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 – 2025

Очная форма обучения

Владивосток, 2025

Рабочая программа учебной дисциплины «Прокурорский надзор за исполнением законов и соответствием законам правовых актов» обсуждена и одобрена на совместном заседании кафедр Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации от 16.05.2025, протокол № 13.

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:

Винокуров Максим Владимирович	Доцент кафедры уголовно-правовых дисциплин Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации
Гаврилов Максим Александрович	Профессор кафедры основ организации и управления в органах прокуратуры Казанского юридического института (филиала) Университета прокуратуры Российской Федерации, к.ю.н.
Гундерич Галина Альбертовна	Доцент кафедры уголовно-правовых дисциплин Крымского юридического института (филиала) Университета прокуратуры Российской Федерации, к.т.н., доцент
Кондратюк Сергей Викторович	И.о. заведующего кафедрой уголовно-правовых дисциплин Луганского юридического института (филиала) Университета прокуратуры Российской Федерации, к.ю.н., доцент
Побегайло Анастасия Эдуардовна	Доцент кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации, к.ю.н.
Попов Александр Николаевич	заведующий кафедрой уголовного права, криминологии и уголовно-исполнительного права Санкт-Петербургского юридического института (филиала) Университета прокуратуры Российской Федерации, д.ю.н., профессор
Сыромля Лариса Борисовна	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, к.ю.н.

Рецензенты:

Малов А.А., начальник управления правовой статистики, информационных технологий и защиты информации прокуратуры Республики Бурятия.

Хазизулин В.Б., заведующий кафедрой уголовно-правовых дисциплин Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, к.ю.н.

Противодействие киберпреступности: рабочая программа учебной дисциплины. – Владивосток: ДЮИ (ф) УП РФ, 2025. – 48 с.

Рабочая программа разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования – специалитет по специальности 40.05.04 Судебная и прокурорская деятельность, утвержденного приказом Минобрнауки России 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 противодействия киберпреступности; закрепление имеющихся и формирование новых умений и навыков, необходимых для противодействия киберпреступности; 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-2.3.** Применяет правовые нормы при осуществлении уголовного преследования	*Знать:* понятия, виды и состав киберпреступлений; уголовно-правовые нормы, устанавливающих ответственность за киберпреступления; соотношения отраслей права в вопросах охраны информации; *Уметь:* применять на практике нормативные правовые акты материального и процессуального права, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, надзора за

			их расследованием и раскрытием; *Владеть навыками:* по проверке нормативных правовых актов, правовой документации и иных сведений, касающихся сферы информационно-телекоммуникационных технологий, 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	*Знать:* материальное и процессуальное законодательство Российской Федерации в части охраны общественных отношений, связанных с информационно-телекоммуникационными технологиями, цифровой информацией, критической информационной инфраструктурой Российской Федерации; *Уметь:* поддерживать государственное обвинение в рамках судебного разбирательства по делам о киберпреступлениях, *Владеть навыками:* осуществления правильной уголовно-правовой квалификации киберпреступлений.
правоприменительный	**ПК-3.** Способен выполнять должностные обязанности по обеспечению законности, защите прав и законных	**ПК-3.5.** Осуществляет профилактику, предупреждение, пресечение преступлений и правонарушений, выявляет и	*Знать:* законодательство РФ в части регулирования общественных отношений в рамках информационно-телекоммуникационных технологий, цифровой

	интересов граждан, организаций, охраняемых законом интересов общества и государства	устраняет причины и условия, способствующие их совершению	информации, критической информационной инфраструктуры Российской Федерации; *Уметь:* юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности; осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с информационно-телекоммуникационным и технологиями и цифровой информацией, критической информационной инфраструктурой Российской Федерации; находить нужную правовую информацию по вопросам противодействия киберпреступности и правильно ее использовать, составлять юридически значимые документы (протест, представление, постановление, предостережение) в рамках надзора за исполнением законодательства в сфере информационно-телекоммуникационных технологий; *Владеть навыками:* проверки нормативных правовых актов, правовой документации и иных сведений, касающихся сферы информационно-телекоммуникационных технологий, цифровой

			информации, критической информационной инфраструктуры Российской Федерации; уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений

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. Криминология.

Дисциплина «Противодействие киберпреступности» изучается параллельно с дисциплинами:

1. Криминалистика.
2. Квалификация преступлений.

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

4. Объем и структура учебной дисциплины

Объем и виды учебной работы обучающегося по дисциплине в целом по форме обучения

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)					Примечание
		Контактная работа	в том числе:		Самостоятельная работа	Зачет	
			Лекции	Практические занятия			
1	2	3	4	5	6	7	8
Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика	14	6	2	4	8		Проблемная лекция. Решение задач.
Тема 2. Преступления в сфере компьютерной информации	18	10	4	6	8		Проблемная лекция. Решение задач.
Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий	14	8	2	6	6		Проблемная лекция. Решение задач.
Тема 4. Проблемы квалификации киберпреступлений	14	6	2	4	8		Проблемная лекция. Решение задач.
Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе	12	6	2	4	6		Проблемная лекция. Решение задач.
Промежуточная аттестация							зачет
Итого часов	**72**	**36**	**12***	**24***	**36**		
В том числе часов на занятия в активных, интерактивных формах			12	24			

5. Содержание учебной дисциплины

Содержание разделов дисциплины, структурированное по темам (программа курса)

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

Предмет учебной дисциплины «Проблемы противодействия киберпреступности». Метод учебной дисциплины «Проблемы противодействия киберпреступности», ее система и задачи. Понятие киберпреступности. Понятие киберпреступлений и их виды. Цифровая информация как объект преступного посягательство. Киберсредства совершения преступлений.

