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 «26» июня 2018 г. № 10

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.03 Модуль «Социокультурные коммуникации»
Б1.В.03.ДВ.08.08 Кибербезопасность

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

Кибербез-ть.

(краткое наименование дисциплины (модуля))

41.03.01 «Зарубежное регионоведение»

(код, наименование направления подготовки)

Аналитика и консалтинг в международных отношениях (с углубленным изучением иностранных языков)

(направленность (профиль))

бакалавр

(квалификация)

очная

(форма обучения)

Год набора – 2019

Москва, 2018 г.

Автор–составитель:
кандидат социологических наук, доцент, доцент кафедры зарубежного регионоведения и международного сотрудничества Жуликова О.В.

Заведующий кафедрой
Заведующий кафедрой зарубежного регионоведения и международного сотрудничества, доктор социологических наук, доцент В.В.Комлева

СОДЕРЖАНИЕ

Y
1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы....4
2. Объем и место дисциплины в структуре ОП ВО....5
3. Содержание и структура дисциплины....6
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине....7
5. Методические указания для обучающихся по освоению дисциплины....13
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине....14
6.1. Основная литература....14
6.2. Дополнительная литература....15
6.3. Учебно-методическое обеспечение самостоятельной работы....15
6.4. Нормативные правовые документы....15
6.5. Интернет-ресурсы....15
6.6. Иные источники....16
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы....16

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

1.1 Дисциплина Б1.В.03.ДВ.08.08 Кибербезопасность обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКр-5	Способен пользоваться современными информационно-коммуникационными технологиями связи	ПКр-5.2	Способность определять основные требования к применению современными информационно-коммуникационными технологиями связи
ДПК-8	Способен осуществлять консультирование по социокультурным и общественно-политическим вопросам развития региона специализации	ДПК-8.4	Способность проводить оценку социокультурным и общественно-политическим вопросам развития региона специализации
ДПК-10	Способен применять методы исследования общественного мнения для принятия управленческих решений	ДПК-10.2	Способность осваивать методы исследования общественного мнения для принятия управленческих решений

1.2 В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
работать с российскими и зарубежными базами данных, применять технологии поиска информации осуществлять сбор и обработку необходимой информации; проводить анализ информационного пространства, каналов информирования	ПКр-5.2	на уровне знаний: демонстрирует знание основных требований к применению современными информационно-коммуникационными технологиями связи в профессиональной деятельности
		на уровне умений: определяет основные требования к применению современными информационно-коммуникационными технологиями связи в профессиональной деятельности
		на уровне навыков: соблюдает основные требования к применению

		современными информационно-коммуникационными технологиями связи в профессиональной деятельности
осуществлять консультирование по общественно-политическим, социально-экономическим, социокультурным вопросам развития региона специализации; готовить обзоры, информационные, аналитические материалы по вопросам международного сотрудничества, развития зарубежных регионов, региональной политики, общественно-политического, социально-экономического, социокультурного развития регионов	ДПК-8.4	на уровне знаний: демонстрирует знание методики оценивания социокультурных и общественно-политических особенностей региона специализации
		на уровне умений: проводит оценку социокультурных и общественно-политических особенностей региона специализации
		на уровне навыков: опирается на знание методики оценивания социокультурных и общественно-политических особенностей региона специализации
осуществлять консультирование по общественно-политическим, социально-экономическим, социокультурным вопросам развития региона специализации; готовить обзоры, информационные, аналитические материалы по вопросам международного сотрудничества, развития зарубежных регионов, региональной политики, общественно-политического, социально-экономического, социокультурного развития регионов	ДПК-10.2	на уровне знаний: демонстрирует знание источников информации, применение научных подходов, концепций и методов, выработанных в рамках исследования общественного мнения
		на уровне умений: проводит анализ возможностей применения методов исследования общественного мнения для принятия управленческих решений
		на уровне навыков: осуществляет поиск информации, применение научных подходов, концепций и методов, выработанных в рамках исследования общественного мнения

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Общая трудоемкость Б1.В.03.ДВ.08.08 Кибербезопасность составляет 2 зачётные единицы, 72 часа

Количество академических часов, выделенных на контактную работу с преподавателем, составляет 32 час: лекционные занятия – 16 часов, практические занятия – 16 часов. Самостоятельная работа составляет 40 часов.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.В.03.ДВ.08.08 Кибербезопасность предусмотрена на 4 курсе, в 7 семестре.

