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

Институт права и национальной безопасности
Кафедра государственного управления и национальной безопасности

УТВЕРЖДЕНА
решением кафедры
государственного управления
и национальной безопасности
Протокол от «07» сентября 2017 г.
№ 1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.12 Информационная безопасность России
(индекс, наименование дисциплины (модуля), в соответствии с учебным планом)

38.04.04 Государственное и муниципальное управление
(код, наименование направления подготовки (специальности)

Государственное управление и национальная безопасность
(направленность (профиль))

Магистр
(квалификация)

Очно-заочная, заочная
(форма(ы) обучения)

Москва, 2018 г.

Автор(ы)-составитель(и):
доктор полит. наук,
профессор, зав. кафедрой государственного управления и национальной безопасности
Шевченко А.В.
(ученая степень и(или) ученое звание, должность) (наименование кафедры) (Ф.И.О.)

Заведующий кафедрой
государственного управления
и национальной безопасности доктор полит. наук, профессор Шевченко А.В
(наименование кафедры) (ученая степень и(или) ученое звание, должность) (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 «Информационная безопасность России» обеспечивает овладение следующими компетенциями с учетом этапов:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-11	способность осуществлять верификацию и структуризацию информации, получаемой из разных источников	ПК-11.3.	Способность осуществлять синтез и обобщение полученной информации.
ПК-12	способность использовать информационные технологии для решения различных исследовательских и административных задач	ПК-12.2.	Способность использовать информационные технологии для решения различных исследовательских и административных задач, в том числе при подготовке выпускной квалификационной работы.

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

Профессиональные действия	**Код этапа освоения компетенции**	**Результаты обучения**
консультирование государственных, некоммерческих и хозяйственных организаций	ПК-11.3.	**на уровне умений:** - анализировать и синтезировать данные из нескольких источников; - обеспечивать информационную базу научного исследования; **на уровне навыков:** - оценка и верификация получаемой информации; - определения роли информации в социально-экономических и политических процессах.

организация проведения работ по выполнению научно-исследовательских и опытно-конструкторских работ	ПК-12.2.	**на уровне умений:** - применять методы анализа и управления состояниями и процессами информационной безопасности; - осуществлять аудит угроз информационного характера; **на уровне навыков:** - использования информационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач; - оценки информационных угроз;

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

Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е. (108 а.ч.).

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

- очно-заочная форма обучения: лекции – 8 а.ч., практические занятия – 16 а.ч., самостоятельная работа – 57 ч;
- заочная форма обучения: лекции – 4 а.ч., практические занятия – 8 а.ч., самостоятельная работа – 87 ч.

Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность России» (Б1.В.12) относится к вариативной части и в соответствии с учебным планом осваивается в 4-м семестре очно-заочной и заочной форм обучения.

Освоение дисциплины опирается на минимально необходимый объем теоретических знаний в области информационной безопасности, а также на приобретенные ранее умения и навыки в сфере обеспечения национальной безопасности России. Дисциплина «Информационная безопасность России» реализуется после изучения следующих дисциплин: «Исследование социально-экономических и политических процессов», «Информационно-аналитические технологии государственного и муниципального управления», «Конкурентная разведка».

Форма промежуточной аттестации в соответствии с учебным планом – экзамен.

3. Содержание и структура дисциплины (модуля)

Таблица 1.

№ п/п	Наименование тем	Объем дисциплины, час.						Форма текущего контроля успеваемости[1], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очно-заочная форма обучения								
Тема 1	Основы политики информационной безопасности. Теория и практика управления безопасностью информационных процессов	27	2		4		14	Т
Тема 2	Безопасность системы массовой информации и коммуникации	27	2		4		16	КР
Тема 3	Информационное обеспечение стратегических направлений национальной безопасности.	27	2		4		12	П
Тема 4	Информационная безопасность как условие предотвращения информационно-психологической войны	27	2		4		15	П, КР
Промежуточная аттестация								Экзамен
Всего:		**108**	**8**		**16**		**57**	
Заочная форма обучения								
Тема 1	Основы политики информационной безопасности. Теория и практика управления безопасностью информационных процессов	27	1		2	4	15	Т
Тема 2	Безопасность системы массовой информации и коммуникации	27	1		2	4	16	КР
Тема 3	Информационное обеспечение стратегических направлений национальной безопасности.	27	1		2	6	18	П
Тема 4	Информационная безопасность как условие предотвращения	27	1		2	4	20	П, КР