Основные определения термина «киберпреступность» в правовой науке современной России. Основные определения понятия «киберпреступность» в правовой науке иностранных государств. Киберпреступления и компьютерные преступления – вопросы соотношения терминов. Роль прокуратуры в обеспечении кибербезопасности.

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. Международный характер явления: причины и дальнейшее развитие. Истоки современных видов киберпреступлений.

Криминологическая характеристика киберпреступности: понятие, уровень, структура, динамика. Личность киберпреступника, вопросы типологии. Причины и условия киберпреступности. Вопросы общесоциального и специально-криминологического предупреждения киберпреступности. Прокуратура в системе профилактики киберпреступности.

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. NFT и иная цифровая собственность как инструмент легализации преступных доходов. Незаконное использование нейронных сетей как криминологическая проблема.

Тема 2. Преступления в сфере компьютерной информации

Неправомерный доступ к компьютерной информации. Неправомерный доступ к компьютерной информации, осуществляемый с помощью вредоносных программ и иной компьютерной информации – вопросы квалификации. 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.

Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения.

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. Объективные признаки данного состава. Субъективные признаки состава неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Квалифицирующие признаки неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и

целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования. Понятие и виды технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, их нормативно-правовое определение. Вопросы административного регулирования указанных вопросов. Административная преюдиция как условие действия данного состава преступления. Объективные признаки данного состава. Субъективные признаки данного состава. Квалифицирующие признаки нарушения правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"», вопросы квалификации преступлений, предусмотренных главой 28 УК РФ, разъясняемые в нем.

Некоторые актуальные проблемы прокурорского надзора за следствием по делам, предусмотренным главой 28 УК РФ. Отдельные вопросы поддержания обвинения по уголовным делам о преступлениях в сфере компьютерной информации.

Тема 3. Киберпреступления, совершаемые посредством информационно-телекоммуникационных технологий

Преступления против жизни и здоровья, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против половой свободы и половой неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации. Развратные действия, совершаемые путем использования ресурсов сети Интернет.

Преступления против конституционных прав и свобод человека и гражданина, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против общественной безопасности и общественного порядка, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против основ конституционного строя и безопасности государства, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против государственной власти, интересов государственной службы, и службы местного самоуправления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против порядка управления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Преступления против мира и безопасности человечества, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Отдельные проблемные аспекты поддержания государственного обвинения по делам о киберпреступлениях, совершаемых посредством информационно-телекоммуникационных технологий.

Тема 4. Проблемы квалификации киберпреступлений

Особенности квалификации неправомерного доступа к компьютерной информации. Вопросы соотношения неправомерного доступа к компьютерной информации и нарушения тайны переписки, телефонных переговоров, телеграфных и иных сообщений. Особенности квалификации подделки, изготовления или оборота поддельных цифровых документов, соотношение со внесением несанкционированных изменений в государственные базы данных. Нарушение неприкосновенности частной жизни, совершаемой путем неправомерного доступа к компьютерной информации: вопросы квалификации.

Особенности квалификации создания, распространения и использования вредоносных компьютерных программ. Признак вредоносности программы. Признак заведомости. Отдельные проблемные аспекты определения момента окончания создания вредоносной компьютерной программы. Проблемы определения малозначительности создания, распространения и использования вредоносных компьютерных программ.

Особенности квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Конкуренция неправомерного доступа к компьютерной информации и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. Критическая информационная инфраструктура Российской Федерации как предмет преступления – отдельные проблемные аспекты определения.

Вопросы отграничения совокупности преступлений в сфере компьютерной информации от единого продолжаемого преступления.

Тема 5. 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.

Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.

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.

Установление и разграничение юрисдикции при расследовании киберпреступлений, при затрагивании законных интересов граждан двух и более государств.

Основные подходы стран БРИКС по противодействию киберпреступности.

Роль стран ШОС в противодействии кибертерроризму.

Меры по противодействию киберпреступности стран-участниц ЕАЭС.

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

Важным видом работы при изучении дисциплины «Противодействие киберпреступности» является самостоятельная (внеаудиторная) работа обучающегося.

Самостоятельная (внеаудиторная) работа обучающегося, может осуществляться в следующих формах:

1. Подготовка к практическим занятиям.
2. Подготовка и написание контрольных работ.
3. Подготовка докладов.
4. Решение практических задач и ситуаций.
5. Иные формы по выбору преподавателя.

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 «Проблемы противодействия 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.

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

Практическое занятие 1.

1. Дайте определение понятия и предмета дисциплины «Проблемы противодействия киберпреступности».
2. Основные методы изучения киберпреступности
3. Укажите систему и задачи дисциплины «Проблемы противодействия киберпреступности».
4. История развития информационно-телекоммуникационных технологий.
5. Основные этапы развития компьютерной техники.
6. Назовите основные этапы развития языков программирования и машинного обучения.
7. История развития информационно-телекоммуникационных сетей, включая сеть Интернет
8. Основные этапы разработки вредоносных компьютерных программ.
9. Назовите основные этапы зарождения и развития киберпреступности в исторической перспективе.

Практическое занятие 2.

