Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»

Факультет компьютерных технологий и прикладной
математики Кафедра вычислительных технологий

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор

_____ Иванов А.Г.
подпись

«_29_» ____мая_____ 2015 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.В.07 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Направление
подготовки/специальность_02.03.02 **Фундаментальная информатика и ___ информационные технологии**_____
(код и наименование направления подготовки/специальности)

Направленность (профиль) /
специализация__Вычислительные технологии_____
(наименование направленности (профиля) специализации)

Программа подготовки _академический бакалавриат_____
(академическая /прикладная)

Форма обучения ___очная_____
(очная, очно-заочная, заочная)

Квалификация (степень) выпускника ____бакалавр_____
(бакалавр, магистр, специалист)

Краснодар 2015

Рабочая программа дисциплины Б1.В.07 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 02.03.02 Фундаментальная информатика и информационные технологии

Программу составил(а):

Жуков Сергей Александрович, доцент, к. ф.-м. н., доцент — подпись
Ф.И.О., должность, ученая степень, ученое звание

Рабочая программа дисциплины Б1.В.07 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» утверждена на заседании кафедры Вычислительных Технологий
протокол № 9 «20 » апреля 2015 г.

Заведующий кафедрой (разработчика) Миков А. И. _____
фамилия, инициалы — подпись

Рабочая программа обсуждена на заседании кафедры
Вычислительных Технологий протокол № 9 «20» апреля 2015 г.

Заведующий кафедрой (выпускающей)___ Миков А. И
фамилия, инициалы

Утверждена на заседании учебно-методической комиссии факультета Компьютерных Технологий и Прикладной Математики протокол № 5 от «29» апреля 2015 г.

Председатель УМК факультета К.В. Малыхин

Рецензенты:

Гаркуша О.В., доцент кафедры информационных технологий ФБГОУ ВО «Кубанский государственный университет», кандидат физико-математических наук.

Зайков В.П. Ректор НЧОУ ВО «Кубанский институт информзащиты» д.экон. наук, к.т.н., доцент.

1. Цели и задачи освоения дисциплины

1.1 Цель освоения дисциплины

Целью преподавания и изучения дисциплины «Информационная безопасность» является формирование у студентов способности оценивать угрозы информационной безопасности и разрабатывать архитектурные и функциональные спецификации создаваемых систем и средств по ее защите, а также разрабатывать методы реализации и тестирования таких систем.

1.2 Задачи дисциплины

Студент должен знать основные понятия, методы, алгоритмы и технологии защиты информации; уметь применять теории и методы по обеспечению информационной безопасности; владеть технологиями реализации систем такой защиты.

1.3 Место дисциплины в образовательной программе

Дисциплина «Информационная безопасность» относится к вариативной части дисциплин блока Б1.

Для изучения дисциплины необходимо знание дисциплин “Дискретная математика”, “Алгебраические структуры”, “Основы программирования”, “Теория алгоритмов и вычислительных процессов”, “Операционные системы”, “Компьютерные сети”. Знания, получаемые при изучении основ защиты информации, используются при изучении таких дисциплин профессионального цикла учебного плана бакалавра как “Программирование в компьютерных сетях”, “Программирование для мобильных платформ”, а также при работе над выпускной работой.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих **профессиональных компетенций:**

№ п.п.	Индекс компе-тенции	Содержание компетенции (или ее части)	В результате изучения учебной дисциплины обучающие должны		
			знать	уметь	владеть
1.	ОПК-4	Способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применение информационно-коммуникационных технологий и с учётом основных требований информационной безопасности	Фундаментальные концепции и системные методологии, международные и профессиональные стандарты в области информационных технологий	Использовать углубленные теоретические и практические знания в области информационных технологий и прикладной математики, фундаментальные концепции и системные методологии	Методами получения углубленных теоретических и практических знаний в области информационных технологий и прикладной математики,

