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

УТВЕРЖДАЮ
Начальник отдела лицензирования и аккредитации
_____ Чаленко К.Н.
«01» 06 20 20 г.

Рабочая программа дисциплины
Правовые основы защиты экономической информации

Специальность 38.05.01 Экономическая безопасность специализация 38.05.01.01 "Экономико-правовое обеспечение экономической безопасности"

Для набора 2017, 2018, 2019, 2020 года

Квалификация
Экономист

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по курсам

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Практические	4	4	4	4
Итого ауд.	8	8	8	8
Контактная работа	8	8	8	8
Сам. работа	60	60	60	60
Часы на контроль	4	4	4	4
Итого	72	72	72	72

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 25.02.2020 протокол № 8.

Программу составил(и): к.т.н., доцент Серпенинов О.В. _____

Зав. кафедрой: Ефимова Е.В. _____

Методическим советом направления: д.э.н., профессор Суржиков М.А. _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	приобретение знаний по правовому обеспечению защиты экономической информации и формирование практических навыков использования актуальной нормативно-правовой базы для решения задач защиты экономической информации.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-41:способностью принимать участие в разработке стратегии обеспечения экономической безопасности организаций, подготовке программ по ее реализации

ОК-12: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации

В результате освоения дисциплины обучающийся должен:

Знать:

особенности подходов к разработке стратегии защиты экономической информации правовыми методами;
способы организации процесса сбора, анализа и систематизации информации по формированию системы защиты экономической информации в организациях с различными формами собственности.

Уметь:

применять нормативно-правовые акты в области информационной безопасности для решения задач защиты экономической информации;
работать с различными информационными ресурсами для поиска и подбора необходимой нормативно-правовой базы для целей защиты экономической информации.

Владеть:

навыками анализа угроз экономической информации;
методологией организации технологического процесса защиты экономической информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература
	Раздел 1. Общие вопросы правовой защиты экономической информации				
1.1	Тма 1. "Информация как объект правового регулирования": определение; принципы; правовое регулирование общественных отношений, связанных с использованием информации;федеральное и международное законодательство в области защиты информации /Лек/	4	2	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.2	Тема 1. "Информация как объект правового регулирования": анализ актуальной нормативной-правовой базы; особенности реализации законодательства /Пр/	4	2	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3
1.3	Тема 1. "Информация как объект правового регулирования": самостоятельная работа по теме лекции /Ср/	4	30	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
	Раздел 2. Защита коммерческой тайны				
2.1	Тема 1. "Основы защиты коммерческой тайны":классификация угроз и нарушителей; методы и средства защиты коммерческой тайны /Лек/	4	2	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.2	Тема 1. "Основы защиты коммерческой тайны": модель угроз; модель нарушителя; правовые методы защиты с использованием Microsoft Office и Консультант + /Пр/	4	2	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4
2.3	Тема 1. "Основы защиты коммерческой тайны": самостоятельная работа по теме лекции /Ср/	4	30	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

2.4	/Зачёт/	4	4	ОК-12 ПК-41	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Л2.4

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Руденков Н. А., Пролетарский А. В., Смирнова Е. В., Суровов А. М.	Технологии защиты информации в компьютерных сетях	Москва: Национальный Открытый Университет «ИНТУИТ», 2016	https://biblioclub.ru/index.php?page=book&id=428820 неограниченный доступ для зарегистрированных пользователей
Л1.2	Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87995.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	https://biblioclub.ru/index.php?page=book&id=562246 неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Тищенко Е. Н.	Инструментальные методы анализа потребительского качества защищенных информационных систем: учеб. пособие	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2016	68
Л2.2	Братановский С. Н.	Специальные правовые режимы информации: монография	Москва: Директ-Медиа, 2012	https://biblioclub.ru/index.php?page=book&id=131866 неограниченный доступ для зарегистрированных пользователей
Л2.3	Заляжных, В. А., Гирик, А. В.	Экспертные системы комплексной оценки безопасности автоматизированных информационных и коммуникационных систем	Санкт-Петербург: Университет ИТМО, 2014	http://www.iprbookshop.ru/65733.html неограниченный доступ для зарегистрированных пользователей
Л2.4		БИТ. Бизнес & Информационные технологии: журнал	Москва: Положевец и партнеры, 2019	https://biblioclub.ru/index.php?page=book&id=562409 неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Гарант