1. Понятие киберпреступности.
2. Отражение понятия киберпреступность в российской и иностранной правовых науках.
3. Современное состояние киберпреступности в РФ и основные тенденции ее дальнейшего развития как массового, социально-негативного, уголовно-правового явления.
4. Основные условия и причины возникновения киберпреступлений.
5. Современные структура, динамика и общее состояние киберпреступности.
6. Прогноз развития киберпреступности
7. Международный характер киберпреступности
8. Основные проблемы в противодействии противодействия киберпреступности
9. Влияние сетевой псевдоанонимности и сетевой культура на киберпреступность

Тема 2. Преступления в сфере компьютерной информации

Практическое занятие 1.

1. Проблемы квалификации неправомерного доступа к компьютерной информации

2. Основные приемы и способы неправомерного доступа к компьютерной информации

3. Основные средства и способы создания, использования и распространения вредоносных компьютерных программ

4. 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.

Практическое занятие 2.

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

2. Основные вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

3. Назовите основные проблемы квалификации нарушения правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети Интернет и сети связи общего пользования

4. Особенности информации как предмета преступления. Назовите основные аспекты использования киберсредств как средства и способа совершения преступления.

Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий

Практическое занятие 1.

1. Назовите преступления против жизни и здоровья, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

3. Назовите преступления против половой свободы и половой неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

4. Перечислите преступления против конституционных прав и свобод человека и гражданина, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

5. Преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Практическое занятие 2.

1. Назовите преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

3. Назовите преступления против общественной безопасности и общественного порядка, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

4. Преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

5. Перечислите преступления против основ конституционного строя и безопасности государства, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Практическое занятие 3.

1. Назовите преступления против государственной власти, интересов государственной службы, и службы местного самоуправления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

2. Преступления против порядка управления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации

3. Назовите преступления против мира и безопасности человечества, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

Тема 4. Проблемы квалификации киберпреступлений

Практическое занятие 1.

1. Особенности квалификации неправомерного доступа к компьютерной информации

2. Конкуренция неправомерного доступа к компьютерной информации и нарушения тайны переписки, телефонных переговоров, телеграфных и

иных сообщений

3. Основные вопросы квалификации нарушения неприкосновенности частной жизни, совершаемой путем неправомерного доступа к компьютерной информации

4. Основные особенности квалификации создания, распространения и использования вредоносных компьютерных программ?

Практическое занятие 2.

1. Конкуренция составов неправомерного доступа к компьютерной информации и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

2. Проблемные аспекты нормативного определения критической информационной инфраструктуры Российской Федерации как предмета преступления

3. Основные проблемные аспекты определения момента начала и момента окончания киберпреступлений

4. Основные вопросы совокупности преступлений в сфере компьютерной информации от единого продолжаемого преступления?

Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе

Практическое занятие 1.

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

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

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

4. Правила по разграничению юрисдикции при расследовании киберпреступлений и нормативные правовые акты, их содержащие.

5. Конвенция Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.

Практическое занятие 2.

1. Основные подходы стран БРИКС по противодействию киберпреступности

2. Роль стран ШОС в противодействии кибертерроризму

3. Меры по противодействию киберпреступности предпринимаются странами-участницами ЕАЭС

Методические рекомендации по написанию аудиторных и домашних 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:

Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993 г. [с изменениями, одобренными в ходе общероссийского голосования 01.07.2020] // СПС «КонсультантПлюс».

Федеральный закон от 17.01.1992 № 2202–1 «О прокуратуре Российской Федерации» // СПС «КонсультантПлюс».

Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации // СПС «КонсультантПлюс».

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: «Нечевин Д.К. Противодействие экстремизму в глобальной компьютерной сети Интернет: история и современность / Д.К. Нечевин, В.В. Баранов // Административное право и процесс. – 2022. – № 2. – С. 26–33». 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.

Варианты аудиторных и домашних 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. В чем заключаются основные актуальные вопросы противодействию угрозам убийством в сети Интернет?

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. В чем состоят актуальные проблемы квалификации преступлений, совершенных с использованием Даркнет-ресурсов?

Вариант 9

1. Каковы существуют наиболее распространенные ошибки, допускаемые при расследовании и раскрытии преступлений, связанных с неправомерным доступом к компьютерной информации?

2. Назовите основные способы совершения мошенничества в сфере электронных средств платежа и проблемы его отграничения от смежных составов.

Вариант 10

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

2. Каковы основные проблемные вопросы квалификации преступлений, совершаемых с использованием криптовалют?

Вариант 11

1. Какие существуют проблемы квалификации склонения к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети?

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

Вариант 12

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

2. Каковы проблемные аспекты квалификации развратных действий, совершаемых путем использования ресурсов сети Интернет?

Вариант 13

1. Охарактеризуйте основные проблемные аспекты квалификации нарушения неприкосновенности частной жизни, совершенного путем использования информационно-телекоммуникационных технологий.

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 вы можете назвать проблемы, возникающие при квалификации вовлечения несовершеннолетних в совершение антиобщественных действий и преступлений, осуществляемое с использованием информационно-телекоммуникационных сетей и сетевых ресурсов?

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 борьбе с киберпреступностью?

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 электронных средств платежа», указав его проблемные аспекты.
2. Дайте уголовно-правовую характеристику составу вовлечения несовершеннолетнего в совершение действий, представляющих опасность для его жизни, совершенное с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

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 кражи с банковского счета, а равно в отношении электронных денежных средств – в чем заключаются проблемы квалификации, каковы основные пути совершения такого деяния?

2. В чем заключаются основные вопросы квалификации мошенничества в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств)?

Вариант 22

1. Каковы основные проблемные аспекты квалификации незаконных организации и проведения азартных игр, совершаемых с использованием сети Интернет и иных информационно-телекоммуникационных сетей?

