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

СЕВЕРО-ЗАПАДНЫЙ ИНСТИТУТ УПРАВЛЕНИЯ-филиал РАНХИГС

ФАКУЛЬТЕТ БЕЗОПАСНОСТИ И ТАМОЖНИ
Кафедра безопасности

УТВЕРЖДЕНО

Директор Северо-Западного института управления – филиала РАНХиГС
Хлутков А.Д.

ПРОГРАММА СПЕЦИАЛИТЕТА

Государственно-правовая
(*специализация)*

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ,
реализуемой без применения электронного (онлайн) курса

Б1.В.03.05 «Правовое обеспечение информационной безопасности»

40.05.01. Правовое обеспечение национальной безопасности
по специальности

очная, заочная
форма(ы) обучения

Год набора - 2022 г.

Санкт-Петербург, 2022

Автор–составитель:
к.э.н., доцент С.Е. Елкин

Заведующий кафедрой безопасности
к.э.н., доцент Т.Н. Тарасова

РПД одобрена на заседании кафедры. Протокол от 30.08.2022 № 1

СОДЕРЖАНИЕ

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

1.1. Дисциплина Б1.В.03.05. «Правовое обеспечение информационной безопасности» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКр ОС-1	Способность обеспечивать безопасность личности, общества, государства правовыми средствами	ПКр ОС-1.2	Принимает правовые меры по нейтрализации угроз безопасности личности, общества, государства

2. Объем и место дисциплины в структуре образовательной программы

Объем дисциплины

Общая трудоемкость дисциплины (очная/заочная) составляет 3 зачетных единицы, 108 академических часа.

Для очной формы обучения трудоемкость контактной работы с преподавателем составляет 48 академических часа (из них 24 часов – лекции, 24 часов – практические занятия), самостоятельной работы – 60 академических часа.

Для заочной формы обучения трудоемкость контактной работы с преподавателем составляет 12 академических часа (из них 4 часов – лекции, 8 часов – практические занятия), самостоятельной работы – 92 академических часа, контроль – 4 часа.

Место дисциплины в структуре образовательной программы

Дисциплина Б1.В.03.05. «Правовое обеспечение информационной безопасности» включена в состав дисциплин по выбору учебного плана подготовки специалистов по специальности 45.05.01 «Правовое обеспечение национальной безопасности».

Дисциплина относится к блоку 1 (Б1), (Б1.В).

Дисциплина для очной формы обучения изучается на 4 курсе в 7 семестре.

Дисциплина для заочной формы обучения изучается на 4 курсе в 7 семестре.

Форма промежуточной аттестации в соответствии с учебным планом: зачет.

Доступ к системе дистанционных образовательных технологий осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://lms.ranepa.ru/. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

3. Содержание и структура дисциплины

Очная форма обучения

№ п/п	Наименование тем и/или разделов	Объем дисциплины (модуля), час.						Форма текущего контроля успеваемости, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л/ЭО ДОТ	ЛР/ЭО ДОТ	ПЗ/ЭО ДОТ	КСР/ЭО ДОТ		
Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению	9	2		2		5	*О*

Тема 2	Нормативно-правовая база обеспечения ИБ в России	9	2		2		5	*О*
Тема 3	Информация как объект правового регулирования и защиты	9	2		2		5	*О, Т*
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус	9	2		2		5	*О, Т*
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика	9	2		2		5	*О*
Тема 6	Правовая защита личности в информационной сфере	9	2		2		5	*О*
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению	9	2		2		5	*О*
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий	9	2		2		5	*О*
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС)	9	2		2		5	*О*
Тема 10	Правовая защита коммерческой тайны (КТ)	9	2		2		5	*О*
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации	9	2		2		5	*О*
Тема 12	Предупреждение преступлений в информационной сфере в современной России	2	-		2		-	*О*
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ	7	2		-		5	*О*
	Промежуточная аттестация	**-**						**Зачет**
	Всего:	**108**	**24**	**-**	**24**	**-**	**60**	

О – опрос; Т – тестирование

Заочная форма обучения

№ п/п	**Наименование тем и/или разделов**	**Объем дисциплины (модуля), час.**					**Форма текущего контроля успеваемости, промежуточной аттестации**
		Всего	**Контактная работа обучающихся с преподавателем по видам учебных занятий**			**СР**	
			Л/ЭО ДОТ	**ЛР/ЭО ДОТ**	**ПЗ/ЭО ДОТ**	**КСР/ЭО ДОТ**	

Тема 1	Информационная безопасность (ИБ) РФ и задачи по ее обеспечению	9	1		1		7	*О*
Тема 2	Нормативно-правовая база обеспечения ИБ в России	9	1		1		7	*О*
Тема 3	Информация как объект правового регулирования и защиты	9	1		1		7	*О, Т*
Тема 4	Система субъектов обеспечения ИБ в России и их правовой статус	9	1		1		7	*О, Т*
Тема 5	Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика	8			1		7	*О*
Тема 6	Правовая защита личности в информационной сфере	8			1		7	*О*
Тема 7	Правовой режим государственной тайны и меры по ее обеспечению	8			1		7	*О*
Тема 8	Правовые и организационные способы защиты информации в сфере высоких технологий	8			1		7	*О*
Тема 9	Правовое обеспечение права интеллектуальной собственности (ПИС)	7					7	*О*
Тема 10	Правовая защита коммерческой тайны (КТ)	7					7	*О*
Тема 11	Правовое регулирование отношений в сфере лицензирования и сертификации	7					7	*О*
Тема 12	Предупреждение преступлений в информационной сфере в современной России	7					7	*О*
Тема 13	Юридическая ответственность за правонарушения в сфере ИБ	8					8	*О*
	Промежуточная аттестация	**4**						**Зачет**
	Всего:	**108**	**4**	**-**	**8**	**-**	**92**	

О – опрос; Т – тестирование

Содержание учебной дисциплины

Тема 1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению.

