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

Институт права и национальной безопасности
Кафедра основ правоохранительной деятельности

УТВЕРЖДЕНА

на заседании кафедры основ правоохранительной деятельности
протокол от 6 июня 2019 г. № 5

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.07.01Уголовная ответственность в информационной сфере
(индекс, наименование дисциплины, в соответствии с учебным планом)

40.03.01 Юриспруденция
(код, наименование направления подготовки)

Информационно-правовой профиль (Правовое обеспечение цифровой экономики)
(направленность (профиль))

Бакалавр
(квалификация)

Очная
(форма(ы) обучения)

Москва, 2019 г.

Автор(ы)–составитель(и):
д.ю.н. профессор А.П. Дмитренко

Заведующий кафедрой
основ правоохранительной деятельности к.ю.н. доцент А.К.Романов

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы
2. Объем дисциплины в зачетных единицах с указанием количества академических и астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся и место дисциплины в структуре образовательной программы
3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических и астрономических часов, видов учебных занятий и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине
5. Методические указания для обучающихся по освоению дисциплины
6. Основная и дополнительная учебная литература, необходимая для освоения дисциплины, ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
7. Материально-техническая база, информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости

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

1.1. Дисциплина Б1.В.ДВ.07.01Уголовная ответственность в информационной сфере обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-6	способность юридически правильно квалифицировать факты и обстоятельства	ПК-6.1.5	Способность юридически грамотно толковать и интерпретировать факты и обстоятельства, с которыми закон связывает возникновение правоотношений, а также осуществлять на их основе планирование и организацию исследовательской работы.
ПК-7	владение навыками подготовки юридических документов	ПК-7.1.6	Способность подготовить нормативные акты, юридические документы применительно к различным сферам профессиональной деятельности и на основе их подготовить исследовательский проект.
ПК-16	способностью давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности	ПК-16.2.4	Способность применять различные методики и модели ведения юридической консультации, в том числе с целью организации и систематизации результатов исследовательской работы.

Примечание:

Таблица заполняется в соответствии с Приложением 1 («паспорта компетенций») и Приложением 2 (схема освоения компетенций).

В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ[1] *(при наличии профстандарта)*/трудовые /профессиональные действия	Код этапа освоения компетенции	Результаты обучения
		на уровне знаний *(только для учебной*

1. [1] Столбец вводится только для ПК, при необходимости для ОПК, СПК, ДПК и только для ОП ВО, реализуемых на основе ОС.

		практики):
		на уровне умений *(типовые действия выполняются по заданному алгоритму)*:
		на уровне навыков *(типовые действия выполняются автоматически, без воспроизведения алгоритма):*
		на уровне знаний:
		на уровне умений:
		на уровне навыков:

Заполняются только те результаты обучения, которые планируется сформировать в рамках дисциплины. Отдельные уровни могут не указываться.

2. Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся и место дисциплины в структуре образовательной программы

Объем дисциплины

Общая трудоемкость дисциплины составляет 72 а.ч. (2 з.е.)

Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся: 40 а.ч., в том числе:

- лекции – 16 а.ч., практические занятия – 24 а.ч., самостоятельная работа – 32 а.ч.

Место дисциплины в структуре ОП ВО

Указывается:

– дисциплина Б1.В.ДВ.07.01Уголовная ответственность в информационной сфере реализуется на 4 курсе в 8 семестре.

– дисциплина реализуется после изучения:

Б1.Б.01 Философия, Б1.Б.02 Профессиональная этика, Б1.Б.05 Теория государства и права, Б1.Б.06 История государства и права России, Б1.Б.07 История государства и права зарубежных стран, Б1.Б.08 Экономика, Б1.Б.09 Информационные технологии в юридической деятельности, Б1.Б.13 Административное право, Б1.Б.11 Криминология, Б1.Б.14 Уголовное право, Б1.Б.17 Гражданское право, Б1.Б.18 Гражданский процесс, Б1.Б.19 Финансовое право, Б1.Б.20 Трудовое право, Б1.Б.21 Право социального обеспечения, Б1.Б.22 Земельное право, Б1.Б.23 Налоговое право, Б1.Б.24 Семейное право, Б1.В.02 Правоохранительные органы, Б1.В.08 Права граждан в информационной сфере, Б1.В.10 Правовое обеспечение информационной безопасности, Б1.В.12 Юридическая ответственность в информационной сфере.

3. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий и структура дисциплины

Структура дисциплины

№ п/п	Наименование тем	Объем дисциплины, час.	Форма

	(разделов)	Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	текущего контроля успеваемости[4], промежуточной аттестации
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Понятие, виды и меры уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий.	8	2		4		2	О Т КЗ
Тема 2	Понятие, уголовно-правовая характеристика и классификация киберпреступлений.	18	4		8		6	О Т КЗ
Тема 3	Уголовная ответственность за преступления против личности, совершаемые с использованием информационно-коммуникационных технологий.	16	4		4		8	О Т КЗ
Тема 4	Уголовная ответственность за преступления против собственности, совершаемые с использованием информационно-коммуникационных технологий.	16	4		4		8	О Т КЗ
Тема 5	Уголовная ответственность за преступления в сфере экономической деятельности, совершаемые с использованием информационно-коммуникационных технологий.	14	2		4		8	О Т КЗ
Промежуточная аттестация		зачет						
Всего:		**72**	**16**		**24**		**32**	

Примечание: 1 – формы текущего контроля успеваемости: кейс-задание (КЗ), ситуационные задачи (СЗ), тесты (Т), О – опрос

Содержание дисциплины

Тема 1. Понятие, виды и меры уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий

Понятие уголовной ответственности. Виды уголовной ответственности. Система мер уголовно-правового характера. Уголовно-правовое понятие информационной сферы. Позитивная и негативная ответственность в информационной сфере. Социальная обусловленность и задачи уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий. Источники (формы) уголовного права по вопросам ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий. Дифференциация и индивидуализация уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (киберпреступлений).

Тема 2. Понятие, уголовно-правовая характеристика и виды киберпреступлений

Понятие киберпреступления. Уголовно-правовая классификация киберпреступлений. Объекты киберпреступлений. Уголовно-правовая классификация киберпреступелний. Юридическая природа и понятие IT-технологий в составах киберпреступлений. Задачи и особенности квалификации киберпреступлений.

Неправомерный доступ к компьютерной информации. Неправомерный доступ к компьютерной информации, осуществляемый с помощью вредоносных программ. Неправомерный доступ к информации, осуществляемый с помощью иной компьютерной информации. Неправомерный доступ к компьютерной информации, осуществляемый с использованием аппаратных высокотехнологичных средств. Преступные последствия неправомерного доступа к компьютерной информации: понятие и виды. Квалифицирующие признаки неправомерного доступа к компьютерной информации. Создание, использование и распространение вредоносных компьютерных программ. Основные виды вредоносных компьютерных программ. Компьютерные вирусы в исторической перспективе. Наиболее опасные из современных видов вирусных программ, механизм их действия. Троянские программы: отличие от вирусов, механизм их действия. Иная компьютерная информация как средство совершения преступления. Нейтрализация средств защиты компьютерной информации как специфическое деяние, способы и средства его совершения. Квалифицирующие признаки создания, использования и распространения вредоносных компьютерных программ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Основные способы и средства совершения такого рода преступных деяний. Информация как предмет киберпреступления. Неправомерное воздействие на критическую информационную инфраструктуру РФ. Понятие критической информационной инфраструктуры РФ. Объективные им субъективные признаки неправомерного воздействия на критическую информационную инфраструктуру РФ. Квалифицирующие признаки неправомерного воздействия на критическую информационную инфраструктуру РФ.

