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
решением кафедры основ
правоохранительной деятельности
Протокол от «21» мая 2020 г. №5

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.02.02 Судопроизводство по делам о преступлениях, совершаемых в сфере высоких технологий
(индекс, наименование дисциплины, в соответствии с учебным планом)

40.04.01 Юриспруденция
(код, наименование направления подготовки)

Юрист в уголовном судопроизводстве
(направленность (профиль))

Магистр
(квалификация)

Очная, заочная
(форма(ы) обучения)

Год набора 2020

Москва, 2020 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.02.02 Судопроизводство по делам о преступлениях, совершаемых в сфере высоких технологий обеспечивает овладение следующими компетенциями с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПК-2	Способность квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	ПК–2.3	Способность квалифицированно применять нормативные правовые акты, реализовывать нормы процессуального права в судопроизводственной и правозащитной деятельности в отдельных сферах государственного управления, в том числе в информационной среде.
ПК-8	Способность принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические заключения и консультации в конкретных сферах юридической деятельности	ПК-8.2	Способность к формулированию выводов, описанию и оформлению результатов проведения юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические заключения по вопросам в области судопроизводственной и правозащитной деятельности

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 *(при наличии профстандарта)*/трудовые /профессиональные действия	**Код этапа освоения компетенции**	**Результаты обучения**

	ПК–2.3	*на уровне знаний:* - теории правореализации и теории правоприменения - правовые основы обеспечения эффективности судебной власти - основных положений о правозащитной деятельности - правовых основ и процедур судопроизводственной и правозащитной деятельности - основных положений правоприменительной практики в судопроизводственной и правозащитной деятельности
		на уровне умений : - квалифицировать факты и обстоятельства в судопроизводственной и правозащитной деятельности; - собирать сведения, необходимые для оказания юридической помощи, в том числе запрашивать справки, характеристики и иные документы от органов государственной власти, органов местного самоуправления, общественных объединений и иных организаций - собирать и представлять предметы и документы, которые могут быть признаны вещественными и иными доказательствами, в порядке, установленном законодательством - составлять процессуальные акты; - проверят юридическую силу выбранной нормы; - обобщать судебную практику; - привлекать на договорной основе специалистов для разъяснения вопросов, связанных с оказанием юридической помощи - применять современные информационные технологии для поиска и обработки правовой информации, оформления юридических документов и проведения статистического анализа информации;
		на уровне навыков: - толкования норм процессуального права; - предварительной юридической квалификации совершенным действиям; - обработки и анализа правовой информации в сфере государственного управления и правоприменительной деятельности органов государственной власти.

	ПК-8.2	*на уровне знаний:* - видов и способов толкования норм права, правил юридической техники - системы источников процессуального права - системы правоприменительной практики - понятия, системы и процедур юридической экспертизы проектов нормативных правовых актов; - правил построения юридического заключения; - требований, предъявляемые к юридическим консультациям
		на уровне умений: - разрабатывать проекты экспертных заключений; - проводить юридическое консультирование - давать правовую оценку формы акта, его целей и задач, предмета правового регулирования, компетенции органа, принявшего акт, содержащихся в нем норм, порядка принятия, обнародования (опубликования) на предмет наличия коррупционных факторов в соответствии с критериями коррупциогенности
		на уровне навыков: - обработки и анализа правовой информации в судопроизводственной и правозащитной деятельности; - проведения юридической экспертизы нормативных правовых актов и их проектов; - выявления и оценки фактов коррупционного поведения; - на основе результатов исследования определять стратегию и тактику юридической помощи в конкретном деле

1. 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:

- лекции – 4 а.ч., практические занятия – 12 а.ч., самостоятельная работа – 56 а.ч.

Заочная Форма Количество академических часов, выделенных на контактную работу с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся:

- лекции – 4 а.ч., практические занятия – 12 а.ч., самостоятельная работа – 50 а.ч.

Место дисциплины в структуре ОП ВО

Б1.В.ДВ.02.02 Судопроизводство по делам о преступлениях, совершаемых в сфере высоких технологий

– дисциплина (модуль) реализуется после изучения:

Б1.В.06 Международное уголовное право изучается в 3 семестре;

– дисциплина (модуль) реализуется после изучения:

Б1.Б.01 Философия права;

Б1.Б.02 История политических и правовых учений;

Б1.Б.03 История и методология юридической науки;

Б1.Б.05 Актуальные проблемы уголовного процесса и судопроизводственной деятельности

Б1.Б.06 Иностранный язык в сфере профессиональной деятельности.