	ПК-6	Способностью эффективно применять базовые математические знания и информационные технологии при решении проектно-технических и прикладных задач, связанных с развитием и использованием информационных технологий	Знания, которые находятся на передовом рубеже данной науки, корпоративную техническую политику развития корпоративной инфраструктуры информационных технологий на принципах открытых систем	Применять базовые математические знания и информацион-ные технологии при решении проектно-технических и прикладных задач, разрабатывать корпоративную техническую политику развития корпоративной инфраструктуры информационных технологий на принципах открытых систем	Базовыми математическим и знаниями и информацион-ными технологиями, которые находятся на передовом рубеже данной науки, методами разработки корпоративной инфраструктуры информационных технологий, основаных на принципах открытых систем

2. Структура и содержание дисциплины

2.1 Распределение трудоѐмкости дисциплины по видам работ

Общая трудоѐмкость дисциплины составляет 7 зач.ед. (252 часа), их распределение по видам работ представлено в таблице.

Вид учебной работы	Всего часов	Семестры (часы)	
		5	6
Аудиторные занятия (всего)	149	76,2	72,3
В том числе:			
Занятия лекционного типа	70	36	34
Лабораторные занятия	70	36	34
КСР	8	4	4
ИКР	0,5	0,2	0,3
Самостоятельная работа (всего)	59	31,8	27
В том числе:			
Проработка учебного (теоретического) материала	59	31,8	27
Промежуточная аттестации		зачет	экзамен
Контроль	45		44,7
Общая трудоемкость час зач. ед.	252 7	108 3	144 4

2.2 Структура дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в _5_ семестре *(очная форма)*.

№	Наименование разделов	Количество часов					
		Всего	Аудиторная работа				Внеаудиторная работа
			Л	КСР	ИКР	ЛР	СРС
1	2	3	4	5	6	7	8
1	Содержание понятия безопасность и его структура.	8	4				4
2	Проектирование алгоритмов поддержки информационной безопасности.	26				16	10
3	Стандарты информационной безопасности.	6	2			2	2
4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.	14	6	2		2	4
5	Модели управления доступом к информации.	44	20	2	0,2	14	7,8
6	Модели поддержания целостности информации	10	4			2	4
	Итого по дисциплине:	108	36	4	0,2	36	31,8

Разделы дисциплины, изучаемые в _6_ семестре *(очная форма)*.

№	Наименование разделов	Количество часов						
		Всего	Аудиторная работа				Внеаудиторная работа	
			Л	КСР	ИКР	ЛР	КОНТРОЛЬ	СРС
1	2	3	4	5	6	7	8	9
7	Аудит вычислительной системы и архивация	10	2			4		4
8	Анализ уязвимости системы. DLP-системы	12	4			4		4
9	Системы обнаружения вторжений	10	2			4		4
10	Поддержка информационной безопасности в вычислительных сетях	10	4			4		2
11	Зловредное программное обеспечение	10	4			2		4
12	Основы криптографии	16	6	2		6		2
13	Криптография с секретным ключом	14	6			4		4
14	Криптография с открытым ключом	62	6	2	0,3	6	44,7	3
	Итого по дисциплине:	144	34	4	0,3	34	44,7	27

2.3 Содержание разделов дисциплины

2.3 Содержание разделов дисциплины

2.3.1 Занятия лекционного типа

№ раздела	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1	Содержание понятия безопасность и	Виды безопасности и связи между ними. Анализ угроз информационной безопасности. Правовая поддержка организации	ЛР