Тема 3. Уголовная ответственность за преступления против личности, совершаемые с использованием информационно-коммуникационных технологий

Доведение до самоубийства, совершенное с использованием сети Интернет. Склонение к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети. Организация деятельности, направленной на побуждение к совершению самоубийства. Угроза убийством, совершаемая с использованием киберсредств и вопросы ее квалификации. Торговля людьми, совершаемая с использованием информационно-

телекоммуникационных сетей. Клевета, осуществляемая с использованием информационно-телекоммуникационных сетей и сетевых ресурсов. Развратные действия, совершаемые путем использования ресурсов сети Интернет. Нарушение неприкосновенности частной жизни, совершенное путем использования информационно-телекоммуникационных технологий. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенные с использованием киберсредств. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации, осуществляемый через информационно-телекоммуникационные сети. Нарушение авторских и смежных прав, совершенное с использованием киберсредств. Нарушение изобретательских и патентных прав, совершенное с использованием информационно-телекоммуникационных технологий. Вовлечение несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

Тема 4. Уголовная ответственность за преступления против собственности, совершаемые с использованием информационно-коммуникационных технологий

Уголовная ответственность за кражи, совершаемые из электронных банковских сетей и с использованием электронных платежных систем. Уголовная ответственность за мелкое хищение, совершенное лицом, подвергнутым административному наказанию, совершенное с использованием информационно-телекоммуникационных сетей путем обмана или злоупотребления доверием.

Уголовная ответственность за мошенничество с использованием электронных средств платежа и с применением IT-технологий. Мошенничество в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств). Спам: понятие, вопросы квалификации и уголовной ответственности за причиненный вред.

Тема 5. Уголовная ответственность за преступления в сфере экономической деятельности, совершаемые с использованием информационно-коммуникационных технологий

Уголовная ответственность за незаконное предпринимательство, совершаемое с использованием информационно-телекоммуникационных сетей. Незаконные организация и проведение азартных игр, совершаемые с использованием сети Интернет и иных информационно-телекоммуникационных сетей. Незаконная банковская деятельность, осуществляемая посредством использования информационно-телекоммуникационных сетей и иных киберсредств. Манипулирование рынком, осуществляемое с использованием информационно-телекоммуникационных сетей. Неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.

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.

4.1.1. В ходе реализации дисциплины *Б1.В.ДВ.07.01Уголовная ответственность в информационной сфере* используются следующие методы текущего контроля успеваемости обучающихся:

При проведении занятий лекционного типа: опрос.

при проведении занятий семинарского типа:

опрос, тест, ситуационные задачи, кейс-задания.
при контроле результатов самостоятельной работы студентов:
тестирование, решение ситуационных задач.

4.1.2. Зачет проводится с применением следующих методов (средств):

Указываются методы (средства, применяемые для выявления уровня освоения компетенции (устная, письменная с применением (на основе) компьютерного тестирования и т.п):

Устный ответ на вопросы зачета, собеседование по вопросам преподавателя.

4.2. Материалы текущего контроля успеваемости обучающихся

Типовые оценочные материалы

По теме 1

Вопросы к опросу:

1. Соотношение понятий киберпреступность и киберпреступление.
2. Объекты киберпреступлений.
3. Задачи и особенности квалификации киберпреступлений.
4. Проблемы дифференциации и индивидуализации уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (киберпреступлений).

Тестовые задания:

1. Киберпреступление - это

1) любое преступление, совершаемое в сфере компьютерной информации или с использованием IT-технологий, совершенное при помощи компьютерной системы или телекоммуникационной сети или против них;
2) хищение компьютерных программ;
3) хищение компьютерной техники;
4) хищение или уничтожение компьютерной информации.

2. Особенностями киберпреступлений являются:

1) чрезвычайная скрытность деяний, которая достигается применением механизмов анонимности и шифрования;
2) трансграничность, преступник и жертва могут быть разделены тысячами километров, границами нескольких государств;
3) нестандартность способов совершения;
4) автоматизированный режим;
5) все выше перечисленные признаки.

3. В УК РФ компьютерная информация - это:

1) сведения (сообщения, данные), представленные в форме электрических сигналов и изображений на бумажных носителях, независимо от средств их хранения, обработки и передачи;
2) сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи;
в) только сведения (сообщения, данные) о ЭВМ и их сетях;
3) только сведения (сообщения, данные), представленные в форме электрических сигналов и содержащих государственную тайну.

Ситуационные задачи и кейс задания:

Задание 1

Определите основание уголовно-правовой классификации киберпреступлений.

Задание 2

Определите особенности и юридические признаки киберпреступления.

Задание 3

Проанализируйте международно-правовые акты в сфере уголовной ответственности и борьбы с киберпреступлениями.

По теме 2

Вопросы к опросу:

1. Понятие киберпреступления.
2. Уголовно-правовая характеристика и виды киберпреступлений.
3. Неправомерный доступ к компьютерной информации: способы, квалифицирующие признаки.
4. Создание, использование и распространение вредоносных компьютерных программ: виды вредоносных компьютерных программ, наиболее опасные из современных видов вирусных программ, механизмы их действия.
5. Уголовная ответственность за использование троянских программ при совершении компьютерных преступлений. Отличие от вирусов, механизм действия.
6. Понятие иной компьютерной информации в уголовном праве.
7. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: основные способы и средства совершения такого рода преступных деяний, информация как предмет данного преступления.
8. Понятие критической информационной инфраструктуры Российской Федерации.
9. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
10. Составы неправомерного воздействие на критическую информационную инфраструктуру Российской Федерации.
11. Уголовная ответственность за неправомерный доступ к компьютерной информации.
12. Понятие компьютерной информации, ее уголовно-правовое значение.
13. Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ.
14. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Тестовые задания:

1. Последствиями неправомерного доступа к компьютерной информации являются:

1) уничтожение компьютерной информации;
2) блокирование компьютерной информации;
3) модификация компьютерной информации;
4) копирование компьютерной информации;
5) все перечисленные последствия.

2. Под компьютерной информацией понимаются:

1) сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи;
2) только сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, относящиеся к категории государственной тайны;
3) только сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, относящиеся к категории коммерческой тайны.

3. Состав преступления, предусмотренный ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ, по конструкции объективной стороны является:
1) формальным;
2) усеченным;
3) материальным;
4) формально-материальным.

4. Состав преступления, предусмотренный ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, по конструкции объективной стороны является:
1) формальным;
2) усеченным;
3) материальным;
4) формально-материальным.

5. Состав преступления, предусмотренный ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ, по конструкции объективной стороны является:
1) формальным;
2) усеченным;
3) материальным;
4) формально-материальным.

6. Укажите последствия, предусмотренные диспозицией ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ:
1) уничтожение компьютерной информации;
2) модификация компьютерной информации;
3) уничтожение или повреждение компьютера;
4) крупный ущерб собственнику компьютера.

7. Субъектом преступления, предусмотренного ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, является:
1) только собственник компьютера, с которого был осуществлен неправомерный доступ;
2) должностное лицо;
3) физическое вменяемое лицо, достигшее 16-летнего возраста;
4) физическое вменяемое лицо, достигшее 18-летнего возраста.

Ситуационные задачи и кейс задания:
Задание 1

Синибояров создал поддельный сайт, который в точности повторял интернет-ресурс, занимающийся сбором денежных средств для помощи больным онкологическими заболеваниями. В течение работы сайта Синибояров получил денежные средства в размере 42 125 руб.

