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

Институт государственной службы и управления

Кафедра зарубежного регионоведения и международного сотрудничества

УТВЕРЖДЕНА

решением кафедры зарубежного регионоведения и международного сотрудничества

Протокол от «05» сентября 2016 г. № 1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.4.2 Информационная безопасность

(индекс, наименование дисциплины (модуля), в соответствии с учебным планом)

Инф.безоп.

(краткое наименование дисциплины (модуля))

41.03.01 «Зарубежное регионоведение»

(код, наименование направления подготовки)

Информационно-аналитическое обеспечение международного сотрудничества

(направленность (профиль))

бакалавр

(квалификация)

очная

(форма(ы) обучения)

Год набора - 2016

Москва, 2016 г.

Автор–составитель:

Доцент, кандидат политических наук И.Н. Кохтюлина

Заведующий кафедрой

Заведующий кафедрой зарубежного регионоведения и международного сотрудничества (ЗРиМС), доктор социологических наук В.В.Комлева

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

1.1 Дисциплина Б1.В.ДВ.4.2 Информационная безопасность обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-5	владением знаниями об основных тенденциях развития ключевых интеграционных процессов современности	ПК-5.3	Способность ориентироваться в основных тенденциях развития ключевых интеграционных процессов современности

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

ОТФ/ТФ (при наличии профстандарта или по результатам форсайт-сессии)	Код этапа освоения компетенции	Результаты обучения
готовить обзоры, информационные, аналитические материалы по вопросам международного сотрудничества, развития зарубежных регионов, региональной политики, общественно-политического, социально-экономического, социокультурного развития регионов	ПК-5.3	на уровне знаний: демонстрирует знания понятия и принципов информационной безопасности
		на уровне умений: оценивает целесообразность и эффективность использования различных мер информационной безопасности
		на уровне навыков: анализирует угрозы информационной безопасности, понимает их природу

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость Б1.В.ДВ.4.2 Информационная безопасность составляет 2 зачётные единицы, 72 часа. Количество академических часов, выделенных на контактную работу с преподавателем, составляет 36 часов: лекционные занятия – 18 часов, практические занятия – 18 часов. Самостоятельная работа составляет 36 часов.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.4.2 Информационная безопасность предусмотрена на 4 курсе, в 7 семестре.

Дисциплина Б1.В.ДВ.4.2 Информационная безопасность относится к дисциплинам Блока 1 «Дисциплины (модули)».

В содержательном плане дисциплина является основой для изучения Б1.В.ДВ.6.1 Гуманитарное вмешательство и миротворчество (8 семестр), Б1.В.ДВ.10.1 Международное сотрудничество в области защиты прав человека (8 семестр).

Форма промежуточной аттестации в соответствии с учебным планом – зачет.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем (разделов),	Объем дисциплины , час.						Форма текущего контроля успеваемости**, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Раздел 1. Национальная безопасность России в условиях информационной глобализации								
1.1	Информационно-коммуникационные технологии – локомотив глобализации	18	2		2		4	О,Д
1.2	Эволюция становления информационной составляющей национальной безопасности России	9	2		2		4	О,Д
Раздел 2. Информационная безопасность России в контексте Госпрограммы «Информационное общество 2011-2020»								
2.1	Приоритеты и цели государственной политики в сфере развития информационного общества в Российской Федерации	9	2		2		4	О,Д
2.2	Основные мероприятия Госпрограммы «Информационное общество 2011-2020»	9	2		2		4	О,Д
2.3	Прогноз конечных результатов реализации Госпрограммы «Информационное общество 2011-2020»	9	2		2		4	О,Д
Раздел 3. Информационное противоборство и безопасность								
3.1	Основы информационного противоборства	9	4		4		8	О,Д
3.2	Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики	9	4		4		8	О,Д
Промежуточная аттестация								За
Всего:		72	18		18		36	

Примечание:

*** – формы текущего контроля успеваемости: опрос (О), диспут (Д), реферат (Р).*

**** - формы промежуточной аттестации: зачет (За).*

Содержание дисциплины

Раздел 1. Национальная безопасность России в условиях информационной глобализации

1.1 Информационно-коммуникационные технологии – локомотив глобализации

Базовые понятия и отличительные черты информационного общества. Теоретические концепции информационного общества. Электронное правительство. Международный опыт создания электронного правительства.

