

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»**

Институт экономики, математики и информационных технологий

Школа IT-менеджмента

(наименование структурного подразделения (института/факультета/филиала))

Системы управления бизнес-процессами

(наименование кафедры)

УТВЕРЖДЕНА

ученым советом

Института ЭМИТ

Протокол от «9» сентября 2020 г.

№ 1-20/21

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.10 Комплексное обеспечение безопасности
автоматизированных систем

(индекс, наименование дисциплины, в соответствии с учебным планом)

КОБАС

краткое наименование дисциплины (при наличии)

38.04.02, Менеджмент

(код, наименование направления подготовки (специальности))

Информационный менеджмент

(направленность(и) (профиль (и)/специализация(ии))

магистр

(квалификация)

очно-заочная, заочная

(форма(ы) обучения)

Год набора - 2021

Москва, 2021 г.

Автор(ы)–составитель(и):

к.т.н., доцент, старший преподаватель
кафедры Системы управления
бизнес-процессами

М.М.Котухов

Заведующий кафедрой
Системы управления бизнес-процессами

д.т.н., профессор Рыжов А.П.

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем и место дисциплины в структуре образовательной программы
3. Содержание и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине
5. Методические указания для обучающихся по освоению дисциплины
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине
 - 6.1. Основная литература
 - 6.2. Дополнительная литература
 - 6.3. Учебно-методическое обеспечение самостоятельной работы
 - 6.4. Нормативные правовые документы
 - 6.5. Интернет-ресурсы
 - 6.6. Иные источники
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина Б1.В.10 Комплексное обеспечение безопасности автоматизированных систем обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКс-6	Способность управлять персоналом, обслуживающим ресурсы и осуществляющим предоставление сервисов ИТ	3 этап (код этапа – ПКс-6.2)	Контроль работы персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ
ПКс-7	Способность управлять информационной безопасностью ресурсов ИТ и непрерывностью сервисов ИТ	2 этап (код этапа – ПКс-7.1)	Организация процесса управления информационной безопасностью

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
Контроль работы персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ Контроль работы персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ	3 этап (код этапа – ПКс-6.2)	на уровне знаний: Принципы и методики управления персоналом, Принципы управления персоналом ИТ, Принципы эффективных коммуникаций, Профессиональные стандарты ИТ, Кадровый документооборот, Особенности управления персоналом ИТ
		на уровне умений: Мотивировать, обучать персонал и создавать условия для его развития, Управлять персоналом ИТ, Организовывать разработку и внедрение политик, регламентов, положений, должностных инструкций, Управлять персоналом, в том числе осуществлять прием на работу и увольнение работников
		на уровне навыков: Формирование целей, приоритетов, обязанностей и полномочий персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ, Формирование и внедрение организационной и функциональной структур персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ, Построение

		<p>эффективных коммуникаций между персоналом, осуществляющим предоставление сервисов ИТ и обслуживающим ресурсы ИТ с заинтересованными лицами, Организация и мотивация персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ для выполнения поставленных целей, Прием на работу и увольнение персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ, Контроль персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ, достижения им поставленных целей и выполнения задач, в том числе проведение аттестации персонала, Обучение и реализация мер по профессиональному развитию персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ</p>
Организация процесса управления информационной безопасностью	2 этап (код этапа – ПКС-7.1)	<p>на уровне знаний: Стандарты информационной безопасности, Методики управления процессом информационной безопасности, Методики управления рисками, Стандарты и методики обеспечения непрерывности бизнеса, Методики управления проектами и процессами ИТ</p>
		<p>на уровне умений: Выявлять требования и потребности в области информационной безопасности, Управлять процессами, оценивать и контролировать качество процесса управления информационной безопасностью, Оптимизировать процесс управления информационной безопасностью, Управлять рисками ИТ, Управлять непрерывностью бизнеса, Управлять процессами и проектами ИТ</p>
		<p>на уровне навыков: Формирование и согласование с заинтересованными лицами целей, требований и приоритетов управления, информационной безопасностью ресурсов ИТ и обеспечения непрерывности сервисов ИТ, Организация процесса управления информационной безопасностью ресурсов ИТ и обеспечения непрерывности сервисов ИТ,, вовлечение и привлечение необходимых ресурсов, Согласование (отклонение) ключевых решений по информационной безопасности ресурсов ИТ и обеспечению непрерывности сервисов ИТ, Контроль изменений процесса управления информационной безопасностью ресурсов ИТ и обеспечения непрерывности сервисов ИТ, Формирование системы оценки процесса управления информационной безопасностью ресурсов ИТ и обеспечения непрерывности</p>

