МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Филиал в г. Хасавюрте

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Информационная безопасность»

наименование дисциплины / модуля

Кафедра юридических дисциплин

(наименование кафедры, обеспечивающей преподавание дисциплины)

Образовательная программа

40.03.01. Юриспруденция

(код и наименование направления/специальности)

Профиль подготовки
уголовно-правовой

наименование профиля подготовки

Уровень высшего образования
Бакалавриат

(бакалавриат, специалитет, магистратура)

Форма обучения
Очная, очно-заочная

(очная, очно-заочная, заочная)

Статус дисциплины: **вариативная по выбору**

(базовая, вариативная, вариативная по выбору)

Хасавюрт -2020

Фонд оценочных средств по дисциплине «Информационная безопасность» составлен в 2020 году в соответствии с требованиями ФГОС ВО по направлению подготовки 40.03.01. Юриспруденция (уровень бакалавриата) 1 декабря 2016 г. № 1511

Разработчик(и): кафедра юридических дисциплин, Дадаев Д.Х., к.ф.-м.н.

Фонд оценочных средств по дисциплине «Информационная безопасность» одобрен:

на заседании кафедры юридических дисциплин от «26» марта 2020 г. протокол №7

Зав. кафедрой _____ Р.М.Касумов

(подпись)

на заседании учебно-методической комиссии филиала ДГУ в г. Хасавюрте протокол №7 от «26» марта 2020 года.

Председатель _____ А. М. Шахбанов

(подпись)

1. ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине

«Информационная безопасность»

наименование дисциплины

1.1. Основные сведения о дисциплине

Общая трудоемкость дисциплины составляет 1 зачетная единица (36 академических часов).

Очная форма обучения

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**36**	**36**
Контактная работа:	**24**	**24**
Лекции (Л)	12	12
Практические занятия (ПЗ)	12	12
Контроль	-	-
Промежуточная аттестация	-	-
Самостоятельная работа: *- контрольная работа* *- написание реферата (Р);* *- самостоятельное изучение разделов:* *Модуль 1.* *Модуль 2.* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям.*	**12** *4* *2* *2* *2* *2*	**12** *4* *2* *2* *2* *2*
Вид итогового контроля: зачет		

Очно-заочная форма обучения

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**36**	**36**
Контактная работа:	**24**	**24**
Лекции (Л)	12	12
Практические занятия (ПЗ)	12	12
Контроль	-	-
Промежуточная аттестация	-	-
Самостоятельная работа:	**12**	**12**

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
- контрольная работа *- написание реферата (Р);* *- самостоятельное изучение разделов:* *Модуль 1.* *Модуль 2.* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- подготовка к практическим занятиям.*	*2* *3* *3* *2* *2*	*2* *3* *3* *2* *2*
Вид итогового контроля: зачет		

1.2. Требования к результатам обучения по дисциплине, формы их контроля и виды оценочных средств

№ п/п	Контролируемые модули, разделы (темы) дисциплины	Индекс контролируемой компетенции (или её части)	Оценочные средства		Способ контроля
			наименование	№№ заданий	
Модуль 1					
1.	Тема 1. Понятие "информационная безопасность". Проблема информационной безопасности общества. Составляющие информационной безопасности.	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	1-10	Устно
2.	Тема 2. Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности Нормативно-правовые основы информационной безопасности в РФ.	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	11-22	Устно

3.	Тема 3. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Функциональные требования, требования доверия	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	23-27	Устно
4.	Тема 4. Стандарты информационной безопасности в РФ. Федеральная служба по техническому и экспортному контролю и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	28-37	Устно
Модуль 2					
5.	Тема 5. Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности. Классификация угроз "информационной безопасности". Каналы	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	38-43	Устно

	несанкционированного доступа к информации.				
6.	Тема 6. Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов. Классификация компьютерных вирусов	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	44-54	Устно
7.	Тема 7. Антивирусные программы, особенности их работы. Классификация антивирусных программ, факторы, определяющие их качество.	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	55-66	Устно
8.	Тема 8. Классификация удаленных угроз в вычислительных сетях, их характеристика. Механизмы обеспечения "информационной безопасности».	ОК-3, ПК-6, ПК-15, ПК-16	Контрольный опрос	67-84	Устно