№ п/п	Наименование тем	Объем дисциплины, час.						Форма текущего контроля успеваемости[1], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
	информационно-психологической войны							
Промежуточная аттестация								Экзамен
Всего:		**108**	**4**		**8**	**18**	**69**	

Примечание: 1 – формы текущего контроля успеваемости: тест (Т), презентация (П), контрольная работа (КР).

Содержание дисциплины (модуля)

Тема 1. Основы политики информационной безопасности. Теория и практика управления безопасностью информационных процессов

Понятие, принципы и содержание информационно-аналитической деятельности. Общие вопросы организации информационно-аналитической деятельности в органах государственного и муниципального управления; общие понятия о работе информационно-аналитических и ситуационных центров. Принципы и способы отнесения аналитических видов деятельности к различным уровням интеллектуального труда. Интеллектуальные системы в международной политике: определение, классификация, специфика функционирования.

Тема 2. Безопасность системы массовой информации и коммуникации

Принципы создания когнитивных карт (степень общности, «масштаба» и организации) Карта-обозрение, карта-путь (дорожная карта). Методология когнитивного моделирования; анализ и принятие решений в плохо определенных ситуациях. Метод когнитивного картирования: выявление особенностей каузальных связей объекта, составление ориентированных графов - индивидуальных и коллективных схем (карт), мягкое и жесткое когнитивное картирование. Базовые процедуры КК, интерпретация результатов, сфера реализации. Метод сети связей.

Тема 3. Информационное обеспечение стратегических направлений национальной безопасности

Виды, типы, структура информации. Характеристики, разнообразие, особенности информационных технологий. Определение и классификация источников информации и их надежности. Информационная среда, ресурсы, информационная инфраструктура органа государственного управления. Способы получения, обработки, представления информации. Распознавание дезинформирующих, манипулятивных информационных технологий. Работа информационно-аналитических структур по формированию «повестки дня» деятельности российских представительств, составлению долгосрочных планов. Алгоритм работы с аналитической информацией в международных отношениях.

Тема 4. Информационная безопасность как условие предотвращения информационно-психологической войны

Реферативные, справочные и аналитические материалы. Информационная сводка, реферативный обзор, записка, доклад. Содержание основных этапов работы над справкой-политико-экономической, социально-политической и т.п. характеристикой. Методика подготовки информационной сводки и реферативного обзора.

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

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

4.1.1. В ходе реализации дисциплины «Информационная безопасность России» (Б1.В.12) используются следующие методы текущего контроля успеваемости обучающихся:

4.1.1. В ходе реализации дисциплины «Информационная безопасность России» используются следующие методы текущего контроля успеваемости обучающихся:
- при проведении занятий лекционного типа: опрос
- при проведении практических занятий: тестирование, контрольная работа, защита презентаций.

4.1.2. Экзамен проводится с применением следующих методов (средств):
решений ситуационных задач в области информационной безопасности.

4.2. Материалы текущего контроля успеваемости.

Типовые оценочные материалы по Теме 1. Основы политики информационной безопасности. Теория и практика управления безопасностью информационных процессов

Тестирование:

1. Информация, которая составляется на базе прямого наблюдения или опроса, на основе непосредственной регистрации совершающихся событий, называется:

A. **Первичной**
B. Непосредственной
C. Вторичной
D. Второстепенной

2. Результат выполнения неких операций над данными, приводящих к получению нового массива данных, доступных для дальнейшей обработки и интерпретации:

A. **Информационный продукт**
B. Информационная технология
C. Информационная инфраструктура
D. Информационная система

3. Информацию, генерируемую целенаправленно в интересах управления системой, называют:

A. Сгенерированной информацией
B. **Управляющей информацией**
C. Внутренней информацией
D. Знаковой информацией

4. Совокупность определяемых функциональным назначением и топологией системы каналов информационного взаимодействия, информационных ресурсов и технологического инструментария информационной работы, обеспечивающую процесс управления системой, принято называть:

