Федеральное государственное бюджетное образовательное учреждение высшего образования «Дипломатическая академия Министерства иностранных дел Российской Федерации»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«ОСНОВЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 41.03.05 Международные отношения
Направленность (профиль) подготовки: Международные отношения и внешняя политика
Формы обучения: очная
Квалификация выпускника: Бакалавр
Объем дисциплины (модуля):
в зачетных единицах: 16 з.е.
в академических часах: 576 ак.ч.

2025

Сурма И.В. «Основы международной информационной безопасности»: Рабочая программа дисциплины (модуля). – Москва: Дипломатическая академия МИД России, 2025 г.

Рабочая программа по дисциплине (модулю) «Основы международной информационной безопасности» по направлению подготовки 41.03.05 Международные отношения, направленность (профиль) программы «Международные отношения и внешняя политика» составлена Сурма И.В. в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки, утвержденного приказом Министерства науки и высшего образования от 15.06.2017 г. № 555.

Руководитель ОПОП Фрадкова В.И.

Директор библиотеки Толкачева Ю.В.

Рабочая программа:
обсуждена и рекомендована к утверждению решением кафедры
от 6 февраля 2025 г., протокол № 5
Зам. заведующего кафедрой
Международной и национальной безопасности Иванов О.П.

рекомендована Учебно-методическим советом (УМС) академии
от 20 марта 2025 г., протокол № 6
Председатель УМС Ткаченко М.Ф.

одобрена Ученым Советом Академии
от 26 марта 2025 г., протокол № 4

© Дипломатическая Академия МИД России, 2025
© Сурма И.В., 2025

1. Цели и задачи освоения дисциплины (модуля) «Основы международной информационной безопасности»

Цель: Формирование у бакалавров системного представления о наиболее важных аспектах, составляющих основы международной информационной безопасности и изучение основных направлений обеспечения международной информационной безопасности в современных условиях.

Задачи:

сформировать у бакалавров четкое представление о понятийном аппарате дисциплины;

выработать навыки системного и целостного подхода к проблеме обеспечения международной информационной безопасности, раскрыть основные принципы, угрозы и задачи обеспечения международной информационной безопасности;

дать основы международной информационной безопасности и защиты информации в информационно-коммуникационных системах государственной власти. Познакомить с основными протоколами и адресацией в глобальной сети Интернет;

показать глобальный и региональный аспекты обеспечения международной информационной безопасности;

дать представление и проанализировать источники, причины и цели современной информационной войны;

познакомить бакалавров с методами анализа эффективности использования ИТ-технологий и оценке рисков в результате их внедрения;

дать представление об информационных войнах по поколениям и технологиям, довести взгляды на войны будущего;

раскрыть содержание новых стратегических документов США и НАТО в области информационной безопасности;

раскрыть сущность современного противоборства в информационной сфере;

дать бакалаврам представление об основах обеспечения международной информационной безопасности.

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

Изучение дисциплины направлено на формирование у обучающихся следующих компетенций: *УК-5.1; УК-5.2; ПК-2.3; ПК-3.3*

№ п/п	Формируемые компетенции (код и наименование компетенции)	Код и формулировка индикатора компетенции	Планируемые результаты обучения
1	УК-5 – Способен воспринимать межкультурное разнообразие	УК-5.1 – Имеет базовые представления о межкультурном разнообразии общества в социально-историческом,	**Знать:** имеет теоретические и практические знания основ межкультурного разнообразия общества в социально-историческом,

	общества в социально-историческом, этическом и философском контекстах	этическом и философском контекстах	этическом и философском контекстах;
			Уметь: применять теоретические и практические знания межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах в профессиональной сфере.
		УК-5.2 – Понимает необходимость восприятия и учета межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах	**Знать:** и понимать необходимость восприятия и учета межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах;
			Уметь: воспринимать и учитывать межкультурное разнообразие общества в социально-историческом, этическом и философском контекстах.
2	ПК-2 - Способен ориентироваться в механизмах многосторонней дипломатии и выявлять особенности современной российской политики	ПК-2.3 - Анализирует сложные механизмы многосторонней и интеграционной дипломатии с учетом особенностей их функционирования	**Знать:** порядок действий по проведению анализа сложных механизмов многосторонней и интеграционной дипломатии с учетом особенностей их функционирования. **Уметь:** осуществлять анализ сложных механизмов многосторонней и интеграционной дипломатии с учетом особенностей их функционирования.
3	ПК-3 - Способен понимать исторические, культурные, географические, экономические, политические, правовые аспекты международных отношений и применять на практике теоретические основы для исследования развития современных государств	ПК-3.3 - Выявляет особенности социально-политических и экономических процессов в мировой политике, закономерности глобальных и региональных политических и экономических процессов и понимает их роль во внешней политике Российской Федерации и других государств	**Знать:** порядок выявления особенностей социально-политических и экономических процессов в мировой политике, закономерности глобальных и региональных политических и экономических процессов и понимает их роль во внешней политике Российской Федерации и других государств. **Уметь:** осуществлять действия по выявлению особенностей социально-политических и экономических процессов в мировой политике, закономерности глобальных и региональных политических и экономических процессов и

			понимать их роль во внешней политике Российской Федерации и других государств.

3. Объем дисциплины (модуля) и виды учебной работы

Объем дисциплины (модуля) и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

*Очная форма обучения**

Виды учебной деятельности		Всего	По семестрам					
			1	2	3	4	5	6
1. Контактная работа обучающихся с преподавателем***:		129					64,5	64,5
Аудиторные занятия, часов всего, в том числе:		128					64	64
• занятия лекционного типа		64					32	32
• занятия семинарского типа:		64					32	32
практические занятия								
лабораторные занятия								
в том числе занятия в интерактивных формах								
в том числе занятия в форме практической подготовки								
Контактные часы на аттестацию в период экзаменационных сессий -		1					0,5	0,5
2. Самостоятельная работа студентов****, всего		447					223,5	223,5
• курсовая работа (проект)								
• др. формы самостоятельной работы:		447					223,5	223,5
– *Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы*		394					197	197
Подготовка к экзамену		53					26,5	26,5
3.Промежуточная аттестация: *экзамен*							экзамен	экзамен
ИТОГО:	Ак.часов	576					288	288
Общая трудоемкость	зач. ед.	16					16	16

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

4.1. Содержание дисциплины «Основы международной информационной безопасности»

Тема 1. Международное информационное общество и проблемы информационного обеспечения безопасности.

Рассматривается международная информационная безопасность как категория и тенденции развития глобального информационного общества, которые во многом обусловлены проблемой обеспечения международной информационной безопасности. В глобальной информационной сфере формируются линии разделения и направления различных политических конфликтов, государства разрабатывают

планы ведения информационных войн и информационного противоборства. Транснациональная же природа информационного общества формирует ситуацию взаимозависимости, что придает импульс международному сотрудничеству по обеспечению информационной безопасности. Раскрываются основные принципы обеспечения международной информационной безопасности, основные потенциальные и реальные угрозы, основные задачи в области обеспечения международной информационной безопасности.

Тема 2. Направления в международной информатизации и основные этапы создания экономических информационных систем и компьютерных систем безопасности.