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

Методические рекомендации по устному и письменному решению задач

Задание направлено на формирование следующих компетенций: ПК-2 (ПК - 2.3).

Для правильного решения задачи необходимо внимательно прочитать задачу для того, чтобы ни одна деталь не осталась неучтенной, так как иногда именно она содержит необходимые для верного решения данные. Кроме того, необходимо точно усвоить, что требуется от принимающего решение, на какие вопросы ему надлежит отвечать. Задача решается только на основании тех обстоятельств, которые прямо в ней сформулированы, если иное не оговорено. Эти обстоятельства нужно считать усыновленными и доказанными.

Важным этапом решения является поиск правовых норм, в соответствии с которыми оно принимается, их анализ и сопоставление. В основе этого лежит хорошее знание положений УК РФ, умение свободно в нем ориентироваться, усвоение закона и теоретического материала по всем ранее изученным темам. Решение некоторых задач требует знания решений высших судебных органов, как общего порядка, так и по конкретным делам, иных подзаконных актов.

Отвечая на поставленные в задаче вопросы, нельзя ограничиться ответами, например, «Да, верно» или «Нет, не обоснованно» и т.д. Решение должно быть мотивированным, т.е. содержать обоснование, аргументы, суждения из которых оно следует.

Решение задачи следует изложить в письменном виде в виде развернутых ответов на поставленные вопросы с обязательной ссылкой на соответствующие статьи (части, пункты) УК РФ, нормативных актов, постановлений Пленумов РФ, в которых разъясняется то или иное положение закона.

Мотивировка решения предполагает не только указание на нормы УК РФ, но и приведение аргументов из научной литературы и судебной практики. Если условие задачи дает основание для нескольких вариантов решения, то необходимо предложить решения по каждой версии.

Решение задачи, даже содержащее правильную ссылку на соответствующие нормы УК РФ, но должным образом не аргументированное, не засчитывается. Напротив, решение, хотя и спорное, но свидетельствующее о стремлении студента должным образом его обосновать, может быть зачтено.

Пример задачи и ее решения

Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за крайне поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема - одного из элементов компьютерной системы.

Подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

В качестве образца предлагается решение задачи:

В деянии Шатурина можно усмотреть признаки состава преступления, предусмотренные ст. 274 УК РФ «нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей». законодательная база для решения задачи – ст. 274 УК РФ, примечания к ст. 272 УК РФ.

Родовым объектом данного преступления являются общественная безопасность и общественный порядок; видовым – отношения в сфере компьютерной безопасности. Непосредственный объект – это отношения, обеспечивающие правила эксплуатации хранения, обработки, передачи компьютерной информации и информационно-телекоммуникационных сетей.

Объективная сторона преступления сконструирована в качестве материального состава. Обязательные условия наступления уголовной ответственности – причинение крупного ущерба. В деянии Шатурина усматриваются отдельные признаки объективной стороны деяния, в частности, нарушения правил эксплуатации информационно-телекоммуникационных сетей. Он также обладает признаками субъекта данного преступления – вменяем и достиг 16 лет. Субъективная сторона

преступления характеризуется виной как в форме умысла, так и неосторожности.

Однако, вопрос об уголовной ответственности Шатурина зависит от того, в каком размере был причинен ущерб его деянием, так как состав преступления является материальным. Согласно примечанию к ст. 22 УК РФ крупным ущербом в статьях данной главы признается ущерб сумма которого превышает один миллион рублей. Таким образом, Шатурин будет подлежать уголовной ответственности по ч. 1 ст. 274 УК РФ, если его деянием причинен ущерб на сумму свыше одного миллиона рублей.

Критерии оценки:

Для оценивания выполнения заданий практической письменной работы используются следующие критерии:

правильность по содержанию,

последовательность;

самостоятельность суждений и выводов;

степень развития логического мышления;

культура речи учащихся.

Каждый критерий оценивается в 1 балл, общая оценка складывается из суммы полученных баллов; максимальный балл за ответ – 5. Отказ от выполнения задания или отсутствие выполненного задания может быть оценено выставлением в журнал оценки «неудовлетворительно», влечет необходимость выполнения невыполненного задания и отработки соответствующей темы в форме, определяемой преподавателем.

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

Изучение учебной дисциплины «Противодействие киберпреступности» завершается промежуточной аттестацией – зачетом в устной и (или) письменной форме.

Методические рекомендации по подготовке к зачету

Билеты для сдачи зачета содержат 2 теоретических вопроса и задачу. 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. Алгоритм решения задач, образцы задач см. раздел 6.

Примерный перечень вопросов для подготовки к зачету

1. Предмет, метод, задачи 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. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения.
11. Создание, использование и распространение вредоносных компьютерных программ, их основные виды; квалифицирующие признаки данного деяния и вопросы определения момента его окончания.
12. «Вредоносная программа» как средство совершения преступления: понятие, виды, особенности квалификации.
13. «Иная компьютерная информация» как средство совершения преступления: понятие, виды, особенности квалификации.
14. Нейтрализация средств защиты компьютерной информации как специфическое деяние, способы и средства его совершения.
15. Вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
16. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие, особенности конструкции состава, вопросы квалификации.
17. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации

информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

18. Информация как предмет преступления.

19. Информационно-телекоммуникационные (кибернетические) технологии как способ и средство совершения преступления.

