Федеральное государственное казенное
образовательное учреждение высшего образования
«Университет прокуратуры Российской Федерации»

Дальневосточный юридический институт (филиал)

Кафедра уголовно-правовых дисциплин

УТВЕРЖДАЮ
Директор
И.В. Малофеев
16. 05 .2025

Противодействие киберпреступности

Рабочая программа учебной дисциплины

Специальность 40.05.04 Судебная и прокурорская деятельность

Уровень профессионального образования
высшее образование - специалитет

Специализация
Прокурорская деятельность

Год начала подготовки – 2022

Очная форма обучения

Владивосток, 2025

Рабочая программа учебной дисциплины «Противодействие киберпреступности» обсуждена и одобрена на совместном заседании кафедр Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации от 28.02.2025, протокол № 8.

Рабочая программа учебной дисциплины рекомендована к использованию в образовательном процессе решением учебно-методического совета Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации от 16.05.2025, протокол № 1.

Авторы-составители:

Побегайло А.Э., доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, кандидат юридических наук;

Сыромля Л.Б., заведующий кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук.

Рецензент:

Хазизулин В.Ю., доцент кафедры прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук.

Противодействие киберпреступности: рабочая программа учебной дисциплины. – Владивосток: ДЮИ (ф) УП РФ, 2025. – 47 с.

Рабочая программа учебной дисциплины «Противодействие киберпреступности» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.04 Судебная и прокурорская деятельность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 18.08.2020 № 1058.

Оглавление

1. Цели освоения учебной дисциплины

Целями освоения учебной дисциплины «Противодействие киберпреступности» являются: структурирование имеющихся и получение новых знаний по вопросам борьбы с киберпреступностью; закрепление имеющихся и формирование новых умений и навыков, необходимых для борьбы с киберпреступностью; формирование компетенций, указанных в разделе 2 настоящей программы.

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование у обучающегося следующих компетенций и их структурных элементов:

Профессиональные компетенции

Тип задач профессиональной деятельности:	Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции, которую формирует дисциплина	Планируемые результаты обучения по дисциплине
правоприменительный	**ПК-2.** Способен квалифицированно применять правовые нормы при осуществлении прокурорской деятельности	**ПК–2.1.** Применяет правовые нормы при осуществлении прокурорского надзора за соблюдением Конституции Российской Федерации и исполнением законов, действующих на территории Российской Федерации	**Знает**: законодательство РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; комплекса нормативных правовых актов, касающегося

			правоотношений в сфере охраны цифровой информации; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности; **Умеет:** осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам борьбы с киберпреступностью); **Владеет навыками***:* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений.
		ПК-2.3. Применяет правовые нормы при осуществлении уголовного преследования	**Знает:** понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за

			них; соотношения отраслей права в вопросах охраны информации; **Умеет:** применять на практике нормативные правовые акты материального и процессуального права, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; **Владеет навыками***:* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений.
		ПК-2.4. Применяет правовые нормы, регламентирующие участие прокурора в рассмотрении дел судами	**Знает:** законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации; **Умеет:** осуществлять правильную уголовно-правовую квалификацию

			киберпреступлений; **Владеет навыками:** правоприменения в сфере борьбы с киберпреступностью.

3. Место учебной дисциплины в структуре основной образовательной программы

Учебная дисциплина «Противодействие киберпреступности» относится к части дисциплин основной образовательной программы, формируемой участниками образовательных отношений.

Для освоения учебной дисциплины необходимы знания, умения и навыки, сформированные в ходе изучения следующих дисциплин:

1. Уголовное право.
2. Уголовный процесс.
3. Квалификация преступлений.
4. Криминология.

Дисциплина «Противодействие киберпреступности» изучается параллельно с дисциплинами:

1. Противодействие коррупции;
2. Практика и проблемы назначения уголовных наказаний.

В результате освоения дисциплины формируются знания, умения и навыки, необходимые для прохождения преддипломной практики и государственной итоговой аттестации.

4. Объем и структура учебной дисциплины

Общая трудоемкость дисциплины в ЗЕТ (час.) 2 ЗЕТ, 72 час.	
Виды учебной работы	**Очная форма обучения**
	Семестр (семестры) изучения
	8
	Часы
Контактная работа	**36**
в том числе:	
лекции	12
практические занятия	24
Самостоятельная работа	**36**
Промежуточная аттестация – зачет	

Тематический план для очной формы обучения

Раздел, тема учебной дисциплины, формы контроля	Всего часов	Виды учебной деятельности студента (в часах)				
		Контактная работа	в том числе:		Самостоятельная работа	Зачет
			Лекции	Практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*
Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика	9	4	2	2*	5	
Тема 2. История зарождения и современное состояние киберпреступности в РФ и иностранных государствах	9	4	2	2*	5	
Тема 3. Преступления в сфере компьютерной информации как вид киберпреступлений	11	6	2	4*	5	
Тема 4. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий	13	8	4	4*	5	
Тема 5. Проблемы квалификации киберпреступлений. Криминологическая характеристика киберпреступности и основные проблемы борьбы с ней	9	4	2	2*	5	
Тема 6. Некоторые вопросы, связанные с расследованием киберпреступлений	9	4		4*	5	
Тема 7. Соотношение уголовного, административного и гражданского права в вопросах охраны	8	4		4*	4	

информации						
Тема 8. Международно-правовые аспекты противодействия киберпреступности на современном этапе	4	2		2	2	
Зачет						
Итого часов	**72**	**36**	**12**	**24**	**36**	
В том числе часов на занятия в активных, интерактивных формах	24	24		24		

Примечание: В графе 5 звездочкой «» отмечены часы, отводимые на занятия, организуемые в активных, интерактивных формах.*

5. Содержание учебной дисциплины

Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика

Предмет учебной дисциплины «Противодействие киберпреступности». Метод учебной дисциплины «Противодействие киберпреступности», ее система и задачи. Понятие киберпреступности.

Основные определения термина «киберпреступность» в правовой науке современной России. Основные определения понятия «киберпреступность» в правовой науке иностранных государств. Киберпреступность и компьютерные преступления — вопросы соотношения терминов.

Тема 2. История зарождения и современное состояние киберпреступности в Российской Федерации и иностранных государствах

Киберпреступность в исторической перспективе. Исторический подход к изучению развития информационно-телекоммуникационных технологий как необходимая предпосылка изучения киберпреступности. Этапы развития вычислительной техники, языков программирования и программного обеспечения; основные причины и условия возникновения киберпреступлений на каждом из данных этапов. Появление и развитие информационно-телекоммуникационных сетей. Зарождение киберпреступлений, их первоначальные виды. Развитие и эволюция киберпреступлений. Современное состояние киберпреступности, ее уровень, структура и динамика. Прогноз состояния киберпреступности. Международный характер явления: причины и дальнейшее развитие.

Тема 3. Преступления в сфере компьютер-ной информации как вид 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, 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 4. Киберпреступления, совершаемые посредством информационно-телекоммуникационных 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.

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.

Разжигание национальной, классовой и иной розни, угроза убийством, осуществляемые с помощью киберсредств.

Кибертерроризм –его определение, предмет и способы совершения. 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.

Незаконные изготовление и оборот порнографических материалов или предметов, совершаемые с использованием информационно-телекоммуникационных сетей. Использование компьютеров, компьютерных сетей и иных технологичных киберсредств в создании и распространении детской порнографии. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов, совершаемые путем применения кибертехнологий.

Прочие киберпреступления.

Тема 5. Проблемы квалификации кибер-преступлений. Криминологическая характеристика киберпреступности и основные проблемы борьбы с ней

Транснациональный характер киберпреступности как один из основных проблемных аспектов борьбы с нею. Недостатки конструкции норм уголовного закона, регулирующих уголовную ответственность за совершение киберпреступлений, а равно и нормативных правовых актов, относящихся к иным отраслям, регулирующих смежные общественные отношения.

Проблемы, связанные с механизмом процессуального взаимодействия правоохранительных и судебных органов разных стран.

Проблемы технического плана, касающиеся процессуальной деятельности следственных органов по обнаружению и фиксации доказательств цифрового характера, а равно и оперативно-розыскной деятельности, связанной с расследованием и раскрытием киберпреступлений. Сетевая «анонимность» и правовой нигилизм. Некоторые аспекты сетевой культуры и менталитета как поведенческий детерминант преступности. Незаконное использование криптовалют и средств электронных платежей как криминологическая проблема. «Даркнет», «глубокие сети» и их торговые площадки – вопросы криминализации их незаконного использования и влияния на преступность.