Б1.В.07 Психология уголовного судопроизводства

Б1.В.08 Примирительные процедуры в уголовном судопроизводстве

2. 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 (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
Тема 1	Особенности и задачи судопроизводства (раскрытия и расследования) преступлений, совершаемых в сфере высоких технологий	10	-		2		8	
Тема 2	Судопроизводство по делам о преступлениях	12			2		10	

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Очная форма обучения								
	против компьютерной информации, совершаемых в сфере высоких технологий							
Тема 3	Судопроизводство по делам о преступлениях против личности, совершаемые в сфере высоких технологий	11	1		2		8	
Тема 4	Судопроизводство по делам о преступлениях против собственности, совершаемых в сфере высоких технологий	13	1		2		10	
Тема 5	Судопроизводство по делам о преступлениях против общественной безопасности и общественного порядка, совершаемые с использованием высоких технологий	13	1		2		10	
Тема 6	Преступления против общественной нравственности, совершаемые в сфере высоких технологий	13	1		2		10	
Промежуточная аттестация								
Всего:		**72**	**4**		**12**		**56**	зачет

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

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости[4], промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Заочная форма обучения								
Тема 1	Особенности и задачи судопроизводства (раскрытия и расследования) преступлений, совершаемых в сфере высоких технологий	10	2		2		5	О
Тема 2	Судопроизводство по делам о преступлениях против компьютерной информации, совершаемых в сфере высоких технологий	12	2		4		5	О Т СЗ КЗ
Тема 3	Судопроизводство по делам о преступлениях против личности, совершаемые в сфере высоких технологий	11			2		10	О Т СЗ КЗ
Тема 4	Судопроизводство по делам о преступлениях против собственности, совершаемых в сфере высоких технологий	13			2		10	О Т СЗ КЗ
Тема 5	Судопроизводство по делам о преступлениях против общественной безопасности и общественного порядка, совершаемые с использованием высоких технологий	13			2	2	10	О Т СЗ КЗ
Тема 6	Преступления против общественной нравственности, совершаемые в сфере высоких технологий	13			2	2	10	О Т СЗ КЗ
Промежуточная аттестация								
Всего:		**72**	**4**		**14**	**4**	**50**	Зачет с оценкой

Содержание дисциплины

Тема 1. Особенности и задачи судопроизводства (раскрытия и расследования) преступлений, совершаемых в сфере высоких технологий

Понятие киберпреступности. Понятие киберпреступления. Уголовно-правовая классификация киберпреступлений. Социальная обусловленность и задачи уголовной ответственности за киберпреступления. Объекты киберпреступлений. Место IТтехнологий в составах киберпреступлений. Задачи и особенности квалификации киберпреступлений. Проблемы дифференциации и индивидуализации уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (киберпреступлений).

Тема 2. Судопроизводство по делам о преступлениях против компьютерной информации, совершаемых в сфере высоких технологий

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, виды, характеристика. Квалифицирующие признаки неправомерного доступа к компьютерной информации. Создание, использование и распространение вредоносных компьютерных программ. Основные виды вредоносных компьютерных программ. Вирусы в исторической перспективе. Наиболее опасные из современных видов вирусных программ, механизмы их действия. Троянские программы: отличие от вирусов, механизм 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 данного преступления. Вопросы правоприменительной практики по данному составу. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Понятие критической информационной инфраструктуры Российской Федерации. Объективная сторона данного деяния. Квалифицирующие признаки неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Тема 3. Судопроизводство по делам о преступлениях против личности, совершаемые в сфере высоких 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. Судопроизводство по делам о преступлениях в сфере экономики, совершаемых использованием высоких технологий

Мошенничество, совершенное с использованием платежных карт, осуществляемое с применением IT-технологий. Кража финансовых средств граждан из электронных банковских сетей и платежных систем: проблемы квалификации, основные пути совершения. Мелкое хищение, совершенное лицом, подвергнутым административному наказанию, совершаемое с использованием информационно-телекоммуникационных сетей путем обмана или злоупотребления доверием. Мошенничество в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств). Спам: понятие, вопросы уголовно-правовой ответственности. 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.

Тема 5. Судопроизводство по делам о преступлениях против общественной безопасности и общественного порядка, совершаемые с использованием высоких технологий

