



**Компонент образовательной программы**

Образовательная программа утверждена

Решением Ученого совета

ГБУ «НИИОЗММ ДЗМ»

Протокол от 25.08.2023 г. № 2.1

с изменениями и (или) дополнениями

от 31.01.2024 г. Протокол № 1

Аннотация к рабочей программе дисциплины

**ЗАЩИТА ИНФОРМАЦИИ В МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ**

по направлению подготовки

**09.04.02 Информационные системы и технологии**

направленность (профиль): **Информационные системы и технологии в  
здравоохранении**

**(квалификация выпускника: магистр)**

Форма обучения: очная

**1. Код и наименование дисциплины (модуля):** Б1.В.Э.2.1 Защита информации в медицинской организации.

**2. Уровень высшего образования:** магистратура.

**3. Направление подготовки:** 09.04.02 Информационные системы и технологии, направленность (профиль): Информационные системы и технологии в здравоохранении.

**4. Цель изучения дисциплины (модуля):** приобретение обучающимися знаний и навыков, основных понятий в области защиты информации в медицинских учреждениях.

**5. Задачи дисциплины (модуля):**

1. Изучение принципов и способов защиты медицинской информации в медицинских организациях на разных уровнях (законодательном, аппаратном, программном, на уровне доступа);

2. Изучение несанкционированных способов и методов доступа к медицинской информации и противостояния им;

3. Изучение методов и способов защиты информации от потери и искажения.

**6. Место дисциплины (модуля) в структуре ОПОП:** дисциплины (модули), часть, формируемая участниками образовательных отношений, элективные дисциплины (модули), 2 курс обучения, 3 семестр.

**7. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):**

В результате освоения программы магистратуры у выпускника должны быть сформированы: профессиональные компетенции.

В результате освоения указанной программы магистратуры выпускник должен обладать следующими компетенциями:

**профессиональными компетенциями:**

– способен разрабатывать и управлять проектной и программной документацией в области информационных систем (ПК-2).

**8. Планируемые результаты обучения**

Магистр должен:

**знать:**

- особенности обеспечения информационной безопасности в компьютерных сетях и специфику средств защиты компьютерных сетей в медицинской организации;
- законодательство Российской Федерации в области защиты информации.

**уметь:**

- применять компьютерные технологии для решения задач обеспечения защиты информации в медицинском учреждении;
- настраивать политику безопасности современных операционных систем на основе проектной и программной документации.

**владеть:**

- методами использования компьютерных технологий для решения задач обеспечения защиты информации в медицинском учреждении;
- прикладными и инструментальными средствами создания систем информационной безопасности.

**Карта формирующих компетенций (или их частей) дисциплины  
(модуля)**

№ п/п	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемый результат обучения по дисциплине		
			Знать	Уметь	Владеть
1.	Способен разрабатывать и управлять проектной и программной документацией в области информационных систем (ПК-2)	ПК-2.1 ПК-2.2 ПК-2.3	Знать законодательство Российской Федерации в области защиты информации; нормативно-правовые основы организации информационной безопасности; стандарты и руководящие документы по защите информационных систем	Уметь разрабатывать политику информационной безопасности в медицинской организации; настраивать политику безопасности современных операционных систем на основе проектной и программной продукции	Владеть прикладными и инструментальными средствами создания систем информационной безопасности; методами использования компьютерных технологий для решения задач обеспечения защиты информации в медицинском учреждении

**9. Содержание разделов и тем.**

**Тема 1. Правовое обеспечение информационной безопасности.**

Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Правовые особенности обеспечения информационной безопасности в медицинских организациях.

## **Тема 2. Методы и способы защиты информации от потери, искажения, подлога и несанкционированного копирования.**

Модели нарушителей безопасности информации в медицинской организации. Законодательная защита информации в медицинском учреждении РФ. Мировой опыт в законодательной защите информации в медицине. Предполагаемые последствия от потери, искажения, подлога и несанкционированного копирования медицинской информации, Обзор методов и способов защиты информации от потери. Обзор методов и способов защиты информации от искажения. Обзор методов и способов защиты информации от подлога. Обзор методов и способов защиты информации от несанкционированного копирования. Особенности медицинской информации, подлежащей защите. Защита данных при обмене информацией между медицинскими организациями.

## **Тема 3. Особенности обеспечения информационной безопасности в медицинской организации на аппаратном уровне.**

Работоспособность персонального компьютера в целом, его частей и офисной техники. Безопасность информации на автоматизированном рабочем месте врача. Защита информации в медицинской организации на уровне персонального компьютера. Аппаратные средства пользователя информации в медицинском учреждении. Аппаратные средства с ЭВМ различных медицинских организаций. Требования к ЭВМ диагностической аппаратуры. Требования к ЭВМ терапевтической аппаратуры. Требования к ЭВМ хирургической аппаратуры. Информационная безопасность на сетевом уровне. Видео и аудио наблюдение, и видео и аудиорегистрация в медицинской организации.