Дайте юридическую оценку действиям Синибоярова.

Задание 2

Иванов решил выяснить содержание личной переписки своей сожительницы Афанасьевой. С этой целью он через Интернет познакомился с Рязанкиным, который за вознаграждение взломал смартфон Афанасьевой и предоставил Иванову возможность получать в режиме реального времени сведения о всех сообщениях, которые отправляет и получает Афанасьева.

Дайте юридическую оценку действиям указанных в задаче лиц.

Задание 3

Петрухин пришел в дежурную часть отдела внутренних дел с заявлением о краже принадлежащего ему аккаунта многопользовательской онлайн игры. По словам Петрухина, общий ущерб от действий неизвестных ему лиц составил 35 000 руб. Эти средства Петрухин инвестировал в развитие своего аккаунта, покупая за реальные деньги виртуальное обмундирование и оружие. Дежурный следователь отказал Петрухину в принятии заявления, сославшись на то, что «игрушками полиция не занимается».

Дайте юридическую оценку действиям указанных в задаче лиц.

Задание 4

Боярова, используя сеть Интернет, взломала личный компьютер высокопоставленного менеджера крупной фирмы Соколова. Используя имеющиеся навыки программиста, Боярова зашифровала все документы Соколова с расширением .doc и .docx. Позднее Боярова отправила Соколову сообщение с предложением перечислить по указанным ею реквизитам 10 000 долл. США взамен восстановления доступа к документам. Опасаясь срыва крупной сделки, Соколов выполнил требование Бояровой.

Дайте юридическую оценку действиям указанных в задаче лиц.

Задание 5

Кривцов, Балашевич и Осипов, используя сеть зараженных компьютеров, совершали информационные атаки на сайты компаний, реализующих свои товары и услуги через сеть Интернет. После блокировки указанных сайтов в течение нескольких часов они прекращали атаку и связывались с руководителями организаций, предлагая им «сотрудничество» в целях недопущения подобных фактов в будущем. За свои «услуги по информационной защите» они требовали 50 000 руб. в месяц.

Установлено, что данная группа осуществляла свою деятельность в течение двух лет и получила денежные средства от своих «клиентов» на общую сумму 6 845 592 руб.

Дайте юридическую оценку действиям указанных в задаче лиц.

По теме 3

Вопросы к опросу:

1. Сеть Интернет и информационно-телекоммуникационной сети как средство совершение преступления – соотношение понятий.
2. Киберсредство совершения преступления как конструктивный или квалифицирующий признак совершения преступления.
3. Квалификация незаконного оборота специальных технических средств, предназначенных для негласного получения информации, осуществляемого через информационно-телекоммуникационные сети.

4. Нарушение авторских и смежных прав, совершенное с использованием киберсредств.
5. Квалификация вовлечения несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемых с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

Тестовые задания:

1. Совершение преступления с использованием сети интернет является:

1) только квалифицирующим признаком преступления;
2) только конструктивным признаком преступления;
3) как конструктивным, так и квалифицирующим признаком преступления.

2. К квалифицирующим признакам преступлений в информационной сфере относятся:

1) сеть Интернет;
2) киберсредство;
3) информационно-телекоммуникационные сети и сетевые ресурсы;
4) все перечисленные средства.

Ситуационные задачи и кейс-задания

Задание 1

Петраков решил открыть интернет-клуб. С этой целью он установил вагон-бытовку, которую оборудовал 10 компьютерами. Данные компьютеры Петраков по локальной сети подключил к компьютеру администратора, имеющему выход к информационно-телекоммуникационной сети Интернет, с целью выхода на сайты, на которых содержатся азартные игры. В течение восьми месяцев Петраков ежедневно получал денежные средства от посетителей за возможность посредством предоставленного им компьютерного оборудования, осуществить выход в сеть Интернет на сайты, содержащие азартные игры. Доход от деятельности составил 3 442 815 руб.

Дайте юридическую оценку действиям Петракова.

Задание 2

Свиридов изготовил вирус, позволяющий получить управление над модулем выдачи наличных банкомата. Позднее через Интернет он познакомился с Артеминым, работающим в организации, занимающейся обслуживанием банкоматов. За 2000 долл. США Свиридов предложил Артемину установить вирусное программное обеспечение на ряд банкоматов. В течение недели Артемин, используя флэш-носитель, установил вирус на 15 банкоматов, о чем сообщил Свиридову. Через два дня Свиридов вместе с Кожуховым, выполняющим роль охраны, путем ввода определенной комбинации цифр на *PIN*-клавиатуре, изъял из указанных банкоматов 42 562 715 руб.

Дайте юридическую оценку действиям указанных в задаче лиц.

Задание 3

Аванесян, обладая познаниями в программировании, изготовил программу, позволяющую направлять в банк от имени клиента запросы на проведение финансовых операций. При этом все смс-сообщения от банка умная программа перехватывала и скрывала. Желая использовать созданный вирус в целях обогащения, Аванесян обратился к Даурову, лидеру одной из этнических преступных группировок. Дауров, используя свои преступные связи, организовал распространение изготовленного Аванесяном вируса. В течение года у нескольких тысяч клиентов банков по всей стране было похищено 215 632 724 руб. Известно, что распространением вирусов, переводом денежных средств

между счетами и обналичиванием занимались отдельные группы злоумышленников по всей стране. На завершающем этапе полученные деньги «отмывались» через сеть автомастерских.

Дайте юридическую оценку действиям указанных в задаче лиц.

По теме 4

Вопросы к опросу:

1. Уголовная ответственность за кражу, совершенную с использованием электронных банковских сетей и с использованием электронных платежных систем.
2. Уголовная ответственность за мошенничество, совершенное с использованием электронного платежного средства и с применением IT-технологий.
3. Уголовно-правовое понятие и виды электронных средств платежа.
4. Проблемы квалификации кражи финансовых средств с использованием электронных банковских сетей и платежных систем.
5. Уголовная ответственность за мелкое хищение с использованием информационно-телекоммуникационных сетей путем обмана или злоупотребления доверием.
6. Уголовная ответственность за мошенничество с использованием электронных средств платежа и с применением IT-технологий.
7. Уголовная ответственность за мошенничество в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств).
8. Уголовно-правовая характеристика и природа электронного спама.

Тестовые задания:

1. Мелкое хищение с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ), совершенное лицом, подвергнутым административному наказанию, квалифицируется по:

1) ч. 1 ст. 158 УК РФ;
2) п. г ч. 3 ст. 158 УК РФ;
3) ч. 1 ст. 158.1 УК РФ.

2. Состав преступления, предусмотренный ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, по конструкции объективной стороны является:

1) формальным;
2) усеченным;
3) материальным;
4) формально-материальным.

3. Согласно УК РФ хищение денежных средств клиента банка, связанное со взломом его личного кабинета на сайте кредитной организации:

1) охватывается диспозицией ст. 159.6 «мошенничество в сфере компьютерной информации» и не требует дополнительной квалификации по ст. 272 «неправомерный доступ к компьютерной информации»;

2) образует совокупность преступлений, предусмотренных ст. 159.6 «мошенничество в сфере компьютерной информации» и ст. 272 «неправомерный доступ к компьютерной информации»;

3) охватывается диспозицией ст. 158 «кража»;

4) охватывается диспозицией ст. 274 «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

4. По УК РФ хищение денежных средств, совершенное путем использования оставленного потерпевшим телефона с подключенным сервисом мобильный банк, следует квалифицировать по:

1) ст. 159.6 «Мошенничество в сфере компьютерной информации»;

2) совокупности преступлений, предусмотренных ст. 159.6 «Мошенничество в сфере компьютерной информации» и ст. 272 «Неправомерный доступ к компьютерной информации»;

3) охватывается диспозицией ст. 158 «Кража»;

4) охватывается диспозицией ст. 272 «Неправомерный доступ к компьютерной информации».

