МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Факультет истории, социологии и международных отношений

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____Хагуров Т.А.
подпись
«31» мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки/специальность
41.03.05 Международные отношения
(код и наименование направления подготовки/специальности)

Направленность (профиль) / специализация

Международное сотрудничество
(наименование направленности (профиля) / специализации)

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

Квалификация бакалавр

Краснодар 2024

Рабочая программа дисциплины ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 41.03.05 Международные отношения.

Программу составил(и):
М.В. Донцова, доцент кафедры социологии,
канд. социол. наук

подпись

Т.А. Рунаев, доцент кафедры социологии,
канд. социол. наук

подпись

Рабочая программа дисциплины «Информационная безопасность» утверждена на заседании кафедры (разработчика) социологии
протокол № 10 от 26.03.2024 г.
Заведующий кафедрой (разработчика) Хагуров Т.А.

подпись

Утверждена на заседании учебно-методической комиссии факультета истории, социологии и международных отношений
протокол № 6 от 15.05.2024 г.
Председатель УМК факультета Э.Г. Вартаньян

подпись

Рецензенты:

Муха Виктория Николаевна, кандидат социологических наук, доцент, доцент кафедры социологии, правоведения и работы с персоналом ФГБОУ ВО КубГТУ

Касьянов Валерий Васильевич, доктор исторических наук, доктор социологических наук, профессор, заведующий кафедрой истории России ФГБОУ ВО КубГУ

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Формирование у студентов знаний об основных направлениях исследований в области информационной безопасности, а также развития навыков применения актуальных цифровых методов, предназначенных для анализа состояния информационной безопасности социальных групп и организаций, в том числе международного уровня.

1.2 Задачи дисциплины.

Для достижения цели в ходе учебного процесса предполагается решить следующие задачи:

− познакомить студентов с современными теориями и концепциями информационного общества;

− выработать у студентов навыки сбора, систематизации и обработки информации, необходимой для выявления рисков информационной безопасности социальных групп и организаций, в том числе на международном уровне;

− развить способность проектирования индивидуального и (или) группового исследования с применением анализа данных для решения проблем информационной безопасности.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Информационная безопасность» относится к части факультативных дисциплин учебного плана. Дисциплина рассчитана на слушателей без предварительной подготовки. Необходимо общее знакомство со спецификой профессиональной деятельности, а также знание иностранного языка на уровне, достаточном для изучения рекомендуемых источников.

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 профессиональных компетенций:

Код и наименование индикатора	Результаты обучения по дисциплине
ОПК-2. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ОПК-2.5 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	***знает*** основные программные цифровые решения, необходимые для поддержания информационной безопасности общества и организаций, знает принципы работы современных информационных технологий
	умеет ориентироваться в программных цифровых решениях (в частности в пакетах RStudio и библиотеках Python), позволяющих выявлять риски для информационной безопасности, умеет использовать цифровые технологии защиты информации
	владеет базовыми навыками программирования на языках R и Python, необходимыми для определения рисков и поддержания информационной безопасности, владеет навыками использования антивирусов и иных средств защиты информации, информационной гигиены и этикета.

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 2 зач.ед. (72 часа), их распределение по видам работ представлено в таблице (*для студентов ОФО*)

Вид учебной работы		Всего	Семестры			
		часов		(часы)		
			6			
Контактная работа, в том числе:		**36**	**36**			
Аудиторные занятия (всего):		**36**	**36**			
Занятия лекционного типа		16	16			
Лабораторные занятия		-	-			
Занятия семинарского типа (семинары, практические занятия)		16	16			
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		3,8	3,8			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**36**	**36**			
Курсовая работа		-	-			
Проработка учебного (теоретического) материала		12	12			
Выполнение индивидуальных заданий (подготовка проектов, презентаций)		14	14			
Реферат		10	10			
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**72**	**72**			
	в том числе контактная работа	**36**	**36**			
	зач.ед	**2**	**2**			

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 6 семестре *(очная форма)*

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Теоретические основания информационной безопасности. Классификация информационных угроз	10	2	2	-	6
2.	Риски информационного поля	10	2	2	-	6
3.	Законодательство в области информационной безопасности	10	2	2	-	6
4.	Способы обеспечения информационной безопасности. Индивидуальная и государственная защита информации	10	2	2	-	6
5.	Информационно-психологическая безопасность в цифровой среде	14	4	4	-	6
6.	Цифровые методы выявления рисков информационного поля	14	4	4		6