Кибертерроризм, его понятие и особенности квалификации. Осуществление публичных призывов к осуществлению террористической деятельности или публичное оправдание терроризма, совершаемое с помощью информационно-телекоммуникационных технологий. Содействие террористической деятельности, осуществляемое с помощью сети Интернет и иных информационно-телекоммуникационных сетей. Организация террористического сообщества или организации и участие в нем (ней), осуществляемые с использованием киберсредств. Заведомо ложное сообщение об акте терроризма, совершаемое с использованием киберсредств. Организация преступного сообщества (преступной организации) или участие в нем (ней), совершаемая путем использование информационно-телекоммуникационных сетей и ресурсов. Организация массовых беспорядков, совершаемая с использованием Интернета и иных информационно-телекоммуникационных сетей. Незаконные приобретение, передача, сбыт оружия, его основных частей, боеприпасов, взрывных устройств или взрывчатых веществ, осуществляемая с использованием информационно-телекоммуникационных сетей и их ресурсов. Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, либо прокуроров наркотических веществ и растений, их содержащих, совершаемые с использованием информационно-телекоммуникационных сетей и иных киберсредств. Склонение к потреблению наркотических средств, психотропных веществ или их аналогов, совершаемое с помощью Интернета и иных информационно-телекоммуникационных сетей. Незаконный оборот сильнодействующих или ядовитых веществ, а равно новых потенциально опасных психоактивных веществ в целях сбыта, совершаемый с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

Тема 6. Преступления против общественной нравственности, совершаемые в сфере высоких технологий

Уголовно-правовая классификация и виды преступлений против общественной нравственности, совершаемых с использованием IT-технологий.

Квалификация незаконных изготовления и оборота порнографических материалов или предметов, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет». Квалификация изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием IT-технологий. Понятие материалов и предметов с порнографическими

изображениями несовершеннолетних. Материалы и предметы, содержащие изображение или описание половых органов несовершеннолетнего, не являющиеся материалами и предметами, с порнографическими изображениями. Квалификация использования несовершеннолетнего в целях изготовления порнографических материалов или предметов с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

3. 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 *(индекс, наименование)* **используются следующие методы текущего контроля успеваемости обучающихся:**

При проведении занятий лекционного типа:

при проведении занятий семинарского типа: опрос, тест, ситуационные задачи, кейс-задания.

при контроле результатов самостоятельной работы студентов: тестирование, решение задач, доклады.

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).

4.2. Материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы

<u>По теме 1</u>

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 в электронной сфере, совершенное при помощи компьютерной системы или сети, или против них;
2) хищение компьютерных программ;
3) хищение компьютерной техники.

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 перечисленные признаки.

5. Согласно УК РФ под компьютерной информацией понимаются:

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

Охарактеризуйте современную структуру, динамику, и общее состояние киберпреступности.

Задание 2

Дайте характеристику основным условиям возникновения киберпреступлений.

Задание 3

Назовите причины международного характера киберпреступности.

<u>По теме 2</u>

Вопросы к опросу:

1. Неправомерный доступ к компьютерной информации: способы, квалифицирующие признаки.

2. Создание, использование и распространение вредоносных компьютерных программ: виды вредоносных компьютерных программ, наиболее опасные из современных видов вирусных программ, механизмы их действия.
3. Троянские программы: отличие от вирусов, механизм действия.
4. Иная компьютерная информация как средство совершения преступления.
5. 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.
6. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие критической информационной инфраструктуры Российской Федерации; объективная сторона данного деяния; квалифицирующие признаки.

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.

<u>По теме 3</u>

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 может являться

1) только квалифицирующим признаком преступления;

2) только конструктивным признаком преступления;

3) как конструктивным, так и квалифицирующим признаком преступления.

2. Квалифицирующими признаками преступлений могут являться

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.

<u>По теме 4</u>

Вопросы к опросу:

1. Проблемы квалификации мошенничества, совершаемого с использованием платежных карт, осуществляемого с применением IT-технологий.
2. Проблемы квалификации кражи финансовых средств граждан из электронных банковских сетей и платежных систем.
3. Проблемы квалификации незаконного предпринимательства, совершаемого с использованием 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. 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 Волхлнцева.

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.

<u>По теме 5</u>

Вопросы к опросу:

1. Кибертерроризм, его понятие и особенности квалификации.
2. Квалификация осуществления публичных призывов к осуществлению террористической деятельности или публичного оправдание терроризма, совершаемых с помощью информационно-телекоммуникационных технологий.
3. Квалификация содействия террористической деятельности, осуществляемых с помощью сети Интернет и иных информационно-телекоммуникационных сетей.
4. Квалификация организации террористического сообщества или организации и участие в нем (ней), осуществляемых с использованием киберсредств.
5. Квалификация организации массовых беспорядков, совершаемых с использованием Интернета и иных информационно-телекоммуникационных сетей.
6. Квалификация незаконных производства, сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, а также незаконного сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, либо прокуроров наркотических веществ и растений, их содержащих, совершаемых с использованием информационно-телекоммуникационных сетей и иных киберсредств.

Тестовые задания:

1. Квалифицирующим признаком осуществления публичных призывов к осуществлению террористической деятельности или публичного оправдание терроризма является:

1) использование средств массовой информации;

2) использование электронных или информационно-телекоммуникационных сетей;

3) использование сети "Интернет";

4) все указанные признаки.

2. Квалифицирующим признаком организации массовых беспорядков, совершаемых с использованием Интернета и иных 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.