Дисциплина Б1.В.03.ДВ.08.08 Кибербезопасность входит в дисциплины по выбору части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины (модули)».

В содержательном плане опирается на

Б1.В.01.02 Информационные ресурсы и базы данных по зарубежному регионоведению (3 семестр),

Б1.В.03.01 Социология (3 семестр),

Б1.В.03.ДВ.02.01 Этнология и этнопсихология (2 семестр),
Б1.В.03.ДВ.02.02 Этика делового общения (2 семестр),
Б1.В.03.ДВ.03.01 Религии мира (2 семестр),
Б1.В.03.ДВ.03.02 Религии мира (Religions of the world) (2 семестр),
Б1.В.03.ДВ.03.03 Логика (2 семестр),
Б1.В.03.ДВ.07.01 Конфликтология и управление конфликтами (6 семестр),
Б1.В.03.ДВ.07.02 Конфликтология и управление конфликтами (Conflictology and conflict management) (6 семестр),
Б1.В.03.ДВ.07.03 Политические конфликты (6 семестр).

Форма промежуточной аттестации в соответствии с учебным планом – зачет с оценкой.

3. Содержание и структура дисциплины
Очная форма обучения

№ п/п	Наименование тем и/или 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		
Тема 1	Киберпространство и основы кибербезопасности, векторы риска	18	4		4		10	О
Тема 2	Теоретические основы и практические аспекты защиты киберпространства.	18	4		4		10	О
Тема 3	Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности	18	4		4		10	О
Тема 4	Государственная политика в области кибербезопасности и государственный аудит	18	4		4		10	О, Р
Промежуточная аттестация								ЗаО
	Всего:	108	16		16		40	

Примечание:
*** – формы текущего контроля успеваемости: опрос (О), реферат (Р)*
**** - формы промежуточной аттестации: зачет с оценкой (ЗаО)*

Содержание дисциплины

Тема 1 Киберпространство и основы кибербезопасности, векторы риска
Концептуальные основы кибербезопасности. Структура стандарта по киберпезопасности. Базовые меры по кибербезопасности. Национальные стандарты в области киберпезопасности.
Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации. Проверка подлинности (аутентификация) в Интернете. Меры безопасности для пользователя WiFi. Настройка безопасности. Настройка компьютера для безопасной работы. Ошибки пользователя. Меры личной безопасности при сетевом общении. Настройки приватности в социальных сетях

Тема 2 Теоретические основы и практические аспекты защиты киберпространства.

Задачи и уровни обеспечения защиты киберпространства. Аспекты кибербезопасности. Доктрина информационной безопасности РФ.
Технологии защиты. Стратегии снижения рисков. Аудит безопасности. Мониторинг инцидентов кибербезопасности. Реагирование на инциденты кибербезопасности. Адаптивная архитектура безопасности.
Кибератаки и техногенные катастрофы. Защита IT-инфраструктур критически важных объектов. Понятие и виды хакерских атак. Способы защиты от хакерских атак. Кибертерроризм: понятие, приемы, способы предотвращения.

Тема 3 Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности
Информационное противоборство в бизнесе и кибербезопаснсть. Конфиденциальность информации. Угрозы конфиденциальной безопасности. Механизмы обеспечения конфиденциальности файлов и требования к ним. Система защиты информации и требования, предъявляемые к ней.
Кибербезопасность как основной фактор национальной и международной безопасности. Государственные стратегии кибербезопасности: ЕС, США, Канада Япония. Общие принципы стратегии кибербезопасности. Руководство по кибербезопасности для развивающихся стран. Международные нормы по кибербезопасности.

Тема 4 Государственная политика в области кибербезопасности и государственный аудит
Концепция стратегии кибербезопасноти в РФ. Вопросы кибербезопасности в современной государственной политике в области обеспечения национальной безопасности. Государственный аудит в области киберпезопасности. Задачи, стоящие в области государственной политике по обеспечению национальной кибербезопасности.
Деятельность по аттестации объектов информатизации по требованиям безопасности информации. Добровольная и обязательная аттестация. Органы входящие в структуру системы аттестации. Документы и данные необходимые для проведения аттестации объектов вычислительной техники

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.03.ДВ.08.08 Кибербезопасность используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)		Методы текущего контроля успеваемости
Тема 1	Киберпространство и основы кибербезопасности, векторы риска	опрос
Тема 2	Теоретические основы и практические аспекты защиты киберпространства.	опрос
Тема 3	Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности	опрос
Тема 4	Государственная политика в области кибербезопасности и государственный аудит	опрос, защита

		реферата

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

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,
- участие в обсуждении докладов,
- защита реферата.

