Образовательное частное учреждение высшего образования
«Российская международная академия туризма»

Факультет менеджмента туризма
Кафедра гражданско-правовых дисциплин

Принято Ученым Советом
18 февраля 2026 г.
Протокол № 02-06-01

УТВЕРЖДАЮ
Первый проректор
_____В.Ю. Питюков
16 февраля 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»

по направлению подготовки 41.03.04
Политология
профиль – «Правовое регулирование международных отношений»
квалификация (степень) выпускника – бакалавр
Б1.УОО.11

Рассмотрено и одобрено
на заседании кафедры
23 января 2026 г., протокол №05

Разработчик: Грачев В.С., к.ю.н.

Химки 2026

1. Цели и задачи дисциплины

Цель дисциплины – формирование у обучающихся компетенции ПК-9 средствами дисциплины «Информационная безопасность».

Задачи дисциплины:

1) развитие у обучающихся знаний, умений и способностей анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности;

2) формирование у обучающихся практических навыков правильного выбора решений при разработке средств защиты информации, анализе рисков и угроз, безопасной работы в информационных системах.

2. Перечень формируемых компетенций и индикаторов их достижения, соотнесенные с результатами обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих компетенций, представленных в компетентностной карте дисциплины в соответствии с ФГОС ВО, компетентностной моделью выпускника, определенной вузом и представленной в ОПОП, и содержанием дисциплины (модуля):

Категория компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
Технологии	**ПК-9** Способен анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности	**ПК-9.1** Юридически корректно оценивает содержание и действие нормативно-правовых актов в сфере информационной безопасности: -выявляет систематизирует и применимые нормативные источники (федеральные законы, указы Президента РФ, постановления Правительства РФ, ведомственные акты, национальные стандарты); - определяет юридическую силу и иерархию актов (от Конституции РФ до локальных регламентов организаций); - анализирует предмет регулирования и сферу действия норм (персональные данные, государственная тайна, коммерческая тайна,	**Знать:** - систему и иерархию нормативно-правовых актов в сфере информационной безопасности в РФ, механизмы имплементации международных стандартов и соглашений в российское законодательство об информационной безопасности; - ключевые принципы правового регулирования в сфере информационной безопасности. **Уметь:** находить и отбирать применимые нормативно-правовые

		критическая информационная инфраструктура и др.); - отслеживает изменения в законодательстве и оценивает их влияние на действующие требования; -разграничивает обязанности субъектов разного уровня (государственные органы, операторы персональных данных, провайдеры, пользователи). **ПК-9.2** Профессионально квалифицирует факты и ситуации с точки зрения соответствия требованиям информационной безопасности: - сопоставляет реальные действия и процессы (обработка данных, защита информации, инциденты) с нормами законодательства; - выявляет нарушения требований к защите персональных данных определяет юридические последствия нарушений (административная, головная, гражданско-правовая ответственность). **ПК-9.3** Применяет результаты анализа нормативно-правовой базы для обеспечения информационной безопасности в профессиональной деятельности, обосновывает необходимость внедрения технических и организационных мер защиты (с опорой на нормативные требования); - составляет документы для взаимодействия с регуляторами (уведомления, отчёты, запросы);	акты для анализа конкретных ситуаций в сфере информационной безопасности; анализировать и интерпретировать нормы законодательства с учётом их целей, предмета регулирования и сферы действия; сопоставлять фактические обстоятельства (инциденты, процессы обработки данных, внедрение ИТ-решений) с требованиями нормативных актов; выявлять нарушения требований к: защите персональных данных; обеспечению безопасности объектов; оценивать соответствие ИТ-систем и бизнес-процессов требованиям законодательства. **Владеть:** - навыками применения норм права при подготовке документов в сфере информационной безопасности: заключения и правовые мнения по вопросам соответствия ИТ-решений; - политики, регламенты, инструкции по информационной безопасности для организаций; - уведомления и отчёты для регуляторов (Роскомнадзор); - претензии и ответы на запросы контролирующих

		- предлагает пути устранения нарушений и минимизации рисков с учётом правовых предписаний; - консультирует сотрудников и руководство по вопросам соблюдения требований информационной безопасности в рамках действующего законодательства.	органов.

3. Место дисциплины в структуре ОПОП и этапы формирования компетенций

Дисциплина «Информационная безопасность» относится к дисциплинам по выбору части ОПОП, формируемой участниками образовательных отношений. Компетенции, формируемые дисциплиной «Информационная безопасность», также формируются и на других этапах в соответствии с учебным планом.