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

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

22. Преступления против жизни и здоровья, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

24. Преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

26. Преступления против собственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

28. Преступления против общественной безопасности и общественного порядка, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

30. Преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

31. Кража с банковского счёта или электронных денежных средств: проблемы квалификации, основные пути совершения.

32. Преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

34. Преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

35. Преступления против основ конституционного строя и безопасности государства, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

37. Преступления против мира и безопасности человечества, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

39. Преступления против государственной власти, интересов государственной службы, и службы местного самоуправления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

41. Преступления против половой свободы и половой неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

43. Преступления против конституционных прав и свобод человека и гражданина, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

45. Преступления против порядка управления, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

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

48. Нарушение неприкосновенности частной жизни, совершенное путем использования информационно-телекоммуникационных технологий.

49. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, совершенные с использованием

киберсредств.

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

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

52. Мошенничество, совершенное с использованием электронных средств платежа, осуществляемое с применением кибертехнологий.

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

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

55. Кибертерроризм – определение, предмет и способы совершения.

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

57. 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.

58. Склонение к совершению самоубийства или содействие совершению самоубийства, совершенное с помощью информационно-телекоммуникационной сети.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

74. 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.

75. Незаконные изготовление и оборот порнографических материалов или предметов, совершаемые с использованием информационно-телекоммуникационных сетей.

76. Содействие диверсионной деятельности, прохождение обучения в целях осуществления диверсионной деятельности, организация диверсионного сообщества и участие в нем, осуществляемые с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

77. Вопросы взаимодействия правоохранительных и судебных органов разных стран в рамках борьбы с киберпреступностью.

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

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

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

81. Соотношение неправомерного доступа к компьютерной информации и нарушения тайны переписки, телефонных переговоров, телеграфных и иных сообщений.

82. Подделка, изготовление или оборот поддельных цифровых документов, его соотношение со внесением несанкционированных изменений в государственные базы данных.

83. Нарушение неприкосновенности частной жизни, совершаемой путем неправомерного доступа к компьютерной информации.

84. Вопросы квалификации преступления, предусмотренного ст. 273 УК РФ: признак вредоносности программы и признак заведомости.

85. Определение момента окончания создания вредоносной компьютерной программы.

86. Проблемы определения малозначительности создания, распространения и использования вредоносных компьютерных программ.

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

88. Цифровые доказательства и их процессуальный статус.

89. Вопросы поддержания обвинения по делам о киберпреступлениях.

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

91. Конкуренция неправомерного доступа к компьютерной информации и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.

92. Критическая информационная инфраструктура Российской Федерации как предмет преступления – отдельные проблемные аспекты определения.

93. Вопросы отграничения совокупности преступлений в сфере компьютерной информации от единого продолжаемого преступления.

94. Вопросы разграничения административных и уголовных дел в сфере связи и информации, а равно совершенных с использованием информационно-телекоммуникационных технологий.

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

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

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

Критерии оценки:

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

– *знания*: законодательства РФ в части регулирования общественных

отношений в рамках информационно-телекоммуникационных технологий 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 информационно-телекоммуникационными технологиями и цифровой информацией; поддерживать государственное обвинение по делам о киберпреступлениях; осуществлять консультационную деятельность по предупреждению и борьбе с киберпреступлениями; 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 борьбы с киберпреступностью); разрабатывать нормативные правовые акты в сфере борьбы с киберпреступностью; 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 информационно-телекоммуникационных технологий, цифровой информации, уголовно-правовой квалификации преступлений в сфере компьютерной информации и иных киберпреступлений; законодательной техники и правоприменения в сфере борьбы с киберпреступностью.

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

1. Абдусаламова, Д.М. Коррупционная киберпреступность как новый вид преступления / Д.М. Абдусаламова, И.А. Бурмистров // Актуальные исследования. – 2023. – № 2–2(132). – С. 10–13. – URL: https://www.elibrary.ru/item.asp?id=50104121

2. Алексеев, С.А. Предупреждение и противодействие киберпреступности: основные теоретические положения и эмпирический опыт / С.А. Алексеев, О.Д. Калашников, Е.Л. Шапошников // Евразийский юридический журнал. – 2022. – № 1(164). – С. 392–396. – URL: https://www.elibrary.ru/item.asp?id=48157305

3. Баранова, Е. К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. – 4-е изд., перераб. и доп. – Москва: РИОР: ИНФРА-М, 2022. – 336 с. – (Высшее образование). – DOI: https://doi.org/10.29039/1761–6. – ISBN 978–5–369–01761–6. – URL: https://znanium.com/catalog/product/1861657

4. Введение в инфокоммуникационные технологии: учебное пособие / Л.Г. Гагарина, Г.А. Кузнецов, Е.М. Портнов, А.А. Доронина; под ред. д-ра техн. наук, проф. Л.Г. Гагариной. – 2-е изд., испр. – Москва: ИНФРА-М, 2023. – 339 с. – (Высшее образование: Бакалавриат). – DOI 10.12737/1189946. – ISBN 978–5–16–016577–6. – URL: https://znanium.com/catalog/product/1893911

5. Геккель, Д.О. Историко-правовые аспекты компьютерных преступлений / Д.О. Геккель //. – 2023. – № 1(70). – С. 64–65. – EDN FQWPYM. – URL: https://www.elibrary.ru/item.asp?id=50104121

6. Гуриков, С. Р. Интернет-технологии: учебное пособие / С.Р. Гуриков. – 2-е изд., перераб. и доп. – Москва: ИНФРА-М, 2023. – 174 с. – (Высшее образование: Бакалавриат). – DOI 10.12737/1044018. – ISBN 978–5–16–016517–2. – URL: https://znanium.com/catalog/product/1902731

7. Денисов Н.Л. Негативные изменения киберпреступности в период пандемии и пути противодействия им // Безопасность бизнеса. 2020. № 4. С. 37–42. // СПС «КонсультантПлюс».

