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

Факультет информационных технологий и анализа данных
Кафедра системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры системного анализа и информатики

Протокол от «03» сентября 2019 г.

№1

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.07 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

по направлению подготовки
38.03.05 Бизнес-информатика
(код и наименование направления подготовки)

Цифровой бизнес
направленность (профиль)

Бакалавр
квалификация выпускника

Очная
форма обучения

набор 2020 г.

Москва, 2019 г.

Автор–составитель:

к.в.н., преподаватель Ковальчук Н. Н.

(ученое звание, ученая степень, должность) *(Ф.И.О.)*

Заведующий кафедрой системного анализа и информатики

(наименование кафедры)

к.т.н., доцент Маруев С. А.

(ученая степень и(или) ученое звание) *(Ф.И.О.)*

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы…… 4
2. Объем и место дисциплины (модуля) в структуре образовательной программы ……... 6
3. Содержание и структура дисциплины (модуля)……... 6
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине (модулю)……..……... 12
5. Методические указания для обучающихся по освоению дисциплины (модуля)……... 17
6. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине (модулю)……..……. 19
   6.1. Основная литература……..……...…… 19
   6.2. Дополнительная литература……...……...…...…… 19
   6.3. Учебно-методическое обеспечение самостоятельной работы…… 19
   6.4. Нормативные правовые документы…….……..…….. 19
   6.5. Интернет-ресурсы…….……..……... 21
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы …...……...…..…….. 21

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

Дисциплина «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-16	умение разрабатывать контент и ИТ-сервисы предприятия и Интернет-ресурсов	ПК-16.2	2 этап (код этапа: ПК-16.2) Способен управлять процессами создания и использования информационных сервисов (контент-сервисов) с учетом защиты информационной безопасности
ПК-27	способность использовать лучшие практики продвижения инновационных программно-информационных продуктов и услуг	ПК-27.2	Способен управлять процессами жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов) с соблюдением информационной безопасности

Менеджер продуктов в области информационных технологий. Приказ Минтруда России от 20.11.2014 N 915н (Зарегистрировано в Минюсте России 18.12.2014 N 35273)

В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
С - Управление серией продуктов и группой их менеджеров. Заказ и анализ результатов технологических исследований в интересах серии продуктов (С/01.6) Разработка бизнес-планов, ценовой политики и стратегии развития серии продуктов (С/02.6) Заключение партнерских соглашений и развитие отношений с партнерами (С/01.3) Управление бюджетом серии продуктов (С/01.4) Управление группой менеджеров продуктов (С/01.5) Продвижение продуктов(С/016) Заказ и контроль выполнения программы проектов по созданию, развитию, выводу на	ПК-16.2	На уровне знаний: знать: основные положения теории информационной безопасности (основные понятия и определения, интересы и ценности в области информационной безопасности, основные факторы и угрозы, закономерности и принципы, направления обеспечения информационной безопасности; состав, структуру и основные функции органов обеспечения информационной безопасности организации); основные нормативно-правовые документы Российской Федерации и международного права в изучаемой области.
		На уровне умений : уметь определять интересы и ценности в информационной сфере, ранжировать их по приоритетности; выявлять и оценивать угрозы интересам в информационной сфере при различных условиях обстановки, осуществлять прогноз их развития; принимать управленческие решения по вопросам обеспечения информационной безопасности и реализовывать их на практике.
		На уровне навыков: владеть: механизмах принятия

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
рынок и продажам продуктов серии (С/01.7) Управление патентами на технологии, создаваемые в рамках продуктов (С/01.8) Разработка предложений по приобретению и продаже технологических, продуктовых и прочих интеллектуальных активов и организаций (С/01.9)		решений по обеспечению информационной безопасности в условиях риска и неопределенности, вопросах информационно-аналитического обеспечения процессов принятия решений в области информационной безопасности, с существующими и перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере;
	ПК-27.2	На уровне знаний: знать: основные положения теории информационной безопасности (основные понятия и определения, интересы и ценности в области информационной безопасности, основные факторы и угрозы, закономерности и принципы, направления обеспечения информационной безопасности; состав, структуру и основные функции органов обеспечения информационной безопасности организации); основные нормативно-правовые документы Российской Федерации и международного права в изучаемой области**.**
		На уровне умений : уметь определять интересы и ценности в информационной сфере, ранжировать их по приоритетности; выявлять и оценивать угрозы интересам в информационной сфере при различных условиях обстановки, осуществлять прогноз их развития; принимать управленческие решения по вопросам обеспечения информационной безопасности и реализовывать их на практике.
		На уровне навыков: владеть механизмах принятия решений по обеспечению информационной безопасности в условиях риска и неопределенности, вопросах информационно-аналитического обеспечения процессов принятия решений в области информационной безопасности, с существующими и перспективными возможностями по недопущению возникновения и нейтрализации угроз в информационной сфере;

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

Дисциплина «Основы информационной безопасности» имеет индекс Б1.В.07, объем академических часов 108 академических часов, 3 з.е., изучается на 4 курсе в 7 семестре в соответствии с учебным планом. Количество академических часов, выделенных на контактную работу с преподавателем – 28 часов, на самостоятельную работу обучающихся - 80 часов; форма промежуточной аттестации – зачет.