Проблемы и перспективы формирования в России электронного правительства

1.2 Эволюция становления информационной составляющей национальной безопасности России

Информационная безопасность: определение, сущность.

Государственная политика Российской Федерации в области информационной безопасности. Сущность и содержание государственной политики РФ в области информационной безопасности, цели и задачи. Законодательно-правовое обеспечение информационной безопасности в России.

Раздел 2. Информационная безопасность России в контексте Госпрограммы «Информационное общество 2011-2020»

2.1 Приоритеты и цели государственной политики в сфере развития информационного общества в Российской Федерации

Характеристика текущего состояния сферы создания и использования информационных и телекоммуникационных технологий в Российской Федерации.

2.2 Основные мероприятия Госпрограммы «Информационное общество 2011-2020»

Качество жизни граждан и условия развития бизнеса в информационном обществе, электронное государство и эффективность государственного управления, базовая инфраструктура информационного общества.

2.3. Прогноз конечных результатов реализации Госпрограммы «Информационное общество 2011-2020»

Изучение и анализ места России в различных международных рейтингах готовности к информационному обществу, электронному правительству. Изучение индекса транспарентности, рейтинга фактора «мягкой силы» и др.

Раздел 3. Информационное противоборство и безопасность

3.1. Основы информационного противоборства

Основные направления информационного противоборства. Новые объекты информационной безопасности: безопасность открытых информационных сетей, информационная безопасность бизнеса, информационно-психологическая безопасность, криминальные интересы, информационное оружие – новый вид оружия массового поражения.

Информационный (кибер-) терроризм

3.2. Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики

Россия – инициатор и локомотив продвижения МИБ.

Российские инициативы в области МИБ, история их выдвижения и продвижения. Альтернативные инициативы США. Расстановка сил на мировой арене в связи с российскими инициативами по МИБ. Формирование подходов к проблеме международной информационной безопасности в мире. Дискурс МИБ в ООН. Переговорный процесс и международное сотрудничество в области ограничения информационных видов оружия.

Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, «восьмерки», Евросоюза в области МИБ.
Нормативно-правовое обеспечение МИБ в России
Базовые положения «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года». Новая редакция Концепции внешней политики России о МИБ. Основные угрозы в области МИБ. Военно-политическая страта. «Цифровой джихад»: ИКТ в террористических целях, ИКТ и суверенитет России, киберпреступность. «Таллинское руководство» по ведению кибервойн НАТО.

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

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

4.1.1. В ходе реализации дисциплины Б1.В.ДВ.4.2 Информационная безопасность используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)		Методы текущего контроля успеваемости
Тема 1.1	Информационно-коммуникационные технологии – локомотив глобализации	Опрос, диспут
Тема 1.2	Эволюция становления информационной составляющей национальной безопасности России	Опрос, диспут
Тема 2.1	Приоритеты и цели государственной политики в сфере развития информационного общества в Российской Федерации	Опрос, диспут
Тема 2.2	Основные мероприятия Госпрограммы «Информационное общество 2011-2020»	Опрос, диспут
Тема 2.3	Прогноз конечных результатов реализации Госпрограммы «Информационное общество 2011-2020»	Опрос, диспут
Тема 3.1	Основы информационного противоборства	Опрос, диспут
Тема 3.2	Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики	опрос, защита реферата

4.1.2. Зачет в устной форме проводится с применением следующих методов (средств): в устной форме по вопросам.

4.2. Материалы текущего контроля успеваемости.

Преподаватель оценивает уровень подготовленности обучающихся к занятию по следующим показателям:

- устные ответы на вопросы преподавателя по теме занятия,
- выступление с докладами по вопросам к опросам (дискуссиям),
- участие в обсуждении докладов.

Критерии оценивания доклада:

- степень усвоения понятий и категорий по теме;
- умение работать с документальными и литературными источниками;
- грамотность изложения материала;

- самостоятельность работы, наличие собственной обоснованной позиции.