4. Объем дисциплины и виды учебной работы

4.1. Очная форма обучения

Вид учебной работы	**Всего часов**	**Семестры**	
		6	**-**
Контактная работа обучающихся с преподавателем, в том числе:	52	52	-
занятия лекционного типа (ЗЛТ)	24	24	-
лабораторные работы (ЗСТ (ЛР))	-	-	-
практические занятия (ЗСТ ПР)	24	24	-
групповые консультации, и (или) индивидуальную работу обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации) (ГК)	2	2	-
групповые консультации по подготовке курсового проекта (работы)	-	-	-
контактная работа при проведении промежуточной аттестации (в том числе при оценивании результатов курсового проектирования (выполнения курсовых работ) (ПА конт)	2	2	-
Самостоятельная работа обучающегося (СРО), в том числе	128	128	-
СРуз - самостоятельная работа обучающегося при подготовке к учебным занятиям и курсовым проектам (работам)	94	94	-
СРпа - самостоятельная работа обучающегося при подготовке к промежуточной аттестации	34	34	-
Форма промежуточной аттестации (экзамен)	Экзамен		
Общая трудоемкость дисциплины: часы **Зачетные единицы**	180 5	180 5	

5. Содержание дисциплины

5.1. Содержание разделов и тем дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Информационная безопасность и защита информации в России.	Понятие «информационная безопасность» и «защита информации». Основные стандарты в области обеспечения информационной безопасности. Доктрина информационной безопасности в Российской Федерации. Основы государственной политики Российской Федерации в области международной информационной безопасности. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
2.	Правовое регулирование отношений в сфере информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности и защите информации. Международные и отечественные нормы права, определяющие вопросы информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.
3.	Информационная безопасность в условиях функционирования в России глобальных информационных сетей и IT-технологий	Основные положения теории информационной безопасности. Модели информационной безопасности и их применение. Интернет и его информативные ресурсы, как доступный информационный источник, должен обеспечивать размещение актуальной, достоверной безопасно защищенной информации в условиях креативных политтехнологий и политического пиара с использованием современных IT-продуктов. Особенности безопасной работы с современными мессенджерами в глобальной информационной сети Интернет в условиях необходимости соблюдения установленных законодательством требований по защите информации. Правовые проблемы информационной безопасности. Понятие информационного оружия, информационной войны в политической сфере, используемых в медиа-пространстве и СМИ.
4.	Анализ способов нарушений информационной безопасности	Классификации угроз безопасности информации и средств защиты информации. Виды возможных нарушений информационной безопасности. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения и их классификация. Общие понятия антивирусной защиты. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных

		программ. Естественные и человеческие факторы информационных угроз. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации. Вредоносные программы. Разглашение и утечка конфиденциальной информации. Каналы утечки конфиденциальной информации. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации угроз информационной безопасности. Способы воздействия угроз на информационные объекты.
5.	Ответственность за нарушение в области информационной безопасности по законодательству Российской Федерации.	Меры дисциплинарной, административной и уголовной ответственности за правонарушения в области информационной безопасности и защиты информации. Нарушение законодательства о персональных данных. Нарушение правил защиты информации. Разглашение информации с ограниченным доступом. Незаконная деятельность в области защиты информации. Неправомерный доступ к компьютерной информации. Создание, использование вредоносных программ. Нарушение правил эксплуатации критической информационной инфраструктуры.

5.2. Разделы дисциплин и виды занятий

5.2.1. Очная форма обучения

№	Наименование разделов и тем дисциплины	Формируемая компетенция	Всего часов	Контактная работа с обучающимися (час.)					СРО
				Итого	в том числе				
					ЗЛТ	ЗСТ (ЛР)	ЗСТ (ПР)	ГК/ПА	
1	Информационная безопасность и защита информации в России.	ПК-9	34	8	4	-	4	-	26
2	Правовое регулирование отношений в информационной сфере	ПК-9	32	8	4	-	4	-	24
3	Информационная безопасность в условиях функционирования в России глобальных сетей	ПК-9	34	8	4	-	4	-	26
4	Анализ способов нарушений информационной безопасности	ПК-9	38	12	6	-	6	-	26
5	Ответственность за нарушение в области информационной безопасности по	ПК-9	38	12	6	-	6	-	26