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующими дисциплинами: комплексный междисциплинарный учебный курс, базирующийся на теории безопасности жизнедеятельности, политологии, социологии, права, менеджмента, теоретических основ информатики, программирования, операционных сред, систем и оболочек, вычислительных систем, сетей и коммуникаций, позволяющих раскрыть основные положения по обеспечению информационной безопасности Российской Федерации в современных условиях.

Наименования последующих учебных дисциплин: управление разработкой ИС, правовая защита интеллектуальной собственностью, хранилища данных.

3. Содержание и структура дисциплины (модуля)

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Введение. Роль и место информационной безопасности в развитии современного общества.	8	1		1		6	
Раздел 1. Теоретические основы информационной безопасности.								
Тема 2	Тема 1.1. Основные понятия и определения, сущность и содержание информационной безопасности.	6	1		1		4	
Тема 3	Тема 1.2. Угрозы и уровни обеспечения информационной безопасности в условиях глобализации.	8	1		1		6	
Тема 4	Тема 1.3. Нормативно-правовое и концептуальное обеспечение информационной безопасности.	6	1		1		4	
Тема 5	Тема 1.4. Система обеспечения информационной безопасности Российской Федерации (региона, муниципального образования).	8	1		1		6	
Тема 6	Тема 1.5. Информационная безопасность различных сфер жизнедеятельности общества.	8	1		1		6	
Тема 7	Тема 1.6. Информационная безопасность отраслей социально-трудовой сферы Российской Федерации.	8	1		1		6	
Тема 8	Тема 1.7. Применение методов системных исследований при анализе	6	1		1		4	

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
	процессов обеспечения информационной безопасности.							
Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности организации (предприятия).								
Тема 9	Тема 2.1. Основы информационной безопасности организации (предприятия).	6	1		1		4	
Тема 10	Тема 2.2. Особенности нормативно - правового обеспечения информационной безопасности в государственном секторе и бизнесе.	6	1		1		4	
Тема 11	Тема 2.3. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).	8	1		1		6	
Тема 12	Тема 2.4. Информационный аудит организации (предприятия).	8	1		1		6	
Тема 13	Тема 2.5. Информационно-технические аспекты обеспечения информационной безопасности.	8	1		1		6	
Тема 14	Тема 2.6. Методы, способы и средства защиты информации в автоматизированных информационных системах.	8	1		1		6	
Тема 15	Тема 2.7. Информационно – психологические аспекты обеспечения информационной безопасности.	6					6	
	Промежуточная аттестация							Зачет
Всего по дисциплине		**108**	**14**		**14**		**80**	

соответствии с учебным планом;

*** – формы текущего контроля успеваемости: опрос (О), тестирование (Т), контрольная работа (КР), коллоквиум (К), эссе (Э), реферат (Р), диспут (Д) и др.*

Содержание дисциплины (модуля)

Содержание тем дисциплины с указанием лабораторных и/или практических занятий при наличии

Вводная лекция. Роль и место информационной безопасности в развитии современного общества.

Информация как стратегический ресурс государства и общества. Необходимость изучения вопросов информационной безопасности. Предмет курса, его цели, задачи, структура и порядок изучения.

Исторические аспекты вопроса. Основные факторы, влияющие на процесс обеспечения информационной безопасности в ретроспективе глобального исторического процесса и на современном этапе. Информатизация государства и общества. Эволюция приоритетов угроз информационной безопасности в XXI веке. Теории информационного общества. Концепции информационных войн иностранных государств. Последствия глобализации для информационной безопасности.

Раздел 1. Теоретические основы информационной безопасности.

Тема 1.1. Основные понятия и определения, сущность и содержание информационной безопасности.

Основные понятия и определения теории информационной безопасности в соответствии с действующими нормативно-правовыми документами Российской Федерации и международным правом, а также современными научными взглядами.

Информационная безопасность как составная часть национальной безопасности страны. Составляющие национальных интересов в информационной сфере. Сущность и содержание информационной безопасности с позиций системного подхода.

Цели, задачи, направления (составные части), закономерности и принципы обеспечения информационной безопасности.

Тема 1.2. Угрозы и уровни обеспечения информационной безопасности в условиях глобализации.

Системный подход к построению иерархии последовательно вложенных уровней глобальных угроз информационной безопасности. Особенности форм и содержания угроз на каждом уровне применительно к России. Фасетно-иерархическая классификация угроз информационной безопасности. Специфика информационных угроз на региональном, ведомственном и муниципальном уровнях.

Возможности по нейтрализации угроз информационной безопасности на различных уровнях применительно к существующему состоянию рассматриваемых аспектов в Российской Федерации. Сравнительный анализ проводимых мероприятий по обеспечению информационной безопасности в России и других развитых странах.

Тема 1.3. Нормативно-правовое и концептуальное обеспечение информационной безопасности.

