Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Макаренко Елена Николаевна
Должность: Ректор
Дата подписания: 03.10.2022 10:57:33
Уникальный программный ключ:
c098bc0c1041cb2a4cf926cf171d6715d99a6ae00adc8e27b55cbe1e2dbd7c78

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 2018 г.

Рабочая программа дисциплины

Методы защиты информации в юриспруденции

Специальность 40.05.03 Судебная экспертиза специализация 40.05.03.04 "Экономические экспертизы"

Квалификация

Судебный эксперт

Ростов-на-Дону
2018 г.

КАФЕДРА **Информационные технологии и защита информации**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	2 (1.2)		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Практические	36	36	36	36
В том числе инт.	18	18	18	18
Итого ауд.	54	54	54	54
Контактная	54	54	54	54
Сам. работа	54	54	54	54
Итого	108	108	108	108

ОСНОВАНИЕ

Федеральный государственный образовательный стандарт высшего образования по специальности 40.05.03 Судебная экспертиза(уровень специалитета)(приказ Минобрнауки России от 28.10.2016г. №1342)

Рабочая программа составлена

Специальность 40.05.03 Судебная экспертиза специализация 40.05.03.04 "Экономические экспертизы"

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

Программу составил(и): *к.э.н., доцент, Т.Н. Шарыпова* 10.05.2018

Зав. кафедрой д.э.н., профессор, зав. кафедрой ИТиЗИ Тищенко Е.Н. 11.05.2018

Методическим советом направления *д.ю.н., профессор, А.Н. Позднышов* 24.05.2018

Отделом образовательных программ и планирования учебного процесса Торопова Т.В. 29.05.18

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, зав. кафедрой ИТиЗИ Тищенко Е.Н. _____

Программу составил(и)*к.э.н., доцент, Т.Н. Шарыпова* _____

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, зав. кафедрой ИТиЗИ Тищенко Е.Н. _____

Программу составил(и): *к.э.н., доцент, Т.Н. Шарыпова* _____

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, зав. кафедрой ИТиЗИ Тищенко Е.Н. _____

Программу составил(и): *к.э.н., доцент, Т.Н. Шарыпова* _____

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, зав. кафедрой ИТиЗИ Тищенко Е.Н. _____

Программу составил(и): *к.э.н., доцент, Т.Н. Шарыпова* _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Цель дисциплины: изучение методов и средств защиты информации в юриспруденции.
1.2	Задачи изучения дисциплины: получение теоретических знаний и практических навыков при решении типовых задач по обеспечению информационной безопасности в юриспруденции; знание проблем защиты информации, стоящих перед современной вычислительной техникой; умение использовать полученные знания для правильного выбора решений при защите юридической информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ООП:	Б1.В.ДВ.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике в объеме средней школы
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Судебно-компьютерная экспертиза
2.2.2	Практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно -исследовательской деятельности
2.2.3	Статистические методы анализа и прогнозирования в юридической деятельности
2.2.4	Методы защиты информации в юриспруденции

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Знать:

основы применения инфокоммуникационных технологий для решения задач профессиональной деятельности

Уметь:

защитить компьютерную информацию от несанкционированного разглашения

Владеть:

навыками самостоятельной работы на компьютере и в компьютерных сетях

ПК-9: способностью соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Знать:

основные термины, понятия, определения в области информационной безопасности

Уметь:

обеспечивать правовую защиту компьютерной информации в профессиональной деятельности

Владеть:

способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Интре ракт.	Примечание
	Раздел 1. Общие вопросы защиты информации в юриспруденции						