A. Информационно-аналитическое обеспечение
B. **Информационную инфраструктуру**
C. Процесс информационно-аналитического обеспечения
D. Систему информационно-аналитического обеспечения

5. Термин, обозначающий то, что было извлечено из данных в результате их интерпретации с применением некоторой другой модели (не той, которой располагал некто или нечто, запечатлевшее информацию):

A. Дезинформация
B. **Эксформация**
C. Первичная информация
D. Вторичная информация

6. Техника сбора информации, производимого на основе систематического выявления соответствующих целям и задачам исследования характеристик текстов (понятий, словосочетаний, фреймов текста и пр.) –

A. Ивент-анализ
B. Интент-анализ
C. **Контент-анализ**
D. Корреляционный анализ

7. Этот вид анализа позволяет определить степень зависимости, сопряженности между двумя и более признаками –

A. Факторный
B. Интент-анализ
C. Контент-анализ
D. **Корреляционный**

8. Прикладная аналитическая методика изучения особенностей индивидуального (реже группового) мышления, показывающая взаимосвязь лингвистических структур текста и представлений его автора –

A. **Когнитивное картрование**
B. Интент-анализ
C. Контент-анализ
D. Корреляционный анализ

9. Вид когнитивного картирования, подразумевающий не только анализ текста, но и знание ситуации аналитиком –

A. **Мягкое**
B. Жесткое
C. Направленное

D. Ненаправленное

10. Свойство концепции (концептуального продукта) в информационно-аналитической работе, выражающееся в том, что все функциональные блоки концепции должны быть тесно увязаны, и она не должна распадаться на не объединенные единым замыслом блоки:

A. Оптимальность
B. **Целостность**
C. Адаптивность
D. Однородность

Типовые оценочные материалы по Теме 2. Безопасность системы массовой информации и коммуникации

Контрольная работа:

1. Каковы закономерности формирования и развития информационных процессов в больших открытых социальных системах?
2. Как социальная память влияет на процессы самоорганизации в больших социальных системах?
3. Проведите политико-правовой анализ проблемной ситуации в сфере защиты информационных ресурсов, средств массовых коммуникаций, блогосферы на основе знания основных положений Конституции РФ, Доктрины информационной безопасности Российской Федерации (2016 г.), законодательства о средствах массовой информации и правового регулирования Интернета.
4. Дайте оценку состояния государственной информационной политики России.
5. Каковы формы и методы защиты общественного сознания от деструктивных информационных воздействий?
6. Перечислите методы и технологии выявление основных угроз информационно-технической безопасности в системах государственного (муниципального) управления и социальных сетях.

Типовые оценочные материалы по Теме 3. Информационное обеспечение стратегических направлений национальной безопасности

Примерные темы для презентаций:

1. Международное законодательство и практика законоприменения в сфере реализации свободы слова.
2. Проблемы законотворчества в области охраны прав граждан на свободу слова.
3. Взаимосвязь свободы слова и права на свободный доступ к информации.
4. Доктрина информационной безопасности РФ и Окинавская хартия о соблюдении баланса интересов граждан, общества и государства.
5. Доктрина информационной безопасности РФ и проблемы совершенствования информационного законодательства Российской Федерации.
6. Принципы формирования информационных ресурсов органов государственной власти и управления.
7. Механизмы влияния (воздействия) информационной сферы на общественное сознание и массовую психику.
8. Государственная информационная политика в области информационной безопасности: принципы и методы формирования.

Типовые оценочные материалы по Теме 4. Информационная безопасность как условие предотвращения информационно-психологической войны

Примерные темы для презентаций:

1. Социально-психологическое воздействие средств массовой информации на общественное сознание и общественное мнение.
2. Формы и методы обеспечения информационно-психологической безопасности личности.
3. Информационные технологии упреждения и разрешения конфликтов. Проблемы правового разрешения информационных споров.
4. Международное право о свободе слова и свободе обмена информацией.
5. Модели безопасного типа информационного взаимодействия прессы и институтов государственной власти.
6. Формы и методы организационного, правового, социокультурного регулирования информационных процессов.