Структура правового обеспечения Российской Федерации в области информационной безопасности: Конституция, Федеральные законы, законы, подзаконные нормативно-правовые акты (Указы Президента, Постановления Правительства, концептуальные и доктринальные документы), государственные стандарты, правовые акты, организационно-распорядительные и методические документы соответствующих федеральных министерств и ведомств. Концепция национальной безопасности, Доктрина информационной безопасности России. Нормативные документы РФ по стандартизации.

Международная нормативно-правовая база по вопросам информационной безопасности. Международные стандарты обеспечения информационного обмена.

Тема 1.4. Система обеспечения информационной безопасности Российской Федерации (региона, муниципального образования).

Состав и структура системы обеспечения информационной безопасности России. Функции и взаимосвязь системообразующих элементов. Особенности обеспечения информационной безопасности на федеральном, региональном, ведомственном и муниципальном уровнях. Основные механизмы обеспечения информационной безопасности: организационный, нормативно-правовой, методическое и технологическое обеспечение, кадровое и научное обеспечение.

Тема 1.5. Информационная безопасность различных сфер жизнедеятельности общества.

Составляющие национальных интересов в информационной области для различных сфер жизнедеятельности общества: политической, экономической, социальной, духовной. Специфика информационных угроз, особенности решения вопросов обеспечения информационной безопасности в различных сферах жизнедеятельности общества. Субъекты, объекты, цели и задачи, механизмы обеспечения информационной безопасности. Защита интеллектуальной собственности. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Федеральных целевых программ в области информационных технологий.

Тема 1.6. Информационная безопасность отраслей социально-трудовой сферы Российской Федерации.

Система обеспечения информационной безопасности социально-трудовой сферы России. Особенности формирования и развития жизненно-важных интересов и ценностей, угроз и опасностей в информационной области для различных отраслей социально-трудовой сферы: образования, здравоохранения, культуры, рынка труда, процессов обеспечения занятости, жилищно-коммунального хозяйства и др. Специфика рассматриваемых вопросов применительно к проблемам демографии, миграции и эмиграции населения, этническим вопросам. Роль и место вопросов обеспечения информационной безопасности в ходе реализации Приоритетных национальных проектов.

Тема 1.7. Применение методов системных исследований при анализе процессов обеспечения информационной безопасности.

Основные положения современной теории системных исследований. Методология применения системного подхода при анализе процессов обеспечения информационной безопасности, соотношение гуманитарных, естественнонаучных и технических аспектов.

Проблема информационно-аналитического обеспечения в достижении опережающего информационного эффекта при осуществлении реформ. Анализ возможностей использования методов математического моделирования при исследовании проблем обеспечения информационной безопасности.

Особенности прогнозирования информационной обстановки. Основные показатели и критерии обеспечения информационной безопасности. Особенности оценки эффективности мероприятий по обеспечению информационной безопасности. Модель принятия управленческого решения, вопросы обеспечения его информационной безопасности.

Раздел 2. Подготовка и проведение мероприятий по обеспечению информационной безопасности организации (предприятия).

Тема 2.1. Основы информационной безопасности организации (предприятия).

Роль и место информационной безопасности в системе комплексной безопасности организации (предприятия). Анализ способов нарушения информационной безопасности. Информационные угрозы, цели и задачи обеспечения информационной безопасности. Принципы, методы и способы обеспечения информационной безопасности. Концепция информационной безопасности организации (предприятия). Модели безопасности и их применение.

Тема 2.2. Особенности нормативно-правового обеспечения информационной безопасности в государственном секторе и бизнесе.

Нормативно-правовая база обеспечения информационной безопасности организации (предприятия). Закон РФ “О государственной тайне”. Федеральный закон РФ “О коммерческой тайне”.

Лицензирование деятельности в области информационной безопасности, сертификация средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации.

Структура внутреннего нормативно-правового обеспечения информационной безопасности в организации. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке. Содержание руководства по обеспечению информационной безопасности в организации.

Создание защищенного документооборота в организации.

Тема 2.3. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).

Основные этапы процесса организации мероприятий по обеспечению информационной безопасности на предприятии (фирме).

Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции. Порядок действий должностных лиц по вопросам обеспечения информационной безопасности в различных условиях обстановки.

Тема 2.4. Информационный аудит организации (предприятия).

Организация и проведение анализа информационной уязвимости предприятия (фирмы). Роль и место информационного аудита в ходе комплексного аудита организации (предприятия), в процессе информационной санации. Виды информационного аудита, условия их проведения, содержание и взаимосвязь. Нормативно-правовая база проведения аудита.

Этапы алгоритма анализа и оценки информационных рисков. Основные направления управления рисками.

Тема 2.5. Информационно-технические аспекты обеспечения информационной безопасности.

Демаскирующие признаки информационных объектов. Органы, принципы, методы, способы и средства добывания информации. Технические каналы утечки информации. Способы и средства предотвращения утечки информации.

Угрозы и объекты обеспечения информационно-технической безопасности, принципы, методы и способы ее обеспечения. Технология процесса обеспечения информационно-технической безопасности. Контроль состояния технической защиты информации.

Тема 2.6. Методы, способы и средства защиты информации в автоматизированных информационных системах.

Анализ способов нарушений информационной безопасности в сетях и их таксономия. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах. Средства программно-математического и программно-технического воздействия. Виды “вирусов” и защита от них.