Тема 6. Некоторые вопросы, связанные с расследованием киберпреступлений

Техника, тактика и методика расследования киберпреступлений.

Некоторые вопросы оперативно-розыскной деятельности, связанной с

киберпреступлениями. Отдельные моменты уголовно-процессуального характера в расследовании киберпреступлений.

Наиболее распространенные ошибки, допускаемые при расследовании и раскрытии данного рода преступлений.

Тема 7. Соотношение уголовного, административного и гражданского права в вопросах охраны информации

Право интеллектуальной собственности. Важность разграничения полномочий между уголовным и гражданским правом в аспекте защиты общественных отношений информационного характера.

Административно-правовые нормы, устанавливающие ответственность за проступки в сфере связи и информации.

Тема 8. Международно-правовые аспекты противодействия киберпреступности на современном этапе

Имплементация международно-правовых норм, регулирующих вопросы, связанные с цифровыми технологиями, информационно-телекоммуникационными сетями и смежными вопросами в национальное законодательство. Вопросы гармонизации норм уголовного и уголовно-процессуального законодательства, касающихся криминализации киберпреступлений, их расследования и судебного разбирательства.

Основные международно-правовые договоры, регулирующие расследование киберпреступлений.

Международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними.

Подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений.

Разграничение юрисдикции при расследовании киберпреступлений.

6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине

Важным видом работы при изучении дисциплины «Противодействие киберпреступности» является самостоятельная (внеаудиторная) работа обучающегося, которая осуществляется в следующих формах:

1. Подготовка к практическим занятиям.
2. Подготовка и написание контрольных работ.
3. Подготовка и написание докладов.

Примерный перечень вопросов для самостоятельной подготовки к практическим занятиям, структурированный по темам

Тема 1. Понятие киберпреступности

1. Каким образом возникло такое явление как киберпреступность?

2. Каков современный взгляд на киберпреступность в российской и иностранной правовых науках?

3. Что является предметом учебной дисциплины «Противодействие киберпреступности».

4. Каков метод учебной дисциплины «дисциплины «Противодействие киберпреступности», ее система и задачи?

Тема 2. История зарождения и современное состояние киберпреступности в РФ и иностранных государствах

1. Каково современное состояние киберпреступности в РФ и основные тенденции развития?

2. Киберпреступность в исторической перспективе – зарождение и развитие.

3. Какие существуют основные условия возникновения киберпреступлений?

4. Какова современная структура, динамика, и общее состояние киберпреступности?

5. Каков прогноз развития киберпреступности?

6. Почему преступность имеет международный характер?

Тема 3. Преступления в сфере компьютерной информации как вид киберпреступлений

1. Каковы проблемы квалификации неправомерного доступа к компьютерной информации?

2. Какие существуют основные приемы и способы неправомерного доступа к компьютерной информации?

3. Каковы основные средства и способы создания, использования и распространения вредоносных компьютерных программ?

4. Какие существуют вопросы квалификации преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ?

5. Назовите основные вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

6. Назовите основные аспекты квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

7. Каковы основные вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации?

8. В чем состоят особенности информации как предмета преступления? Назовите основные аспекты использования киберсредств как средства и способа совершения преступления.

Тема 4. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий

1. Каковы основные направления борьбы с распространением детской порнографии в сети Интернет?
2. Назовите составы преступлений, предусматривающие ответственность за доведение до самоубийства, пособничество и подстрекательство к нему, совершаемые с помощью информационно-телекоммуникационных сетей и дайте им характеристику.
3. Какие существуют основные проблемы противодействия экстремизму и терроризму в сети Интернет?
4. Назовите основные виды мошенничества, связанного с кредитными картами, осуществляемого с применением высоких технологий.
5. Каковы особенности расследования краж финансовых средств из электронных банковских сетей?
6. Дайте характеристику и назовите основные проблемы квалификации нарушения авторских, патентных и смежных прав, совершаемых с использованием киберсредств.
7. Что такое кибертерроризм (определение, его предмет и способы совершения)?
8. Назовите основные пути финансирования терроризма через информационно-телекоммуникационные сети и вопросы, связанные с квалификацией данного деяния.
9. Какие существуют основные проблемы расследования случаев мошенничества, совершенных с помощью высоких технологий?
10. В чем основные особенности состава преступления, связанного с нарушением коммерческой и личной тайны?

Тема 5. Криминологическая характеристика киберпреступности и основные проблемы противодействия

В чем заключается транснациональный характер киберпреступности, и как он влияет на раскрытие такого рода преступлений?

1. Назовите основные проблемы, связанные с недочетами соответствующего законодательства, регулирующего уголовную и административную ответственность за совершение киберпреступлений и киберпроступков.
2. Каковы основные пути совершенствования механизмов взаимодействия правоохранительных и судебных органов разных стран по вопросам расследования киберпреступлений и судебного разбирательства по такого рода делам?
3. Какие существуют основные проблемы технического характера, возникающие при расследовании такого рода дел?
4. Как влияет сетевая псевдоанонимность и сетевая культура на киберпреступность?

5. Назовите основные аспекты влияния незаконного использования криптовалют на киберпреступность и иные виды преступности.

6. Феномен «глубокой сети» и «Даркнета» в генезисе преступности.

Тема 6. Некоторые вопросы, связанные с расследованием киберпреступлений

1. Каковы основные приемы и рекомендации техники, тактики и методики расследования компьютерных и сопряженных с ними преступлений?

2. Назовите основные вопросы оперативно-розыскной деятельности, связанной с киберпреступлениями.

3. Какие существуют проблемные моменты уголовно-процессуального характера в расследовании киберпреступлений?

4. Каковы наиболее распространенные ошибки, допускаемые при расследовании и раскрытии данного рода преступлений?

Тема 7. Соотношение уголовного, административного и гражданского права в вопросах охраны информации

1. Что такое право интеллектуальной собственности, и какие нормативные акты его регулируют?

2. В чем заключается важность разграничения полномочий между уголовным, гражданским и административным правом в аспекте защиты общественных отношений информационного характера?

3. Каковы основные проблемы гражданских исков по делам о киберпреступлениях?

4. Каковы основные вопросы административного производства по делам, связанным с проступками в сфере информации?

Тема 8. Международно-правовой аспект противодействия киберпреступности

1. Назовите основные международно-правовые договоры, регулирующие расследование киберпреступлений.

2. Какие существуют международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними?

3. Какие существуют подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений?

4. Каковы правила по разграничению юрисдикции при расследовании киберпреступлений, и в каких нормативных правовых актах они содержатся?

Методические рекомендации по подготовке к практическим занятиям

Практическое занятие по данной дисциплине, как и по другим учебным дисциплинам, представляет собой групповое обсуждение студентами темы

учебной программы под руководством преподавателя. В рамках практического занятия проверяется степень усвоения студентами изучаемого материала, закрепляются, углубляются и расширяются знания, полученные на лекциях или в результате самостоятельного изучения, подводятся итоги самостоятельного изучения.

Тщательная подготовка к практическим занятиям является важной составляющей успеха при сдаче зачета по дисциплине «Противодействие киберпреступности». В этих целях при подготовке к практическому занятию каждый студент должен:

внимательно ознакомиться с вопросами, выносимыми на обсуждение;

заблаговременно изучить необходимую учебную и научную литературу, законодательные акты и нормативный материал по теме обсуждения;

при наличии интереса выбрать тему научного сообщения или доклада и подготовить его;

по указанию преподавателя аннотировать научную статью по теме занятия;

подготовиться к решению практических задач или участию в деловой игре;

по соответствующим темам выполнить письменную практическую домашнюю работу;

подготовить презентацию по теме, указанной преподавателем.

При обсуждении вопросов, обозначенных в планах практических занятий, необходимо ссылаться на конкретные нормы правовых актов. Практическое занятие предполагает активное участие всех студентов в обсуждении вопросов темы. Поощряется самостоятельность суждений и использование в ответе примеров из прокурорской и судебной практики.

Варианты контрольных работ

Вариант 1

1. В чем заключается транснациональный характер киберпреступности, и как он влияет на раскрытие такого рода преступлений?