Контрольная работа:

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.
5. Информационно-аналитические и психолингвистические системы анализа текстов (WAAL-2000, ВИКА-БОС и др.).

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-11	способность осуществлять верификацию и структуризацию информации, получаемой из разных источников	ПК-11.3.	Способность осуществлять синтез и обобщение полученной информации.
ПК-12	способность использовать информационные технологии для решения различных исследовательских и административных задач	ПК-12.2.	Способность использовать информационные технологии для решения различных исследовательских и административных задач, в том числе при подготовке выпускной квалификационной работы.

4.3.2 Типовые оценочные средства

Вопросы для экзамена по дисциплине «Информационная безопасность России»

1. Развитие информационной теории в трудах российских и зарубежных ученых (В. Вернадский, Н. Моисеев, А. Урсул, Н. Винер, К. Шеннон, М. Кастельс, Д. Белл)
2. Философия информационной безопасности (Р. Абдеев, С.П. Расторгуев, Н.Н. Рыбкин)
3. Развитие информационной теории в трудах российских и зарубежных ученых (В. Вернадский, Н. Моисеев, А. Урсул, Н. Винер, К. Шеннон, М. Кастельс, Д. Белл)
4. Сущность и содержание понятия «информационная безопасность».
5. Место и роль информационной безопасности в общей системе национальной безопасности России.
6. Общая характеристика угроз информационной безопасности.
7. Цель и задачи обеспечения информационной безопасности.
8. Общая характеристика Доктрины информационной безопасности Российской Федерации (2000 г.)
9. Национальные интересы России в информационной сфере (по Доктрине информационной безопасности 2000 г.)
10. Конституция России как основной источник правовых норм в области обеспечения информационной безопасности.
11. Международное право и информационное законодательство Российской Федерации.
12. Базовые законодательные акты Российской Федерации в области информационной безопасности.
13. Основные направления построения информационного общества в Российской Федерации.
14. Управление безопасностью информационных процессов (теоретический аспект).
15. Методологические основы информационной безопасности.
16. Формирование, использование и защита информационных ресурсов государства.
17. Сущность и содержание информационно-психологической безопасности.
18. Характеристика основных угроз информационно-психологической безопасности в современных условиях.
19. Роль и место СМИ в обеспечении информационно-психологической безопасности.
20. Сущность и содержание информационно-технической безопасности.
21. Актуальные проблемы обеспечения безопасности в автоматизированных системах государственного и муниципального управления.
22. Организация обеспечения информационной безопасности – планирование, текущее руководство, координация и взаимодействие.
23. Развитие институтов (субъектов, сил и средств) системы обеспечения информационной безопасности.
24. Высшие органы стратегического руководства системой обеспечения информационной безопасности.
25. Роль министерств и ведомств в системе обеспечения информационной безопасности.
26. Роль негосударственных организаций в формируемой системе обеспечения информационной безопасности.
27. Развитие правовых основ обеспечения информационной безопасности.
28. Информационная глобализация и информационное общество: каузальные связи и противоречия.
29. Формы и методы защиты информационных ресурсов от несанкционированного использования.
30. Права и обязанности государственных служащих в области информационной безопасности.

31. Манипулирование общественным сознанием – проблема информационной безопасности.
32. Сущность и содержание понятия «информационная безопасность».
33. Место и роль информационной безопасности в общей системе национальной безопасности России.
34. Общая характеристика угроз информационной безопасности.
35. Цель и задачи обеспечения информационной безопасности.
36. Общая характеристика Доктрины информационной безопасности Российской Федерации (2000 г.) и новой редакции (2016 г.)
37. Национальные интересы России в информационной сфере (по Доктрине информационной безопасности 2016 г.)
38. Конституция России как основной источник правовых норм в области обеспечения информационной безопасности.
39. Международное право и информационное законодательство Российской Федерации.
40. Базовые законодательные акты Российской Федерации в области информационной безопасности.
41. Основные направления построения информационного общества в Российской Федерации.
42. Управление безопасностью информационных процессов (теоретический аспект).
43. Методологические основы информационной безопасности.
44. Формирование, использование и защита информационных ресурсов государства.
45. Сущность и содержание информационно-психологической безопасности.
46. Характеристика основных угроз информационно-психологической безопасности в современных условиях.
47. Роль и место СМИ в обеспечении информационно-психологической безопасности.
48. Сущность и содержание информационно-технической безопасности.
49. Актуальные проблемы обеспечения безопасности в автоматизированных системах государственного и муниципального управления.
50. Организация обеспечения информационной безопасности – планирование, текущее руководство, координация и взаимодействие.
51. Развитие институтов (субъектов, сил и средств) системы обеспечения информационной безопасности.
52. Высшие органы стратегического руководства системой обеспечения информационной безопасности.
53. Роль министерств и ведомств в системе обеспечения информационной безопасности.
54. Роль негосударственных организаций в формируемой системе обеспечения информационной безопасности.
55. Развитие правовых основ обеспечения информационной безопасности.
56. Информационная глобализация и информационное общество: каузальные связи и противоречия.
57. Формы и методы защиты информационных ресурсов от несанкционированного использования.
58. Права и обязанности государственных служащих в области информационной безопасности.
59. Манипулирование общественным сознанием – проблема информационной безопасности.