	его структура	информационной безопасности. Смысл компьютерной безопасности, ее основные требования. Основные понятия актуализации компьютерной безопасности.	
2	Проектирование алгоритмов поддержки информационной безопасности	Организация вычислений на графе. Кодирующие и декодирующие преобразования. Алгоритмы защиты данных, основанные на комбинаторике и теории чисел.	ЛР
3	Стандарты информационной безопасности	Критерии безопасности компьютерных систем (Оранжевая книга). ISO/IEC 17799:2002 “Управление информационной безопасностью”. ISO 15408 “Общие критерии безопасности информационных технологий” “Common Criteria” (ОК). Российские стандарты в области информационной безопасности.	ЛР
4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации	Подходы к идентификации и аутентификации. Понятие полномочий и ролей, их виды. Реализация сценария идентификации-аутентификации-авторизации в операционных системах Windows и Unix.	ЛР
5	Модели управления доступом к информации	Монитор безопасности. Основные политики доступа. Модель HRU. Модель Белла-ЛаПадулы. Модель МакЛина. Модель Take-Grant. Модель Китайская стена.	ЛР
6	Модели поддержания целостности информации	Ролевые модели доступа. Модель Биба. Модель Кларка-Вильсона.	ЛР
7	Аудит вычислительной системы и архивация	Смысл аудита и ресурсы, необходимые для его осуществления. Способы и инструментарий для аудита в операционных системах Windows и Unix. Выполнение backup-а системы, архивация данных.	ЛР
8	Анализ уязвимости системы. DLP-системы	Классификация уязвимостей. Пример уязвимости и ее использование. Методология гипотетического дефекта. Обзор DLP-систем	ЛР
9	Системы обнаружения вторжений	Обзор моделей обнаружения вторжений. Архитектура IDS-системы. Средства детекции вторжений в операционных системах.	ЛР
10	Поддержка информационной безопасности в вычислительных сетях	Анализ стека протоколов ISO OSI с точки зрения информационной безопасности. Межсетевой экран. Технология сетей VPN. Протоколы защиты информации различных уровней. Протокол Kerberos. Инфраструктура управления открытыми ключами.	ЛР
11	Зловредное программное	Анализ различных видов вирусов. Жизненный цикл вирусов. Признаки заражения вирусом.	ЛР

	обеспечение	Методы и средства антивирусной защиты.	
12	Основы криптографии	Основные схемы шифрования. Основные факты об арифметике вычетов. Алгоритмы Евклида и Рабина.	ЛР
13	Криптография с секретным ключом	Алгоритмы шифрования методами замены, перестановки, гаммирования. Алгоритмы DES, AES. Управление ключами.	ЛР
14	Криптография с открытым ключом	Система Диффи-Хелмана. Шифр Эль-Гамаля. Алгоритм RSA. Электронная цифровая подпись. Инфраструктура открытых ключей.	ЛР

2.3.2 Занятия семинарского типа

Учебным планом не предусмотрены.

2.3.3 Лабораторные занятия

№ работы	№ раздела дисциплины	Наименование лабораторных работ
1−9	2	Проектирование алгоритмов поддержки информационной безопасности.
10	3	Стандарты информационной безопасности.
11	4	Сценарий Идентификация-Аутентификация-Авторизация и варианты реализации.
12−18	5	Модели управления доступом к информации.
19	6	Модели поддержания целостности к информации
20−21	7	Аудит вычислительной системы и архивация.
22-23	8	Анализ уязвимости системы. DLP-системы
24−25	9	Системы обнаружения вторжений
26−27	10	Поддержка информационной безопасности в вычислительных сетях
28	11	Зловредное программное обеспечение
29-31	12	Основы криптографии
32-33	13	Криптография с секретным ключом
34-36	14	Криптография с открытым ключом

2.3.4 Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрены.

2.3.5 Самостоятельное изучение разделов дисциплины

Раздел 1. Законодательные акты: О безопасности, Доктрина информационной безопасности РФ, Об охране интеллектуальной собственности, О персональных данных, Об информации, информационных технологиях и о защите информации, О государственной тайне, О международном обмене информацией.

Раздел 2. Учебники и пособия по проектированию структур данных и алгоритмов их обработки. Руководства, учебники и пособия по языку Visual C++ и работе в среде Visual Studio 2012 и выше.

Раздел 3. Международные и российские стандарты РФ по информационной безопасности: закон РФ "О техническом регулировании", "Критерии оценки доверенных компьютерных систем" (Department of Defense Trusted Computer System

Evaliation Criteria, TCSEC − Оранжевая книга), ISO/IEC 15408:1999 "Критерии оценки безопасности информационных технологий" (Evaluation criteria for IT security − ОК) , ГОСТ Р 50739, ГОСТ Р 50922-96, ГОСТ Р 51188-98, ГОСТ Р 50739-95.