Ситуационные задачи и кейс задания:

Задание 1

Говорова знакомилась в социальных сетях с мужчинами. После непродолжительного общения она высказывала намерение приехать погостить и просила помочь ей с оплатой проезда. После получения денежных средств от доверчивых ухажеров Говорова блокировала их и искала новых кандидатов. Подобным образом в течение шести месяцев Говорова обманула 27 мужчин на общую сумму 148 576 руб.

Дайте юридическую оценку действиям Говоровой.

Задание 2

Волхонцев, используя полученные им сведения о держателях банковских карт, звонил клиентам банка и, представившись сотрудником отдела технической поддержки, под предлогом необходимости устранения неполадок просил ввести определенные команды через мобильный телефон или банкомат. Как только клиент вводил все необходимые команды, денежные средства перечислялись на счет Волхонцева. В результате деятельности Волхонцева пострадало 145 клиентов банка, общая сумма ущерба составил 1 327 045 руб.

Дайте юридическую оценку действиям Волхонцева.

Задание 3

Потапкин, находясь на праздновании дня рождения, попросил у подвыпившего Саурова мобильный телефон, чтобы сделать срочный звонок. Получив телефон, Потапкин через компьютерное приложение мобильный банк перевел деньги Саурова в размере 2500 руб. на свой счет в банке. После этого Потапкин вернул телефон Саурову и через непродолжительное время покинул празднование.

Дайте юридическую оценку действиям Потапкина.

По теме 5

Вопросы к опросу:

1. Уголовно-правовая характеристика незаконного предпринимательства, совершаемого с использованием информационно-телекоммуникационных сетей и IT-технологий.
2. Проблемы квалификации незаконного предпринимательства, совершаемого с использованием информационно-телекоммуникационных сетей и IT-технологий.

3. Уголовно-правовая характеристика незаконной организации и проведения азартных игр, совершаемого с использованием сети Интернет и иных информационно-телекоммуникационных сетей.
4. Проблемы квалификации незаконной организации и проведения азартных игр, совершаемого с использованием сети Интернет и иных информационно-телекоммуникационных сетей.

Тестовые задания:

1. Квалифицирующим признаком незаконного предпринимательства с использованием информационно-телекоммуникационных сетей является:

1) использование средств массовой информации;
2) использование электронных или информационно-телекоммуникационных сетей;
3) использование сети "Интернет";
4) все указанные признаки.

2. Квалифицирующим признаком незаконной организации и проведения азартных игр с использованием сети Интернет и иных информационно-телекоммуникационных сетей:

1) использование средств массовой информации;
2) использование электронных или информационно-телекоммуникационных сетей;
3) использование сети "Интернет";
4) ни один из названных признаков.

3. Квалифицирующим признаком незаконной банковской деятельности посредством использования информационно-телекоммуникационных сетей и иных киберсредств является:

1) использование средств массовой информации;
2) использование электронных или информационно-телекоммуникационных сетей;
3) использование сети "Интернет";
4) ни один из названных признаков.

4. Квалифицирующим признаком манипулирования рынком с использованием информационно-телекоммуникационных сетей является:

1) использование средств массовой информации;
2) использование электронных или информационно-телекоммуникационных сетей;
3) использование сети "Интернет";
4) ни один из названных признаков.

5. Квалифицирующим признаком неправомерного оборота средств платежей, в том числе электронных, с использованием информационно-телекоммуникационных технологий является:

1) использование средств массовой информации;
2) использование электронных или информационно-телекоммуникационных сетей;
3) использование сети "Интернет";
4) ни один из названных признаков.

Ситуационные задачи и кейс задания:

Задание 1

Свиридов, с помощью программы *DistanceCopyMaster*, предназначенной для скрытого копирования в сети Интернет файлов, содержащих пароли других

пользователей, получил реквизиты доступа к компьютеру индивидуального предпринимателя Говорова. В течение суток Свиридов скопировал всю служебную информацию Говорова о его коммерческих партнерах, совершенных сделках, движении денежных средств и т.д.

Квалифицируйте действия Свиридова.

Задание 2

Аслаханов, имея доступ к сети Интернет, из корыстных побуждений совершал доступ к принадлежащим потерпевшим учетным записям интернет-сервиса *Icloud*, после чего изменял пароли к ним. Используя учетные записи, Аслаханов стирал и (или) блокировал всю имеющуюся на мобильных телефонах потерпевших информацию и выводил на экране устройств текст примерно следующего содержания: «Это устройство было утеряно и стерто. Для возврата напишите письмо на … Укажите в письме этот код устройства: …». После получения электронного письма от потерпевшего Аслаханов направлял в ответ инструкцию в виде текста, согласно которой он требовал для разблокировки устройства перечисления денежных средств. Потерпевшие, выполняя условия Аслаханова, переводили указанные им суммы.

Квалифицируйте действия Аслаханова.

Задание 3

Балакшин, используя навыки работы с компьютерными программами, взламывал учетные записи (аккаунты) пользователей социальной сети ВКонтакте и, представляясь знакомым потерпевших, просил сообщить реквизиты банковской карты под предлогом перевода денежных средств. В результате действий Балакшина пострадало 32 потерпевших, общий ущерб составил 276 517 руб.

Квалифицируйте действия Балакшина.

4.3. Оценочные средства для промежуточной аттестации

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

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа формирования компетенции
ПК-6	способность юридически правильно квалифицировать факты и обстоятельства	ПК-6.1.5	Способность юридически грамотно толковать и интерпретировать факты и обстоятельства, с которыми закон связывает возникновение правоотношений, а также осуществлять на их основе планирование и организацию исследовательской работы.
ПК-7	владение навыками подготовки юридических документов	ПК-7.1.6	Способность подготовить нормативные акты, юридические документы применительно к различным сферам профессиональной деятельности и на основе

			их подготовить исследовательский проект.
ПК-16	способностью давать квалифицированные юридические заключения и консультации в конкретных видах юридической деятельности	ПК-16.2.4	Способность применять различные методики и модели ведения юридической консультации, в том числе с целью организации и систематизации результатов исследовательской работы.

4.3.2 Показатели и критерии оценивания компетенций на различных этапах их формирования

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*
1 этап (ПК-6.1.1)	квалификация юридических фактов	собрана полная информация и проведена классификация юридического факта;
2 этап (ПК-6.1.2)	процессуально правильно оформлены и закреплены юридические факты	собрана полная информация о юридическом факте и правильное его процессуальное закрепление;
3 этап (ПК-6.1.3)	осуществлен отбор жизненных обстоятельств, с которыми закон связывает возникновение правоотношений; проведена оценка жизненных обстоятельств, с которыми закон связывает возникновение правоотношений	собрана полная информация о жизненных обстоятельствах, с которыми закон связывается возникновение правоотношений; осуществлена оценка жизненных обстоятельств, с которыми закон связывается возникновение правоотношений;
4 этап (ПК-6.1.4)	квалифицированы факты и обстоятельства, с которыми закон связывает возникновение правоотношений	адекватно и полно найдены, отобраны, проанализированы и систематизированы законоположения, относящиеся к ситуациям, нуждающимся в правовой оценке, регулировании;
5 этап (ПК-6.1.5)	толкование и интерпретация фактов и обстоятельств, с которыми закон связывает	толкует и комментирует законодательство относящееся к ситуациям, нуждающимся в правовой оценке и регулировании