1.1	Тема 1.1 «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации". Понятие информации, защиты информации, информационной системы, безопасности автоматизированных систем обработки информации. Цель защиты информации. Базовые свойства информации: конфиденциальность, целостность, доступность. /Лек/	2	2	ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	0	
1.2	Тема 1.1 «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации. Нормативно-правовая база функционирования систем защиты информации. Российское законодательство по защите информационных технологий. Правовая защита программного обеспечения авторским правом. Компьютерные преступления и особенности их расследования. /Пр/	2	4	ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	0	
1.3	Тема 1.1 «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации". Правовая защита информации /Ср/	2	6	ПК-9	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
1.4	Тема 1.2. «Санкционированный и несанкционированный доступ». Понятие доступа к информации, субъекта и объекта доступа, санкционированного и несанкционированного доступа, нарушителя. Причины несанкционированного доступа к информации. Последствия несанкционированного доступа к информации. /Лек/	2	2	ПК-9	Л1.1 Л1.2 Л2.2 Э1 Э2	0	
1.5	Тема 1.2. «Санкционированный и несанкционированный доступ». Несанкционированный доступ к информации (НСД). Идентификация. Аутентификация. Выбор паролей. /Пр/	2	4	ОК-12	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	2	
1.6	Тема 1.2. «Санкционированный и несанкционированный доступ». Административная защита информации. /Ср/	2	6	ПК-9	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
1.7	Тема 1.3. «Понятие угрозы, уязвимости, риска». Понятие угрозы, классификация угроз. Понятие уязвимости, атаки на компьютерную систему. Понятие риска. Виды утечки информации в юриспруденции. Понятие канала утечки информации, основные каналы утечки информации. Классификация злоумышленников. /Лек/	2	2	ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	0	

1.8	Тема 1.3. «Понятие угрозы, уязвимости, риска». Технологии организации работы с информацией в среде Windows. Поиск, сохранение информации, проверка на вирусы. /Пр/	2	4	ОК-12	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	2	
1.9	Тема 1.3. «Понятие угрозы, уязвимости, риска». Уязвимость компьютерных систем. /Ср/	2	6	ПК-9	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
1.10	Тема 1.4. «Ценность информации». Понятие ценности информации. Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации /Лек/	2	2	ПК-9	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
1.11	Тема 1.4. «Ценность информации». Способы защиты информации на ПК, вирусы, антивирусные программы. /Пр/	2	4	ОК-12	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	2	
1.12	Тема 1.4. «Ценность информации». Административная защита информации . /Ср/	2	6	ПК-9	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
1.13	Тема 1.5. «Парольные системы идентификации и аутентификации пользователей». Особенности парольных систем, основные типы угроз безопасности парольных систем. Требования к выбору и использованию паролей. /Лек/	2	2	ОК-12	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	0	
1.14	Тема 1.5. «Парольные системы идентификации и аутентификации пользователей». Архиваторы. Архивы. Методы сжатия архиваторов. Сегментирование.Возможности ОС по созданию учетной записи пользователя с ограниченными правами. Порядок удаления ограниченной учетной записи. /Пр/	2	4	ОК-12	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2	4	
1.15	Тема 1.5. «Парольные системы идентификации и аутентификации пользователей». Защита электронной почты /Ср/	2	6	ПК-9	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
	Раздел 2. Методы и средства криптографической защиты						
2.1	Тема 2.1. «Принципы криптографической защиты информации». Понятие криптографии, шифрования и дешифрования, ключа шифровании, шифротекста, криптоалгоритма. Принципы функционирования криптографической системы. Классификация криптосистем. /Лек/	2	2	ОК-12	Л1.1 Л1.2 Л2.1 Э1 Э2	0	
2.2	Тема 2.1. «Принципы криптографической защиты информации». Процесс шифрования текста с помощью таблицы Вижинера. Расшифровка текста с помощью таблицы Вижинера. /Пр/	2	4	ПК-9	Л1.1 Л1.2 Л3.1 Э3	2	
2.3	Тема 2.1. «Принципы криптографической защиты информации». Таблица Вижинера. /Ср/	2	6	ОК-12	Л1.1 Л1.2 Э3	0	