2. Каковы правила по разграничению юрисдикции при расследовании киберпреступлений, и в каких нормативных правовых актах они содержатся?

Вариант 2

1. Каков современный взгляд на киберпреступность в российской и иностранной правовых науках?

2. Каким образом возникло такое явление как киберпреступность?

Вариант 3

1. Каково современное состояние киберпреступности в РФ и основные тенденции развития?

2. Какие существуют подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений?

Вариант 4

1. Какие существуют международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними?
2. Какие вы можете назвать основные международно-правовые договоры, регулирующие расследование киберпреступлений?

Вариант 5

1. Какие существуют основные условия возникновения киберпреступлений?
2. Что такое кибертерроризм (определение, его предмет и способы совершения)?

Вариант 6

1. Какова современная структура, динамика, и общее состояние киберпреступности?
2. Что такое право интеллектуальной собственности, и какие нормативные акты его регулируют?

Вариант 7

1. Какие существуют научные прогнозы развития киберпреступности в ближайшем будущем?
2. Почему киберпреступность имеет столь ярко выраженный международный характер?

Вариант 8

1. Назовите основные проблемы квалификации неправомерного доступа к компьютерной информации.
2. Проанализируйте основные проблемные моменты уголовно-процессуального характера в расследовании киберпреступлений.

Вариант 9

1. Каковы наиболее распространенные ошибки, допускаемые при расследовании и раскрытии преступлений, связанных с неправомерным доступом к компьютерной информации?
2. Назовите основные виды мошенничества, связанного с кредитными картами, осуществляемого с применением высоких технологий.

Вариант 10

1. Какие существуют основные приемы и способы неправомерного доступа к компьютерной информации?

2. В чем заключаются основные проблемные аспекты действий оперативно-розыскного характера, связанных с расследованием киберпреступлений?

Вариант 11

1. Какие существуют основные проблемы технического характера, возникающие при расследовании уголовных дел, связанных с созданием, использованием и распространением вредоносных компьютерных программ?

2. Раскройте основные проблемы, связанные с несовершенством соответствующего законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.

Вариант 12

1. Каковы основные орудия и способы создания, использования и распространения вредоносных компьютерных программ?

2. Назовите и раскройте сущность основных приемов и рекомендаций техники, тактики и методики расследования компьютерных и сопряженных с ними преступлений.

Вариант 13

1. Назовите основные уголовно-процессуальные вопросы расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ.

2. Назовите основные пути совершенствования механизмов взаимодействия правоохранительных и судебных органов разных стран по вопросам расследования киберпреступлений и судебного разбирательства по ним.

Вариант 14

1. Назовите основные вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

2. В чем основные особенности информации как предмета преступления?

Вариант 15

1. В чем основные особенности состава преступления, связанного с нарушением коммерческой и личной тайны?

2. Каковы основные направления борьбы с распространением детской порнографии в сети Интернет?

Вариант 16

1. Какие существуют основные проблемы противодействия экстремизму в сети Интернет?

2. Какие существуют основные проблемы расследования случаев мошенничества, совершенных с помощью высоких технологий?

Вариант 17

1. Каковы основные способы нарушения авторских и смежных прав, совершаемые с использованием киберсредств, в чем заключаются основные проблемы квалификации таких деяний?

2. Каково значение правовой компаративистики в рамках развития российского законодательства, посвященного противодействию киберпреступности?

Вариант 18

1. Каковы основные особенности вовлечения несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов, чем обусловлены проблемы выявления таких деяний?

2. Перечислите и раскройте основные криминогенные фоновые явления киберпреступности.

Вариант 19

1. Дайте характеристику составу преступления, предусмотренному ст. 159.3 УК РФ «Мошенничество, совершенное с использованием платежных карт», указав его проблемные аспекты.

2. Каковы основные особенности нарушения изобретательских и патентных прав, совершаемых с использованием киберсредств.

Вариант 20

1. Дайте уголовно-правовую характеристику незаконного распространения объектов авторского права и смежных прав путем использования файлообменного протокола «торрент».

2. Каковы особенности незаконного сбыта или пересылки наркотических средств, психотропных веществ или их аналогов, а также незаконных сбыта или пересылки растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, совершаемых с использованием информационно-телекоммуникационных сетей и иных киберсредств?

Вариант 21

1. Дайте уголовно-правовую характеристику состава склонения к совершению самоубийства или содействия совершению самоубийства.

2. В чем заключаются основные вопросы разграничения составов, связанных с хищениями путем обмана или злоупотребления доверием, осуществляемыми с использованием информационно-телекоммуникационных сетей?

Вариант 22

1. Каковы основные особенности нарушения патентных и смежных прав, осуществляемых с использованием киберсредств, в чем заключаются основные проблемы квалификации таких деяний?

2. Назовите основные механизмы рецепции международных правовых норм, касающихся цифровых общественных отношений, в национальное законодательство.

Методические рекомендации по написанию контрольных работ

Целями написания студентом контрольных работ являются: а) изучение студентом теоретического материала по определенным вопросам в соответствии с заданиями по выполнению контрольных работ; б) изучение действующего законодательства; в) развитие навыков применения правовых предписаний к конкретным ситуациям; г) развитие навыков работы с нормативными правовыми актами, специальной литературой; д) приобретение опыта поиска и отбора необходимого материала для раскрытия поставленных вопросов.

Содержание работы должно свидетельствовать о знании студентом понятийного аппарата, правовой регламентации общественных отношений, об умении правильно применять нормативные правовые акты и их анализировать. Также приветствуется творческий подход студента к раскрытию вопросов, изложению предложений по совершенствованию законодательства.

Практические рекомендации. Выполнение контрольной работы предполагает несколько этапов.

Первоначально студенту необходимо ознакомиться с заданиями и методическими рекомендациями по выполнению контрольных работ. Студент выполняет работу по одному варианту заданий, который определяется по согласованию с преподавателем. В случае если контрольная работа студента выполнена не в соответствии с заданиями по выполнению контрольных работ на новый учебный год, то она не подлежит проверке и возвращается студенту с отметкой «не зачтено».

Каждый вариант работы состоит из двух тем. В рамках выполнения контрольной работы студенту необходимо кратко изложить основные научные воззрения на тему, где необходимо – привести также примеры из судебной и/или следственной практики. В работе должны присутствовать постраничные сноски на литературные источники и список литературы. Список литературы не является исчерпывающим. Студент может дополнить его как специальной литературой, так и нормативными правовыми актами, судебными решениями, но лишь в той мере, которая необходима для более полного раскрытия теоретического вопроса, решения задачи (казуса, конфликтной ситуации).

Затем студент приступает к собственно *выполнению контрольной работы*. После изучения необходимых источников студент приступает к написанию работы. Если задание содержит теоретический вопрос, то его следует раскрывать по существу поставленного вопроса. Решение задачи (казуса, конкретной ситуации) следует начинать с внимательного ознакомления с предложенными условиями и поставленными вопросами. Ответы на них должны быть даны по существу с указанием ссылок на соответствующие статьи законов и иных нормативных правовых актов. В случае противоречия предписаний законов и иных нормативных правовых актов, студент должен указать, почему он руководствовался именно этим правовым актом, а не другим, регулирующим это общественное отношение и проанализировать выявленную коллизию.

При выполнении работы необходимо использовать СПС «КонсультантПлюс» или СПС «Гарант».

Оформление контрольной работы. Работа должна быть оформлена надлежащим образом. Её объем должен быть не более 15 машинописных страниц (шрифт 14 через 1,5 интервал).

Работа должна иметь титульный лист с указанием названия вуза и кафедры, наименования дисциплины, фамилии, имени, отчества преподавателя, номера контрольного задания, данных о студенте (фамилия, имя, отчество, форма обучения, курс). В работе указывается: а) название теоретического вопроса и излагается его раскрытие; б) задача (казус, конкретная ситуация в случае ее наличия) и её решение; в) список использованной литературы, оформленный в соответствии с предъявляемыми требованиями.

Страницы работы должны быть пронумерованы и прошиты (переплетены) без использования файл-вкладыша.

Список использованной литературы должен состоять из нескольких разделов. Первый раздел – «нормативные правовые акты», в котором указывается перечень нормативных правовых актов с учетом их соподчиненности по юридической силе. Например:

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. [Электронный ресурс] // Консультант Плюс - Режим доступа: http://base.consultant.ru/.