Понятие ИБ и информационного общества. Цели, задачи и принципы обеспечения ИБ. Угроза национальной безопасности и их виды. Информационные войны и информационное оружие. Информационный терроризм. Информационное общество в РФ и его характеристики. Информационная сфера и ее области. Национальные интересы России в информационной сфере. Государственная политика РФ в сфере обеспечения ИБ и ее принципы.

Тема 2. Нормативно-правовая база обеспечения ИБ в России.

Понятие правового обеспечения и правовой защиты. История формирования законодательства РФ об информации и ее защите. Система нормативно-правовых актов России, регулирующих отношения в сфере ИБ. Международно-правовые нормы и стандарты в сфере ИБ. Место Окинавской Хартии глобального информационного общества в системе международно-правовых актов обеспечения ИБ. Предмет и метод правового регулирования в сфере ИБ страны. Информационное право. Информационные отношения. Виды ведомственных и корпоративных норм и их место в системе правового регулирования ИБ в РФ. Правовое регулирование деятельности средств массовой информации. Основные тенденции развития законодательства РФ в сфере ИБ. Особенности стандартизации нормативной базы в сфере ИБ в современном мире.

Тема 3. Информация как объект правового регулирования и защиты.

Информация, ее виды и признаки. Информация как объект юридической защиты. Информационная сфера общества и ее характеристики. Информационные ресурсы. Понятие и виды. Виды и источники информации, подлежащие защите. Правовой режим защиты государственной тайны. Способы обеспечения сохранности информации, составляющей государственную тайну и система контроля за состоянием ее защиты. Основные принципы засекречивания информации. Конфиденциальная информация и возможные каналы ее утечки. Информационная инфраструктура и информационная среда. Их структура и характеристики. Международный опыт деятельности по правовому обеспечению ИБ и основные направления его развития. Государственная политика РФ в сфере правового обеспечения ИБ.

Тема 4. Система субъектов обеспечения ИБ в России и их правовой статус.

Понятие государственного управления в сфере обеспечения ИБ. Система органов государственной власти, обеспечивающая ИБ и особенности их компетентности. Правовой статус и система органов государственной власти, обеспечивающая право доступа к информации. Особенности правового статуса и организация работы органов государственной власти, обеспечивающих защиту информации, обрабатываемой техническими средствами. Служба Специальной связи и информации Федеральной службы охраны РФ, ее задачи и правовой статус.

Тема 5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика.

Понятие и виды преступности в информационной сфере. Основные этапы и тенденции развития компьютерной преступности в России. Особенности детерминации преступлений, совершаемых в информационной сфере. Криминологическая и криминалистическая характеристики основных способов мошенничества, совершаемых с помощью сети Интернет. Понятие преступления в сфере компьютерной информации. Виды преступлений в сфере компьютерной информации. Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Особенности объективных признаков компьютерных преступлений. Основные способы их совершения. Субъективные признаки компьютерных преступлений. Характерные мотивы и цели их совершения. Криминологическая и уголовно-правовая характеристика лиц, совершающих преступления в сфере компьютерной информации.

Тема 6. Правовая защита личности в информационной сфере.

Система и структура нормативных актов, обеспечивающих защиту прав личности в информационной сфере. Конституционные гарантии правовой охраны прав личности в информационной сфере. Правовые средства защиты права на доступ к информации и неприкосновенности частной жизни. Правовой механизм защиты права на неприкосновенность частной жизни. Врачебная тайна как институт защиты интересов личности. Защита права на личную информацию с ограниченным доступом. Персональная тайна и ее виды. Обработка и правовая охрана персональных данных. Правовая база обеспечения защиты личности от воздействия «вредной» информации. Российская и зарубежная модели обеспечения защиты личности от воздействия «вредной» информации.

Тема 7. Правовой режим государственной тайны и меры по ее обеспечению.

Понятие государственной тайны и правового режима ее обеспечения. Принципы и механизм отнесения сведений к государственной тайне (ГТ). Процедура засекречивания и рассекречивания сведений, составляющих государственную тайну. Субъекты обеспечения режима государственной тайны и их правовой статус. Организационно-правовые меры защиты ГТ. Допуск и доступ к ГТ. Обеспечение ИБ при международном обмене информацией. Система контроля за режимом обеспечения ГТ. Особенности юридической ответственности за нарушение режима обеспечения ГТ.

Тема 8. Правовые и организационные способы защиты информации в сфере высоких технологий.

Правовое обеспечение защиты информации, обрабатываемой вычислительной техникой и передаваемой по компьютерным цепям. Организационно-управленческие меры обеспечения защиты информации в сфере высоких технологий. Компьютерные преступления и особенности их идентификации и предупреждения. Правовые основы применения «электронной цифровой подписи» (ЭЦП). Криптографическая защита информации (КЗИ). Правовые и организационные способы обеспечения КЗИ в России и других странах современного мира. Контроль за разработкой, производством и применением криптографических средств. КЗИ и их правовая основа. Органы лицензирования и сертификации и их правовой статус.