Последовательно раскрываются основные этапы развития информационных технологий и международной информатизации. Рассматриваются экономические законы развития информационных технологий. Показаны место и роль информационных технологий в условиях формирования информационного общества. Дан обзор современного состояния и перспектив развития информационных технологий, проблемы их развития. Рассматривается существующая на сегодня сегментация рынка информационных технологий и регулирующая деятельность государственных органов, направленная на развитие информационной сферы общества, которая охватывает не только телекоммуникации, информационные системы или средства массовой информации, а всю совокупность производств и отношений, связанных с созданием, хранением, обработкой, демонстрацией, передачей информации во всех ее видах - деловой, развлекательной, научно-образовательной, новостной и т.п. Представлена классификация информационных угроз и характеристика их последствий, построение системы защиты информации, особенности организации информационной безопасности в отдельных экономических системах и принципы построения системы информационной безопасности.

Тема 3. Распределенная обработка международной информации и компьютерные сети. Международная компьютерная сеть INTERNET, основные протоколы и адресация в глобальной сети.

Классификация компьютерных сетей. Локальные и глобальные сети. Internet - Всемирная паутина и её российский сегмент. Топология сетей. Internet: адресация, доменная структура. Основные элементы технологии WWW: язык гипертекстовой разметки документов (Hyper Text Markup Language - HTML); протокол обмена гипертекстовой информацией (Hyper Text Transfer Protocol - HTTP); универсальный способ адресации ресурсов в сети (Universal Resource Identifier - URI, и Universal Resource Locator - URL); система доменных имен (Domain Name System - DNS); универсальный интерфейс шлюзов (Common Gateway Interface - CGI), добавленный позже сотрудниками Национального Центра Суперкомпьютерных Приложений (National Center for Supercomputing Applications - NCSA). расширяемый язык разметки (eXtensible Markup Language - XML), рекомендованный Консорциумом Всемирной паутины. Виды сервиса Интернет.

Тема 4. Международные информационные системы поддержки деятельности органов государственной власти. Интеллектуальный кабинет руководителя и применение ситуационных (кризисных) центров.

Принципы построения информационно-аналитических систем (ИАС). Системы информационной поддержки принятия внешнеполитических решений. Ситуационные центры: опыт создания и применения (США, Германии, Франции, России, ЕС и др.). Ситуационно-кризисная дипломатия - цифровые технологии и возможности систем ИИ. Информационно-аналитическое обеспечение внешнеполитического процесса в РФ.

Тема 5. Основы международной информационной безопасности и защита информации в ИКТ системах государственного управления. Экспертно-аналитические системы.

Построение информационной безопасности на основе ГОСТ 27 002 и ISO 27032. Модель гонки вооружений. Стратегическая и геоцивилизационная матрицы в долгосрочном макропрограммировании. Зарубежный опыт долгосрочного прогнозирования и стратегического планирования с использованием ИКТ и ИИ. Справочно-правовые и геоинформационные системы. Анализ данных социально-политического характера. Зарубежные центры, занимающиеся проблемами анализа и прогнозирования.

Тема 6. Государственная политика Российской Федерации в области международной информационной безопасности.

Раскрываются основы государственной политики России в области обеспечения международной информационной безопасности. Представлен указ Президента РФ от 12 апреля 2021 г. № 213, основы государственной политики России в области международной информационной безопасности и даются ключевые векторы реализации государственной политики Российской Федерации через: продвижение российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в этой сфере; содействие созданию международно-правовых механизмов предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве и организацию межведомственного взаимодействия. Рассматриваются основные угрозы в данной сфере: использование IT-технологий в военно-политической и иной сферах для подрыва суверенитета государств, нарушения их территориальной целостности, а также в террористических, экстремистских и преступных целях.

Тема 7. Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы.

Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы. Рассматриваются результаты деятельности Первого комитета Генеральной Ассамблеи ООН в процессе решения проблемы международной информационной безопасности (МИБ).
Представлены возможности создания международного режима по запрещению информационного оружия. Обосновываются актуальность и возрастающая важность

изучения этих процессов со стороны научного сообщества. Рассматривается история вопроса, а также дается прогноз перспектив решения проблемы обеспечения МИБ в рамках ООН.

Тема 8. Стратегическое сотрудничество в области МИБ в рамках международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.)

Рассматривается деятельность международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.) в сфере безопасности. Представлены государства-участники международных организаций имеющие общие цели и интересы, а также сходные стратегические задачи по укреплению международного сотрудничества в сфере международной информационной безопасности.

Тема 9. Основные направления развития ИКТ и технологий искусственного интеллекта в дипломатии и международных отношениях.

Дипломатия 2.0 и 3.0 – зарубежный опыт и геополитические вызовы современности. Глобальные социальные сети и МИБ. Роль международных организаций в управлении Интернетом. Экстраполяция тенденций и компьютерные методики анализа общественно-политических процессов. Практико-ориентированные подходы по повышению эффективности и безопасности при работе с технологиями искусственного интеллекта.

Тема 10. Современные ИКТ, искусственный интеллект и противоборство в информационной сфере: риски и угрозы. Искусственный интеллект в гибридных и когнитивно-ментальных войнах современности.

Даются теоретические подходы к информационной борьбе (информационному противоборству). При этом раскрываются основополагающие понятия: «информация» в узком и широком смысле; уровни информационной борьбы (информационного противоборства); «информационная борьба» и «информационное противоборство»; «информационное поле» и «информационный ресурс»; средства информационной борьбы (информационного противоборства); полное определение информационной борьбы. Раскрываются современные вызовы и угрозы в информационной сфере. Показано основное различие между кибербезопасностью и международной информационной безопасностью. Даются современные взгляды на информационный ресурс и особенности информационного воздействия, направленного против России.

Рассматривается Национальная Стратегия развития искусственного интеллекта до 2030, дается анализ внесенных изменений и раскрывается суть внесённых поправок (Указ Президента Российской Федерации от 15.02.2024 № 124). Раскрывается сущность стратегии информационной войны, новые угрозы информационной безопасности России, а также новые информационные технологии, применяемы Западом (США и НАТО) против России.

Особое внимание обращается на такие новые направления борьбы в информационной сфере, как кибернетический терроризм и информационно-психологическое противоборство. Представлена эволюция термина «стратегическая коммуникация» в доктринах Министерства обороны США и НАТО. Анализируются

потенциальные возможности и показаны новые функции искусственного интеллекта в применении к стратегическим коммуникациями. Обзор докладов Центра передового опыта НАТО по стратегическим коммуникациям.

Тема 11. Использование современных ИКТ и технологий ИИ в обеспечении безопасности и обороны страны и тенденции их применения в военных целях (опыт США, Китая, Германии, Японии и др.)

Рассматриваются основные вызовы и угрозы использования современных информационно-коммуникационных технологий и систем искусственного интеллекта в военной сфере. Представлен обзор стратегий развития и управления искусственным интеллектом ведущих стран мира (США, Великобритания, Россия, ЕС, Китай, Франция, Германия, Южная Корея и др.).

Тема 12. Международно-правовая база и инструменты обеспечения международной информационной безопасности.

