Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 15.04.2021 15:47:21
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adcec7e57befe1e2d4f7c72

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Первый проректор –
проректор по учебной работе
_____Н.Г. Кузнецов
«01» июня 2018г.

Рабочая программа дисциплины

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Организационное и правовое обеспечение информационной безопасности

по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Квалификация

Бакалавр

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	7 (4.1)		8 (4.2)		Итого	
Недель	17,3		7,8			
Вид занятий	УП	РПД	УП	РПД	УП	РПД
Лекции	36	36	24	24	60	60
Лабораторные	36	36	32	32	68	68
В том числе инт.	20	20	20	20	40	40
Итого ауд.	72	72	56	56	128	128
Контактная работа	72	72	56	56	128	128
Сам. работа	36	36	52	52	88	88
Часы на контроль			36	36	36	36
Итого	108	108	144	144	252	252

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 "Информационная безопасность" (уровень бакалавриата) (приказ Минобрнауки России от 01.12.2016г. №1515)

Рабочая программа составлена по профессионально-образовательной программе направление 10.03.01 "Информационная безопасность" профиль 10.03.01.02 "Организация и технология защиты информации"

Учебный план утвержден учёным советом вуза от 27.03.2018 протокол № 10.

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____ 11.05.18

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____ 11.05.18

Методическим советом направления: к.ф.м.н., декан, Карасев Денис Николаевич _____ 15.05.18

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. _____ 30.05.18

Проректором по учебно-методической работе Джуха В.М. _____ 31.05.18

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2019-2020 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2020-2021 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2021-2022 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

Визирование РПД для исполнения в очередном учебном году

Отдел образовательных программ и планирования учебного процесса Торопова Т.В. _____

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2022-2023 учебном году на заседании кафедры Информационные технологии и защита информации

Зав. кафедрой: д.э.н., профессор Тищенко Е.Н. _____

Программу составил(и): к.т.н., доцент, Серпенинов Олег Витальевич _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цели дисциплины:
1.2	приобретение обучаемыми знаний по организационному обеспечению защиты информации и формирование практических навыков работы в реальных конкретных условиях; раскрытие правовых основ защиты объектов информационных правоотношений в информационной сфере; правовую защиту государственной, коммерческой, служебной, профессиональной тайны, персональных данных; содержание, виды и условия применения правовых норм уголовной, гражданско-правовой, административной и дисциплинарной ответственности в области защиты информации.
1.3	Задачи дисциплины:
1.4	изучение теоретических, методологических и практических проблем формирования, функционирования и развития систем организационной защиты информации;изучение информационного законодательства Российской Федерации;изучение системы защиты государственной коммерческой, служебной, профессиональной и личной тайны;изучение правил лицензирования и сертификации в области защиты информации;изучение международного законодательства в области защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.Б.16
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Необходимыми условиями для успешного освоения дисциплины являются знания, умения и навыки, полученные в результате изучения дисциплин:
2.1.2	Основы управленческой деятельности
2.1.3	Техническая защита информации
2.1.4	Основы информационной безопасности
2.1.5	Системы защищенного электронного документооборота
2.1.6	Защита и обработка конфиденциальных документов
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Преддипломная практика
2.2.2	Итоговая государственная аттестация
2.2.3	Моделирование процессов и систем защиты информации
2.2.4	Подготовка к сдаче и сдача государственного экзамена

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ
ОК-4: способностью использовать основы правовых знаний в различных сферах деятельности
Знать:
- теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию; - цели, функции и процессы управления системами организационной защиты информации в организациях с различными формами собственности на базовом уровне
Уметь:
- анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития; - разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации на базовом уровне
Владеть:
методологией организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации на базовом уровне
ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности
Знать:
- основные направления и методы организационной защиты информации на базовом уровне
Уметь:
- организовывать работу с персоналом, обладающим конфиденциальной информацией; - организовывать охрану персонала, территорий, зданий, помещений и продукции организаций на базовом уровне
Владеть:
методологией организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации на базовом уровне

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
Знать:
-понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; - содержание основных понятий по правовому обеспечению информационной безопасности на базовом уровне
Уметь:
- организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней на базовом уровне
Владеть:
- методологией прведения анализа информационной безопасности объектов и систем на соответствие требованиям стандартов и нормативных документовФедеральной службой по техническому и экспортному контролю в области информационной безопасности на базовом уровне
ПСК-2.2: способностью формировать рекомендации по оптимизации функционального процесса объекта информатизации и разрабатывать комплекс организационно-технических мер по обеспечению информационной безопасности объекта защиты, с осуществлением его технико-экономического обоснования
Знать:
-правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности на базовом уровне
Уметь:
- организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации. -отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства на базовом уровне
Владеть:
- способностью по разработке комплекса организационно--технических мер по обеспечению информационной безопасности объекта защиты на базовом уровне
ПСК-2.4: способностью организовать контроль защищенности объекта информатизации в соответствии с нормативными документами
Знать:
-основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; -правила лицензирования и сертификации в области защиты информации на базовом уровне
Уметь:
-применять действующую законодательную базу в области защиты информации; -разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов на базовом уровне
Владеть:
-способностью организовать контроль защищенности объекта информатизации в соответствии с требованиями нормативных документов Федеральной службой по техническому и экспортному контролю на базовом уровне