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.

<u>По теме 6</u>

Вопросы к опросу:

1. Проблемы квалификации незаконных изготовления и оборота порнографических материалов или предметов, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет».
2. Проблемы квалификации изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием IT-технологий.
3. Проблемы квалификации использования несовершеннолетнего в целях изготовления порнографических материалов или предметов с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

Тестовые задания:

1. Квалифицирующим признаком незаконных изготовления и оборота порнографических материалов или предметов являются:

1) использование средств массовой информации;

2) использование электронных или информационно-телекоммуникационных сетей;

3) использование сети "Интернет";

4) все указанные признаки.

2. Квалифицирующим признаком использования несовершеннолетнего в целях изготовления порнографических материалов или предметов являются:

1) использование средств массовой информации;

2) использование информационно-телекоммуникационных сетей (включая сеть "Интернет").

Ситуационные задачи и кейс задания:

Задание 1

Арташевский на одном из сайтов в сети Интернет скопировал файл с фильмом порнографического характера. Желая поделиться «находкой» со

своими друзьями и знакомыми, он выложил данный фильм в локальной сети «Круг».

Дайте юридическую оценку действиям Арташевского.

Задание 2

Гражданин Акулиничев, имея умысел на хранение в целях распространения материалов с порнографическими изображениями лиц достигших 18-летнего возраста, содержащие изображение и описание сексуальных действий с участием указанных лиц, изображение и описание нестандартных форм сексуальной активности (орогенитальные) половые акты, детализированное изображение крупного плана этапов полового акта, и реализуя задуманное, из неустановленного источника информации, посредством глобальной сети Интернет и пиринговой сети передачи данных, скопировал в ранее им созданную папку «Закачка», расположенную в томе «G» носителя информации на жестких магнитных дисках типа Винчестер марки Seagate Barracuda номер модели видеофайлы порнографического содержания.

Дайте юридическую оценку действиям Акулиничева.

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 освоения компетенции
ПК-2	Способность квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности	ПК–2.3	Способность квалифицированно применять нормативные правовые акты, реализовывать нормы процессуального права в судопроизводственной и правозащитной деятельности в отдельных сферах государственного управления, в том числе в информационной среде.
ПК-8	Способность принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные	ПК-8.2	Способность к формулированию выводов, описанию и оформлению результатов проведения юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для

	юридические заключения и консультации в конкретных сферах юридической деятельности		проявления коррупции, давать квалифицированные юридические заключения по вопросам в области судопроизводственной и правозащитной деятельности

4.3.2 Показатели и критерии оценивания компетенций на различных этапах их формирования

Этап освоения компетенции	Показатель оценивания	Критерий оценивания	Средства (методы) оценивания
ПК–2.3 Способность квалифицированно применять нормативные правовые акты, реализовывать нормы процессуального права в судопроизводственной и правозащитной деятельности в отдельных сферах государственного управления, в том числе в информационной среде	- демонстрирует системные представления о правоприменительной практике в отдельных сферах государственного управления и административной деятельности государства, в том числе в информационной среде	- в полном объеме отобраны, проанализированы и систематизированы правоположения в сфере государственного управления и административной деятельности государства, нуждающиеся в правовой оценке; - отобраны, проанализированы и систематизированы материалы судебной практики в сфере государственного управления и административной деятельности государства; - предложены варианты решения казусов, размещенных в информационной среде	Опрос Тест Кейс задания Ситуационные задачи Самостоятельная работа
ПК– 8.2 Способность к формулированию выводов, описанию и оформлению результатов проведения юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические	- отбирает и систематизирует информацию о состоянии законности проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции, давать квалифицированные юридические заключения по вопросам в области	- отобрана и проанализирована информация о состоянии общественных отношений в судопроизводственной и правозащитной деятельности; - квалифицированы факты и обстоятельства	Опрос Отчет

заключения по вопросам в области судопроизводственной и правозащитной деятельности	судопроизводственной и правозащитной деятельности		

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 киберпреступности.
2. Понятие киберпреступления.
3. Уголовно-правовая классификация киберпреступлений.
4. Объекты киберпреступлений.
5. Проблемы дифференциации и индивидуализации уголовной ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (киберпреступлений).
6. Уголовно-правовая характеристика неправомерного доступа к компьютерной информации.
7. Создание, использование и распространение вредоносных компьютерных программ.
8. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Вопросы правоприменительной практики по данному составу.
9. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.
10. Доведение до самоубийства, совершенное с использованием сети Интернет.
11. Склонение к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети.
12. Организация деятельности, направленной на побуждение к совершению самоубийства.
13. Угроза убийством, совершаемая с использованием киберсредств и вопросы ее квалификации.
14. Торговля людьми, совершаемая с использованием информационно-телекоммуникационных сетей.
15. Клевета, осуществляемая с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.
16. Развратные действия, совершаемые путем использования ресурсов сети Интернет.
17. Нарушение авторских и смежных прав, совершенное с использованием киберсредств.
18. Вовлечение несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.
19. Кража финансовых средств граждан из электронных банковских сетей и платежных систем: проблемы квалификации, основные пути совершения.
20. Мошенничество в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств).
21. Неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.
22. Кибертерроризм, его понятие и особенности квалификации.
23. Осуществление публичных призывов к осуществлению террористической деятельности или публичное оправдание терроризма, совершаемое с помощью информационно-телекоммуникационных технологий.