Оценка знаний, умений, навыков проводится на основе балльно-рейтинговой системы 70% из 100% (70 баллов из 100) - вклад по результатам посещаемости занятий, активности на занятиях, выступления с докладами, участия в обсуждениях докладов других обучающихся, ответов на вопросы преподавателя в ходе занятия, защита реферата.

Детализация баллов и критерии оценки текущего контроля успеваемости утверждается на заседании кафедры.

Вопросы темы для подготовки к опросам (дискуссиям) (темы докладов):

Раздел 1. Национальная безопасность России в условиях информационной глобализации

Тема 1.1 Информационно-коммуникационные технологии – локомотив глобализации.

1 Базовые понятия и отличительные черты информационного общества.
2 Теоретические концепции информационного общества.
3 Электронное правительство.
4 Международный опыт создания электронного правительства.
5 Проблемы и перспективы формирования в России электронного правительства

Тема 1.2 Эволюция становления информационной составляющей национальной безопасности России

1 Информационная безопасность: определение, сущность.
2 Государственная политика Российской Федерации в области информационной безопасности.
3 Сущность и содержание государственной политики РФ в области информационной безопасности, цели и задачи.
4 Законодательно-правовое обеспечение информационной безопасности в России.

Раздел 2. Информационная безопасность России в контексте Госпрограммы «Информационное общество 2011-2020»

Тема 2.1 Приоритеты и цели государственной политики в сфере развития информационного общества в Российской Федерации

1 Характеристика текущего состояния сферы создания и использования информационных и телекоммуникационных технологий в Российской Федерации.

Тема 2.2 Основные мероприятия Госпрограммы «Информационное общество 2011-2020»

1 Качество жизни граждан и условия развития бизнеса в информационном обществе.
2 Электронное государство и эффективность государственного управления.
3 Базовая инфраструктура информационного общества.

Тема 2.3 Прогноз конечных результатов реализации Госпрограммы «Информационное общество 2011-2020»

1 Изучение и анализ места России в различных международных рейтингах готовности к информационному обществу, электронному правительству.
2 Изучение индекса транспарентности, рейтинга фактора «мягкой силы» и др.

Раздел 3. Информационное противоборство и безопасность

Тема 3.1. Основы информационного противоборства

1 Основные направления информационного противоборства.

2 Новые объекты информационной безопасности: безопасность открытых информационных сетей, информационная безопасность бизнеса, информационно-психологическая безопасность, криминальные интересы, информационное оружие – новый вид оружия массового поражения.
3 Информационный (кибер-) терроризм

Тема 3.2. Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики

1 Россия – инициатор и локомотив продвижения МИБ. Российские инициативы в области МИБ, история их выдвижения и продвижения.
2 Альтернативные инициативы США.
3 Расстановка сил на мировой арене в связи с российскими инициативами по МИБ.
4 Формирование подходов к проблеме международной информационной безопасности в мире. Дискурс МИБ в ООН.
5 Переговорный процесс и международное сотрудничество в области ограничения информационных видов оружия.
6 Работа Комитетов ООН по безопасности и разоружению, по космосу, МСЭ, «восьмерки», Евросоюза в области МИБ.
7 Нормативно-правовое обеспечение МИБ в России
8 Базовые положения «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года».
9 Новая редакция Концепции внешней политики России о МИБ.
10 Основные угрозы в области МИБ.
11 Военно-политическая страта.
12 «Цифровой джихад»: ИКТ в террористических целях, ИКТ и суверенитет России, киберпреступность.
13 «Таллинское руководство» по ведению кибервойн НАТО.