	Контроль самостоятельной работы (КСР)	3,8	-	-	-	-
	Промежуточная аттестация (ИКР)	0,2	-	-	-	-
	Итого по дисциплине:	72	16	16	-	36

Примечание: Л - лекции, ПЗ - практические занятия / семинары, ЛР - лабораторные занятия, СРС - самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Теоретические основания информационной безопасности. Классификация информационных угроз	Понятие информации. Эволюция каналов передачи информации. Концепт «глобальной деревни» М. Маклюэна. Теория информационного общества М. Кастельса, концепция четвертой промышленной революции К. Шваба, концепция «второй эры машин» Э. Бринолфссона и Э. МакАфи, сетевая теория современных сообществ М. Грановеттера. Развитие Интернета в России и за рубежом: история возникновения, динамика числа подключенных пользователей. Техносоциальная реальность (пересечение пространственных логик онлайн и оффлайн). Типология сообществ в киберпространстве. Big Data и датификация социальной жизни. Типы информационных уроз	Опрос
2.	Риски информационного поля	Информационная война. Угрозы идеологической безопасности государства. Информационный терроризм / кибертерроризм. Кибербуллинг. Киберсталкинг. Информационные фейки в СМИ. Посягательства на личное информационное пространство. Кибермошенничество.	Опрос
3.	Законодательство в области информационной безопасности	ФЗ «О средствах массовой информации» от 27 декабря 1991 г. ФЗ «О противодействии экстремисткой деятельности» от 25 июля 2002 г. ФЗ «О коммерческой тайне» от 29 июня 2004 г. ФЗ «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. ФЗ «О персональных данных» от 27 июля 2006 г. ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29 декабря 2010 г. Доктрина информационной безопасности РФ от 5 декабря 2016 г. Стратегия национальной безопасности РФ от 2 июля 2021 г.	Опрос

4.	Способы обеспечения информационной безопасности. Индивидуальная и государственная защита информации	Процедурный уровень обеспечения информационной безопасности. Компьютерные вирусы и антивирусы. Криптография / шифрование в цифровой среде. Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство. Защиты несанкционированного доступа. Средства родительского контроля. Цифровая компетентность. Алгоритмическая грамотность.	Опрос
5.	Информационно-психологическая безопасность в цифровой среде	Понятие информационно- психологической безопасности. Типы источников информационно-психологического воздействия. Средства и методы воздействия. Виды информационного манипулирования. Пропаганда в СМИ. Методы противодействия информационно-психологическому воздействию. Информационная гигиена. Информационная культура и сетевой этикет. Девиантное поведение в сфере информационно-коммуникационных технологий.	Опрос
6.	Цифровые методы выявления рисков информационного поля	Пакеты в RStudio. Обзор пакетов интеллектуального анализа текстов. Способы построения авторских словарей тональностей. Алгоритм выявления тональности текста. Описание методов тематического моделирования. Анализ совпадений (co-occurrence): построение сетей терминов. Латентное размещение Дирихле (LDA)	Опрос

2.3.2 Занятия семинарского типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
1.	Теоретические основания информационной безопасности. Классификация информационных угроз	Обсуждения теорий информационной безопасности: концепт «глобальной деревни» М. Маклюэна; теория информационного общества М. Кастельса, концепция четвертой промышленной революции К. Шваба, концепция «второй эры машин» Э. Бринолфссона и Э. МакАфи, сетевая теория современных сообществ М. Грановеттера	Доклады
2.	Риски информационного поля	Обсуждение кейсов ведения современной информационной войны, угроз идеологической безопасности государства. Примеры информационных фейки в СМИ: практика распознавания и противодействия. Кибермошенничество и способы индивидуальной защиты	Доклады, обсуждение современных кейсов
3.	Законодательство в области информационной безопасности	Анализ законодательной базы страны и субъектов РФ в сфере информационной безопасности и защиты информации	Практическая работа

