МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ»
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПРОСВЕЩЕНИЯ)

Факультет истории, политологии и права
Кафедра политологии и права

Согласовано
деканом факультета истории,
политологии и права
« 26 » 03 2025 г.
/Багдасарян В.Э./

Рабочая программа дисциплины
Политика информационной безопасности

Направление подготовки
41.03.04 Политология

Профиль:
Политика и национальная безопасность

Квалификация
Бакалавр

Форма обучения
Очная

Согласовано учебно-методической комиссией факультета истории, политологии и права
Протокол « 26 » 03 2025 г. № 6
Председатель УМКом
/Куренкова Е.А./

Рекомендовано кафедрой политологии и права
Протокол от « 24 » 02 2025 г. № 7
Зав. кафедрой
/Лескова И.В./

Москва
2025

Автор-составитель:
Абрамова Ю.А., кандидат исторических наук, доцент

Рабочая программа дисциплины «Политика информационной безопасности» составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 41.03.04 Политология, утвержденного приказом МИНОБРНАУКИ РОССИИ от 23.08.2017 г. № 814.

Дисциплина входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» и является элективной дисциплиной.

Год начала подготовки (по учебному плану) 2025

СОДЕРЖАНИЕ

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

1.1. Цель и задачи дисциплины

Изучение дисциплины «Политика информационной безопасности» является элементом формирования у студентов, будущих специалистов в области политики и национальной безопасности, знаний и навыков, необходимых для профессиональной деятельности.

В результате изучения данной дисциплины у обучающихся должна сформироваться система знаний, умений и навыков в области информационной безопасности: знать, уметь выявлять и противодействовать источникам информационных угроз и рисков как в профессиональной деятельности, так и в повседневной жизни; определять степень их влияния на политический процесс.

Цель освоения дисциплины – сформировать представление об информационной составляющей системы национальной безопасности, об источниках угроз в данной сфере, о роли информационных войн в политической жизни; выработать умение выявлять риски развития информационного общества и ИИ, коммуникативных процессов, а также деструктивного воздействия на индивидуальное и массовое сознание; способствовать выработке умения минимизировать негативное воздействие и разрабатывать комплекс мер в области политики информационной безопасности.

Задачи дисциплины:

- сформировать представление о национальных интересах и стратегических приоритетах России, о Стратегии национальной безопасности РФ, ее компонентах и особенностях;
- сформировать представление об информационной безопасности как составляющей национальной безопасности;
- сформировать представление об информационных и ментальных войнах в политической жизни общества;
- сформировать представление о государственной политике в сфере информационной безопасности;
- сформировать представление о проблемах информационного общества;
- развить психологическую устойчивость к деструктивной коммуникации, связанной с информационными процессами;
- сформировать умение защищать сознание от негативного воздействия со стороны деструктивных (националистических, террористических, экстремистских и других) сил;
- научить выявлять и прогнозировать риски в информационном поле, а также минимизировать или предотвращать их;
- сформировать умение проводить информационную компанию по популяризации способов защиты от манипуляционного и деструктивного влияния во всех сферах, связанных с информацией.

1.2. Планируемые результаты обучения

В результате освоения данной дисциплины у обучающихся формируются следующие компетенции:

СПК-1. Способен владеть знаниями о коммуникативных процессах, каналах массовой коммуникации, средствах массовой информации, особенностях их функционирования в современном мире.

СПК-2. Способен участвовать в информационно-коммуникационных процессах разного уровня, в проведении информационных кампаний.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина входит в часть, формируемую участниками образовательных отношений, Блока 1 «Дисциплины (модули)» и является элективной дисциплиной.

Курс «Политическая символика» предполагает наличие предварительной базовой подготовки по обществознанию и дисциплинам исторического направления (История России и Всеобщая история) в среднем образовательном учреждении.

Для освоения дисциплины студенты используют знания, умения, навыки, сформированные в ходе освоения дисциплин: «Безопасность жизнедеятельности», «Основы финансово-экономической грамотности», «Основы права», «Политическая история России» при параллельном изучении «Информатики».