Использование защищенных компьютерных систем. Системы обнаружения и предотвращения атак. Методы и средства защиты данных, применяемые в сетях. Методы криптографии. Электронная цифровая подпись.

Тема 2.7. Информационно - психологические аспекты обеспечения информационной безопасности.

Теоретические основы межличностной коммуникации, скрытного информационно-психологического управления. Методы и приемы информационно-психологического воздействия на должностных лиц: продуктивного общения, приемы ведения дискуссии, методы и приемы “жесткого” информационно-психологического воздействия. Психологический анализ учебных видеофрагментов. Алгоритмы информационно-психологической защиты: активная защита, пассивная защита.

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

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

В ходе реализации дисциплины используются следующие методы текущего контроля успеваемости обучающихся: при проведении занятий лекционного типа: беседа (диалог) с обучающимися, при проведении занятий семинарского типа: домашние работы по темам практических заданий

4.2. Материалы текущего контроля успеваемости.

Примерные темы докладов:

1. Роль и место информационной безопасности экономических систем в системе национальной безопасности Российской Федерации.
2. Совершенствование законодательства Российской Федерации в области информационной безопасности.
3. Компьютерная преступность как угроза информационной безопасности и основные направления противодействия ей.
4. Анализ основных положений Доктрины информационной безопасности Российской Федерации.
5. “Информационная революция” и информационная безопасность.
6. Анализ использования моделей управления рисками в области информационной безопасности.

7. Значение обеспечения конкурентоспособности отечественной продукции в области информационных технологий для информационной безопасности.

8. Информационная безопасность и реализация Федеральных целевых программ в области информационных технологий.

9. Проблемы создания информационного общества и обеспечение информационной безопасности.

10. Сравнительный анализ состояния и развития систем обеспечения информационной безопасности России и экономически наиболее развитых зарубежных стран.

11. Организация международного сотрудничества по вопросам информационной безопасности в экономической сфере.

12. Система информационной безопасности организации (конкретная организация может быть выбрана слушателем).

13. Использование программно-аппаратных средств для обеспечения требуемого уровня информационной безопасности предприятия (организации).

14. Роль и место информационно-аналитического компонента в системе обеспечения информационной безопасности организации (предприятии).

15. Лицензирование и сертификация как необходимые условия обеспечения информационной безопасности.

16. Проблемы информационной безопасности в Internet и пути их решения.

17. Угрозы информационной безопасности локальной (корпоративной) сети и возможности по их нейтрализации.

18. Информационная безопасность при использовании электронной цифровой подписи.

19. Значение информационно-психологической безопасности в системе информационной безопасности организации (предприятия).

20. Роль и место СМИ в обеспечении информационной безопасности экономической сферы.

21. Оценка эффективности мероприятий по обеспечению информационной безопасности организации (предприятия).

22. Проекты создания технопарков и обеспечение информационной безопасности.

23. Анализ технологий манипулирования личностью и обществом, направления обеспечения информационно-психологической защиты.

24. Информационная безопасность интеллектуальной собственности в России: состояние и перспективы.

25. Категорирование объектов при обеспечении информационной безопасности предприятия (организации).

26. Основные направления компьютерной вирусологии в современном мире.

27. Информационный терроризм и борьба с ним.

28. Современный “киберконтроль” и защита прав человека.

29. Политика обеспечения информационной безопасности организации.

30. Достижения научно-технической революции и обеспечение информационной безопасности.

Целью подготовки докладов является приобретение студентами знаний в области информационной безопасности путем самостоятельного изучения научной, учебной и методической литературы, нормативно-правовой базы Российской Федерации и международного права по вопросам информационной безопасности.

Доклад выполняется в форме реферата объемом до 20 страниц. Тему доклада и литературу по ней слушатель выбирает самостоятельно, учитывая прилагаемый перечень тем и список литературы.

Результаты выполнения этих работ являются основанием для выставления оценок текущего контроля. Выполнение всех работ является обязательным для всех студентов.

Учитываются также результаты работы на практических занятиях. Обучающиеся не выполнившие в полном объеме все эти работы, не допускаются к сдаче экзамена, как не выполнившие график учебного процесса по данной дисциплине. Студент допускается к экзамену, если у него есть положительные оценки по всем материалам

Шкала оценивания текущего контроля

10-бальная шкала	Традиционная шкала	«Зачтено»/ «Не зачтено»	Определение
10	Отлично	Зачтено	Полные, глубокие и систематические знания, знакомство с дополнительной литературой, полный и правильный ответ, творческий подход в понимании и изложении учебного материала, полное выполнение мероприятий текущего контроля.
9	Отлично	Зачтено	Полные, глубокие и систематические знания, полный и правильный ответ, полное выполнение мероприятий текущего контроля.
8	Отлично	Зачтено	Полные и систематические знания, отсутствие существенных неточностей в ответе, полное выполнение мероприятий текущего контроля.
7	Хорошо	Зачтено	Достаточно полные и систематические знания, отсутствие существенных неточностей в ответе, имеются погрешности при выполнении мероприятий текущего контроля.
6	Хорошо	Зачтено	Достаточно полные и систематические знания, отсутствие существенных неточностей в ответе, имеются погрешности при выполнении мероприятий текущего контроля.
5	Удовлетворительно	Зачтено	Знание основного учебного материала в объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий текущего контроля и при ответе.
4	Удовлетворительно	Зачтено	Знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий промежуточного контроля и при ответе.
3	Неудовлетворительно	Не зачтено	Имеются существенные погрешности при выполнении мероприятий текущего контроля, допущены существенные ошибки при ответе, необходима некоторая дополнительная работа.
2	Неудовлетворительно	Не зачтено	Имеются пробелы в знаниях по значительной части учебного материала, допущены существенные ошибки при ответе, необходима значительная дополнительная учебная работа.

