Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Институт права и национальной безопасности
Факультет национальной безопасности
Кафедра международной безопасности и внешнеполитической деятельности России

Утверждена
решением кафедры международной
безопасности и внешнеполитической
деятельности России
«26» июня 2017 г. № 16

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Б1.В.15 Внешнеполитическая деятельность России в области информационной безопасности

по направлению подготовки
38.04.04 Государственное и муниципальное управление
Государственное управление и внешнеполитическая деятельность России

магистр
квалификация выпускника

очно-заочная, заочная
форма(ы) обучения

Год набора - 2018

Москва, 2018 г.

Автор(ы)–составитель(и):

к.и.н., доцент, зав.кафедрой____ Кафедра МБиВПДР /Харитонова Н.И./
(ученое звание, ученая степень, должность) *(кафедра)* *(Ф.И.О.)*

Заведующий кафедрой
международной безопасности и
внешнеполитической деятельности России доц., к.и.н. /Харитонова Н.И./
(наименование кафедры) *(уч.звание, степень)* *(Ф.И.О.)*

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.....
2.Объем и место дисциплины (модуля) в структуре образовательной программы.....
3.Содержание и структура дисциплины (модуля).....
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю)…….....
5.Методические указания для обучающихся по освоению дисциплины (модуля).....
6.Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю).....
6.1. Основная литература.....
6.2. Дополнительная литература.....
6.3. Учебно-методическое обеспечение самостоятельной работы.....
6.4. Нормативные правовые документы.....
6.5. Интернет-ресурсы.....
6.6. Иные источники.....
7.Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы.....

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

1.1. Дисциплина Б1.В.15 «Внешнеполитическая деятельность России в области информационной безопасности» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
СК-2	способность выявлять угрозы национальным интересам и оценивать уровень эффективности реализации внешней политики Российской Федерации	СК-2.2	способность применять знание основ внешнеполитической деятельности в борьбе с транснациональным терроризмом, религиозным экстремизмом, с угрозам информационной безопасности России, в том числе в рамках научно-исследовательской работы;
СК-3	владение навыками организации управленческой деятельности для формирования современных систем национальной и международной безопасности, эффективной внешней политики Российской Федерации	СК-3.3	способность применять в профессиональной деятельности знание методов прогнозирования в сфере внешней политики, правовых основ международной деятельности России, специфики внешнеполитической деятельности России в борьбе с транснациональным терроризмом и угрозами информационной безопасности для формирования современных систем национальной и международной безопасности, эффективной внешней политики Российской Федерации в условиях современной мировой политики и международных отношений, в том числе в рамках научно-исследовательской работы.

1.2. В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)/ профессиональные действия	Код этапа освоения компетенции	Результаты обучения
Сбор, переработка и анализ информации для решения задач, поставленных руководителем (Код ПС 447) Разработка программ и механизмов эффективного политического,	СК-2.2	На уровне умений: - с помощью специальных средств ИКТ выбирать и анализировать индикаторы и критерии оценки состояния информационной защищенности личности, общества и государства; - работать с научными базами данных и другими источниками научной информации при помощи современных информационно-коммуникативных технологий;
		На уровне навыков:

экономического и гуманитарного противодействия существующим и потенциальным угрозам Российской Федерации и мировому сообществу (Справочник) Содействие укреплению международной безопасности (Справочник)		- навыками оценки состояния массмедийной инфраструктуры и киберсреды по критерию антитеррористического противоборства; - навыками использования материально-технических средств при проведении исследований в сфере обеспечения информационной безопасности и решении административных задач; - навыками разработки и реализации программ исследований информационных процессов с помощью современных технических средств;
Подготовка информационно-аналитических материалов (Код ПС 447) Разработка тематического плана обзорного документа, доклада (по 447)	СК-3.3	На уровне умений: - осуществлять аналитическое обеспечение принятия управленческих решений в области обеспечения информационной безопасности,
		На уровне навыков: - разработки и реализации программ исследований информационных процессов с помощью современных технических средств; - разработки управленческих решений в области обеспечения информационной безопасности

2. Объем и место дисциплины (модуля) в структуре ОП ВО

Объем дисциплины:

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

- очно-заочная форма обучения: лекции – 6 а.ч., практические занятия – 16 а.ч., самостоятельная работа – 50 а.ч;

- заочная форма обучения: лекции – 4 а.ч., практические занятия – 12 а.ч., самостоятельная работа – 52 ч.

Место дисциплины (модуля) в структуре ОП ВО

Дисциплина Б1.В.15 «Внешнеполитическая деятельность России в области информационной безопасности» относится к вариативной части ОП ВО и входит в профессиональный цикл, в соответствии с учебным планом осваивается в 4 семестре очно-заочной формы обучения, на 3 курсе заочной формы обучения.

Общая трудоемкость дисциплины Б1.В.16 «Внешнеполитическая деятельность России в области информационной безопасности» составляет 2 з.е. (72 а.ч.).

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области международных отношений, политологии.

Форма промежуточной аттестации в соответствии с учебным планом: зачет.

3. Содержание и структура дисциплины (модуля)

Таблица 1.

№ п/п	Наименование тем	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очно-заочная форма обучения								
Тема 1	Мировой политический процесс и информационная безопасность.	17	2		4	5	6	О, КР
Тема 2	Государственная политика России в сфере информационной безопасности	19	2		4	5	8	Т, О
Тема 3	Международная информационная безопасность в глобальных сетях (компьютерная безопасность).	18	1		4	5	8	Т, О
Тема 4	Информационное обеспечение стратегических направлений национальной и международной безопасности.	18	1		4	5	8	О, Д, СЗ
Промежуточная аттестация								Зачет
	Всего:	**72**	**6**		**16**	**20**	**30**	
Заочная форма обучения								
Тема 1	Мировой политический процесс и информационная безопасность.	16	1		2	5	8	О, КР
Тема 2	Государственная политика России в сфере информационной безопасности	16	1		2	5	8	Т, О
Тема 3	Международная информационная безопасность в глобальных сетях (компьютерная безопасность).	18	1		4	5	8	Т, О
Тема 4	Информационное обеспечение	18	1		4	5	8	О, Д, СЗ

№ п/п	Наименование тем	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
	стратегических направлений национальной и международной безопасности.							
Промежуточная аттестация		4						Зачет
	Всего:	**72**	**4**		**12**	**20**	**32**	

Примечание: 4 – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), доклад (Д), ситуационные задачи (СЗ).

Содержание дисциплины (модуля)

Тема 1. Мировой политический процесс и информационная безопасность

Сущность и содержание понятия «информационная безопасность», ее место и роль в системе обеспечения национальной безопасности. Развитие современного информационного общества и влияние на процессы обеспечения информационной безопасности. Философия информационной безопасности. Возрастание угроз международной информационной безопасности. Принципы и методы анализа и управления состояниями и процессами информационной безопасности. Массовая информационная сфера как объект управления.

Тема 2. Государственная политика России в сфере информационной безопасности

Становление международного информационного права. Информационное обеспечение международных актов: правовое, политическое, организационное содержание и реализация. Конвенция «Об обеспечении международной информационной безопасности» (2011 г.). Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Система современного миропорядка и состояние информационных ресурсов политических акторов. Состояние и перспективы формирования и развития государственных информационных ресурсов. Противодействие угрозам развития отечественной индустрии информации.

Тема 3. Международная информационная безопасность в глобальных сетях (компьютерная безопасность).

1. Содержание понятия «глобальная сеть». Особенности обеспечения безопасности глобальных информационных сетей. Противодействие угрозам безопасности информационных и телекоммуникационных средств и систем. Региональные центры использования ИКТ. Серия международных конференций по развитию информатизации международных связей (2000-2016 гг.). Окинавская Хартия глобального информационного общества как «международная конституция». Основные инициативы Российской Федерации в области МИБ. Конвенция «Об обеспечении международной информационной безопасности» (2011 г.).