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интер акт.	Примечание
	Раздел 1. Основные положения правовой и организационной защиты информации.						
1.1	"Правовое обеспечение информационной безопасности в системе национальной безопасности РФ":основные положения Стратегии национальной безопасности РФ и Доктрины информационной безопасности РФ. /Лек/	7	2	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
1.2	Основные направления обеспечения информационной безопасности и защиты информации в РФ. /Лаб/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
1.3	Основные направления обеспечения информационной безопасности и защиты информации в РФ. /Ср/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	

1.4	"Система защиты информации":роль и место организационной защиты информации в структуре системы защиты информации. /Лек/	7	2	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
1.5	Классификация информации по видам тайны и степеням конфиденциальности. /Лаб/	7	4	ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
1.6	Организация работы со с ведениями, отнесенных к государственной тайне и конфиденциальной информации. /Лаб/	7	4	ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
1.7	"Законодательно-правовые и организационные основы обеспечения информационной безопасности":характеристика основных законодательных и нормативно-правоых актов. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
1.8	"Структура законодательства РФ в области защиты информации":взаимосвязь нормативно-правовых актов и особенность их применения в области информационной безопасности. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
1.9	Структура законодательства и нормативно-методических документов в области защиты информации. /Ср/	7	5	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
1.10	"Политика безопасности предприятия": политика безопасности предприятия как основа организационного управления защитой информации. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
1.11	Разработка политики безопасности предприятия. /Лаб/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	2	
1.12	Формирование политики безопасности предприятия. Организационное управление защитой информации. /Ср/	7	6	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
1.13	"Структура организационной защиты информации": основные элементы системы защиты информации и их характеристика. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
	Раздел 2. Правовой режим защиты государственной тайны.						
2.1	"Информация как объект правового регулирования":правовые основы использования конфиденциальной информации. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	

2.2	"Источники конфиденциальной информации":организационные каналы утечки конфиденциальной информации. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
2.3	"Принципы, механизм и процедура отнесения сведений к государственной тайне":рассмотрение основных принципов, механизмов и процедуры отнесения сведений к государственной тайне. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
2.4	"Государственная тайна как особый вид защищаемой нформации": отличительные особенности организации защиты сведений, составляющих государственную тайну, от других сведений конфиденциального характера. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
2.5	Оформление основных форм документов на допуск к сведениям, составляющих государственную тайну. /Лаб/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
2.6	Принципы, механизм и процедура отнесения сведений к государственной тайне. /Ср/	7	3	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
2.7	Порядок оформления основных форм документов на допуск к сведениям, составляющих государственную тайну. /Ср/	7	5	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
2.8	"Порядок засекречивания сведений, документов и продукции":основные требования при организации засекречивания сведений, документов и продукции. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
2.9	"Порядок рассекречивания сведений, документов и продукции":основные требования при организации рассекречивания сведений, документов и продукции. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
2.10	"Система контроля за состоянием защиты государственной тайны": организация контроля за состоянием защиты государственной тайны; органы защиты государственной тайны и их полномочия /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
2.11	Подготовка и проведение специальной экспертизы предприятия /Лаб/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
2.12	Государственная аттестация руководителей предприятий. /Лаб/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	

2.13	Подготовка и проведение специальной экспертизы предприятия. /Ср/	7	5	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
2.14	"Юридическая ответственность за нарушения правового режима защиты государственной тайны":основные положения Кодекса об административных нарушениях и Уголовного кодекса об юридической ответственности за нарушение режима защиты государственной тайны. /Лек/	7	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
	Раздел 3. Лицензирование и сертификация в области защиты информации						
3.1	"Структура системы государственного лицензирования":основные элементы и ситемы государственного лицензирования и их характеритика. /Лек/	7	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
3.2	"Лицензирование в области защиты информации":основные требования при осуществлении деятельности в области защиты информации и порядок организации лицензирования. /Лек/	7	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
3.3	Оформление запроса на лицензирование по видам деятельности. /Лаб/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
3.4	"Структура системы сертификации в области защиты информации": основные требования при сертификации средств защиты информации и порядок организации сертификации. /Лек/	7	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
3.5	Лицензирование и сертификация в области защиты информации. /Ср/	7	4	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Л3.2 Э1	0	
3.6	"Проведение аттестации объектов информатизации":основные требования и характеристика основных этапов проведения аттестации объектов информатизации. /Лек/	7	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
3.7	Проведения аттестации объектов информатизации и оформление ее результатов. /Лаб/	7	4	ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
3.8	Организация проведения аттестации объектов информатизации и оформления ее результатов. /Ср/	7	6	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
3.9	/Зачёт/	7	0	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	