24. Содействие террористической деятельности, осуществляемое с помощью сети Интернет и иных информационно-телекоммуникационных сетей.

25. Организация массовых беспорядков, совершаемая с использованием Интернета и иных информационно-телекоммуникационных сетей.

26. Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, либо прокуроров наркотических веществ и растений, их содержащих, совершаемые с использованием информационно-телекоммуникационных сетей и иных киберсредств.

27. Склонение к потреблению наркотических средств, психотропных веществ или их аналогов, совершаемое с помощью Интернета и иных информационно-телекоммуникационных сетей.

28. Незаконный оборот сильнодействующих или ядовитых веществ, а равно новых потенциально опасных психоактивных веществ в целях сбыта, совершаемый с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

29. Квалификация незаконных изготовления и оборота порнографических материалов или предметов, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет».

30. Квалификация изготовления и оборота материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием IT-технологий.

31. Квалификация использования несовершеннолетнего в целях изготовления порнографических материалов или предметов с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет»).

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

Оценивание обучающихся в процессе поэтапного освоения ими компетенций, формируемых данной дисциплиной осуществляется в форме зачета, который предполагает оценивание *знаний* с помощью устного собеседования по узловым вопросам и *умений* решать ситуационные задачи и/или кейс-задания.

Знания и умения обучающегося на зачете оцениваются с дифференцированной оценкой по шкале «зачтено с оценкой отлично», «зачтено с оценкой хорошо», «зачтено с оценкой удовлетворительно», «не зачтено».

Шкала оценивания

Оценка	Критерии оценки
на уровне знаний:	
Зачтено на «отлично»	*1. Полнота, системность, прочность знаний*: студент демонстрирует изложение полученных знаний в устной и/или письменной форме, полное, системное, в соответствии с требованиями учебной программы (допускаются единичные несущественные ошибки, самостоятельно исправляемые студентами); демонстрирует знание основных понятий, положений учебной дисциплины; полностью

	раскрывает содержания вопроса, может устанавливать внутрипредметные и межпредметные связи, демонстрирует знание различных точек зрения (если вопрос предполагает характеристику концепций (положений) разных авторов). *2. Обобщенность знаний*: студент выделяет существенные признаки изученного с помощью операций анализа и синтеза; проводит собственный анализ и оценку излагаемого материала (если вопрос предполагает, сопоставление концепций (положений) разных авторов), приводит примеры, выявляет и раскрывает возможные противоречия, проблемы, осуществляет их оценку; выявляет причинно-следственные связи; формулирует выводы и обобщения; свободно оперирует законодательством известными фактами и сведениями с использованием сведений из других предметов. *3. Полнота и правильность ответа*: студент полно излагает материал в рамках учебной программы, демонстрирует знания основной и дополнительной литературы, знания нормативно-правовых документов; дает правильное определение основных понятий. *4. Степень осознанности, понимания изученного*: обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и из дополнительной литературы, а также самостоятельно составленные, дает анализ. *5. Четкость и грамотность речи*: излагает материал последовательно и правильно с точки зрения норм литературного языка и риторики; отсутствуют ошибки, оговорки.
Зачтено на «хорошо»	*1. Полнота, системность, прочность знаний*: студент демонстрирует изложение полученных знаний в устной и/или письменной и форме, полное, системное, в соответствии с требованиями учебной программы (допускаются отдельные несущественные ошибки, исправляемые студентами после указания преподавателя на них); демонстрирует знание основных понятий, положений учебной дисциплины; полностью раскрывает содержания вопроса, может устанавливать внутрипредметные и межпредметные связи. *2. Обобщенность знаний*: студент выделяет существенные признаки изученного с помощью операций анализа и синтеза; приводит примеры; выявляет возможные противоречия; выявляет причинно-следственные связи; формулирует выводы и обобщения, в которых могут быть отдельные несущественные ошибки; делает ссылки на законодательство, подтверждает изученное известными фактами и сведениями. *3. Полнота и правильность ответа*: студент полно излагает материал в рамках учебной программы, демонстрирует знания основной литературы и фрагментарные знания дополнительной литературы, хорошо ориентируется в нормативно-правовых документах; дает правильное определение основных понятий.