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*
	возникновение правоотношений	
1 этап (ПК-7.1.1)	составление нормативных правовых и иных юридических документов	составляет нормативные правовые и иные юридические документы;
2 этап (ПК-7.1.2)	применение основных правил юридической техники, включая базовые знания о структуре и реквизитах, правовых актов, а также предъявляемых к ним юридико-технических требованиях	применяет основные правила юридической техники, включая базовые знания о структуре и реквизитах, правовых актов, а также предъявляемых к ним юридико-технических требованиях;
3 этап (ПК-7.1.63	подготовка заключения по проектам распорядительных актов и иных правовых актов на предмет их соответствия требованиям действующего законодательства	готовит заключения по проектам распорядительных актов и иных правовых актов на предмет их соответствия требованиям действующего законодательства;
4 этап (ПК-7.1.4)	описание возможных перспектив принятия разрабатываемого нормативно-правового акта	квалифицировано описывает перспективы разработки и принятия нормативно-правового акта;
5 этап (ПК-7.1.5)	осуществление сбора и обработки информации для разработки нормативно-правового акта	грамотно осуществлять сбор и обработку информации для разработки нормативно-правового акта;
5 этап (ПК-7.1.6)	проектирование нормативных актов; составление процессуальных документов и материальных документов, опосредующих конкретные правоотношения или процессуальные действия	готовит проект нормативного акта согласно всем требованиям, предъявляемым к нему; составляет процессуальный документ или договор, опосредующие конкретные правоотношения или процессуальные действия;
1 этап ПК-16.1.1	– осуществление анализа сложной правовой	грамотно анализирует правовые ситуации;

Этап освоения компетенции	**Показатель оценивания** *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	**Критерий оценивания** *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*
	ситуации; – предложение рекомендаций по осуществлению конкретных действий в рамках действующего законодательства	самостоятельно предлагает различные предложения по осуществлению конкретных действий в рамках действующего законодательства;
1 этап ПК-16.1.2	– Осуществление юридической экспертизы конкретной юридической ситуации; – Квалифицированное применение нормативно-правовых актов в процессе экспертизы конкретной юридической ситуации	уверенное осуществление юридической экспертизы конкретной юридической ситуации; самостоятельно и грамотно применяет нормативно-правовые акты в процессе экспертизы конкретной юридической ситуации;
1 этап ПК-16.1.3	– Подготовка квалифицированного юридического заключения; – Предложение юридически обоснованных выводов по итогам составленного юридического заключения	проект юридического заключения; квалифицированная формулировка юридически обоснованных выводов;
1 этап ПК-16.2.1	Оказание устной юридической консультации по конкретной ситуации	уверенно осуществляет консультирование по конкретным ситуациям;
1 этап ПК-16.2.2	Применение различных техник в процессе оказания юридической консультации в конкретных видах юридической деятельности	квалифицировано применяет в зависимости от конкретной ситуации различные технологии юридической консультации;
1 этап ПК-16.2.3	Проектирование процесса юридической консультации в зависимости от конкретной ситуации в различных отраслях права	оформление проекта процесса юридической консультации в зависимости от конкретной ситуации в различных отраслях права; грамотное описание основных этапов процесса консультирования;
1 этап ПК-16.2.4	оперативно и квалифицированно	уверено применяет различные методики и модели

Этап освоения компетенции	Показатель оценивания *Что делает обучающийся (какие действия способен выполнить), подтверждая этап освоения компетенции*	Критерий оценивания *Как (с каким качеством) выполняется действие. Соответствует оценке «отлично» в шкале оценивания в РПД.*
	применяет различные методики и модели ведения юридической консультации	ведения юридической консультации.

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

Вопросы для зачета

1. Понятие киберпреступления.
2. Уголовно-правовая классификация киберпреступлений.
3. Объекты киберпреступлений.
4. Проблемы дифференциации и индивидуализации уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (киберпреступлений).
5. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.
6. Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ.
7. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
8. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
9. Уголовная ответственность за доведение до самоубийства, совершенное с использованием сети Интернет.
10. Уголовная ответственность за склонение к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети.
11. Уголовная ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства.
12. Уголовная ответственность за угрозу убийством с использованием компьютерных IT-технологий.
13. Уголовная ответственность за торговлю людьми с использованием информационно-телекоммуникационных сетей.
14. Уголовная ответственность за клевету с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.
15. Уголовная ответственность за развратные действия с использованием ресурсов сети Интернет.
16. Уголовная ответственность за нарушение авторских и смежных прав с использованием киберсредств.

17. Уголовная ответственность за вовлечение с использованием информационно-телекоммуникационных сетей и сетевых ресурсов несовершеннолетних в совершение преступлений и антиобщественных действий.
18. Уголовная ответственность за кражу из электронных банковских сетей и с использованием платежных систем, совершаемую с использованием компьютерных программ, сетей, иных высокотехнологичных средств.
19. Уголовная ответственность за неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.

Шкала оценивания

Оценивание обучающегося на зачете

Оценка	Критерии оценки	Результаты обучения
«зачтено»	– уверенно и в точном соответствии с требованиями закона систематизирует нормы Общей части уголовного права, определяет их виды; – в соответствии с требованиями норм Общей части УК РФ определяет понятие задачи УК РФ по охране общественных отношений в сфере цифровой экономики; – правильно и полно отвечает на вопросы ситуационных задач по Общей части УК РФ; – применяет подзаконные нормативные правовые акты уголовно-исполнительного права; – демонстрирует умение пользоваться положениями УК РФ по вопросам Общей части уголовного права; – уверенно владеет содержанием норм и институтов Общей части уголовного права РФ.	ПК-6.1.5 *на уровне знаний:* знание норм Общей части УК РФ; знание правил квалификации преступлений, совершаемых в сфере цифровой экономики; знание видов и признаков составов преступлений, совершаемых в сфере цифровой экономики; знание объектов уголовно-правовой охраны в сфере цифровой экономики; знание системы наказаний и иных мер уголовно-правового характера, применяемых в рамках уголовной ответственности за преступления в сфере цифровой экономики; знание структуры уголовно-правовой нормы, видов гипотез, диспозиций и санкций. *на уровне умений:* умение определять основание уголовной ответственности за совершение преступления в сфере цифровой экономики; умение применять положения УК РФ при решении вопросов уголовной ответственности и квалификации деяний, совершаемых в сфере цифровой экономики;

«не зачтено»	– не способен анализировать и систематизировать требования норм Общей части уголовного права; – допускает грубые ошибки при решении ситуационных задач и правоприменения по вопросам уголовной ответственности и применения мер уголовно-правового характера при обеспечении безопасности цифровой экономики; – не владеет содержанием норм и институтов Общей части уголовного права Российской Федерации; – не знает задачи УК РФ по обеспечению безопасности в сфере цифровой экономики уголовно-правовыми средствами.	умение толковать уголовный закон по вопросам уголовной ответственности за преступления в сфере цифровой экономики. ПК-7.1.6: *на уровне знаний:* знание основных понятий и институтов Общей части уголовного права; знание обстоятельств, исключающих преступность деяния, совершаемого в сфере цифровой экономики; знание оснований освобождения от уголовной ответственности по делам о преступлениях в сфере цифровой экономики; знание правил назначения наказания за преступления, совершаемые в сфере цифровой экономики. *на уровне умений:* умение обеспечивать соблюдение требований принципа законности, равенства граждан перед законом, вины, справедливости и гуманизма при решении вопросов уголовной ответственности за совершение преступлений в сфере цифровой экономики; умение определять применимый уголовный закон с учетом его действия во времени, в пространстве и по кругу лиц. ПК-16.2.4 *на уровне знаний:* знание оснований уголовной ответственности за совершение оконченного и неоконченного преступления; порядок принятия решений и условия и основания совершения юридических действий в точном соответствии с законом; *на уровне умений:* устанавливать вину при совершении преступления в сфере цифровой экономики; умение, пользуясь положениями УК РФ, определять признаки состава преступления, установленные законом; умение определять возраст лица, подлежащего уголовной ответственности; решать задачи обеспечения безопасности в сфере цифровой экономики

		с применением мер уголовной ответственности.

