



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

Рабочая программа дисциплины

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ 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.2.2 Информационная безопасность 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): Целью освоения дисциплины является приобретение обучающимися знаний и навыков, основных понятий в области защиты информации предприятия.

5. Задачи дисциплины (модуля):

5.1. освоение основных свойств информации, делающих ее уязвимой для злоумышленников;

5.2. ознакомление с основными видами угроз целостности, конфиденциальности и доступности информации;

5.3. изучение современного математического аппарата, применяемого при защите целостности и конфиденциальности информации;

5.4. изучение современных средств обеспечения доступности информации;

5.5. усвоение концепции совершенствования правового обеспечения информационной безопасности Российской Федерации;

5.6. выработка практических навыков экспериментального и аналитического исследования электрических цепей и электронных устройств.

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: основные типы угроз информационной безопасности и способы обнаружения и защиты от таких угроз; современные направления развития систем информационной безопасности; нормативно-правовые основы организации информационной безопасности; стандарты и руководящие документы по защите информационных систем.

уметь: идентифицировать и проводить анализ угроз информационной безопасности предприятия; настраивать политику безопасности современных операционных систем на основе проектной и программной документации

владеть: приемами идентификации и анализа угроз информационной безопасности предприятия; 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	нормативно правовые основы организации информационной безопасности; стандарты и руководящие документы по защите информационных систем.	настраивать политику безопасности современных операционных систем на основе проектной и программной документации.	прикладными и инструментальными средствами создания систем информационной безопасности.

9. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

Объем дисциплины (модуля) составляет **2** зачетные единицы, всего **72** часа, из которых **36** часов составляет контактная работа обучающегося с преподавателем (**18** часов – лекционные занятия, **18** часов - практические занятия, мероприятие промежуточной аттестации – зачет), **36** часов составляет самостоятельная работа обучающегося.

10. Форма обучения: очная.

11. Применяемые образовательные технологии для различных видов учебных занятий и для контроля освоения обучающимися запланированных результатов обучения:

В процессе реализации дисциплины применяются следующие образовательные технологии:

- лекционно-практические (учебный материал сконцентрирован в блоки и преподносится как единое целое);
- коммуникативные (обучаемый выступает в роли активного, сознательного, равноправного участника учебного процесса, развивающегося по своим возможностям);
- саморазвивающиеся (основывается на самоорганизации, самоопределении, самоутверждении обучающегося);
- компьютерные (дидактическая система подготовки и трансляции информации обучающемуся, основным средством реализации которой является компьютер).

12. Форма аттестации

Форма промежуточной аттестации по дисциплине (модулю) – зачет.

13. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и виды учебных занятий

№ п/п	Наименование разделов (тем) дисциплины, промежуточная аттестация	Всего часов	Их них:			Форма текущего контроля знаний/ промежуточной аттестации	Код компетенции	Литература для самостоятельной работы
			Лекции	Практические занятия (семинарские)	Самостоятельная работа			
1.	Понятие информации в современном научном мире, информационные концепции. Информационные революции. Основные свойства информации, делающей ее уязвимой для злоумышленников	10	3	3	4	Реферат/ Собеседование	ПК-2	1-10
2.	Понятие опасности и безопасности. Современная терминология в сфере защиты информации. Понятия персональных данных, коммерческой и государственной тайны	10	3	3	4	Тест/ Собеседование	ПК-2	1-10
3.	Уязвимость информации. Угрозы информационной безопасности закрытых	8	2	2	4	Тест/ Собеседование	ПК-2	1-10

	автоматизированных систем обработки информации							
4.	Математические методы защиты конфиденциальности и целостности информации. Основы современной абстрактной алгебры	10	2	2	6	Реферат/ Собеседование	ПК-2	1-10
5.	Основы методов средств помехоустойчивого кодирования, криптографии стеганографии	8	2	2	4	Реферат/ Собеседование	ПК-2	1-10
6.	Реализация современных средств обеспечения доступности информации в автоматизированных системах обработки информации	10	2	2	6	Реферат/ Собеседование	ПК-2	1-10
7.	Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации	16	4	4	8	Реферат/ Собеседование	ПК-2	1-10
		72	18	18	36			

14. Содержание разделов и тем.