10-бальная шкала	Традиционная шкала	«Зачтено»/ «Не зачтено»	Определение
1	Неудовлетворительно	Не зачтено	Не выполнены предусмотренные программой задания, не отработаны практические или лабораторные занятия, необходимы дополнительные занятия по соответствующей дисциплине.
0	Неудовлетворительно	Не зачтено	Нарушение академических норм (плагиат и т.п.)

4.3. Формы, методы (средства) промежуточной аттестации.

4.3.1. Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен *(в соответствии с учебным планом)*, который проводится в устной форме. Задания содержат вопросы, в которых необходимо использовать теоретические знания и практическое задание, демонстрирующие способность организация взаимодействия с клиентами и партнерами в процессе решения задач управления информационной безопасностью ИТ-инфраструктуры предприятия и умение консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия. На экзамен выносятся основные вопросы, рассматриваемые в рамках всего курса. Основой для определения оценки служит объем и уровень усвоения студентами материала, предусмотренного программой данного курса и подведения итогов по результатам выполнения заданий текущего контроля успеваемости

Список вопросов для подготовки к экзамену:

1. Основные понятия и определения теории информационной безопасности.
2. Роль и место информационной безопасности в системе национальной безопасности Российской Федерации.
3. Основные положения Доктрины информационной безопасности Российской Федерации.
4. Сущность и содержание информационно-технической безопасности.
5. Сущность и содержание информационно-психологической безопасности.
6. Информационно-аналитическое обеспечение в системе информационной безопасности.
7. Нормативно-правовая база российского законодательства в области информационной безопасности.
8. Международные нормативно-правовые документы по вопросам информационной безопасности.
9. Состояние и перспективы борьбы с компьютерной преступностью в России. Анализ положений Уголовного кодекса Российской Федерации.
10. Основные направления реализации Федеральной целевой программы “Электронная Россия” и информационная безопасность.
11. Интересы личности, общества и государства в информационной сфере.
12. Угрозы жизненно-важным интересам личности, общества и государства в информационной сфере.
13. Система обеспечения информационной безопасности России.
14. Система информационной безопасности региона, ведомства, муниципального образования.
15. Роль и место негосударственных организаций и частных лиц в системе обеспечения информационной безопасности Российской Федерации.
16. Международные стандарты информационного обмена.

17. Виды “нарушителей” режима защиты информации, модели их действий.
18. Основные нормативно-правовые и руководящие документы, касающиеся вопросов соблюдения государственной тайны и их содержание.
19. Основные нормативно-правовые и руководящие документы, касающиеся вопросов соблюдения коммерческой тайны и их содержание.
20. Определение и содержание процессов лицензирования и сертификации.
21. 20. Система информационной безопасности организации (предприятия).
22. Органы обеспечения информационной безопасности организации (предприятия): состав, структура и функции в различных условиях обстановки.
23. Организация мероприятий по обеспечению информационной безопасности предприятия (фирмы).
24. Разрабатываемые в организации документы по вопросам информационной безопасности и требования по их корректировке.
25. Создание и обеспечение защищенного документооборота в организации.
26. 24. Информационный аудит организации (предприятия).
27. Анализа информационных рисков и управление ими.
28. Органы, методы, способы и средства добывания информации по техническим каналам.
29. Способы и средства защиты информации от утечки по техническим каналам в автоматизированных информационных системах.
30. Средства программно-математического и программно-технического воздействия и защита от них.
31. Виды компьютерных “вирусов” и защита от них.
32. Методы и средства защиты данных, применяемые в сетях.
33. Понятие и содержание криптографии, основные методы.
34. Электронная цифровая подпись (понятие, содержание процесса использования ЭЦП, проблемы).
35. Методы и приемы информационно-психологического воздействия на должностных лиц.
36. Алгоритмы информационно-психологической защиты.
37. Использование интернет - технологий и обеспечение информационной безопасности.
38. Основные технологии построения защищенных информационных систем.
39. Формы контроля состояния технической защиты информации.
40. Государственные стандарты, регламентирующие терминологию в области защиты информации.
41. Средства защиты информации от утечки по техническим каналам.
42. Защита интеллектуальной собственности (определение, содержание процесса защиты, проблемы).