Освоение данной дисциплины является необходимым и эффективным основанием для изучения «Теория национальной безопасности», «Политические технологии в киберпространстве», «Теория и практика политической пропаганды», «Духовная и психологическая безопасность России», «Технологии искусственного интеллекта в политическом процессе», «Современная российская политика»,

Курс «Политика информационной безопасности» позволяет развить политическое мышление и учит анализировать политические процессы и отношения. Он опирается на знания и умения, полученные при освоении других дисциплин, но одновременно является базой для изучения смежных научных направлений, что позволяет студентам использовать накопленные знания о политике для анализа и обобщения.

3.ОБЪЕМ И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем дисциплины

Показатель объема дисциплины	**Формы обучения**
	Очная
Объем дисциплины в зачетных единицах	4
Объем дисциплины в часах	144
Контактная работа	38,3
Лекции	12
Практические занятия	24
Из них, в форме практической подготовки	24
Контактные часы на промежуточную аттестацию:	0,3
Экзамен	0,3
Предэкзаменационная консультация	2
Самостоятельная работа	96
Контроль	9,7

Форма промежуточной аттестации – экзамен в 3 семестре

3.2. Содержание дисциплины

Наименование разделов (тем) Дисциплины с кратким содержанием	**Кол-во часов**		
	Лекции	**Практические занятия**	
		Общее количество	**Из них, в форме практической подготовки**

Тема 1. Политика информационной безопасности как учебная дисциплина. Национальная безопасность России. Объект, предмет, цель, задачи, основные методы дисциплины и ее основные категории. Определение термина «безопасность» в политологии. Классическая трактовка. Т. Гоббс «Левиафан». А. Волферс. Д. Болдвин. Конструктивистская трактовка. Секьюритизация безопасности. Переосмысление понятия «безопасность» в постбиполярный период. Виды безопасности. Объекты безопасности. Безопасность как инструмент управления. «Театр безопасности». Основные подходы к пониманию категории «нация». Национальная безопасность России: понятие и компоненты. Стратегия национальной безопасности России 2021 г. и ее особенности в сравнении с предыдущими Концепциями (1997 г., 2000 г.) и Стратегиями (2009 г., 2015 г.). Трактовки понятия «информационная безопасность». Понятие «защита информационной безопасности». Информационная безопасность как компонент национальной безопасности. Информация как объект защиты: понятие, уровни представления информации, свойства, шкала ценности информации, виды защищаемой информации (государственная тайна, персональные данные, коммерческая тайна, служебная тайна, профессиональная тайна, процессуальная тайна). Интеллектуальная собственность и особенность ее защиты.	4	8	8

Тема 2. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности. Основные этапы развития российского законодательства в сфере информационной безопасности. 1 этап. 1990-е гг. Оформление законодательной базы. Конституция РФ (1993 г.). ФЗ «Об информации, информатизации и защите информации» (1995 г.). Законы о «Государственной тайне» (1993 г., 1997 г.). Указ о перечне сведений конфиденциального характера (1997 г.). 2 этап. 2000-2016 гг. Формирование основных направлений развития российского законодательства в области информационной безопасности. Доктрины информационной безопасности личности РФ (2000 г.). ФЗ «О коммерческой тайне» (2004 г.), ФЗ «Об информации, информационных технологиях и о защите информации» (2006 г.) ФЗ «О персональных данных». Стратегия развития информационного общества в РФ (2008 г.) Доктрина информационной безопасности РФ (2016 г.). 3 этап. С 2016 г. по настоящее время. Приведение законодательства в соответствие с уровнем развития информационных технологий. Новые редакции ФЗ «Об информации, информационных технологиях и о защите информации» (2006 г.). ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (2020 г.). Органы обеспечения информационной безопасности и защиты информации, их задачи и функции. Особенности политики национальной безопасности США, Франции, Германии, Канады, Китая.	4	8	8

Тема 3. Угрозы информационной безопасности и их классификация. Уровень развития информационных технологий в России. Угрозы информационной безопасности и их классификация. Субъекты информационного противоборства. Причины, виды, каналы утечки и искажения информации. Компьютерная система как объект информационной войны. Методы защиты от несанкционированного доступа. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Криптографические методы.	2	4	4
Тема 4. Психологическая война. Соотношение понятий: «психологические», «ментальные» и информационно-психологические» войны. Проблемы и угрозы, связанные с развитием информационного общества. Технологии психологического, в т.ч. информационно-психологического, воздействия. Пропаганда. «Новая холодная война». Подмена ценностей. Конструирование и деконструирование системы идентичностей. Технологии дегероизации и расчеловечивания. Провоцирование и управление массовыми фобиями. Провоцирование межэтнических и межконфессиональных конфликтов. «Мягкая», «жесткая» и «умная» силы. Антироссийские исторические и политические мифы. Гибридные войны и «цветные революции». «Информационный каскад». Способы противодействия.	2	4	4
Итого	12	24	24