Примеры ситуационных задач

1. Спроектируйте систему информационной безопасности воображаемой организации экономического (финансового, кредитного и др.) профиля. Определите модель зрелости разрабатываемой организации.
2. Изучите основные положения Доктрину информационной безопасности и оцените ее соответствие актуальным направлениям обеспечения информационной безопасности экономической деятельности. Какие меры предусматривает Доктрина для обеспечения информационной безопасности экономической сферы? Оцените их своевременность, полноту, результативность. Что нужно сделать для повышения эффективности реализации Доктрины в сфере обеспечения экономической безопасности России?
3. Ознакомьтесь с документами Саммита НАТО в Варшаве в 2016. Выявите в их содержании положения, касающиеся политики организации в области информационной безопасности и кибербезопасности, и определите характер угроз для информационной безопасности России, связанных с намерением стран-участниц НАТО развивать средства информационного противоборства.

Шкала оценивания

Этап освоения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания
ПК-11.3. Способность осуществлять синтез и обобщение полученной информации.	Быстро усваивает новую информацию, синтезирует информацию из нескольких источников. Умеет самостоятельно находить ключевые особенности, сходства и различия, обобщать информацию.	Успешно осуществляет анализ и синтез полученной информации. Корректно обобщает полученную информацию из разных источников.	Защита презентаций
ПК-12.2. Способность использовать информационные технологии для решения различных исследовательских и административных задач, в том числе при подготовке выпускной квалификационной работы.	Самостоятельно использует информационные технологии для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач. Обладает навыками пользования информационными базами данных, электронными библиотеками и т.д.	Корректно использует информационные технологии для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач. Демонстрирует навыками пользования информационными базами данных, электронными библиотеками и т.д.	Ситуационные задачи Защита презентаций

4.4. Методические материалы

Оценивание обучающихся в процессе поэтапного освоения ими компетенций, формируемых данной дисциплиной осуществляется в форме экзамена, который предполагает оценивание умений и навыков с помощью решения ситуационных задач и/или кейс-задания.

К экзамену 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 экзамену 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 экзамен.

Экзамен принимает лектор. Умения и навыки обучающегося на экзамене оцениваются как «неудовлетворительно», «удовлетворительно», «хорошо» или «отлично».

Оценивание обучающегося на зачете по дисциплине

Оценка	**Критерии оценки**	**Результаты обучения**
«отлично»	- качественно анализирует и синтезирует данные из нескольких источников; - эффективно обеспечивает информационную базу научного исследования; - на высоком уровне владеет навыком оценки и верификации получаемой информации; - корректно определяет роль информации в социально-экономических и политических процессах; - применяет методы анализа и управления состояниями и процессами информационной безопасности; - эффективно осуществляет аудит угроз информационного характера; - владеет навыком применения информационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач; - эффективно оценивает	ПК-11.3. **на уровне умений:** - анализировать и синтезировать данные из нескольких источников; - обеспечивать информационную базу научного исследования; **на уровне навыков:** - оценка и верификация получаемой информации; - определения роли информации в социально-экономических и политических процессах. ПК-12.2. **на уровне умений:** - применять методы анализа и управления состояниями и процессами информационной безопасности; - осуществлять аудит угроз информационного характера; **на уровне навыков:** - использования информационных технологий для интенсификации процесса