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, по результатам защиты реферата.
Детализация баллов и критерии оценки текущего контроля успеваемости утверждается на заседании кафедры.

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

Тема 1 Киберпространство и основы кибербезопасности, векторы риска

1. Концептуальные основы кибербезопасности.
2. Структура стандарта по киберпезопасности.
3. Национальные стандарты в области киберпезопасности.
4. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации.
5. Настройка компьютера для безопасной работы.

Тема 2 Теоретические основы и практические аспекты защиты киберпространства.

1. Задачи и уровни обеспечения защиты киберпространства.
2. Доктрина информационной безопасности РФ.
3. Технологии защиты.
4. Аудит безопасности.
5. Мониторинг инцидентов кибербезопасности.
6. Реагирование на инциденты кибербезопасности.
7. Кибератаки и техногенные катастрофы.
8. Способы защиты от хакерских атак.
9. Кибертерроризм: понятие, приемы, способы предотвращения.

Тема 3 Менеджмент кибербезопасности в национальном контексте, международные организации по кибербезопасности

1. Информационное противоборство в бизнесе и кибербезопаснсть.
2. Конфиденциальность информации.
3. Система защиты информации и требования, предъявляемые к ней.
4. Кибербезопасность как основной фактор национальной и международной безопасности.
5. Государственные стратегии кибербезопасности: ЕС, США, Канада Япония.
6. Общие принципы стратегии кибербезопасности.
7. Руководство по кибербезопасности для развивающихся стран.
8. Международные нормы по кибербезопасности.

Тема 4 Государственная политика в области кибербезопасности и государственный аудит

1. Концепция стратегии кибербезопасноти в РФ.
2. Вопросы кибербезопасности в современной государственной политике в области обеспечения национальной безопасности.
3. Государственный аудит в области киберпезопасности.
4. Задачи, стоящие в области государственной политике по обеспечению национальной кибербезопасности.
5. Деятельность по аттестации объектов информатизации по требованиям безопасности информации.
6. Документы и данные необходимые для проведения аттестации объектов вычислительной техники

Примерные темы рефератов

1. Национальные стандарты России в области киберпезопасности
2. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации
3. Характеристика современного вредоносного программного обеспечения и виды кибератак
4. Новые технологии и новые угрозы информационной безопасности
5. Особенности современных информационных систем как объекта защиты информации
6. Основные международные стандарты и наборы рекомендаций в области проектного и процессного управления
7. Основные угрозы, риски и уязвимости в сфере кибербезопасности и критической информационной инфраструктуры
8. Основные понятия в сфере функциональной безопасности
9. Положения основных нормативных актов, регулирующих сферу безопасности критической информационной инфраструктуры Российской Федерации

4.3. Оценочные средства для промежуточной аттестации.

4.3.1. Перечень компетенций 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
ПКр-5	Способен пользоваться современными информационно-коммуникационными технологиями связи	ПКр-5.2	Способность определять основные требования к применению современными информационно-коммуникационными технологиями связи
ДПК-8	Способен осуществлять консультирование по социокультурным и общественно-политическим вопросам развития	ДПК-8.4	Способность проводить оценку социокультурным и общественно-политическим вопросам развития региона специализации

	региона специализации		
ДПК-10	Способен применять методы исследования общественного мнения для принятия управленческих решений	ДПК-10.2	Способность осваивать методы исследования общественного мнения для принятия управленческих решений