Показано, что в настоящее время вопросы международной информационной безопасности на универсальном уровне регулируются документами, нормы которых носят морально-политический характер и относятся к мягкому праву. С одной стороны, современным международным правом закрепляются основы обеспечения международной информационной безопасности, а с другой – поведение государств в информационно-коммуникационном пространстве в настоящее время подробно не регламентировано. Рассматривается международное сотрудничество в области поддержания международной информационной безопасности, которое осуществляется в институциональной и конвенционной форме.

Рассматриваются Будапештская конвенция и российские инициативы по совершенствованию международно-правового сотрудничества в области информационной безопасности (Концепция Конвенции об обеспечении международной информационной безопасности и внесённый в Спецкомитет ООН российский проект универсальной международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях).

*Очная форма обучения**

№	Раздел дисциплины, тема	Занятия лекционного типа	Практические занятия	Лабораторные работы	Самостоятельная работа
		ак.час.	ак.час.	ак.час.	ак.час.
5-й семестр					
1	Тема 1: Международное информационное общество и проблемы информационного обеспечения безопасности.	4	4		32

2	Тема 2: Направления в международной информатизации и основные этапы создания экономических информационных систем и компьютерных систем безопасности.	4	4		33
3	Тема 3: Распределенная обработка международной информации и компьютерные сети. Международная компьютерная сеть INTERNET, основные протоколы и адресация в глобальной сети.	6	6		33
4	Тема 4: Международные информационные системы поддержки деятельности органов государственной власти. Интеллектуальный кабинет руководителя и применение ситуационных (кризисных) центров.	6	6		33
5	Тема 5: Основы международной информационной безопасности и защита информации в ИКТ системах государственного управления.	6	6		33

	Экспертно-аналитические системы.				
6	Тема 6: Государственная политика Российской Федерации в области международной информационной безопасности.	6	6		33
ИТОГО		**32**	**32**		**197**
6-й семестр					
7	Тема 7: Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы.	4	4		32
8	Тема 8: Стратегическое сотрудничество в области МИБ в рамках международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.)	4	4		33
9	Тема 9: Основные направления развития ИКТ и технологий искусственного интеллекта в дипломатии и международных отношениях.	6	6		33
10	Тема 10: Современные ИКТ, искусственный интеллект и противоборство в информационной сфере: риски и	6	6		33

	угрозы. Искусственный интеллект в гибридных и когнитивно-ментальных войнах современности.				
11	Тема 11: Использование современных ИКТ и технологий ИИ в обеспечении безопасности и обороны страны и тенденции их применения в военных целях (опыт США, Китая, Германии, Японии и др.)	6	6		33
12	Тема 12: Международно-правовая база и инструменты обеспечения международной информационной безопасности.	6	6		33
ИТОГО		**32**	**32**		**197**
ВСЕГО		**64**	**64**		**394**

4.2. Самостоятельное изучение обучающимися разделов дисциплины

Очная форма обучения

Вопросы, выносимые на самостоятельное изучение	**Формы самостоятельной работы**	**Оценочное средство для проверки выполнения самостоятельной работы**
5-й семестр		
Тема 1: Международное информационное общество и проблемы информационного обеспечения безопасности.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 2: Направления в международной информатизации и	Освоение рекомендованной преподавателем и	Устный опрос по темам

основные этапы создания экономических информационных систем и компьютерных систем безопасности.	методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	
Тема 3: Распределенная обработка международной информации и компьютерные сети. Международная компьютерная сеть INTERNET, основные протоколы и адресация в глобальной сети.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 4: Международные информационные системы поддержки деятельности органов государственной власти. Интеллектуальный кабинет руководителя и применение ситуационных (кризисных) центров.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 5: Основы международной информационной безопасности и защита информации в ИКТ системах государственного управления. Экспертно-аналитические системы.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 6: Государственная политика Российской Федерации в области международной информационной безопасности.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
6-й семестр		
Тема 7: Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 8: Стратегическое сотрудничество в области МИБ в рамках международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.)	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 9: Основные направления развития ИКТ и технологий искусственного интеллекта в дипломатии и международных отношениях.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 10: Современные ИКТ, искусственный интеллект и противоборство в информационной сфере: риски и угрозы.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной	Устный опрос по темам

Искусственный интеллект в гибридных и когнитивно-ментальных войнах современности.	и дополнительной учебной литературы	
Тема 11: Использование современных ИКТ и технологий ИИ в обеспечении безопасности и обороны страны и тенденции их применения в военных целях (опыт США, Китая, Германии, Японии и др.)	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам
Тема 12: Международно-правовая база и инструменты обеспечения международной информационной безопасности.	Освоение рекомендованной преподавателем и методическими указаниями по данной дисциплине основной и дополнительной учебной литературы	Устный опрос по темам

Основная цель самостоятельной работы студента при изучении дисциплины «Основы международной информационной безопасности» – закрепить теоретические знания, полученные в ходе лекционных занятий, сформировать навыки в соответствии с требованиями, определенными в ходе занятий семинарского типа.

Подробная информация о видах самостоятельной работы и оценочных средствах для проверки выполнения самостоятельной работы приведена в Методических рекомендациях по самостоятельной работе обучающихся.

5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Образцы заданий текущего контроля и промежуточной аттестации Фонда оценочных средств (ФОС) представлены в Приложении к Рабочей программе дисциплины (модуля) (РПД). В полном объеме ФОС хранится в печатном виде на кафедре, за которой закреплена дисциплина.

6. Перечень нормативных правовых документов, основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1. Нормативные правовые документы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) - URL: http://www.consultant.ru/document/cons_doc_LAW_28399/ (дата обращения: 13.01.2025). - Текст : электронный.
2. Указ Президента Российской Федерации от 31.03.2023 г. № 229 Об утверждении Концепции внешней политики Российской Федерации. - URL: http://www.kremlin.ru/acts/bank/49090 (дата обращения: 24.01.2025). - Текст : электронный.
3. Указ Президента РФ от 02.07.2021 N 400 "О Стратегии национальной безопасности Российской Федерации". - URL:

http://www.kremlin.ru/acts/bank/47046 (дата обращения: 13.01.2025). – Текст : электронный.
4. Указ Президента РФ от 12.04.2021 N 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности") - URL: http://www.kremlin.ru/acts/bank/46614 (дата обращения: 13.01.2025). - Текст : электронный.
5. Указ Президента РФ от 10.10.2019 N 490 (ред. от 15.02.2024) "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") - URL: http://www.kremlin.ru/acts/bank/44731 (дата обращения: 13.01.2025). - Текст : электронный.

6.2. Основная литература

1. Кардашова, И. Б. Основы теории национальной безопасности : учебник для вузов / И. Б. Кардашова. - 3-е изд. - Москва : Юрайт, 2025. - 334 с. - ISBN 978-5-534-15789-5. - URL: https://urait.ru/bcode/563515 (дата обращения: 24.01.2025). - Режим доступа: для авторизир. пользователей. - Текст электронный.
2. Лебедева, М. М. Мировая политика : учебник / М. М. Лебедева. - Москва : КноРус, 2025. - 254 с. - ISBN 978-5-406-14160-1. - URL: https://book.ru/book/956676 (дата обращения: 24.01.2025). - Режим доступа: для авторизир. пользователей. - Текст электронный.
3. Международные отношения и мировая политика : учебник для вузов / под редакцией П. А. Цыганкова. - 2-е изд., перераб. и доп. - Москва : Юрайт, 2025. - 267 с. - ISBN 978-5-534-20564-0. - URL: https://urait.ru/bcode/558389 (дата обращения: 24.01.2025). - Режим доступа : для авторизир. пользователей. - Текст : электронный.