2. Федеральный закон «О прокуратуре Российской Федерации» от 17.01.1992 №2202-1 [Электронный ресурс] // Консультант Плюс - Режим доступа: http://base.consultant.ru/.

3. Федеральный закон от «О порядке рассмотрения обращений граждан Российской Федерации» от 02.05.2006 №59-ФЗ [Электронный ресурс] // Консультант Плюс - Режим доступа: http://base.consultant.ru/.

Второй раздел – «судебные решения» (или судебная практика), если при выполнении контрольной работы использовались решения Конституционного Суда РФ, Верховного Суда РФ и иных судебных органов. Третий раздел – «международные правовые акты», в случае их использования при написании

работы. Четвертый раздел – «специальная литература». В него включаются монографии, научные статьи, материалы научно-практических конференций по вопросу, поставленному в заданиях по выполнению контрольных работ. В этом разделе литература указывается в алфавитном порядке по фамилии автора или первой букве названия работы. Газетные статьи включаются в список специальной литературы также в алфавитном порядке по фамилии автора статьи. Например:«Головинская И.В., Крестинский М.В., Головинский М.М. Ретроспектива и перспектива стадии возбуждения уголовного дела // Современное право. – 2016. –№11». Указанная статья включается в список специальной литературы.

Затем обучающемуся необходимо предоставить контрольную работу на проверку. Срок представления работы на проверку определяется в соответствии с учебным графиком. Студент должен своевременно представить выполненную работу на проверку. Следует учесть, что проверка осуществляется преподавателем в течение 10 дней с момента регистрации работы на кафедре. Поэтому рекомендуется представлять её до начала сессии, поскольку она может быть не зачтена и потребуется время для ее доработки.

Контрольная работа оценивается с учетом ее содержания и оформления. Она не может быть зачтена, если не раскрыт теоретический вопрос, неправильно решены задачи (казусы) или она выполнена на основе нормативных правовых актов, которые утратили свою силу. Если работа не зачтена, то она с письменными замечаниями преподавателя (рецензией) возвращается студенту.

В случае возвращения работы студент знакомится с замечаниями, изложенными в рецензии. Они могут касаться содержания работы (например, не раскрыт теоретический вопрос, отсутствует законодательная база исследования) и её оформления (например, неправильно оформлен или отсутствует список использованной литературы, неправильно оформлены или отсутствуют ссылки в работе).

В соответствии с рецензией устранение замечаний может осуществляться несколькими способами. Во-первых, посредством переработки всей работы и представления нового варианта выполнения контрольной работы в соответствии с предъявляемыми требованиями. Во-вторых, дополнением к тексту первоначальной работы материала, который полнее раскрывает вопрос. В-третьих, приложением к первоначальному варианту работы нового решения задачи (казуса, конкретной ситуации) или нового варианта составленной задачи (казуса, конкретной ситуации). Способ устранения замечаний указывается преподавателем в рецензии. В случае если он не указан в рецензии, то студент должен переработать текст работы и представить её на повторную проверку в соответствии с предъявляемыми требованиями. После устранения замечаний работа повторно представляется на проверку. Повторная работа оценивается положительно только в том случае, если студентом учтены все замечания, изложенные в рецензии.

Примерная тематика докладов

1. Основные подходы к определению понятия «киберпреступность» и смежных понятий в правовой науке иностранных государств.
2. Основные подходы к определению понятия «киберпреступность» и смежных понятий в правовой науке современной России.
3. Современное состояние киберпреступности в Российской Федерации и мире – основные тенденции развития.
4. Киберпреступность в исторической перспективе.
5. Причины и условия возникновения киберпреступлений.
6. Современная структура, динамика, и общее состояние киберпреступности.
7. Киберпреступность: прогноз развития.
8. Международный характер киберпреступности.
9. Неправомерный доступ к компьютерной информации – проблемы квалификации.
10. Основные проблемные аспекты квалификации создания, использования и распространения вредоносных компьютерных программ.
11. Понятие «вредоносной программы» как средства совершения преступления.
12. «Иная компьютерная информация» как средство совершения преступления.
13. Вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
14. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие, особенности конструкции состава, вопросы квалификации.
15. Информация как предмет преступления.
16. Кибернетические (цифровые) способы совершения преступлений как критерий квалификации.
17. Основные направления борьбы с распространением детской порнографии в сети Интернет.
18. Проблемы противодействия экстремизму в сети Интернет.
19. Мошенничество, совершенное с использованием платежных карт.
20. Расследование краж финансовых средств из электронных банковских сетей.
21. Кибертерроризм – определение, его предмет и способы совершения.
22. Проблемы расследования случаев мошенничества в сфере компьютерной информации.
23. Нарушение коммерческой тайны, совершенное с использованием киберсредств.
24. Нарушение личной тайны, совершенное с использованием киберсредств.

25. Транснациональный характер киберпреступности как актуальная проблема борьбы с нею.

26. Основные проблемы законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.

27. Основные проблемы механизмов взаимодействия правоохранительных и судебных органов разных стран.

28. Основные технические проблемы противодействия киберпреступности.

29. «Анонимность» в информационно-телекоммуникационных сетях как фактор развития правового нигилизма.

30. Основные аспекты сетевой культуры и менталитета, выступающие как поведенческие детерминанты преступности.

31. Незаконное использование криптовалют и средств электронных платежей как криминологическая проблема.

32. Влияние на преступность и вопросы криминализации незаконного использования «глубоких сетей» и их торговых площадок.

33. Техника, тактика и методика расследования компьютерных преступлений.

34. Техника, тактика и методика расследования преступлений, совершенных с использованием киберсредств и способов.

35. Отдельные моменты уголовно-процессуального характера в расследовании киберпреступлений.

36. Наиболее распространенные ошибки, допускаемые при расследовании и раскрытии киберпреступлений.

37. Соотношение уголовного, административного и гражданского права в вопросах охраны интеллектуальной собственности.

38. Важность разграничения полномочий между уголовным и гражданским правом в аспекте защиты общественных отношений информационного характера.

39. Основные международно-правовые договоры, регулирующие расследование киберпреступлений.

40. Международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними, их полномочия.

41. Подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений.

42. Вопросы разграничения юрисдикции при расследовании киберпреступлений.

Методические рекомендации по подготовке доклада

Доклад (нем. referat, от лат. refere - докладывать, сообщать) –письменный доклад или выступление по определённой теме, в котором обобщается информация из одного или нескольких источников.

Доклад в учебном процессе представляет собой краткое изложение в письменном виде или в форме публичного доклада содержания научного

труда или трудов специалистов по избранной теме, обзор литературы определенного направления.

Структура доклада включает следующие обязательные части: титульный лист; содержание (оглавление); введение; основная часть (раскрывается сущность выбранной темы); заключение; список использованной литературы.

Доклад должен быть правильно и аккуратно оформлен. Текст доклада (рукописный или в компьютерном исполнении) должен быть разборчивым, без стилистических и грамматических ошибок. Примерный объем доклада составляет 15–25 машинописных страниц.

Выбор темы доклада. Темы докладов указаны в настоящей рабочей программе. После консультации с преподавателем обучающийся может обосновать и сформулировать иную тему доклада.

Этапы работы над докладом**:** подготовительный этап; изложение материала; оформление доклада; устное сообщение по теме доклада.

Подготовительный этап предполагает составление плана, который служит организующим началом в самостоятельной работе студента, способствует систематизации материала и последовательности его изложения. Выделяются два способа составления плана: хронологический и проблемный. Хронологический предусматривает изучение явления в его историческом развитии. Проблемный предполагает рассмотрение нескольких явлений во взаимосвязи. Допустимо использование обоих способов. Как правило, пункты плана дословно повторяются в тексте доклада в качестве заголовков разделов. План составляется студентом самостоятельно.

Подготовительный этап включает поиск источников. Тема доклада определяет предмет изучения и задача студента – найти информацию, относящуюся к данному предмету. Работу с источниками целесообразно начинать с предварительного чтения, при этом следует выделять структурные единицы текста (закладками отмечаются те страницы, которые требуют более внимательного изучения). Исходя из результатов предварительного чтения, определяется дальнейший способ работы с источниками. Для ускорения работы с большими объемами текста вначале следует подробно изучить оглавление источника. Далее, выбрав разделы (фрагменты) текста, необходимо вдумчиво, неторопливо прочитать с «осмысленной проработкой» материал.