Критерии оценивания уровня формирования компетенций

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*	**Оценка (баллы)**

Этап освоения компетенции	Показатель оценивания *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	Критерий оценивания *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*	Оценка (баллы)
ОПК - 1.2	Самостоятельно проводит сбор и оценку достоверности собранной информации. Осуществляет декомпозицию описываемого объекта на структурные элементы. Устанавливает иерархические связи между элементами.	Собрана полная информация об объекте. Исключена недостоверная информация. Названы все структурные элементы. Между элементами установлены прямые и опосредованные взаимосвязи. Выстроена иерархия элементов.	Промежуточная аттестация зачет
2 этап (код этапа: ПК-27.2) Способен управлять процессами жизненного цикла контента предприятия и Интернет-ресурсов, управлять процессами создания и использования информационных сервисов (контент-сервисов) с соблюдением информационной безопасности	Оценка уровня качества ИТ-инфраструктуры с точки зрения применимости модели контента на различных этапах жизненного цикла Определяет оптимальное количество необходимых стадий жизненного цикла контента для развития ИТ-инфраструктуры. Разрабатывает модель организационной и функциональной структур предприятия, осуществляющего предоставление сервисов ИТ.	1. Определен уровень качества ИТ-инфраструктуры предприятия для выбранной модели контента. 2. Определено оптимальное количество необходимых стадий жизненного цикла контента для развития ИТ-инфраструктуры 3. Разработана модель организационной и функциональной структур предприятия, осуществляющего предоставление сервисов ИТ	Промежуточная аттестация
2 этап (код этапа: ПК-16.2) Способен управлять процессами создания и использования информационных сервисов (контент-сервисов) с учетом защиты информационной безопасности	Оценка степени безопасности ИТ-инфраструктуры с точки зрения типа ИТ инфраструктуры, угроз, ресурсов и существующих ограничений. Определяет оптимальное количество необходимых ресурсов для оценки угроз ИБ и мер для их устранения. Контролирует степень изменений ИБ ИТ инфраструктуры.	Даны предложения по оптимизации процесса управления информационной безопасностью Разработаны меры по организации процесса управления информационной безопасностью ресурсов ИТ, вовлечение и привлечение необходимых ресурсов Предложены необходимые изменения процесса управления информационной безопасностью ресурсов ИТ	Промежуточная аттестация

Критерии оценки знаний, умений, навыков при сдаче экзамена:

- *оценка "отлично"* выставляется студенту, показавшему глубокое и всестороннее знание и понимание учебного материала, предусмотренного программой курса, грамотно и правильно отвечающему на все вопросы билета и дополнительные вопросы;
- *оценка "хорошо"* выставляется студенту, обнаружившему полное знание учебного материала, предусмотренного программой курса, без существенных недочетов, ответившему на все вопросы экзаменационного билета, но некоторые ответы являются не совсем полными.
- *оценка "удовлетворительно"* выставляется студенту, обнаружившему знание основного учебного материала, предусмотренного программой курса, в объеме необходимом для дальнейшей работы, но допустившему погрешности непринципиального характера в ответе на экзамене;
- *оценка "неудовлетворительно"* выставляется студенту, обнаружившему пробелы в знании основного материала, предусмотренного программой курса, допустившему принципиальные ошибки в ответе на экзамене и при выполнении дополнительных экзаменационных заданий, предусмотренных программой.

Пересдача экзамена (в случае получения студентом оценки "неудовлетворительно") осуществляется в установленном порядке.

4.4. Методические материалы по проведению промежуточной аттестации

Экзамен проводится в соответствии с графиком учебного процесса учетом проведения мониторинга уровня освоения компетенции по результатам выполнения самостоятельных заданий. Оценивание осуществляется в соответствии со шкалой оценивания. Студентам, не выполнившим домашние задания и (или) контрольные задания по уважительным причинам, предоставляется возможность их выполнения и сдачи.

5. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студента по дисциплине предусмотрена учебным планом и составляет 36 часов по очной форме обучения. Студенты выполняют следующие виды заданий: подготовка реферата, подготовка доклада (сообщения).

Подготовка докладов и сообщений может широко использоваться студентами при подготовке к практическим занятиям. Данный вид самостоятельной работы рассматривается как вспомогательный. В то же время темы выступлений на занятиях могут быть развернуты в темы студенческих научных исследований и стать основой для участия в студенческих научно-практических конференциях, олимпиадах, конкурсах студенческих научных работ.

1. Советы по планированию и организации времени, необходимого для изучения дисциплины. Рекомендуется следующим образом организовать время, необходимое для изучения дисциплины: Изучение конспекта лекции в тот же день после лекции – 10-15 минут. Повторение лекции за день перед следующей лекцией – 10-15 минут. Изучение теоретического материала по учебнику и конспекту – 1 час в неделю. Подготовка к практическому занятию – 1 час. Тогда общие затраты времени на освоение курса студентами составят около 2,5 часа в неделю.

2. Описание последовательности действий студента («сценарий изучения дисциплины»). Следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий: 1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10-15 минут). 2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10-15 минут). 3. В течение недели выбрать время для работы с литературой в библиотеке и для решения задач (по 1 часу). 4. При подготовке к практическим занятиям повторить основные понятия и разобрать примеры на

компьютере. Решая упражнение или задачу, – предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1-2 аналогичные задачи.