Тема 4. Информационное обеспечение стратегических направлений национальной и международной безопасности.
Национальные/транснациональные массовые информационные системы. Средства массовой информации как критически важные структуры системы международных отношений. Информационное противоборство в современном мире. Основные концепции информационно-психологических войн. Теория и методы ведения информационной войны. Соотношение информационная война – «гибридная» война. Особенности подготовки и ведения информационно-психологических войн в исторической ретроспективе. Характер, сущность и содержание информационно-психологических войн современности.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю)

4.1. Формы и методы текущего контроля успеваемости и промежуточной аттестации.

4.1.1. В ходе реализации дисциплины Б1.В.15 «Внешнеполитическая деятельность России в области информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

При проведении занятий лекционного типа: опрос

при проведении занятий семинарского типа: опрос

при контроле результатов самостоятельной работы студентов: тестирование, контрольная работа, доклад.

4.1.2. Экзамен (зачет) проводится с применением следующих методов (средств):

Промежуточная аттестация проводится в форме устного ответа на вопросы билета.

4. 2. Материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по темам 1-4:

Вопросы для опроса на занятиях.
Тема 1.
Лекция: Основы политики международной информационной безопасности.
1. Развитие информационного общества и информационная безопасность: теоретико-методологические аспекты исследования.
2. Философия информационной безопасности. Переход к информационному обществу и возрастание угроз международной информационной безопасности.
3. Геокультурное, геоидеологическое и геоинформационное пространство. Трансформация традиционной геополитики в информационную.

Практическое занятие: Теория и практика управления безопасностью международных информационных процессов.

1. Методы анализа и управления состояниями и процессами информационной безопасности.
2. Массовая информационная сфера как объект управления.
3. Идеология как теоретическая основа управления информационными процессами. Технологии достижения глобального демонстрационного эффекта, «эффекта лавины».
4. Технологии «мягкой силы»: культурно-лингвистическая экспансия. Проблемы формализации международных коммуникационных процессов.

Тема 2.
Лекция: Правовое обеспечение политики в сфере информационной безопасности.

1. Устав ООН о способах разрешения международных споров информационными средствами.
2. Информационное обеспечение международных актов: правовое, политическое, организационное содержание и реализация.
3. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года

Практическое занятие: Обеспечение безопасности государственных информационных ресурсов.

1. Зависимость структуры системы современного миропорядка от состояния информационных ресурсов (потенциалов) международных акторов.
2. Условия формирование нового мирового порядка, сопутствующие им информационные вызовы международной безопасности: информационная насыщенность современного мира, публичность, транспарентность межгосударственных отношений. Эффекты социально-политической темпоральности.
3. Состояние и перспективы формирования и развития государственных информационных ресурсов.

Тема 3.
Лекция: Основы безопасности глобальных информационных сетей

1. Общая характеристика безопасности глобальных сетей.
2. Деятельность рабочих групп по национальным и региональным стратегиям использования электронных технологий.
3. Противодействие угрозам безопасности информационных и телекоммуникационных средств и систем.

Практическое занятие: Международное сотрудничество в области противодействия кибертерроризму
1. Региональные центры использования ИКТ. Серия международных конференций по развитию информатизации международных связей (2000-2015гг.).
2. Разработка и реализация международной программы развития людских ресурсов и наращиванию потенциала: взаимодействие с учреждениями ООН, представителями частного и государственного секторов.
3. Основные инициативы Российской Федерации в области МИБ. Конвенция «Об обеспечении международной информационной безопасности» (2011 г.).

Тема 4.
Лекция: Безопасность системы массовой информации и коммуникации.

1. Национальные/транснациональные массовые информационные системы.
2. Средства массовой информации как критически важные структуры системы международных отношений.
3. Роль СМИ в балансе сил в международных отношениях. СМИ и гибридные образования как источники глобальных угроз: объединение государственных и негосударственных структур в области бизнеса и СМИ. Влияние СМИ на формирование геокультуры Запада, Евразийского региона, Центрально-Азиатского региона и др.

Практическое занятие: Информационная безопасность как условие предотвращения информационно-психологической войны.

1. Информационное противоборство. Основные научные концепции информационно-психологических войн.
2. Базовые категории и теоретическое обоснование понятий «информационное противоборство», «информационная война», «мягкая сила».
3. Теория, приемы, средства, методы и системы ведения информационной войны.
4. Тенденции и перспективы обеспечения информационно-психологической безопасности: российские инициативы и практики.

Тестовые задания

Тема 2. Государственная политика России в сфере информационной безопасности

1. Основополагающий документ, утвержденный Президентом Российской Федерации В.Путиным 9 сентября 2000 г. и регулирующий деятельность государства по обеспечению информационной безопасности России, называется:
A. *Доктрина информационной безопасности России*
B. Стратегия информационной безопасности России
C. Концепция информационной безопасности России
D. Основы информационной безопасности России

2. Согласно Доктрине информационной безопасности России (утверждена Президентом Российской Федерации В.Путиным 9 сентября 2000 г.) к интересам государства в информационной сфере относится:
A. *развитие равноправного и взаимовыгодного международного сотрудничества*
B. поддержание тенденций к усилению отдельных государств в мировых информационно-политических процессах
C. создание условий для интеграции системы информационной безопасности России в международную систему информационной безопасности
D. стимулирование процессов распространения демократических ценностей на другие страны

3. Концепция Дж. Ная, касающаяся несиловых методов влияния политику государств называется:
A. *мягкая (гибкая) сила*
B. жесткая сила
C. умная сила
D. экономическая сила

4. Документ «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» был утвержден в:
A. 2000 г
B. 2005 г
C. *2013 г*
D. 1996 г

5. Согласно «Основам государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» под международной информационной безопасностью понимается
A. *такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры*
B. устойчивое развитие мировой информационно-коммуникативной системы в интересах мирового сообщества
C. защищенность информационных интересов граждан и общества
D. техническая защищенность глобальной информационной сети Интернет

6. Согласно «Основам государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» система международной информационной безопасности призвана
A. обеспечить стремительное развитие информационно-коммуникативных технологий
B. *оказать противодействие угрозам стратегической стабильности и способствовать равноправному стратегическому партнерству в глобальном информационном пространстве*
C. стимулировать развитие мировой информационной экономики
D. преодолеть технологический суверенитет государств в области информационных и коммуникационных технологий

7. Соглашение между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности вступило в силу в:
A. *2011 г*
B. 2003 г
C. 2014 г
D. 2001 г

8. Окинавская хартия Глобального информационного общества была подписана лидерами стран-участниц G8 в:
A. 2011 г
B. *2000 г*
C. 1992 г
D. 2005 г

9. Какое из перечисленных направлений не закреплено в Окинавской хартии Глобального информационного общества:
A. продолжение содействия развития конкуренции и открытию рынков для информационной технологии и телекоммуникационной продукции и услуг
B. защита прав интеллектуальной собственности на информационные технологии

C. разработка информационных сетей, обеспечивающих быстрый, надежный, безопасный и экономичный доступ с помощью конкурентных рыночных условий и соответствующих нововведений к сетевым технологиям, их обслуживанию и применению
D. *противодействие использованию информационных и коммуникационных технологий в качестве информационного оружия в военно-политических целях, противоречащих международному праву*

10. Целью «Конвенция об обеспечении международной информационной безопасности» (концепция) является:
A. *противодействие использованию информационно-коммуникационных технологий для нарушения международного мира и безопасности*
B. защита прав интеллектуальной собственности на информационные технологии
C. стимулирование использования информационных технологий в экономических процессах
D. продолжение содействия развития конкуренции и открытию рынков для информационной технологии и телекоммуникационной продукции и услуг

Тема 3. Международная информационная безопасность в глобальных сетях.