Просмотр источников предусматривает выделение в тексте: 1) главного; 2) основных доводов (аргументов); 3) выводов.

Следует обращать внимание на то, чтобы тезис вытекал из аргумента. Особое внимание надо уделить утверждениям автора, носящим проблематичный и гипотетический характер, а также скрытым вопросам по теме работы. Наиболее часто применяемый способ выделения главного в тексте – улавливание проблематичного характера утверждений, при этом следует давать оценку авторской позиции. В качестве рационального приема написания доклада применяют сравнительное чтение, предполагающее

ознакомление с различными мнениями по одному и тому же вопросу, анализ весомости и доказательности аргументов авторов текста, что позволяет сделать вывод о наибольшей убедительности одной из позиций.

Написание доклада. Текст доклада должен раскрывать тему, обладать цельностью и связностью. Раскрытие темы предполагает, что в тексте доклада излагаются относящиеся к теме материалы и предлагаются пути решения содержащейся в контексте проблемы. Связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность – смысловую законченность текста.

Сокращение слов в тексте не допускается. Исключения составляют общеизвестные сокращения и аббревиатуры.

Во введении раскрываются цели и задачи, стоящие перед автором, объект и предмет изучения, дается общая характеристика использованным источникам. Объем введения не должен превышать 2-3 страницы.

В основной части доклада рассматриваются вопросы, раскрывающие поставленную проблему. Если при подборе материала студент сталкивается с тем, что в литературе нет единой точки зрения на рассматриваемую проблему, то нужно привести основные, наиболее интересные точки зрения разных авторов и дать им свою оценку.

Заголовки разделов и подразделов печатаются без абзацного отступа, прописными буквами, без точки в конце, без подчеркивания, по центру. Если заголовок состоит из двух предложений, их разделяют точкой.

Статистический, цифровой материал должен обосновывать и иллюстрировать мнения и выводы автора. Не следует перегружать доклад цифрами, статистическими выкладками (при необходимости их можно поместить в приложении), так как это отвлекает от понимания главных узлов темы и связи между ними. В части доклада необходимо достаточно полно и убедительно раскрыть все пункты плана, сохраняя логическую связь между ними и последовательность перехода от одного к другому. Каждый раздел заканчивается кратким выводом.

В заключении доклада должны быть аргументированные, т.е. обоснованные выводы и показано, насколько решены поставленные задачи. Здесь обобщаются изложенные в основной части материалы, формулируются общие выводы, указывается, что нового лично для себя вынес автор доклада из работы над ним. Делая выводы, необходимо учитывать различные опубликованные точки зрения на изложенную в работе проблему, сопоставить их и отметить, какая из них больше импонирует автору доклада.

В докладе, в частности, во введении и заключении, необходимо излагать личное отношение автора к раскрываемым вопросам. Заключение по объему, как правило, не должно превышать введения.

Список источников следует за заключением и оформляется с новой страницы. Список использованной литературы призван показать научную, теоретическую и практическую базу проведенного исследования.

Рекомендуемое количество использованной литературы для письменных работ для текущего контроля – не менее 5 и не более 50 литературных источников, нормативных правовых документов и иных источников.

Все указанные в тексте авторы и их работы, а также процитированные труды должны быть включены в этот список.

Представление доклада и его защита. Подготовленный студентом доклад на бумажном и электронном носителях представляется на кафедру, где регистрируется в журнале поступающих работ. Датой сдачи работы считается ее регистрация на кафедре.

Устное сообщение по теме доклада делается на практических занятиях. Время устного изложения доклада 10–15 минут. Затем он обсуждается аудиторией. Докладчику задают вопросы по теме доклада. Вопросы могут быть заданы как преподавателем, так и присутствующими на защите доклада студентами.

Оценка доклада зависит от полноты и правильности освещения вопросов темы, степени использования литературы и нормативных источников, соблюдения требований к оформлению доклада, а также от качества ответов на устные вопросы при защите.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Изучение учебной дисциплины « Противодействие киберпреступности» завершается промежуточной аттестацией – зачетом в устной форме .

Методические рекомендации по подготовке к зачету

Билеты для сдачи зачета содержат 2 теоретических вопроса. Для подготовки к зачету, учащемуся необходимо использовать лекционный материал, а также основную и дополнительную литературу, указанную в данной рабочей программе, совместно с перечнем вопросов для подготовки к зачету. Ответ на каждый теоретический вопрос из перечня рекомендуется выписать в тетрадь для подготовки к зачету, для лучшего структурирования и закрепления знаний.

Перечень вопросов для подготовки к зачету

1. Предмет и метод учебной дисциплины «Противодействие киберпреступности».
2. Понятие киберпреступности в узком и расширительном толковании термина.
3. Основные определения термина «киберпреступность» в правовой науке современной России; вопросы соотношения с определением термина «компьютерная преступность».

4. Основные определения понятия «киберпреступность» в правовой науке западных иностранных государств.

5. Киберпреступность в исторической перспективе (зарождение киберпреступлений, их развитие и эволюция).

6. Современное состояние киберпреступности, ее уровень, структура и динамика.

7. Прогноз дальнейшего состояния киберпреступности.

8. Международный характер явления киберпреступности: причины и влияние на предотвращение киберпреступлений.

9. Неправомерный доступ к компьютерной информации (осуществление с помощью вредоносных программ; осуществление с помощью иных высокотехнологичных средств); преступные последствия данного деяния и его квалифицирующие признаки.

10. Создание, использование и распространение вредоносных компьютерных программ, их основные виды; квалифицирующие признаки данного деяния и вопросы определения момента его окончания.

11. «Вредоносная программа» как средство совершения преступления: понятие, виды, особенности квалификации.

12. «Иная компьютерная информация» как средство совершения преступления: понятие, виды, особенности квалификации.

13. Нейтрализация средств защиты компьютерной информации как специфическое деяние, способы и средства его совершения.

14. Вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

15. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие, особенности конструкции состава, вопросы квалификации.

16. Информация как предмет преступления.

17. Кибернетические (цифровые) способы совершения преступлений как критерий квалификации.

18. Наиболее опасные из современных видов вирусных программ, механизм их действия.

19. Троянские программы, их отличие от вирусов, механизм их действия.

20. Информация как предмет преступления.

21. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, осуществляемые с использованием информационно-телекоммуникационных технологий.

22. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации, осуществляемые с использованием сети Интернет.

23. Разжигание национальной, классовой и иной ненависти и вражды, а равно унижение человеческого достоинства, осуществляемые с помощью киберсредств.

24. Угрозы убийством, осуществляемые с помощью информационно-телекоммуникационных технологий.

25. Кража финансовых средств из электронных банковских сетей и основные пути ее совершения. Кража финансовых средств граждан (физических лиц) из электронных банковских сетей и платежных систем: проблемы квалификации, основные пути совершения.

26. Мошенничество, совершенное с применением киберсредств (компьютерных программ, сетей, иных высокотехнологичных средств).

27. Спам (как средство совершения преступлений): понятие, общественная опасность, основные способы борьбы.

28. Нарушение коммерческой и личной тайны: основные составы, вопросы квалификации.

29. Незаконные организация и проведение азартных игр, совершаемые с использованием сети Интернет и иных информационно-телекоммуникационных сетей.

30. Манипулирование рынком, осуществляемое с использованием информационно-телекоммуникационных технологий.

31. Основные проблемные аспекты законодательства, регулирующего уголовную и иную ответственность за совершение киберпреступлений.

32. Вопросы взаимодействия правоохранительных и судебных органов разных стран в рамках противодействия киберпреступности.

33. Основные аспекты сетевой культуры и менталитета, выступающие как поведенческие детерминанты преступности. «Анонимность» в информационно-телекоммуникационных сетях как фактор развития правового нигилизма.

34. Незаконное использование криптовалют и средств электронных платежей как криминологическая проблема.

35. Влияние на преступность и вопросы криминализации незаконного использования «глубоких сетей» и их торговых площадок.

36. Техника, тактика и методика расследования компьютерных преступлений.

37. Техника, тактика и методика расследования преступлений, совершенных с использованием киберсредств и способов.

38. Основные проблемы технического характера, препятствующие расследованию киберпреступлений.

39. Некоторые вопросы оперативно-розыскной деятельности, связанной с киберпреступлениями.

40. Отдельные моменты уголовно-процессуального характера в расследовании киберпреступлений.