Тема № 1: Понятие информации в современном научном мире, информационные концепции. Информационные революции. Основные свойства информации, делающей ее уязвимой для злоумышленников.

Определение термина информация в современном его понимании. Антропоцентрическая (социоориентированная), атрибутивная и функциональная концепции понятия информация, их достоинства и недостатки. Пять информационных революций в сфере коммуникаций и их влияние на развитие цивилизации. Основные свойства и особенности информации, материальные носители информации.

Тема № 2: Понятие опасности и безопасности. Современная терминология в сфере защиты информации. Понятия персональных данных, коммерческой и государственной тайны.

Угрозы информации, адекватность методов защиты уровню опасности. Открытая и закрытая информация, конфиденциальная информация, секретная информация, персональные данные физических лиц.

Тема № 3: Уязвимость информации. Угрозы информационной безопасности закрытых автоматизированных систем обработки информации.

Источники угроз информационной безопасности. Основные принципы организации работы автоматизированных систем обработки закрытой информации.

Тема № 4: Математические методы защиты конфиденциальности и целостности информации. Основы современной абстрактной алгебры.

Общие методы обеспечения защиты целостности, конфиденциальности и доступности информации. Основы современной абстрактной алгебры. Конечные группы, кольца, поля, векторные пространства. Структура конечного поля.

Тема № 5: Основы методов средств помехоустойчивого кодирования, криптографии стеганографии.

Основы компьютерной вирусологии. Основные положения теории помехоустойчивого кодирования, линейные блочные коды, циклические коды, сверточные коды. Современные симметричные и несимметричные методы шифрования. Современные подходы к стеганографии.

Тема № 6: Реализация современных средств обеспечения доступности информации в автоматизированных системах обработки информации.

Автоматизация методов работы с документами ограниченного доступа. Методы и средства идентификации, аутентификации и аудита.

Тема № 7: Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации.

Состояние правового обеспечения информационной безопасности Российской Федерации. Цели и принципы правового обеспечения информационной безопасности Российской Федерации. Основные направления совершенствования правового обеспечения информационной безопасности Российской Федерации. Реализация Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации.

15. Организация самостоятельной работы

При организации самостоятельно работы обучающимся необходимо учитывать следующие особенности взрослых людей:

- осознанное отношение к процессу своего обучения;
- потребность в самостоятельности;
- потребность в осмысленности обучения (для решения важной проблемы и достижения конкретной цели), что обеспечивает мотивацию;
- наличие жизненного опыта – важного источника обучения;
- влияние на процесс обучения профессиональных, социальных, бытовых и временных факторов.

В качестве главного признака самостоятельной деятельности рассматривается не то, что магистр работает без привлечения преподавателя, а то, что каждое действие, выполняемое обучающимся, им осознается, подчиненно цели, которую он сам поставил.

Основной смысл самостоятельной работы состоит в том, чтобы:

- мотивировать магистра к освоению учебного материала;
- повысить ответственность обучающегося за свою учебу;
- формировать у магистра системного мышления на основе самостоятельной работы.

Самостоятельная работа требует упорядочения и системной организации.

Основным видом самостоятельной работы обучающихся при освоении дисциплины является изучение литературы и интернет-ресурсов, рекомендуемых в рабочей программе дисциплины, а также, ответы на вопросы для самопроверки и подготовка в промежуточной аттестации,

При работе с литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом.

Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать.

Различаются четыре типа конспектов:

- план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения;
- текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника;
- свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом;
- тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу.