4. Рекомендации по работе с литературой. Рекомендуется, кроме «заучивания» материала, добиться понимания изучаемой темы дисциплины. С этой целью после прочтения очередной главы желательно выполнить несколько простых упражнений на соответствующую тему. Кроме того, очень полезно мысленно задать себе и попробовать ответить на следующие вопросы: о чем эта глава, какие новые понятия в ней введены, каков их смысл.

5. Советы по подготовке к зачету. Дополнительно к изучению конспектов лекций необходимо пользоваться учебниками по дисциплине. Вместо «заучивания» материала важно добиться понимания изучаемых тем дисциплины. При подготовке к нужно освоить теорию: разобрать определения всех понятий структурного программирования, рассмотреть примеры и самостоятельно решить несколько типовых задач из каждой темы. При решении задач всегда необходимо комментировать свои действия и не забывать о содержательной интерпретации.

6. Указания по организации работы с контрольно-измерительными материалами. При выполнении домашних заданий и подготовке к контрольной работе необходимо сначала прочитать теорию и изучить примеры по каждой теме. Решая конкретную задачу, предварительно следует понять, что требуется от Вас в данном случае, какой теоретический материал нужно использовать, наметить общую схему решения. Если задача решается «по образцу» рассмотренного на практическом занятии или в методическом пособии примера, то желательно после этого обдумать процесс решения и попробовать решить аналогичную задачу самостоятельно.

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. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие: гриф УМО / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - 7-е изд., стер. - М.: Академия, 2012.
2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www-biblio-online-ru.ezproxy.ranepa.ru:2443/bcode/431080

6.2. Дополнительная литература.

1. Мельников, В. П. Информационная безопасность и защита информации: учебное пособие: гриф УМО / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 3-е изд., стер. - М.: Академия, 2008.
2. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства: учебное пособие : гриф УМО / В. Ф. Шаньгин. - М.: ДМК Пресс, 2008.
3. Информационная безопасность компьютерных систем и сетей: учебное пособие: гриф МО / В. ф. Шаньгин. - М.: Форум : ИНФРА-М, 2008.
4. Ярочкин В. И. Информационная безопасность: учебник: гриф МО / В. И. Ярочкин. - 5-е изд. - М.: Академический Проект, 2008.

6.3. Учебно-методическое обеспечение самостоятельной работы.

1. Ласковец С.В. Методология научного творчества [Электронный ресурс]: Учебное пособие. – Москва : Евразийский открытый институт, 2010. – 32 с. – URL: http://www.biblioclub.ru/90384_Metodologiya_nauchnogo_tvorchestva_Uchebnoe_posobie.html
2. Радаев В.В. Как организовать и представить исследовательский проект. 75 простых правил. – Москва : ГУ-ВШЭ : Инфра-М, 2001. – 203 с.
3. Панкратов В.Н. Искусство управлять собой: Практическое руководство. – Москва : Издательство института психотерапии, 2001. – 256 с.
4. ПОЛОЖЕНИЕ об организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. приказа РАНХиГС от 11.05.2016 г. № 01-2211)
5. ПОРЯДОК освоения в РАНХиГС факультативных и элективных дисциплин (модулей) образовательных программ высшего образования - программ бакалавриата, программ специалитета, программ магистратуры. Приложение к приказу от 26 июля 2016 г. № 02-417.

6.4. Нормативные правовые документы.

1. Федеральный закон от 29.12.2012 N 273-ФЗ (ред. от 13.07.2015) "Об образовании в Российской Федерации" (с изм. и доп.).
2. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки 38.03.05 Бизнес-информатика (квалификация (степень) «бакалавр»), утвержденный приказом Министерства образования и науки Российской Федерации от «11» августа 2016 г. № 1002.
3. Нормативно-методические документы Минобрнауки России.
4. Устав Федерального государственного бюджетного образовательного учреждения высшего профессионального образования «Российская академия народного хозяйства и государственной службы при Президенте РФ».
5. Конституция Российской Федерации. М., 1993.
6. Закон Российской Федерации “О безопасности” от 1992 г. № 2446-1, М., Российская газета, 6.05.92.
7. Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17.12.1997 г., в редакции Указа Президента РФ от 10.01.2000 № 24).
8. Доктрина информационной безопасности РФ. Указ Президента РФ от 9.09.2000 № 1895. Российская газета, 28 сентября 2000 года, стр.4-6.
9. Федеральная целевая программа “Электронная Россия”.
10. Закон Российской Федерации «О государственной тайне» № 5485. М., 1993.
11. Правила отнесения сведений, составляющих государственную тайну, к различным степеням секретности. - СЗ РФ, 1995, № 37, ст. 3619.
12. Сборник руководящих документов по защите информации от несанкционированного доступа. // ГТК при Президенте РФ. М., 1998.
13. Уголовный кодекс Российской Федерации. Принят 13 июня 1996 г., № 63-ФЗ. // Глава 19. Преступления против конституционных прав и свобод человека и гражданина. Глава 22. Преступления в сфере экономической деятельности. Глава 24. Преступления против общественной безопасности. Глава 25. Преступления против здоровья населения и общественной нравственности. Глава 28. Преступления в сфере компьютерной информации.
14. Указ Президента Российской Федерации от 8 ноября 1995 г. “О межведомственной комиссии по защите государственной тайны” № 1108. // СЗ РФ, 1995, № 46, ст. 4418.