Раздел 4. Руководства и учебники по администрированию в операционных системах Windows, Unix, Linux.

Раздел 5. Учебники и пособия из рекомендованного списка литературы.

Раздел 6. Руководства и учебники по администрированию в операционных системах Windows, Unix, Linux, учебные ресурсы в internet.

Раздел 7. Учебники и пособия из рекомендованного списка литературы.

Раздел 8. Учебники и пособия из рекомендованного списка литературы, а также обучающие материалы от производителей антивирусного ПО.

3. Образовательные технологии

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
5, 6	Л	Компьютерные презентации и обсуждение	70
	ЛР	Разбор конкретных ситуаций (задач) с использованием штатного ПО, выполнение тестов на знание терминологии, сведений из области информационной безопасности, программирование алгоритмов	70

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий, лабораторных работ, средств для итоговой аттестации (экзамена в 6 семестре).

Оценка успеваемости осуществляется по результатам:

- выполнения лабораторных работ;

- ответа на экзамене

4.2.1 Перечень вопросов к зачету

1. Классификация информационных угроз.
2. Основные качества защищенной информации в ИС.
3. В чем смысл политики безопасности.
4. Что такое несанкционированный доступ (НСД) и их виды.
5. Что такое уязвимость, атака, структура атаки и возможные виды атак.
6. Виды моделей доступа к данным, их характеристика.
7. Назначение стандартов информационной безопасности. Структура стандартов.
8. Что такое сниффинг, спуффинг и hijacking.
9. Что такое DOS-атака, DDOS-атака ,SYN-атака.

10. Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
11. Какого вида данные обязаны находиться в открытом доступе.
12. Назовите уровни секретности данных, которые регламентирует закон РФ “О государственной тайне”.

4.2.2 Критерии оценивания к зачету

Оценка “зачтено” - практические задания выполнены в срок в объеме не менее 80%. Студент демонстрирует правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при аргументации ответов на вопросы при защите лабораторных.

Оценка «не зачтено» - практические задания не выполнены либо предоставлены не в срок в объеме менее 60%, Студент демонстрирует наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4.2.3 Перечень вопросов к экзамену

1. Классификация информационных угроз.
2. Основные качества защищенной информации в ИС.
3. В чем смысл политики безопасности.
4. Что такое несанкционированный доступ (НСД) и их виды.
5. Что такое уязвимость, атака, структура атаки и возможные виды атак.
6. Виды моделей доступа к данным, их характеристика.
7. Назначение стандартов информационной безопасности. Структура стандартов.

8. Что такое сниффинг, спуффинг и hijacking.
9. Что такое DOS-атака, DDOS-атака ,SYN-атака.
10. Является ли алгоритмически разрешимым свойство быть безопасной системой в модели HRU.
11. Какого вида данные обязаны находиться в открытом доступе.
    Назовите уровни секретности данных, которые регламентирует закон РФ "О государственной тайне".
12. Механизм идентификации, аутентификации и авторизации в ОС Unix.
13. Механизм идентификации, аутентификации и авторизации в ОС Windows.
14. Биометрические методы аутентификации
15. Механизм одноразовых паролей
16. Протокол аутентификации Kerberos
17. Основные положения дискреционной модели полномочий HRU
18. Основные положения мандатной модели полномочий Белла-ЛаПадулы
19. Модель полномочий Мак-Лина.
20. Классификация зловредного программного обеспечения.
21. Особенности полиморфного вируса и руткита.
22. Основные положения VPN-сети.
23. Назначение методов социальной инженерии и их формы.
24. Назначение и формы аудита в ОС Windows.
25. Назначение и механизм сетевого экрана.
26. Характеристика средств информационной безопасности в рамках стека протоколов ISO OSI.
27. Структура угроз информационной безопасности.
28. Содержание основных понятий ИБ: «защищенность данных», «уязвимость», «атака», «злоумышленник» и др. Их отражение в стандартах ИБ.