ПРАКТИЧЕСКАЯ ПОДГОТОВКА

Тема	Задание на практическую подготовку	Количество часов
Тема 1. Политика информационной безопасности как	Организация и проведение политических дебатов	8

учебная дисциплина. Национальная безопасность России.		
Тема 2. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	Публикация статей, пресс-релизов и других материалов для медиа, учитывая специфику различных форматов и целевых аудиторий	8
Тема 3. Угрозы информационной безопасности и их классификация.	Разработка эффективных стратегических коммуникаций для политических кампаний	4
Тема 4. Психологическая война.	Исследование общественного мнения. Проведение опросов и фокус-групп для изучения общественного мнения по политическим вопросам	4
Итог		24

4.УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Темы для самостоятельного изучения	Изучаемые вопросы	Кол-во часов	Формы самостоятельной работы	Методическое обеспечение	Формы отчетности

Тема 1. Политика информационной безопасности как учебная дисциплина. Национальная безопасность России.	1. Объект, предмет, цель, задачи, основные методы дисциплины. 2. Определение понятия «безопасность» в политологии. Классическая трактовка. Т. Гоббс «Левиафан». А. Волферс. Д. Болдвин. Конструктивистская трактовка. Секьюритизация безопасности. Переосмысление понятия «безопасность» в постбиполярный период. 3. Виды безопасности. 4. Объекты безопасности. Безопасность как инструмент управления. «Театр безопасности». 5. Основные подходы к пониманию категории «нация». 6. Национальная безопасность России: понятие и компоненты. 7. Стратегия национальной безопасности России 2021 г. и ее особенности в сравнении с предыдущими Концепциями (1997 г., 2000 г.) и Стратегиями (2009 г., 2015 г.). 8. Трактовки понятия «информационная безопасность». Понятие «защита информационной безопасности». Информационная безопасность как компонент национальной безопасности. 9. Информация как объект защиты: понятие, уровни представления информации, свойства, шкала ценности информации, виды защищаемой информации (государственная тайна, персональные данные, коммерческая тайна, служебная тайна, профессиональная тайна, процессуальная тайна). Интеллектуальная собственность и особенность ее защиты.	32 10	Анализ источников и литературы по теме. Подготовка к практическому занятию	Основная и дополнительная литература, интернет-источники	Устный опрос, доклад, реферат, презентация

Тема 2. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности.	1. Основные этапы развития российского законодательства в сфере информационной безопасности. 1-й этап. 1990-е гг. Оформление законодательной базы. Конституция РФ (1993 г.). ФЗ «Об информации, информатизации и защите информации» (1995 г.). Законы о «Государственной тайне» (1993 г., 1997 г.). Указ о перечне сведений конфиденциального характера (1997 г.). 2. 2-й этап. 2000-2016 гг. Формирование основных направлений развития российского законодательства в области информационной безопасности. Доктрины информационной безопасности личности РФ (2000 г.). ФЗ «О коммерческой тайне» (2004 г.), ФЗ «Об информации, информационных технологиях и о защите информации» (2006 г.) ФЗ «О персональных данных». Стратегия развития информационного общества в РФ (2008 г.) Доктрина информационной безопасности РФ (2016 г.). 3. 3-й этап. С 2016 г. по настоящее время. Приведение законодательства в соответствие с уровнем развития информационных технологий. Новые редакции ФЗ «Об информации, информационных технологиях и о защите информации» (2006 г.). ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (2020 г.). 4. Органы обеспечения информационной безопасности и защиты информации, их задачи и функции. 5. Особенности политики	32 11	Анализ источников и литературы по теме. Подготовка к практическому занятию	Основная и дополнительная литература, интернет-источники	Устный опрос, доклад, реферат, презентация