Перечень тем рефератов и докладов по курсу:

1 Понятие информационного общества. Теоретические подходы
2 Измерение информационного общества Международным союзом электросвязи
3 Истинность и ошибочность тезиса: «Кто владеет информацией тот владеет миром».
4 Роль «цифровых аборигенов» в развитии информационного общества.
5 Международный опыт формирования электронного правительства.
6 Опыт Российской Федерации в формировании электронного правительства.
7 Актуальные проблемы перехода России к информационному обществу в контексте Государственной программы «Информационное общество 2011-2020».
8 Жизнь в информационном обществе: реальные проблемы и воздушные замки.
9 Изменение понятия «безопасности» в информационном обществе.
10 Стратегия национальной безопасности России до 2020 года об обеспечении информационной безопасности
11 Позиция России по обеспечению международной информационной безопасности в контексте «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» от 24 июля 2013 г.
12 Роль СМИ при подготовке, проведении и достижении базовых эффектов «цветных революций»
13 Использование информационно-коммуникационных технологий в продвижении фактора «мягкой силы» государства.

14 Базовые теоретико-методологические подходы к фактору «мягкой силы»
15 Дефиниции понятия «мягкая сила».
16 «Мягкая сила» по Дж.Наю.
17 Анализ рейтинга фактора «мягкой силы» по странам.
18 Критерии составляющих «мягкой силы».
19 Особенности «мягкой силы» США, ЕС, Китая и России.
20 Основные факторы, определяющие новые параметры проблемы обеспечения информационной безопасности
21 Изменение характера и приоритетности угроз международной информационной безопасности
22 Соотношение задач обеспечения национальной и международной информационной безопасности.
23 Изменение угроз и вызовов информационной безопасности на современном этапе.
24 Проблема международного информационного терроризма.
25 Изменение парадигм терроризма в информационном обществе.
26 Проблема распространения информационного оружия.
27 Проблема контроля над информационными вооружениями.
28 Сотрудничество и противоречия между США и европейскими странами по вопросам международной информационной безопасности.
29 Изменение характера и приоритетности угроз безопасности в информационном обществе.
30 Сотрудничество и расхождения в подходах в сфере обеспечения международной информационной безопасности между РФ и США.
31 Деятельность ООН по обеспечению международной информационной безопасности.

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Формируемые компетенции с указанием этапов их формирования в процессе освоения образовательной программы. Показатели и критерии оценивания компетенций с учетом этапа их формирования

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-5	владением знаниями об основных тенденциях развития ключевых интеграционных процессов современности	ПК-5.3	Способность ориентироваться в основных тенденциях развития ключевых интеграционных процессов современности

Этап освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
ПК-5.3 Способность ориентироваться в основных тенденциях развития ключевых интеграционных процессов	Анализ интересов, политических решений, стратегий и действий зарубежных акторов, анализ международных проектов, анализ	Ориентируется в основных тенденциях развития ключевых интеграционных процессов современности Дает оценку тенденциям развития ключевых

современности	целевых аудиторий (стейкхолдеров)	интеграционных процессов современности

4.3.2. Типовые оценочные средства

Вопросы к зачету

1. Понятия «информации», основные экспликации термина.
2. Информационное общество. Теоретические концепции информационного общества.
3. Базовые понятия и отличительные черты информационного общества.
4. Измерение информационного общества Международным союзом электросвязи.
5. Роль «цифровых аборигенов» в развитии информационного общества.
6. Международный опыт создания информационного общества.
7. Актуальные проблемы перехода России к информационному обществу в контексте Государственной программы «Информационное общество 2011-2020»
8. Электронное правительство – базовые понятия и термины.
9. Международный опыт формирования электронного правительства.
10. Проблемы и перспективы формирования в России электронного правительства.
11. Информационная безопасность – определение, сущность.
12. Государственная политика Российской Федерации в области информационной безопасности.
13. Сущность и содержание государственной политики РФ в области информационной безопасности, цели и задачи.
14. Законодательно-правовое обеспечение информационной безопасности в России.
15. Виды угроз информационной безопасности Российской Федерации.
16. Источники угроз информационной безопасности Российской Федерации.
17. Методы обеспечения информационной безопасности Российской Федерации.
18. Позиция России по обеспечению международной информационной безопасности в контексте «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года от 24.07.2013.
19. Цель и задачи государственной политики Российской Федерации в области МИБ. Четыре угрозы международной информационной безопасности.
20. Основные направления государственной политики Российской Федерации в области МИБ.
21. Механизмы реализации государственной политики Российской Федерации в сфере информационной безопасности.
22. Эволюция становления информационной составляющей национальной безопасности России
23. Информационная безопасность России в контексте Госпрограммы «Информационное общество 2011-2020»
24. Приоритеты и цели государственной политики в сфере развития информационного общества в Российской Федерации
25. Основные мероприятия госпрограммы «Информационное общество 2011-2020»
26. Прогноз конечных результатов реализации госпрограммы «Информационное общество 2011-2020»
27. Основы информационного противоборства – базовые понятия и термины.
28. Типизация активных действий в информационном пространстве
29. Новые объекты безопасности в информационной сфере (открытые информационные сети, бизнес, общественное сознание, интересы личности).
30. Кибертерроризм – определение, сущность
31. Кибертерроризм и трансформация международного терроризма, информационная преступность