41. Наиболее распространенные ошибки, допускаемые при расследовании и раскрытии компьютерных преступлений.

42. Право интеллектуальной собственности и его связь с борьбой с киберпреступностью.

43. Важность разграничения полномочий между уголовным и гражданским правом в аспекте защиты общественных отношений информационного характера.

44. Основные международно-правовые акты, регулирующие вопросы международного взаимодействия по борьбе с киберпреступностью, включая вопросы расследования киберпреступлений.

45. Международные организации, занимающиеся расследованием киберпреступлений и борьбой с ними.

46. Подразделения правоохранительных органов основных иностранных государств, занимающихся расследованием киберпреступлений.

47. Разграничение юрисдикции при расследовании киберпреступлений.

48. Доведение до самоубийства, совершенное с использованием сети «Интернет».

49. Клевета, осуществляемая с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

50. Нарушение неприкосновенности частной жизни, совершенное путем использования информационно-телекоммуникационных технологий. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенные с использованием киберсредств.

51. Нарушение авторских и смежных прав, совершенное с использованием киберсредств.

52. Вовлечение несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов.

53. Мошенничество, совершенное с использованием платежных карт, осуществляемое с применением кибертехнологий.

54. Неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.

55. Разжигание национальной, классовой и иной розни, угроза убийством, осуществляемые с помощью киберсредств.

56. Кибертерроризм – определение, его предмет и способы совершения.

57. Осуществление публичных призывов к осуществлению террористической деятельности или публичное оправдание терроризма, совершаемое с помощью информационно-телекоммуникационных технологий.

58. 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, совершаемые с использованием информационно-телекоммуникационных сетей и иных киберсредств.

59. Склонение к совершению самоубийства или содействие совершению

самоубийства, совершенное с помощью информационно-телекоммуникационной сети.

60. Организация деятельности, направленной на побуждение к совершению самоубийства.

61. Торговля людьми, совершаемая с использованием информационно-телекоммуникационных сетей.

62. Развратные действия, совершаемые путем использования ресурсов сети Интернет.

63. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации, осуществляемый через информационно-телекоммуникационные сети.

64. Нарушение изобретательских и патентных прав, совершенное с использованием информационно-телекоммуникационных технологий.

65. Мелкое хищение, совершенное лицом, подвергнутым административному наказанию, совершаемое с использованием информационно-телекоммуникационных сетей путем обмана или злоупотребления доверием.

66. Незаконная банковская деятельность, осуществляемая посредством использования информационно-телекоммуникационных сетей и иных киберсредств.

67. Неправомерный оборот средств платежей, в том числе электронных, осуществляемый с использованием информационно-телекоммуникационных технологий.

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

69. Организация террористического сообщества или организации и участие в нем (ней), осуществляемые с использованием киберсредств.

70. Заведомо ложное сообщение об акте терроризма, совершаемое с использованием киберсредств.

71. Организация преступного сообщества (преступной организации) или участие в нем (ней), совершаемая путем использование информационно-телекоммуникационных сетей и ресурсов.

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

73. Незаконные приобретение, передача, сбыт оружия, его основных частей, боеприпасов, взрывных устройств или взрывчатых веществ, осуществляемая с использованием информационно-телекоммуникационных сетей и их ресурсов.

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

75. 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.

76. Незаконные изготовление и оборот порнографических материалов или

предметов, совершаемые с использованием информационно-телекоммуникационных сетей.

Критерии оценки:

Оценка *«зачтено»* выставляется, если студент ответил на теоретические вопросы, содержащиеся в билете, продемонстрировав:

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках ИТТ и цифровой информации; уголовно-правового понятия, видов и сущности киберпреступлений, уголовно-правовых норм, устанавливающих ответственность за них; основных положений, законодательной техники по разработке нормативных правовых актов в сфере общественных отношений по охране цифровой информации; соотношения отраслей права в вопросах охраны информации; комплекса нормативных правовых актов, касающегося правоотношений в сфере охраны цифровой информации; соотношения уголовного, административного и гражданского права в вопросах охраны информации;

– *умения*: осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с ИТТ и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по предупреждению и противодействию киберпреступности; осуществлять правильную уголовно-правовую квалификацию киберпреступлений; находить нужную правовую информацию по вопросам киберпреступности и правильно ее использовать, составлять юридические документы (в части их мотивировки по вопросам противодействия киберпреступности); разрабатывать нормативные правовые акты в сфере противодействия киберпреступности; применять на практике нормативные правовые акты материального и процессуального права, их нормы, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, квалификации киберпреступлений, а равно надзора за их расследованием и раскрытием; юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности,

– *навыки* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы ИТТ, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере противодействия киберпреступности.

Оценка *«не зачтено»* выставляется, если студент не ответил на теоретические вопросы, содержащиеся в билете, либо допустил грубые ошибки при ответе на теоретические вопросы, показав тем самым отсутствие вышеперечисленных знаний, умений, навыков.

8. Учебно-методическое и информационное обеспечение учебной дисциплины

Основная учебная литература

1. Винокуров, Ю. Е. Прокурорский надзор : учебник для вузов / Ю. Е. Винокуров, А. Ю. Винокуров. – 15–е изд., перераб. и доп. – Москва : Юрайт, 2021. – 556 с

2. Винокуров, Ю. Е. Прокурорский надзор : учебник для вузов / Ю. Е. Винокуров, А. Ю. Винокуров ; под редакцией Ю. Е. Винокурова. – 17-е изд., перераб. и доп. – Москва : Юрайт, 2025. – 549 с. – (Высшее образование). – ISBN 978-5-534-20627-2. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/558480 (дата обращения: 05.03.2025). – Режим доступа: по подписке.

3. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / под научной редакцией И.А. Калиниченко. – Москва : ИНФРА-М, 2024. – 642 с. – (Высшее образование: Специалитет). –. – ISBN 978-5-16-017838-7. – Текст : электронный // ЭБС Znanium [сайт]. – URL: https://znanium.ru/catalog/product/2121606 (дата обращения: 05.03.2025). – Режим доступа: по подписке.

Дополнительная учебная литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 161 с. – (Высшее образование). – ISBN 978-5-534-07248-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/537247 (дата обращения: 05.03.2025).

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2023. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://www.urait.ru/bcode/530927 (дата обращения: 05.03.2025). – Режим доступа: по подписке.

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. – Москва : Юрайт, 2024. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/543351 (дата обращения: 05.03.2025).

4. Овчинский, В. С. Основы борьбы с киберпреступностью и кибертерроризмом : хрестоматия / сост. В.С. Овчинский. – Москва : Норма : ИНФРА-М, 2024. – 528 с. – ISBN 978-5-91768-814-5. – Текст : электронный // ЭБС Znanium [сайт]. – URL: https://znanium.com/catalog/product/2098567 (дата обращения: 05.03.2025). – Режим доступа: по подписке.

5. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. – 2-е изд., перераб. и доп. – Москва : Юрайт, 2024. – 357 с. – (Высшее образование). – ISBN 978-5-534-19108-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://www.urait.ru/bcode/555950 (дата обращения: 05.03.2025). – Режим доступа: по подписке.

Научные труды

Тема 1. Понятие киберпреступности

1. Гвоздева, В. А. Информатика, автоматизированные информационные технологии и системы: учебник / В.А. Гвоздева. — Москва : ФОРУМ : ИНФРА-М, 2021. — 542 с. - ISBN 978-5-8199-0877-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1220288 (дата обращения: 12.02.2021).

Тема 2. История зарождения и современное состояние киберпреступности в РФ и иностранных государствах

2. Введение в инфокоммуникационные технологии : учебное пособие / Л. Г. Гагарина, А. М. Баин, Г. А. Кузнецов [и др.] ; под ред. Л. Г. Гагариной. — Москва : ФОРУМ : ИНФРА-М, 2021. — 336 с. — (Высшее образование). - ISBN 978-5-8199-0768-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1144494

3. 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 «КонсультантПлюс».

4. 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 «КонсультантПлюс».

5. 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.

6. 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 «КонсультантПлюс».

Тема 3. Преступления в сфере компьютерной информации как вид киберпреступлений

1. Амелин Р.В. Правовой режим государственных информационных систем: монография / под ред. С.Е. Чаннова. М.: ГроссМедиа, 2016. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

2. 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.