	Раздел 4. Допуск и доступ к конфиденциальной информации						
4.1	"Основные требования, предъявляемые к организации защиты конфиденциальной информации": обоснование и характеристика основных требований к организации защиты конфиденциальной информации. /Лек/	8	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.2	"Основы защиты конфиденциальной информации":основные принципы организации защиты конфиденциальной информации. /Лек/	8	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.3	Задачи режима защиты информации. /Лаб/	8	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.4	Реализация режимных мер в ходе подготовки и проведения закрытых совещаний и переговоров. /Лаб/	8	4	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.5	Основные требования, предъявляемые к организации защиты конфиденциальной информации. /Ср/	8	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	
4.6	"Правовое обеспечение защиты коммерческой тайны":сведения,составляющие коммерческую тайну;требования к обеспечению защиты коммерческой тайны. /Лек/	8	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.7	Особенности доступа и обязанности персонала, допущенного к конфиденциальной информации. /Лаб/	8	4	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.8	"Организация и принципы допускной работы":особенности организации допускной работы на предприятии. /Лек/	8	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.9	Подбор персонала на должности, связанные с работой с конфиденциальной информацией. /Ср/	8	8	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.10	Оформление документов при подборе и приеме на должности, связанные с доступом к конфиденциальной информации. /Ср/	8	6	ОК-4 ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.11	"Порядок выдачи справок о форме допуска, учет и уничтожение":организация работы по учету и уничтожению допусков; порядок выдачи справок о форме допуска. /Лек/	8	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	

4.12	"Оформление и переоформление допусков": виды допусков; особенности оформления и переоформления допусков. /Лек/	8	2	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.13	Оформление документов при подборе и приеме на должности, связанные с доступом к конфиденциальной информации. /Лаб/	8	4	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	2	
4.14	"Организация работы по допуску персонала к конфиденциальной информации":учет, хранение и порядок уничтожения допусков, справок о допуске и контракта об оформлении допуска к государственной тайне /Лек/	8	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.15	Учет, хранение и порядок уничтожения допусков, справок о допуске и контракта об оформлении допуска к государственной тайне Учет, хранение и порядок уничтожения допусков, справок о допуске и контракта об оформлении допуска к государственной тайне /Ср/	8	8	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.16	"Рассекречивание конфиденциальных сведений, документов и продукции": основные требования при организации рассекречивания конфиденциальных сведений, документов и продукции. /Лек/	8	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.17	"Персонал организации как источник утечки конфиденциальной информации":характеристика основных путей разглашения конфиденциальной информации персоналом организации. /Лек/	8	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.18	Организация контроля за соблюдением персоналом требований защиты информации. /Лаб/	8	4	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.19	Организация контроля за соблюдением персоналом требований защиты информации. /Ср/	8	6	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.20	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. /Лаб/	8	4	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	2	
4.21	Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. /Ср/	8	8	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	

4.22	"Подбор персонала на должности, связанные с работой с конфиденциальной информацией": основные требования при подборе персонала, связанных с работой с конфиденциальной информацией. /Лек/	8	2	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.23	Основные формы обучения и методы контроля знаний персонала по защите информации. /Лаб/	8	4	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.24	Основные формы обучения и методы контроля знаний персонала по защите информации. /Ср/	8	4	ОК-4 ОПК-5	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	0	
4.25	"Цели и задачи пропускного режима":харктеристика целей изадач организации пропускного режима. /Лек/	8	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.26	Оборудование и организация работы контрольно-пропускных пунктов. /Лаб/	8	4	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	1	
4.27	Оборудование и организация работы контрольно-пропускных пунктов. /Ср/	8	8	ОПК-5 ПК-10 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Л3.2 Э1	0	
4.28	"Виды,порядок оформления и выдачи пропусков": виды пропусков, порядок их оформления и вывдачи. /Лек/	8	2	ОК-4 ОПК-5 ПК-10	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.1 Э1	1	
4.29	ЭКЗАМЕН /Экзамен/	8	36	ОК-4 ОПК-5 ПК-10 ПСК-2.2 ПСК-2.4	Л1.1 Л1.2 Л1.3 Л2.1 Л2.2 Л2.3 Л3.2 Л3.1 Э1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачету:

1.Угрозы безопасности информации.

2.Система защиты информации.

3.Законодательно – правовые и организационные основы обеспечения защиты информации.

4.Организация защиты информации на предприятии.