1. Согласно «Конвенции об обеспечении международной информационной безопасности» (концепция) к информационным ресурсам относятся:
A. только информационная инфраструктура
B. только информационные потоки
C. *информационная инфраструктура, а также собственно информация и ее потоки*
D. ничего из перечисленного

2. Что из перечисленного не упоминается в «Конвенции об обеспечении международной информационной безопасности» (концепция) в качестве основных угроз международному миру и безопасности в информационном пространстве
A. неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы
B. использование информационных технологий и средств для осуществления враждебных действий и актов агрессии
C. действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество
D. *протекционистская политика государств в отношении производителей средств информатизации и защиты информации*

3. Какое из перечисленных государств не являлось инициатором документа «Правила поведения в области обеспечения международной информационной безопасности», который обсуждался на 66-й сессии ГА ООН 12 сентября 2011 г:
A. Китай
B. Россия
C. *Монголия*
D. Таджикистан

4. К критически важным объектам информационной инфраструктуры относят:
A. часть (элемент) информационной инфраструктуры, который интегрирован в международную информационную инфраструктуру

B. *часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства*
C. часть (элемент) информационной инфраструктуры, обслуживание которого является наиболее опасным для здоровья персонала
D. часть (элемент) информационной инфраструктуры, воздействие на которую не может иметь последствий, непосредственно затрагивающих национальную безопасность

5. В каком году была принята Конвенцию о киберпреступности Совета Европы (Будапештская конвенция)
A. *2001 г*
B. 1997 г
C. 2009 г
D. 2012 г

6. Какое положение не относится к принципам обеспечения международной информационной безопасности
A. государства-участники в ходе формирования системы международной информационной безопасности будут руководствоваться принципом неделимости безопасности
B. все государства-участники в информационном пространстве пользуются суверенным равенством, имеют одинаковые права и обязанности и являются равноправными субъектами информационного пространства независимо от различий экономического, социального, политического или иного характера
C. каждое государство-участник должно придерживаться принципа ответственности за собственное информационное пространство
D. *каждое государство-участник не вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством.*

7. В каком году был подписан Протокол о взаимодействии государств – членов ОДКБ по противодействию преступной деятельности в информационной сфере в рамках?
A. *2011*
B. 2000
C. 1998
D. 2002

8. Что такое «цифровое неравенство» (барьер) ?
A. *ограничение возможностей государства или социальной группы из-за отсутствия у неё доступа к современным средствам ИКТ*
B. невозможность передачи информации другому государству
C. отсутствие условий для развития конкуренции на рынке ИКТ
D. невозможность защиты прав интеллектуальной собственности на информационные технологии

9. В каком документе стратегического планирования России впервые подчеркнута необходимость интернационализации управления информационно-телекоммуникационной сетью «Интернет»
A. Доктрина информационной безопасности
B. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года
C. *Стратегия развития информационного общества в Российской Федерации*
D. Ни в одном из указанных документов

10. Что из перечисленного не относится к внутренним угрозам информационной безопасности согласно Доктрине информационной безопасности

A. недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах

B. нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений

C. отсутствие единой методологии сбора, обработки и хранения информации оперативно-разыскного, справочного, криминалистического и статистического характера

D. *деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов*

Примерные темы для написания докладов

Тема 4. Информационное обеспечение стратегических направлений национальной и международной безопасности.

1. Координация и взаимодействие субъектов международной деятельности в сфере обеспечения информационной безопасности
2. Принципы и пути создания безопасного информационного пространства региона (приграничная, пограничная, трансграничная территории).
3. Управление безопасностью информационных процессов (теоретический аспект).
4. Методологические основы международной информационной безопасности.
5. Формирование, использование и защита информационных ресурсов государства.
6. Сущность и содержание информационно-психологической безопасности.
7. Характеристика основных угроз информационно-психологической безопасности в международных отношениях.
8. Роль и место СМИ в обеспечении международной информационно-психологической безопасности.
9. Развитие институтов (субъектов, сил и средств) системы обеспечения международной информационной безопасности.
10. Роль министерств и ведомств России в системе обеспечения информационной безопасности.

Примерные темы для написания контрольных работ

Тема 1. Мировой политический процесс и информационная безопасность.

1. Проблемы законотворчества в области охраны прав граждан на свободу слова.
2. Взаимосвязь свободы слова и права на свободный доступ к информации. Информационное обеспечение исполнения международных актов информационной безопасности (МИБ).
3. Влияние СМИ на формирование геокультуры Запада / Евразийского региона, Центрально-Азиатского региона и др.
4. Информационная политика в области информационной безопасности: параметры и пределы государственного регулирования.
5. Информационная политика как инструмент осуществления «гибкой власти»

6. Роль государственной информационной политики в разрешении глобальных проблем международной безопасности.
7. Информационная политика как средство реализации политической воли государства в международных отношениях.
8. Роль журналистов и СМИ в урегулировании международных конфликтов.
9. Участие СМИ в формировании международного имиджа государства (страны).
10. Роль СМИ в формировании индексов мирового развития.

Примеры ситуационных задач:

Тема 4.

Ситуационная задача 1. ПЕРСОНА / КОМПАНИЯ – РЕПУТАЦИОННЫЕ УГРОЗЫ: Вброс недостоверной информации и скорость реакции

Кейс относится к недавней акции — телемарафону «Всем миром», который 29 сентября проводил «Первый канал». Цель акции была в мощном информационном посыле, побуждающем население делать пожертвования в пользу пострадавших от наводнения на Дальнем Востоке. Сбор средств осуществлялся через SMS и системы электронных платежей.

В целом акция прошла успешно и сопровождалась активным обсуждением в социальных сетях: с 26 по 30 сентября опубликовано 43 176 сообщений по теме от 29 742 авторов. Однако, именно активное обсуждение акции, а точнее — отсутствие мониторинга за этим обсуждением и привело к проблеме, которая не позволила получить максимально возможную сумму пожертвований.

Утром 29 сентября в соцмедиа была опубликована недостоверная информация о том, что сотовые операторы заберут себе половину пожертвований, отправленных через SMS, и эта информация, подхваченная популярными Твиттерянами, инициировала лавинообразное обсуждение в социальных сетях: порядка 5% всех сообщений об акции – обсуждение именно этого нюанса. Это стало одной из основных причин, которые удерживали людей от отправки SMS-сообщений.

Реакция «Первого канала» появилась с существенным опозданием, когда недостоверная информация получила уже широкое распространение.

Рис.1: Обсуждение акции "Всем миром" в социальных медиа 29.09.13

Таким образом, информационное пространство соцмедиа продемонстрировало свою силу: появление

недостоверной информации резко негативно сказалось, как на имидже акции и организаторов, так и на сумме собранных средств.

Организаторы акции и «большая тройка» дали развернутое объяснение в Ведомостях только на следующий день, что не смогло исправить ситуацию – время было уже упущено.

Выводы: Информационный поток в соцмедиа, сопровождающий публичные персоны, компании и, тем более, специализированные акции, является важным элементом воздействия на общественное мнение. Поэтому необходимо осуществлять **реал-тайм мониторинг реакции**, особенно в случае «социального телевидения», когда зрители выплескивают эмоции по ходу передачи, выступления, конкурса, шоу, теледебатов.

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
СК-2	способность выявлять угрозы национальным интересам и оценивать уровень эффективности реализации внешней политики Российской Федерации	СК-2.2	способность применять знание основ внешнеполитической деятельности в борьбе с транснациональным терроризмом, религиозным экстремизмом, с угрозам информационной безопасности России, в том числе в рамках научно-исследовательской работы; 3 этап (СК-2.3)
СК-3	владение навыками организации управленческой деятельности для формирования современных систем национальной и международной безопасности, эффективной внешней политики Российской Федерации	СК-3.3	способность применять в профессиональной деятельности знание методов прогнозирования в сфере внешней политики, правовых основ международной деятельности России, специфики внешнеполитической деятельности России в борьбе с транснациональным терроризмом и угрозами информационной безопасности для формирования современных систем национальной и международной безопасности, эффективной внешней политики Российской Федерации в условиях современной мировой политики и международных отношений, в том числе в рамках научно-исследовательской работы.