	законодательству Российской Федерации.								
	Групповые консультации, и (или) индивидуальную работу обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации) (ГК)	ПК-9	2	2	-	-	-	2	-
	Форма промежуточной аттестации (экзамен)	ПК-9	2	2	-	-	-	2	
	Всего часов		180	52	24	-	24	4	128

6. Контактная и самостоятельная работа обучающихся

Контактная работа при проведении учебных занятий по дисциплинам (модулям) включает в себя: занятия лекционного типа (лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками РМАТ и (или) лицами, привлекаемыми РМАТ к реализации образовательных программ на иных условиях, обучающимся) и (или) занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия), и (или) групповые консультации, и (или) индивидуальную работу обучающихся с педагогическими работниками РМАТ и (или) лицами, привлекаемыми РМАТ к реализации образовательных программ на иных условиях (в том числе индивидуальные консультации).

Занятия лекционного типа проводятся в соответствии с объемом и содержанием, представленным в таблице раздела 5.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, содержание дисциплины (модуля) составлено на основе результатов научных исследований, проводимых РМАТ, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

6.1. Занятия семинарского типа (семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и др.)

Тема 1. Информационная безопасность и защита информации в России.

Цель занятия: Изучение понятий «информационная безопасность» и «защита информации», назначения и задач государства в сфере обеспечения информационной безопасности.

Компетенции: ПК-9 Способен анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности.

Тип занятия: семинар

Форма проведения: Доклад (в форме презентации)

Основная тема (либо проблема) для обсуждения: Современное состояние информационной безопасности и защиты информации в России.

Представление доклада в форме презентации на тему*:*

1. Понятие «информационная безопасность» и «защита информации».
2. Основные стандарты в области обеспечения информационной безопасности. Доктрина информационной безопасности в Российской Федерации.
3. Основы государственной политики Российской Федерации в области международной информационной безопасности.
4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Тема 2. Правовое регулирование отношений в сфере информационной безопасности.

Цель занятия: Изучение основных нормативно-правовых актов в области информационной безопасности и защиты информации в правовой системе Российской Федерации.

Компетенции: ПК-9 Способен анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности.

Тип занятия: семинар

Форма проведения: Устный ответ (в форме дискуссии), эссе.

Основная тема (либо проблема) для обсуждения: Правовое регулирование отношений в сфере информационной безопасности.

Вопросы для подготовки к дискуссии:

1. Основные нормативно-правовые акты в области информационной безопасности и защите информации.
2. Международные и отечественные нормы права, определяющие вопросы информационной безопасности.
3. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Представление эссе на тему «Политика безопасности и основные стандарты в области обеспечения информационной безопасности.».

Тема 3. Информационная безопасность в условиях функционирования в России глобальных информационных сетей.

Цель занятия: Изучение содержания основных положений теории информационной безопасности. Модели информационной безопасности и их применение.

Компетенции: ПК-9 Способен анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности.

Тип занятия: семинар

Форма проведения: дискуссия, решение кейс-задач и ситуационных задач.

Основная тема (либо проблема) для обсуждения: Раскрытие основных положений понятия теории информационной безопасности, моделей безопасности и их практического применения.

Вопросы для подготовки к дискуссии:

1. Основные положения теории информационной безопасности.
2. Модели информационной безопасности и их применение.
3. Интернет и его информативные ресурсы, как доступный информационный источник для размещения актуальной, достоверной безопасно защищенной информации в

условиях креативных политтехнологий и политического пиара с использованием современных IT-продуктов.

4. Особенности безопасной работы с современными мессенджерами в глобальной информационной сети Интернет в условиях необходимости соблюдения установленных законодательством требований по защите информации.

5. Интернет и его информационные ресурсы как источник информации, отвечающий за актуальность, достоверность, информативность, доступность каналов связи, обеспечивающих безопасность информации в условиях современных политтехнологий и политического пиара.

6. Особенности работы с современными мессенджерами в глобальной информационной сети Интернет в условиях необходимости соблюдения информационной безопасности при оценке источников политической информации.

7. Правовые проблемы информационной безопасности.

8. Понятие информационного оружия, информационной войны в политической сфере, используемых в медиа-пространстве и СМИ.