Консультант+

Официальный сайт ФСТЭК России/fstec.ru

5.4. Перечень программного обеспечения

Microsoft Office

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

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

1.1 Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ПК-41:способностью принимать участие в разработке стратегии обеспечения экономической безопасности организаций, подготовке программ по ее реализации			
З: особенности подходов к разработке стратегии защиты экономической информации правовыми методами	поиск и сбор информации с целью разработки стратегии защиты экономической информации правовыми методами	полнота собранной информации и соответствие ее возможности по формированию стратегии защиты экономической информации правовыми методами	О (вопросы 1-17) З (вопросы 1-17)
У: применять нормативно-правовые акты в области информационной безопасности для решения задач защиты экономической информации	анализ соответствия разрабатываемой нормативно-правовой документации действующим нормативно-правовым актам в области информационной безопасности и защиты экономической информации	соответствие результатов анализа требованиям, представленных в нормативно-правовых актов в области информационной безопасности и защиты экономической информации	ПЗ (раздел 1, тема 1) ПОЗ (вопросы 38,39)
В: навыками анализа угроз экономической информации	формирование модели угроз экономической информации с учетом действующих нормативных и методических	соответствие разработанной модели угроз экономической информации действующим нормативным и методическим	ПЗ (раздел 1, тема 1) ПОЗ (вопросы 40,42)
	документов в области информационной безопасности	документам в области информационной безопасности, а также объекту защиты	
ОК-12: способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации			
З: способы организации процесса сбора, анализа и систематизации информации по формированию системы защиты информации в организациях с различными формами собственности	поиск и сбор информации по организации анализа и выбора методов и средств защиты информации при формировании системы защиты информации	полнота собранной информации и соответствие ее формируемой системе защиты информации	О (вопросы 18-37) З (вопросы 18-37)
У: работать с различными информационными ресурсами для поиска и подбора необходимой нормативно-правовой базы для целей защиты экономической информации	анализ состояния системы защиты экономической информации, выявление ее уязвимых мест и определение направления ее совершенствования	соответствие результатов анализа текущему состоянию системы защиты экономической информации	ПЗ (раздел 2, тема 1) ПОЗ (вопросы 41-43)
В: методологией организации технологического процесса защиты экономической информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России	использование методов и средств защиты информации в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России и ФСТЭК России	соответствие технологического процесса защиты экономической информации требованиям нормативно-методических документов ФСБ России и ФСТЭК России	ПЗ (раздел 2, тема 1) ПОЗ (вопросы 40,44)

О – опрос; ПЗ – практические задания; З – вопросы к зачету, ПОЗ – практико-ориентированные задания к зачету

1.2 Шкалы оценивания:

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

- 50-100 баллов (зачет);
- 0-49 баллов (незачет).

2 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

Вопросы к зачету

по дисциплине Правовые основы защиты экономической информации

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.
3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведения конфиденциального характера.
8. Организация работы со сведениями, отнесенные к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
11. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
12. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
13. Права обладателя коммерческой тайны.
14. Организация защиты информации на предприятии.
15. Обеспечение сохранности документов, дел и изданий.
16. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
17. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
18. Обязанности персонала организации по сохранению коммерческой тайны.
19. Политика безопасности предприятия как основа организационного управления защитой информации.
20. Права и обязанности работника и работодателя по защите конфиденциальной информации.
21. Ответственность за нарушение конфиденциальности информации.
22. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
23. Организация защиты персональных данных в организации.
24. Планирование мероприятий по организационной защите информации на предприятии.
25. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.

26. Организация аналитической работы в области защиты информации на предприятии.
27. Основные объекты и формы контроля за состоянием защиты информации.
28. Основные задачи и методы контроля.
29. Основные направления аналитической работы.
30. Организация аудита информационной безопасности предприятия.
31. Функции аналитического подразделения в области защиты информации на предприятии.
32. Основные этапы аналитической работы в области защиты информации на предприятии.
33. Содержание и основные виды аналитических отчетов.
34. Классификация методов анализа информации.
35. Компьютерные преступления в электронной коммерции.
36. Информационная безопасность в электронной коммерции.
37. Юридическая ответственность за нарушение правовых норм защиты информации.

Практико-ориентированные вопросы к зачету

38. Обосновать основные направления обеспечения информационной безопасности и защиты информации в РФ.
39. Правовое обеспечение защиты коммерческой тайны на предприятии.
40. Разработка политики безопасности предприятия.
41. Определение прав и обязанностей оператора, обрабатывающего персональные данные.
42. Определение уровня защищенности ИСПДн.
43. Определить основные объекты и формы контроля за состоянием защиты информации.
44. Сформулировать основные задачи и методы контроля.

Критерии оценивания:

- оценка «зачет» (50-100 баллов) – изложенный материал верен, наличие знаний в объеме пройденного курса в соответствии с поставленными программой курса целями и задачами обучения; правильные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, усвоение основной и знакомство с дополнительной литературой;
- оценка «незачет» (0-49 баллов) – 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.