## **Тема 4. Обеспечение информационной безопасности в медицинской организации на программном уровне.**

Системы и прикладные программы, используемые в медицинских организациях. Безопасность баз данных и СУБД в медицинских организациях. Безопасность МИС и ЕГИС. Безопасность системы поддержки принятия решений. Безопасность программного обеспечения диагностической, терапевтической, хирургической аппаратуры. Безопасность сетевого программного обеспечения. Компьютерные вирусы их разновидности и борьба с ними. Невирусное вредоносное ПО, его разновидности и борьба с ним. Безопасность информации на уровне мобильных технологий. Безопасность программных продуктов, разработанных в медицинской организации.

## **Тема 5. Обеспечение информационной безопасности на уровне информационной политики медицинской организации.**

Информационная политика медицинской организации. Обзор информации, к которой разрешён и запрещён доступ пациентам. Обзор информации, к которой разрешён и запрещён доступ докторам и их руководству. Обзор информации, к которой разрешён и запрещён доступ третьим лицам. Обзор медицинских данных разрешённых и запрещённых для публикации в средствах массовой информации. Безопасность медицинской информации на уровне интернет и социальных сетей. Биометрические устройства доступа в медицинской организации. Оценка рисков и меры по их уменьшению в медицинских организациях. Управление системой безопасности в медицинской организации. Государственная тайна, коммерческая тайна, врачебная тайна.

## **10. Учебно-методическое и информационное обеспечение дисциплины:**

### **10.1. Литература**

1. Entity Data Management Handbook 2021 / editor Sarah Underwood. - Seventh edition. - Herefordshire: A-Team Group, 2021. - 36 p.
2. Информатика и информационные технологии: учебник / М.В. Гаврилов, В.А. Климов. - 3-е изд., перераб. и доп. - М.: Юрайт, 2013. - 378 с.
3. Информационные технологии: учебник / А.А. Хлебников. - М.: Кнорус, 2016. - 465 с.
4. Кибербезопасность предприятия: учебное пособие / А.А. Грушо, Е.Е. Тимонина. - Электронные текстовые данные. - Москва: РУДН, 2023. - 78 с.
5. Криптоанализ RSA / С.Й. Ян; Пер. с англ. Ю.Р.Айдарова. - М.; Ижевск: Ижевский институт компьютерных исследований: НИЦ "Регулярная и хаотическая динамика", 2011. - 312 с.
6. Медицинская информатика: учебник / В.П. Омельченко, А.А. Демидова. - М.: ГЭОТАР-Медиа, 2016. - 528 с.
7. Медицинская информатика: учебник / Т.В. Зарубина, Б.А. Кобринский, С.С. Белоносов, Липкин Ю.Г. и др.; Под общ. ред. Т.В. Зарубиной, Б.А. Кобринского. - М.: ГЭОТАР-Медиа, 2016. - 507 с.
8. Медицинская информатика в общественном здоровье и организации здравоохранения: национальное руководство / гл. ред. Г.Э. Улумбекова, В.А. Медик. - 3-е изд.; Электронные текстовые данные. - Москва: ГЭОТАР-Медиа, 2022. - 1184 с.
9. Системный анализ в защите информации: учебное пособие для вузов / А.А. Шумский, А.А. Шелупанов. - М.: Гелиос АРВ, 2005.
10. Словарь-справочник терминов в области кибербезопасности / И.М. Воронков, А.В. Дроздов, С.В. Петров [и др.]. - М.: ООО "Сам полиграфист", 2014. - 232 с.

### **10.2. Программное обеспечение и Интернет-ресурсы**

– Microsoft Office Стандартный 2010

- Microsoft Office 2016 Professional Plus
- Научная электронная библиотека elibrary.ru
- Научная электронная библиотека УНИБЦ (НБ) РУДН library@rudn.ru
- Научная электронная библиотека <https://cyberleninka.ru/>
- Сайт Департамента здравоохранения города Москвы. Режим доступа: <https://mosgorzdrav.ru/>, свободный.
- Официальный интернет-портал правовой информации. Государственная система правовой информации. Режим доступа: <http://pravo.gov.ru/ips/>, свободный.
- Сайт Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека. Режим доступа: <https://rospotrebnadzor.ru/documents/documents.php>, свободный.
- Электронный фонд правовой и нормативно-технической документации Режим доступа: <http://docs.cntd.ru/>, свободный.
- Сайт ГБУ «НИИОЗММ ДЗМ». Режим доступа: <http://niioz.ru/>, свободный.

#### Зарубежные ресурсы:

- Реферативная база научных публикаций Web of Science <http://www.webofscience.com>
- База Scopus [scopus.com](http://scopus.com)
- Всемирная полнотекстовая база PhD диссертаций Proquest <https://www.proquest.com/>
- Международная база данных научных периодических изданий Jstore <https://www.jstor.org/>