5.Политика безопасности предприятия.

6.Структура системы государственного лицензирования.

7.Порядок проведения лицензирования.

8.Основные лицензионные требования и условия.

9.Порядок проведения аттестации и контроля объектов информатизации.

10. Объекты защиты.

11.Структура системы сертификации.

12.Перечень видов деятельности в области защиты информации, подлежащих лицензированию.

13.Государственная аттестация руководителей предприятий.

14. Организационные и технические способы защиты государственной тайны.

15.Организационное управление защитой информации.

16.Перечень сведений конфиденциального характера.

17.Мероприятия по защите конфиденциальной информации.

18.Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.

19.Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.

20.Порядок засекречивания сведений и их носителей.

21.Порядок рассекречивания сведений и их носителей.

22.Распоряжение сведениями, составляющими ГТ.

23.Органы защиты ГТ.

24.Порядок допуска к ГТ.

25.Контроль за обеспечением защиты государственной тайны.

26.Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.

27.Организация допуска должностных лиц и граждан к государственной тайне.

28.Информация как объект правового регулирования.

29.Виды информации, защищаемой законодательством РФ.

30.Государственная тайна как особый вид защищаемой информации.

31.Система защиты государственной тайны.

Вопросы к экзамену:
1) Угрозы безопасности информации.
2) Система защиты информации.
3) Законодательно - правовые и организационные основы обеспечения защиты информации.
4) Организация защиты информации на предприятии.
5) Политика безопасности предприятия.
6) Структура системы государственного лицензирования.
7) Порядок проведения лицензирования.
8) Основные лицензионные требования и условия.
9) Порядок проведения аттестации и контроля объектов информатизации.
10) Объекты защиты.
11) Структура системы сертификации.
12) Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
13) Государственная аттестация руководителей предприятий.
14) Организационные и технические способы защиты государственной тайны.
15) Организационное управление защитой информации.
16) Перечень сведений конфиденциального характера.
17) Мероприятия по защите конфиденциальной информации.
18) Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.
19) Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.
20) Порядок засекречивания сведений и их носителей.

22) Распоряжение сведениями, составляющими ГТ.
23) Органы защиты ГТ.
24) Порядок допуска к ГТ.
25) Контроль за обеспечением защиты государственной тайны.
26) Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.
27) Организация допуска должностных лиц и граждан к государственной тайне.
28) Информация как объект правового регулирования.
29) Виды информации, защищаемой законодательством РФ.
30) Государственная тайна как особый вид защищаемой информации.
31) Система защиты государственной тайны.
32) Организационное управление защитой информации. (Принципы ИБ предприятия. Направления (методическое, организационной, техническое) и этапы по созданию комплексной системы безопасности. Уровни ПБ предприятия.)
33) Структура организационной защиты информации. (Объекты защиты. Структура организации защиты информации (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты информации.)
34) Организация и порядок проведения специальных экспертиз предприятий.
35) Порядок оформления запроса на лицензирование по видам деятельности.
36) Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).
37) Информация, которая не подлежит засекречиванию.
38) Обеспечение сохранности документов, дел и изданий.
39) Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
40) Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
41) Обязанности персонала организации по сохранению коммерческой тайны.
42) Состав и структура системы безопасности предприятия.
43) Правовые основы деятельности службы безопасности.
44) Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
45) Организация информационно - аналитической работы.
46) Организация охраны предприятий.
47) Основные задачи организации режима и охраны.
48) Организация пропускного режима.
49) Пропускные документы.
50) Требования внутриобъектового режима.
51) Основные документы, разрабатываемые на охраняемых объектах.
52) Организация информационной безопасности и защиты информации.
53) Оценка и управление рисками. Экономическая оценка систем и средств защиты.

5.2. Фонд оценочных средств для проведения текущего контроля

Структура и содержание фонда оценочных средств представлены в Приложении 1 к рабочей программе дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Тищенко Е. Н.	Основы информационной безопасности: учеб.- метод. разраб.	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2012	10
Л1.2	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: учеб. пособие	М.: РИО□, 2014	11
Л1.3	Аверченков В. И.	Аудит информационной безопасности: учебное пособие для вузов	Москва: Издательство «Флинта», 2016	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Тищенко Е. Н.	Проблемы информационной безопасности: материалы V Всерос. науч. конф. 19-20 мая 2016 г.	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2016	3
Л2.2	Серпенинов О. В., Тишин В. Р.	Правовая защита информации. Словарь-глоссарий терминов в области защиты информации и информационной безопасности: для студентов спец. 090103 "Орг. и технологии защиты информ."	Ростов н/Д: Изд-во РГЭУ "РИНХ", 2010	10