4.	Способы обеспечения информационной безопасности. Индивидуальная и государственная защита информации	Процедура электронной защиты информации. Компьютерные вирусы и антивирусы. Криптография / шифрование в цифровой среде. Защита информации и личных данных. Средства родительского контроля. Цифровая компетентность. Алгоритмическая грамотность.	Практическая работа, доклады
5.	Информационно-психологическая безопасность в цифровой среде	Обсуждение способов противодействия информационно-психологическому воздействию. Информационная гигиена. Информационная культура и сетевой этикет. Виды девиантного поведения в цифровой среде.	Доклады
6.	Цифровые методы выявления рисков информационного поля	Практика интеллектуального анализа текстов	Групповой проект

2.3.3 Лабораторные занятия.

Лабораторные занятия - не предусмотрены

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) - не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются 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.

3. Образовательные технологии.

При реализации различных видов учебной работы по дисциплине «Информационная безопасность», используются следующие образовательные технологии: активные и интерактивные формы проведения занятий - интерактивные и проблемные лекции; опросы; самостоятельная работа - работа с публикациями в предметной области дисциплины; подготовка рефератов, выполнение практических занятий.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность».

Оценочные средства включает контрольные материалы для проведения текущего контроля в форме тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых

заданий, ролевой игры, ситуационных задач и промежуточной аттестации в форме вопросов и заданий к зачету

Структура оценочных средств для текущей и промежуточной аттестации

№ п/п	Код и наименование индикатора	Результат обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-2.5 Знание современных цифровых технологий, возможность их применения для цифровой безопасности, потенциальные риски и способы их нейтрализации.	***знает*** основные программные цифровые решения, необходимые для поддержания информационной безопасности общества и организаций, знает принципы работы современных информационных технологий	контрольный опрос (КО); тестирование (Т)	Вопрос на зачете
		умеет ориентироваться в программных цифровых решениях (в частности в пакетах RStudio и библиотеках Python), позволяющих выявлять риски для информационной безопасности, умеет использовать цифровые технологии защиты информации	разработка проекта (РП)	Вопрос на зачете
		владеет базовыми навыками программирования на языках R и Python, необходимыми для определения рисков и поддержания информационной безопасности, владеет навыками использования антивирусов и иных средств защиты информации, информационной гигиены и этикета.	доклад с презентацией (ДП)	Вопрос на зачете

4.1 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы на зачет

1. Понятие информации. Эволюция каналов передачи информации.
2. Концепция «глобальной деревни» М. Маклюэна.

3. Теория информационного общества М. Кастельса.
4. Концепция четвертой промышленной революции К. Шваба.
5. Концепция «второй эры машин» Э. Бринолфссона и Э. МакАфи.
6. Сетевая теория современных сообществ М. Грановеттера.
7. Развитие Интернета в России и за рубежом: история возникновения.
8. Типология сообществ в киберпространстве.
9. Типы современных информационных угроз.
10. Информационная война в современном. Угрозы безопасности государства в информационной и идеологической сфере.
11. Типы информационных атак: информационный терроризм / кибертерроризм, кибербуллинг, киберсталкинг, информационные фейки в СМИ, кибермошенничество.
12. Законодательная база информационной безопасности и защиты информации.
13. Средства защиты информации: компьютерные вирусы и антивирусы, криптография / шифрование в цифровой среде, парольная защита и т.д.
14. Понятие информационно- психологической безопасности.
15. Типы источников информационно- психологического воздействия. Средства и методы воздействия. Виды информационного манипулирования.
16. Информационная гигиена. Информационная культура и сетевой этикет.
17. Девиантное поведение в сфере информационно- коммуникационных технологий.
18. Искусственный интеллект в информационной безопасности.
19. Data mining и Text mining как инструменты обеспечения информационной безопасности.
20. Анализ тональности текста.
21. Латентное размещение Дирихле (LDA).
22. Коррелированное тематическое моделирование (CTM).
23. Латентно-семантический анализ (LSA).

Критерии оценивания по зачету:

«зачтено»: студент владеет теоретическими знаниями по данному разделу, допускает незначительные ошибки; студент умеет правильно объяснять теоретический материал, иллюстрируя его примерами различных социальных ситуаций из жизни коллектива и / или организации.