4.3.2 Типовые оценочные средства

Перечень вопросов для подготовки к промежуточной аттестации (зачёту):

1. Философия безопасности и философия информационной безопасности: общее и особенное
2. Сущность и содержание понятия «информационная безопасность».
3. Место и роль информационной безопасности в общей системе международной безопасности.
4. Влияние мировых политических процессов на состояние безопасности глобального информационного пространства
5. Общая характеристика угроз международной информационной безопасности.
6. Цель и задачи обеспечения международной информационной безопасности.
7. Реализация мер по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена
8. Постановка проблемы информационной безопасности в Концепции внешней политики Российской Федерации (2013 г.)
9. Общая характеристика Конвенции международной информационной безопасности (Концепции.)
10. Обеспечение основных направлений государственной политики Российской Федерации в области международной информационной безопасности
11. Использование методов непрямых действий и «мягкой силы» в целях обеспечения информационной безопасности (мировой и российский опыт)
12. Влияние информационных потоков на формирование и состояние глобальных угроз современности
13. Национальные интересы России в информационной сфере
14. Основные направления формирования внешнего имиджа России в целях обеспечения информационной безопасности.
15. Основные направления обеспечения компьютерной безопасности в системе международных отношений.
16. Конституция России как основной источник правовых норм в области обеспечения информационной безопасности.
17. Международное право и информационное законодательство Российской Федерации.
18. Базовые законодательные акты Российской Федерации в области информационной безопасности.
19. Основные направления построения информационного общества в Российской Федерации.
20. Координация и взаимодействие субъектов международной деятельности в сфере обеспечения информационной безопасности
21. Принципы и пути создания безопасного информационного пространства региона (приграничная, пограничная, трансграничная территории).
22. Управление безопасностью информационных процессов (теоретический аспект).
23. Методологические основы международной информационной безопасности.
24. Формирование, использование и защита информационных ресурсов государства.
25. Сущность и содержание информационно-психологической безопасности.
26. Характеристика основных угроз информационно-психологической безопасности в международных отношениях.
27. Роль и место СМИ в обеспечении международной информационно-психологической безопасности.
28. Развитие институтов (субъектов, сил и средств) системы обеспечения международной информационной безопасности.

29. Роль министерств и ведомств России в системе обеспечения информационной безопасности.
30. Роль негосударственных организаций в формируемой системе обеспечения международной информационной безопасности.
31. Развитие правовых основ обеспечения международной информационной безопасности.
32. Информационная глобализация и информационное общество: каузальные связи и противоречия.
33. Формы и методы защиты информационных ресурсов государства от несанкционированного использования.
34. Манипулирование общественным сознанием мировой общественности как проблема информационной безопасности.
35. Роль и место национальных массмедийных систем в обеспечении информационно-психологической безопасности
36. СМИ как критически важные структуры и объекты систем национальной безопасности: российский и международный опыт оценки и регулирования
37. Информационное обеспечение мер по реализации внешнеполитического курса Российской Федерации (в соответствии с Указом Президента Российской Федерации от 7.05.2012 г. № 605)
38. Функции МИД РФ, Минсвязи, федеральных служб и агентств в системе обеспечения внешней информационной безопасности.
39. Межгосударственные системы обеспечения информационной безопасности в экономической, политической, социокультурной сфере (по выбору студента)
40. Основные направления информационной политики России в сфере международного военного сотрудничества
41. Виды и характеристика СМИ (печатные, телевизионные, электронные, мультимедийные средства) и возможности их использования в обеспечении международной информационной безопасности (МИБ)
42. Международный опыт борьбы с преступлениями в информационной сфере.
43. Зарубежный опыт обеспечения информационной безопасности (на примерах США, Канады, Германии, Франции, Китая и др. - по выбору).
44. Методы и средства защиты информации и информационных ресурсов в Интернете и Интранете.

Ситуационные задачи:

Ситуационная задача 1. МИРОВОЙ (ПОЛИТИКА, ДОЛГОСРОЧНЫЕ ТРЕНДЫ) — НАСАЖДЕНИЕ СТЕРЕОТИПОВ

Отношение к России в мире: “Pew Research” (США) vs “Vox Populi” (Россия)

Кейс спровоцирован исследованием «Pew Research Centre», которое было проведено в марте-апреле 2013 года и результаты которого «удивительно удачно» опубликованы 3 сентября – прямо к заседанию G20 в Санкт-Петербурге.

В рамках исследования было изучено отношение к России в 38-ми странах мира, на основании чего был сделан вывод о негативном восприятии России в 36 (!) странах. Позитивно к России относятся, якобы, только жители Греции (63%) и Ю. Кореи (53%). Круто, особенно если посмотреть методологию (опрашивались по 1000 человек в каждой стране) и вероятность ошибки, доходящей до 7.7%.

Российский фонд Vox Populi провел «защитное» исследование: с 9 по 13 сентября было собрано и проанализировано свыше 770 тыс. сообщений о России в СМИ и соцмедиа от 440 тыс. авторов из 231

страны. Исследование показало, что в индивидуальном отношении людей к России преобладает позитив, в то время как в официальных источниках (СМИ, информагентства, официальные лица) — преобладает негатив. Ниже показана аналитика по данным (СМИ и соцмедиа) 74 тыс. жителей США, высказавшихся за 4 дня сентября по теме Россия:

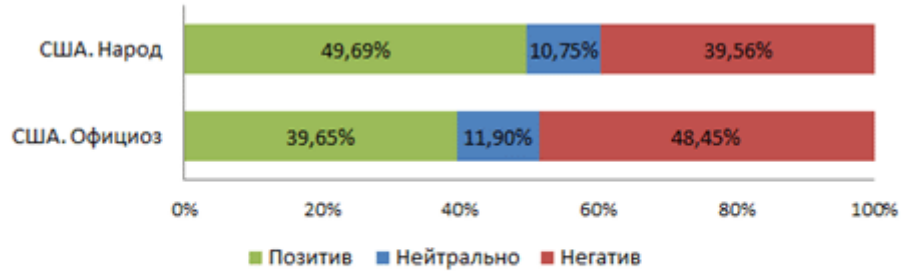

Рис.2: Тональность сообщений по отношению к России в официальных СМИ и социальных медиа США. Источник: Vox Populi

Кроме того, нельзя не обратить внимания на резкие различия в акцентировании тематик по отношению к России в «официозе» (официальные СМИ, известные политологи и экс-чиновники) и среди народа:

Тематики обсуждений	США. Официоз	США. Народ
Сирия	65,2%	69,9%
ЛГБТ	14,3%	11,6%
Отсутствие свобод	**14,0%**	**0,6%**
Статья Путина в NYT	**4,6%**	**7,2%**
Олимпиада в Сочи	0,1%	1,1%
Другое	1,8%	9,6%

Рис.3: Наиболее активные темы в контексте обсуждений России в СМИ и соцмедиа США

Выводы: За общественное мнение можно принять стереотипы, которые пытаются насаждать официальные СМИ, информагентства или лица, заинтересованные в определенной «окраске» событий, персон, ситуаций. Исследование общественного мнения в соцмедиа становится мощным «щитом» в противостоянии мифам и стереотипам, блокируя их как оружие в международной политике.

Промежуточные итоги: рассмотрены только пара кейсов из представленных в докладе (в случае заинтересованности читателей остальные мы приведем в следующей статье), показывающих подходы к выявлению наиболее распространенных информационных угроз.

Шкала оценивания

Этап освоения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания
СК-2.2 способность применять знание основ внешнеполитической деятельности в борьбе с транснациональным терроризмом, религиозным экстремизмом, с угрозами информационной безопасности России, в том числе в рамках научно-исследовательской работы.	- анализирует ход реализации внешнеполитической деятельности России в борьбе с транснациональным терроризмом, религиозным экстремизмом, с угрозами информационной безопасности России; - вырабатывает решения, учитывающие основные положения теории международных отношений и Концепции внешней политики России; - даёт качественную оценку конкретным международным ситуациям в сфере борьбы с транснациональным терроризмом, религиозным экстремизмом, с угрозами информационной безопасности; - разрабатывает управленческие решения в области внешней политики России с учётом основ теории государственного управления и теории международных отношений и внешней политики.	Посещает учебные занятия по дисциплине для получения итоговой оценки. Вовлечен в групповую работу в аудитории. Добросовестно выполняет самостоятельную работу. Свободно использует научную терминологию. Свободно использует карты и другие наглядные вспомогательные материалы. При ответе выстраивает логичную систему аргументов, подкрепленных конкретными примерами. Демонстрирует творческое, гибкое мышление.	Устный опрос Тестирование по основным категориям и понятиям. Доклад Контрольная работа Решение ситуационных задач Отчет о практике Подготовка и защита ВКР.