Тема 9. Правовое обеспечение права интеллектуальной собственности (ПИС).

Понятие интеллектуальной собственности и ее правовой статус. Законодательство РФ об авторских и смежных правах. Особенности правоотношений, обеспечивающих ПИС. Объекты и субъекты ПИС. Правовой механизм обеспечения защиты авторских и смежных прав. Государственная регистрация ПИС. Особенности правовой защиты программ для электронных вычислительных машин и баз данных. Патентное право и патентные правоотношения. Правовой статус участников. Сфера действия патентного законодательства. Показатели и условия патентоспособности. Правовой статус автора и патентообладателя. Механизм правовой защиты прав автора и патентообладателей. Товарный знак и механизм его правовой защиты. Государственная регистрация товарного знака. Прекращение права на товарный знак. Программы для ЭВМ и механизм их правовой защиты. Правовое регулирование договорных отношений в сфере ПИС.

Тема 10. Правовая защита коммерческой тайны (КТ).

Понятие КТ и ее правовой статус. Признаки КТ. Защита КТ и патентование как способы правового закрепления права собственности на промышленный образец и полезную модель. Объекты защиты КТ. Особенности правового обеспечения режима КТ. Промышленный шпионаж и его объекты. Критерии определения секретности при определении режима КТ. Организационные меры обеспечения защиты КТ и особенности их реализации в рамках гражданско-правовых (договорных) и трудовых отношений. Режим представления информации, составляющей КТ органам государственной власти. Юридическая ответственность за нарушения режима обеспечения КТ.

Тема 11. Правовое регулирование отношений в сфере лицензирования и сертификации.

Правовое обеспечение деятельности организаций по лицензированию и сертификации в сфере ИБ. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию в сфере ИБ. Система государственного лицензирования в сфере ИБ и ее функции. Субъекты лицензирования в сфере ИБ и их правовой статус. Порядок лицензирования, приостановления или аннулирования действия лицензии. Специальная экспертиза

предприятия и государственная аттестация их руководителей. Контроль за условиями обеспечения ИБ лицензиатами. Понятие сертификации средств защиты информации (ССЗИ) и ее правовая основа в РФ. Цели создания системы ССЗИ. Организационная структура системы ССЗИ и особенности правового статуса ее субъектов. Объекты сертификационной деятельности и режимы сертификации. Особенности аттестации и контроля за деятельностью объектов обработки особо важной информации. Юридическая ответственность за нарушением правил лицензирования и сертификации.

Тема 12. Предупреждение преступлений в информационной сфере в современной России.

Информационная безопасность России и задачи по ее обеспечению. Система детерминант преступности в информационной сфере. Уровневый подход. Мотивационная сфера лиц, совершающих правонарушения в сфере ИБ. Субъекты деятельности по обеспечению противодействия правонарушениям в сфере ИБ и их правовой статус. Оперативно-розыскные и криминалистические мероприятия по борьбе с преступлениями в сфере ИБ. Особенности расследования преступлений в сфере ИБ. Совершенствование правовых норм как средство обеспечения профилактического воздействия на отношения в сфере ИБ. Зарубежный опыт борьбы с преступностью в сфере ИБ.

Тема 13. Юридическая ответственность за правонарушения в сфере ИБ.

Понятие и виды юридической ответственности (ЮО) за правонарушения в сфере ИБ. Уголовная ответственность за правонарушения в сфере ИБ и ее особенности. Объективные и субъективные признаки составов преступлений, посягающих на ИБ страны. Уголовная ответственность за компьютерные преступления и особенности их реализации в современной России. Правовое регулирование отношений, связанных с привлечением к ответственности лиц, совершивших административные правонарушения в сфере ИБ. Составы административных правонарушений, посягающих на ИБ страны. Органы государственной власти и должностные лица, уполномоченные рассматривать административные правонарушения в сфере защиты информации и их правовой статус.

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

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

Промежуточная аттестация проводятся устно в ДОТ/письменно с прокторингом / тестирование с прокторингом. Для успешного освоения курса учащемуся рекомендуется ознакомиться с литературой, размещенной в разделе 6, и материалами, выложенными в ДОТ.

4.1.1. В ходе реализации дисциплины Б1.В.03.05. «Правовое обеспечение информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

Тема занятия	Вид занятия / Оценочное средство
Информационная безопасность (ИБ) РФ и задачи по ее обеспечению	ПЗ / опрос
Нормативно-правовая база обеспечения ИБ в России	ПЗ / опрос
Информация как объект правового регулирования и защиты	ПЗ / опрос
Система субъектов обеспечения ИБ в России и их правовой статус	ПЗ / опрос
Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика	ПЗ / опрос
Правовая защита личности в информационной сфере	ПЗ / опрос
Правовой режим государственной тайны и меры по ее обеспечению	ПЗ / опрос

Правовые и организационные способы защиты информации в сфере высоких технологий	ПЗ / опрос
Правовое обеспечение права интеллектуальной собственности (ПИС)	ПЗ / опрос
Правовая защита коммерческой тайны (КТ)	ПЗ / опрос
Правовое регулирование отношений в сфере лицензирования и сертификации	ПЗ / опрос
Предупреждение преступлений в информационной сфере в современной России	ПЗ / опрос
Юридическая ответственность за правонарушения в сфере ИБ	ПЗ / опрос

4.1.2. Промежуточная аттестация проводится с применением следующих методов:
Зачет проводится на основе компьютерного тестирования в ДОТ/устно/письменно

4.2. Материалы текущего контроля успеваемости обучающихся
Полный перечень типовых оценочных материалов находится на кафедре безопасности.