	информационные угрозы.	получения, обработки и оценки информации в рамках решения административных, исследовательских задач; - оценки информационных угроз.
«хорошо»	- анализирует и синтезирует данные из нескольких источников; - обеспечивает информационную базу научного исследования; - владеет навыком оценки и верификации получаемой информации; - определяет роль информации в социально-экономических и политических процессах; - испытывает сложности при применении методов анализа и управления состояниями и процессами информационной безопасности; - осуществляет аудит угроз информационного характера; - владеет навыком применения информационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач; - оценивает информационные угрозы.	
«удовлетворительно»	- с затруднениями анализирует и синтезирует данные из нескольких источников; - испытывает сложности при обеспечении информационной базой научное исследование; - владеет навыком оценки и верификации получаемой информации на низком уровне; - некорректно определяет роль информации в социально-экономических и политических процессах; - не умеет применять методы анализа и управления	

	состояниями и процессами информационной безопасности; - не умеет осуществлять аудит угроз информационного характера; - не владеет навыком применения информационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач; - с трудом оценивает информационные угрозы.	
«неудовлетворительно»	- с большими затруднениями анализирует и синтезирует данные из нескольких источников; - испытывает сложности при обеспечении информационной базой научное исследование; - не владеет навыком оценки и верификации получаемой информации; - некорректно определяет роль информации в социально-экономических и политических процессах; - не владеет методами анализа и управления состояниями и процессами информационной безопасности; - не владеет навыком применения информационных технологий для интенсификации процесса получения, обработки и оценки информации в рамках решения административных, исследовательских задач; - с большим трудом оценивает информационные угрозы.	

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.

5.1. Рекомендации по подготовке к лекционным занятиям (теоретический курс)

Дисциплина «Информационная безопасность России» ориентирована на формирование у обучающихся умений и навыков верификации и структуризации информации, получаемой из разных источников, в целях обеспечения информационной безопасности, применения информационных технологий для решения различных исследовательских и административных задач.

Изучение дисциплины «Информационная безопасность России» 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.

5.2. Рекомендации по подготовке к практическим (семинарским) занятиям

Цель семинарских занятий заключается в ознакомлении обучающихся с новыми подходами в сфере аналитического обеспечения системы информационной безопасности, изучением зарубежного опыта в данной сфере, формировании навыков оценки информационного характера.

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 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 лекционным и семинарским занятиям

Тема 1. Лекция: Развитие информационного общества и информационная безопасность: теоретико-методологические аспекты исследования.

1. Сущность и содержание понятия «информационная безопасность» Ее место и роль в системе обеспечения национальной безопасности.
2. Цели и задачи обеспечения информационной безопасности.
3. Переход к информационному обществу и возрастание отрицательного воздействия угроз социально-экономического, медицинского, воспитательного и образовательного характера.
4.Информационные вызовы и угрозы устойчивости политической системе государства.

Практическое занятие: Государственная политика России в сфере информационной безопасности.

1. Информационная политика как форма социально-политического управления. Информационная политика и безопасность гуманитарной сферы.
2. Национальные интересы России в обеспечении информационной безопасности. Проблемы формирования и реализации государственной информационной политики: федеральный и региональный уровни.
3. Развитие доктринальных положений информационной политики в области права, экономики и культуры. Потенциальные и реальные формы и методы обеспечения национальных интересов и предотвращения угроз информационной безопасности Российской Федерации в информационной сфере посредством государственной информационной политики.

4. Возможности органов власти и управления, общественных институтов по предотвращению, локализации и нейтрализации угроз информационной безопасности.

Тема 2. Лекция: Управление безопасностью информационных и коммуникационных процессов

1. Управление информационными процессами как элемент государственной информационной политики.
2. Массовая информационная сфера как объект управления.
3. Идеология как теоретическая основа управления информационными процессами.
4. Цели, стратегия, проект, план, программа, технологии управления информационными процессами.
5. Место и роль социологических, политических, психологических исследований в системе обеспечения информационной безопасности.
6. Проблемы формализации коммуникационных процессов.