Тема 4. Анализ способов нарушений информационной безопасности

Цель занятия: Рассмотреть классификации угроз безопасности информации и средств защиты информации. Виды возможных нарушений информационной безопасности.

Компетенции: ПК-9 Способен анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности.

Тип занятия: семинар

Форма проведения: дискуссия, решение кейс-задач и ситуационных задач, групповой проект.

Основная тема (либо проблема) для обсуждения: Рассмотрение сущностной характеристики классификации угроз безопасности информации, средств защиты информации и видов наиболее распространенных нарушений информационной безопасности.

Вопросы для обсуждения:

1. Классификации угроз безопасности информации и средств защиты информации.

2. Виды возможных нарушений информационной безопасности.

3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

4. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров.

5. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения и их классификация.

6. Общие понятия антивирусной защиты. Классификация вредоносных программ.

7. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.

8. Естественные и человеческие факторы информационных угроз.

9. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации. Вредоносные программы.

10. Разглашение и утечка конфиденциальной информации. Каналы утечки конфиденциальной информации.

11. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации угроз информационной безопасности.

12. Способы воздействия угроз на информационные объекты.

Выполнение группового проекта на выявление сформированности умений находить и отбирать применимые нормативно-правовые акты для анализа конкретных ситуаций в сфере

информационной безопасности, анализировать и интерпретировать нормы законодательства с учётом их целей, предмета регулирования и сферы действия, сопоставлять фактические обстоятельства с требованиями нормативных актов, выявлять нарушения требований к защите персональных данных.

Тема 5. Ответственность за нарушение в области информационной безопасности по законодательству Российской Федерации.

Цель занятия: Изучить требования законодательства Российской Федерации, предусматривающие меры дисциплинарной, административной и уголовной ответственности за правонарушения в сфере информационной безопасности и защиты информации.

Компетенции: ПК-9 Способен анализировать нормативно-правовые акты, регламентирующие требования к информационной безопасности.

Тип занятия: семинар

Форма проведения: доклад (в форме презентации)

Основная тема (либо проблема) для обсуждения: Рассмотрение и анализ мер дисциплинарной, административной и уголовной ответственности за правонарушения в области информационной безопасности и защиты информации.

Вопросы для обсуждения:

1. Меры дисциплинарной, административной и уголовной ответственности за правонарушения в области информационной безопасности и защиты информации.
2. Нарушение законодательства о персональных данных.
3. Нарушение правил защиты информации.
4. Разглашение информации с ограниченным доступом.
5. Незаконная деятельность в области защиты информации.
6. Неправомерный доступ к компьютерной информации.
7. Создание, использование вредоносных программ.
8. Нарушение правил эксплуатации критической информационной инфраструктуры.

6.2. Самостоятельная работа обучающихся

Тема 1. Информационная безопасность и защита информации в России.

Вид работы: изучение литературы по теме, подготовка к семинарскому занятию.

Вопросы для подготовки к дискуссии:

1. Понятие «информационная безопасность» и «защита информации».
2. Основные стандарты в области обеспечения информационной безопасности. Доктрина информационной безопасности в Российской Федерации.
3. Основы государственной политики Российской Федерации в области международной информационной безопасности.
4. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.

Подготовка к выполнению группового проекта на выявление сформированности умений выявлять и анализировать особенности туристского продукта**,** используя современные технологии: информационные и коммуникативные технологии.

Тема 2. Правовое регулирование отношений в сфере информационной безопасности.

Вид работы: изучение литературы по теме, подготовка к семинарскому занятию.

Вопросы для подготовки к дискуссии:

1. Основные нормативно-правовые акты в области информационной безопасности и защите информации.
2. Международные и отечественные нормы права, определяющие вопросы информационной безопасности.
3. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны.

Подготовка эссе на тему «Политика безопасности и основные стандарты в области обеспечения информационной безопасности.».

Подготовка к выполнению группового проекта на выявление сформированности умений выявлять и анализировать особенности туристского продукта, используя современные технологии: информационные и коммуникативные

Тема 3. Информационная безопасность в условиях функционирования в России глобальных информационных сетей.

Вид работы: изучение литературы по теме, подготовка к семинарскому занятию.