«не зачтено»: материал не усвоен или усвоен частично, студент имеет довольно ограниченный объем знаний программного теоретического материала.

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 (модулю) 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.

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

5.1 Основная литература:

1. Козырь, Н. С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н. С. Козырь, Н. В. Седых. — Москва : Издательство Юрайт, 2024. — 170 с. — (Высшее образование). — ISBN 978-5-534-17153-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544965 (дата обращения: 31.05.2024).

2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029 (дата обращения: 31.05.2024).Миркин Б.Г. Введение в анализ данных : учебник и практикум / Б.Г. Миркин. – Москва : Издательство Юрайт, 2023. – 174 с. – (Высшее образование). – ISBN 978-5-9916-5009-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. — Режим доступа: https://urait.ru/bcode/511121.

3. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 327 с. — (Высшее образование). — ISBN 978-5-534-16772-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/542739 (дата обращения: 31.05.2024).

5.2 Дополнительная литература:

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290 (дата обращения: 31.05.2024).

2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543351 (дата обращения: 31.05.2024).

3. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/555950 (дата обращения: 31.05.2024).

3.3 Периодические издания:

1) Вестник СПбГУ.Серия: Психология, социология, педагогика
2) Вестник МГУ.Серия: Социология и политология
3) Журнал практического психолога
4) Журналист. Социальные коммуникации
5) Общественные науки и современность
6) Социально-гуманитарные знания

7) СОЦИС / Социологические исследования

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

http://lib.socio.msu.ru/l/library - Электронная библиотека социологического факультета МГУ имени М.В. Ломоносова

http://window.edu.ru/window_catalog - Единое окно доступа к образовательным ресурсам

http://www.hh.ru - Хэд Хантер

http://www.isras.ru/ - Институт социологии РАН.

http://www.i-u.ru/biblio - Русский гуманитарный интернет-университет http://www.job.ru - Джоб ру

http://www.kadrovichka.ru - Кадровичка

www.ecsocman.edu.ru - Федеральный образовательный портал по социологии, экономике и менеджменту

www.soc.pu.ru - электронный ресурс социологического факультета Санкт- Петербургского государственного университета

www.socionet.ru - портал по общественным наукам

www.wciom.ru -официальный сайт ВЦИОМ

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

Подготовку к *практическим занятиям* рекомендуется осуществлять по следующему алгоритму: работа с планами семинарских занятий. При подготовке к семинарскому занятию необходимо найти ответы на поставленные вопросы. Рекомендуется делать конспекты в форме тезисов на каждый вопрос.

Для более глубокого понимания и лучшего усвоения экономических категорий и терминов рекомендуется обращаться к основной и дополнительной литературе, работать с информационными ресурсами, справочными материалами и периодическими изданиями. Целесообразно вести собственный словарь терминов и использовать его для повторения.

После изучения материала необходимо построить логическую схему знаний, сформулировать вопросы по тем моментам, которые вызвали затруднения, с целью последующего их вынесения на семинарское занятие для обсуждения.

Важным видом работы студентов при изучении дисциплины является *самостоятельная работа*. Самостоятельная работа должна носить творческий и планомерный характер. В процессе организации самостоятельной работы большое значение имеют консультации преподавателя. Они могут быть как индивидуальными, так и в составе учебной группы.

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.*

- Использование электронных презентаций при проведении практических занятий.

8.2 *Перечень необходимого программного обеспечения.*

При проведении занятий используется пакет PowerPoint Microsoft Office, ОС Microsoft Windows 10, RStidio, PyCharm.

8.3 *Перечень информационных справочных систем:*

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)
2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)

3. Электронная библиотечная система "Университетская библиотека ONLINE" (www.biblioclub.ru)

4. Электронная библиотечная система издательства "Лань" (http://e.lanbook.com/)

5. Электронная библиотечная система "Юрайт" (http://www.biblio-online.ru)

6. Электронная библиотека "Издательского дома "Гребенников" (www.grebennikon.ru)

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

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Семинарские занятия	Аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (ПО).
2.	Лекционные занятия	Аудитория 244, 246, 249, 250, 258.
3.	Текущий контроль, промежуточная аттестация	Аудитория 244, 246, 249, 250, 258.
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченный доступом в электронную информационно-образовательную среду университета (библиотека).