		сервисов ИТ, оценка процесса и выполнение управленческих действий по результатам оценки
--	--	---

2. Объем и место дисциплины в структуре ОП ВО

Дисциплина «Комплексное обеспечение безопасности автоматизированных систем» относится к блоку Б1.В «Дисциплины(модули). Вариативная часть. Обязательные дисциплины». Код дисциплины Б1.В.10 Дисциплина изучается на 2 курсе, в 3 семестре. Общая трудоемкость дисциплины 108 (33Е).

Содержание курса является логическим продолжением и развитием дисциплин:

Управление требованиями

Количество академических часов, выделяемых на контактную работу с преподавателем составляет 32 часа, из них 16 – на лекционные занятия, 16 – на практические занятия, на самостоятельную работу обучающихся отводится 76 часов.

Формой промежуточной аттестации в соответствии с учебным планом является зачет с оценкой.

3. Содержание и структура дисциплины

Очно-заочная форма обучения

п/п	№	Наименование тем и/или разделов	Объем дисциплины, час.					Форма текущего контроля успеваемости**, промежуточной аттестации***	
			Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий					СР
				Л/ЭО, ДОТ*	ЛР/ ЭО, ДОТ*	ПЗ/ ЭО, ДОТ*	КС Р		
Тема 1		Нормативно-правовые основы менеджмента информационной безопасности	36	6		5		25	О, Т
Тема 2		Основы криптологии	36	5		5		26	О, Т
Тема 3		Практические вопросы менеджмента информационной безопасности	36	5		6		25	О, Т
Промежуточная аттестация									Зачет с оценкой
Всего:			108	16		16		40	

Примечание:

* – при применении электронного обучения, дистанционных образовательных технологий в соответствии с учебным планом;

** – формы текущего контроля успеваемости: опрос (О), тест (Т)

Содержание дисциплины

Тема 1. Нормативно-правовые основы менеджмента информационной безопасности

Содержание проблемы менеджмента информационной безопасности, Законодательные и нормативные основы обеспечения информационной безопасности на государственном уровне и в негосударственных структурах, Государственная система технического регулирования, система национальных и международных стандартов в

области информационной безопасности, Система лицензирования и сертификации в области защиты информации

Тема 2. Основы криптологии

Криптографические методы и средства защиты информации, Основы практического применения криптографических методов, Понятие криптоанализа

Тема 3. Практические вопросы менеджмента информационной безопасности

Методические основы построения системы информационной безопасности, Методика проведения аудита информационной безопасности и анализа рисков

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости обучающихся и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.10 Комплексное обеспечение безопасности автоматизированных систем используются следующие методы текущего контроля успеваемости обучающихся:

- при проведении занятий лекционного типа: опрос
- при проведении занятий практического типа: тест

4.1.2. Зачет с оценкой проводится с применением следующих методов (средств):

Устный: ответить на вопросы

4.2. Материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы для подготовки к опросу:

1. Основные понятия и определения. Современное состояние проблемы обеспечения информационной безопасности и направления ее решения. Понятие информационной безопасности корпоративной информационно-вычислительной сети. Типовые угрозы, уязвимости и атаки.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации», основные положения и требования
3. Другие законодательные акты и их взаимосвязь
4. Руководящие документы ФСТЭК России (Гостехкомиссии России)
5. Руководящие документы ФСБ России (ФАПСИ)
6. Лицензирование деятельности в области защиты информации
7. Закон «О техническом регулировании»
8. Система технических регламентов и национальных стандартов в области защиты информации
9. Взаимосвязь международных и национальных стандартов
10. ГОСТ Р ИСО/МЭК 15408-2002
11. Профили защиты информации
12. Лицензирование деятельности в области защиты информации. Виды лицензируемой деятельности. Органы по лицензированию.
13. Сертификация средств защиты информации. Виды сертификатов
14. Симметричная криптография
15. Криптография с открытым ключом и ЭЦП
16. Особенности применения криптографических средств защиты информации.
17. Основные ошибки при применении криптографических средств защиты информации.
18. Принципы построения системы информационной безопасности
19. Разработка политики информационной безопасности
20. Выбор мер и средств защиты информации
21. Разработка регламентирующих документов
22. Проблемные вопросы и практические рекомендации

