. Бибарсова Г.Ш. Правовое обеспечение информационных технологий. Ставрополь: Изд-во СГПИ, 2010. 100 с.
19. Квалификационный справочник должностей руководителей, специалистов и других служащих (утв. Постановлением Минтруда России от 21.08.1998 № 37). URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).
20. Приказ Минздравсоцразвития РФ от 22.04.2009 № 205 «Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"». URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).

21. Приказ Минздрава РФ от 09.06.2003 № 230 «Об утверждении штатных нормативов служащих и рабочих государственных и муниципальных учреждений здравоохранения и служащих централизованных бухгалтерий при государственных и муниципальных учреждениях здравоохранения». URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).
22. Методические рекомендации по формированию службы информационных технологий в медицинских организациях (утв. ФГБУ «ЦНИИОИЗ» Минздрава России 04.03.2022). URL: <http://www.consultant.ru/> (дата обращения: 14.04.2025).

## References

1. Deming W.E. *New Economy*. Moscow: Eksmo; 2006. 208 p.
2. Kapger I.V., Shaburov A.S. *Information security management*. Perm: Perm National Research Polytechnic University Publishing House; 2023. 91 p.
3. Mazein A.V. *Legal regulation of management activities*. Moscow: Yurayt; 2025. 189 p.
4. Mikhailova Yu.V., Miroshnikova Yu.V., Knyazev A.A. Leading personnel of health authorities and institutions (sociological research). *Bulletin of Roszdravnadzor*. 2014; (6): 71–77.
5. Naigovzina N.B., Son I.M., Zimina E.V. Approaches to assessing the number of health care management personnel. *Modern problems of health care and medical statistics*. 2022; (4): 537–558. DOI: 10.24412/2312-2935-2022-4-537-558
6. Model of competencies of the head in the field of health protection / O.V. Kungurtsev, D.S. Tyufilin, O.B. Pavlenko [et al.]. *Social aspects of public health*. 2024; (S5): 1–8. DOI: 10.21045/2071-5021-2024-70-5S-7
7. Federal Law of 26.07.2017 No. 187-FZ "On the Security of the Critical Information Infrastructure of the Russian Federation". URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
8. Decree of the President of the Russian Federation of 01.05.2022 No. 250 "On additional measures to ensure information security of the Russian Federation". URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
9. Decree of the Government of the Russian Federation of 15.07.2022 No. 1272 "On approval of the standard regulation on the deputy head of the body (organization) responsible for ensuring information security in the body (organization), and the standard regulation on the structural unit in the body (organization) ensuring information security of the body (organization)". URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
10. Maksimova E.A. *Models and methods for assessing the information security of a subject of critical information infrastructure under destructive impacts of infrastructure genesis: dis. ... Dr. Tech. sciences*. St. Petersburg; 2023. 448 p.
11. Influence of Human Factors on Cyber Security within Healthcare Organizations: A Systematic Review / S. Nifakos, K. Chandramouli, C.K. Nikolaou [et al.]. *Sensors*. 2021; (21): 1–25. DOI: 10.3390/s21155119
12. What happens to rural hospitals during a ransomware attack? Evidence from Medicare data / Hannah T. Neprash, Claire C. McGlave, Katie Rydberg, Carrie Henning-Smith. *The Journal of Rural Health*. 2024; (I. 4): 728–737. DOI: 10.1111/jrh.12834
13. Zone of infection: cybercriminals began to attack hospitals more often. URL: <https://iz.ru/1734712/dmitrii-bulgakov/zona-zarazheniia-kiberprestupniki-stali-chashche-atakovat-bolnitcy> (accessed date: 14.04.2025).
14. Alarm signal. URL: <https://www.connect-wit.ru/trevozhnyj-signal.html> (accessed date: 14.04.2025).

15. Letter of the Ministry of Health of the Russian Federation of 04.06.2022 No. 18-4/I/2-9129 "On increasing the stability and safety of the functioning of information resources of the Russian Federation". URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
16. Gavrishev A.A. Study of certain issues of personnel management on information security in medical institutions. *Scientific Journal NRU ITMO. Series: Economics and Environmental Management*. 2024; (1): 31–41. DOI: 10.17586/2310-1172-2024-17-1-31-41
17. Gavrishev A.A. State of the labor market in the segment of management personnel on information security of healthcare institutions. *Scientific journal NRU ITMO. Series: Economics and Environmental Management*. 2025; (1): 123–133. DOI: 10.17586/2310-1172-2025-18-1-123-133
18. Bibarsova G.Sh. Legal support of information technologies. Stavropol: Publishing House SGPI; 2010. 100 p.
19. Qualification directory of positions of managers, specialists and other employees (approved by Decree of the Ministry of Labor of Russia of 21.08.1998 No. 37). URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
20. Order of the Ministry of Health and Social Development of the Russian Federation of 22.04.2009 No. 205 "On approval of the Unified Qualification Directory of Positions of Managers, Specialists and Employees, section "Qualification Characteristics of Positions of Managers and Specialists in Ensuring Information Security in Key Information Infrastructure Systems, Countering Technical Intelligence and Technical Information Protection"". URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
21. Order of the Ministry of Health of the Russian Federation of 09.06.2003 No. 230 "On approval of staff standards for employees and workers of state and municipal health care institutions and employees of centralized accounting departments at state and municipal health care institutions". URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).
22. Methodological recommendations on the formation of an information technology service in medical organizations (approved by FSBI "TsNIIOIZ" of the Ministry of Health of Russia 04.03.2022). URL: <http://www.consultant.ru/> (accessed date: 14.04.2025).

#### **Информация об авторе:**

**Гавришев Алексей Андреевич**, канд. техн. наук, доцент каф. международной информационной безопасности, ФГБОУ ВО «Московский государственный лингвистический университет», г. Москва, alexxx.2008@inbox.ru

DOI: <https://doi.org/10.63973/2949-1258/2025-3/095-105>

EDN: <https://elibrary.ru/ZIFOJG>

Дата поступления:  
15.05.2025

Одобрена после рецензирования:  
18.07.2025

Принята к публикации:  
01.08.2025