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКр ОС-1	Способность обеспечивать безопасность личности, общества, государства правовыми средствами	ПКр ОС-1.2	Принимает правовые меры по нейтрализации угроз безопасности личности, общества, государства

Компоненты:
- определение объектов безопасности личности, общества, государства и их жизненно важных интересов;
- прогнозирование, выявление, анализ и оценка угроз и рисков безопасности личности, общества, государства, в том числе с применением риск-ориентированного подхода;
- принятие правовых мер по нейтрализации угроз безопасности личности, общества, государства.

Описание критериев оценивания компетенции

Критерий оценивания	Характеристика критерия оценивания
системность	системный подход к определению объектов безопасности личности, общества, государства и их жизненно важных интересов
объективность	выявление объективных обстоятельств, способствующих возникновению угроз и рисков безопасности личности, общества, государства;
оперативность	система правовых мер, позволяющая осуществить нейтрализацию угроз безопасности личности, общества, государства кратчайшие сроки

Схема расчета рейтинговых баллов по дисциплине
Б1.В.03.05. «Правовое обеспечение информационной безопасности»
по специальности 45.05.01 «Правовое обеспечение национальной безопасности»

Недели	Виды учебных занятий (лекции/семинары)	Посещение учебных занятий	Письменные работы			Устные выступления		Компенсирующие задания (сверх расчетных 100 баллов)	Промежуточная аттестация	Итого (максимально-расчетное количество баллов)
			Контрольные	Решение ситуационной задачи	Тестирование	Ролевые игры	Опрос			
Кол-во баллов										

за 1 вид мероприятия										
1	лекция	1								
2	семинар	1		4/5			2	1 (эссе)		
3	лекция	1								
4	лекция	1								Σ за 4 недели =8/9
5	семинар	1		4/5			2	1 (эссе)		
6	семинар	1		4/5			2	1 (эссе)		
7	лекция	1								
8	лекция	1								Σ за 8 недель =25/29
9	семинар	1		4/5			2	1 (эссе)		
	Текущий* контроль 1									29
10	семинар	1		4/5			2	1 (эссе)		
11	лекция	1								
12	лекция	1								Σ за 12 недель = 37/42
13	лекция	1		4/5			2	1 (эссе)		
14		1		4/5			3	1 (эссе)		
15	лекция	1								
16	семинар	1		4/5***			5	1 (эссе)		Σ за 16 недель
										64/76
	Текущий** контроль 2								24	24
Всего за семестр (баллов)		16		32/40			20	8	24	100

*Количество баллов, достаточное для аттестации текущего контроля

**Количество баллов, достаточное для возможного освобождения от промежуточной аттестации

*** возможна замена на результаты тестирования

4.3. Оценочные средства для промежуточной аттестации

Вопросы к зачету

1. Информационная безопасность (ИБ) РФ и задачи по ее обеспечению
2. Нормативно-правовая база обеспечения ИБ в России
3. Информация как объект правового регулирования и защиты
4. Система субъектов обеспечения ИБ в России и их правовой статус
5. Преступность в информационной сфере и ее криминологическая и уголовно-правовая характеристика
6. Правовая защита личности в информационной сфере
7. Правовой режим государственной тайны и меры по ее обеспечению
8. Правовые и организационные способы защиты информации в сфере высоких технологий
9. Правовое обеспечение права интеллектуальной собственности (ПИС)
10. Правовая защита коммерческой тайны (КТ)
11. Правовое регулирование отношений в сфере лицензирования и сертификации
12. Предупреждение преступлений в информационной сфере в современной России
13. Юридическая ответственность за правонарушения в сфере ИБ

Вопросы для обсуждения

1. Какими факторами обусловлена актуальность проблемы обеспечения защиты информации?

2. Каковы основные задачи информационной безопасности?
3. Какие классы угроз информационной безопасности можно выделить?
4. Каковы основные методы реализации угроз информационной безопасности?
5. Какие существуют средства и методы обеспечения целостности информации?
6. Какие существуют средства и методы обеспечения конфиденциальности информации?
7. Каковы особенности защиты информации при работе с сетевыми сервисами?
8. Какова цель резервного копирования данных?
9. Каковы место и роль системы обеспечения информационной безопасности в национальной безопасности РФ?
10. Каково состояние системы защиты информации в России и в ведущих зарубежных странах?
11. Какие Международные стандарты в области информационного обмена Вам известны?
12. Какие основные понятия и определения защиты информации Вы можете привести?
13. Какие уровни обеспечения информационной безопасности Вам известны?
14. В чем заключается особенность государственной политики в области информационной безопасности?
15. Когда была принята Доктрина информационной безопасности РФ?
16. Какие нормативные руководящие документы, касающиеся государственной тайны Вам известны?
17. Какие преступления можно отнести к компьютерным?
18. Как классифицируются компьютерные преступления?
19. Что такое угроза информационной безопасности?
20. По каким признакам можно классифицировать угрозы информационной безопасности?
21. Каковы причины успешной реализации угроз информационной безопасности?
22. Какие каналы утечки и искажения информации Вам известны?
23. Каковы основные методы реализации угроз информационной безопасности?
24. Какое влияние на состояние информационной безопасности оказывает развитие глобальных сетей?
25. Какие виды нарушения информационной системы Вам известны?