Тема 3. Угрозы информационной безопасности и их классификация.	1. Уровень развития информационных технологий в России. Угрозы информационной безопасности и их классификация. 2. Субъекты информационного противоборства. 3. Причины, виды, каналы утечки и искажения информации. 4. Компьютерная система как объект информационной войны. 5. Методы защиты от несанкционированного доступа. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Криптографические методы.	16	Анализ источников и литературы по теме. Подготовка к практическому занятию	Основная и дополнительная литература, интернет-источники	Устный опрос, доклад, реферат, презентация

Тема 4. Психологическая война.	1. Соотношение понятий: «психологические», «ментальные» и информационно-психологические» войны: трактовки содержания понятий. 2. Проблемы и угрозы, связанные с развитием информационного общества. 3. Технологии психологического, в т.ч. информационно-психологического, воздействия. 4. Пропаганда. «Новая холодная война». Подмена ценностей. Конструирование и деконструирование системы идентичностей. Технологии дегероизации и расчеловечивания. 5. Провоцирование и управление массовыми фобиями. 6. Провоцирование межэтнических и межконфессиональных конфликтов. 7. «Мягкая», «жесткая» и «умная» силы. Антироссийские исторические и политические мифы. Гибридные войны и «цветные революции». Способы противодействия.	16	Анализ источников и литературы по теме. Подготовка к практическому занятию	Основная и дополнительная литература, интернет-источники	Устный опрос, доклад, реферат, презентация
Итого:		96			

5.ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

5.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код и наименование компетенции	Этапы формирования компетенции
СПК-1. Способен владеть знаниями о коммуникативных процессах, каналах массовой коммуникации, средствах массовой информации,	1. Работа на учебных занятиях

особенностях их функционирования в современном мире	2. Самостоятельная работа
СПК-2. Способен участвовать в информационно-коммуникационных процессах разного уровня, в проведении информационных кампаний.	1. Работа на учебных занятиях 2. Самостоятельная работа

5.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оцениваемые компетенции	Уровень сформированности	Этап формирования	Показатели	Критерии оценивания	Шкала оценивания
СПК-1	Пороговый	Работа на учебных занятиях Самостоятельная работа	**Знать:** - содержание терминов «безопасность» и «нация»; - главные национальные интересы и приоритеты России; - компоненты Стратегии национальной безопасности РФ; - виды защищаемой информации; - содержание терминов «психологическая война», «ментальная война» и «информационно-психологическая война»; - главные проблемы современного информационного общества; - основные элементы госполитики в сфере информационной безопасности. **Уметь:** - защищать сознание от негативного воздействия со стороны деструктивных сил; - защищать информацию от несанкционированного доступа.	Устный опрос	Шкала оценивания устного опроса
	Продвинутый	Работа на учебных занятиях Самостоятельная работа	**Знать:** - разные подходы к пониманию термина «безопасность» в политологии; - основные подходы к пониманию термина «нация»; - национальные интересы и приоритеты России; - компоненты и особенности Стратегии национальной безопасности РФ; - виды защищаемой информации; - содержание и соотнесение терминов «психологическая война», «ментальная война» и «информационно-психологическая война»; а также их роль в политической жизни общества; - проблемы современного информационного общества; - основные элементы госполитики в	Устный опрос, доклад, реферат, презентация, практическая подготовка	Шкала оценивания устного опроса; шкала оценивания доклада; шкала оценивания реферата; шкала оценивания презентации; шкала оценивания практическ

			сфере информационной безопасности; - основные принципы проведения контрпропаганды как в реальности, так и в сети Интернет. **Уметь:** - защищать сознание от негативного воздействия со стороны деструктивных (националистических, террористических, экстремистских и других) сил; - проводить информационную компанию по популяризации способов защиты от манипуляционного и деструктивного влияния во всех сферах, связанных с информацией; - защищать информацию от несанкционированного доступа. **Владеть**: - навыком выявлять и прогнозировать риски в информационном поле, а также минимизировать или предотвращать их.		ой подготовки.
СПК-2	Пороговый		**Знать:** - особенности Стратегии национальной безопасности РФ; - основные виды защищаемой информации; - методы «психологической войны» и «информационно-психологической войны»; - основные угрозы современного информационного общества и ИИ; - базовые элементы госполитики в сфере информационной безопасности. **Уметь:** - защищать сознание от ключевых элементов негативного воздействия со стороны деструктивных сил; - проводить информационную компанию по популяризации способов защиты от манипуляционного и деструктивного влияния во всех сферах, связанных с информацией; - организовывать и проводить кампании по защите информации.	Устный опрос	Шкала оценивания устного опроса
	Продвинутый		**Знать:** - особенности Стратегии национальной безопасности РФ 2021 г. в сравнении с др. Стратегиями (Концепциями) НБ; - виды защищаемой информации; - методы «психологической войны», «ментальной войны» и «информационно-психологической войны»;	Устный опрос, доклад, реферат, презентация, практи	Шкала оценивания устного опроса; шкала оценивания доклада; шкала оценивания