2.4	Тема 2.2. «Элементы криптоанализа». Понятие криптоанализа, криптоаналитической атаки. Основные типы криптоаналитических атак, криптостойкость шифра. Требования к шифрам, используемым для криптографической защиты информации. /Лек/	2	2	ОК-12	Л1.1 Л1.2 Э3	0	
2.5	Тема 2.2. «Элементы криптоанализа». Метод встречи в середине атаки. Вероятностный метод криптоанализа. Анализ возможности возникновения коллизии. /Пр/	2	4	ПК-9	Л1.1 Л1.2 Л3.1 Э3	2	
2.6	Тема 2.2. «Элементы криптоанализа». Особенности использования вычислительной техники в криптографии. /Ср/	2	6	ОК-12	Л1.1 Л1.2 Э3	0	
2.7	Тема 2.3. «Симметричные криптосистемы». Принцип функционирования симметричных криптосистем. Функциональная схема взаимодействия участников симметричного криптографического обмена. Недостатки симметричных криптосистем. Основные виды симметричных шифров /Лек/	2	2	ОК-12	Л1.1 Л1.2 Э1	0	
2.8	Тема 2.3. «Симметричные криптосистемы». Система шифрования Цезаря. Шифры перестановки /Пр/	2	4	ПК-9	Л1.1 Л1.2 Л3.1 Э3	2	
2.9	Тема 2.3. «Симметричные криптосистемы». Шифр Гронсфельда. Шифры многоалфавитной замены. /Ср/	2	6	ОК-12	Л1.1 Л1.2 Э3	0	
2.10	Тема 2.4. «Асимметричные криптосистемы». Принцип функционирования асимметричных криптосистем, Функциональная схема взаимодействия участников асимметричного криптографического обмена. Достоинства и недостатки асимметричных криптосистем. Реализация двустороннего обмена ключевой информацией. Понятие и назначение центра распределения ключей. Требования Диффи и Хеллмана. Алгоритм шифрования RSA. Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA /Лек/	2	2	ОК-12	Л1.1 Л1.2 Л2.2 Э1	0	
2.11	Тема 2.4. «Асимметричные криптосистемы». Принципы и процедурные аспекты алгоритма электронной цифровой подписи (ЭЦП). Целостность передаваемых данных. Авторство сообщений /Пр/	2	4	ПК-9	Л1.1 Л1.2 Л3.1 Э3	2	

2.12	Тема 2.4. «Асимметричные криптосистемы». Основные математические соотношения, используемые в алгоритме RSA. Технология взлома шифра методом полного перебора. /Ср/	2	6	ОК-12	Л1.1 Л1.2 Э3	0	
2.13	/Зачёт/	2	0	ОК-12 ПК-9	Л1.1 Л1.2 Л2.1 Л2.2 Э1 Э2 Э3	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Фонд оценочных средств для проведения промежуточной аттестации

Вопросы к зачету:

1. Понятия и основные свойства информации.
2. Информатизация общества и его правовой системы, значение информатизации для юридической деятельности.
3. История возникновения ИС.
4. Структура и основные характеристики информационных систем.
5. Классы задач, решаемые с помощью компьютерных технологий
6. Основные типы специализированных информационных технологий, используемых в юридической деятельности.
7. Архитектура персонального компьютера (ПК).
8. Основные устройства ПК: назначение, основные технические характеристики.
9. Системное ПО.
10. Прикладное ПО.
11. Инструментарий программирования.
12. Текстовые редакторы: назначение и функции.
13. Назначение и возможности электронных таблиц для обработки юридической информации.
14. Программы для создания презентаций.
15. Информационные модели данных.
16. Реляционная база данных.
17. Структура базы данных.
18. Средства создания базы данных.
19. Назначение и основные возможности СПС.
20. Государственные СПС.
21. Коммерческие СПС.
22. Современные информационно-телекоммуникационные технологии и виды компьютерных сетей.
23. Локальные и глобальные компьютерные сети.
24. Топология сетей.
25. Понятие протокола.
26. Понятие защиты информации.
27. Понятие угрозы, классификация угроз.
28. Понятие уязвимости, атаки на компьютерную систему.
29. Понятие риска.
30. Виды утечки информации в юриспруденции.
31. Понятие канала утечки информации, основные каналы утечки информации.
32. Классификация злоумышленников.
33. Онтологическое понятие системы.
34. Гносеологическое понятие системы.
35. Понятие объекта, свойства объекта.
36. Понятие информации, функциональная и атрибутивная концепции.
37. Свойства информации: прагматические и атрибутивные.
38. Меры информации.
39. Понятие сигнала. Сообщение.
40. Информационные правовые порталы.
41. Роль и место информационных технологий в правовой сфере.
42. Информатизация деятельности Госдумы РФ.
43. Автоматизированные информационные системы судов и органов юстиции.
44. Основные направления информатизации согласно «Концепции правовой информатизации России».
45. Правовая информация и ее виды.
46. Автоматизированные информационные системы МВД РФ.
47. Автоматизированные информационные системы ФСБ РФ.
48. Структура и состав автоматизированных информационных систем следственной деятельности.
49. Особенности информационных систем Судебного департамента при Верховном Суде РФ.
50. Автоматизированные информационные системы Прокуратуры РФ.
51. Структура и состав автоматизированных информационных систем оперативно-розыскной деятельности.
52. Структура и состав автоматизированных информационных систем экспертной деятельности.
53. Особенности информационных систем Конституционного, Верховного и Высшего Арбитражного Судов РФ.