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.3	Кришталюк А. Н.	Правовые аспекты системы безопасности: курс лекций	Орел: МАБИВ, 2014	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Тищенко Е. Н.	Инструментальные методы анализа потребительского качества защищенных информационных систем: учеб. пособие	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2016	68
Л3.2	Смирнов В. И.	Защита информации: лабораторный практикум	Йошкар-Ола: ПГТУ, 2017	http://biblioclub.ru/ - неограниченный доступ для зарегистрированных пользователей
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	ФСТЭК России/fstec.ru			
6.3. Перечень программного обеспечения				
6.3.1	Microsoft Office			
6.3.2	Анализатор уязвимостей XSpider			
6.3.3	Анализатор уязвимостей MaxPatrol			
6.3.4	Межсетевой экран PFSense			
6.3.5	Удостоверяющий центр VipNet			
6.4 Перечень информационных справочных систем				
6.4.1	Consultant Plus			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения. Для проведения лекционных занятий используется демонстрационное оборудование. Лабораторные занятия проводятся в компьютерных классах, рабочие места в которых оборудованы необходимыми лицензионными программными средствами и выходом в Интернет.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)
Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры Информационные
технологии и защита информации
Протокол № 10 от «11» мая 2018 г.
Зав. кафедрой _____ Тищенко Е.Н.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Организационное и правовое обеспечение информационной безопасности

Направление подготовки
10.03.01 Информационная безопасность

Профиль
10.03.01.02 Организация и технология защиты информации

Уровень образования
Бакалавриат

Составитель _____ Серпенинов О.В. доцент к.т.н. доцент
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону, 2018

Оглавление

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Перечень компетенций с указанием этапов их формирования представлен в п. 3. «Требования к результатам освоения дисциплины» рабочей программы дисциплины.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

2.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОК-4 способностью использовать основы правовых знаний в различных сферах деятельности			
З. - теоретические основы функционирования систем организационной защиты информации, ее современные проблемы и терминологию; - цели, функции и процессы управления системами организационной защиты информации в организациях с различными формами собственности;	Угрозы безопасности информации. Система защиты информации. Законодательно - правовые и организационные основы обеспечения защиты информации.	полнота и содержательность ответа умение приводить примеры	О
У. - анализировать эффективность систем организационной защиты информации и разрабатывать направления ее развития; - разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации;	Организация защиты информации на предприятии. Политика безопасности предприятия. Структура системы государственного лицензирования.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. методологией организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации	Порядок проведения лицензирования. Основные лицензионные требования и условия. Порядок проведения аттестации и контроля объектов информатизации.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
ОПК-5 способностью использовать нормативные правовые акты в профессиональной деятельности			
З. - основные направления и методы организационной защиты информации.	Объекты защиты. Структура системы сертификации. Перечень видов	полнота и содержательность ответа умение приводить примеры	О

	деятельности в области защиты информации, подлежащих лицензированию.		
У. - организовывать работу с персоналом, обладающим конфиденциальной информацией; - организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;	Государственная аттестация руководителей предприятий. Организационные и технические способы защиты государственной тайны. Организационное управление защитой информации.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. методологией организации технологического процесса защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации	Перечень сведений конфиденциального характера. Мероприятия по защите конфиденциальной информации. Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
ПК-10 способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности			
З. -понятие и виды защищаемой информации, особенности государственной тайны как вида защищаемой информации; - содержание основных понятий по правовому обеспечению информационной безопасности;	Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ. Порядок засекречивания сведений и их носителей. Порядок рассекречивания сведений и их носителей.	полнота и содержательность ответа умение приводить примеры	О
У. - организовывать и проводить служебное расследование по фактам разглашения, утечки информации и несанкционированного доступа к ней;	Распоряжение сведениями, составляющими ГТ. Органы защиты ГТ. Порядок допуска к ГТ.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. Федеральной службой по техническому и экспортному контролю.	Контроль за обеспечением защиты государственной тайны. Правила отнесения сведений, составляющих ГТ, к различным степеням секретности. Организация допуска должностных лиц и граждан к государственной тайне.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
ПСК-2.2 способностью формировать рекомендации по оптимизации функционального процесса объекта информатизации и разрабатывать комплекс организационно-технических мер по обеспечению информационной			