Темы докладов (в форме презентации):

1. Основные положения теории информационной безопасности.
2. Модели информационной безопасности и их применение.
3. Интернет и его информативные ресурсы, как доступный информационный источник для размещения актуальной, достоверной безопасно защищенной информации в условиях креативных политтехнологий и политического пиара с использованием современных IT-продуктов.
4. Особенности безопасной работы с современными мессенджерами в глобальной информационной сети Интернет в условиях необходимости соблюдения установленных законодательством требований по защите информации.
5. Интернет и его информационные ресурсы как источник информации, отвечающий за актуальность, достоверность, информативность, доступность каналов связи, обеспечивающих безопасность информации в условиях современных политтехнологий и политического пиара.
6. Особенности работы с современными мессенджерами в глобальной информационной сети Интернет в условиях необходимости соблюдения информационной безопасности при оценке источников политической информации.
7. Правовые проблемы информационной безопасности.
8. Понятие информационного оружия, информационной войны в политической сфере, используемых в медиа-пространстве и СМИ.

Тема 4. Современные технологии разработки рекламного обращения туристского предприятия

Вид работы: изучение литературы по теме, подготовка к семинарскому занятию.

Вопросы для подготовки к дискуссии:

1. Классификации угроз безопасности информации и средств защиты информации.
2. Виды возможных нарушений информационной безопасности.

3. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.

4. Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров.

5. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения и их классификация.

6. Общие понятия антивирусной защиты. Классификация вредоносных программ.

7. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ.

8. Естественные и человеческие факторы информационных угроз.

9. Несанкционированный доступ к защищаемой информации. Типовые пути несанкционированного доступа к информации. Вредоносные программы.

10. Разглашение и утечка конфиденциальной информации. Каналы утечки конфиденциальной информации.

11. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации угроз информационной безопасности.

12. Способы воздействия угроз на информационные объекты.

Подготовка к выполнению группового проекта на выявление сформированности умений выявлять, анализировать особенности туристского продукта, использовать методы продвижения турпродукта, а также использовать современные технологии продвижения.

Тема 5. Ответственность за нарушение в области информационной безопасности по законодательству Российской Федерации.

Вид работы: изучение литературы по теме, подготовка к семинарскому занятию.

Вопросы для подготовки к дискуссии:

1. Меры дисциплинарной, административной и уголовной ответственности за правонарушения в области информационной безопасности и защиты информации.

2. Нарушение законодательства о персональных данных.

3. Нарушение правил защиты информации.

4. Разглашение информации с ограниченным доступом.

5. Незаконная деятельность в области защиты информации.

6. Неправомерный доступ к компьютерной информации.

7. Создание, использование вредоносных программ.

8. Нарушение правил эксплуатации критической информационной инфраструктуры.

6.3. Методические рекомендации по самостоятельной работе обучающихся и подготовке к промежуточной аттестации

Методические рекомендации по самостоятельной работе составлены с целью оптимизации процесса освоения обучающимися учебного материала.

Самостоятельная работа обучающегося направлена на углубленное изучение разделов и тем рабочей программы и предполагает изучение литературных источников, выполнение домашних заданий и контрольных работ, проведение исследований разного характера. Работа основывается на анализе материалов, публикуемых в интернете, а также реальных фактов, личных наблюдений.

Самостоятельная работа обучающегося над усвоением материала по дисциплине может выполняться в читальном зале РМАТ, специально отведенных для самостоятельной работы помещениях, посредством использования электронной библиотеки и ЭИОС РМАТ.

Содержание и количество самостоятельной работы обучающегося определяется учебным планом, методическими материалами и указаниями преподавателя.

Также самостоятельная работа включает подготовку и анализ материалов по темам пропущенных занятий.

Самостоятельная работа во внеаудиторное время включает:

- работу с лекционным материалом, предусматривающую проработку конспекта лекций;
- изучение учебной и научной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по индивидуально заданной проблеме курса, написание доклада, исследовательской работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- подготовку к практическим занятиям;
- подготовка к промежуточной аттестации.

В зависимости от выбранных видов самостоятельной работы студенты самостоятельно планируют время на их выполнение. Предлагается равномерно распределить изучение тем учебной дисциплины.