	4. Степень осознанности, понимания изученного: обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры из учебника и дополнительной литературы, а также самостоятельно составленные. *5. Четкость и грамотность речи*: излагает материал последовательно и правильно с точки зрения норм литературного языка, отсутствуют ошибки, оговорки.
Зачтено на «удовлетворительно»	*1. Полнота, системность, прочность знаний*: студент демонстрирует изложение полученных знаний неполное, однако это не препятствует усвоению последующего программного материала (допускаются отдельные существенные ошибки, исправленные с помощью преподавателя). *2. Обобщенность знаний*: студент испытывает затруднения при выделении существенных признаков изученного, при выявлении причинно-следственных связей и формулировке выводов. *3. Полнота и правильность ответа*: студент излагает материал недостаточно полно, демонстрирует неполное знание основной литературы; ориентируется в нормативно-правовых документах; допускает неточности в определении понятий или формулировке правил, исправляемые с помощью преподавателя. *4. Степень осознанности, понимания изученного*: обнаруживает понимание материала, но не умеет достаточно глубоко и доказательно обосновать свои суждения или привести свои примеры. *5. Четкость и грамотность речи*: есть нарушения в последовательности изложения материала, допускает отдельные нарушения норм литературного языка, есть несущественные ошибки, оговорки.
Не зачтено - «неудовлетворительно»	*1. Полнота, системность, прочность знаний*: студент демонстрирует изложение учебного материала неполное, бессистемное, что препятствует усвоению последующей учебной информации; студент допускает существенные ошибки, неисправляемые даже с помощью преподавателя. *2. Обобщенность знаний*: студент демонстрирует бессистемное выделение случайных признаков изученного; неумение производить простейшие операции анализа и синтеза; делать обобщения, выводы. *3. Полнота и правильность ответа*: излагает материал неполно, демонстрирует не знание основной литературы, нормативно-правовых документов; допускает существенные ошибки в определении понятий или формулировке правил. *4. Степень осознанности, понимания изученного*: нет понимания материала. *5. Четкость и грамотность речи*: излагает материал непоследовательно, нормы литературного языка не выдержаны, допускает существенные ошибки, оговорки.

на уровне умений:	
Зачтено на «отлично»	*1. Степень самостоятельности выполнения действия (умения)*: свободно применяет умение (выполняет действие) на практике (при решении кейс-задач), в различных ситуациях. Студент самостоятельно и правильно решил учебно-профессиональную задачу, уверенно, логично, последовательно и аргументировано излагает свое решение, используя понятия профессиональной сферы. *2. Осознанность выполнения действия (умения)*: свободно комментирует выполняемые действия (умения), уверенно отвечает на вопросы преподавателя.
Зачтено на «хорошо»	*1. Степень самостоятельности выполнения действия (умения)*: применяет умение (выполняет действие) на практике(при решении кейс-задач), возможны не значительные ошибки, которые студент исправляет сам; применяет умение (выполняет действие) по алгоритму, с опорой на подсказки преподавателя. Студент самостоятельно и в основном правильно решил учебно-профессиональную задачу, уверенно, логично, последовательно и аргументировано излагает свое решение, используя понятия профессиональной сферы. *2. Осознанность выполнения действия (умения)*: в комментариях выполняемых действий имеются не значительные пропуски, дает ответы на вопросы преподавателя (допускаются отдельные несущественные ошибки, исправляемые студентами после указания преподавателя на них).
Зачтено на «удовлетворительно»	*1. Степень самостоятельности выполнения действия (умения)*: испытывает незначительные затруднения при применении умений (выполнении действий). Студент в основном решил учебно-профессиональную задачу, допустил несущественные ошибки, слабо аргументировал свое решение. *2. Осознанность выполнения действия (умения)*: в комментариях выполняемых действий имеются пропуски, не грубые ошибки, могут быть не большие затруднения при ответах на вопросы преподавателя (допускаются отдельные существенные ошибки, исправленные с помощью преподавателя).
Не зачтено - «неудовлетворительно»	*1. Степень самостоятельности выполнения действия (умения)*: испытывает значительные затруднения при применении умений (выполнении действий). Студент не решил учебно-профессиональную задачу или решил с грубыми ошибками, не смог аргументировать свое решение. *2. Осознанность выполнения действия (умения)*: затрудняется прокомментировать выполненные действия (умения) и/или допускает грубые ошибки, не отвечает на вопросы преподавателя; студент допускает существенные ошибки, неисправляемые даже с помощью преподавателя.
на уровне навыков:	
Зачтено на	Даны исчерпывающие и обоснованные ответы на все