безопасности объекта защиты, с осуществлением его технико-экономического обоснования			
З. -правовые способы защиты государственной тайны, конфиденциальной информации и интеллектуальной собственности;	Информация как объект правового регулирования. Виды информации, защищаемой законодательством РФ. Государственная тайна как особый вид защищаемой информации.	полнота и содержательность ответа умение приводить примеры	О
У. - организовывать и проводить аналитическую работу по предупреждению утечки конфиденциальной информации. -отыскивать необходимые нормативные правовые акты и информационно-правовые нормы в системе действующего законодательства;	Система защиты государственной тайны. Организационное управление защитой информации. (Принципы ИБ предприятия. Направления (методическое, организационной, техническое) и этапы по созданию комплексной системы безопасности. Уровни ПБ предприятия.) Структура организационной защиты информации. (Объекты защиты. Структура организации защиты информации (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты информации.)	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
В. Федеральной службой по техническому и экспортному контролю.	Организация и порядок проведения специальных экспертиз предприятий. Порядок оформления запроса на лицензирование по видам деятельности. Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР
ПСК-2.4 способностью организовать контроль защищенности объекта информатизации в соответствии с нормативными документами			
З. -основы правового регулирования взаимоотношений администрации и персонала в области защиты информации; -правила лицензирования и сертификации в области защиты информации.	Информация, которая не подлежит засекречиванию. Обеспечение сохранности документов, дел и изданий. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.	полнота и содержательность ответа умение приводить примеры	О
У. -применять действующую законодательную базу в области защиты информации; -разрабатывать проекты	Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну. Обязанности персонала	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение	О, ЛР

нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов.	организации по сохранению коммерческой тайны. Состав и структура системы безопасности предприятия.	поставленных задач	
В. Федеральной службой по техническому и экспортному контролю.	Правовые основы деятельности службы безопасности. Организационное обеспечение информационной безопасности при проведении закрытых мероприятий. Организация информационно - аналитической работы.	полнота и содержательность ответа умение приводить примеры умение самостоятельно находить решение поставленных задач	О, ЛР

О – опрос, ЛР- лабораторная работа

2.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале.

- 84-100 баллов (оценка «отлично») - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка удовлетворительно) - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка неудовлетворительно) - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

В разделе приводятся типовые варианты оценочных средств: вопросы к зачету, вопросы к экзамену, задания для опроса, лабораторные работы, экзаменационный билет.

Вопросы к зачету
по дисциплине «Организационное и правовое обеспечение информационной безопасности»

1.Угрозы безопасности информации.
2.Система защиты информации.
3.Законодательно – правовые и организационные основы обеспечения защиты информации.
4.Организация защиты информации на предприятии.
5.Политика безопасности предприятия.
6.Структура системы государственного лицензирования.
7.Порядок проведения лицензирования.
8.Основные лицензионные требования и условия.
9.Порядок проведения аттестации и контроля объектов информатизации.
10. Объекты защиты.
11.Структура системы сертификации.
12.Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
13.Государственная аттестация руководителей предприятий.
14. Организационные и технические способы защиты государственной тайны.
15.Организационное управление защитой информации.
16.Перечень сведений конфиденциального характера.
17.Мероприятия по защите конфиденциальной информации.
18.Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.
19.Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.
20.Порядок засекречивания сведений и их носителей.
21.Порядок рассекречивания сведений и их носителей.
22.Распоряжение сведениями, составляющими ГТ.
23.Органы защиты ГТ.
24.Порядок допуска к ГТ.
25.Контроль за обеспечением защиты государственной тайны.
26.Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.
27.Организация допуска должностных лиц и граждан к государственной тайне.
28.Информация как объект правового регулирования.
29.Виды информации, защищаемой законодательством РФ.
30.Государственная тайна как особый вид защищаемой информации.
31.Система защиты государственной тайны.

Вопросы к экзамену
по дисциплине «Организационное и правовое обеспечение информационной безопасности»

1) Угрозы безопасности информации.
2) Система защиты информации.
3) Законодательно - правовые и организационные основы обеспечения защиты информации.
4) Организация защиты информации на предприятии.
5) Политика безопасности предприятия.
6) Структура системы государственного лицензирования.
7) Порядок проведения лицензирования.
8) Основные лицензионные требования и условия.

9) Порядок проведения аттестации и контроля объектов информатизации.
10) Объекты защиты.
11) Структура системы сертификации.
12) Перечень видов деятельности в области защиты информации, подлежащих лицензированию.
13) Государственная аттестация руководителей предприятий.
14) Организационные и технические способы защиты государственной тайны.
15) Организационное управление защитой информации.
16) Перечень сведений конфиденциального характера.
17) Мероприятия по защите конфиденциальной информации.
18) Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.
19) Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.
20) Порядок засекречивания сведений и их носителей.
21) Порядок рассекречивания сведений и их носителей.
22) Распоряжение сведениями, составляющими ГТ.
23) Органы защиты ГТ.
24) Порядок допуска к ГТ.
25) Контроль за обеспечением защиты государственной тайны.
26) Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.
27) Организация допуска должностных лиц и граждан к государственной тайне.
28) Информация как объект правового регулирования.
29) Виды информации, защищаемой законодательством РФ.
30) Государственная тайна как особый вид защищаемой информации.
31) Система защиты государственной тайны.
32) Организационное управление защитой информации. (Принципы ИБ предприятия. Направления (методическое, организационной, техническое) и этапы по созданию комплексной системы безопасности. Уровни ПБ предприятия.)
33) Структура организационной защиты информации. (Объекты защиты. Структура организации защиты информации (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты информации.)
34) Организация и порядок проведения специальных экспертиз предприятий.
35) Порядок оформления запроса на лицензирование по видам деятельности.
36) Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).
37) Информация, которая не подлежит засекречиванию.
38) Обеспечение сохранности документов, дел и изданий.
39) Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
40) Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
41) Обязанности персонала организации по сохранению коммерческой тайны.
42) Состав и структура системы безопасности предприятия.
43) Правовые основы деятельности службы безопасности.
44) Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
45) Организация информационно - аналитической работы.
46) Организация охраны предприятий.
47) Основные задачи организации режима и охраны.
48) Организация пропускного режима.
49) Пропускные документы.
50) Требования внутриобъектового режима.
51) Основные документы, разрабатываемые на охраняемых объектах.
52) Организация информационной безопасности и защиты информации.