54.	Информационное пространство и его значение для современного общества.
55.	Современные условия информационного обеспечения деятельности судов общей юрисдикции.
56.	Конфиденциальность информации.
57.	Понятие информационного общества. Его основные характеристики.
58.	Задачи и функции информатизации судебной деятельности.
59.	История возникновения концепции информационного общества.
60.	Основные изменения в обществе, подтверждающие правомочность концепции информационного общества.

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	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учеб. пособие для студентов вузов, обучающихся по спец. "Информ. системы и технологии"	М.: Академия, 2012	20
Л1.2	Э.В. Сысоев, А.В. Селезнев, И.П. Рак, Е.В. Бурцева	Новые информационные технологии в судебной экспертизе: учебное пособие [Электронный ресурс]. - URL: //biblioclub.ru/index.php?page=book&id=277923	Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тамбовский государственный технический университет». - Тамбов, 2012	неограниченный доступ для зарегистрированных пользователей

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Хорев П. Б.	Программно-аппаратная защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. "Информ. безопасность"	М.: ФОРУМ, 2015	25
Л2.2	Савельева Н. Г., Веретенникова Е. Г.	Информатика и программирование: учеб. пособие	Ростов н/Д: Изд-во РГЭУ (РИНХ), 2016	64

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Соколов С. В., Серпенинов О. В., Тищенко Е. Н.	Криптографическая защита информации: учеб. пособие для студентов высш. учеб. заведений, обучающихся по напр. подгот. "Информ. безопасность"	Ростов н/Д: Изд-во РГЭУ "РИНХ", 2011	66

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Мельников Д. А. Информационная безопасность открытых систем: учебник. - М.: Флинта, 2012. http://biblioclub.ru/index.php?page=book_red&id=363419
Э2	Башлы П. Н., Баранова Е. К., Бабаш А. В. Информационная безопасность: учебно-практическое пособие. - Издатель: Евразийский открытый институт, 2011. http://biblioclub.ru/index.php?page=book_red&id=90539&sr=1
Э3	Введение в криптографию: сборник задач и упражнений Автор: Кукина Е. Г., Романьков В. А. - Издательство: Омский государственный университет, 2013. http://biblioclub.ru/index.php?page=book&id=237674

6.3. Перечень программного обеспечения

6.3.1	MicrosoftOffice

6.4 Перечень информационных справочных систем

6.4.1	Консультант+
6.4.2	Гарант

6.4.3	Кодекс

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.

8. МЕТОДИЧЕСТКИЕ 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 Информационных
технологий и защиты информации
Протокол № 10 от «11» мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Методы защиты информации в юриспруденции

(наименование дисциплины)

Специальность

40.05.03 Судебная экспертиза

Специализация

Экономические экспертизы

Уровень образования

специалитет

Составитель _____ Шарыпова Т.Н., доцент, к.э.н.

(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

1.1 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-12 – способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации			
З: основы применения инфокоммуникационных технологий для решения задач профессиональной деятельности	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных	С – собеседование

		работы (в полном, не полном объеме); соответствие отчета требованиям	
У: защитить компьютерную информацию от несанкционированного разглашения	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям	С – собеседование
В: навыками самостоятельной работы на компьютере и в компьютерных сетях	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной	С – собеседование

	информационных ресурсов	литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям	
ПК-9 – способность соблюдать в профессиональной деятельности требования правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности			
З: основные термины, понятия, определения в области информационной безопасности	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет;	С – собеседование

		обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям	
У: обеспечивать правовую защиту компьютерной информации в профессиональной деятельности	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям	С – собеседование