«отлично»	поставленные вопросы, правильно решены практические задачи со ссылкой на нормативно-правовые документы; при ответах выделялось главное, все теоретические положения умело увязывались с требованиями нормативно-правовых документов и руководящих документов; ответы были четкими и краткими, а мысли излагались в логической последовательности; показано умение самостоятельно анализировать факты, события, явления, процессы в их взаимосвязи и диалектическом развитии.
Зачтено на «хорошо»	Даны полные, достаточно обоснованные ответы на поставленные вопросы, правильно решены практические задания со ссылкой на нормативно-правовые документы; при ответах не всегда выделялось главное, отдельные положения недостаточно увязывались с требованиями руководящих документов; ответы в основном были краткими, но не всегда четкими.
Зачтено на «удовлетворительно»	Даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования, при решении практических задач были допущены несущественные ошибки (допускается: отдельные положения недостаточно увязывались с требованиями нормативно-правовых и руководящих документов), однако, на уточняющие вопросы даны правильные ответы; при ответах не выделялось главное; ответы были многословными, нечеткими и без должной логической последовательности; на отдельные дополнительные вопросы не даны положительные ответы.
Не зачтено - «неудовлетворительно»	Затрудняется при выполнении практических задач, работа проводится с опорой на преподавателя.

5. Методические указания для обучающихся по освоению дисциплины

К зачету по дисциплине Б1.В.ДВ.02.02 «Судопроизводство по делам о преступлениях, совершаемых в сфере высоких технологий» необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине.

В самом начале освоения дисциплины следует ознакомиться со следующей учебно-методической документацией:

- рабочей программой дисциплины;
- перечнем знаний, умений которыми обучающийся должен овладеть;
- тематическими планами занятий;
- контрольными мероприятиями;
- учебником, учебными пособиями, а также электронными ресурсами;
- перечнем вопросов к зачету и заданий.

После этого у обучающегося должно сформироваться четкое представление об объеме и характере знаний, умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение заданий учебной работы на лекциях и семинарских занятиях позволит успешно освоить дисциплину и создать хорошую базу для сдачи экзамена.

Промежуточная аттестация по дисциплине проводится в соответствии с учебным планом по семестрам в виде зачета.

Обучающийся допускается к зачету по дисциплине в случае выполнения им учебного плана. В случае наличия учебной задолженности обучающийся отрабатывает пропущенные занятия в форме, предложенной преподавателем.

Обучение по дисциплине предполагает контактную форму работы (лекционные, семинарские занятия) и самостоятельную работу обучающихся.

5.1. Методические рекомендации по подготовке к лекционным и семинарским занятиям

Изучение дисциплины содействует: приобретению студентами необходимой научно-теоретической базы и профессиональной подготовки по ключевым направлениям деятельности прокурора в судебном разбирательстве, формированию юридического мышления, знаний, умений и навыков применения положений и норм законодательства, иных нормативных правовых актов, регламентирующих деятельность прокурора в уголовном судопроизводстве, высокого уровня правосознания, ориентации на неукоснительное соблюдение Конституции Российской Федерации, норм действующего законодательства.

В связи с чем предполагается следующая последовательность в подготовке обучающихся к лекции:

- ознакомление с материалом предыдущей лекции;
- знакомство с тематикой предстоящей лекции (по тематическому плану, представленному в настоящей рабочей программе дисциплины);
- прочтение и анализ учебных пособий, учебников, научных статей по теме предстоящего лекционного занятия;
- подготовить вопросы, которые предполагается задать лектору по проблеме предстоящей лекции.

Цель семинарских занятий заключается в умении применять полученные знания в практической деятельности; в более глубоком осмыслении механизмов правового регулирования; в формировании гражданского мировоззрения на основе знаний принципов правосудия, нормативно-правовых актов.

5.2. Методические рекомендации к самостоятельной работе

Основной целью самостоятельной работы студентов является улучшение юридической профессиональной подготовки специалистов, направленное на формирование системы фундаментальных и профессиональных знаний, умений и навыков, которые они могли бы свободно и самостоятельно применять в практической деятельности.

Самостоятельная работа обучающихся направлена на решение следующих задач – углублять, расширять юридические профессиональные знания специалистов, формировать у них интерес к учебно-познавательной деятельности в сфере уголовного судопроизводства:

- углублять, расширять профессиональные знания студентов и формировать у них интерес к учебно-познавательной деятельности;
- научить студентов овладевать приемами анализа уголовного дела;
- развивать у них самостоятельность, активность, ответственность в ходе изучения учебной дисциплины;
- развивать познавательные способности будущих юристов по овладению профессиональной компетенцией.