53) Оценка и управление рисками. Экономическая оценка систем и средств защиты.

Критерии оценивания:

- оценка «отлично» - изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

оценка «хорошо» - наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- оценка удовлетворительно - наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- оценка неудовлетворительно - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы».

Задания для опроса
по дисциплине Организационное и правовое обеспечение информационной безопасности

Вариант 1
Угрозы безопасности информации.
Система защиты информации.
Законодательно - правовые и организационные основы обеспечения защиты информации.

Вариант 2
Организация защиты информации на предприятии.
Политика безопасности предприятия.
Структура системы государственного лицензирования.

Вариант 3
Порядок проведения лицензирования.
Основные лицензионные требования и условия.
Порядок проведения аттестации и контроля объектов информатизации.

Вариант 4
Объекты защиты.
Структура системы сертификации.
Перечень видов деятельности в области защиты информации, подлежащих лицензированию.

Вариант 5
Государственная аттестация руководителей предприятий.
Организационные и технические способы защиты государственной тайны.
Организационное управление защитой информации.

Вариант 6
Перечень сведений конфиденциального характера.
Мероприятия по защите конфиденциальной информации.
Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.

Вариант 7
Перечень сведений, составляющих ГТ. Отнесение сведений к ГТ.
Порядок засекречивания сведений и их носителей.
Порядок рассекречивания сведений и их носителей.

Вариант 8
Распоряжение сведениями, составляющими ГТ.
Органы защиты ГТ.
Порядок допуска к ГТ.

Вариант 9
Контроль за обеспечением защиты государственной тайны.
Правила отнесения сведений, составляющих ГТ, к различным степеням секретности.
Организация допуска должностных лиц и граждан к государственной тайне.

Вариант 10
Информация как объект правового регулирования.
Виды информации, защищаемой законодательством РФ.
Государственная тайна как особый вид защищаемой информации.

Вариант 11
Система защиты государственной тайны.
Организационное управление защитой информации. (Принципы ИБ предприятия. Направления (методическое, организационной, техническое) и этапы по созданию комплексной системы безопасности. Уровни ПБ предприятия.)
Структура организационной защиты информации. (Объекты защиты. Структура организации защиты информации (СЗИ; мероприятия по ЗИ; мероприятия по контролю эффективности защиты информации.)

Вариант 12
Организация и порядок проведения специальных экспертиз предприятий.
Порядок оформления запроса на лицензирование по видам деятельности.
Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).

Вариант 13
Информация, которая не подлежит засекречиванию.
Обеспечение сохранности документов, дел и изданий.
Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.

Вариант 14
Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
Обязанности персонала организации по сохранению коммерческой тайны.
Состав и структура системы безопасности предприятия.

Вариант 15
Правовые основы деятельности службы безопасности.
Организационное обеспечение информационной безопасности при проведении закрытых мероприятий.
Организация информационно - аналитической работы.

Вариант 16
Организация охраны предприятий.
Основные задачи организации режима и охраны.
Организация пропускного режима.

Вариант 17
Пропускные документы.
Требования внутриобъектового режима.
Основные документы, разрабатываемые на охраняемых объектах.

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Кафедра Информационные технологии и защита информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине Организационное и правовое обеспечение информационной безопасности

1) Угрозы безопасности информации.
2) Законодательство РФ о ГТ. Полномочия органов государственной власти и должностных лиц.
3) Порядок отнесения сведений к коммерческой тайне. (Закон о КТ).

Составитель _____ Серпенинов О.В.

Заведующий кафедрой ИТ и ЗИ_____ Тищенко Е.Н.

«____» _____ 20____ г.

Критерии оценивания:
- 84-100 баллов (оценка «отлично») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии

с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;

- 67-83 баллов (оценка «хорошо») – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка удовлетворительно) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка неудовлетворительно) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

Лабораторные работы
по дисциплине «Организационное и правовое обеспечение информационной безопасности»

Лабораторная работа №1
Основные направления обеспечения информационной безопасности и защиты информации в РФ.