3. Клименко А.К. Хищения безналичных и электронных денежных средств: вопросы квалификации // Российский следователь. 2020. N 5. С. 38 - 42. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

4. Русскевич Е.А. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ): вопросы квалификации // Уголовное право. 2020. N 5. С. 94 - 104. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

5. Русскевич Е.А. Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. 2018. N 10. С. 46 - 49. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

6. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. М.: Статут, 2016.– [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

7. 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 «КонсультантПлюс».

Тема 4. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий

1. 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 «КонсультантПлюс».

2. Васильева Н.А. Анализ цифровых платформ в сфере незаконного оборота наркотиков для построения криминалистической характеристики данного вида преступлений // Юридическая наука. 2020. №2. URL: https://cyberleninka.ru/article/n/analiz-tsifrovyh-platform-v-sfere-nezakonnogo-oborota-narkotikov-dlya-postroeniya-kriminalisticheskoy-harakteristiki-dannogo-vida

3. Гурко А. Пиратство и майнинг // ИС. Авторское право и смежные права. 2017. №11. С. 17-26.– [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

4. Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети Интернет //

Lexrussica. 2017. №7. С. 166-177.– [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

5. 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 «КонсультантПлюс».

6. 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.

7. Кочанова Т. Клевета: анализ судов по теме с важными примерами // Жилищное право. 2019. N 3. С. 105 - 112; Административное право. 2019. N 2. С. 15-19. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

8. Липин Д. Проблемы оценки ущерба, причиненного кибератакой // Административное право. 2017. №1. С. 17-21. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

9. Лопашенко Н.А. Компьютерное мошенничество - новое слово в понимании хищения или ошибка законодателя? / под ред. О.А. Кузнецовой, В.Г. Голубцова, Г.Я. Борисевич, Л.В. Боровых, Ю.В. Васильевой, С.Г. Михайлова, С.Б. Полякова, А.С. Телегина, Т.В. Шершень // Пермский юридический альманах. Ежегодный научный журнал. 2019. N 1. С. 598 - 609. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

10. 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 «КонсультантПлюс».

11. Скляров С.В. Квалификация снятия денежных средств через банкомат по чужой платежной карте // Уголовное право. 2019. №4. С. 92 - 96. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

12. Степанов-Егиянц В.Г., Абазехова З.И. Борьба с онлайн-казино: правовые проблемы и перспективы // Безопасность бизнеса. 2019. №4. С. 57 - 64. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

13. 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.

14. Чернышов В.Н., Кочеткова М.Н. Уголовно-правовая охрана авторских прав в сети Интернет как элемент обеспечения безопасности информационного общества // Современное право. 2018. №7-8. С. 103 - 109. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

15. Шестак В.А. Актуальные проблемы обеспечения уголовно-правовой защиты авторских прав // Адвокатская практика. 2019. N 3. С. 44 - 49. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

Тема 5. Криминологическая характеристика киберпреступности и основные проблемы борьбы с ней

1. Денисов Н.Л. Негативные изменения киберпреступности в период пандемии и пути противодействия им // Безопасность бизнеса. 2020. №4. С. 37 - 42. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

2. Евдокимов К.Н. Самодетерминация технотронной преступности в Российской Федерации // Российский судья. 2020. №7. С. 48-53. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

3. Иванцов С. В. и др. Преступления, связанные с использованием криптовалюты: основные криминологические тенденции // Всероссийский криминологический журнал. – 2019. – Т. 13. – №. 1. – [Электронный ресурс]. – Режим доступа: http://pdfs.semanticscholar.org/6640/15b7bb8767b6e7861f6135d6ec1b14c56fe5.pdf

4. 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.

5. 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.

6. Сидоренко Э.Л. Наркотики и криптовалюта: мировые криминологические тренды // Наркоконтроль. – 2018. – №. 2. – С. 8-13. – [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/download/elibrary_35145934_10083444.pdf

7. Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. №6. URL: https://cyberleninka.ru/article/n/kriminologicheskie-riski-oborota-kriptovalyuty

Тема 6. Некоторые вопросы, связанные с расследованием киберпреступлений

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. 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

«КонсультантПлюс».

3. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. №4 (44). URL: https://cyberleninka.ru/article/n/elektronnye-nositeli-informatsii-v-ugolovnom-sudoproizvodstve

4. Григорьев А.Н., Серых А.Б., Маханек А.Б. Некоторые проблемы раскрытия и расследования преступлений, связанных с рапросранением детской порнографии в сети Интернет // Право и практика. 2017. №1. URL: https://cyberleninka.ru/article/n/nekotorye-problemy-raskrytiya-i-rassledovaniya-prestupleniy-svyazannyh-s-raprosraneniem-detskoy-pornografii-v-seti-internet

5. Зуев С.В., Никитин Е.В. Информационные технологии в решении уголовно-процессуальных проблем // Всероссийский криминологический журнал. 2017. №3. URL: https://cyberleninka.ru/article/n/informatsionnye-tehnologii-v-reshenii-ugolovno-protsessualnyh-problem

6. 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 «КонсультантПлюс».

7. 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 «КонсультантПлюс».

8. 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 «КонсультантПлюс».

9. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе: монография. – 4-е изд., доп. / Е.Р. Россинская. – М.: НОРМА: НИЦ ИНФРА-М, 2020. – [Электронный ресурс]. – Режим доступа: http://znanium.com/catalog/document?id=347476&pid=1058231.

10. Россинская Е.Р. 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.

11. Скобелин С.Ю. Цифровая криминалистика: объект и направления развития // Российский следователь. 2020. № 4. С. 42-44. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

12. 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 «КонсультантПлюс».

13. Уголовно-юрисдикционная деятельность в условиях цифровизации: монография / Н.А. Голованова, А.А. Гравина, О.А. Зайцев и др. М.: ИЗиСП, КОНТРАКТ, 2019. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

14. Харитонов А.Н., Никульченкова Е.В. Квалификация мошенничества в сфере компьютерной информации // Российская юстиция. 2019. N 11. С. 35 - 38. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

Тема 7. Соотношение уголовного, административного и гражданского права в вопросах охраны информации

1. Гуриков С.Р. Интернет-технологии: учеб. пособие / С.Р. Гуриков. – М.: ФОРУМ: ИНФРА-М, 2017. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=908584.

2. Девлятшина М. Защита прав на компьютерную программу // ЭЖ-Юрист. 2017. №25. С. 13.– [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

3. Защита данных: научно-практический комментарий к судебной практике / Э.В. Алимов, Д.Р. Алимова, Х.И. Гаджиев и др.; отв. ред. В.В. Лазарев, Х.И. Гаджиев. М.: ИЗиСП, КОНТРАКТ, 2020. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

4. Зараменских Е.П. Интернет вещей. Исследования и область применения: монография / Е.П. Зараменских, И.Е. Артемьев. – М.: ИНФРА-М, 2018. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=959279.

5. 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 «КонсультантПлюс».

6. 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.

7. 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 «КонсультантПлюс».

8. 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.

9. Савельев А.И. Электронная коммерция в России и за рубежом: правовое регулирование. – 2-е изд. М.: Статут, 2016 – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

10. Смирнова К.М. Проблема информационной безопасности в

контексте использования "Интернета вещей" в медицине // Медицинское право. 2019. №1. С. 31 - 37. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

11. Смоленцев Д.В. Применение информационных систем в практической деятельности органов прокуратуры // Прокурор. 2016. №3. С. 108-112. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

12. Терещенко Л.К. Государственное регулирование и дерегулирование в сфере связи // Журнал российского права. 2019. №10. С. 98-108. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

Тема 8. Международно-правовой аспект противодействия киберпреступности

1. Акопов Г. Л. Политика и Интернет: монография / Г.Л. Акопов. – М.: ИНФРА-М, 2018. – [Электронный ресурс]. – Режим доступа: http://znanium.com/bookread2.php?book=462249.

2. 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.

3. Бельский А.И., Ягодин Р.С. О перспективах и формах информационного взаимодействия органов внутренних дел России с международными правоохранительными организациями и правоохранительными органами иностранных государств // Российский следователь. 2017. №12. С. 52 - 56. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

4. 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 «КонсультантПлюс».

5. Татаринов М.К. Уголовное право и уголовная юрисдикция Европейского союза // Международное уголовное право и международная юстиция. 2019. №6. С. 13-17. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

6. Чекулаев С.С., Бирюкова Е.Н. Сравнительно-правовой анализ интеллектуального права России и стран Азиатско-Тихоокеанского региона // Электронное приложение к "Российскому юридическому журналу". 2018. N 2. С. 113 - 117. – [Электронный ресурс]. – Режим доступа: СПС «КонсультантПлюс».