8. Евдокимов К.Н. Самодетерминация технотронной преступности в Российской Федерации // Российский судья. 2020. № 7. С. 48–53. // СПС «КонсультантПлюс».

9. Кобец, П.Н. Киберпреступность: современные виды, причины, ее порождающие, и особенности предупреждения / П.Н. Кобец // Вестник Самарского юридического института. – 2022. – № 1(47). – С. 52–58. – URL: https://www.elibrary.ru/item.asp?id=48223508

10. Комлев, Ю.Ю. От цифровизации социума к киберпреступности, кибердевиантности и развитию цифровой девиантологии / Ю.Ю. Комлев // Российский девиантологический журнал. – 2022. – № 2(1). – С. 17–26. – URL: https://www.elibrary.ru/item.asp?id=48339055

11. Санникова Л.В., Харитонова Ю.С. Цифровые активы: правовой анализ: монография. – Москва: 4 Принт, 2020. // СПС «КонсультантПлюс».
Серебренникова, А.В. Противодействие киберпреступности: актуальные вопросы / А.В. Серебренникова // Пробелы в российском законодательстве. – 2023. – Т. 16, № 1. – С. 104–112. – URL: https://www.elibrary.ru/item.asp?id=50236843

Тема 2. Преступления в сфере компьютерной информации

1. Винокуров В.Н., Федорова Е.А. Предмет неправомерного доступа к компьютерной информации (ст. 272 УК) // Законность. – 2021. – № 5. С. 50–52. // СПС «КонсультантПлюс».

2. Волженин В.В. К вопросу о квалификации, раскрытии и расследовании преступлений, предусмотренных статьей 273 УК РФ / В.В. Волженин // Вестник науки и образования. – 2019. – № 24–2(78). – С. 52–55. – URL: https://elibrary.ru/item.asp?id=41588943

3. Галушин П.В. Иная вредоносная компьютерная информация как пред-мет преступления, предусмотренного статьей 273 УК РФ / П.В. Галушин, Е.А. Лапина // Научный компонент. – 2020. – № 1(5). – С. 61–67. – URL: https://elibrary.ru/item.asp?id=42863608

4. Гладких В.И. Проблемы совершенствования уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации / В.И. Гладких, И.Н. Мосечкин // Всероссийский криминологический журнал. – 2021. – Т. 15, № 2. – С. 229–237. – URL: https://elibrary.ru/item.asp?id=46235184

5. Дремлюга Р.И. Критическая информационная инфраструктура как предмет преступного посягательства / Р.И. Дремлюга, С.С. Зотов, В.Ю. Павлинская // Азиатско-тихоокеанский регион: экономика, политика, право. – 2019. – Т. 21, № 2. – С. 130–139. – URL: https://elibrary.ru/item.asp?id=41587493

6. Нечаева Е.В. Посягательства на цифровую информацию: современное состояние проблемы / Е.В. Нечаева, Э.Ю. Латыпова, Э.М. Гильманов // Человек. Преступление и наказание – 2019. – Т. 27, № 1. – С. 80–86. – URL: https://elibrary.ru/item.asp?id=37375601

7. 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. – № 5. С. 94–104. // СПС «КонсультантПлюс».

8. Харламова, А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации / А.А. Харламова // Вестник Уральского юридического института МВД России. – 2020. – № 2(26). – С. 162–167. – URL: https://elibrary.ru/item.asp?id=43945052

Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий

1. Бегишев, И.Р. Создание, распространение, приобретение или применение вооруженных роботов / И.Р. Бегишев // Российский следователь. – 2021. – № 5. – С. 47–51. – URL: https://www.elibrary.ru/item.asp?id=45726168

2. Ермакова, А.Л. Фишинг как распространенное киберпреступление современности / А.Л. Ермакова, В.Н. Чаплыгина // Закон и право. – 2022. – № 2. – С. 149–151. – URL: https://www.elibrary.ru/item.asp?id=47992931

3. Клименко А.К. Хищения безналичных и электронных денежных средств: вопросы квалификации // Российский следователь. 2020. № 5. С. 38–42. // СПС «КонсультантПлюс».

4. 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. № 1. С. 598–609. // «КонсультантПлюс».

5. Нечевин, Д.К. Противодействие экстремизму в глобальной компьютерной сети Интернет: история и современность / Д.К. Нечевин, В.В. Баранов // Административное право и процесс. – 2022. – № 2. – С. 26–33. – URL: https://www.elibrary.ru/item.asp?id=47979492

6. 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. № 5. С. 94–104. // СПС «КонсультантПлюс».

7. Скляров С.В. Квалификация снятия денежных средств через банкомат по чужой платежной карте // Уголовное право. 2019. № 4. С. 92–96. // СПС «КонсультантПлюс».

8. Филатова, М.А. Разграничение посягательств на безналичные денежные средства по формам хищения / М.А. Филатова // Уголовное право. – 2020. – № 1. – С. 85–92.