32. Информационное оружие – новый вид оружия массового поражения
33. Укрепление международной информационной безопасности (МИБ) как мегатренд современной мировой политики
34. Российские инициативы в области МИБ, история их выдвижения и продвижения.
35. Расстановка сил на мировой арене в связи с российскими инициативами по МИБ
36. Переговорный процесс и международное сотрудничество в области ограничения информационных видов оружия
37. Формирование подходов к проблеме международной информационной безопасности в ООН и других международных организациях.
38. Дискурс МИБ в ООН.
39. Нормативно-правовое обеспечение МИБ в России
40. Базовые положения «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года».
41. Новая редакция Концепции внешней политики России о МИБ.
42. Основные угрозы в области МИБ
43. ИКТ и суверенитет России
44. Киберпреступность – базовые понятия.
45. Подходы НАТО к ведению кибервойн.
46. «Таллинское руководство» по ведению кибервойн НАТО
47. Социальные сети – базовые понятия и определения.
48. Социальные сети – инструмент информационно-психологического воздействия на человека.
49. Глобальные социальные сети – инструмент «цветных революций».
50. Социальная сеть микроблоггинга Twitter – главный инструмент «цветных революций».

Шкала оценивания.

Выполнение всех заданий текущего контроля является обязательным для всех обучающихся.

Критерии оценки:

Оценка	**Критерий оценки**
«зачтено»	Обучающийся показывает высокий уровень компетентности, знания программного материала, учебной, периодической и монографической литературы, законодательства и практики его применения, раскрывает не только основные понятия, но и анализирует их с точки зрения различных авторов. Обучающийся показывает не только высокий уровень теоретических знаний по дисциплинам, включенным в государственный экзамен, но и видит междисциплинарные связи. Профессионально, грамотно, последовательно, хорошим языком четко излагает материал, аргументированно формулирует выводы. Знает в рамках требований к направлению и профилю подготовки законодательно-нормативную и практическую базу. На вопросы отвечает кратко, аргументировано, уверенно, по существу.
«не зачтено»	Обучающийся показывает слабые знания лекционного материала, учебной литературы, законодательства и практики его применения, низкий уровень компетентности, неуверенное изложение вопроса. Обучающийся показывает слабый уровень профессиональных знаний, затрудняется при анализе практических ситуаций. Не может привести примеры из реальной практики. Неуверенно и логически непоследовательно излагает материал. Неправильно отвечает на вопросы или затрудняется с ответом.

4.4. Методические материалы

Устный опрос является одним из основных способов проверки усвоения знаний обучающимися. Развернутый ответ студента должен представлять собой связное, логически последовательное сообщение на определенную тему, показывать его умение применять определения, правила в конкретных случаях. Основные критерии оценки устного ответа: правильность ответа по содержанию; полнота и глубина ответа; логика изложения материала (учитывается умение строить целостный, последовательный рассказ, грамотно пользоваться специальной терминологией); использование дополнительного материала.

5. Методические указания для обучающихся по освоению дисциплины

Методические указания по самостоятельной подготовке к занятиям лекционного, практического (семинарского) типа:

Подготовка к занятиям должна носить систематический характер. Это позволит обучающемуся в полном объеме выполнить все требования преподавателя. Обучающимся рекомендуется изучать как основную, так и дополнительную литературу, а также знакомиться с Интернет-источниками (список приведен в рабочей программе по дисциплине).