			- угрозы современного информационного общества ИИ; - основные элементы госполитики в сфере информационной безопасности. **Уметь:** - защищать сознание от негативного воздействия со стороны деструктивных (националистических, террористических, экстремистских и других) сил; - организовывать и проводить информационную компанию по популяризации способов защиты от манипуляционного и деструктивного влияния во всех сферах, связанных с информацией; - организовывать и проводить кампании по защите информации. **Владеть**: - навыком анализа информационного поля, выявления и нейтрализации рисков; - технологиями контрпропаганды как в реальности, так и в сети Интернет.	ческая подготовка	реферата; шкала оценивания презентации; шкала оценивания практической подготовки.

Шкала оценивания практической подготовки

Критерии оценивания	Баллы
высокая активность на практической подготовке/ показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации / методическое решение задачи выполнено верно/ анализ и оценка условий полученных результатов выполнены верно (не менее 3)	5
средняя активность на практической подготовке/ показано умение иллюстрировать теоретические положения конкретными примерами / методическое решение задачи выполнено частично/ анализ и оценка условий полученных результатов выполнены частично (не менее 1)	2
низкая активность на практической подготовке/ методическое решение задачи не выполнено/ анализ и оценка условий полученных результатов не выполнены	0

Шкала оценивания устного опроса

Уровень оценивания	Критерии оценивания	Баллы
Устный опрос	Свободное владение материалом	3
	Достаточное усвоение материала	2
	Поверхностное усвоение материала	1
	Неудовлетворительное усвоение материала	0

Шкала оценивания доклада

Уровень оценивания	Критерии оценивания	Баллы
Доклад	Соответствие содержания теме доклада; глубина проработки материала; грамотность и полнота использования источников; грамотность речи и владение текстом доклада	10
	Соответствие содержания теме доклада; глубина проработки материала;	7

	использовано недостаточное количество источников; грамотность речи и владение текстом доклада	
	Соответствие содержания теме доклада; не достаточная глубина проработки материала; использовано недостаточное количество источников; грамотность речи и владение текстом доклада	4
	Несоответствие содержания теме доклада; не достаточная глубина проработки материала; использовано недостаточное количество источников; недостаточное владение текстом доклада	0

Шкала оценивания реферата

Уровень оценивания	Критерии оценивания	Баллы
Реферат	Ключевая идея статьи отражена в реферате полностью, что показывает глубокое понимание содержания реферируемой статьи	10
	Основная идея стати показана, однако понимание ее вызывает сомнение	7
	Идея статьи с трудом проглядывается, отсутствует понимание ее автором, наличие ошибок в изложенном материале.	4
	Идея статьи не отражена, либо реферат – сокращенная реферируемая статья.	0

Шкала оценивания презентации

Уровень оценивания	Критерии оценивания	Баллы
Презентация	Соответствие содержания теме; правильная структурированность информации; эстетичность оформления	10
	Соответствие содержания теме; правильная структурированность информации; недостаточная эстетичность в оформлении	7
	Соответствие содержания теме; отсутствует структурированность информации; недостаточная эстетичность в оформлении	4
	Несоответствие содержания теме; отсутствует структурированность информации; недостаточная эстетичность в оформлении	0

5.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы и задания для устного опроса:

1. Назовите объект, предмет, цель и задачи курса «Политика информационной безопасности».
2. Объясните, что такое «безопасность» в политологии с учетом разных подходов.
3. Назовите подходы к пониманию категории «нация».
4. Что такое национальная безопасность России?
5. Назовите структурные компоненты национальной безопасности России.
6. Выделите особенности Стратегии национальной безопасности РФ 2021 г. в сравнении со Стратегиями НБ 2009 г. и 2015 г.
7. Что такое информация? Назовите уровни представления информации, ее свойства.
8. Какова шкала ценности информации?
9. Перечислите виды защищаемой информации и приведите примеры на каждый вид.
10. Назовите особенности защиты интеллектуальной собственности.