Задание (тип 1):

Разработать нормативную документацию организации (государственного органа/хозяйствующего субъекта) в сфере информационной безопасности:

1. Политика информационной безопасности
2. Концепция обеспечения информационной безопасности
3. Положение о службе информационной безопасности
4. План защиты информационных активов от несанкционированного доступа
5. Правила обеспечения безопасности при работе пользователей в корпоративной сети
6. Политика управления доступом к ресурсам корпоративной сети
7. Политика управления инцидентами информационной безопасности
8. Политика обеспечения безопасности при взаимодействии с сетью Интернет
9. Политика антивирусной защиты
10. Парольная политика
11. Политика обеспечения безопасности платежных систем организации
12. Руководство по защите конфиденциальной информации
13. Регламент работы с цифровыми носителями конфиденциальной информации
14. Политика предотвращения утечки информации по каналам связи

15. Политика обеспечения безопасности электронного документооборота и другие.

Задание (тип 2):

Выполнить задания по использованию информационных ресурсов (справочно-правовые системы, электронный документооборот, электронные торговые площадки).

4.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующие этапы формирования компетенций

Оценочные средства (формы текущего и промежуточного контроля)	Показатели оценки	Критерии оценки
Доклад	Соблюдение регламента (15 мин.); характер источников (более трех источников); подача материала (презентация); ответы на вопросы (владение материалом).	Каждый критерий оценки доклада оценивается в 0,25 балла, максимум 1 балл за доклад. Допускается не более одного доклада в семестр, десяти докладов в год (всего до 10 баллов)
Тестирование	Процент правильных ответов на вопросы теста	Менее 60% – 0 баллов; 61 - 75% – 6 баллов; 76 - 90% – 8 баллов; 91 - 100% – 10 баллов.
Зачет	В соответствии с балльно-рейтинговой системой на промежуточную аттестацию отводится 30 баллов. Зачет проводится по тестам.	Менее 60% – 0 баллов; 61 - 75% – 10 баллов; 76 - 90% – 20 баллов; 91 - 100% – 30 баллов.
Устный опрос	Корректность и полнота ответов	Сложный вопрос: полный, развернутый, обоснованный ответ – 10 баллов Правильный, но не аргументированный ответ – 5 баллов Неверный ответ – 0 баллов Обычный вопрос: полный, развернутый, обоснованный ответ – 4 балла Правильный, но не аргументированный ответ – 2 балла Неверный ответ – 0 баллов. Простой вопрос: Правильный ответ – 1 балл; Неправильный ответ – 0 баллов
Выполнение проблемных заданий	Правильность решения; корректность выводов обоснованность решений	баллы начисляются от 1 до 3 в зависимости от сложности задачи/вопроса (не более 38 баллов за семестр)

Критерии оценки ответа на зачетное тестирование:

Процент правильных ответов на вопросы теста.

Шкала оценивания

Оценка результатов производится на основе балльно-рейтинговой системы (БРС). Использование БРС осуществляется в соответствии с приказом от 06 сентября 2019 г. №306 «О применении балльно-рейтинговой системы оценки знаний обучающихся».

Схема расчетов сформирована в соответствии с учебным планом направления, согласована с руководителем научно-образовательного направления, утверждена деканом факультета.

Схема расчетов доводится до сведения студентов на первом занятии по данной дисциплине, является составной частью рабочей программы дисциплины и содержит информацию по

изучению дисциплины, указанную в Положении о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС.

В соответствии с балльно-рейтинговой системой максимально-расчетное количество баллов за семестр составляет 100, из них в рамках дисциплины отводится:

40 баллов - на промежуточную аттестацию

40 баллов - на работу на семинарских занятиях

20 баллов - на посещаемость занятий

В случае если студент в течение семестра не набирает минимальное число баллов, необходимое для сдачи промежуточной аттестации, то он может заработать дополнительные баллы, отработав соответствующие разделы дисциплины, получив от преподавателя компенсирующие задания.

В случае получения на промежуточной аттестации неудовлетворительной оценки студенту предоставляется право повторной аттестации в срок, установленный для ликвидации академической задолженности по итогам соответствующей сессии.

Обучающийся, набравший в ходе текущего контроля в семестре от 51 до 60 баллов, по его желанию может быть освобожден от промежуточной аттестации.

Шкала перевода оценки из многобалльной в систему «зачтено»/«не зачтено»:

от 0 по 50 баллов	«не зачтено»
от 51 по 100 баллов	«зачтено»

5. Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов включает подготовку к практическим занятиям, которая предусматривает подготовку докладов и презентаций. Учебно-методическое обеспечение самостоятельной работы студентов представлено в данной программе. Контроль за качеством самостоятельно подготовленных материалов осуществляется в процессе проведения практических занятий с помощью соответствующих оценочных средств, также представленных в данной программе.