Вопросы для самостоятельной подготовки (самопроверки):

1 Понятие информационного общества. Теоретические подходы.
2 Международный опыт создания информационного общества.
3 Роль «цифровых аборигенов» в развитии информационного общества.
4 Измерение информационного общества Международным союзом электросвязи.
5 Роль ООН в построении глобального информационного общества.
6 Изменение понятия «безопасности» в информационном обществе.
7 Изменение угроз и вызовов при переходе к информационному обществу.
8 Изменение парадигм терроризма в информационном обществе.
9 Стратегия национальной безопасности России до 2020 года об обеспечении информационной безопасности.
10 Основные факторы, определяющие новые параметры проблемы обеспечения информационной безопасности.
11 Изменение характера и приоритетности угроз безопасности в информационном обществе.
12 «Мягкая сила» - базовые понятия.
13 «Мягкая сила» по Дж.Наю.
14 Критерии составляющих «мягкой силы».
15 Базовые понятия и классификация социальных сетей.
16 Социальные сети как инструмент «мягкой силы 2.0.».

Методические указания по подготовке докладов:

Подготовка обучающихся к опросу предполагает изучение в соответствии тематикой дисциплины основной/ дополнительной литературы, нормативных документов, интернет-ресурсов.

Обучающийся готовит доклад в форме устного сообщения по теме дисциплины.

Предлагается следующая структура доклада:

1. Введение:

– указывается тема и цель доклада;

– обозначается проблемное поле, тематические разделы доклада.

2. Основное содержание доклада:

– последовательно раскрываются тематические разделы доклада.

3. Заключение:

– приводятся основные результаты и суждения автора по поводу путей возможного решения рассмотренной проблемы, которые могут быть оформлены в виде рекомендаций.

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

6.1. Основная литература

1 Аверченков В.И. Аудит информационной безопасности - М.: ФЛИНТА, 2011. (ЭБС «Лань» http://e.lanbook.com/view/book/20195)

2 Бурда А.Г. Современные информационные технологии в управлении - Краснодар: Южный институт менеджмента, 2013 - http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/25983 — ЭБС «IPRbooks»

3 Макарова, Н. В. Информатика : учебник - СПб. : Питер, 2012. – 576 с.

4 Рассолов И.М. ИНФОРМАЦИОННОЕ ПРАВО 4-е изд., пер. и доп. Учебник и практикум для академического бакалавриата. - М.: Издательство Юрайт, 2015. (ЭБС "Юрайт" http://www.biblio-online.ru/thematic/?id=urait.content.82422031-14DE-4333-8292-677C5CD29748&type=c_pub)

6.2. Дополнительная литература

1 Гаврилов, М. В. Информатика и информационные технологии : учебное пособие : рекомендовано УМО вузов России - М.: Эксмо, 2011. – 540 с.

2 Зиновьева Е.С. Международное управление Интернетом: конфликт и сотрудничество - М.: МГИМО-Университет, 2011. (ЭБС «Лань» http://e.lanbook.com/view/book/46354)

3 Петросян С.И. Политическое управление и информационные технологии в сфере предоставления государственных и муниципальных услуг // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2015. № 3-2 (53). С. 140-144. - ЭБС elibrary http://elibrary.ru/item.asp?id=22966743

4 Соколова М.Ю., Мухина Ю.В. Практика применения информационных технологий в государственном и региональном управлении // Системное управление. 2014. № 4 (25). С. 89-95. - ЭБС elibrary http://elibrary.ru/item.asp?id=22988955

5 Grudin, J. Human-computer interaction Ann. Rev. Info. Sci. Tech., 2011, 45: 367–430. - ЭБС Wiley Online Library http://onlinelibrary.wiley.com.ezproxy.ranepa.ru:3561/doi/10.1002/aris.2011.1440450115/abstract