Примерные задания по практической подготовке:

1. Организация и проведение политических дебатов
2. Публикация статей, пресс-релизов и других материалов для медиа, учитывая специфику различных форматов и целевых аудиторий
3. Разработка эффективных стратегических коммуникаций для политических кампаний
4. Исследование общественного мнения. Проведение опросов и фокус-групп для изучения общественного мнения по политическим вопросам

Примерная тематика докладов:

1. Сравнительный анализ «информационной войны» и «информационного противоборства».
2. Сравнительный анализ «информационной войны» и «вооруженного конфликта».
3. Виды информационных войн.
4. Межкорпоративная информационная война.
5. Реклама как средство ведения информационной борьбы.
6. Особенности информационно-психологической войны.
7. Стандарты информационной безопасности.
8. Оранжева книга – критерии безопасности компьютерных систем в США.
9. Европейские критерии безопасности информационных технологий.
10. Критерии адекватности и их функции.

Примерная тематика рефератов:

1. Приемы ведения информационной войны: во время предвыборных кампаний на примере… (по выбору студента).
2. Информационно-психологическая война: история возникновения и методы ведения.
3. Информационная война: понятие, цели, методы, особенности.
4. Кибер-война: ближайшее будущее или вымышленное реальность.
5. Искусственный интеллект: польза и/или вред.
6. Канадские критерии безопасности компьютерных систем.
7. Технологии ведения современных информационных войн: общие принципы.
8. Технология ведения современных информационных войн: провокации.
9. Метальная война.
10. Методы психологической войны.

Примерная тематика презентаций:

1. Информационное оружие: понятие и виды.
2. Развитие международной нормативной базы в области информационной безопасности.
3. Технология ведения современных информационных войн: информационной блокады.
4. Структура Общих критериев безопасности информационных технологий.
5. Технология ведения современных информационных войн: дезинформации.
6. Информационно-психологическое воздействие как «мягкая сила» в современной мировой политике.
7. Войны памяти.
8. Гибридный характер современных информационных войн.
9. Ментальный ресурс нации как фактор цивилизационной безопасности России.
10. Стратегия национальной безопасности России 2021 г.: условия создания, содержание, особенности.

Примерные экзаменационные вопросы

1. Политика информационной безопасности: объект, предмет, цель и задачи курса.
2. Определение термина «безопасность» в политологии. Виды и объекты безопасности.
3. Подходы к пониманию категории «нация».

4. Безопасность как инструмент управления. «Театр безопасности»
5. Национальная безопасность России: понятие и компоненты.
6. Стратегия национальной безопасности России 2021 г. и ее особенности в сравнении с предыдущими Концепциями (1997 г., 2000 г.) и Стратегиями (2009 г., 2015 г.).
7. Информация как объект защиты: понятие, уровни представления информации, свойства, шкала ценности информации.
8. Интеллектуальная собственность и особенность ее защиты.
9. Краткая характеристика основных этапов развития российского законодательства в сфере информационной безопасности. 1990-е гг.
10. Краткая характеристика основных этапов развития российского законодательства в сфере информационной безопасности. 2000-2016 гг.
11. Краткая характеристика основных этапов развития российского законодательства в сфере информационной безопасности. С 2016 г. по настоящее время
12. Органы обеспечения информационной безопасности и защиты информации, их задачи и функции.
13. Особенности политики национальной безопасности США, Франции, Германии, Канады, Китая.
14. Характеристика уровня развития информационных технологий в России. Угрозы информационной безопасности и их классификация.
15. Субъекты информационного противоборства.
16. Причины, виды, каналы утечки и искажения информации.
17. Компьютерная система как объект информационной войны.
18. Методы защиты от несанкционированного доступа.
19. Система защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Криптографические методы.
20. Соотношение понятий: «психологические», «ментальные» и информационно-психологические» войны.
21. Проблемы и угрозы, связанные с развитием информационного общества.
22. Основные технологии психологического, в т.ч. информационно-психологического, воздействия. Информационно-психологическая составляющая пропаганды.
23. «Новая холодная война».
24. Подмена ценностей. Конструирование и деконструирование системы идентичностей. Технологии дегероизации и расчеловечивания.
25. Провоцирование и управление массовыми фобиями.
26. Провоцирование межэтнических и межконфессиональных конфликтов.
27. «Мягкая», «жесткая» и «умная» силы.
28. Антироссийские исторические и политические мифы.
29. Информационная составляющая гибридных войн и «цветных революций». «Информационный каскад». Способы противодействия гибридным войнам и «цветным революциям».