В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную

структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

16. Текущий контроль успеваемости и промежуточная аттестации

16.1. Текущий контроль успеваемости

Текущий контроль направлен на систематическую проверку качества (не менее двух раз за период освоения дисциплины) усвоения разделов (тем) дисциплины. Выбор оценочного средства для проведения текущего контроля успеваемости на усмотрение преподавателя.

Оценочные материалы для проведения текущего контроля успеваемости

Перечень тем рефератов:

Тема № 1: «Понятие информации в современном научном мире, информационные концепции. Информационные революции. Основные свойства информации, делающей ее уязвимой для злоумышленников».

1. Определение термина информация в современном его понимании.
2. Антропоцентрическая (социоориентированная), атрибутивная и функциональная концепции понятия информация, их достоинства и недостатки.
3. Пять информационных революций в сфере коммуникаций и их влияние на развитие цивилизации.
4. Основные свойства и особенности информации, материальные носители информации.

Тема № 2: «Понятие опасности и безопасности. Современная терминология в сфере защиты информации. Понятия персональных данных коммерческой и государственной тайны».

1. Угрозы информации, адекватность методов защиты уровню опасности.
2. Открытая и закрытая информация, конфиденциальная информация, секретная информация, персональные данные физических лиц.

Тема № 3: «Уязвимость информации. Угрозы информационной безопасности закрытых автоматизированных систем обработки информации».

1. Источники угроз информационной безопасности.
2. Основные принципы организации работы автоматизированных систем обработки закрытой информации.

Тема № 4: «Математические методы защиты конфиденциальности и целостности информации. Основы современной абстрактной алгебры».

1. Общие методы обеспечения защиты целостности, конфиденциальности и доступности информации
2. Основы современной абстрактной алгебры. Конечные группы, кольца, поля, векторные пространства. Структура конечного поля.

Тема № 5: «Основы методов и средств помехоустойчивого кодирования, криптографии и стеганографии».

1. Основы компьютерной вирусологии.
2. Основные положения теории помехоустойчивого кодирования, линейные блочные коды, циклические коды, сверточные коды.
3. Современные симметричные и несимметричные методы шифрования.
4. Современные подходы к стеганографии.

Тема № 6: «Реализация современных средств обеспечения доступности информации в автоматизированных системах обработки информации»

1. Автоматизация методов работы с документами ограниченного доступа
2. Методы и средства идентификации, аутентификации и аудита.

Тема № 7: «Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации»

1. Состояние правового обеспечения информационной безопасности Российской Федерации.
2. Цели и принципы правового обеспечения информационной безопасности Российской Федерации.
3. Основные направления совершенствования правового обеспечения информационной безопасности Российской Федерации.
4. Реализация Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации.

Вопросы для проведения собеседования:

1. Место информационной безопасности в обеспечении системы общественной безопасности.
2. Определение информационной безопасности.
3. Основные направления и задачи обеспечения информационной безопасности общества.
4. Основные компоненты информационной безопасности автоматизированных информационных систем.
5. Уровни реализации информационной безопасности.
6. Определение и классификация информационных ресурсов.
7. Основные виды угроз информационным ресурсам.