6.3. Учебно-методическое обеспечение самостоятельной работы

1. Агапов, В. С. Социально-психологические детерминанты креативной компетентности студентов : монография / Агапов, Валерий Сергеевич, Давлетова, Рада Уеловна. - М. : Макеев Игорь Вячеславович, 2016. - 163 с.
2. Модель позиционного обучения студентов [Электронный ресурс]: теоретические основы и методические рекомендации/ И.Б. Шиян [и др.].— Электрон. текстовые данные.— М.: Московский городской педагогический университет, 2012.— 152 с.— Режим доступа: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/27375.html.— ЭБС «IPRbooks»
3. Образовательные инновации и практики карьеры : сборник методических материалов и статей / РАНХиГС при Президенте РФ. - М. : Дело, 2015. - 192 с.
4. Психология адаптации и социальная среда. Современные подходы, проблемы,

перспективы [Электронный ресурс]/ Л.Г. Дикая [и др.].— Электрон. текстовые данные. — М.: Пер Сэ, 2007.— 624 с.— Режим доступа: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/7431.html.— ЭБС «IPRbooks»
5. Социально-психологические аспекты формирования культуры самообучающейся организации / А. Я. Николаев [и др.] // Вопросы психологии. - 2014. - № 6. - С. 44-52.

6.4. Нормативные правовые документы

1. Концепция долгосрочного социально-экономического развития Российской Федерации до 2020 года.(Утв. распоряжением Правительства РФ от 8 декабря 2011 г. N 2227-р).

6.5. Интернет-ресурсы

1. Центральная библиотека образовательных ресурсов. Режим доступа: http://www.edulib.ru/
2. Сводный каталог электронных библиотек. Режим доступа: http://www.lib.msu.ru/journal/Unilib/main.htm
3. Базы данных ИНИОН. Режим доступа: http://www.inion.ru/product/db.htm
4. Библиотека образовательного портала «Экономика, социология, менеджмент». Режим доступа: http://ecsocman.edu.ru/
5. Библиотека федерального портала «Российское образование». Режим доступа: http://www.edu.ru/
6. Библиотека учебной и научной литературы русского гуманитарного интернет университета. Режим доступа: http://www.i-u.ru/biblio/default.aspx

6.6. Иные источники

1 Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт [Электронный ресурс]: монография/ Ефимова Л.Л., Кочерга С.А.— Электрон. текстовые данные.— М.: ЮНИТИ-ДАНА, 2015.— 239 с.— Режим доступа: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/52672.html.— ЭБС «IPRbooks»
2 Зыкова И.В. Культура как информационная система. Духовное, ментальное, материально-знаковое - М. : URSS : ЛИБРОКОМ, 2011. – 368 с.
3 Информационная политика: в контексте социальной информациологии : хрестоматия / РАГС при Президенте РФ ; сост. Н.П. Арапова ; отв. ред.: В.Д. Попов, А.В. Шевченко. - М. : Изд-во РАГС, 2007. - 248 с.
4 Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны [Электронный ресурс]: монография/ Манойло А.В., Петренко А.И., Фролов Д.Б.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2012.— 542 с.— Режим доступа: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/11982.html.— ЭБС «IPRbooks»
5 Новиков В.К. Информационное оружие – оружие современных и будущих войн [Электронный ресурс]/ Новиков В.К.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 262 с.— Режим доступа: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/37186.html.— ЭБС «IPRbooks»
6 Цыганов В.В. Информационные войны в бизнесе и политике. Теория и методология [Электронный ресурс]/ Цыганов В.В., Бухарин С.Н.— Электрон. текстовые данные.— М.: Академический Проект, 2009.— 336 с.— Режим доступа: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/36332.html.— ЭБС «IPRbooks»

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

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Программное обеспечение: Microsoft Windows 10 LTSB 1607, Microsoft Office Professional 2016.

Информационные справочные системы: Научная библиотека РАНХиГС. URL: http://lib.ranepa.ru/; Научная электронная библиотека eLibrary.ru. URL: http://elibrary.ru/defaultx.asp; Национальная электронная библиотека. URL: www.nns.ru; Российская государственная библиотека. URL: www.rsl.ru; Российская национальная библиотека. URL: www.nnir.ru; Электронная библиотека Grebennikon. URL: http://grebennikon.ru/; Электронно-библиотечная система Издательства «Лань». URL: http://e.lanbook.com; Электронно-библиотечная система ЮРАЙТ. URL: http://www.biblio-online.ru/.