9. Хабибулин, А.Г. Проблемы противодействия преступлениям в сфере миграции, совершаемым с использованием сети "Интернет" / А.Г. Хабибулин, В.Н. Анищенко // Юридический мир. – 2021. – № 7. – С. 46–51. – URL: https://elibrary.ru/item.asp?id=46289572

10. Харитонов А.Н., Никульченкова Е.В. Квалификация мошенничества в сфере компьютерной информации // Российская юстиция. 2019. № 11. С. 35–38. // СПС «КонсультантПлюс».

11. Хисамова, З.И. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты / З.И. Хисамова, И.Р. Бегишев // Всероссийский криминологический журнал. – 2019. – Т. 13. – № 4. – С. 564–574.

12. Шестак В.А. Актуальные проблемы обеспечения уголовно-правовой защиты авторских прав // Адвокатская практика. 2019. № 3. С. 44–49. // СПС «КонсультантПлюс».

Тема 4. Проблемы квалификации киберпреступлений

1. Баландин, В. И. О понимании официального документа по статьям 292 и 327 УК РФ для целей квалификации преступлений / В. И. Баландин // Юридический вестник Самарского университета. – 2020. – Т. 6, № 2. – С. 63–69. – DOI 10.18287/2542–047X-2020–6–2–63–69.

2. Бегишев, И. Р. Безопасность критической информационной инфраструктуры Российской Федерации / И. Р. Бегишев // Безопасность бизнеса. – 2019. – № 1. – С. 27–32. – URL: https://elibrary.ru/item.asp?id=36703181

3. Бегишев, И. Р. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты / И. Р. Бегишев, З. И. Хисамова, С. Г. Никитин // Всероссийский криминологический журнал. – 2020. – Т. 14, № 1. – С. 96–105. – DOI 10.17150/2500–4255.2020.14(1).96–105. – URL: https://elibrary.ru/item.asp?id=42634448

4. Кибальник, А. Г. Квалификация преступлений против личных прав и свобод человека в новом Постановлении Пленума Верховного Суда / А. Г. Кибальник, О. П. Амвросов // Уголовное право. – 2019. – № 3. – С. 32–36. – URL: https://elibrary.ru/item.asp?id=42669042

5. Ларичев, В. Д. Характеристика преступлений, совершаемых с использованием усиленной квалифицированной подписи / В. Д. Ларичев // Общество и право. – 2020. – № 2(72). – С. 15–20. – URL: https://elibrary.ru/item.asp?id=43032423

6. Нудель, С. Л. Вопросы квалификации неправомерного оборота средств платежей (по признаку предмета) / С. Л. Нудель, Д. А. Печегин // Уголовное право. – 2020. – № 3. – С. 27–38. – URL: https://elibrary.ru/item.asp?id=44421348

7. Пикуров, Н. И. Проблемы квалификации преступных посягательств на частную жизнь: теория и судебная практика / Н. И. Пикуров // Уголовное право. – 2019. – № 2. – С. 51–58. – URL: https://elibrary.ru/item.asp?id=38563288

8. Стельмах, В. Ю. Малозначительность деяния как частный случай отсутствия состава преступления / В. Ю. Стельмах // Вестник Московского университета МВД России. – 2021. – № 1. – С. 153–159. – DOI 10.24412/2073–0454–2021–1–153–159. – URL: https://elibrary.ru/item.asp?id=44874392

Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе

1. Акопов, Г. Л. Политика и Интернет: монография / Г.Л. Акопов. – Москва: ИНФРА-М, 2023. – 202 с. – (Научная мысль). – DOI 10.12737/4155. – ISBN 978–5–16–009930–9. – URL: https://znanium.com/catalog/product/1894766

2. Бойков В.А. Борьба с киберпреступностью на международном уровне / В.А. Бойков // Международный журнал гуманитарных и естественных наук. – 2021. – № 5–3(56). – С. 51–54. – URL: https://elibrary.ru/item.asp?id=46181042

3. Гладыч Н.В. Международно-правовые основы противодействия киберпреступности / Н.В. Гладыч // Современный ученый. – 2023. – № 1. – С. 219–224. – URL: https://elibrary.ru/item.asp?id=50214260

4. Жижина М.В., Завьялова Д.В. Возбуждение уголовного дела по факту преступления в сфере компьютерной информации: российский и зарубежный опыт // Актуальные проблемы российского права. – 2021. – № 12. – С. 156–166. // СПС «КонсультантПлюс».

5. Линь Д. Основы правового регулирования и административного контроля Интернета в Китае / Д. Линь // NB: Административное право и практика администрирования. – 2020. – № 2. – С. 1–9. – URL: https://elibrary.ru/item.asp?id=43869248

6. Меньшиков, П.В. Система противодействия угрозам информационной безопасности КНР / П.В. Меньшиков, Л.К. Михина //. – 2022. – Т. 28, № 1. – С. 124–139. – URL: https://elibrary.ru/item.asp?id=47803076

7. Пан, Д. Новые направления развития уголовного законодательства в современном Китае: обзор изменений китайского уголовного законодательства / Д. Пан // Всероссийский криминологический журнал. – 2021. – Т. 15, № 1. – С. 115–123. – DOI 10.17150/2500–4255.2021.15(1).115–123. – URL: https://elibrary.ru/item.asp?id=45694517

8. Побегайло А.Э. Транснациональная киберпреступность: учеб. пособие / А.Э. Побегайло; Ун- т прокуратуры Рос. Федерации. – Москва, 2024.

9. Чекулаев С.С., Бирюкова Е.Н. Сравнительно-правовой анализ интеллектуального права России и стран Азиатско-Тихоокеанского региона // Электронное приложение к "Российскому юридическому журналу". 2018. № 2. С. 113–117. // СПС «КонсультантПлюс».