6.3. Дополнительная литература

1. Анненков, В. И. Современные аспекты международной безопасности : учебник / В. И. Анненков, А. В. Моисеев, А. И. Муравых ; под общей редакцией В. И. Анненкова. - Москва : КноРус, 2022. - 395 с. - ISBN 978-5-406-09271-2. - URL: https://book.ru/book/942823 (дата обращения: 24.01.2025). - Режим доступа: для авторизир. пользователей. - Текст электронный.
2. Цифровые международные отношения: учебное пособие. В 2-х тт. Т.1 / под редакцией Е.С. Зиновьевой , С.В. Шитькова. - Москва : Аспект Пресс, 2023. - 354 с. - ISBN 978-5-7567-1252-0. - URL: https://e.lanbook.com/book/364712 (дата обращения: 24.01.2025). - Режим доступа: для авторизир. пользователей. - Текст : электронный.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения, профессиональных баз данных и информационных справочных систем

7.1. Ресурсы информационно-телекоммуникационной сети «Интернет», включая профессиональные базы данных.

1. Министерство иностранных дел: официальный сайт. - Москва. - URL: https://mid.ru/. (дата обращения: 24.01.2025). - Текст : электронный.
2. Правительство Российской Федерации: официальный сайт. - Москва. - Обновляется в течение суток. - URL: http://government.ru (дата обращения: 24.01.2025). - Текст: электронный.
3. Сервер органов государственной власти России: официальный сайт. - Москва. - URL: http://www.gov.ru/. (дата обращения: 24.01.2025). - Текст : электронный.
4. Совет Безопасности Российской Федерации : официальный сайт. - Москва. - URL: http://www.scrf.gov.ru/. (дата обращения: 24.01.2025). - Текст : электронный.
5. Национальная Ассоциация международной информационной безопасности : официальный сайт. - Москва. - URL: https://namib.online/. (дата обращения: 24.01.2025). - Текст : электронный.

7.2. Информационно-справочные системы

СПС КонсультантПлюс. компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

7.3. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства.

Академия обеспечена необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

-Microsoft Office - 2016 PRO (Полный комплект программ: Access, Excel, PowerPoint, Word и т.д);
-Программное обеспечение электронного ресурса сайта Дипломатической Академии МИД России, включая ЭБС; 1С: Университет ПРОФ (в т.ч., личный кабинет обучающихся и профессорско-преподавательского состава);
-Программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» версия 3.3 (отечественное ПО);
-Электронная библиотека Дипломатической Академии МИД России на платформе «МегаПро» - https://elib.dipacademy.ru/MegaPro/Web.;
-ЭБС «Лань» - https://e.lanbook.com/.;
-Справочно-информационная полнотекстовая база периодических изданий «East View» - http://dlib.eastview.com.;
-ЭБС «Университетская библиотека - online» - http://biblioclub.ru.;
-ЭБС «Юрайт» - http://www.urait.ru.;
-ЭБС «Book.ru» - https://www.book.ru/.;
-ЭБС «Znanium.com» - http://znanium.com/;
-ЭБС «IPR SMART» - http://www.iprbookshop.ru/.;
-7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО);
-AIMP Бесплатный аудио проигрыватель (лицензия бесплатного программного

обеспечения) (отечественное ПО);
-Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения);
-Система видеоконференц связи BigBlueButton (https://bbb.dipacademy.ru) (свободно распространяемое программное обеспечение).
-Система видеоконференц связи «Контур.Талк» (отечественное ПО);
- Система видеоконференц связи МТС.Линк (отечественное ПО).

Каждый обучающийся в течение всего обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной системе и электронной информационно-образовательной среде.

8. Описание материально–технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Дисциплина «Основы международной информационной безопасности» обеспечена:

учебной аудиторией для проведения занятий лекционного типа, оборудованной мультимедийными средствами обучения для демонстрации лекций-презентаций, набором демонстрационного оборудования;

учебной аудиторией для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованной учебной мебелью и техническими средствами обучения, служащими для представления учебной информации: (перечислить)

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, обеспечивающей доступ к сети Интернет и электронной информационно-образовательной среде Академии.

.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы дисциплины (модуля), в который внесены изменения

(измененное содержание раздела)

Наименование раздела рабочей программы дисциплины (модуля), в который внесены изменения

(измененное содержание раздела)

Наименование раздела рабочей программы дисциплины (модуля), в который внесены изменения

(измененное содержание раздела)

Рабочая программа дисциплины (модуля):
обновлена, рассмотрена и одобрена на 20___/___ учебный год на заседании кафедры
_____от ____ _____ 20___г., протокол №_____

Приложение к РПД

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Дипломатическая академия Министерства иностранных дел Российской Федерации»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля и промежуточной аттестации по дисциплине (модулю)

«ОСНОВЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 41.03.05 Международные отношения
Направленность (профиль) подготовки: Международные отношения и внешняя политика
Формы обучения: очная
Квалификация выпускника: Бакалавр

Москва

Цель фонда оценочных средств по дисциплине (модулю) (далее ФОС) - установление соответствия уровня сформированности компетенций обучающегося, определенных в ФГОС ВО по соответствующему направлению подготовки и ОПОП ВО.

Задачи ФОС:

– контроль и управление достижением целей реализации ОПОП, определенных в виде набора компетенций выпускников;

– оценка достижений обучающихся в процессе изучения дисциплины с выделением положительных/отрицательных;

– контроль и управление процессом приобретения обучающимися необходимых знаний, умений, навыков, определенных в ФГОС ВО и ОПОП ВО;

– обеспечение соответствия результатов обучения задачам будущей профессиональной деятельности через совершенствование традиционных и внедрение инновационных методов обучения в образовательный процесс Академии.

Оценочные материалы разрабатываются с учетом следующих принципов:

-актуальность (соответствие действующим нормативным правовым актам, отраслевым регламентам, ГОСТ (ам) и т.д.);

-адекватность (ориентированность на цели и задачи ОПОП, дисциплины (модуля), практик, НИР, их содержание);

-валидность (возможность использования для «измерения» сформированности компетенций с целью получения объективных результатов);

-точность и однозначность формулировок (недопущение двусмысленного толкования содержания задания);

-достаточность (обеспечение наличия многовариантности заданий);

-наличие разнообразия методов и форм.

1. Область применения, цели и задачи фонда оценочных средств

Фонд оценочных средств (ФОС) является неотъемлемой частью рабочей программы дисциплины и предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу данной дисциплины.