Вид учебных занятий, промежуточная аттестация	Организация деятельности студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, формулы, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, сложный материал, формулы, которые вызывают трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или при выполнении лабораторной работы.
Лабораторные работы	Лабораторные работы направлены на экспериментальное подтверждение теоретических положений и формирование учебных и профессиональных практических умений. В процессе лабораторного занятия обучающиеся выполняют задания под руководством преподавателя в соответствии с изучаемым содержанием учебного материала. Все студенты, находящиеся в лаборатории, должны соблюдать инструкцию по охране труда при проведении лабораторных занятий в аудиториях кафедры. Перед выполнением лабораторной работы необходимо познакомиться с теоретическим материалом и описанием соответствующей работы, используя методическую литературу по данной теме.
Практические занятия	Практические занятия направлены на формирование учебных и профессиональных практических умений, выполнение расчетов и задач.
Научно-исследовательская работа	При выполнении НИР студенты должны решать задачи практической направленности на основании теоретических положений, получая реальные результаты на основе обоснованного анализа данных.
Подготовка к экзамену	При подготовке к зачету необходимо ориентироваться на конспекты лекций, рекомендуемую литературу и др.

При проведении учебных занятий предусмотрено применение разных форм учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, включая проведение интерактивных лекций, групповых дискуссий.

В процессе лекционного занятия обучающийся ведет свой конспект лекций, делая записи, касающиеся основных тезисов лектора. Это могут быть исходные проблемы и вопросы, ключевые понятия и их определения, важнейшие положения и выводы, существенные оценки и т.д.

В заключительной части лекции обучающийся может задать вопросы преподавателю по содержанию лекции, уточняя и уясняя для себя теоретические моменты, которые остались ему непонятными.

Самостоятельная работа обучающегося, прежде всего, подразумевает изучение им учебной литературы, рекомендуемой рабочей программой дисциплины.

Значительную роль в изучении данной дисциплины выполняют семинарские занятия, которые призваны, прежде всего, закреплять теоретические знания, полученные в ходе прослушивания и запоминания лекционного материала, изучения источников, ознакомления с учебной и научной литературой. Тем самым семинары способствуют получению студентами наиболее качественных знаний, а также позволяют осуществлять со стороны преподавателя текущий контроль над успеваемостью студентов.

Семинарские занятия преподаватель может проводить в форме обсуждения вопросов темы, заслушивания докладов по отдельным вопросам и их обсуждения, рекомендуется выполнение письменных работ, тестирование и решение практических задач.

В процессе подготовки к семинару студент самостоятельно аккумулирует знания путем изучения конспекта лекций и соответствующих разделов учебника, ознакомления с дополнительной литературой и источниками, рекомендованными к этому практическому занятию.

Отвечать на тот или иной вопрос обучающимся рекомендуется формулировать наиболее полно и точно, при этом нужно уметь логически грамотно выражать и обосновывать свою точку зрения, свободно оперировать юридическими понятиями и терминами.

Предусмотрена работа слушателей на практических занятиях (семинарах) по рассмотрению основных тенденций мировой экономики и международных экономических отношений. Есть часы лабораторной работы с практической оценкой мировых тенденций по изучаемым вопросам.

Таким образом, посещение обучающимся лекционных занятий, активная самостоятельная работа, а также участие на семинарских занятиях необходимы для подготовки и успешной сдачи экзамена как формы итогового контроля.

При подготовке к зачету необходимо исходить из перечня контрольных вопросов. зачет, как правило, проводится в устной форме.

При оценивании знаний студентов экзаменатор руководствуется, прежде всего, следующими критериями:

- правильность ответов на вопросы;
- полнота и лаконичность ответа;
- логика и аргументированность изложения.

Более подробную информацию о методике подготовки и сдачи зачета обучающийся может получить у преподавателя.

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

6.1. Основная учебная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст :

электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235

2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

6.2. Дополнительная учебная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

2. Баранова, Е.К. Информационная безопасность и защита информации : учебное пособие / Баранова Е.К., Бабаш А.В., - 4-е изд., перераб. и доп. – Москва : РИОР, ИНФРА-М, 2018. - 336 с.

6.3. Учебно-методическое обеспечение самостоятельной работы

Для успешного овладения учебным материалом и методами системного анализа студент обязан не менее 4-х часов в неделю уделять самостоятельной работе: подготовке к семинарским занятиям, нахождению в учебнике ответов на тестовые задания к каждой теме дисциплины, организации учебно-исследовательской деятельности.

В самостоятельной работе студентов могут также найти свое применение специально созданные научно-просветительские и образовательные мультимедиа продукты с ориентацией на историко-культурные и историко-политические сюжеты, изданные на CD-R.

Положительной стороной образовательной технологии является ее гибкость, адаптация к индивидуальным особенностям студентов за счет исходной диагностики уровня и объема знаний, варьирования темпа усвоения учебного материала.

В компьютерном классе организована система предварительной записи студентов.

Тестовые задания ориентированы на альтернативный, простой выборочный, выборочно-конструируемый и свободно-конструируемый ответы. При компьютерном тестировании эти задания группируются в фреймы, где последовательность вопросов генерируется в диалоговом режиме и может включать в себя цепочки уточняющих вопросов (вопросы с продолжением), а в некоторых случаях и обучающие комментарии.

