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

Дальневосточный юридический институт (филиал)

Кафедра уголовно-правовых дисциплин

УТВЕРЖДАЮ

Директор

И.В. Малофеев

15.06.2023

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 – 2023

Владивосток, 2023

Рабочая программа учебной дисциплины «Противодействие киберпреступности» обсуждена и одобрена решением кафедры уголовно-правовых дисциплин Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации от 07.06.2023, протокол № 10.

Автор-составитель:

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

Рецензенты:

Тимошенко Ю.А., профессор кафедры уголовно-правовых дисциплин Университета прокуратуры Российской Федерации доктор юридических наук, доцент

Карабанова Е.Н., заведующая отделом научного обеспечения прокурорского надзора и укрепления законности в сфере уголовно-правового регулирования, исполнения уголовных наказаний и иных мер уголовно-правового характера Университета прокуратуры Российской Федерации, доктор юридических наук

Противодействие киберпреступности: рабочая программа учебной дисциплины. – Владивосток: ДЮИ (ф), 2023.– 47 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.

Рабочая программа предназначена для подготовки студентов 2023 гг. начала подготовки.

Оглавление

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, юридически правильно толковать и применять нормы законодательства различных отраслей права при осуществлении прокурорской деятельности, в том числе в их системной связи	**ПК-2.3.** Юридически правильно применяет нормы законодательства различных отраслей права при осуществлении уголовного преследования	**Знает:** понятия, виды и состав киберпреступлений; уголовно-правовые нормы, устанавливающих ответственность за киберпреступления; соотношения отраслей права в вопросах охраны информации; **Умеет:** применять на практике нормативные правовые акты материального и процессуального права, касающиеся защиты цифровой информации, в рамках осуществления прокурорской деятельности, надзора за их расследованием и раскрытием; **Владеет 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. Юридически правильно применяет нормы законодательства, регламентирующие участие прокурора в рассмотрении дел судами	**Знает:** материальное и процессуальное законодательство Российской Федерации в части охраны общественных отношений, связанных с информационно-телекоммуникационными технологиями, цифровой информацией, критической информационной инфраструктурой Российской Федерации; **Умеет:** поддерживать государственное обвинение в рамках судебного разбирательства по делам о киберпреступлениях, **Владеет навыками:** осуществления правильной уголовно-правовой квалификации киберпреступлений.
правоприменительный	**ПК-3.** Способен выполнять должностные обязанности по обеспечению законности, защите прав и законных интересов граждан, организаций, охраняемых законом интересов общества и государства	**ПК-3.5.** Осуществляет профилактику, предупреждение, пресечение преступлений и правонарушений, выявляет и устраняет причины и условия, способствующие их совершению	**Знает:** законодательство РФ в части регулирования общественных отношений в рамках информационно-телекоммуникационных технологий, цифровой информации, критической информационной инфраструктуры Российской Федерации; **Умеет:** юридически грамотно мотивировать свою позицию по вопросам противодействия киберпреступности;

			осуществлять надзор за исполнением законодательства, регулирующего общественные отношения, связанные с информационно-телекоммуникационными 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; **Владеет 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.

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

4. Объем и структура учебной дисциплины

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

Тематический план для очной формы обучения

Раздел, тема учебной дисциплины, формы контроля	Всего часов	Виды учебной деятельности студента (в часах)				
		Контактная работа	в том числе:		Самостоятельная работа	Зачет
			Лекции	Практические занятия		
1	*2*	*3*	*4*	*5*	*6*	*7*
Тема 1. Киберпреступность: понятие, история развития, виды, криминологическая характеристика	14	8	2	6*	6	
Тема 2. Преступления в сфере компьютерной информации	14	6	2	4*	8	

Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий	14	10	4	6*	6	
Тема 4. Проблемы квалификации киберпреступлений	14	6	2	4*	8	
Тема 5. Международно-правовые аспекты противодействия киберпреступности на современном этапе	12	6	2	4*	8	
Зачет						
Итого часов	72	36	12	24	36	
В том числе часов на занятия в активных, интерактивных формах	24	24		24		

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

5. Содержание учебной дисциплины

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

Предмет учебной дисциплины «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 уго-

ловного 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.

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 кри-

тическую 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.