Этап освоения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания
СК-3.3 способность применять в профессиональной деятельности знание методов прогнозирования в сфере внешней политики, правовых основ международной деятельности России, специфики внешнеполитической деятельности России в борьбе с транснациональным терроризмом и угрозами информационной безопасности для формирования современных систем национальной и международной безопасности, эффективной внешней политики Российской Федерации в условиях современной мировой политики и международных отношений, в том числе в рамках научно-исследовательской работы.	- анализирует результаты прогноза международной ситуации; - самостоятельно прогнозирует развитие международной ситуации в сфере безопасности с учетом правовых основ международной деятельности России; - дает качественную оценку эффективности внешнеполитической деятельности России в борьбе с транснациональным терроризмом и угрозами информационной безопасности; - разрабатывает управленческие решения для формирования эффективной современных систем национальной и международной безопасности, эффективной внешней политики Российской Федерации	Посещает учебные занятия по дисциплине для получения итоговой оценки. Вовлечен в групповую работу в аудитории. Добросовестно выполняет самостоятельную работу. Свободно использует научную терминологию. Свободно использует карты и другие наглядные вспомогательные материалы. При ответе выстраивает логичную систему аргументов, подкрепленных конкретными примерами. Демонстрирует творческое, гибкое мышление.	Устный опрос Тестирование по основным категориям и понятиям. Доклад Контрольная работа Решение ситуационных задач Отчет по практике Отчет о НИР Подготовка и защита ВКР.

4.4. Методические материалы

Оценивание обучающихся в процессе поэтапного освоения ими компетенций, формируемых данной дисциплиной осуществляется в форме зачета, который предполагает оценивание *умений и навыковс помощью* устных ответов на вопросы билета и решения ситуационных задач и/или кейс-задания.

К зачету допускаются студенты, выполнившие все требования учебной программы, выполнившие в установленные сроки все виды заданий и работ, не имеющим задолженностей по итогам текущего контроля успеваемости.
Подготовка к зачету предусматривает устное повторение пройденного учебного материала по дисциплине (с использованием конспектов, учебных пособий, дополнительной литературы), а также дополнительное конспектирование этих источников по перечню вопросов, выносимых на зачет.
Зачет принимает лектор. Умения и навыки обучающегося на зачете оцениваются «зачтено» или «незачтено».

Оценивание обучающегося на зачете по дисциплине

Оценка	Критерии оценки	Результаты обучения
«зачтено»	- знает сущность и содержание категорий и понятий в области информационной безопасности; - знает теоретические и методологические основы обеспечения международной информационной безопасности; - знает пути и способы разрешения противоречия и предотвращения кризисных ситуаций в сфере обеспечения международной информационной безопасности. - знает методики анализа состояния международной информационной безопасности; - знает теорию и практику организации управленческой деятельности в сфере обеспечения международной информационной безопасности; - знает технологии эффективного управления в сфере международной информационной безопасности; - знает технологии критической оценки информации и выработки решений на основе анализа и синтеза; - знает принципы, средства и методы критической оценки информации и конструктивного принятия решений на основе анализа и синтеза; - знает проблемы обеспечения международной информационной безопасности; - умеет на основе научных подходов анализировать различные управленческие ситуации в сфере международной информационной безопасности; - умеет анализировать различные ситуации в практической управленческой деятельности, идентифицировать и грамотно	СК-2.2 На уровне умений: - с помощью специальных средств ИКТ выбирать и анализировать индикаторы и критерии оценки состояния информационной защищенности личности, общества и государства; - работать с научными базами данных и другими источниками научной информации при помощи современных информационно-коммуникативных технологий; На уровне навыков: - навыками оценки состояния массмедийной инфраструктуры и киберсреды по критерию антитеррористического противоборства; - навыками использования материально-технических средств при проведении исследований в сфере

	интерпретировать тенденции и закономерности изменений в объектах управления; - умеет системно анализировать командную деятельность по реализации международных проектов в сфере международной информационной безопасности; - умеет применять технологии эффективного управления в сфере международной информационной безопасности; - умеет выявлять новые, ранее неизвестные и скрытые возможности и угрозы для стабильного функционирования системы международной информационной безопасности;	обеспечения информационной безопасности и решении административных задач; - навыками разработки и реализации программ исследований информационных процессов с помощью современных технических средств; СК-3.3 На уровне умений: - осуществлять аналитическое обеспечение принятия управленческих решений в области обеспечения информационной безопасности, На уровне навыков: - разработки и реализации программ исследований информационных процессов с помощью современных технических средств; - разработки управленческих решений в области обеспечения информационной безопасности
«незачтено»	- не знает сущность и содержание категорий и понятий в области информационной безопасности; - не знает теоретические и методологические основы обеспечения международной информационной безопасности; - не знает пути и способы разрешения противоречия и предотвращения кризисных ситуаций в международной информационной безопасности. - не знает методики анализа состояния международной информационной безопасности; - не знает теорию и практику организации управленческой деятельности в сфере обеспечения международной информационной безопасности; - не знает технологии эффективного управления в сфере международной информационной безопасности; - не знает технологии критической оценки информации и выработки решений на основе анализа и синтеза; - знает принципы, средства и методы критической оценки информации и конструктивного принятия решений на основе анализа и синтеза; - не знает проблемы обеспечения международной информационной безопасности; - не умеет на основе научных подходов анализировать различные управленческие ситуации в сфере международной информационной безопасности; - не умеет анализировать различные ситуации в практической управленческой деятельности,	

	идентифицировать и грамотно интерпретировать тенденции и закономерности изменений в объектах управления; - не умеет системно анализировать командную деятельность по реализации международных проектов в сфере международной информационной безопасности; - не умеет применять технологии эффективного управления в сфере международной информационной безопасности; - не умеет выявлять новые, ранее неизвестные и скрытые возможности и угрозы для стабильного функционирования системы международной информационной безопасности;	

Опрос.

Опрос проводится по темам 1, 2, 3, 4 и реализуется на основе разноуровневых задач и заданий:

а) ***репродуктивного уровня***, позволяющие оценить и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины.

Разные задания этого уровня оцениваются на основании следующих *критериев:*

– точность воспроизведения учебного материала (воспроизведение терминов, алгоритмов, методик, правил, фактов и т.п.);

– точность в описании фактов, явлений, процессов с использованием терминологии;

– точность различения и выделения изученных материалов;

б) ***реконструктивного уровня***, позволяющие оценить и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;

Критерием оценки является:

– продемонстрирована способность анализировать и обобщать информацию;

– продемонстрирована способность синтезировать на основе данных новую информацию;

– сделаны обоснованные выводы на основе интерпретации информации, разъяснения;

– установлены причинно-следственные связи, выявлены закономерности;

в) **творческого уровня**, позволяющие оценить и диагностировать умения интегрировать знания различных областей, аргументировать собственную точку зрения.

Критерии оценки:

– продемонстрирована способность оценивать, делать заключения с учетом внутренних условий или внешних критериев;

– продемонстрирован междисциплинарный подход к решению задачи, осуществлена интеграция знаний из разных научных областей;

– сформулированы критерии для оценки, создана система доказательств, убедительно аргументирующая выводы, положенные в основу решения задачи.

Оценка «5» Задание выполнено полностью

Оценка «4» Задание выполнено с незначительными погрешностями

Оценка «3» Обнаруживает знание и понимание большей части задания

При оценке доклада используются следующие критерии (каждый критерий - 1 балл):
– соответствие выступления теме, поставленным целям и задачам;
– проблемность / актуальность;
– новизна / оригинальность полученных результатов;
– глубина / полнота рассмотрения темы;
– доказательная база / аргументированность / убедительность / обоснованность выводов;
– логичность / структурированность / целостность выступления;
– речевая культура (стиль изложения, ясность, четкость, лаконичность, красота языка, учет аудитории, эмоциональный рисунок речи, доходчивость, пунктуальность, невербальное сопровождение, оживление речи афоризмами, примерами, цитатами и т.д.);
– используются ссылки на информационные ресурсы (сайты, литература);
– наглядность / презентабельность (если требуется);
– самостоятельность суждений / владение материалом / компетентность.
Оценка «5» Доклад соответствует всем критериям
Оценка «4» Доклад выполнен с незначительными погрешностями
Оценка «3» Доклад соответствует большей части критериев оценки
Общая оценка за доклад учитывает также его презентацию, и ответы на вопросы.