8. Особенности угроз конфиденциальной информации.
9. Причины возникновения каналов несанкционированного доступа к информации.
10. Классификация видов каналов несанкционированного доступа к информации.
11. Технические каналы несанкционированного доступа к информации.
12. Легальные и нелегальные методы обеспечения действия каналов утечки информации.
13. Особенности угроз автоматизированным информационным системам.
14. Классификация удаленных атак.
15. Основные направления правовой защиты информации.
16. Нормативные акты, защищающих право граждан на своевременное получение достоверной информации.
17. Объекты защиты авторских прав.
18. Сведения, составляющие государственную тайну и сведения, которые не могут относиться к государственной тайне.
19. Определение коммерческой тайны и сведения, которые не могут быть ее объектом.
20. Принципы и направления комплексного подхода к обеспечению информационной безопасности предприятия.
21. Основные положения концепции информационной безопасности предприятия.
22. Регламент обеспечения информационной безопасности предприятия.
23. Основные методы и способы работы службы безопасности предприятия по защите конфиденциальной информации.
24. Схема каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети, проанализировать степень опасности каждого канала.
25. Способы и элементы программно-технической защиты информационных ресурсов.
26. Классификация компьютерных вирусов.
27. Основные антивирусные программы.
28. Основные способы криптографического преобразования данных.
29. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
30. Виды угроз информационной безопасности Российской Федерации.
31. Роль и место информационной безопасности в общей системе национальной безопасности Российской Федерации.
32. Состояние информационной безопасности Российской Федерации.
33. Основные цели и задачи обеспечения информационной безопасности Российской Федерации.

34. Объекты информационной безопасности Российской Федерации.
35. Основные факторы, влияющие на состояние информационной безопасности Российской Федерации.
36. Оценка состояния и ключевые проблемы обеспечения информационной безопасности Российской Федерации.
37. Источники угроз информационной безопасности Российской Федерации.
38. Способы воздействия угроз на объекты информационной безопасности Российской Федерации.
39. Возможные последствия воздействия угроз информационной безопасности Российской Федерации.
40. Общие методы обеспечения информационной безопасности.
41. Базовые методы предотвращения, парирования и нейтрализации угроз информационной безопасности.
42. Особенности обеспечения информационной безопасности в различных сферах деятельности.
43. Особенности обеспечения информационной безопасности в общегосударственных информационных и телекоммуникационных системах.
44. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности.
45. Основные положения государственной политики обеспечения информационной безопасности Российской Федерации.
46. Основные положения государственной политики обеспечения информационной безопасности субъектов Российской Федерации.
47. Правовое обеспечение информационной безопасности Российской Федерации.
48. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности Российской Федерации.
49. Основные функции системы обеспечения информационной безопасности Российской Федерации.
50. Организационная структура системы информационной безопасности Российской Федерации.
51. Основные элементы организационной основы системы обеспечения информационной безопасности Российской Федерации.
52. Состояние правового обеспечения информационной безопасности Российской Федерации.
53. Цели и принципы правового обеспечения информационной безопасности Российской Федерации.
54. Основные направления совершенствования правового обеспечения информационной безопасности Российской Федерации.
55. Реализация Концепции совершенствования правового обеспечения информационной безопасности Российской Федерации.

16.2. Промежуточная аттестация

Целью промежуточной аттестации является оценка соответствия результатов освоения дисциплины планируемым результатам обучения: указанных в разделах 7 и 8 настоящей рабочей программы дисциплины.

Материалы для проведения промежуточной аттестации по дисциплине (модулю) представлен в оценочных материалах

Критерии и шкала оценивания

Критерии оценивания	Шкала оценивания	
	Не зачтено	Зачтено
Полнота знаний	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Могут быть допущены незначительные ошибки
Наличие умений	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи, выполнены все задания. Могут быть допущены незначительные ошибки.
Наличие навыков (владение опытом)	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Продемонстрированы базовые навыки при решении стандартных задач. Могут быть допущены незначительные ошибки.
Мотивация (личностное отношение)	Учебная активность и мотивация слабо выражены, готовность решать поставленные задачи качественно отсутствуют.	Проявляется учебная активность и мотивация, демонстрируется готовность выполнять поставленные задачи.
Характеристика сформированности компетенций	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач. Требуется повторное обучение.	Сформированность компетенций соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения практических (профессиональных) задач.
Уровень сформированности компетенций	Низкий.	Стандартный/высокий.