5.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Основными формами текущего контроля являются: устный опрос, доклад, реферат, презентация и задания по практической подготовке.

Промежуточная аттестация проводится в форме экзамена. Экзамен проводятся устно по вопросам. Максимальное количество баллов, которое может набрать бакалавр в течение семестра за текущий контроль, равняется 70 баллам.

Максимальная сумма баллов, которые бакалавр может получить на экзамене, равняется 30 баллам. Максимальная сумма баллов студентов по изучаемой дисциплине составляет 100 баллов.

Шкала оценивания экзамена

Баллы	Критерии оценивания
16-30	Студент прочно усвоил предусмотренный программный материал; правильно и аргументировано ответил на все вопросы с приведением примеров; показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников; теорию связывает с практикой, другими темами данного курса.
11-15	Студент прочно усвоил предусмотренный программный материал; но не всегда аргументировано отвечал на вопросы с приведением примеров; показал систематизированные знания, не всегда владеет приемами рассуждения и сопоставляет материал из разных источников; теорию связывает с практикой, другими темами данного курса.
6-10	Студент недостаточно прочно усвоил предусмотренный программный материал; но не всегда аргументировано отвечал на вопросы с приведением примеров; показал недостаточно систематизированные знания, не всегда владеет приемами рассуждения и сопоставляет материал из разных источников; не связывает теорию с практикой.
0-5	Студент не усвоил предусмотренный программный материал; не ответил на большинство вопросов преподавателя, не связывает теорию с практикой.

Итоговая шкала оценивания результатов освоения дисциплины

Итоговая оценка по дисциплине выставляется по приведенной ниже шкале. При выставлении итоговой оценки преподавателем учитывается работа обучающегося в течение освоения дисциплины, а также оценка по промежуточной аттестации.

Количество баллов	Оценка по традиционной шкале
81-100	Отлично
61-80	Хорошо
41-60	Удовлетворительно
0-40	Неудовлетворительно

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И РЕСУРСНОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Основная литература

1. Суворова Г.М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029

2. Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации : учебник / сост. И. Г. Дровникова, А.В. Калач, И.И. Лившиц [и др]. - Воронеж : Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1999941 (дата обращения: 09.04.2024). – Режим доступа: по подписке.

3. Дербин Е.А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности : учебное пособие / Е.А. Дербин, А.В. Царегородцев. — Москва : ИНФРА-М, 2024. — 267 с. — (Высшее образование). — DOI 10.12737/2084342. - ISBN 978-5-16-019050-1. - Текст : электронный. - URL:

https://znanium.ru/catalog/product/2084342 (дата обращения: 09.04.2024). – Режим доступа: по подписке.

6.2. Дополнительная литература.