23. Основные нормативные и методические документы по проведению аудита состояния информационной безопасности
24. Международный стандарт ISO 17799-2000 (BS 7799)
25. Методика проведения аудита
26. Сбор и анализ информации
27. Анализ рисков
28. Выработка рекомендаций
29. Рекомендации по выбору аудитора

Типовые тестовые задания:

1. Какие грифы секретности разрешено использовать для носителей сведений, составляющих гос. тайну?
 - ☐ - Особой важности
 - ☐ - Совершенно секретно
 - ☐ - Секретно
 - ☐ - Для служебного пользования
 - ☐ - Конфиденциально
2. Разрешено ли использование грифов секретности для документов, содержащих сведения, не отнесенные к гос. тайне?
 - ☐ - Да
 - ☐ - Нет
3. Кто уполномочен выдавать лицензии на работу со сведениями, составляющими гос. тайну?
 - ☐ - УФСБ России по тер. округу
 - ☐ - ЦЛСЗГТ ФСБ России
 - ☐ - ФСТЭК России
4. Кто определяет режим защиты конфиденциальной информации?
 - ☐ - Уполномоченный гос. орган
 - ☐ - Собственник информации
5. Требуется ли обязательная сертификация средств обработки и защиты документированной информации с ограниченным доступом не составляющей гос. тайну?
 - ☐ - Да
 - ☐ - Нет
6. Сколько определено уровней возможностей нарушителей, имеющих доступ к работе с АС и СВТ?
 - ☐ - Три
 - ☐ - Четыре
 - ☐ - Пять
7. Сколько определено классов защищенности средств вычислительной техники?
 - ☐ - Пять
 - ☐ - Шесть
 - ☐ - Семь
8. Сколько определено классов защищенности автоматизированных систем?
 - ☐ - Шесть
 - ☐ - Семь
 - ☐ - Восемь
 - ☐ - Девять
9. Сколько определено классов защищенности межсетевых экранов?

- ☐ - Пять
 - ☐ - Шесть
10. Сколько определено уровней контроля отсутствия недеklarированных возможностей программных средств ?
- ☐ - Четыре
 - ☐ - Пять
 - ☐ - Шесть
 - ☐ - Семь
11. Сколько определено оценочных уровней доверия в соответствии с ГОСТ Р ИСО/МЭК 15408-2002?
- ☐ - Четыре
 - ☐ - Пять
 - ☐ - Шесть
 - ☐ - Семь
12. Могут ли применяться межсетевые экраны между АС классов 1Д – 1А?
- ☐ - Да
 - ☐ - Нет
13. Возможна ли связь АС классов 1Д – 1А с сетью Интернет при обработке защищаемой в соответствии с законом информации?
- ☐ - Да
 - ☐ - Нет
 - ☐ - Да, но при выполнении требований Указа от 17.03.2008 № 351
14. Какую лицензию надо получить для выполнения работ по защите конфиденциальной информации в АС, не использующих средств шифрования?
- ☐ - Лицензию ФСБ России
 - ☐ - Лицензию ЦЛСЗГТ ФСБ России
 - ☐ - Лицензию ФСТЭК России
15. Какую лицензию надо получить для выполнения работ по разработке средств защиты конфиденциальной информации с использованием средств шифрования?
- ☐ - Лицензию ФСБ России
 - ☐ - Лицензию ЦЛСЗГТ ФСБ России
 - ☐ - Лицензию ФСТЭК России
16. Является ли обязательным использование сертифицированных средств защиты конфиденциальной информации, отнесенной к охраняемой законом информации?
- ☐ - Да
 - ☐ - Нет
17. Сертифицируются ли СЗИ, созданные организациями, не имеющими лицензий?
- ☐ - Да
 - ☐ - Нет
18. Является ли обязательным одобрение ФСБ России алгоритма криптозащиты до его реализации?
- ☐ - Да
 - ☐ - Нет
19. Могут ли приниматься на сертификацию импортные средства защиты информации, не использующие встроенные шифровальные алгоритмы и средства?
- ☐ - Да
 - ☐ - Да, от имени отечественных компаний
 - ☐ - Нет

20. Могут ли приниматься на сертификацию импортные шифровальные алгоритмы и средства?

- ☐ - Да
- ☐ - Да, от имени отечественных компаний
- ☐ - Нет

21. Укажите алгоритмы шифрования, использующие методы шифрования с секретным ключом.