Лабораторная работа №2
Классификация информации по видам тайны и степеням конфиденциальности.

Лабораторная работа №3
Организация работы со с ведениями, отнесенных к государственной тайне и конфиденциальной информации

Лабораторная работа №4
Оформление основных форм документов на допуск к сведениям, составляющих государственную тайну

Лабораторная работа №5
Подготовка и проведение специальной экспертизы предприятия

Лабораторная работа №6
Государственная аттестация руководителей предприятий.

Лабораторная работа №7
Разработка политики безопасности предприятия

Лабораторная работа №8
Оформление запроса на лицензирование по видам деятельности

Лабораторная работа №9
Проведения аттестации объектов информатизации и оформление ее результатов.

Лабораторная работа №10
Оформление документов при подборе и приеме на должности, связанные с доступом к конфиденциальной информации

Лабораторная работа №11
Особенности доступа и обязанности персонала, допущенного к конфиденциальной информации.

Лабораторная работа №12
Основные формы обучения и методы контроля знаний персонала по защите информации.

Лабораторная работа №13
Организация контроля за соблюдением персоналом требований защиты информации.

Лабораторная работа №14
Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации.

Лабораторная работа №15
Задачи режима защиты информации.

Лабораторная работа №16
Оборудование и организация работы контрольно-пропускных пунктов.

Лабораторная работа №17
Реализация режимных мер в ходе подготовки и проведения закрытых совещаний и переговоров

1 . Методические рекомендации по выполнению лабораторных работ

Лабораторные работы выполняются с учетом приобретенных знаний по предшествующим дисциплинам, теоретического материала дисциплины, с помощью и консультациями (при необходимости) преподавателя на занятиях.

2. Критерии оценки:

- 84-100 баллов (оценка «отлично») – изложенный материал фактически верен, наличие глубоких исчерпывающих знаний в объеме пройденной программы дисциплины в соответствии с поставленными программой курса целями и задачами обучения; правильные, уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- 67-83 баллов (оценка «хорошо») – наличие твердых и достаточно полных знаний в объеме пройденной программы дисциплины в соответствии с целями обучения, правильные действия по применению знаний на практике, четкое изложение материала, допускаются отдельные логические и стилистические погрешности, обучающийся усвоил основную литературу, рекомендованную в рабочей программе дисциплины;

- 50-66 баллов (оценка удовлетворительно) – наличие твердых знаний в объеме пройденного курса в соответствии с целями обучения, изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов; правильные в целом действия по применению знаний на практике;

- 0-49 баллов (оценка неудовлетворительно) – ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

4. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета и экзамена.

Экзамен проводится по расписанию экзаменационной сессии в устном виде. Количество вопросов в экзаменационном задании – 3. Объявление результатов производится в день экзамена. Результаты аттестации заносятся в экзаменационную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2
к рабочей программе

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ростовский государственный экономический университет (РИНХ)»

Рассмотрено и одобрено
на заседании кафедры Информационные технологии и
защита информации
Протокол № 10 от «11» мая 2018 г.
Зав. кафедрой Тищенко Е.Н.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Организационное и правовое обеспечение информационной безопасности

Направление подготовки

10.03.01 Информационная безопасность

Профиль

10.03.01.02 Организация и технология защиты информации

Уровень образования

Бакалавриат

Составитель Серпенинов О.В., доцент, к.т.н., доцент
(подпись) Ф.И.О., должность, ученая степень, ученое звание

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Организационное и правовое обеспечение информационной безопасности» адресованы студентам всех форм обучения.

Учебным планом по направлению подготовки 10.03.01 «Информационная безопасность предусмотрены следующие виды занятий:

лекционные

лабораторные

В ходе лекционных занятий рассматриваются основные теоретические вопросы, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

При подготовке к лабораторным занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме;

– письменно решить домашнее задание, рекомендованные преподавателем при изучении каждой темы.

По согласованию с преподавателем студент может подготовить реферат, доклад или сообщение по теме занятия. В процессе подготовки к лабораторным занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на аудиторных занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса или контрольной работы. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящим лабораторным занятиям по всем, обозначенным в рабочей программе дисциплины вопросам.

При реализации различных видов учебной работы используются разнообразные (в т.ч. интерактивные) методы обучения, в частности:

- интерактивная доска для подготовки и проведения лекционных занятий;

- размещение материалов курса в системе дистанционного обучения http://do.rsue.ru.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронной библиотекой ВУЗа http://library.rsue.ru/. Также обучающиеся могут взять на дом необходимую литературу на абонементе вузовской библиотеки или воспользоваться читальными залами вуза.