Внеаудиторная самостоятельная работа выполняется по заданию преподавателя, но без его непосредственного участия. Для обеспечения внеаудиторной самостоятельной работы по дисциплине преподавателем разрабатывается перечень заданий для самостоятельной работы, который необходим для эффективного управления данным видом учебной деятельности обучающихся. Самостоятельная работа студентов включает

подготовку к устному опросу. Для этого студент изучает лекции, основную и дополнительную литературу, публикации, информацию из Интернет-ресурсов, и электронных библиотечных баз. Самостоятельная работа может осуществляться индивидуально или группами студентов 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 обучающийся должен уделять выполнению внеаудиторной самостоятельной работы в среднем не менее 3 часов. При выполнении внеаудиторной самостоятельной работы обучающийся может обращаться к преподавателю за консультацией с целью уточнения задания, формы контроля выполненного задания. Эффективность подготовки студентов зависит от качества ознакомления с рекомендованной литературой. Для подготовки к устному опросу студенту необходимо ознакомиться с материалом, посвященным изучаемой теме в учебнике или другой рекомендованной литературе, записях с лекционного занятия. Развернутый ответ должен следовать определенной логике и последовательности изложения, состоять из многих предложений, содержать доводы и выводы.

5.3. Методические рекомендации для подготовки к опросам по вынесенным на обсуждение темам

Устные опросы проводятся во время семинарских/практических занятий и возможны при проведении зачета в качестве дополнительного испытания при недостаточности результатов тестирования и решения заданий. Вопросы опроса не должны выходить за рамки объявленной для данного занятия темы. Устные опросы необходимо строить так, чтобы вовлечь в тему обсуждения максимальное количество обучающихся в группе, проводить параллели с уже пройденным учебным материалом данной дисциплины и смежными курсами, находить удачные примеры из современной действительности, что увеличивает эффективность усвоения материала на ассоциациях. Основные вопросы для устного опроса доводятся до сведения студентов на предыдущем практическом занятии. Письменные опросы позволяют проверить уровень подготовки к практическому занятию всех обучающихся в группе, при этом оставляя достаточно учебного времени для иных форм педагогической деятельности в рамках данного занятия. Письменный опрос проводится без предупреждения, что стимулирует обучающихся к систематической подготовке к занятиям. Вопросы для опроса готовятся заранее, формулируются узко, дабы обучающийся имел объективную возможность полноценно его осветить за отведенное время (10 – 15 мин.). Письменные опросы целесообразно применять в целях проверки усвояемости значительного объема учебного материала, например, во время проведения экзамена, когда необходимо проверить знания студентов по всему курсу. При оценке опросов анализу подлежит точность формулировок, связность изложения материала, обоснованность суждений, опора на действующее семейное законодательство.

5.4. Методические рекомендации по решению ситуационных задач и кейс-заданий

Кейс-задача, кейс (case) – это конкретная практическая ситуация, рассказывающая о той или иной ситуации, в которой зачастую заложена некая проблема.

Решение кейс-заданий осуществляется с целью проверки уровня 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.

5.5. Методические рекомендации по выполнению тестовых заданий

Тестирование проводится 1 раз в течение семестра. Не менее чем за 1 неделю до тестирования, преподаватель должен определить студентам исходные данные для подготовки к тестированию: назвать разделы (темы, вопросы), по которым будут задания в тестовой форме, нормативные правовые акты и теоретические источники (с точным указанием разделов, тем, статей) для подготовки. При прохождении тестирования пользоваться конспектами лекций, учебниками, и нормативными актами не разрешено.

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 является как один, так и несколько вариантов. Выбор должен быть сделан в пользу наиболее правильного или правильных ответов.

На выполнение теста отводится ограниченное время. Оно может варьироваться в зависимости от уровня тестируемых, сложности и объема теста.

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

1. *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

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

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

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

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

5. 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».

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

7. 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

8. Уголовное право России. Общая часть: учебник / под ред. Н.Г. КАдникова. – М.: Юриспруденция, 2018.

9. Уголовное право России. Особенная часть: учебник / под ред. Н.Г. КАдникова. – М.: Юриспруденция, 2018.

10. 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

1. ГАС РФ «Правосудие» - www.sudrf. ru
2. Интернет-библиотека СМИ Public.- ruwww.public. ru
3. Сайт Верховного Суда РФ - www.vsrf. ru
4. Сайт Государственной Думы - http://duma.gov.ru
5. Сайт Московского городского суда - www.mos-gorsud.ru
6. Сайт Президента РФ - http://www.kremlin.ru
7. Справочная правовая система «КонсультантПлюс» www.consultant. ru
8. СПС Гарант v.7 - Справочно-Правовая Система
9. Университетская информационная система Россия. УИС РОССИЯ - http:// www.cir.ru
10. Электронная Библиотека Диссертаций Российской государственной библиотеки ЭБД РГБ - http://diss.rsl. ru
11. 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».