Этап освоения компетенции	**Показатель оценивания**	**Критерий оценивания**
ПКр-5.2 Способность определять основные требования к применению современными информационно-коммуникационными технологиями связи	Определяет основные требования основные требования к применению современными информационно-коммуникационными технологиями связи в профессиональной деятельности Соблюдает основные требования к применению современными информационно-коммуникационными технологиями связи в профессиональной деятельности	Определены основные требования к применению современными информационно-коммуникационными технологиями связи в профессиональной деятельности Продемонстрированы основные требования к применению современными информационно-коммуникационными технологиями связи в профессиональной деятельности
ДПК-8.4 Способность проводить оценку социокультурным и общественно-политическим вопросам развития региона специализации	Опирается на знание методики оценивания социокультурных и общественно-политических особенностей региона специализации Проводит оценку социокультурных и общественно-политических особенностей региона специализации	Демонстрирует знание методики оценивания социокультурных и общественно-политических особенностей региона специализации Проведение оценки социокультурных и общественно-политических особенностей региона специализации
ДПК-10.2 Способность осваивать методы исследования общественного мнения для принятия управленческих решений	Осуществляет поиск информации, применение научных подходов, концепций и методов, выработанных в рамках исследования общественного мнения Проводит анализ возможностей применения методов исследования общественного мнения для принятия управленческих	Выявлены научных подходов, концепций и методов, выработанных в рамках исследования общественного мнения Проведен анализ возможностей применения методов исследования общественного мнения для принятия управленческих решений

	решений	

4.3.2. Типовые оценочные средства

Типовые вопросы к зачету с оценкой

1. Концептуальные основы кибербезопасности.
2. Структура стандарта по киберпезопасности.
3. Национальные стандарты в области киберпезопасности.
4. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации.
5. Настройка компьютера для безопасной работы.
6. Задачи и уровни обеспечения защиты киберпространства.
7. Доктрина информационной безопасности РФ.
8. Технологии защиты.
9. Аудит безопасности.
10. Мониторинг инцидентов кибербезопасности.
11. Реагирование на инциденты кибербезопасности.
12. Кибератаки и техногенные катастрофы.
13. Способы защиты от хакерских атак.
14. Кибертерроризм: понятие, приемы, способы предотвращения.
15. Информационное противоборство в бизнесе и кибербезопаснсть.
16. Конфиденциальность информации.
17. Система защиты информации и требования, предъявляемые к ней.
18. Кибербезопасность как основной фактор национальной и международной безопасности.
19. Государственные стратегии кибербезопасности: ЕС, США, Канада Япония.
20. Общие принципы стратегии кибербезопасности.
21. Руководство по кибербезопасности для развивающихся стран.
22. Международные нормы по кибербезопасности.
23. Концепция стратегии кибербезопасноти в РФ.
24. Вопросы кибербезопасности в современной государственной политике в области обеспечения национальной безопасности.
25. Государственный аудит в области киберпезопасности.
26. Задачи, стоящие в области государственной политике по обеспечению национальной кибербезопасности.
27. Деятельность по аттестации объектов информатизации по требованиям безопасности информации.
28. Документы и данные необходимые для проведения аттестации объектов вычислительной техники

Типовые задания к зачету с оценкой

1. Составьте практические рекомендации по использованию результатов научных исследований для организации работ по исследованию кибербезопасности (информационной безопасности) «Интернета вещей» и объектов КИИ.
2. Проанализируйте актуальные угрозы кибербезопасности (информационной безопасности) в системах «Интернета вещей» и объектов КИИ
3. Опишите неформализованные модели средств, систем и процессов, применяемых в системах «Интернета вещей» и объектов КИИ, проанализируйте их с точки зрения кибербезопасности (информационной Выступление на семинаре. 5 безопасности)
4. Назовите основные проблемы безопасности IoT инфраструктуры в разрезе типов атак по уровням модели OSI
5. Перечислите основные положения стандартов по функциональной безопасности АСУТП («Индустриального Интернета вещей»).

6. Раскройте основные требования НПА и положения стандартов и лучших практик по обеспечению информационной безопасности (кибербезопасности) «Интернета вещей» и объектов КИИ

Шкала оценивания.
Оценка знаний, умений, навыков проводится на основе балльно-рейтинговой системы: 30% из 100% (или 30 баллов из 100) - вклад в итоговую оценку по результатам промежуточной аттестации.
При оценивании ответа обучающегося в ходе промежуточной аттестации можно опираться на следующие критерии:

Баллы	Критерий оценки
26-30	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, 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.
16-25	Обучающийся показывает достаточный уровень компетентности, знания материалов занятий, учебной и методической литературы, законодательства и практики его применения. Уверенно и профессионально, грамотным языком, ясно, четко и понятно излагает состояние и суть вопроса. Знает нормативно-законодательную и практическую базу, но при ответе допускает несущественные погрешности. Обучающийся показывает достаточный уровень профессиональных знаний, свободно оперирует понятиями, методами оценки принятия решений, имеет представление: о междисциплинарных связях, увязывает знания, полученные при изучении различных дисциплин, умеет анализировать практические ситуации, но допускает некоторые погрешности. Ответ построен логично, материал излагается хорошим языком, привлекается информативный и иллюстрированный материал, но при ответе допускает некоторые погрешности. Вопросы не вызывают существенных затруднений.
6-15	Обучающийся показывает достаточные знания материалов занятий, но при ответе отсутствует должная связь между анализом, аргументацией и выводами. На поставленные членами комиссии вопросы отвечает неуверенно, допускает погрешности. Обучающийся владеет практическими навыками, привлекает иллюстративный материал, но чувствует себя неуверенно при анализе междисциплинарных связей. В ответе не всегда присутствует логика, аргументы привлекаются недостаточно веские. На поставленные вопросы затрудняется с ответами, показывает недостаточно глубокие знания.
0-5	Обучающийся показывает слабые знания материалов занятий, 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.

Шкала перевода из многобалльной системы в традиционную:

- обучающемуся выставляется оценка «неудовлетворительно» если обучающийся набрал менее 50 баллов,
- оценка «удовлетворительно» выставляется при условии, если обучающийся набрал от 50 до 65 баллов;
- оценка «хорошо» выставляется при условии, если обучающийся набрал от 66 до 75 баллов;
- оценка «отлично» выставляется при условии, если обучающийся набрал от 76 до 100 баллов.

100 баллов выставляется при условии выполнения всех требований, а также при обязательном проявлении творческого отношения к предмету, умении находить оригинальные, не содержащиеся в учебниках ответы, умении работать с источниками, которые содержатся дополнительной литературе к курсу, умении соединять знания, полученные в данном курсе со знаниями других дисциплин.

4.4. Методические материалы

Студент допускается к зачету с оценкой по дисциплине в случае выполнения им всех заданий и мероприятий, предусмотренных программой дисциплины.

Зачет с оценкой проводится в форме ответа на вопросы и выполнения практических заданий, представленных в Разделе 4.3.2. Готовиться к зачету с оценкой необходимо последовательно, на протяжении всего периода изучения дисциплины.

Студенту необходимо внимательно изучить и осмыслить содержание вопросов к зачету с оценкой, отраженное в рекомендованных учебниках и других источниках (Интернет-ресурсы, научно-методические журналы и пр.). Структурировать теоретический материал, составить план его представления.

Ответ вопрос и решение практического задания важно излагать с позиции значения для профессиональной деятельности. При этом важно показать знание не только теории вопроса, но и практическое применение.

Результат по сдаче зачета с оценкой объявляется студентам и вносится в экзаменационную ведомость и зачетную книжку. Оценка «неудовлетворительно» проставляется в ведомости.

5. Методические указания для обучающихся по освоению дисциплины

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.

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. Архитектура основных подсистем обеспечения ИБ объектов КИИ
2. Основные определения СМИБ и особенности построения СМИБ для объектов КИИ на промышленных объектах
3. Положения нормативных актов, устанавливающих ответственность за нарушение

требований законодательства РФ в сфере обеспечения безопасности КИИ и КВО ТЭК
4. Основные средства обеспечения кибербезопасности (архитектура, принципы построения)
5. Принципы проектирования систем безопасности значимых объектов КИИ
6. Состав и способы организации деятельности сил обеспечения кибербезопасности объектов КИИ
7. Основные риски и проблемы усовершенствования системы кибербезопасности
8. Состав и классификация систем для «Умного города», критерии оценки безопасности, основных угроз, рисков и проблем, структуры и особенностей построения модели угроз

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.