В: способностью сознавать опасности и угрозы, возникающие в развитии современного информационного общества	поиск и сбор необходимой литературы, использование различных баз данных, использование современных информационно-коммуникационных технологий и глобальных информационных ресурсов	соответствие проблеме исследования; полнота и содержательность ответа; умение приводить примеры; умение отстаивать свою позицию; умение пользоваться дополнительной литературой при подготовке к занятиям; соответствие представленной в ответах информации материалам лекции и учебной литературы, сведениям из информационных ресурсов Интернет; обоснованность обращения к базам данных; целенаправленность поиска и отбора; объем выполненных работы (в полном, не полном объеме); соответствие отчета требованиям	С – собеседование

2.2 Шкалы оценивания:

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

50-100 баллов (зачет) - 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 (незачет) 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

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

Кафедра Информационных технологий и защиты информации
(наименование кафедры)

Вопросы к зачету

по дисциплине **Методы защиты информации в юриспруденции**
(наименование дисциплины)

1. Информация как объект защиты. Цели защиты информации.
2. Информационная безопасность. Понятие. Аспекты. Угрозы информационной безопасности.
3. Защита информации. Основные термины и определения. Последствия нарушения безопасности.
4. Три базовых аспекта информационной безопасности. Доступность, целостность и конфиденциальность.
5. Угрозы безопасности информации. Классификация угроз.
6. Виды типичных атак на информационную систему.
7. Несанкционированный доступ и утечка информации. Классификация каналов несанкционированного доступа.
8. Методы и средства информационной защиты. Определение и система мер, направленных на обеспечение информационной безопасности.
9. Уровни системы защиты информации.
10. Основные принципы формирования политики информационной безопасности. Организация доступа к информационным ресурсам.
11. Анализ рисков нарушения защиты информации. Ущерб, вероятность атаки, таблица рисков.
12. Программные средства оценки рисков. Этапы осуществления анализа в системе ГРИФ.
13. Правовое обеспечение защиты информации с ограниченным доступом.
14. Информационное право и информационные отношения. Основные положения Конституции России в области защиты информации.
15. Основные понятия и структура Федерального Закона Российской Федерации «Об информации, информатизации и защите информации».

16. Режимные ограничения на доступ к информационным ресурсам. Задачи, решаемые при ограничении доступа.
17. Классификация информации с ограниченным доступом. Государственная, коммерческая и банковская тайны.
18. Преступления в сфере компьютерной безопасности. Положения ст. ст. 272, 273 и 274 УК РФ.
19. Организационные (неформальные) методы защиты информации, особенности их использования.
20. Принципы организации работ по защите информации. Перечень организационных мер.
21. Компьютерные вирусы: основные понятия.
22. Файловые вирусы и схемы их функционирования.
23. Полиморфные вирусы и схемы их функционирования.
24. Пути проникновения вирусов в компьютер.
25. Механизм распределения вирусных программ.
26. Способы несанкционированного доступа к информации.
27. Аутентификация пользователей на основе паролей и модели «рукопожатия».
28. Аутентификация пользователей по их биометрическим характеристикам, клавиатурному почерку и росписи мышью.
29. Аутентификация пользователей при удаленном доступе.
30. Физические средства охраны объектов информатизации.
31. Возможные воздействия при физическом доступе.
32. Предотвращение утечки информации за счет побочных электромагнитных излучений и наводок..
33. Основные понятия криптологии.
34. Криптография и криптоанализ.
35. Задачи криптографии. Основные термины и определения.
36. Криптограмма, шифр, ключ.
37. Криптосистемы с секретным ключом.
38. Криптосистемы с секретным ключом.
39. Криптосистемы с открытым ключом.
40. Алгоритм шифрования RSA.
41. Системы аутентификации электронных данных.
42. Загрузочные вирусы и схемы их функционирования.

Критерии оценки:

50-100 баллов (зачет) - 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 (незачет) 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».

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

Кафедра Информационных технологий и защиты информации

Вопросы для собеседования

по дисциплине **Методы защиты информации в юриспруденции**

Модуль 1 Общие вопросы защиты информации в юриспруденции

Тема 1.1. «Понятие защиты информации в юриспруденции. Базовые свойства безопасности информации».