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 «Проблемы противодействия киберпреступности» является самостоятельная (внеаудиторная) работа обучающегося, которая осуществляется в следующих формах:

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

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

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

1. Дайте определение понятия и предмета дисциплины «Проблемы противодействия киберпреступности».
2. Каковы основные методы изучения киберпреступности?
3. Укажите систему и задачи дисциплины «Проблемы противодействия киберпреступности».
4. Как развивались информационно-телекоммуникационные технологии до современного этапа?
5. Какие вы можете назвать основные этапы компьютерной техники?
6. Назовите основные этапы развития языков программирования и машинного обучения.
7. Как развивались информационно-телекоммуникационные сети, включая сеть Интернет?
8. Назовите основные этапы развития вредоносных компьютерных программ.
9. Назовите основные этапы зарождения и развития киберпреступности в исторической перспективе.
10. Каким образом возникло такое явление как киберпреступность?
11. Каков современный взгляд на киберпреступность в российской и иностранной правовых науках?
12. Каково современное состояние киберпреступности в РФ и основные тенденции ее дальнейшего развития как массового, социально-негативного, уголовно-правового явления?
13. Какие существуют основные условия возникновения киберпреступлений?
14. Каковы современные структура, динамика и общее состояние киберпреступности?
15. Каков прогноз развития киберпреступности?
16. Почему преступность имеет международный характер?

17. Какие вы можете назвать проблемы противодействия киберпреступности?

18. Как влияет сетевая псевдоанонимность и сетевая культура на киберпреступность?

Тема 2. Преступления в сфере компьютерной информации

1. Каковы проблемы квалификации неправомерного доступа к компьютерной информации?

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

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

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

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

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

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

8. 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?

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

Тема 3. Преступления, совершаемые посредством информационно-телекоммуникационных технологий

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

2. Какие существуют преступления против свободы, чести и достоинства личности, совершаемые посредством информационно-телекоммуникационных технологий, в чем заключаются 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. Какие существуют преступления против семьи и несовершеннолетних, совершаемые посредством информационно-телекоммуникационных технологий, в чем заключаются их объективные и субъективные признаки, вопросы квалификации?

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

7. Какие существуют преступления в сфере экономической деятельности, совершаемые посредством информационно-телекоммуникационных технологий, в чем заключаются их объективные и субъективные признаки, вопросы квалификации?

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

9. Какие преступления против здоровья населения и общественной нравственности, совершаемые посредством информационно-телекоммуникационных технологий вы можете назвать, в чем заключаются их объективные и субъективные признаки, вопросы квалификации?

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

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

12. Какие существуют преступления против порядка управления, совершаемые посредством информационно-телекоммуникационных технологий, в чем заключаются их объективные и субъективные признаки, вопросы квалификации?

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

Тема 4. Проблемы квалификации киберпреступлений

1. Какие вы можете назвать особенности квалификации неправомерного доступа к компьютерной информации?

2. Как необходимо решать вопрос о конкуренции неправомерного

доступа к компьютерной информации и нарушения тайны переписки, телефонных переговоров, телеграфных и иных сообщений?

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

4. В чем состоят основные особенности квалификации создания, распространения и использования вредоносных компьютерных программ?

5. Как необходимо решать вопросы конкуренции составов неправомерного доступа к компьютерной информации и неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации?

6. В чем состоят проблемные аспекты нормативного определения критической информационной инфраструктуры Российской Федерации как предмета преступления?

7. Каковы основные проблемные аспекты определения момента начала и момента окончания киберпреступлений?

8. В чем состоят основные вопросы совокупности преступлений в сфере компьютерной информации от единого продолжаемого преступления?

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

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

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

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

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

5. В чем состоят основные подходы стран БРИКС по противодействию киберпреступности?

6. Какова роль стран ШОС в противодействии кибертерроризму?

7. Какие меры по противодействию киберпреступности предпринимаются странами-участницами ЕАЭС?

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.

Варианты контрольных работ

Вариант 1

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

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

Вариант 2

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

2. Каким образом возникло такое явление как киберпреступность?

Вариант 3

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

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

Вариант 4

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

2. Какие вы можете назвать основные международно-правовые договоры, регулирующие расследование киберпреступлений?

Вариант 5

1. Какие существуют основные условия возникновения киберпреступлений?

2. Что такое кибертерроризм (определение, его предмет и способы совершения)?

Вариант 6

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

2. 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 написанию контрольных работ

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

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

Практические рекомендации. Выполнение контрольной работы предполагает несколько этапов.

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

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

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

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

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

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

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

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

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.