1.3. Показатели и критерии определения уровня сформированности компетенций

№ п/п	Индекс компетенции	Уровни сформированности компетенции			
		Недостаточный	Удовлетворительный (достаточный)	Базовый	Повышенный
1.	ОК-3	Отсутствие признаков удовлетворительного уровня	**Обучающийся демонстрирует слабое знание** основных закономерностей создания и функционирования	**У обучающегося выработано хорошее знание** закономерностей создания и функционирования информационных	**Обучающийся отличное знает** основные закономерности создания и функционирования информационных

			информационных процессов в правовой сфере. **Наблюдается слабое умение** применять современные информационные технологии для поиска и обработки правовой информации **Обучаемый владеет на достаточном** навыками сбора и обработки правовой информации	процессов в правовой сфере. **Демонстрирует уверенное умение** применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов. **Демонстрирует хорошее владение** навыками сбора и обработки информации, имеющей значение для реализации правовых норм	процессов в профессиональной деятельности. **Выработано устойчивое умение** применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации. **Демонстрирует отличное владение** навыками сбора и обработки информации, имеющей значение для реализации правовых норм в соответствующих сферах профессиональной деятельности.
2.	ПК-6	Отсутствие признаков удовлетворительного уровня	**Демонстрирует слабое знание** понятий, видов и способов квалификаций фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности, с точки зрения разных авторов на проблемные вопросы **Демонстрирует слабое умение** правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств. **Демонстрирует слабое владение** юридической	**Демонстрирует хорошее знание** понятий, видов и способов квалификаций фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности, с точки зрения разных авторов на проблемные вопросы **Демонстрирует хорошее умение** правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации	**Демонстрирует отличное знание** понятий, видов и способов квалификаций фактов и обстоятельств, этапы юридической квалификации, содержание источников информационной безопасности, с точки зрения разных авторов на проблемные вопросы **Демонстрирует отличное умение** правильно давать юридическую оценку фактам и обстоятельствам, обоснованно применять нормы права при правовой квалификации обстоятельств. **Демонстрирует**

			терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства	обстоятельств. **Демонстрирует хорошее владение** юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства	**отличное владение** юридической терминологией отраслей права, позволяющей юридически правильно квалифицировать факты и обстоятельства
3.	ПК-15	Отсутствие признаков удовлетворительного уровня	**Демонстрирует слабое знание** понятий, видов и способов толкования правовых норм **Демонстрирует слабое умение** анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств **Демонстрирует слабое владение** навыками работы по толкованию правовых норм.	**Демонстрирует хорошее знание** понятий, видов и способов толкования правовых норм **Демонстрирует хорошее умение** анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств **Демонстрирует хорошее владение** навыками работы по толкованию правовых норм.	**Демонстрирует отличное знание** понятий, видов и способов толкования правовых норм **Демонстрирует отличное умение** анализировать содержание правовых норм, использовать различные приемы толкования для уяснения точного смысла нормы при квалификации фактов и обстоятельств **Демонстрирует отличное владение** навыками работы по толкованию правовых норм.
4.	ПК-16	Отсутствие признаков удовлетворительного уровня	**Демонстрирует слабое знание** содержания нормативных правовых актов. **Демонстрирует слабое умение** осуществлять правовую экспертизу нормативных правовых актов - принимать решения и совершать юридические действия в точном соответствии с законом. **Демонстрирует слабое владение** навыками принятия необходимых мер защиты прав человека и гражданина	**Достаточно уверенно демонстрирует знание** содержания нормативных правовых актов в профессиональной деятельности. **Уверенно умеет** осуществлять правовую экспертизу нормативных правовых актов - принимать решения и совершать юридические действия в точном соответствии с законом. **Демонстрирует хорошее владение**	**Демонстрирует отличное знание** содержания нормативных правовых актов в профессиональной деятельности. **Демонстрирует отличное умение** осуществлять правовую экспертизу нормативных правовых актов - принимать решения и совершать юридические действия в точном соответствии с законом. **Демонстрирует отличное владение** навыками принятия