15. Указ Президента Российской Федерации от 20 января 1996 г. “Вопросы межведомственной комиссии по защите государственной тайны». № 71. // СЗ РФ, 1996, № 4, ст. 268.
16. Указ Президента Российской Федерации от 30 ноября 1995 г. “Об утверждении перечня сведений, отнесенных к государственной тайне” № 1203. // СЗ РФ, 1995, № 49, ст. 4775.
17. 13. Федеральный закон “Об участии в международном информационном обмене” от 4 июля 1996 г. № 85-ФЗ.
18. Федеральный закон «Об электронной цифровой подписи» (ЭЦП) от 10 января 2002 года. // Федеральные законы. Выпуск 6. М., “ИНФРА-М”, 2002.
19. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ “Об информации, информационных технологиях и о защите информации”. // Российская газета от 29 июля 2006 г.
20. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ “О персональных данных”. // Российская газета от 29 июля 2006 г.
21. Государственные стандарты (ГОСТы):
22. ГОСТ 29339-92. Информационные технологии (ИТ). Защита информации от утечки за счет побочных электромагнитных излучений при ее обработке средствами вычислительной техники. Методы испытаний.
23. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.
24. ГОСТ Р. 51583-00. Защита информации (ЗИ). Порядок создания автоматизированных систем в защищенном исполнении. Общие положения.
25. ГОСТ Р. 51624-00. Защита информации (ЗИ). Автоматизированные системы в защищенном исполнении. Общие требования.
26. ГОСТ Р. 51275-99. Защита информации (ЗИ). Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
27. ГОСТ РВ. 50600-93. Защита секретной информации от технической разведки. Система документов. Общие положения.
28. ГОСТ Р. 50739-95. СВТ. Защита от несанкционированного доступа к информации.
29. ГОСТ Р. 50922-96. Защита информации (ЗИ). Основные термины и определения.
30. ГОСТ Р. 51188-98. Защита информации (ЗИ). Испытания программных средств на наличие компьютерных вирусов. Типовое руководство.

6.5. Интернет-ресурсы, справочные системы.

1. AnnualReviews [Электронный ресурс]. – URL: http://arjournals.annualreviews.org/.
2. EbscoHost [Электронный ресурс]. – URL: http://www.ebscohost.com/.
3. e-Library.ru [Электронный ресурс]: Научная электронная библиотека. – URL: http://elibrary.ru/.
4. Научная электронная библиотека «КиберЛенинка» [Электронный ресурс]. – URL: http://cyberleninka.ru//
5. ProQuest [Электронный ресурс]. – URL: http://search.proquest.com/index.
6. http://www.hr-training.net
7. http://www.lseptember.ru
8. http://www.tolerance.ru
9. Словари и энциклопедии на Академике [Электронный ресурс] // Академик. – URL: http://dic.academic.ru.
10. Университетская библиотека online [Электронный ресурс]. – URL: http://biblioclub.ru/.
11. Консультант Плюс http://www.consultant.ru/law/hotdocs/t7/

7. Материально-техническое и программное обеспечение дисциплины (модуля)

7.1. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для реализации данной дисциплины (модуля), необходимы специализированные компьютерные аудитории для проведения всех видов контактной и самостоятельной работы. Аудитории должны быть оборудованы компьютерами в соответствии с минимальными техническими требованиями. Количество рабочих мест обучаемых должно быть не менее количества студентов в учебной группе. При использовании виртуальных машин должен быть единый защищенный сетевой ресурс, на котором обучаемые смогут сохранять результаты своей работы. В обязательном порядке в аудитории должна присутствовать проекционная аппаратура, обеспечивающая как показ презентаций по теме занятий, так и демонстрацию работы преподавателя в среде разработки в реальном режиме времени. Оборудование класса должно обеспечивать выход преподавателя и обучаемых в глобальную сеть Интернет для выполнения учебных занятий. К обязательному программному обеспечению для поддержки образовательного процесса необходимо отнести: MS Excel

7.2. Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине (модулю)

При осуществлении образовательного процесса применяются информационные технологии, необходимые для подготовки презентационных материалов и материалов к занятиям (компьютеры с программным обеспечением для создания и показа презентаций, с доступом в сеть «Интернет», поисковые системы и справочные, профессиональные ресурсы в сети «Интернет»).

Содержание дисциплины размещено на сайте информационно-коммуникационной сети Интернет: ranepa.ru/.

7.3. Необходимое программное обеспечение

Для подготовки презентаций и их демонстрации необходима программа Impress из свободного пакета офисных приложений OpenOffice (или иной аналог с коммерческой или свободной лицензией).

Для контактной и самостоятельной работы используются мультимедийные комплексы, электронные учебники и учебные пособия, адаптированные к ограничениям здоровья обучающихся. Информационные средства обучения: электронные учебники, учебные фильмы по тематике дисциплины, презентации, интерактивные учебные и наглядные пособия, технические средства предъявления информации (многофункциональный мультимедийный комплекс) и контроля знаний (тестовые системы).