Рабочей программой дисциплины «Основы международной информационной безопасности» предусмотрено формирование следующих компетенций: УК-5.1; УК-5.2; ПК-2.3; ПК-3.3

2. Показатели и критерии оценивания контролируемой компетенции на различных этапах формирования, описание шкал оценивания

Применение оценочных средств на этапах формирования компетенций

Код и наименование формируемой компетенции	**Код и формулировка индикатора достижения формируемой компетенции**	**Результаты обучения**	**Наименование контролируемых разделов и тем дисциплины (модуля)**	**Наименование оценочного средства**	
				контрольная точка текущего контроля	**промежуточная аттестация**
УК-5 – Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе возникновения чрезвычайных ситуаций и военных конфликтов.	УК-5.1 – Имеет базовые представления о межкультурном разнообразии общества в социально-историческом, этическом и философском контекстах	Знает имеет теоретические и практические знания основ межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах	**5 семестр** Тема 1: Международное информационное общество и проблемы информационного обеспечения безопасности. Тема 2: Направления в международной информатизации и основные этапы создания экономических информационных систем и компьютерных систем безопасности. Тема 3: Распределенная обработка международной информации и компьютерные сети. Тема 4:	**5 семестр** Контрольная работа в виде теста по темам 1-3 **6 семестр** Контрольная работа в виде теста по темам 7-9	**Вопросы для экзаменов 5 и 6 семестр**
	УК-5.2 – Понимает необходимость восприятия и учета межкультурного разнообразия общества в социально-историческом, этическом и философском контекстах	Знает порядок и необходимые условия проведения операций по поддержанию мира. Умеет оценивать подходы, основанные на различных методах обеспечения взаимного сдерживания и идентифицировать разноплановые риски, вызовы и угрозы международной и национальной безопасности			

			Международные информационные		

ПК-2 - Способен ориентироваться в механизмах многосторонней дипломатии и выявлять особенности современной российской политики.	ПК-2.3. Анализирует сложные механизмы многосторонней и интеграционной дипломатии с учетом особенностей их функционирования.	Знать: порядок действий по проведению анализа сложных механизмов многосторонней и интеграционной дипломатии с учетом особенностей их функционирования. Уметь: осуществлять анализ сложных механизмов многосторонней и интеграционной дипломатии с учетом особенностей их функционирования.	системы поддержки деятельности органов государственной власти. Тема 5: Основы международной информационной безопасности и защита информации в ИКТ системах государственного управления. Тема 6: Государственная политика Российской Федерации в области международной информационной безопасности. **6 семестр** Тема 7: Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы. Тема 8:		

ПК-3 - Способен понимать исторические, культурные, географические, экономические, политические, правовые аспекты международных отношений и применять на практике теоретические основы для исследования развития современных государств	ПК-3.3 - Выявляет особенности социально-политических и экономических процессов в мировой политике, закономерности глобальных и региональных политических и экономических процессов и понимает их роль во внешней политике Российской Федерации и других государств	Знать: порядок выявления особенностей социально-политических и экономических процессов в мировой политике, закономерности глобальных и региональных политических и экономических процессов и понимает их роль во внешней политике Российской Федерации и других государств. Уметь: осуществлять действия по выявлению особенностей социально-политических и экономических процессов в мировой политике, закономерности глобальных и региональных политических и экономических процессов и понимать их роль во внешней политике Российской Федерации и других государств.	Стратегическое сотрудничество в области МИБ в рамках международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.) Тема 9: Основные направления развития ИКТ и технологий искусственного интеллекта в дипломатии и международных отношениях. Тема 10: Современные ИКТ, искусственный интеллект и противоборство в информационной сфере: риски и угрозы. Тема 11: Использование современных ИКТ и технологий ИИ в обеспечении безопасности и обороны страны и тенденции их применения в		

			военных целях (опыт США, Китая, Германии, Японии и др.) Тема 12: Международно-правовая база и инструменты обеспечения международной информационной безопасности.		

3. Контрольные задания и материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности (индикаторов достижения компетенций), характеризующих результаты обучения в процессе освоения дисциплины (модуля) и методические материалы, определяющие процедуры оценивания

3.1. Оценочные средства для проведения текущего контроля

5 семестр

Тема 1. Международное информационное общество и проблемы информационного обеспечения безопасности.

1. Международная информационная безопасность как категория и тенденции развития глобального информационного общества.
2. Линии разделения и направления различных политических конфликтов, государства.
3. Планы ведения информационных войн и информационного противоборства.
4. Транснациональная природа информационного общества и формирование ситуации взаимозависимости и импульс международному сотрудничеству по обеспечению информационной безопасности.
5. Основные принципы обеспечения международной информационной безопасности, основные потенциальные и реальные угрозы, основные задачи в области обеспечения международной информационной безопасности.

Тема 2. Направления в международной информатизации и основные этапы создания экономических информационных систем и компьютерных систем безопасности.

1. Основные этапы развития информационных технологий и международной информатизации.
2. Экономические законы развития информационных технологий.
3. Место и роль информационных технологий в условиях формирования информационного общества.
4. Обзор современного состояния и перспектив развития информационных технологий, проблемы их развития.
5. Сегментация рынка информационных технологий и регулирующая деятельность государственных органов, направленная на развитие информационной сферы общества.
6. Классификация информационных угроз и характеристика их последствий, построение системы защиты информации, особенности организации информационной безопасности.

Тема 3. Распределенная обработка международной информации и компьютерные сети.

1. Международная компьютерная сеть INTERNET, основные протоколы и адресация в глобальной сети.
2. Классификация компьютерных сетей. Локальные и глобальные сети.
3. Всемирная паутина и её российский сегмент.
4. Топология сетей.
5. Основные элементы технологии WWW
6. Виды сервиса Интернет.

Тема 4. Международные информационные системы поддержки деятельности органов государственной власти.

1. Интеллектуальный кабинет руководителя и применение ситуационных (кризисных) центров.
2. Принципы построения информационно-аналитических систем (ИАС).
3. Системы информационной поддержки принятия внешнеполитических решений. Ситуационные центры: опыт создания и применения (США, Германии, Франции, России, ЕС и др.).
4. Ситуационно-кризисная дипломатия - цифровые технологии и возможности систем ИИ. Информационно-аналитическое обеспечение внешнеполитического процесса в РФ.

Тема 5. Основы международной информационной безопасности и защита информации в ИКТ системах государственного управления. Экспертно-аналитические системы.

1. Построение информационной безопасности на основе ГОСТ 27 002 и ISO 27032.
2. Модель гонки вооружений.
3. Стратегическая и геоцивилизационная матрицы в долгосрочном макропрограммировании.
4. Зарубежный опыт долгосрочного прогнозирования и стратегического планирования с использованием ИКТ и ИИ.
5. Справочно-правовые и геоинформационные системы.
6. Анализ данных социально-политического характера.
7. Зарубежные центры, занимающиеся проблемами анализа и прогнозирования.

Тема 6. Государственная политика Российской Федерации в области международной информационной безопасности.

1. Основы государственной политики России в области обеспечения международной информационной безопасности. Р

2. Оновные угрозы: использование IT-технологий в военно-политической и иной сферах для подрыва суверенитета государств, нарушения их территориальной целостности, а также в террористических, экстремистских и преступных целях.