7. Фонд оценочных средств

Фонд оценочных средств по дисциплине разработан в соответствии с Методическими рекомендациями и является составной частью ОПОП.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1. Основная литература

1. Алексеева, М. В. Защита конфиденциальной информации в российском праве / М. В. Алексеева. — СПб.: Питер, 2021. — 380 с.
2. Данилова, Н. И. Правовая защита информации в России: теория и практика / Н. И. Данилова. — М.: Юрайт, 2021. — 350 с.
3. Кабак, В. М. Охрана и защита информации в России: правовые основы / В. М. Кабак. — М.: Эксмо, 2021. — 290 с.
4. Климентьев, П. А. Ответственность за правонарушения в сфере информационной безопасности / П. А. Климентьев. — М.: Юридическая литература, 2021. — 310 с.
5. Раченко, Т. А. Информационная безопасность: учебно-методическое пособие / Т. А. Раченко. — Тольятти: ТГУ, 2024. — 135 с. — ISBN 978-5-8259- 1612-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/427130
6. Смирнов, В. В. Правовое обеспечение защиты информации: Учебник для вузов / В. В. Смирнов. — М.: Инфра-М, 2022. — 420 с.
7. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 с. — ISBN 978 5-4497-2418-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/133957.html

8.2. Дополнительная литература

1. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2021. – 336 с. (Высшее образование). Текст: электронный. – URL: https://znanium.com/catalog/product/1189326.

2. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. – Москва: ИНФРА-М, 2021. – 201 с. – (Высшее образование: Бакалавриат). – Текст: электронный. – URL: https://znanium.com/catalog/product/1013711.

9. Обновляемые современные профессиональные базы данных и информационные справочные системы

9.1. Обновляемые современные профессиональные базы данных

1. https://www.elibrary.ru/defaultx.asp?amp& - научная электронная библиотека eLIBRARY.RU - это крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования.
2. https://wciom.ru/ - открытая база данных ВЦИОМ-Навигатор содержит результаты более тысячи опросов с 1992 г. по настоящее время, и постоянно пополняется (для исследователей, ученых, преподавателей, студентов, практиков, работающих с общественным мнением).
3. https://www.scopus.com - Реферативная и справочная база данных рецензируемой литературы Scopus;
4. https://apps.webofknowledge.com - Политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных Web of Science;
5. https://www.sciencealert.com - Science Alert является академическим издателем журналов открытого доступа. Также издает академические книги и журналы. Science Alert в настоящее время имеет более 150 журналов открытого доступа в области бизнеса, экономики, информатики, коммуникации, инженерии, медицины, математики, химии, общественной и гуманитарной науки;
6. https://sciencepublishinggroup.com - Science Publishing Group электронная база данных открытого доступа включающая в себя более 500 научных журналов, около 50 книг, 30 материалов научных конференций в области статистики, экономики, менеджмента, педагогики, социальных наук, психологии, биологии, химии, медицины, пищевой инженерии, физики, математики, электроники, информатики, науке о защите природы, архитектуре, инженерии, транспорта, технологии, творчества, языка и литературы.

9.2. Обновляемые информационные справочные системы

1. Информационно-правовая система «Гарант». – URL: http://www.garant.ru/;
2. Информационно-правовая система «Консультант плюс». – URL: http://www.consultant.ru/.

10. Обновляемый комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. Microsoft Office. Интегрированный пакет прикладных программ;
2. Microsoft Windows;
3. Корпоративная информационная система «КИС».

11. Электронные образовательные ресурсы

1. ЭБС «Университетская библиотека Онлайн»;
2. ЭБС «Юрайт»;
3. Корпоративная информационная система «КИС».

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Изучение дисциплины обеспечивается в соответствии требованиями Федерального государственного образовательного стандарта по направлению подготовки 41.03.04 Политология к материально-техническому обеспечению. Материально-техническое обеспечение необходимое для реализации дисциплины включает: учебные аудитории для проведения учебных занятий, оснащенные оборудованием (специализированной мебелью-посадочные места по количеству обучающихся; рабочее место преподавателя; шкафы, стенды, компьютеры с выходом в интернет (12 шт.)) и техническими средствами обучения (ноутбук, телевизор).

Помещения для самостоятельной работы обучающихся оснащены персональными компьютерами (10 шт.) с возможностью подключения к информационно-телекоммуникационной сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду, к современным профессиональным базам данных и информационным справочным системам; комплект мебели.

РМАТ обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства (состав определен в п.10 и подлежит обновлению при необходимости).

При использовании в образовательном процессе печатных изданий библиотечный фонд укомплектован печатными изданиями из расчета не менее 0,25 экземпляра каждого из изданий, указанных в п.8, на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль), проходящих соответствующую практику.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется в п.9 и подлежит обновлению (при необходимости).