Критерии оценки текста контрольной работы и защиты.
- актуальность и прикладная значимость;
- информационная достаточность;
- соответствие материала теме и плану;
- стиль и язык изложения (целесообразное использование терминологии, пояснение новых понятий, лаконичность, логичность, правильность применения и оформления цитат и др.);
- наличие выраженной собственной позиции;
- оформление;
- адекватность и количество использованных источников (7 – 10);
- владение материалом;
- наличие и качество презентационного материала;
- полнота и качество ответов на вопросы.
Оценка «5» Контрольная работа соответствует всем критериям
Оценка «4» Контрольная работа выполнена с незначительными погрешностями
Оценка «3» Контрольная работа соответствует большей части критериев оценки

Тесты.
Тестирование проводится по теме 2 и 3 и реализуется на основе блока тестовых заданий.
Оценочные параметры тестового задании (пример):
Длительность контроля - 15 мин, предлагаемое количество заданий -10.
Критерием оценки выступает количество выполненных заданий:
Оценка «5» : 9-10 правильных ответов
Оценка «4» : 7-8 правильных ответов
Оценка «3»: 5-6 правильных ответов

Ситуационные задачи
Ситуационные задачи представляются к решению по теме 4 и реализуется на основе :
а) репродуктивного уровня, позволяющие оценить и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины.
Разные задания этого уровня оцениваются на основании следующих критериев:
– точность воспроизведения учебного материала (воспроизведение терминов, алгоритмов, методик, правил, фактов и т.п.);

– точность в описании фактов, явлений, процессов с использованием терминологии;
– точность различения и выделения изученных материалов;
б) реконструктивного уровня, позволяющие оценить и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей;
Критерием оценки является:
– продемонстрирована способность анализировать и обобщать информацию;
– продемонстрирована способность синтезировать на основе данных новую информацию;
– сделаны обоснованные выводы на основе интерпретации информации, разъяснения;
– установлены причинно-следственные связи, выявлены закономерности
Критерии оценки:
– продемонстрирована способность оценивать, делать заключения с учетом внутренних условий или внешних факторов;
– продемонстрирован междисциплинарный подход к решению задачи, осуществлена интеграция знаний из разных научных областей;
– сформулированы критерии для оценки, создана система доказательств, убедительно аргументирующая выводы, положенные в основу решения задачи.
Оценка «5» Задание выполнено полностью
Оценка «4» Задание выполнено с незначительными погрешностями
Оценка «3» Обнаруживает знание и понимание большей части задания

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

Цель методических рекомендаций - обеспечить студенту оптимальную организацию процесса изучения дисциплины, а также выполнения различных форм самостоятельной работы.
Студентам необходимо ознакомиться: с содержанием рабочей программы дисциплины, с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимся на образовательном портале и сайте кафедры, с графиком консультаций преподавателей кафедры.
Рекомендации по подготовке к лекционным занятиям (теоретический курс).
Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры.
Студентам необходимо:
- перед каждой лекцией просматривать рабочую программу дисциплины, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;
- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;
- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущей лекции. При затруднениях в восприятии материала следует обратиться к основным литературным источникам. Если разобраться в материале опять не удалось, то обратитесь к лектору (по графику его консультаций) или к преподавателю на практических занятиях.
Рекомендации по подготовке к практическим (семинарским) занятиям.
Студентам следует:

- приносить с собой рекомендованную преподавателем литературу к конкретному занятию;
- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия и отработать задания, определённые для подготовки к практическому занятию;
- при подготовке к практическим занятиям следует обязательно использовать не только лекции, учебную литературу, но и нормативно-правовые акты и материалы правоприменительной практики;
- теоретический материал следует соотносить с правовыми нормами, так как в них могут быть внесены изменения, дополнения, которые не всегда отражены в учебной литературе;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- в ходе практического занятия давать конкретные, четкие ответы по существу вопросов;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

Методические рекомендации по подготовке доклада.

Одной из форм самостоятельной работы студента является подготовка научного доклада, для обсуждения его на практическом (семинарском) занятии по темам 1, 2, 4.

Цель научного доклада - развитие у студентов навыков аналитической работы с научной литературой, анализа дискуссионных научных позиций, аргументации собственных взглядов. Подготовка научных докладов также развивает творческий потенциал студентов.

Научный доклад готовится под руководством преподавателя, который ведет практические (семинарские) занятия.

Рекомендации студенту:
- перед началом работы по написанию научного доклада согласовать с преподавателем тему, структуру, литературу, а также обсудить ключевые вопросы, которые следует раскрыть в докладе;
- представить доклад научному руководителю в письменной форме;
- выступить на семинарском занятии с 10-минутной презентацией своего научного доклада, ответить на вопросы студентов группы.

Требования:
- к оформлению научного доклада: шрифт – Times New Roman, размер шрифта - 14, межстрочный интервал - 1,5, размер полей - 2,5 см, отступ в начале абзаца - 1,25 см, форматирование по ширине); листы доклада скреплены скоросшивателем. На титульном листе указывается наименование учебного заведения, название кафедры, наименование дисциплины, тема доклада, ФИО студента;
- к структуре доклада - оглавление, введение (указывается актуальность, цель и задачи), основная часть, выводы автора, список литературы (не менее 5 позиций). Объем согласовывается с преподавателей. В конце работы ставится дата ее выполнения и подпись студента, выполнившего работу.

Методические рекомендации по подготовке, написанию и оформлению контрольной работы

Выполнение контрольной работы проводится по теме 1 с целью формирования общепрофессиональных компетенций и способностей к научно-исследовательской работе, позволяющих:
- осуществлять поиск и использование информации (в том числе справочной, нормативной и правовой), сбор данных с применением современных информационных технологий, необходимых для решения профессиональных задач;

- выбирать инструментальные средства для обработки данных в соответствии с поставленной задачей, применяя современный математический и статистический аппарат, программные продукты;
- анализировать результаты расчетов, используя современные методы интерпретации данных, обосновывать полученные выводы.

Темы контрольных работ предлагаются студентам на выбор. Студент имеет право выбрать одну из заявленных тем или тема контрольной работы может быть предложена студентом при условии обоснования им ее целесообразности.

Контрольная работа должна содержать:
- введение, в котором обосновывается актуальность темы, формулируются цели и задачи работы;
- основную часть, в которой раскрывается содержание исследуемой проблемы;
- заключение, в котором содержатся выводы и рекомендации относительно практического применения материалов работы;
- список используемых источников и интернет-ресурсов;

Общий объем контрольной работы до 10 страниц.

Работа оформляются 14 шрифтом Times New Roman через 1,5 межстрочный интервал, выравнивание текста - по ширине страницы.

Иллюстрации (графики, схемы, диаграммы) следует располагать непосредственно после текста, в котором они упоминаются впервые, или на следующей странице. На все иллюстрации должны быть даны ссылки в работе. Иллюстрации следует нумеровать арабскими цифрами сквозной нумерацией.

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Наименование таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Наименование таблицы следует помещать над таблицей слева, без абзацного отступа в одну строку с ее номером. Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице. На все таблицы должны быть ссылки в тексте. При ссылке следует писать слово «таблица» с указанием ее номера.

Нумерация страниц документа должна быть сквозная.

В тексте документа не допускается:
- применять обороты разговорной речи;
- применять произвольные словообразования;
- применять сокращения слов, кроме установленных правилами русской орфографии;

Оформление библиографии производится в соответствии с ГОСТ. Список использованных источников, как правило, содержит сплошную нумерацию.