- ☐ - DES
- ☐ - Triple DES
- ☐ - IDEA
- ☐ - RSA
- ☐ - El Gamal
- ☐ - PGP
- ☐ - ГОСТ 28147-89

22. Укажите алгоритмы шифрования, использующие методы шифрования с открытым ключом.

- ☐ - DES
- ☐ - Triple DES
- ☐ - IDEA
- ☐ - RSA
- ☐ - El Gamal
- ☐ - PGP
- ☐ - ГОСТ 28147-89

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКс-6	Способность управлять персоналом, обслуживающим ресурсы и осуществляющим предоставление сервисов ИТ	3 этап (код этапа – ПКс-6.2)	Контроль работы персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ
ПКс-7	Способность управлять информационной безопасностью ресурсов ИТ и непрерывностью сервисов ИТ	1 этап (код этапа – ПКс-7.1)	Организация процесса управления информационной безопасностью

Этап освоения компетенции	Показатель оценивания	Критерий оценивания
ПКС-6.2. Контроль работы персонала, осуществляющего предоставление сервисов ИТ и обслуживающего ресурсы ИТ	Управлять деятельностью системы, гарантирующей информационную безопасность, пресекать утечки информации, организовывать мероприятия по повышению грамотности сотрудников в области безопасности	Обеспечена безопасность информации, установлены каналы утечки информации, приняты меры по пресечению утечки информации.
ПКС-7.1. Организация процесса управления информационной безопасностью	Формировать цели и требования, расставлять приоритеты в управлении информационной безопасностью	Сформированы цели, требования и приоритеты управления информационной безопасностью.

4.3.2 Типовые оценочные средства

Список вопросов для подготовки к зачету с оценкой:

1. Аутентификация пользователей как защита информации
2. Аутентификация пользователей как системы защиты информации.
3. Дайте описание журналу аудита. Для чего он нужен
4. Информационная безопасность человека и общества
5. Информационная безопасность человека и общества.
6. Какие вирусы вы знаете, опишите их классификацию
7. Какие криптосистемы вы знаете
8. Какие криптосистемы вы знаете?
9. Какие устройства идентификации и аутентификации вы знаете?
10. Классы вирусов.
11. Компьютерные преступления. Основные технологии, используемые при совершении компьютерных преступлений.
12. Криптография. Асимметричные криптосистемы
13. Криптография. Симметричные криптосистемы.
14. Криптосистемы и их классификация.
15. Методы и средства защиты информации
16. Методы и средства защиты информации. Содержание способов и средств обеспечения безопасности информации.
17. Несанкционированный доступ к системе и информации?
18. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна
19. Объекты защиты информации. Защита информации ограниченного доступа: государственная тайна, коммерческая тайна
20. Опишите асимметричную систему шифрования
21. Опишите асимметричные системы криптографии
22. Опишите классификацию атак на систему

23. Опишите классификацию атак на систему
24. Опишите логическую бомбу и для чего она внедряется в вирусы?
25. Основные алгоритмы шифрования данных: DES
26. Основные алгоритмы шифрования данных: DES.
27. Основные каналы утечки информации.
28. Основные каналы утечки информации. Защита от утечки информации по техническим каналам
29. Отличие защиты информации в локальных сетях от глобальных сетях
30. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей»
31. Понятие угрозы. Анализ угроз информационной безопасности. Виды «нарушителей».
32. Расскажите про классификацию атак
33. Реализация методов и средств защиты информации.
34. Средства опознавания и разграничения доступа к информации.
35. Чем отличается симметричная и асимметричная криптосистема
36. Что такое аутентификация и идентификация пользователей
37. Что такое информация
38. Что такое открытый ключ в криптографии?
39. Электронно-цифровая подпись
40. Электронно-цифровая подпись.

Шкала оценивания.

Оценка «отлично» выставляется, если студент показал глубокое полное знание и усвоение материала учебной дисциплины, его взаимосвязи с другими дисциплинами и с предстоящей профессиональной деятельностью, усвоение основной литературы, и знание дополнительной литературы, способность к самостоятельному пополнению и обновлению знаний.

Оценки «хорошо» заслуживает студент, показавший полное знание основного материала учебной дисциплины, знание основной литературы и знакомство с дополнительной литературой, способность к пополнению и обновлению знаний.