Критерии оценивания устного опроса

4-5 баллов	*Сумел четко ответить на все вопросы, убедительно аргументировал выводы, проявил самостоятельность и оригинальность подходов, культуру мышления, использовал все необходимые навыки обобщения и анализа, продемонстрировал знание специальной литературы, способность вести полемику и отстаивать свою точку зрения*
3 балла	*Ответил на все вопросы, вел полемику, отстаивал свою точку зрения, однако не все выводы убедительно аргументировал, не во всех случаях проявил самостоятельность и культуру мышления, в основном опирался на отдельные учебники и учебные пособия*
1-2 балла	*Ответил на часть вопросов, однако аргументировал не все выводы, не проявил самостоятельность и культуры мышления*
0 баллов	*Не сумел ответить ни на один вопрос*

Контрольная работа 5 семестр

Контрольная точка текущего контроля представляет собой тест из 20 вопросов.

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения Безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

15) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

16) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

17) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальность

18) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

19) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной

- Правовой
- Защищаемой

20) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

Критерии оценивания

Контрольная работа в виде теста

Макс. 9-10 баллов (в соответствии с балльно-рейтинговой системой)	*16–20 правильных ответов (80-100 % ответов)*
6-8 баллов	*13-15 правильных ответов (67-79 % ответов)*
3-5 баллов	*10-12 правильных ответов (50-66 % ответов)*
0-2 балла	*0-9 правильных ответов (менее 50% ответов)*

6 семестр

Тема 7. Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы.

1. Институциональный диалог по международной информационной безопасности в ООН: история, состояние, перспективы.
2. Результаты деятельности Первого комитета Генеральной Ассамблеи ООН в процессе решения проблемы международной информационной безопасности (МИБ).
3. Возможности создания международного режима по запрещению информационного оружия.
4. Актуальность и возрастающая важность изучения различных международных процессов со стороны научного сообщества.

Тема 8. Стратегическое сотрудничество в области МИБ в рамках международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.)

1. Деятельность международных организаций (ШОС, БРИКС, ОДКБ, ОБСЕ, АТЭС и др.) в сфере безопасности.
2. Государства-участники международных организаций имеющие общие цели и интересы, а также сходные стратегические задачи по укреплению

международного сотрудничества в сфере международной информационной безопасности.

Тема 9. Основные направления развития ИКТ и технологий искусственного интеллекта в дипломатии и международных отношениях.

1. Дипломатия 2.0 и 3.0 – зарубежный опыт и геополитические вызовы современности. Глобальные социальные сети и МИБ.
2. Роль международных организаций в управлении Интернетом.
3. Экстраполяция тенденций и компьютерные методики анализа общественно-политических процессов.
4. Практико-ориентированные подходы по повышению эффективности и безопасности при работе с технологиями искусственного интеллекта.

Тема 10. Современные ИКТ, искусственный интеллект и противоборство в информационной сфере: риски и угрозы. Искусственный интеллект в гибридных и когнитивно-ментальных войнах современности.

1. Теоретические подходы к информационной борьбе (информационному противоборству).
2. Основное различие между кибербезопасностью и международной информационной безопасностью.
3. Национальная Стратегия развития искусственного интеллекта до 2030.
4. Новые направления борьбы в информационной сфере, как кибернетический терроризм и информационно-психологическое противоборство.
5. Эволюция термина «стратегическая коммуникация» в доктринах Министерства обороны США и НАТО.
6. Потенциальные возможности и функции искусственного интеллекта в применении к стратегическим коммуникациями.

Тема 11. Использование современных ИКТ и технологий ИИ в обеспечении безопасности и обороны страны и тенденции их применения в военных целях (опыт США, Китая, Германии, Японии и др.)

1. Основные вызовы и угрозы использования современных информационно-коммуникационных технологий и систем искусственного интеллекта в военной сфере.
2. Обзор стратегий развития и управления искусственным интеллектом ведущих стран мира (США, Великобритания, Россия, ЕС, Китай, Франция, Германия, Южная Корея и др.).

Тема 12. Международно-правовая база и инструменты обеспечения международной информационной безопасности.

1. Вопросы международной информационной безопасности.

2. Международное сотрудничество в области поддержания международной информационной безопасности.
3. Будапештская конвенция и российские инициативы по совершенствованию международно-правового сотрудничества в области информационной безопасности.

Критерии оценивания устного опроса

4-5 баллов	*Сумел четко ответить на все вопросы, убедительно аргументировал выводы, проявил самостоятельность и оригинальность подходов, культуру мышления, использовал все необходимые навыки обобщения и анализа, продемонстрировал знание специальной литературы, способность вести полемику и отстаивать свою точку зрения*
3 балла	*Ответил на все вопросы, вел полемику, отстаивал свою точку зрения, однако не все выводы убедительно аргументировал, не во всех случаях проявил самостоятельность и культуру мышления, в основном опирался на отдельные учебники и учебные пособия*
1-2 балла	*Ответил на часть вопросов, однако аргументировал не все выводы, не проявил самостоятельность и культуры мышления*
0 баллов	*Не сумел ответить ни на один вопрос*

Контрольная работа 6 семестр

Контрольная точка текущего контроля представляет собой тест из 20 вопросов.

1. Какое определение соответствует понятию «военная угроза».

а) наличие острых противоречий, разрешение которых возможно с применением военной силы;

б) состояние защищенности от угроз ключевым ценностям и интересам человечества.

в) состояние межгосударственных или внутригосударственных отношений, характеризуемое реальной возможностью возникновения военного конфликта между противостоящими сторонами, высокой степенью готовности какого-либо государства (группы государств), сепаратистских (террористических) организаций к применению военной силы (вооруженному насилию).

г) совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

2. Какое определение соответствует понятию «военная опасность».

а) это совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства;

б) состояние межгосударственных или внутригосударственных отношений, характеризуемое совокупностью факторов, способных при определенных условиях привести к возникновению военной угрозы;

в) демонстрация готовности совершить насилие для причинения ущерба;

г) это вполне осознаваемая, но не фатальная вероятность нанесения ущерба интересам общества.

3. Какое определение наиболее полно соответствует понятию «международная безопасность».

а) это готовность мирового сообщества адекватно оценить возникающие перемены в природе, обществе, экономике, идеологии, технике и технологии, обеспечив тем самым собственную трансформацию без скачков, потрясений и революций;

б) состояние защищенности от угроз ключевым ценностям и интересам человека, государства, международного сообщества;

в) это защищенность устойчивого существования и прогрессивного развития мирового сообщества, предполагающая предупреждение, предотвращение и нейтрализацию опасных (кризисных) состояний, создающих угрозу существованию этих субъектов;

г) система международных отношений, основанная на соблюдении всеми государствами общепризнанных принципов и норм международного права, исключающую решение спорных вопросов и разногласий между ними с помощью силы или угрозы.

4. Представителями какой школы являются американцы Дж.Най и Р.Кохэн.

а) школы реалполитики;

б) школы либералполитики;

в) школы демократического мира;

г) школа посмодернизма;

д) школа конструктивизма;

е) школа неореализма.

5. К какой концепции относится следующее положение: «на смену конфликтов между государствами-нациями приходят конфликты между цивилизациями, которые определяются как группы государств и народов, имеющие родственные культурные характеристики: религию, общую историю, этничность, моральные ценности, образ жизни.