7. 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 «КонсультантПлюс».

Нормативные правовые акты и иные источники права

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). Доступ из справ.-правовой системы «КонсультантПлюс».
2. «Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ (ред. от 20.03.2025). Доступ из справ.-правовой системы «КонсультантПлюс».
3. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025). Доступ из справ.-правовой системы «КонсультантПлюс».
4. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025). Доступ из справ.-правовой системы «КонсультантПлюс».
5. «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 № 230-ФЗ (ред. от 22.07.2024). Доступ из справ.-правовой системы «КонсультантПлюс».
6. Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.08.2024) «О государственной тайне». Доступ из справ.-правовой системы «КонсультантПлюс».
7. Закон РФ от 27.12.1991 № 2124-1 (ред. от 23.11.2024) «О средствах массовой информации». Доступ из справ.-правовой системы «КонсультантПлюс».
8. Федеральный закон от 17.01.1992 № 2202-1 (ред. от 30.09.2024) «О прокуратуре Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».
9. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 26.12.2024) (с изм. и доп., вступ. в силу с 01.04.2025) «О связи». Доступ из справ.-правовой системы «КонсультантПлюс».
10. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 23.11.2024) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2023). Доступ из справ.-правовой системы «КонсультантПлюс».
11. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 08.08.2024) «О коммерческой тайне». Доступ из справ.-правовой системы «КонсультантПлюс».
12. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 30.11.2024) «О защите детей от информации, причиняющей вред их здоровью и развитию». Доступ из справ.-правовой системы «КонсультантПлюс».
13. Федеральный закон от 08.01.1998 № 3-ФЗ (ред. от 25.12.2023) «О наркотических средствах и психотропных веществах» (с изм. и доп., вступ. в силу с 01.09.2023). Доступ из справ.-правовой системы «КонсультантПлюс».
14. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 15.05.2024) «О противодействии экстремистской деятельности» (с изм. и доп., вступ. в силу с 15.07.2023). Доступ из справ.-правовой системы «КонсультантПлюс».

15. Федеральный закон от 06.03.2006 № 35-ФЗ (ред. от 28.02.2025) «О противодействии терроризму». Доступ из справ.-правовой системы «КонсультантПлюс».

16. Федеральный закон от 07.08.2001 № 115-ФЗ (ред. от 28.12.2024) «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Доступ из справ.-правовой системы «КонсультантПлюс».

17. Федеральный закон от 25.12.2008 № 273-ФЗ (ред. от 08.08.2024) «О противодействии коррупции». Доступ из справ.-правовой системы «КонсультантПлюс».

18. Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 23.11.2024) «О национальной платежной системе». Доступ из справ.-правовой системы «КонсультантПлюс».

19. Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 25.10.2024) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

20. Федеральный закон от 28.12.2012 № 272-ФЗ (ред. от 08.08.2024) «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

21. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

22. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных». Доступ из справ.-правовой системы «КонсультантПлюс».

23. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

24. Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера». Доступ из справ.-правовой системы «КонсультантПлюс».

25. Указ Президента Российской Федерации от 30.11.1995 № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне». Доступ из справ.-правовой системы «КонсультантПлюс».

26. Постановление Правительства Российской Федерации от 07.10.2017 № 1225 «Об утверждении Правил принятия мотивированного решения о признании сайта в информационно-телекоммуникационной сети «Интернет» копией заблокированного сайта». Доступ из справ.-правовой системы «КонсультантПлюс».

27. Постановление Правительства Российской Федерации от 08.04.2015 № 327 «Об утверждении Правил осуществления контроля за деятельностью организаторов распространения информации в информационно-телекоммуникационной сети «Интернет», связанной с хранением информации

о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях». Доступ из справ.-правовой системы «КонсультантПлюс».

28. Постановление Правительства Российской Федерации от 22.11.2023 № 1952 «Об утверждении Правил взаимодействия провайдеров хостинга с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

29. Постановление Правительства Российской Федерации от 23.09.2020 № 1526 «О Правилах хранения организаторами распространения информации в информационно-телекоммуникационной сети «Интернет» информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» и информации об этих пользователях и предоставления ее уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

30. Постановление Правительства Российской Федерации от 23.11.2017 № 1418 «Об утверждении Правил взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с федеральными органами исполнительной власти, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в целях получения информации об информационно-телекоммуникационных сетях, информационных ресурсах, посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

31. Постановление Правительства Российской Федерации от 30.06.2021 № 1063 «Об утверждении Положения о федеральном государственном контроле (надзоре) за соблюдением требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе в информационно-телекоммуникационной сети «Интернет». Доступ из справ.-правовой системы «КонсультантПлюс».

32. Постановление Правительства Российской Федерации от 31.07.2014 № 743 «Об утверждении Правил взаимодействия организаторов распространения информации в информационнотелекоммуникационной сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение

безопасности Российской Федерации». Доступ из справ.-правовой системы «КонсультантПлюс».

33. Постановление Правительства Российской Федерации от 31.07.2014 № 745 «О порядке взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с организатором распространения информации в информационно-телекоммуникационной сети «Интернет». Доступ из справ.-правовой системы «КонсультантПлюс».

34. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 02.02.2023 № 13 «Об утверждении порядка проведения мониторинга информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также определении видов информации и (или) информационных ресурсов, в отношении которых проводится мониторинг». Доступ из справ.-правовой системы «КонсультантПлюс».

35. Приказ Генерального прокурора Российской Федерации от 14.09.2017 № 627 (ред. от 27.05.2024) «Об утверждении Концепции цифровой трансформации органов и организаций прокуратуры до 2025 года» (вместе с «Концепцией цифровой трансформации органов и организаций прокуратуры Российской Федерации до 2025 года»). Доступ из справ.-правовой системы «КонсультантПлюс».

36. Приказ Генерального прокурора Российской Федерации от 16.03.2016 № 159 «О порядке реализации прокурорами полномочий по направлению в суд заявлений о признании информационных материалов экстремистскими». Доступ из справ.-правовой системы «КонсультантПлюс».

37. Приказ Генерального прокурора Российской Федерации от 24.09.2021 № 557 «Об утверждении Инструкции о порядке подготовки и принятия решения о признании владельца информационного ресурса в информационно-телекоммуникационной сети «Интернет» причастным к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации, гарантирующих в том числе свободу массовой информации». Доступ из справ.-правовой системы «КонсультантПлюс».

38. Приказ Генерального прокурора Российской Федерации 26.08.2019 № 596 (ред. от 24.03.2023) «Об утверждении Инструкции о порядке рассмотрения уведомлений и заявлений о распространяемой с нарушением закона информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет». Доступ из справ.-правовой системы «КонсультантПлюс».

39. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационнокоммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям от 24.12.2024 // URL: https://www.un.org/ru/documents/treaty/A-RES-79-243.

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Официальный сайт Верховного Суда Российской Федерации. URL: http://www.vsrf.ru
2. Официальный сайт Конституционного Суда Российской Федерации. URL: http://www.ksrf.ru
3. Официальный сайт Московского городского суда. URL: http://www.mos-gorsud.ru
4. ГАС РФ «Правосудие».URL: http://www.sudrf.ru

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине

1. Справочная правовая система «Консультант Плюс».
2. Справочная правовая система «Гарант».
3. Электронно-библиотечная система Znanium.com.
4. Электронно-библиотечная система «Проспект».

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Для проведения лекционных и практических занятий по учебной дисциплине «Противодействие киберпреступности» требуется аудитория, оборудованная учебной мебелью и оснащенная мультимедийным комплексом с возможностью подключения к информационно-телекоммуникационной сети «Интернет», презентационной техникой, компьютерной техникой, видео- и аудиовизуальными средствами обучения.

Лист согласования
рабочей программы учебной дисциплины
«Противодействие киберпреступности»

Автор-составитель:
заведующий кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук — Л.Б. Сыромля

Рецензент:
И.о. заведующего кафедрой уголовно-правовых дисциплин Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, кандидат юридических наук — В.Б. Хазизулин

И.о. декана юридического факультета Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации — А.В. Васильева

Начальник учебного отдела Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации — Е.М. Дроздова