				навыками принятия необходимых мер защиты прав человека и гражданина	необходимых мер защиты прав человека и гражданина

2. КОНТРОЛЬНЫЕ ЗАДАНИЯ И ИНЫЕ МАТЕРИАЛЫ ОЦЕНКИ знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения дисциплины «Информационная безопасность»

Перечень контрольных вопросов

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Какие определения информационной безопасности приводятся в "Концепции информационной безопасности сетей связи общего пользования Российской Федерации"?
4. Что понимается под "компьютерной безопасностью"?
5. Составляющие информационной безопасности.
6. Перечислите составляющие информационной безопасности.
7. Приведите определение доступности информации.
8. Приведите определение целостности информации.
9. Приведите определение конфиденциальности информации.
10. Каким образом взаимосвязаны между собой составляющие информационной безопасности?
11. Перечислите задачи информационной безопасности общества.
12. Перечислите уровни формирования режима информационной безопасности.
13. Дайте краткую характеристику законодательно-правового уровня.
14. Какие подуровни включает программно-технический уровень?
15. Что включает административный уровень?
16. В чем особенность морально-этического подуровня?
17. Перечислите основополагающие документы по информационной безопасности.
18. Понятие государственной тайны.
19. Что понимается под средствами защиты государственной тайны?
20. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.
21. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?
22. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?
23. Какие виды требований включает стандарт ISO/IEC 15408?

24. Чем отличаются функциональные требования от требований доверия?
25. В чем заключается иерархический принцип "класс – семейство – компонент – элемент"?
26. Какова цель требований по отказоустойчивости информационных систем?
27. Сколько классов функциональных требований?
28. Дайте характеристику составляющих "информационной безопасности" применительно к вычислительным сетям.
29. Перечислите основные механизмы безопасности.
30. Какие механизмы безопасности используются для обеспечения конфиденциальности трафика?
31. Какие механизмы безопасности используются для обеспечения "неотказуемости" системы?
32. Что понимается под администрированием средств безопасности?
33. Какие виды избыточности могут использоваться в вычислительных сетях?
34. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
35. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?
36. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".
37. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?
38. Цели и задачи административного уровня обеспечения информационной безопасности.
39. Содержание административного уровня.
40. Дайте определение политики безопасности.
41. Направления разработки политики безопасности.
42. Перечислите составные элементы автоматизированных систем.
43. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
44. Перечислите классы угроз информационной безопасности.
45. Назовите причины и источники случайных воздействий на информационные системы.
46. Дайте характеристику преднамеренным угрозам.
47. Перечислите каналы несанкционированного доступа.
48. В чем особенность "упреждающей" защиты в информационных системах.
49. Перечислите классификационные признаки компьютерных вирусов.
50. Охарактеризуйте файловый и загрузочный вирусы.

51. В чем особенности резидентных вирусов?
52. Сформулируйте признаки стелс-вирусов.
53. Перечислите деструктивные возможности компьютерных вирусов.
54. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
55. Поясните понятия "сканирование налету" и "сканирование по запросу".
56. Перечислите виды антивирусных программ.
57. Охарактеризуйте антивирусные сканеры.
58. Принципы функционирования блокировщиков и иммунизаторов.
59. Особенности CRC-сканеров.
60. В чем состоят особенности эвристических сканеров?
61. Какие факторы определяют качество антивирусной программы?
62. Особенности обеспечения информационной безопасности компьютерных сетей.
63. Дайте определение понятия "удаленная угроза".
64. Основные цели информационной безопасности компьютерных сетях.
65. В чем заключается специфика методов и средств защиты компьютерных сетей?
66. Поясните понятие "глобальная сетевая атака", приведите примеры.
67. Перечислите классы удаленных угроз.
68. Как классифицируются удаленные угрозы "по характеру воздействия"?
69. Охарактеризуйте удаленные угрозы "по цели воздействия".
70. Как классифицируются удаленные угрозы "по расположению субъекта и объекта угрозы"?
71. Дайте определение маршрутизатора.
72. Что такое подсеть и сегмент сети? Чем они отличаются?
73. Может ли пассивная угроза привести к нарушению целостности информации?
74. Что понимается под идентификацией пользователя?
75. Что понимается под аутентификацией пользователей?
76. Применим ли механизм идентификации к процессам? Почему?
77. Перечислите возможные идентификаторы при реализации механизма идентификации.
78. Перечислите возможные идентификаторы при реализации механизма аутентификации.
79. Какой из механизмов (аутентификация или идентификация) более надежный? Почему?
80. В чем особенности динамической аутентификации?
81. Опишите механизм аутентификации пользователя.
82. Что такое "электронный ключ"?
83. Перечислите виды аутентификации по уровню информационной безопасности.
84. Какой из видов аутентификации (устойчивая аутентификация или постоянная аутентификация) более надежный?