а) концепция конца истории;

б) концепция столкновения цивилизаций;

в) концепция постмодернизма;

г) мир-системная концепция;

д) концепция конструктивизма.

6. По мнению С.Бжезинского, ключевые позиции в предотвращении угрозы реставрации «Российской империи» на постсоветском геополитическом пространстве занимают:

а) Белоруссия, Молдавия, Украина;

б) Эстония, Латвия, Литва;

в) Грузия, Азербайджан, Армения;

г) Украина, Узбекистан, Азербайджан.

7. Какие три центра силы выделял И. Валлерстайн в своем мир-системном анализе?

а) США, Япония, Европа;

б) США, Китай, Россия;

в) США, Китай, Европа;

г) США, Россия, Европа.

8. Кто был разработчиком школы, основные идеи которой выражаются следующими тезисами: «основной закон политики: силовые отношения между государствами являются определяющими при решении международных проблем; мощь государства определяет уровень силового воздействия на другие страны в кризисных ситуациях…».

а) Дж.Най и Р.Кохэн;

б) Г.Моргентау, К.К.Норр;

в) Д.Бабст, М.Дойл, Б.Рассел;

г) Ж.-Ф. Лиотар, С.Турен.

9. Что относится к скрытым формам насилия?

а) учения у границ сопредельного государства с целью оказать на него давление; военно-морская блокада портов;

б) помощь в организации военного переворота; демонстрация военной силы;

в) продажа, передача, поставки оружия за рубеж, хранение его на территории других стран; оказание помощи государствам в разработке военных доктрин, создании и развитии вооруженных сил, а также военными специалистами;

г) вооруженный террор; военные перевороты; военная блокада.

10. Основные структурные элементы военной силы.

а) военная мощь государства, военная инфраструктура, военно-экономическая сила;

б) вооруженные силы, военно-экономическая сила, военная инфраструктура;

в) вооруженные силы, военно-научная сила, военно-экономическая сила, моральная сила народа, воинов вооруженных сил;

г) вооруженные силы, военная инфраструктура, военно-научная сила, моральная сила народа, воинов вооруженных сил.

11. Что относится к первому типу операционных моделей международной безопасности?

а) коллективная безопасность, «концерт держав», кооперационная безопасность, многополярная модель;

б) однополярная система безопасности, «концерт держав», многополярная модель, глобальная (универсальная) модель;

в) «концерт держав», кооперационная безопасность, глобальная (универсальная) модель;

г) однополярная система безопасности, «концерт держав», кооперационная безопасность, многополярная модель, всеобщая безопасность.

12. Что относится ко второму типу операционных моделей международной безопасности?

а) коллективная безопасность, кооперационная безопасность, «концерт держав»;

б) однополярная система безопасности, коллективная безопасность, глобальная безопасность;

в) коллективная безопасность, кооперационная безопасность, всеобщая безопасность;

г) коллективная безопасность, всеобщая безопасность, кооперационная безопасность.

13. Какой из регионов является наиболее угрозоемким?

а) Африканский;

б) Азиатско-Тихоокеанский;

в) Ближний и Средний Восток;

г) Латинская Америка.

14. Какой из регионов является наименее угрозоемким?

а) Европейский;

б) Латинская Америка;

в) Евразийское постсоветское пространство;

г) Африканский.

15. Кто из перечисленных американских специалистов является теоретиком «управляемого хаоса»

а) Грант Хэммонд;

б) Мартин Кревельд;

в) Джон Шинн;

г) Стивен Манн.

16. Что не относится к информационному ресурсу?

а) массивы документированной информации (документов);

б) информационные каналы;

в) системы коммутации;
г) информационные системы;

17. Сколько стран-членов НАТО?
а) 29;
б) 31;
в) 30;
г) 32.

18. Сколько подсистем ядерного мира?
а) 9;
б) 8;
в) 10;
г) 7.

19. В чем заключается смысл критерия Макнамары?
а) в сохранении возможности нанесения неприемлемого ущерба любому агрессору в процессе обмена ядерными ударами в ответно-встречных действиях;
б) в наличии ядерного потенциала, способного нанести неприемлемый ущерб любому агрессору;
в) в сохранении возможности нанести неприемлемый ущерб любому агрессору в процессе обмена ядерными ударами;
г) в сохранении способности нанесения неприемлемого ущерба любому агрессору в процессе обмена ядерными ударами в ответных действиях.

20. Что не входит в комплексную концепцию неядерного сдерживания?
а) концепция глобального сдерживания;
б) концепция сдерживания за счет системы стратегической обороны (противоракетная оборона, противокосмическая оборона, противовоздушная оборона);
в) концепция информационного сдерживания;
г) концепция сдерживания на основе совершенствования международного права и системы обеспечения международной безопасности.

Критерии оценивания

Контрольная работа в виде теста

Макс. 9-10 баллов (в соответствии с балльно-рейтинговой системой)	*16–20 правильных ответов (80-100 % ответов)*
6-8 баллов	*13-15 правильных ответов (67-79 % ответов)*

3-5 баллов	*10-12 правильных ответов (50-66 % ответов)*
0-2 балла	*0-9 правильных ответов (менее 50% ответов)*

3.2. Оценочные средства для проведения промежуточной аттестации

В качестве оценочного средства для проведения промежуточной аттестации по дисциплине используется: *Экзамены в устной форме*

№ п/п	Форма контроля	Форма и условия проведения промежуточной аттестации	Представление оценочного средства в фонде
1.	Экзамен	Экзамен в устной форме. *Экзаменационный билет состоит из 2 вопросов*	Перечень вопросов к экзамену
2.	Экзамен	*Экзамен в устной форме. Экзаменационный билет состоит из 2 вопросов*	Перечень вопросов к экзамену

Перечень вопросов к экзамену 5 семестр

1. Сущность и характеристика видов безопасности.
2. Основные принципы международной безопасности.
3. Существующие угрозы международной безопасности, цель и основные задачи по ее обеспечению.
4. Основные положения школы реалполитики.
5. Основные положения школы либералполитики.
6. Сущность и содержание школы демократического мира.
7. Основные положения концепции столкновения цивилизаций.
8. Особенности концепций постмодернизма и «конца истории» Ф.Фукуямы.
9. Характеристика геополитических концепций З.Бжезинского.
10. Сущность и содержание мир-системного анализа И.Валлерстайна.
11. Конструктивистская школа: идеи и нормы, которые влияют на международные отношения и международную безопасность.
12. Неореалистическая школа и её подход к международным отношениям и международной безопасности.
13. Основная критика существующих школ и современные подходы к международной безопасности.
14. Характеристика международной безопасности в свете «баланса сил» и «баланса интересов».
15. Военный потенциал государства (потенциальная военная мощь). Военная сила государства. Сущность и виды вооруженного насилия государства.
16. Характеристика скрытых форм насилия,

17.Основные структурные элементы и функции военной силы.
18.Характеристика моделей международной безопасности, относящихся к первому типу.
19.Характеристика моделей международной безопасности, относящихся ко второму типу.
20.Сущность и содержание глобальной безопасности.
21.Характеристика региональной безопасности. Значение субрегионального подуровня в обеспечении региональной безопасности.
22.Характеристика угрозоемкости регионов мира.
23.Современные подходы к понятию войны и мира.
24.Характеристика источников и причин войн.
25.Определение целей войны, навязывание своей воли, проблема убийства людей на войне.