Методические рекомендации по написанию реферата:
Реферат является самостоятельной практической работой обучающихся. Он призван определить степень освоения студентом знаний и навыков, полученных им в процессе изучения дисциплины.
Текст работы должен быть написан в научном стиле. Оформление текста также должно быть выполнено грамотно. Следует избегать пустых пространств и, тем более, страниц. На все таблицы, рисунки и диаграммы делаются ссылки в тексте.
Работа выполняется в формате А4. Шрифт – TimesNewRoman. Основной текст работы набирается 14-м шрифтом через 1,5 интервала, выравнивание по ширине, межбуквенный интервал «Обычный», красная строка 1,25 см. Автоматически расставляются переносы. Поля: верхнее 2,0 см, нижнее 2,0 см, левое 3 см, правое 1 см. Промежутки между абзацами отсутствуют. Введение, главы, заключение, список литературы и приложения форматируются как заголовки первого уровня и начинаются каждый с новой страницы. Подразделы глав с новой страницы не начинаются.
Сноски делаются внизу страницы. Таблицы и рисунки нумеруются отдельно. Номер включает номер главы и номер рисунка/таблицы в данной главе.
Страницы работы должны быть пронумерованы. Нумерация начинается со страницы с оглавлением, на которой ставится цифра «2» и далее – по порядку. Окончание нумерации приходится на последний лист списка литературы. Номер ставится внизу страницы справа. На страницах с приложениями номера не ставятся, и в оглавление они не выносятся. В оглавлении указывается только номер первого листа первого приложения.
Объем реферата 7-15 стр.

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. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/450371 (дата обращения: 26.06.2020).
2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/449350 (дата обращения: 26.06.2020).

6.2. Дополнительная литература

1. Бурда А.Г. Современные информационные технологии в управлении - Краснодар: Южный институт менеджмента, 2013 - http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/25983.— ЭБС «IPRbooks»
2. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/448295 (дата обращения: 26.06.2020).
3. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru.ezproxy.ranepa.ru:3561/bcode/451108
4. Артемов, А. В. Информационная безопасность : курс лекций / А. В. Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/33430.html

6.3. Учебно-методическое обеспечение самостоятельной работы

1. 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»

2. 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»

6.4. Нормативные правовые документы

1. Конституция Российской Федерации.

2. Об общих принципах организации законодательных (представительных) и исполнительных органов государственной власти субъектов Российской Федерации: Федеральный закон от 06.10.1999 № 184-ФЗ

6.5. Интернет-ресурсы

1. Национальная электронная библиотека. Режим доступа: http://www.rusneb.ru
2. Электронный фонд Российской национальной библиотеки (РНБ). Электронная библиотека Режим доступа: http://leb.nlr.ru
3. Электронная библиотека Российской государственной библиотеки (РГБ). Режим доступа: http://elibrary.rsl.ru/
4. Научная электронная библиотека ГПНТБ (каталог Государственной Публичной научно-технической библиотеки) России. Режим доступа: http://ellib.gpntb.ru/
5. Каталог Научной Библиотеки МГУ. Режим доступа: http://search.nbmgu.ru/search/
6. Научная электронная библиотека eLIBRARY.RU. Режим доступа: http://www.elibrary.ru/
7. Электронная Библиотека ГУУ. Полнотекстовые зарубежные базы данных. Режим доступа: http://library.guu.ru/Full_text_foreign_database.html
8. Президентская библиотека им. Б. Н. Ельцина. Режим доступа: http://www.prlib.ru/
9. BIBLIOPHIKA. Электронная библиотека ГПИБ России. Режим доступа: http://www.bibliofika.ru/
10. Электронная библиотека "Научное наследие России». Режим доступа: http://nasledie.enip.ras.ru/index.html

6.6. Иные источники

1. Грибова Н.А. Дипломатический этикет и сервис. - Киров : МЦНИП, 2014. – 33 с.
2. Карпычева Е. В. Дипломатический протокол и этикет: учебно-методический комплекс. - М.: Юридический ин-т МИИТа, 2012. – 200 с.
3. Квасов О.К. Протокол и этикет: дипломатический, деловой, общегражданский: Учебное пособие. - М.: Восток-Запад, 2011. – 183 с.
4. Политология / Бельский В.Ю., Сацута А.И., Гусев Н.Н., Бороздин А.Н., Асонов Н.В., Шикунов Д.В., Вольнов В.А. - М.: ЮНИТИ-ДАНА, 2012 - http://www.iprbookshop.ru.ezproxy.ranepa.ru:3561/8113.- ЭБС «IPRbooks»
5. Фесенко О. П. Практикум по конфликтологии, или учимся разрешать конфликты : рекомендовано Редакционно-издательским советом... / О.П. Фесенко, С.В. Колесникова; Российская академия образования ; Московский психолого-социальный ин-т. - 3-е изд., стер. - М. : ФЛИНТА : МПСУ, 2018. - 125 с.

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/.