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

5. Методические указания для обучающихся по освоению дисциплины

Основной целью самостоятельной работы студентов является полное освоение учебного материала, приобретение навыков и умений определять требования норм уголовного законодательства при решении вопросов противодействия криминальным угрозам в сфере информационной безопасности с использованием уголовно-правовых мер.

Самостоятельная работа обучающихся направлена на систематическое освоение рекомендованной литературы, освоение профессиональных знаний на уровне бакалавриата по юридическим вопросам использования возможностей уголовно-правовых мер при защите информационной безопасности. Систематическая работа учащихся позволяет интенсивно формировать интерес к учебно-познавательной деятельности, расширять юридический кругозор, углублять комплекс необходимых профессиональных знаний, овладевать приемами познания юридического материала, нормативно-правового регулирования уголовно-правовых отношений, развивать самостоятельность, активность и ответственность в ходе изучения учебной дисциплины. Все это гарантирует формирование познавательных способностей и приобретение профессиональных навыков служебной деятельности по обеспечению информационной безопасности уголовно-правовыми мерами.

Задания на внеаудиторную самостоятельную работу учащимися выполняется по заданиям преподавателя, но без его непосредственного участия. Для обеспечения внеаудиторной самостоятельной работы по дисциплине рекомендуется пользоваться разработанным программой перечнем заданий для самостоятельной работы. Данный инструмент необходим для планирования, эффективного управления и контроля учебной деятельности студентов.

Самостоятельная внеаудиторная работа студентов включает подготовку к устному опросу. Для этого предварительно следует изучить материалы лекции, основную и дополнительную рекомендованную литературу, иные публикации и учебные материалы, информацию из Интернет-ресурсов, ЭБС.

Самостоятельная работа учащихся может быть организована в индивидуальной и группой форме в зависимости от цели, объема, конкретной тематики самостоятельной

работы, уровня сложности, уровня подготовленности обучающихся. Обучающийся самостоятельно определяет режим своей внеаудиторной работы и меру труда, затрачиваемого на овладение знаниями и умениями по дисциплине, выполняет внеаудиторную работу по индивидуальному плану, в зависимости от собственной подготовки, бюджета времени и других условий. Ежедневно обучающимся рекомендуется уделять выполнению внеаудиторной самостоятельной работы в среднем не менее 1 часа. При выполнении заданий на внеаудиторную самостоятельную работу обучающиеся должны иметь возможность обращаться к преподавателю за консультацией с целью уточнения задания, контроля качества выполненного задания, оценки результатов.

Эффективность самостоятельной формы работы студентов зависит от качества, полноты и систематичности освоения рекомендованной литературы, положений законодательства, материалов судебной и правоохранительной практики. Для подготовки к устному опросу и решению ситуационных задач студенту и другим формам текущего контроля успеваемости следует ознакомиться с материалами, рекомендованными к изучаемой теме по учебнику, по иному учебному пособию, а также по конспекту лекции. Развернутый ответ должен быть полным и логичным, соответствовать положениями и нормам действующего законодательства, состоять из многих развернутых предложений, содержать аргументированные выводы и обобщения материала.

Методические рекомендации по решению ситуационных задач и кейс-заданий

Кейс-задание – предусматривает изучение практической проблемной ситуации, решение которой предполагает использование учебного материала.

Работа над кейс-заданием осуществляется с целью текущего контроля уровня знаний и навыков (владений) студента по применению норм права, по правильному толкованию норм закона, быстрому и эффективному ориентированию в системе норм законодательства, по решению вопросов в области отдельных правоотношений. Студенту объявляется условие задания, решение которого он излагает устно. Эффективным интерактивным способом решения задания является сопоставления результатов разрешения одного задания двумя и более малыми группами обучающихся. Задачи, требующие изучения значительного объема нормативного или правоприменительного материала, необходимо относить на самостоятельную работу студентов, с непременным разбором результатов во время практических занятий. В данном случае решение ситуационных задач с глубоким обоснованием должно представляться на проверку в письменном виде. При оценке решения заданий анализируется понимание студентом конкретной ситуации, правильность применения норм права, способность обоснования выбранной точки зрения, глубина проработки правоприменительного материала, умением выявить основные положения нормативного документа.

Методические рекомендации по выполнению тестовых заданий

Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать лишь один индекс (цифровое обозначение), соответствующий правильному ответу, если нет специальной оговорки, что может быть несколько правильных ответов.

Тесты составлены таким образом, что в каждом из них правильным может быть как один, так и несколько вариантов. Учащийся должен выбрать и указать все правильные ответы с учетом задания теста.

На выполнение теста отводится ограниченное время. Оно может варьироваться в зависимости от уровня тестируемых, сложности и объема теста. Как правило, время выполнения тестового задания определяется из расчета 30-45 секунд на один вопрос.

Критерии оценки выполненных студентами тестов определяются преподавателем самостоятельно. Рекомендуются следующие критерии оценки:

85% – 100% правильных ответов – «отлично»;
66% – 84% правильных ответов – «хорошо»;
50% – 65% правильных ответов – «удовлетворительно»;
менее 50% правильных ответов – «неудовлетворительно».

При подведении итогов по выполненной работе рекомендуется проанализировать допущенные ошибки, прокомментировать имеющиеся в тестах неправильные ответы.

6. Основная и дополнительная учебная литература, необходимая для освоения дисциплины, ресурсы информационно-телекоммуникационной сети "Интернет", включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

Сверчков, В. В. Уголовное право. Особенная часть : учеб. пособие для вузов / В. В. Сверчков. — 10-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 280 с. — (Серия : Специалист). — ISBN 978-5-534-03248-2. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/431072

6.2. Дополнительная литература

Киберпреступность: Учебное пособие. / Побегайло А.Э. – М.: Акад. Ген. прокуратуры Рос. Федерации, 2018. - 184 с.

Уголовно-правовое противодействие преступлениям в сфере информационно-коммуникационных технологий: Учебное пособие. / Дмитренко А.П., Русскевич Е.А. – М., 2017;

Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: Учебное пособие. / Русскевич Е.А. – М., 2019. - 115 с.

Криминалистика для государственных обвинителей: учебник / Академия Генеральной прокуратуры Российской Федерации; Под ред. А.Ф. Козусева и др. – М.: Норма: НИЦ Инфра-М, 2012. - 479с.

Право интеллектуальной собственности: Учебник. Т. 2: Авторское право. / Е.С. Гринь, В.О. Калятин, С.В. Михайлов и др.; под общ. ред. Л.А. Новоселовой. М.: Статут, 2017. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».

Теория оперативно-розыскной деятельности: учебник. - 3-е изд., перераб. и доп. / под ред. К.К. Горяинова и др. – М.: НИЦ ИНФРА-М, 2016. 712с. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=552645.