1.Понятие информации.

2. Понятие защиты информации.

3. Понятие информационной системы.

4. Понятие безопасности автоматизированных систем обработки информации.

5.Цель защиты информации.

6.Базовые свойства информации: конфиденциальность, целостность, доступность.

Тема 1.2. «Санкционированный и несанкционированный доступ».

1.Понятие доступа к информации.

2. Понятие субъекта и объекта доступа.

3.Понятие санкционированного и несанкционированного доступа.

4. Понятие нарушителя.

5.Причины несанкционированного доступа к информации.

6. Последствия несанкционированного доступа к информации.

Тема 1.3. «Понятие угрозы, уязвимости, риска».

1.Понятие угрозы, классификация угроз.

2.Понятие уязвимости, атаки на компьютерную систему.

3.Понятие риска.

4.Виды утечки информации в юриспруденции.

5.Понятие канала утечки информации. Основные каналы утечки информации.

6.Классификация злоумышленников.

Тема 1.4. «Ценность информации».

1.Понятие ценности информации.

2.Основные подходы к построению моделей защиты информационных систем, основанные на понятии ценности информации.

Тема 1.5. «Парольные системы идентификации и аутентификации пользователей».

1.Особенности парольных систем.

2. Основные типы угроз безопасности парольных систем.

3.Требования к выбору и использованию паролей.

Модуль 2. Методы и средства криптографической защиты.

Тема 2.1. «Принципы криптографической защиты информации».

1. Понятие криптографии.
2. Понятие шифрования и дешифрования,
3. Понятие ключа шифровании, шифротекста,
4. Понятие криптоалгоритма.
5. Принципы функционирования криптографической системы.
6. Классификация криптосистем.

Тема 2.2. «Элементы криптоанализа».

1. Понятие криптоанализа,
2. Понятие криптоаналитической атаки.
3. Основные типы криптоаналитических атак.
4. Криптостойкость шифра.

5.Требования к шифрам, используемым для криптографической защиты информации.

Тема 2.3. «Симметричные криптосистемы».

1.Принцип функционирования симметричных криптосистем.

2.Функциональная схема взаимодействия участников симметричного криптографического обмена.

3.Недостатки симметричных криптосистем.

4.Основные виды симметричных шифров.

Тема 2.4. «Асимметричные криптосистемы».

1.Принцип функционирования асимметричных криптосистем.

2. Функциональная схема взаимодействия участников асимметричного криптографического обмена.

3.Достоинства и недостатки асимметричных криптосистем.

4.Реализация двустороннего обмена ключевой информацией.

5.Понятие и назначение центра распределения ключей.

6.Требования Диффи и Хеллмана.

7.Алгоритм шифрования RSA.

8.Процесс формирования ключевой пары получателем, шифрование и дешифрование сообщений в криптосистеме RSA.

Критерии оценки:

- оценка «зачтено» - изложение ответов с отдельными ошибками, уверенно исправленными после дополнительных вопросов;

- оценка «не зачтено» - ответы не связаны с вопросами, наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса и неточность ответов на дополнительные и наводящие вопросы».

4 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. 3 данного приложения. Результаты текущего контроля доводятся до сведения студентов до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по окончании теоретического обучения до начала экзаменационной сессии.

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 Информационных
технологий и защиты информации
Протокол № 10 от «11» мая 2018 г.
Зав.кафедрой _____ *Тищенко Е.Н.*

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Методы защиты информации в юриспруденции
(наименование дисциплины)

Специальность

40.05.03 Судебная экспертиза

Специализация

Экономические экспертизы

Уровень образования
специалитет

Составитель _____ Шарыпова Т.Н., доцент, к.э.н.
(подпись) *Ф.И.О., должность, ученая степень, ученое звание*

Ростов-на-Дону, 2018

Методические указания по освоению дисциплины «Методы защиты информации в юриспруденции» адресованы студентам очной формы обучения.

Учебным планом по специальности «Судебная экспертиза» предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

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

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки практической работы по защите информации в юриспруденции.

При подготовке к практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

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

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 первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему практическому занятию 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 и семинарских занятий;
- интерактивная доска для подготовки и проведения лекционных и занятий.

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.