Оценки «удовлетворительно» заслуживает студент, показавший при ответе на экзамене знание основных положений учебной дисциплины, допустивший отдельные погрешности и сумевший устранить их с помощью экзаменатора, знакомый с основной литературой.

Оценка «неудовлетворительно» выставляется, если при ответе выявились существенные пробелы в знаниях студента основных положений учебной дисциплины, неумение даже с помощью экзаменатора сформулировать правильные ответы на вопросы.

4.4. Методические материалы

В части обеспечения освоения дисциплины обучающимся предоставляется раздаточный материал по темам дисциплины.

Процедура оценивания знаний, умений и навыков, обеспечивающих формирование компетенций, предусмотренных освоением дисциплины, включает:

- проведение опроса по ключевым вопросам, охватывающему содержание дисциплины.

5. Методические указания для обучающихся по освоению дисциплины

Примерный перечень тем для самостоятельной работы:

1. Законодательное и нормативное правовое обеспечение ИБ
2. Основы криптологии
3. Лицензирование и сертификация в области ИБ

4. Практические вопросы построения СУИБ
5. Основные национальные и международные стандарты в области ИБ
6. Особенности защиты персональных данных

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература.

1. Котухов М.М. Цикл лекций по курсу «Комплексное обеспечение информационной безопасности автоматизированных систем». Учебное пособие. Лекции 1 – 6. – М.: Изд. АНХ, 2009. – 346 с., (электронный вариант).
2. Котухов М.М. Методические основы построения системы защиты информации компьютерной сети. – М.: ИПКИР, 2011. – 158 с., (электронный вариант).
3. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей /Е.А.Карпов, И.В.Котенко, М.М.Котухов, А.С.Марков. – СПб.: Изд. ВАС, 2010. – 190 с., (электронный вариант).

6.2. Дополнительная литература.

1. Котухов М.М. Методическое пособие по разработке Концепции информационной безопасности организации. - М.: Изд. АНХ, 2010. – 57 с., (электронный вариант).
2. Котухов М.М. Методическое пособие по проведению аудита информационной безопасности организации. - М.: Изд. АНХ, 2009. – 45 с., (электронный вариант).

6.3. Учебно-методическое обеспечение самостоятельной работы.

1. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.
2. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.
3. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФО-РУМ, НИЦ ИНФРА-М, 2013. - 416 с.

6.4. Нормативные правовые документы.

1. Комплект законодательных, нормативных правовых и методических документов по защите конфиденциальной информации и персональных данных («Консультант-Плюс»)

6.5. Интернет-ресурсы.

1. Сайты ФСТЭК России, ФСБ России, Роскомнадзора.

6.6. Иные источники.

1. Система Гарант <http://www.garant.ru/>
2. Консультант Плюс <http://www.consultant.ru/>

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для проведения занятий по дисциплине необходимо материально-техническое обеспечение учебных аудиторий (наглядными материалами, экраном, мультимедийным проектором с ноутбуками (ПК) для презентации учебного материала, выходом в сеть Интернет, программными продуктами Microsoft Office (Excel, Word, PowerPoint)) в

зависимости от типа занятий: семинарского и лекционного типов, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Для самостоятельной работы обучающимся необходим доступ в читальные залы библиотеки и/или помещение, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет», доступ в электронную информационно-образовательную среду организации и ЭБС.

Информационные справочные системы:

1. Информационно-правовой портал «Консультант плюс» (правовая база данных). [Электронный ресурс]. – URL: <http://www.consultant.ru/>
2. Информационно-правовой портал «Гарант» (правовая база данных). [Электронный ресурс]. – URL: <http://www.garant.ru/>
3. Научная библиотека РАНХиГС. URL: <http://lib.ranepa.ru/>;
4. Научная электронная библиотека eLibrary.ru. URL: <http://elibrary.ru/defaultx.asp>;
5. Национальная электронная библиотека. URL: <http://rusneb.ru>;
6. Российская государственная библиотека. URL: www.rsl.ru;
7. Российская национальная библиотека. URL: <http://nlr.ru/>;
8. Электронная библиотека Grebennikon. URL: <http://grebennikon.ru/>;
9. Электронно-библиотечная система Издательства «Лань». URL: <http://e.lanbook.com>;
10. Электронно-библиотечная система ЮРАЙТ. URL: <http://www.biblio-online.ru/>;
11. Электронно-библиотечная система IPRbooks. URL: <http://www.iprbookshop.ru/>.