Каждый вопрос, при правильном ответе на него, имеет свою экспертную весовую оценку, которая учитывается при сборе статистической информации и заносится в индивидуальный файл тестируемого. Затем эти данные обрабатываются и группируются в сводные статистические таблицы для учебных (семинарских) групп. Таким образом, создается объективная картина учебных достижений каждого студента на всех этапах обучения. Время, отводимое на компьютерное тестирование, ограничено. По окончании тестирования студенту выдается объективная информация, позволяющая выявить имеющиеся у него пробелы в знаниях и принять меры по их устранению.

На центральном компьютере тестирующей сети с точностью до вводимого символа фиксируются протоколы диалогов и хронометраж каждого тестируемого по всем сеансам его работы. Протоколы используются для разрешения конфликтных ситуаций и совершенствования компьютерного анализатора ответов на тестовые задания.

Методические рекомендации по изучению дисциплины

Для изучения основных вопросов образовательной программы необходимо конспектировать материалы лекций, работать с рекомендованной преподавателем литературой. Для приобретения навыков активного использования знаний полезно обсуждать решаемые задачи на практических занятиях. При разучивании формул полезно записывать их на бумаге. Чтобы легче и прочнее усвоить материал следует постоянно использовать конкретные примеры, сравнения из уже полученных областей наук.

Для закрепления изученного материала даны вопросы по каждой теме дисциплины, на которые следует самостоятельно найти ответы.

При подготовке к практическим занятиям необходимо ознакомиться с методическими указаниями по соответствующей теме и осуществить подготовку по рекомендованным в учебно-методическом комплексе вопросам для обсуждения темы.

После изучения базовых тем курса проводится оперативный контроль знаний студентов в виде опроса или письменного тестирования. Тестовые задания по темам дисциплины приведены в специальном разделе данного учебно-методического комплекса.

Подготовка к рубежному и итоговому контролю предполагает изучение представленных вопросов к экзамену, а также работу над тестами, представленными в данном учебно-методическом комплексе.

Для решения задач целесообразно широко использовать современные информационные технологии.

Применение балльно-рейтинговой системы оценки знаний студентов

При оценивании используется балльно-рейтинговая система. Баллы начисляются за посещаемость (максимум 20 баллов), выступления с докладами (максимум 12 баллов), полный и правильный ответ на вопрос при устном опросе (максимум 30 баллов), результаты выполнения тестовых заданий, ответ на экзамене (максимум 30 баллов). Дисциплина считается освоенной, если экзаменуемый набрал не менее 51 балла в результате выполнения всех типов заданий, включая ответ на экзамене. Минимальное количество баллов для допуска к экзамену – 45.

На основании п. 14 Положения о балльно-рейтинговой системе оценки знаний обучающихся в РАНХиГС в институте принята следующая шкала перевода оценки из многобалльной системы в пятибалльную:

Расчет итоговой рейтинговой оценки:

Количество баллов	**Оценка**	
	прописью	**буквой**
96-100	отлично	A
86-95	отлично	B
71-85	хорошо	C
61-70	хорошо	D
51-60	удовлетворительно	E

Шкала перевода оценки из многобалльной в систему «зачтено»/ «не зачтено»:

от 0 до 50 баллов	«не зачтено»
от 51 до 100 баллов	«зачтено»

Условия выполнения задания:

1. Место выполнения: в учебной аудитории
2. Каждый критерий оценки доклада оценивается в 1 балл, максимум 4 балла за доклад. Допускается не более трех докладов в семестр (всего 12 баллов)
3. За полноту и правильность ответа на вопрос при устном опросе в соответствии со сложностью вопроса присваиваются баллы от 5 до 10 баллов. Всего необходимо получить до 30 баллов в семестр.
4. Тестирование проходит два раза за семестр и оценивается по критерию оценки – правильность ответов на тестовые задания в баллах от 0 до 5, всего необходимо набрать до 10 баллов.

6.4. Нормативные правовые документы

1. Правовая система «Гарант-Интернет» [Электронный ресурс]. – Режим доступа: http: // www.garweb.ru.
2. Правовая система «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: http: // www.consultant.ru.

3. Центр профессиональной подготовки [Электронный ресурс]. – Режим доступа: http: // www.c-pp.ru.

6.5. Интернет-ресурсы

СЗИУ располагает доступом через сайт научной библиотеки http://nwapa.spb.ru/ к следующим подписным электронным ресурсам:

Русскоязычные ресурсы

1. Электронные учебники электронно-библиотечной системы (ЭБС) «Айбукс» http://www.nwapa.spb.ru/index.php?page_id=76
2. Научно-практические статьи по экономики и и менеджменту Издательского дома «Библиотека Гребенникова» http://www.nwapa.spb.ru/index.php?page_id=76
3. Статьи из журналов и статистических изданий Ист Вью http://www.nwapa.spb.ru/index.php?page_id=76

Англоязычные ресурсы

4. EBSCO Publishing- доступ к мультидисциплинарным полнотекстовым базам данных различных мировых издательств по бизнесу, экономике, финансам, бухгалтерскому учету, гуманитарным и естественным областям знаний, рефератам и полным текстам публикаций из научных и научно – популярных журналов.
5. Emerald – крупнейшее мировое издательство, специализирующееся на электронных журналах и базах данных по экономике и менеджменту. Имеет статус основного источника профессиональной информации для преподавателей, исследователей и специалистов в области менеджмента.