Примерная тематика рефератов

1. Основные подходы к определению понятия «киберпреступность» и смежных понятий в правовой науке иностранных государств.
2. Основные подходы к определению понятия «киберпреступность» и смежных понятий в правовой науке современной России.
3. Современное состояние киберпреступности в Российской Федерации и мире – основные тенденции развития.
4. Киберпреступность в исторической перспективе.
5. Причины и условия возникновения киберпреступлений.
6. Современная структура, динамика, и общее состояние киберпреступности.
7. Киберпреступность: прогноз развития.
8. Международный характер киберпреступности.
9. Неправомерный доступ к компьютерной информации – проблемы квалификации.
10. Основные проблемные аспекты квалификации создания, использования и распространения вредоносных компьютерных программ.
11. Понятие «вредоносной программы» как средства совершения преступления.
12. «Иная компьютерная информация» как средство совершения преступления.
13. Вопросы квалификации преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.
14. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: понятие, особенности конструкции состава, вопросы квалификации.
15. 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: особенности конструкции состава, вопросы квалификации.
16. 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.
17. Отдельные проблемные аспекты определения момента окончания создания вредоносной компьютерной программы.
18. Проблемы определения малозначительности создания, распространения и использования вредоносных компьютерных программ.

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

20. Информация как предмет преступления.

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

22. Основные направления борьбы с распространением детской порнографии в сети Интернет.

23. Проблемы противодействия экстремизму в сети Интернет.

24. Мошенничество, совершенное с использованием электронных средств платежа.

25. Расследование краж финансовых средств из электронных банковских сетей.

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

27. Проблемы расследования случаев мошенничества в сфере компьютерной информации.

28. Нарушение коммерческой тайны, совершенное с использованием киберсредств.

29. Нарушение личной тайны, совершенное с использованием киберсредств.

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

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

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

33. Основные технические проблемы борьбы с киберпреступностью.

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

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

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

37. Влияние на преступность и вопросы криминализации незаконного использования Даркнета и торговых площадок в нем.

38. Незаконное использование нейронных сетей как криминологическая проблема.

39. Проблемы правовой регламентации цифровой собственности, борьбы с ее использованием как инструмента легализации преступных доходов.

40. 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.

41. Доведение до самоубийства, склонение к нему и содействие его совершению, осуществляемые с использованием сети Интернет.

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

43. Понуждение к действиям сексуального характера, совершаемые путем использования информационно-телекоммуникационных сетей, в том числе сети Интернет.

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

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

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

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

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

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

50. Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для его жизни, совершенное с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

51. Кража с банковского счета, а равно в отношении электронных денежных средств: проблемы квалификации, основные пути совершения.

52. Базовый состав мошенничества, совершенный посредством информационно-телекоммуникационных технологий.

53. Мошенничество с использованием электронных средств платежа.

54. Мошенничество в сфере компьютерной информации (с использованием компьютерных программ, сетей, иных высокотехнологичных средств).

55. Незаконное предпринимательство, совершаемое с использованием сети Интернет и иных информационно-телекоммуникационных сетей.

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

57. Незаконная банковская деятельность, осуществляемая посредством использования сети Интернет и иных информационно-телекоммуникационных сетей.

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

59. Легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем, и легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в ре-

зультате совершения им преступления, совершаемые с использованием криптовалют и иных цифровых финансовых активов.

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

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

62. Финансирование терроризма, осуществляемое путем использования криптовалют и иной цифровой собственности.

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

64. Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан, публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия, публичное распространение заведомо ложной информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий, совершенные с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

65. Незаконные приобретение, передача, сбыт оружия, его основных частей, боеприпасов, взрывных устройств или взрывчатых веществ, крупнокалиберного огнестрельного оружия, его основных частей и боеприпасов к нему, осуществляемые с использованием информационно-телекоммуникационных сетей и их ресурсов.

66. Незаконные приобретение, сбыт наркотических средств, психотропных веществ или их аналогов, а также незаконные приобретение, сбыт растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества, а также прекурсоров наркотических средств или психотропных веществ и растений, содержащих прекурсоры наркотических средств или психотропных веществ, либо их частей, содержащих прекурсоры наркотических средств или психотропных веществ, совершенные с использованием информационно-телекоммуникационных сетей и иных киберсредств.

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

68. Использование компьютеров, компьютерных сетей и иных технологичных киберсредств в создании и распространении детской порнографии.

69. Жестокое обращение с животными, совершаемое с публичной демонстрацией, в том числе в средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть Интернет).

70. Содействие диверсионной деятельности, прохождение обучения в целях осуществления диверсионной деятельности, организация диверсионного сообщества и участие в нем, осуществляемые с использованием электрон-

ных или информационно-телекоммуникационных сетей (включая сеть Интернет).

71. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства, совершенные путем использования информационно-телекоммуникационных сетей, включая сеть Интернет.