Методические рекомендации по подготовке к решению ситуационных задач

Ситуационные задачи (кейс-технологии) - инструмент, с помощью которого значительно облегчается и качественно улучшается обмен идеями в группе. Ситуационные задачи базируются на реальной информации, однако, как правило, при разработке кейсов используются условные названия и фактические данные могут быть несколько изменены. Ситуационные задачи являются способом повышения интереса учащихся к изучаемому предмету. Кроме того, они позволяют интегрировать знания, полученные в процессе изучения разных предметов. Умело составленные ситуационные задачи могут выступать в качестве ресурса развития мотивации учащихся к познавательной деятельности.

Ситуационные задачи реализуется на основе :

а) репродуктивного уровня, позволяющие оценить и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины.

Разные задания этого уровня оцениваются на основании следующих критериев:

– точность воспроизведения учебного материала (воспроизведение терминов, алгоритмов, методик, правил, фактов и т.п.);
– точность в описании фактов, явлений, процессов с использованием терминологии;
– точность различения и выделения изученных материалов;
б) реконструктивного уровня, позволяющие оценить и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей

Методические рекомендации по выполнению различных форм самостоятельных домашних заданий.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Студентам следует:

- руководствоваться графиком самостоятельной работы, определенным РПД;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на семинарах и консультациях неясные вопросы;
- использовать при подготовке методические разработки кафедры по написанию рефератов, эссе, контрольных работ;
- при подготовке к промежуточному контролю параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на плановой консультации.

Методические рекомендации по работе с литературой.

Любая форма самостоятельной работы студента (подготовка к семинарскому занятию, написание эссе, контрольной работы, доклада и т.п.) начинается с изучения соответствующей литературы как в библиотеке, так и дома.

К каждой теме учебной дисциплины подобрана основная и дополнительная литература.

Основная литература - это учебники и учебные пособия.

Дополнительная литература - это монографии, сборники научных трудов, журнальные и газетные статьи, различные справочники, энциклопедии, интернет ресурсы.

Рекомендации студенту:

- выбранную монографию или статью целесообразно внимательно просмотреть. В книгах следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие. Целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения. Такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, а какие прочитать быстро;
- в книге или журнале, принадлежащие самому студенту, ключевые позиции можно выделять маркером или делать пометки на полях. При работе с Интернет-источником целесообразно также выделять важную информацию;
- если книга или журнал не являются собственностью студента, то целесообразно записывать номера страниц, которые привлекли внимание. Позже следует возвратиться к ним, перечитать или переписать нужную информацию. Физическое действие по записыванию помогает прочно заложить данную информацию в «банк памяти».

Выделяются следующие виды записей при работе с литературой:

Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов. Хороший конспект должен сочетать полноту изложения с краткостью.
Цитата - точное воспроизведение текста. Заключается в кавычки. Точно указывается страница источника.
Тезисы - концентрированное изложение основных положений прочитанного материала.
Аннотация - очень краткое изложение содержания прочитанной работы.
Резюме - наиболее общие выводы и положения работы, ее концептуальные итоги. Записи в той или иной форме не только способствуют пониманию и усвоению изучаемого материала, но и помогают вырабатывать навыки ясного изложения в письменной форме тех или иных теоретических вопросов.

Вопросы для самостоятельной подготовки к семинарским занятиям

Тема 1.

Лекция: Основы политики международной информационной безопасности.

1. Развитие информационного общества и информационная безопасность: теоретико-методологические аспекты исследования.
2. Философия информационной безопасности. Переход к информационному обществу и возрастание угроз международной информационной безопасности.
3. Геокультурное, геоидеологическое и геоинформационное пространство. Трансформация традиционной геополитики в информационную.

Практическое занятие: Теория и практика управления безопасностью международных информационных процессов.

1. Методы анализа и управления состояниями и процессами информационной безопасности.
2. Массовая информационная сфера как объект управления.
3. Идеология как теоретическая основа управления информационными процессами. Технологии достижения глобального демонстрационного эффекта, «эффекта лавины».
4. Технологии «мягкой силы»: культурно-лингвистическая экспансия. Проблемы формализации международных коммуникационных процессов.

Тема 2.

Лекция: Правовое обеспечение политики в сфере информационной безопасности.

1. Устав ООН о способах разрешения международных споров информационными средствами.
2. Информационное обеспечение международных актов: правовое, политическое, организационное содержание и реализация.
3. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года

Практическое занятие: Обеспечение безопасности государственных информационных ресурсов.

1. Зависимость структуры системы современного миропорядка от состояния информационных ресурсов (потенциалов) международных акторов.
2. Условия формирование нового мирового порядка, сопутствующие им информационные вызовы международной безопасности: информационная насыщенность современного мира, публичность, транспарентность межгосударственных отношений. Эффекты социально-политической темпоральности.
3. Состояние и перспективы формирования и развития государственных информационных

ресурсов.

Тема 3.
Лекция: Основы безопасности глобальных информационных сетей

1. Общая характеристика безопасности глобальных сетей.
2. Деятельность рабочих групп по национальным и региональным стратегиям использования электронных технологий.
3. Противодействие угрозам безопасности информационных и телекоммуникационных средств и систем.

Практическое занятие: Международное сотрудничество в области противодействия кибертерроризму
1. Региональные центры использования ИКТ. Серия международных конференций по развитию информатизации международных связей (2000-2015гг.).
2. Разработка и реализация международной программы развития людских ресурсов и наращиванию потенциала: взаимодействие с учреждениями ООН, представителями частного и государственного секторов.
3. Основные инициативы Российской Федерации в области МИБ. Конвенция «Об обеспечении международной информационной безопасности» (2011 г.).

Тема 4.
Лекция: Безопасность системы массовой информации и коммуникации.

1. Национальные/транснациональные массовые информационные системы.
2. Средства массовой информации как критически важные структуры системы международных отношений.
3. Роль СМИ в балансе сил в международных отношениях. СМИ и гибридные образования как источники глобальных угроз: объединение государственных и негосударственных структур в области бизнеса и СМИ. Влияние СМИ на формирование геокультуры Запада, Евразийского региона, Центрально-Азиатского региона и др.

Практическое занятие: Информационная безопасность как условие предотвращения информационно-психологической войны.

1. Информационное противоборство. Основные научные концепции информационно-психологических войн.
2. Базовые категории и теоретическое обоснование понятий «информационное противоборство», «информационная война», «мягкая сила».
3. Теория, приемы, средства, методы и системы ведения информационной войны.
4. Тенденции и перспективы обеспечения информационно-психологической безопасности: российские инициативы и практики.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6.1. Основная литература.
Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.

— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А. — Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— Режим доступа: http://www.iprbookshop.ru/52524.— ЭБС «IPRbooks»

Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks»

Афанасьев А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам [Электронный ресурс]: учебное пособие/ Афанасьев А.А., Веденьев Л.Т., Воронцов А А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 550 с.— Режим доступа: http://www.iprbookshop.ru/11978.— ЭБС «IPRbooks»

Бухарин С.Н. Методы и технологии информационных войн [Электронный ресурс]/ Бухарин С.Н., Цыганов В.В.— Электрон. текстовые данные.— М.: Академический Проект, 2015.— 384 с.— Режим доступа: http://www.iprbookshop.ru/36847.— ЭБС «IPRbooks»

6.2. Дополнительная литература.

Специальная связь и безопасность информации: технологии, управление, экономика [Электронный ресурс]: сборник трудов 3-го Международного научного симпозиума. Россия, Краснодар - пос. Терскол, Кабардино-Балкарской республики, 25-28 апреля 2014 г./ А.Ш. Альбеков [и др.].— Электрон. текстовые данные.— М.: Русайнс, 2015.— 126 с.— Режим доступа: http://www.iprbookshop.ru/48970.— ЭБС «IPRbooks»

Сотов А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации [Электронный ресурс]: монография/ Сотов А.И.— Электрон. текстовые данные.— М.: Русайнс, 2015.— 128 с.— Режим доступа: http://www.iprbookshop.ru/48904.— ЭБС «IPRbooks»

Ворона В.А. Комплексные интегрированные системы обеспечения безопасности [Электронный ресурс]: учебное пособие/ Ворона В.А., Тихонов В.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 160 с.— Режим доступа: http://www.iprbookshop.ru/11989.— ЭБС «IPRbooks»

6.3. Учебно-методическое обеспечение самостоятельной работы.