1. Багдасарян В.Э. Россия — Запад: цивилизационная война : монография / В.Э. Багдасарян. — Москва : ФОРУМ : ИНФРА-М, 2019. — 410 с. — (Научная мысль). — www.dx.doi.org/10.12737/monography_5939275cb6da48.66131437. - ISBN 978-5-00091-442-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1003273 (дата обращения: 08.04.2024).
2. Шамахов В.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов : монография / В. А. Шамахов, А. А. Ковалев. - Москва : РИОР, 2019. - 184 с. - (Научная мысль). - ISBN 978-5-369-00892-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2037326 (дата обращения: 09.04.2024). – Режим доступа: по подписке.
3. Звягин А.А. Россия в гибридной войне. Информационно-психологическая безопасность : монография / А.А. Звягин, Б.А. Артамонов, И.А. Мельников. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2024. — 329 с. — (Научная мысль). - ISBN 978-5-16-112272-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2134590 (дата обращения: 06.04.2024).
4. Ильницкий А.М. Ментальная война России. // Военная мысль. 2021. №8. URL: https://cyberleninka.ru/article/n/mentalnaya-voyna-rossii (дата обращения: 06.04.2024).
5. Михайлёнок О.М. Политические аспекты информационной безопасности личности // Власть. 2010. №12. URL: https://cyberleninka.ru/article/n/politicheskie-aspekty-informatsionnoy-bezopasnosti-lichnosti (дата обращения: 14.03.2024).
6. Кардашова И.Б. Основы теории национальной безопасности: учебник для вузов / И. Б. Кардашова. — 3-е изд. — Москва: Издательство Юрайт, 2024. — 334 с. — (Высшее образование). — ISBN 978-5-534-15789-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/539604 (дата обращения: 08.04.2024).
7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т.А. Поляковой, А.А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536225 (дата обращения: 09.04.2024).
9. Щеглов А.Ю. Защита информации: основы теории : учебник для вузов / А.Ю. Щеглов, К.А. Щеглов. — Москва : Издательство Юрайт, 2024. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/537000
10. Зенко А.В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544290
11. Васильева И.Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2024. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536902
12. Корабельников С.М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С.М. Корабельников. — Москва : Издательство Юрайт, 2024. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/543351

6.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

1. ФСБ РФ. URL: http://www.fsb.ru/?rsd
2. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. URL: https://digital.gov.ru/ru/
3. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор). URL: https://rkn.gov.ru/
4. Социально-гуманитарное и политологическое образование. URL: http://www.humanities.edu.ru
5. Научная электронная библиотека eLIBRARY.RU. URL: http://elibrary.ru/defaultx.asp
6. Политологический раздел библиотеки Максима Мошкова. URL: http://lib.ru/POLITOLOG/
7. Политанализ.Ру. URL: http://www.politanaliz.ru
8. Университетская библиотека onlain. URL: http://www.biblioclub.ru/
9. ПолитНаука - политология в России и мире. URL: http://www.politnauka.org/
10. Библиотека Гумер – Политология. URL: http://www.gumer.info/bibliotek_Buks/Polit/Index_Polit.php
11. Библиотека Михаила Грачева по политологии. URL: http://grachev62.narod.ru/
12. Библиотека Русского Гуманитарного Интернет-Университета. URL: http://www.i-u.ru/biblio/default.aspx?key
13. Российское образование. Федеральный образовательный портал. URL: http://www.edu.ru/index.php
14. Сетевой портал журнала «Полис». URL: http://www.polisportal.ru/index.php?page_id=48
15. Журнал «Обозреватель-Observer». URL: http://www.nasledie.ru/oboz/index.shtml
16. Журнал «ПолитЭкс» (Политическая экспертиза). URL: http://www.politex.info/index.php?option=com_frontpage&Itemid=1
17. «Социологические исследования» (Социс). URL: http://www.isras.ru/socis.html
18. «Власть» http://www.isras.ru/authority.html
19. Рецензируемый научный журнал «Вестник Государственного университета просвещения. Серия: История и политические науки». URL: https://www.istpolitmgou.ru/jour
20. Рецензируемый научный журнал «Российский социально-гуманитарный журнал» (б. «Вестник МГОУ (электронный журнал)». URL: https://www.evestnik-mgou.ru/jour

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1.Методические рекомендации по организации самостоятельной работы бакалавров

8. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Лицензионное программное обеспечение:

Microsoft Windows
Microsoft Office
Kaspersky Endpoint Security

Информационные справочные системы:

Система ГАРАНТ
Система «КонсультантПлюс»

Профессиональные базы данных:

fgosvo.ru – Портал Федеральных государственных образовательных стандартов высшего образования

pravo.gov.ru - Официальный интернет-портал правовой информации

www.edu.ru – Федеральный портал Российское образование

Свободно распространяемое программное обеспечение, в том числе отечественного производства

ОМС Плеер (для воспроизведения Электронных Учебных Модулей)
7-zip
Google Chrome

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение дисциплины включает в себя:

- учебные аудитории для проведения занятий лекционного и семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные учебной мебелью, доской, демонстрационным оборудованием;
- помещения для самостоятельной работы, укомплектованные учебной мебелью, персональными компьютерами с подключением к сети Интернет и обеспечением доступа к электронным библиотекам и в электронную информационно-образовательную среду.