Теория судебной экспертизы (Судебная экспертология): Учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин; Под ред. Е.Р. Россинской - 2-е изд., перераб и доп. – М.: Юр.Норма, НИЦ ИНФРА-М, 2018. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=962111

Уголовное право России: учебник: [в 2 т.] Т.1 Общая часть / [Абдульманов А.А. и др.] под ред. Н.Г. Кадникова. – М.: Юриспруденция, 2018. - 436с.

Уголовное право России: учебник: [в 2 т.] Т.2 Особенная часть / [Абдульманов А.А. и др.] под ред. Н.Г. Кадникова. – М.: Юриспруденция, 2018. - 836 с.

Уголовный процесс: учебник. – 7-е изд., перераб. / А.В. Смирнов, К.Б. Калиновский, под общ. ред. А.В. Смирнова. – М.: Норма: Инфра-М, 2018. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=914141

6.3. Учебно-методическое обеспечение самостоятельной работы

Научные труды

1. Аверьянова Т.В. Судебная экспертиза: курс общей теории: монография / Т.В. Аверьянова – М.: Юр.Норма, НИЦ ИНФРА-М, 2015. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=513735.
2. Акопов Г.Л. Политика и Интернет : монография / Г.Л. Акопов. – М.: ИНФРА-М, 2018. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=940532.
3. Бабурин С.Н. Стратегия национальной безопасности России: теоретико-методологические аспекты: монография / С.Н. Бабурин, М.И. Дзлиев, А.Д. Урсул. – М.: ИНФРА-М, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=635198
4. Баранова Е. К. Информационная безопасность и защита информации: учебное пособие. – 3-е изд. / Е.К. Баранова, А.В. Бабаш. – М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=495249.
5. Баринов С.В. О криминализации преступного нарушения неприкосновенности частной жизни, совершаемого в форме распространения баз персональных данных // Российский следователь. 2017. №4. С. 35-38. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
6. Бикмиев Р.Г., Бурганов Р.С. Собирание электронных доказательств в уголовном судопроизводстве / Р.Г. Бикмиев, Р.С. Бурганов // Информационное право. – 2015. – №3. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
7. Брагин Л.А. Организация розничной торговли в сети Интернет: учебное пособие / Л.А. Брагин, Т.В. Панкина. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=421959.
8. Бородин К.В. Объекты и субъекты правового регулирования борьбы с распространением вредной информации в сети Интернет / К.В. Бородин // Информационное право. – 2016. – №2. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
9. Будылин С.Л. Электронное сообщение как документ и доказательство // Закон. – 2014. – №10. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
10. Букалерова Л.А., Пикуров Н.И. Уголовно-правовая охрана оборота официальной информации / Л.А. Букалерова, Н.И. Пикуров // Правовые вопросы связи. – 2005. – №1. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
11. Васильков А.В. Безопасность и управление доступом в информационных системах: учеб. пособие / А.В. Васильков, И.А. Васильков. – М.: ФОРУМ: ИНФРА-М, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=537054
12. Витко В., Цатурян Е. Споры в сфере доменных имен и товарных знаков // ЭЖ-Юрист. 2015. №16. С. 11. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
13. Волеводз А.Г. Международные правоохранительные организации: понятие и современная система / А.Г. Волеводз // Международное уголовное право и международная юстиция. – 2011. – № 2. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
14. Волеводз А.Г. Юридические сети в сфере судебного и полицейского сотрудничества Европейского Союза / А.Г. Волеводз // Международное уголовное право и международная юстиция. – 2012. – №2. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
15. Гагарина А.А. Меры киберпротиводействия сайтам детской порнографии в сети Интернет / А.А. Гагарина // Российский следователь. – 2008. –№ 19. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».

16. Гурко А. Пиратство и майнинг // ИС. Авторское право и смежные права. 2017. №11. С. 17-26. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
17. Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети Интернет // Lex russica. 2017. №7. С. 166-177. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
18. Девлятшина М. Защита прав на компьютерную программу // ЭЖ-Юрист. 2017. №25. С. 13. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
19. Дубинин Е.А. Оценка относительного ущерба безопасности информационной системы: монография / Е.А. Дубинин, Ф.Б. Тебуева, В.В. Копытов. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=471787.
20. Ефремова М.А. Социальная обусловленность уголовно-правовой охраны информационной безопасности Российской Федерации // Вестник Пермского университета. Юридические науки. 2017. №2. С. 222-230. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
21. Жук А.П. Защита информации: учебное пособие. – 2-е изд. / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=474838.
22. Зазирная М.М. Квалификация распространения порнографических видеоматериалов в режиме реального времени с использованием сети Интернет / М.М. Зазирная // Уголовное право. – 2015. – №6. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
23. Зараменских Е.П. Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е. Артемьев. – М.: ИНФРА-М, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=792679.
24. Земцова С.И. Предмет доказывания при расследовании преступлений, связанных со сбытом наркотических средств, психотропных веществ и их аналогов, совершаемых с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет) / С.И. Земцова // Современное право. – 2015 – №4. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
25. Зубарева С. Чем грозит использование пиратских компьютерных программ / С. Зубарева // Экономика и жизнь. – 2009. – №15. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
26. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов, – 5-е изд., перераб. и доп. – М.: Форум, НИЦ ИНФРА-М, 2016. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=516806.
27. Карпович О.Г. Глобальные проблемы и международные отношения: монография / О.Г. Карпович. – М.: ЮНИТИ-ДАНА: Закон и право, 2014. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=490883
28. Клейменов И.М. Сравнительная криминология: монография / И.М. Клейменов. – М.: Норма: НИЦ Инфра-М, 2012. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=367420.
29. Колычева А.Н. К вопросу об использовании ресурсов сети Интернет в преступной деятельности // Российский следователь. 2016. №24. С. 42- 44. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=367420.
30. Корнева Л.А. Уголовная ответственность за нарушение имущественных авторских и смежных прав в Интернете / Л.А. Корнева // Российский следователь. – 2008. – №6. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».

31. Королева М.М. Клевета и оскорбления в сети Интернет / М.М. Королева // Законность. – 2010. – №7. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
32. Косынкин А.А. Некоторые аспекты преодоления противодействия расследованию преступлений в сфере компьютерной информации на стадии предварительного расследования / А.А. Косынкин // Российский следователь. – 2012. – №2. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
33. Кравцов К.Н. Этапы развития российского законодательства об ответственности за преступления в сфере компьютерной информации / К.Н. Кравцов // История государства и права. – 2006. – №12. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
34. Кузнецов Д.А. Генезис организационно-технического обеспечения Интернета в аспекте его правового регулирования / Д.А. Кузнецов // История государства и права. – 2008. – №1. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
35. Липин Д. Проблемы оценки ущерба, причиненного кибератакой // Административное право. 2017. №1. С. 17-21. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
36. Макаров А.В., Жукова М.В. Актуальные проблемы уголовной ответственности за изготовление с целью распространения порнографических материалов с изображением несовершеннолетних // Российский следователь. 2017. №15. С. 43-47. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
37. Максимов Н.В. Компьютерные сети: учеб. пособие / Н.В. Максимов, И.И. Попов. — 6-е изд., перераб. и доп. — М.: ФОРУМ: ИНФРА-М, 2018. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=792686.
38. Минин А. Я. Актуальные проблемы девиантного поведения несовершеннолетних и молодёжи: пособие / Минин А.Я., Краев О.Ю. – М.: Прометей, 2016. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=557102.
39. Микаева А.С. Проблемы правового регулирования в сети Интернет и их причины // Актуальные проблемы российского права. 2016. N 9. С. 67 - 75. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
40. Моргунова Е.А. Право интеллектуальной собственности: актуальные проблемы: монография. – 2-е изд., перераб. / Е.А. Моргунова и др.; под общ. ред. Е.А. Моргуновой – М.: Норма: НИЦ ИНФРА-М, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=763409.
41. Мороз Н.О. Актуальные вопросы международного сотрудничества в борьбе с преступностью в сфере высоких технологий в рамках СНГ // Международное уголовное право и международная юстиция. 2016. №3. С. 12-14. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
42. Мошков Е.А. Понятие электронного документа и его применение в качестве доказательства в гражданском и арбитражном судопроизводстве Российской Федерации / Е.А. Мошков // Арбитражный и гражданский процесс. – 2016. – №9. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
43. Новоселова Л.А., Рожкова М.А. Интеллектуальная собственность: некоторые аспекты правового регулирования: Монография / Л.А. Новоселова, М.А. Рожкова – М.: Норма: НИЦ ИНФРА-М, 2014. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=448981.
44. Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – М.: Норма, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=771246.