Вопросы к опросу:

1. Информация как объект правового регулирования.
2. Структура законодательства РФ в области информационной безопасности и защиты информации.

3. Основные цели и методы обеспечения ИБ РФ. Источники и виды угроз ИБ РФ.
4. Основные направления обеспечения информационной безопасности и защиты информации в РФ.
5. Структура организационной защиты информации.
6. Виды информации, защищаемой законодательством РФ.
7. Перечень сведения конфиденциального характера.
8. Организация работы со сведениями, отнесенные к конфиденциальной информации.
9. Правовой режим защиты конфиденциальной информации.
10. Порядок отнесения информации к информации, составляющей коммерческую тайну, и ее предоставление.
11. Понятие коммерческой тайны. Правовое обеспечение защиты коммерческой тайны.
12. Сведения, составляющие коммерческую тайну. Сведения, которые не могут составлять коммерческую тайну.
13. Права обладателя коммерческой тайны.
14. Организация защиты информации на предприятии.
15. Обеспечение сохранности документов, дел и изданий.
16. Обязанности лиц, допущенных к сведениям, составляющих коммерческую тайну.
17. Организация контроля за обеспечением режима при работе со сведениями, содержащими коммерческую тайну.
18. Обязанности персонала организации по сохранению коммерческой тайны.
19. Политика безопасности предприятия как основа организационного управления защитой информации.
20. Права и обязанности работника и работодателя по защите конфиденциальной информации.
21. Ответственность за нарушение конфиденциальности информации.
22. Права и обязанности субъекта персональных данных и оператора, обрабатывающего персональные данные.
23. Организация защиты персональных данных в организации.
24. Планирование мероприятий по организационной защите информации на предприятии.
25. Структура и основное содержание плана мероприятий по защите конфиденциальной информации.
26. Организация аналитической работы в области защиты информации на предприятии.
27. Основные объекты и формы контроля за состоянием защиты информации.
28. Основные задачи и методы контроля.
29. Основные направления аналитической работы.
30. Организация аудита информационной безопасности предприятия.

31. Функции аналитического подразделения в области защиты информации на предприятии.
32. Основные этапы аналитической работы в области защиты информации на предприятии.
33. Содержание и основные виды аналитических отчетов.
34. Классификация методов анализа информации.
35. Компьютерные преступления в электронной коммерции.
36. Информационная безопасность в электронной коммерции.
37. Юридическая ответственность за нарушение правовых норм защиты информации.

Критерии оценивания:
правильный ответ на 1 вопрос – 1 балл;
неправильный ответ на 1 вопрос – 0 баллов.
Количество баллов – 20 баллов.

Практические задания

Тематика практических заданий по разделам и темам

Раздел 1. Общие вопросы правовой защиты экономической информации

Тема 1. "Информация как объект правового регулирования".

Практическое задание. Анализ актуальной нормативной-правовой базы; особенности реализации законодательства. Использовать ИСС: Гарант, Консультант+, официальный сайт ФСТЭК России/fstec.ru. (40 баллов)

Раздел 2. Защита коммерческой тайны

Тема 1. "Основы защиты коммерческой тайны".

Практическое задание. Модель угроз; модель нарушителя; правовые методы защиты. (40 баллов)

Критерии оценивания каждого практического задания:

- 20-40 баллов – изложенный материал верен; правильные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при выполнении задания;
- 0-19 баллов – наличие грубых ошибок в задании, непонимание сущности излагаемого задания, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

3 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по окончанию теоретического обучения до начала экзаменационной сессии. Количество вопросов в зачетном задании – 3. Объявление результатов производится в день зачета. Результаты аттестации заносятся в электронную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются основные понятия в области информационной безопасности и защиты информации, методы обнаружения и организации противодействия атак на информационные сети, требования по защите конфиденциальной информации, даются рекомендации для самостоятельной работы и подготовке к лабораторным занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по вопросам технической защиты информации и организации защиты информации в информационных системах, по методологии защиты коммерческой тайны и конфиденциальной информации, по правовым основам защиты персональных данных, организации контроля за состоянием защиты конфиденциальной информации на предприятии, а также даются рекомендации для самостоятельной работы.

При подготовке к практическим занятиям каждый студент должен:

- изучить рекомендованную учебную литературу;
- изучить конспекты лекций;
- подготовить ответы на все вопросы по изучаемой теме.

В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя. При оформлении отчетов по выполненным практическим заданиям использовать программное обеспечение Microsoft Word: шрифт Times New Roman; размер шрифта -12; междустрочный интервал – одинарный: отступ – 1,25.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий методом устного опроса. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных источников. Выделить непонятные термины, найти их значение в энциклопедических словарях и используя профессиональную базу данных Консультант+.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными

системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.