10. Шугурова И.В. Авторско-правовой режим охраны компьютерных программ в законодательстве государств – членов ЕАЭС: вопросы гармонизации в условиях цифровых трансформаций / И.В. Шугурова, М.В. Шугуров // Вестник Саратовской государственной юридической академии. – 2021. – № 6(143). – С. 39–56. – URL: https://elibrary.ru/item.asp?id=47721512

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

Современные профессиональные базы данных

1. Верховный Суд Российской Федерации [Электронный ресурс] : [офиц. сайт]. — URL: http://www.vsrf.ru (дата обращения: 24.01.2025).
2. Генеральная прокуратура Российской Федерации [Электронный ресурс] : [офиц. сайт]. — URL: http://www.genproc.gov.ru (дата обращения: 24.01.2025).
3. Государственная система правовой информации. Официальный интернет-портал правовой информации [Электронный ресурс] : [офиц. сайт]. — URL: http://pravo.gov.ru (дата обращения: 24.01.2025).

4. Государственная автоматизированная система Российской Федерации «Правосудие» [Электронный ресурс] : [офиц. сайт]. — URL: http:// https://sudrf.ru/ (дата обращения: 24.01.2025).

5. Конституционный Суд Российской Федерации [Электронный ресурс] : [офиц. сайт]. — URL: http://www.ksrf.ru (дата обращения: 24.01.2025).

6. Министерство внутренних дел Российской Федерации [Электронный ресурс] : [офиц. сайт]. — URL: http://www.mvd.ru (дата обращения: 24.01.2025).

7. Министерство юстиции Российской Федерации [Электронный ресурс] : [офиц. сайт]. — URL: http://www.mibjust.ru (дата обращения: 24.01.2025).

8. Российская газета [Электронный ресурс] : [офиц. сайт]. — URL: http://rg.ru (дата обращения: 24.01.2025).

9. Российская государственная библиотека [Электронный ресурс] : [сайт]. — URL: https://www.rsl.ru (дата обращения: 24.01.2025).

10. Судебные и нормативные акты РФ [Электронный ресурс] : [офиц. сайт]. — URL: https://sudact.ru (дата обращения: 24.01.2025).

11. Юридическая Россия : Федеральный правовой портал: [сайт]. — URL: http://www.law.edu.ru (дата обращения: 24.01.2025).

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине

В целях обеспечения освоения обучающимися образовательных программ каждому обучающемуся предоставляется индивидуальный неограниченный доступ к электронной информационно-образовательной среде (ЭИОС), включающей в т.ч.:

Электронные библиотечные системы

1. Web ИРБИС. Основной электронный каталог (книги, статьи) Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации. — URL: http://176.215.253.153:22289/CGI/irbis64r_plus/cgiirbis_64_ft.exe?C21COM=F&I21DBN=IBIS_FULLTEXT&P21DBN=IBIS&Z21ID=&S21CNR=5 (дата обращения: 24.02.2025).
2. Znanium.com : электронная библиотечная система : сайт. — URL: http://znanium.com (дата обращения: 24.02.2025).
3. Научная электронная библиотека eLIBRARY.RU : сайт. — URL: http://elibrary.ru (дата обращения: 24.02.2025).
4. Сервер научных, учебных и методических материалов Университета прокуратуры Российской Федерации. — URL: http://213.171.58.226:22289/Fmt6qU02/ (дата обращения: 24.02.2025).

5. Юрайт : образовательная платформа : электронная библиотека : сайт. — URL: http://www.urait.ru (дата обращения: 24.02.2025).

6. Электронная библиотека. – Доступ из локальной сети Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации. – Текст: электронный.

Информационные справочные системы

1. Гарант : информационно-правовой портал : сайт. — URL: http://www.garant.ru (дата обращения: 24.02.2025).

2. Кодекс : законодательство, комментарии, консультации, судебная практика : сайт. — URL: http://www.kodeks.ru (дата обращения: 24.02.2025).

3. КонсультантПлюс : сайт. — URL: http://www.consultant.ru (дата обращения: 24.02.2025).

4. Справочно-правовая система «КонсультантПлюс». — Доступ из локальной сети Иркутского юридического института (филиала) Университета прокуратуры Российской Федерации. — URL: http://www.iagprf.org (дата обращения: 24.02.2025).

Лицензионное программное обеспечение

1. Система дистанционного образования Русский Moodle 3KL.

2. Система автоматизации библиотек ИРБИС64.

3. Операционная система Windows 10 Pro / Microsoft Windows 8 / Microsoft Windows 7 / Microsoft Windows 2008.

4. Офисный пакет приложений Microsoft office 2016.

5. Kaspersky Endpoint Security 10.

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

Для проведения лекционных занятий по учебной дисциплине «Проблемы противодействия киберпреступности» требуется аудитория, оборудованная учебной мебелью для единовременного размещения студентов в количестве 50 человек, оснащенная мультимедийным комплексом с возможностью подключения к информационно-телекоммуникационной сети «Интернет», презентационной техникой, компьютерной техникой, видео- и аудиовизуальными средствами обучения.

Для проведения практических занятий по дисциплине «Проблемы противодействия киберпреступности» требуется аудитория, оборудованная учебной мебелью с возможностью единовременного размещения группы студентов в количестве 25 человек, оснащенная мультимедийным комплексом с возможностью подключения к информационно-телекоммуникационной сети «Интернет», презентационной техникой, компьютерной техникой, видео- и аудиовизуальными средствами обучения.