45. Оконенко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права / Р.И. Оконенко // Актуальные проблемы российского права. – 2015. – №3. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
46. Паненков А.А. Система преступлений в сфере компьютерной информации, входящих в структуру террористической деятельности (кибертерроризм) как реальная угроза внешнему и внутреннему контурам национальной безопасности России / А.А. Паненков. Военно-юридический журнал. –2014. – №4. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
47. Паламарчук А.В. Прокурорский надзор за исполнением законодательства в сфере противодействия правонарушениям в сети Интернет // Законность. 2016. №12. С. 3-9. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
48. Партыка Т.Л. Информационная безопасность: учебное пособие. – 5-е изд., перераб. и доп. / Т.Л. Партыка, И.И. Попов. – М.: Форум: НИЦ ИНФРА-М, 2014. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=420047.
49. Ревенков П.В. Финансовый мониторинг в условиях интернет-платежей / П.В. Ревенков. – М.: КноРус, ЦИПСиР, 2016. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=542583
50. Ромашев Ю.С. Международное правоохранительное право: монография – 2-е изд., доп. / Ю.С. Ромашев. – М.: Норма: НИЦ ИНФРА-М, 2013. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=407593.
51. Россинская Е. Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. – 3-е изд., доп. / Е.Р. Россинская. – М.: НОРМА: НИЦ ИНФРА-М, 2015. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=501090.
52. Русскевич Е.А. Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий // Международное уголовное право и международная юстиция. 2018. № 3. С. 10 - 13.
53. Сидоренко Э.Л. Криминальное использование криптовалюты: международные оценки // Международное уголовное право и международная юстиция. 2016. № 6. С. 8 - 10.
54. Савенков А.Н. Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 5 - 18.
55. 55. Серго А.Г. Что страшнее: пиратство или борьба с ним? // ИС. Авторское право и смежные права. 2017. №11. С.7-16. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
56. Смоленцев Д.В. Применение информационных систем в практической деятельности органов прокуратуры // Прокурор. 2016. №3. С. 108-112. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
57. Степаненко Д.А. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности / Д.А. Степаненко // Российский следователь. – 2015. –№15. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
58. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
59. Терещенко Л.К. Модернизация информационных отношений и информационного законодательства: монография / Л.К. Терещенко. – М.: НИЦ ИНФРА-М: ИЗиСП,

2013. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=442472.
60. Ткаченко В.В. Российский терроризм: проблемы уголовной ответственности: монография / В.В. Ткаченко, С.В. Ткаченко. – М.: НИЦ ИНФРА-М, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=753751.
61. Хорев П.Б. Программно-аппаратная защита информации: учебное пособие. – 2-е изд., испр. и доп. / П.Б. Хорев. – М.: Форум: НИЦ ИНФРА-М, 2015. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=489084.
62. Чекунов И.Г., Шумов Р.Н. Современное состояние киберпреступности в Российской Федерации / И.Г. Чекунов, Р.Н. Шумов // Российский следователь. – 2016. – №10. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
63. Шайхаттарова С.В. Россия и международные стандарты по борьбе с киберпреступностью / С.В. Шайхаттарова // Международное уголовное право и международная юстиция. – 2016. – №4. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
64. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. – М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=775200.
65. Швед Н.А. Неправомерный доступ к компьютерной информации: уголовно-правовая защита в РФ и Республике Беларусь // Информационное право. 2016. №2. С. 30-34. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
66. Шевченко Е.С. О криминалистической трактовке понятия «киберпреступность» / Е.С. Шевченко // Информационное право. – 2014. – №3. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».
67. Энгельгардт А.А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) / А.А. Энгельгардт // Lex russica. – 2014. – №11. – [Электронный ресурс]. – Режим доступа: СПС «Консультант Плюс».

6.4. Нормативные правовые документы.

1. Конституция Российской Федерации: официальный текст. – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
2. Гражданский кодекс Российской Федерации. – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
3. Кодекс Российской Федерации об административных правонарушениях. – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
4. Уголовно-процессуальный кодекс Российской Федерации. – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
5. Уголовный кодекс Российской Федерации. – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
6. Закон РФ от 21.07.1993 №5485-1 «О государственной тайне» – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
7. Закон РФ от 27.12.1991 №2124-1 «О средствах массовой информации». – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
8. Федеральный закон от 02.07.2013 №187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях». – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
9. Федеральный закон от 07.07.2003 №126-ФЗ «О связи» (ред. от 06.07.2016). – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».

10. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации». – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
11. Федеральный закон от 28.12.2013 №398-ФЗ «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации”». – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
12. Федеральный закон от 29.07.2004 №98-ФЗ «О коммерческой тайне». – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».
13. Федеральный закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». – [Электронный ресурс] – Режим доступа: СПС «Консультант Плюс».

6.5. Интернет-ресурсы

1. eLIBRARY : научная электронная библиотека. – URL: http://www.elibrary.ru
2. Справочно-правовая система КонсультантПлюс.
3. Справочно-правовая система ГАРАНТ.

6.6. Иные источники

ГАС РФ «Правосудие» - www.sudrf. ru
Интернет-библиотека СМИ Public.- ruwww.public. ru
Сайт Верховного Суда РФ - www.vsrf. ru
Сайт Государственной Думы - http://duma.gov.ru
Сайт Московского городского суда - www.mos-gorsud.ru
Сайт Президента РФ - http://www.kremlin.ru
Справочная правовая система «КонсультантПлюс» www.consultant. ru
СПС Гарант v.7 - Справочно-Правовая Система
Университетская информационная система Россия. УИС РОССИЯ - http:// www.cir.ru
Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ - http://diss.rsl. ru
Электронная библиотека образовательных и научных изданий Iqlib. - www.iqlib. ru

7. Материально-техническая база, информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. Специализированные залы для проведения лекций и аудитории для проведения семинарских и практических занятий с использованием мультимедийного оборудования и возможностью прямого выхода в сеть Интернет.

2. Специализированная мебель и оргсредства: аудитории и компьютерные классы, оборудованные посадочными местами.

3. Технические средства обучения: Персональные компьютеры; компьютерные проекторы; звуковые динамики; программные средства, обеспечивающие просмотр видеофайлов в форматах AVI, MPEG-4, DivX, RMVB, WMV.

4. Лицензионные электронные ресурсы: Windows, Microsoft Office (Excel, InfoPath, PowerPoint, Publisher, Word).

5. Информационные справочные и поисковые системы «Консультант Плюс», «Гарант».