Практическое занятие: Информационные процессы: этапы и закономерности формирования и развития.
1. Нелинейность информационных процессов в больших открытых самоорганизующихся социальных системах.
2. Неравновесность, сетевой принцип построения информационного пространства больших социальных систем.
3. Интенсивность и цикличность информационных процессов в больших открытых социальных системах.
4. Влияние социальной памяти на процессы самоорганизации в больших социальных системах. Системы со смешанной информационно-материальной структурой.
5. Политико-правовой анализ проблемных ситуаций в сфере защиты информационных ресурсов, средств массовых коммуникаций, блогосферы на основе знания основных положений Конституции РФ, Доктрины информационной безопасности Российской Федерации (2016 г.), законодательства о средствах массовой информации и правового регулирования Интернета.

Тема 3. Лекция: «Роль и место национальной информационной политики в обеспечении информационного порядка»
1. Оценка состояния и задачи совершенствования государственной информационной политики России
2. Использование информационно-коммуникативных средств во внутренней политике государства.
2. Формы и методы защиты общественного сознания от деструктивных информационных воздействий.
3. Средства массовой информации как критически важные структуры системы информационных отношений.

Практическое занятие: Особенности обеспечения технико-технологической безопасности информационных систем органов власти *(демонстрационно-ознакомительное) занятие в компьютерном классе.*
1. Методы и технологии выявление основных угроз информационно-технической безопасности в системах государственного (муниципального) управления и социальных сетях.
2. Демонстрация возможностей защиты автоматизированных информационных систем с помощью новых информационных технологий.

3. Правовые, общественно-политические, административно-организационные меры обеспечения информационной безопасности органами государственного и муниципального управления.

Тема 4. Лекция: Обеспечение информационно-психологической безопасности

1. Основные концепции информационно-психологического противоборства и войн в документах Российской Федерации и зарубежных стран.
2. Особенности подготовки и ведения информационно-психологических войн в исторической ретроспективе.
3. Характер, сущность и содержание информационно-психологических войн современности.
4. Социальные и политические сети как современный театр военных действий.

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.
5.Информационно-аналитические и психолингвистические системы анализа текстов (WAAL-2000, ВИКА-БОС и др.).

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.

1. Крылов Г.О. Понятийный аппарат информационной безопасности [Электронный ресурс]: словарь/ Крылов Г.О., Ларионова С.Л., Никитина В.Л.— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 343 c.— Режим доступа: http://www.iprbookshop.ru/64306.html.— ЭБС «IPRbooks»
2. 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 c.— Режим доступа: http://www.iprbookshop.ru/47262.html.— ЭБС «IPRbooks»
3. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 c.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks»

6.2 Дополнительная литература:

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.:

Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с. — Режим доступа: http://www.iprbookshop.ru/52182.html.— ЭБС «IPRbooks»
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.html.— ЭБС «IPRbooks»

3. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-методический комплекс/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 342 с.— Режим доступа: http://www.iprbookshop.ru/14642.html.— ЭБС «IPRbooks»

6.3. Учебно-методическое обеспечение самостоятельной работы

Тема 1. Основы политики информационной безопасности. Теория и практика управления безопасностью информационных процессов

1. 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.html.— ЭБС «IPRbooks»
2. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с. — Режим доступа: http://www.iprbookshop.ru/52182.html.— ЭБС «IPRbooks»

Тема 2. Безопасность системы массовой информации и коммуникации

1. 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.html.— ЭБС «IPRbooks»
2. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks»

Тема 3. Информационное обеспечение стратегических направлений национальной безопасности.