72. Организация экстремистского сообщества, организация деятельности экстремистской организации, финансирование экстремистской деятельности, осуществляемые с использованием электронных или информационно-телекоммуникационных сетей (включая сеть Интернет).

73. Неоднократные пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами, осуществляемые с использованием ресурсов информационно-телекоммуникационных сетей (включая сеть Интернет).

74. Получение взятки, посредничество во взяточничестве, дача взятки, осуществленные с использованием криптовалют, цифровых финансовых активов и иной цифровой собственности.

75. Оскорбление представителя власти, совершаемое с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

76. Реабилитация нацизма, осуществляемая с использованием информационно-телекоммуникационных сетей, включая сеть Интернет.

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

78. Подразделения правоохранительных органов иностранных государств, занимающихся расследованием киберпреступлений.

79. Вопросы разграничения юрисдикции при расследовании киберпреступлений.

80. Основные подходы стран БРИКС по противодействию киберпреступности.

81. Роль стран ШОС в противодействии кибертерроризму.

82. Меры по противодействию киберпреступности стран-участниц ЕАЭС.

Методические рекомендации по подготовке реферата

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

Реферат в учебном процессе представляет собой краткое изложение в письменном виде или в форме публичного доклада содержания научного труда или трудов специалистов по избранной теме, обзор литературы определенного направления.

Структура реферата включает следующие обязательные части: титульный лист; содержание (оглавление); введение; основная часть (раскрыва-

ется сущность выбранной темы); заключение; список использованной литературы.

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

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

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

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

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

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

Следует обращать внимание на то, чтобы тезис вытекал из аргумента. Особое внимание надо уделить утверждениям автора, носящим проблематичный и гипотетический характер, а также скрытым вопросам по теме работы. Наиболее часто применяемый способ выделения главного в тексте – улавливание проблематичного характера утверждений, при этом следует давать оценку авторской позиции. В качестве рационального приема написания реферата применяют сравнительное чтение, предполагающее ознакомление с различными мнениями по одному и тому же вопросу, анализ весомости и доказательности аргументов авторов текста, что позволяет сделать вывод о наибольшей убедительности одной из позиций.

Написание реферата. Текст реферата должен раскрывать тему, обладать цельностью и связностью. Раскрытие темы предполагает, что в тексте реферата излагаются относящиеся к теме материалы и предлагаются пути

решения содержащейся в контексте проблемы. Связность текста предполагает смысловую соотносительность отдельных компонентов, а цельность – смысловую законченность текста.

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

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

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

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

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

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

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

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

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

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

Представление реферата и его защита. Подготовленный студентом реферат на бумажном и электронном носителях представляется на кафедру,

где регистрируется в журнале поступающих работ. Датой сдачи работы считается ее регистрация на кафедре.

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

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

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

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

Методические рекомендации по подготовке к зачету

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

Перечень вопросов для подготовки к зачету

1. Предмет, метод, задачи учебной дисциплины «Проблемы противодействия киберпреступности».
2. Понятие киберпреступности в узком и расширительном толковании термина.
3. Основные определения термина «киберпреступность» в правовой науке современной России; вопросы соотношения с определением термина «компьютерная преступность».
4. Основные определения понятия «киберпреступность» в правовой науке западных иностранных государств.
5. Киберпреступность в исторической перспективе (зарождение киберпреступлений, их развитие и эволюция).
6. Современное состояние киберпреступности, ее уровень, структура и динамика.
7. Прогноз дальнейшего состояния киберпреступности.

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

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

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

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

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

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

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

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

16. 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.

17. Информация как предмет преступления.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

40. Преступления против половой свободы и половой

неприкосновенности, совершаемые посредством информационно-телекоммуникационных технологий, их объективные и субъективные признаки, вопросы квалификации.

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

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

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

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

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

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

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

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

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

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

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

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

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

54. Кибертерроризм – определение, предмет и способы совершения.

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

56. 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

73. 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.

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

75. 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).

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

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

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

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

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

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

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

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

84. Определение момента окончания создания вредоносной компьютерной программы.

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

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

87. Цифровые доказательства и их процессуальный статус.

88. Вопросы поддержания обвинения по делам о киберпреступлениях.

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

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

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

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

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

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

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

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

Критерии оценки:

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

– *знания*: законодательства РФ в части регулирования общественных отношений в рамках 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.

Учебно-методическое и информационное обеспечение учебной дисциплины

Основная учебная литература

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

2. Противодействие преступлениям, совершаемым в сфере информационных технологий: учебник / под науч. ред. И.А. Калиниченко. – Москва: ИНФРА-М, 2023. – 642 с. – (Высшее образование: Специалитет). – DOI 10.12737/1891229. – ISBN 978–5–16–017838–7. – Текст: электронный. – URL: https://znanium.com/catalog/product/1891229

3. Попов, А.Н. Преступления в сфере компьютерной информации: учебное пособие. / А.Н. Попов – СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. – 68 с.