6.6.Иные источники

1. Правовая система «Гарант-Интернет» [Электронный ресурс]. – Режим доступа: http: // www.garweb.ru.
2. Правовая система «КонсультантПлюс» [Электронный ресурс]. – Режим доступа: http: // www.consultant.
3. Центр профессиональной подготовки [Электронный ресурс]. – Режим доступа: http: // www.c-pp.ru.

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

№ п\п	Наименование дисциплины (модуля), практик в соответствии с учебным планом	Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	Правовое обеспечение информационной безопасности	Тематические аудитории специальности «Правовое обеспечение национальной безопасности», Компьютерные классы. Иные аудитории Факультета таможенного администрирования и безопасности (в соответствии с расписанием занятий), оснащенные средствами мультимедиа и досками Учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования, групповых и индивидуальных консультаций, текущего	Оснащены средствами мультимедиа и досками. Звуковые динамики; программные средства, обеспечивающие прослушивание материалов в формате MP3, WMA, а также просмотр видеоматериалов. Программное обеспечение Microsoft Word, Microsoft Power Point для подготовки текстового материала, графических ил-	Лицензионное соглашение с Microsoft Windows 10 SBR003-1706010146-42 от 07.07.2017 по 31.07.2018 Microsoft Office Professional 2016 SBR003-1706010146-42 от 07.07.2017 по 31.07.2018

		контроля и промежуточной аттестации. Кабинеты, оснащенные макетами, наглядными учебными пособиями, и другими техническими средства и оборудованием, обеспечивающими реализацию проектируемых результатов обучения.	люстраций, презентаций.	

Под информационной технологией понимается процесс, использующий совокупность средств и методов сбора, обработки и передачи данных (первичной информации) для получения информации нового качества о состоянии объекта, процесса или явления (информационного продукта).

В последние годы термин «информационные технологии» часто выступает синонимом термина «компьютерные технологии», так как все информационные технологии в настоящее время так или иначе связаны с применением компьютера. Однако, термин «информационные технологии» намного шире и включает в себя «компьютерные технологии» в качестве составляющей. При этом, информационные технологии, основанные на использование современных компьютерных и сетевых средств, образуют термин «Современные информационные технологии».

Виды информационных технологий:

«ручная» информационная технология, инструментарий которой составляют: перо, чернильница, книга. Коммуникации осуществляется ручным способом (написание конспектов и т.д.). Основная цель технологии - представление информации в нужной форме.

«механическая» технология, оснащенная более совершенными средствами передачи и доставки информации, инструментарий которой составляют: телефон, диктофон. Основная цель технологии - представление информации в нужной форме более удобными средствами.

«электрическая» технология, инструментарий которой составляют: ксероксы, портативные диктофоны. Основная цель информационной технологии начинает перемещаться с формы представления информации на формирование ее содержания.

«электронная» технология, основным инструментарием которой становятся ЭВМ и создаваемые на их базе автоматизированные системы управления (АСУ) и информационно-поисковые системы, оснащенные широким спектром базовых и специализированных программных комплексов. Центр тяжести технологии еще более смещается на формирование содержательной стороны информации для управленческой среды различных сфер общественной жизни, особенно на организацию аналитической работы.

«компьютерная» («новая») технология, основным инструментарием которой является персональный компьютер с широким спектром стандартных программных продуктов разного назначения (Excel, Word, Power Point). На этом этапе происходит процесс персонализации АСУ, который проявляется в создании систем поддержки принятия решений определенными специалистами. Подобные системы имеют встроенные элементы анализа и искусственного интеллекта для разных уровней управления, реализуются на персональном компьютере и используют телекоммуникации. В связи с **переходом** на микропроцессорную базу существенным изменениям подвергаются и технические средства бытового, культурного и прочего назначений.

«сетевая технология» (иногда ее считают частью компьютерных технологий) только устанавливается. Начинают широко использоваться в различных областях глобальные и локальные компьютерные сети. Ей предсказывают в ближайшем будущем бурный рост, обусловленный популярностью ее основателя - глобальной компьютерной сети Internet.

Информационные справочные системы

1. http://sziu.ranepa.ru/component/zoo/vhod-v-elektronnuyu-informacionno-obrazovatelnuyu-sredu - Электронная информационно-образовательная среда
2. http://nwipa.ru/cat/avesta_elcat.php - Автоматизированная информационная библиотечная система
3. http://eds.b.ebscohost.com/eds/search/basic?vid=1&sid=5d27f7d7-ba85-44b2-9c74-

d2a5fc97f07b%40sessionmgr102 – научная библиотека СЗИУ РАНХиГС

4. *https://ibooks.ru/home.php?routine=bookshelf* - электронно-библиотечная система БС Айбукс
5. *https://e.lanbook.com/* - электронно-библиотечная система Лань
6. *http://www.iprbookshop.ru/ - ЭБС IPRBooks*
7. *https://grebennikon.ru/ - ЭБС ИД Гребенников*
8. *https://biblio-online.ru/ - ЭБС Юрайт*
9. *http://site.ebrary.com/lib/ranepa - ЭБС Ebrary*
10. *https://dlib.eastview.com/;jsessionid=aaaQppOlFfNE9_8FcPeaw* – ЭБС Российские журналы, статистика.