Критерии оценки:

- оценка «отлично» выставляется студенту, если студент глубоко понимает изученный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности;
- оценка «хорошо»» выставляется студенту, если студент хорошо понимает изученный материал, но не может теоретически обосновывать некоторые выводы;
- оценка «удовлетворительно» выставляется студенту, если в ответе студента имеются существенные недостатки, изученный материал охвачен «половинчато», в рассуждениях допускаются ошибки;
- оценка «неудовлетворительно выставляется студенту, если в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

Вопросы к зачету

1. Понятие "информационная безопасность".
2. Проблема информационной безопасности общества.
3. Составляющие информационной безопасности. Доступность, целостность, конфиденциальность.
4. Система формирования режима информационной безопасности. Уровни формирования режима информационной безопасности
5. Нормативно-правовые основы информационной безопасности в РФ. Правовые основы информационной безопасности общества.
6. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации.
7. Ответственность за нарушения в сфере информационной безопасности.
8. Стандарты информационной безопасности: "Общие критерии". Требования безопасности к информационным системам. Функциональные требования, требования доверия.
9. Стандарты информационной безопасности распределенных систем. Сервисы безопасности в вычислительных сетях.
10. Механизмы безопасности.
11. Администрирование средств безопасности.
12. Стандарты информационной безопасности в РФ.
13. Федеральная служба по техническому и экспортному контролю и ее роль в обеспечении информационной безопасности в РФ.
14. Документы по оценке защищенности автоматизированных систем в РФ.
15. Административный уровень обеспечения информационной безопасности. Разработка политики информационной безопасности.
16. Классификация угроз "информационной безопасности".
17. Каналы несанкционированного доступа к информации.

18. Вирусы как угроза информационной безопасности. Характерные черты компьютерных вирусов.
19. Классификация компьютерных вирусов по среде обитания, по особенностям алгоритма работы, по деструктивным возможностям.
20. Характеристика "вирусоподобных" программ.
21. Антивирусные программы, особенности их работы. Классификация антивирусных программ, факторы, определяющие их качество.
22. Особенности обеспечения информационной безопасности в компьютерных сетях.
23. Специфика средств защиты в компьютерных сетях.
24. Транспортный протокол TCP и модель TCP/IP. Основы IP-протокола.
25. Система доменных имен.
26. Классификация удаленных угроз в вычислительных сетях, их характеристика.
27. Механизмы обеспечения "информационной безопасности».
28. Определение понятий "идентификация" и "аутентификация". Механизм идентификации и аутентификации пользователей.

Критерии оценки:

Ответы на все вопросы на зачете оцениваются максимум 100 баллами.

- 100 баллов - студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в логической последовательности.

- 90 баллов - студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

- 80 баллов - студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновывать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

- 70 баллов - студент хорошо понимает пройденный материал, но не может теоретически обосновывать некоторые выводы.

- 60 баллов - студент отвечает в основном правильно, но чувствуется механическое заучивание материала.

- 50 баллов - в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки.

- 40 баллов - ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

- 20 - 30 баллов - студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

-10 баллов - студент имеет лишь частичное представление о теме.

-0 баллов - нет ответа.

Таблица перевода рейтингового балла по дисциплине

в «зачтено» или «не зачтено»

Итоговая сумма баллов по дисциплине по 100-балльной шкале	Оценка по дисциплине
0-50	Не зачтено
51-100	Зачтено