<u>Тема 1.</u>

Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные. — М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А. — Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— Режим доступа: http://www.iprbookshop.ru/52524.— ЭБС «IPRbooks»

Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks»

Тема 2.

Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные. — М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А. — Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— Режим доступа: http://www.iprbookshop.ru/52524.— ЭБС «IPRbooks»

Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks»

Тема 3.

Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные. — М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А. — Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— Режим доступа: http://www.iprbookshop.ru/52524.— ЭБС «IPRbooks»

Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— М.: Всероссийский государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks»

Тема 4.

Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные. — М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.— ЭБС «IPRbooks»

Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза [Электронный ресурс]: монография/ Смирнов А.А. — Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 159 с.— Режим доступа: http://www.iprbookshop.ru/52524.— ЭБС «IPRbooks»

Кубанков А.Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект [Электронный ресурс]: учебное пособие/ Кубанков А.Н., Куняев Н.Н.— Электрон. текстовые данные.— М.: Всероссийский

государственный университет юстиции (РПА Минюста России), 2014.— 78 с.— Режим доступа: http://www.iprbookshop.ru/47262.— ЭБС «IPRbooks»

6.4. Нормативные правовые документы.

Стратегии национальной безопасности РФ 31 декабря 2015 г.
Концепция внешней политики РФ 30 ноября 2016 г.
Военная доктрина Российской Федерации 25 декабря 2014 г., № Пр-2976
Доктрина информационной безопасности РФ 5 декабря 2016 г.
Указ Президента Российской Федерации от 7 мая 2012 г. N 605 "О мерах по реализации внешнеполитического курса Российской Федерации"
Нормативные правовые акты Российской Федерации, регулирующие деятельность федеральных органов государственной власти в сфере внешней политики
Федеральный закон от 28 декабря 2010 г. N 390-ФЗ "О безопасности"
Федеральный закон от 28 июня 2014 г. N 172-ФЗ "О стратегическом планировании в Российской Федерации"
Международная конвенция о борьбе с бомбовым терроризмом (Нью-Йорк, 15 декабря 1997 г.) // Собрание законодательства Российской Федерации от 27 августа 2001 г., N 35, ст. 3513
Международная конвенция о борьбе с финансированием терроризма (принята резолюцией 54/109 Генеральной Ассамблеи ООН от 9 декабря 1999 г.) // Собрание законодательства Российской Федерации от 24 марта 2003 г. N 12 ст. 1059
Международная конвенция о борьбе с актами ядерного терроризма (принята резолюцией N A/Res/59/290 Генеральной Ассамблеи ООН от 13 апреля 2005 г.) (не вступила в силу) // Московский журнал международного права, октябрь - декабрь 2005 г., N 4
Соглашение о сотрудничестве государств - участников Содружества по обеспечению стабильного положения на их внешних границах (Бишкек, 9 октября 1992 г.) // Бюллетень международных договоров, 1993 г., N 10, стр. 16.
Шанхайская Конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом (Шанхай, 15 июня 2001 г.) // Собрание законодательства Российской Федерации от 13 октября 2003 г. N 41 ст. 3947
Соглашение между государствами - членами Шанхайской организации сотрудничества о Региональной антитеррористической структуре (Санкт-Петербург, 7 июня 2002 г.) // Собрание законодательства Российской Федерации от 29 ноября 2004 г. N 48 ст. 4692
Хартия Шанхайской организации сотрудничества (Санкт-Петербург, 7 июня 2002 г.) // Собрание законодательства Российской Федерации от 23 октября 2006 г. N 43 ст. 4417
Договор о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с терроризмом (Минск, 4 июня 1999 г.) // Собрание законодательства Российской Федерации от 29 мая 2006 г. N 22 ст. 2291
Устав Организации Объединенных Наций (Сан-Франциско, 26 июня 1945 г.)
Договор о коллективной безопасности (Ташкент, 15 мая 1992 г.) // «Российская газета» от 23 мая 1992 г.
Федеральный закон от 7 августа 2000 г. N 121-ФЗ «О ратификации Европейской конвенции о пресечении терроризма» // «Российская газета» от 10 августа 2000 г.
Резолюция Совета Безопасности ООН от 28 сентября 2001 г. N 1373 (2001) // «Московский журнал международного права», январь-март 2002 г., N 1.
Федеральный закон от 10 января 2003 г. N 3-ФЗ «О ратификации Шанхайской конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом» // «Российская газета» от 14 января 2003 г.

6.5. Интернет-ресурсы.

http:/www.kremlin.ru – официальный сайт Президента Российской Федерации.

http:/www.mid.ru – официальный сайт Министерства иностранных дел Российской Федерации.

http://www.coe.int – Совет Европы.

http://www.rsl.ru – Российская Государственная Библиотека

www.un.org – Организация Объединенных Наций

http://www.osce.org/ - Организация по безопасности и сотрудничеству в Европе

http://www.odkb-csto.org/ - Организация Договора о коллективной безопасности

http://www.scrf.gov.ru/ - Совет безопасности РФ

www.government.ru – интернет-портал Правительства Российской Федерации.

http://minsvyaz.ru/ru/ – Минкомсвязи

http://www.rossvyaz.ru/ – Федеральное агентство связи

http://www.rsoc.ru/ - Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

http://www.fapmc.ru/magnoliaPublic/rospechat.html – Федеральное агентство по печати и массовым коммуникациям

http://www.fsb.ru/ – Федеральная служба безопасности

http://www.council.gov.ru/ – Совет Федерации Федерального собрания РФ (Комиссия по информационной политике)

http://www.duma.gov.ru/ – Государственная дума Федерального собрания РФ (Комитет по информационной политике)

http://www.nak.fsb.ru – Национальный антитеррористический комитет (НАК) -

http://www.infoforum.ru – Национальный форум информационной безопасности (Инфофорум)

http://www.un.int/russia/new/MainRootrus/index_plain.html – Россия в ООН

http://www.infolaw.rniiis.ru – Информационное право (журнал)

http://www.frip.ru/ - Фонд развития информационной политики

6.6. Иные источники.

Арбатов А.Г. Дворкин В.З., Пикаев А.А., Ознобищев С.К. Стратегическая стабильность после холодной войны. М.: ИМЭМО РАН, 2010.

Зверев П.Г. Международное миротворчество в свете вызовов международной безопасности в начале XXI в. // Актуальные проблемы гуманитарных и естественных наук. 2014. №4-2.

Золотарёв П. Глобальное измерение войны. Новые подходы в XXI веке // Россия в глобальной политике. № 1, 2010.

Интересы России в Центральной Азии: содержание, перспективы, ограничители. 2013, №10.

Искакова Г.К. Региональная безопасность в Центральной Азии и стратегии России, США и Китая // PolitBook. 2014, №4.

Кортунов С. В. Россия в мировой политике после кризиса / С. В. Кортунов. – М. : Красная звезда, 2011.
Назарова А.И. Теоретические вопросы обеспечения международной безопасности / А. И. Назарова // Молодой ученый. — 2014. — №4. — С. 859-861.
Полосин А.В. Региональные параметры национальной безопасности // Власть. №12,2011.
Рогов С., Есин В., Золотарев П., Кузнецов В. ПРО для США стало религией // Независимое военное обозрение. 6 июля 2012.
Сурчина С. Особенности международного сотрудничества государств в области физической ядерной безопасности // Международная жизнь. 2015. №12.

7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Специализированные залы для проведения лекций и аудитории для проведения семинарских и практических занятий с использованием мультимедийного оборудования и возможностью прямого выхода в сеть Интернет.
2. Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами.
3. Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.
4. Лицензионные электронные ресурсы: Windows, Microsoft Office (Excel, InfoPath, PowerPoint, Publisher, Word).
5. Информационные справочные и поисковые системы «Консультант Плюс», «Гарант».