4.2.4 Критерии оценивания к экзамену

Оценка «отлично»: точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «хорошо»: при ответе на один вопрос даны точные формулировки алгоритмов, теорем и правильные доказательства; точные определения математических объектов и ясные и правильные определения объектов, характеризующихся неформализованными понятиями; при ответе на второй вопрос имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «удовлетворительно»: при ответе на оба вопроса имеются неточности формулировки алгоритмов, теорем или пробелы в правильных доказательствах; недостаточно точные определения математических объектов или неясные и не совсем правильные определения объектов, характеризующихся неформализованными понятиями.

Оценка «неудовлетворительно»: отсутствует ответ хотя бы на один из вопросов или имеются существенные неточности в формулировках алгоритмов, теорем, приведены неправильные доказательства; неверные определения математических объектов и неправильные определения объектов, характеризующихся неформализованными понятиями.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

5.1 Основная литература

1. Мельников, В. П. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. – 5-е изд., стер. – М. : Академия, 2011. – 331 с. : ил. – (Высшее профессиональное образование . Информатика и вычислительная техника) (Учебное пособие). – Библиогр.: с. 327-328. – ISBN 9785769577383 : 348.70., 36 экз.
2. 2. Основы информационной безопасности [Текст] : учебное пособие для студентов вузов / В. А. Галатенко ; под ред. В. Б. Бетелина. – Изд. 4-е. – М. : Интернет-Университет Информационных Технологий : БИНОМ. Лаборатория знаний, 2008. – 205 с. – (Основы информационных технологий). – Библиогр. : с. 200-202.
3. Голиков, А.М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. - 284 с. : схем., табл., ил. - Библиогр. в кн. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480637

5.2 Дополнительная литература

1. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605.

2. Информационная безопасность [Текст] : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012. - 295 с. (10 экз.)

3. Информационная безопасность и защита информации [Текст] : учебное пособие для студентов вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 4-е изд., стер. - М. : Академия, 2009. - 331 с. : ил. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Библиогр. : с. 327-328. (10 экз.)

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Информационная безопасность / изд. В. Вараксин ; учред. и изд. компания "Гротек" - Москва : Гротек, 2014. - № 4. - 72 с.: ил. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=364894
2. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - Москва : Студенческая наука, 2012. - 1322 с. : ил.,табл., схем. - (Вузовская наука в помощь студенту). -ISBN 978-5-00046-137-2 ;Тоже [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=227774

7. Методические указания для обучающихся по освоению дисциплины (модуля)

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных работ, контрольной работы, зачета.

Важнейшим этапом курса является самостоятельная работа по дисциплине с использованием указанных литературных источников и методических указаний автора курса.

Виды и формы СР, сроки выполнения, формы контроля приведены выше в данном документе.

Для лучшего освоения дисциплины при защите ЛР студент должен ответить на несколько вопросов из лекционной части курса.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

8.1 Перечень информационных технологий

– Проверка домашних заданий и консультирование посредством электронной почты.

– Использование электронных презентаций при проведении лекций и практических занятий.

8.2 Перечень необходимого программного обеспечения

1. Microsoft Visual Studio 2012+ : Visual C++, C#
2. Oracle Virtual Box v 5.1 +
3. Python

8.3 Перечень информационных справочных систем:

1. Электронный каталог Научной библиотеки КубГУ (http://megapro.kubsu.ru/MegaPro/Web).
2. Электронная библиотечная система "Университетская библиотека ONLINE" (www.biblioclub.ru).
3. Электронная библиотечная система издательства "Лань" (https://e.lanbook.com).
4. Электронная библиотечная система "Юрайт" (http://www.biblio-online.ru).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО) PowerPoint. ауд. 129, 131, А305.
2.	Лабораторные занятия	Лаборатория, укомплектованная специализированными

		техническими средствами обучения – компьютерный класс, с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета (лаб. 102-106.).
3.	Групповые (индивидуальные) консультации	Аудитория, (кабинет) – компьютерный класс
4.	Текущий контроль, промежуточная аттестация	Аудитория, приспособленная для письменного ответа при промежуточной аттестации.
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.