17. Ресурсное обеспечение

Материально-техническое обеспечение дисциплины:

Аудитория № 4 (для проведения лекционных, практических занятий, промежуточной аттестации)

Автоматизированное рабочее место (монитор, системный блок, клавиатура, компьютерная мышь) с доступом в Интернет – 1 шт.;

Ноутбук HP ElliteBook 840 G3 – 11 шт.;

Доска магнитно-маркерная 100x150 см лаковое покрытие Attache BlackFrame – 1 шт.;

Мультимедийный проектор Epson H311B- 1 шт.;

Экран настенный с электроприводом Digis Electra 160 - 1 шт.;

Веб-камера Logitech HD Webcam C270 со встроенным микрофоном- 1 шт.;

Точка доступа Ubiquiti UniFi AC LR – 1шт.;

Кресло складное с пюпитром СКП-1 – 20 шт.;

Стол – 2 шт.;

Кресло – 2 шт.

Аудитория № 10 (для проведения лекционных, практических занятий, промежуточной аттестации, итоговой аттестации)

Автоматизированное рабочее место (монитор, системный блок, клавиатура, компьютерная мышь) с доступом в Интернет – 15 шт.;

Доска магнитно-маркерная 100x150 см лаковое покрытие Attache BlackFrame – 1 шт.;

Мультимедийный проектор Mitsubishi XD550U - 1 шт.;

Веб-камера Logitech HD Webcam C270 со встроенным микрофоном- 1 шт.;

Точка доступа Ubiquiti UniFi AC LR – 1шт.;

Экран настенный с электроприводом Digis Electra 160 - 1 шт.;

Стул – 16 шт.;

Кресло – 1 шт.;

Стол – 13 шт.

Аудитория № 8 (для самостоятельной работы)

Автоматизированное рабочее место (монитор, системный блок, клавиатура, компьютерная мышь) с доступом в Интернет – 4 шт.;

Веб-камера Logitech HD Webcam C270 со встроенным микрофоном- 4 шт.;

Точка доступа Ubiquiti UniFi AC LR – 1шт.;

Стул – 6 шт.;

Стол – 6 шт.

18. Учебно-методическое и информационное обеспечение дисциплины:

18.1. Литература

1. Информатика и информационные технологии : учебник / М.В. Гаврилов, В.А. Климов. - 3-е изд., перераб. и доп. - М. : Юрайт, 2013. - 378 с.

2. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД : учебное пособие / А.В. Астахова. - Электронные текстовые данные. - Санкт-Петербург : Троицкий мост, 2014. - 214 с.
3. Информационные системы и технологии управления : учебник для вузов / Под ред. Г.А.Титоренко. - 3-е изд., перераб. и доп. - М. : Юнити-Дана, 2011, 2014. - 591 с.
4. Информационные технологии : учебник / А.А. Хлебников. - М. : Кнорус, 2016. - 465 с.
5. Информационные технологии в документационном обеспечении управления и архивном деле : учебник / Н.Н. Куняев, Т.В. Кондрашова, Е.В. Терентьева, А.Г. Фабричных ; Под общ. ред. Н.Н. Куняева. - Электронные текстовые данные. - М. : Университетская книга, 2016. - 408 с.
6. Кибербезопасность предприятия : учебное пособие / А.А. Грушо, Е.Е. Тимонина. - Электронные текстовые данные. - Москва : РУДН, 2023. - 78 с.
7. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н.Н. Куняев, Т.В. Кондрашова, А.Г. Фабричных ; Под общ. ред. Н.Н.Куняева. - 2-е изд., перераб. и доп. ; Электронные текстовые данные. - М. : Университетская книга, 2016. - 500 с.
8. 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.
9. 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. Современные концепции управления инфокоммуникациями : учебно-методический комплекс / К.Е. Самуйлов, Д.С. Кулябов. - Электронные текстовые данные. - М. : РУДН, 2013. - 234 с.

18.2. 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
- Всемирная полнотекстовая база PhD диссертаций Proquest <https://www.proquest.com/>
- Международная база данных научных периодических изданий Jstore <https://www.jstor.org/>