1. Петров С.В. Информационная безопасность [Электронный ресурс]: учебное пособие/ Петров С.В., Кисляков П.А.— Электрон. текстовые данные.— Саратов: Ай Пи Ар Букс, 2015.— 326 с.— Режим доступа: http://www.iprbookshop.ru/33857.html.— ЭБС «IPRbooks»
2. Крылов Г.О. Понятийный аппарат информационной безопасности [Электронный ресурс]: словарь/ Крылов Г.О., Ларионова С.Л., Никитина В.Л.— Электрон. текстовые данные.— Москва, Саратов: Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016.— 343 с.— Режим доступа: http://www.iprbookshop.ru/64306.html.— ЭБС «IPRbooks»

Тема 4. Информационная безопасность как условие предотвращения информационно-психологической войны

1. Анисимов А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс]/ Анисимов А.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 212 с. — Режим доступа: http://www.iprbookshop.ru/52182.html.— ЭБС «IPRbooks»
2. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебно-методический комплекс/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 342 с.— Режим доступа: http://www.iprbookshop.ru/14642.html.— ЭБС «IPRbooks»

6.4. Нормативные правовые документы

1. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993г (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008г. № 6-ФКЗ и от 30.12.2008г. № 7-ФКЗ) // Российская газета, 2009г. № 7 - от 21января.
2. Федеральный конституционный закон от 17.12.1997г. № 2-ФКЗ «О Правительстве Российской Федерации» (в ред. от от 07.05.2013 N 3-ФКЗ) // СЗ РФ. 1997г. № 51. Ст. 5712; Ст. 3984; 2013. N 19. Ст. 2294.
3. Бюджетный кодекс Российской Федерации от 31.07.1998г. № 145-ФЗ (ред. от 06.04.2011г. № 68-ФЗ) // СЗ РФ.1998г. № 31. Ст. 3823; 2011г. № 15. Ст. 2041.
4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994г. № 51-ФЗ (ред. от 06.04.201г. № 65-ФЗ) // СЗ РФ.1994г. № 32. Ст. 3301; 2011г. № 15. Ст. 2038.
5. Указ Президента РФ от 10.06.1994г. № 1185 «Об обеспечении взаимодействия Президента Российской Федерации и Правительства Российской Федерации» (ред. от 26.11.2001г) // СЗ РФ. 1994г. № 7. Ст. 697; 2001г. № 49. Ст. 4611.

6.5. Интернет-ресурсы

1. www.government.ru – интернет-портал Правительства Российской Федерации.
2. http://www.mid.ru – Министерство иностранных дел Российской Федерации
3. http://www.scrf.gov.ru/ – Совет Безопасности Российской Федерации
4. http://minsvyaz.ru/ru/ – Минкомсвязи
5. http://www.rossvyaz.ru/ – Федеральное агентство связи
6. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) - http://www.rsoc.ru/
7. http://www.fapmc.ru/magnoliaPublic/rospechat.html – Федеральное агентство по печати и массовым коммуникациям
8. http://www.fsb.ru/ – Федеральная служба безопасности
9. http://www.council.gov.ru/ – Совет Федерации Федерального собрания РФ (Комиссия по информационной политике)
10. http://www.duma.gov.ru/ – Государственная дума Федерального собрания РФ (Комитет по информационной политике)
11. http://www.nak.fsb.ru – Национальный антитеррористический комитет (НАК) -
12. http://www.infoforum.ru – Национальный форум информационной безопасности (Инфофорум)
13. http://www.un.int/russia/new/MainRootrus/index_plain.html – Россия в ООН
14. http://www.infolaw.rniiis.ru – Информационное право (журнал)
15. http://www.frip.ru/ - Фонд развития информационной политики

6.6. Иные источники

1. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Информационная безопасность. - М.: МГФ «Знание», ГЭИТИ, 2005.
2. Безопасность и противоборство в информационной сфере /Под общ. ред. проф. В.И. Анненкова. – М.: РУСАВИА, 2010.
3. Информационная безопасность России /Ю.С. Уфимцев, Е.А. Ерофеев и др. – М.: Изд-во «Экзамен», 2008.
4. Информационная эпоха: вызовы человеку. /Под ред. И.Ю. Алексеевой и А.Ю. Сидорова. – М.: РОСПЭН, 2010.
5. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. – М.: Горячая линия – Телеком, 2006.
6. Расторгуев С.П. Основы информационной безопасности. М.:ИЦ «Академия», 2007.
7. Смирнов А.И. Информационная глобализация и Россия: вызовы и возможности. М.: ИД «Парад», 2005.
8. Шевченко А.В. Управление безопасностью информационных процессов. Учебно-методическое пособие. - М.: Изд-во РАГС, 2009

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».