Перечень вопросов к экзамену 6 семестр

1. Характеристика этапов и поколений войн.
2. Особенности войн шестого поколения.
3. Эволюция технологий войн, особенности системно-сетевой войны.
4. Особенности войн будущего.
5. Ядерный мир, характеристика его подсистем и ядерных связей.
6. Структурное построение ядерного мира, системные свойства ядерного мира.
7. Стратегическая стабильность, основные факторы, влияющие на стратегическую стабильность, факторы, повышающие и снижающие уровень стратегической стабильности, оценка уровня стратегической стабильности.
8. Ядерное сдерживание, его цель и сущность, критерий Макнамара, глобальное и региональное ядерное сдерживание.
9. Стратегическая ядерная стабильность, военно-стратегическое равновесие, определение запасов устойчивости равновесия, подходы, основанные на различных методах обеспечения взаимного сдерживания.
10. Современные концепции ядерного сдерживания, трансформация концепции ядерного сдерживания, комплексная концепция неядерного сдерживания.
11. Характеристика Промежуточной стратегии США по национальной безопасности от 4.03.2021 г., выпущенная администрацией Дж. Байдена.
12. Характеристика Комплексного обзора оборонной и внешней политики Великобритании до 2030 года, выпущенной 17.03.2021 г.
13. Современные концепции национальной безопасности Франции: «Стратегический обзор по вопросам обороны и национальной безопасности Франции» 2017 года, «Программа развития вооруженных сил Франции на 2019-2025 годы».
14. Белая книга политики безопасности Германии и будущего Бундесвера.
15. Теоретические подходы к терминологии в сфере информационного противоборства (информационной борьбы).

16. Сущность современного информационного противоборства, стратегическая цель информационной войны, информационно-психологическое противоборство и стратегические коммуникации в доктринах Министерства обороны США, НАТО и ЕС.
17. Проблемные аспекты реализации государственной политики России в области информационного противоборства и необходимые шаги в создании эффективной отечественной системы информационной безопасности.
18. Новые информационные технологии, применяемые Западом (США и НАТО) в борьбе против России и других государств.
19. Стратегии развития и управления искусственным интеллектом ведущих стран мира (США, Великобритания, Россия, ЕС, Китай, Франция, Германия, Южная Корея и др. – по выбору).
20. Основные подходы к сущности миротворчества, характеристика, особенности и признаки субъектов и объекта миротворчества, содержание мандата миротворческой миссии, органы, уполномоченные его выдавать.
21. Принципы миротворчества, вооруженное насилие в миротворчестве, подходы к классификации миротворчества.
22. Характеристика превентивной дипломатии и миростроительства как форм миротворческой деятельности
23. Общая характеристика миротворческих миссий. Примеры организации миротворческих миссий,
24. Характеристика операций по поддержанию мира. Примеры организации операций по поддержанию мира.
25. Характеристика операций по восстановлению мира.

Критерии оценивания (экзамен)
Каждый вопрос равнозначен
Максимально оценивается в 30 баллов

(28-30 баллов) ставится в том случае, когда обучающийся обнаруживает систематическое и глубокое знание программного материала по дисциплине, умеет свободно ориентироваться в вопросе. Ответ полный и правильный на основании изученного материала. Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный. Обучающийся уверенно отвечает на дополнительные вопросы.

(19-27 баллов) ставится в том случае, когда обучающийся обнаруживает полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения.

Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Обучающийся испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, литературным языком.

(10-19 баллов) ставится в том случае, когда обучающийся обнаруживает знание основного программного материала по дисциплине, но допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; ответ носит преимущественно описательный характер. испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.

(менее 10 баллов) ставится в том случае, когда обучающийся не обнаруживает знание основного программного материала по дисциплине, допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные понятия употреблены неправильно, обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; испытывает достаточные трудности в ответах на вопросы. Научная терминология используется недостаточно.

По окончании процедуры промежуточной аттестации производится перевод баллов в традиционную систему оценивания с учетом баллов, полученных за мероприятия текущего контроля, и промежуточной аттестации.

Результатом освоения дисциплины *«Основы международной информационной безопасности»* является установление одного из уровней сформированности компетенций: высокий (продвинутый), хороший, базовый, недостаточный.

Показатели уровней сформированности компетенций

Уровень/балл	**Универсальные компетенции**	**Профессиональные компетенции**
Высокий (продвинутый) (оценка «отлично», «зачтено») **86-100**	Сформированы четкие системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные и верные. Даны развернутые ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции	Обучающимся усвоена взаимосвязь основных понятий дисциплины, в том числе для решения профессиональных задач. Ответы на вопросы оценочных средств самостоятельны, исчерпывающие, содержание вопроса/задания оценочного средства раскрыто полно, профессионально, грамотно. Даны ответы на дополнительные вопросы. Обучающимся продемонстрирован высокий уровень освоения компетенции
Хороший (оценка «хорошо», «зачтено») **71-85**	Знания и представления по дисциплине сформированы на повышенном уровне. В ответах на вопросы/задания оценочных средств изложено понимание вопроса, дано достаточно подробное описание ответа, приведены и раскрыты в тезисной форме основные понятия. Ответ отражает полное знание материала, а также наличие, с незначительными пробелами, умений и навыков по изучаемой дисциплине. Допустимы единичные негрубые ошибки. Обучающимся продемонстрирован повышенный уровень освоения компетенции	Сформированы в целом системные знания и представления по дисциплине. Ответы на вопросы оценочных средств полные, грамотные. Продемонстрирован повышенный уровень владения практическими умениями и навыками. Допустимы единичные негрубые ошибки по ходу ответа, в применении умений и навыков
Базовый (оценка «удовлетворительно», «зачтено») **56-70**	Ответ отражает теоретические знания основного материала дисциплины в объеме, необходимом для дальнейшего освоения ОПОП. Обучающийся допускает неточности в ответе, но обладает необходимыми знаниями для их устранения. Обучающимся продемонстрирован базовый уровень освоения компетенции	Обучающийся владеет знаниями основного материал на базовом уровне. Ответы на вопросы оценочных средств неполные, допущены существенные ошибки. Продемонстрирован базовый уровень владения практическими умениями и навыками, соответствующий минимально необходимому уровню для решения профессиональных задач
Недостаточный (оценка	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие	Демонстрирует полное отсутствие теоретических знаний материала дисциплины, отсутствие практических умений и

Уровень/балл	Универсальные компетенции	Профессиональные компетенции
«неудовлетворительно», «не зачтено») **Менее 56**	практических умений и навыков	навыков

Обновление фонда оценочных средств

Наименование раздела фонда оценочных средств, в который внесены изменения

(измененное содержание раздела)

Наименование раздела фонда оценочных средств, в который внесены изменения

(измененное содержание раздела)

Наименование раздела фонда оценочных средств, в который внесены изменения

(измененное содержание раздела)

Фонд оценочных средств в составе Рабочей программы дисциплины: обновлен, рассмотрен и одобрен на 20___/___ учебный год на заседании кафедры _____от ____ _____ 20___г., протокол №_____