4. Русскевич, Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: учебное пособие / Е.А. Русскевич. – 2-е изд., доп. – Москва: ИНФРА-М, 2022. – 188 с. – (Высшее образование: Магистратура). – ISBN 978–5–16–014392–7. – Текст: электронный. – URL: https://znanium.com/catalog/product/1843095

Дополнительная учебная литература

1. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. – Москва: ИНФРА-М, 2023. – 201 с. 1 DOI 10.12737/1013711. – ISBN 978–5–16–014976–9. – Текст: электронный. – URL: https://znanium.com/catalog/product/1912987

2. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е. В. Глинская, Н. В. Чичварин. – Москва: ИНФРА-М, 2021. – 118 с. – (Высшее образование: Специалитет). – ISBN 978–5–16–016536–3. – Текст: электронный. – URL: https://znanium.com/catalog/product/1178153

3. Информационное право: Учебник для студентов высших учебных заведений, обучающихся по направлению подготовки "Юриспруденция", специальностям "Юриспруденция", "Правоохранительная деятельность" / В.Н. Лопатин. – 3-е издание, измененное и дополненное. – М.: Общество с ограниченной ответственностью "Проспект", 2023.

4. Овчинский, В. С. Криминология цифрового мира: учебник для магистратуры / В. С. Овчинский. – Москва: Норма: ИНФРА-М, 2023. – 352 с. – ISBN 978–5–91768–896–1. – Текст: электронный. – URL: https://znanium.com/catalog/product/1917647

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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – Текст: электронный. – 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. – Текст: электронный. – 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. – [Электронный ресурс]. – 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. – Текст: электронный. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – Текст: электронный. – URL: https://znanium.com/catalog/product/1894766

2. Бойков В.А. Борьба с киберпреступностью на международном уровне / В.А. Бойков // Международный журнал гуманитарных и естествен-

ных наук. – 2021. – № 5–3(56). – С. 51–54. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – 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. – [Электронный ресурс]. – URL: https://elibrary.ru/item.asp?id=45694517

8. 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».

9. 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. – [Электронный ресурс]. – 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) // СПС «КонсультантПлюс».

2. Уголовно-процессуальный кодекс Российской Федерации // СПС «КонсультантПлюс».

3. Уголовный кодекс Российской Федерации // СПС «КонсультантПлюс».

4. Кодекс Российской Федерации об административных правонарушениях // СПС «КонсультантПлюс».

5. Гражданский кодекс Российской Федерации (часть четвертая) // СПС «КонсультантПлюс».

6. Закон РФ от 21.07.1993 № 5485–1 «О государственной тайне» // СПС «КонсультантПлюс».

7. Закон РФ от 27.12.1991 № 2124–1 «О средствах массовой информации» // СПС «КонсультантПлюс».

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

9. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СПС «КонсультантПлюс».

10. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». // СПС «КонсультантПлюс».

11. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне». // СПС «КонсультантПлюс».

12. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СПС «КонсультантПлюс».

13. Федеральный закон от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах» // СПС «КонсультантПлюс».

14. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности». // СПС «КонсультантПлюс».

15. Федеральный закон от 06.03.2006 № 35-ФЗ (в ред. от 26.05.2021) «О противодействии терроризму». // СПС «КонсультантПлюс».

16. Федеральный закон от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». // СПС «КонсультантПлюс».

17. Федеральный закон от 25.12.2008 № 273-ФЗ «О противодействии коррупции». // СПС «КонсультантПлюс».

18. Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе». // СПС «КонсультантПлюс».

19. Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // СПС «КонсультантПлюс».

20. Федеральный закон от 28.12.2012 № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» // СПС «КонсультантПлюс».

21. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СПС «КонсультантПлюс».

22. Приказ Генпрокуратуры России от 14.09.2017 № 627 «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") //

СПС «КонсультантПлюс».

23. Приказ Генпрокуратуры России от 16.03.2016 № 159 «О порядке реализации прокурорами полномочий по направлению в суд заявлений о признании информационных материалов экстремистскими» // СПС «КонсультантПлюс».

24. Приказ Генпрокуратуры России 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» // СПС «КонсультантПлюс».

25. Приказ Генпрокуратуры России от 26.08.2019 № 596 «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"» // СПС «КонсультантПлюс».

Ресурсы информационно-телекоммуникационной сети «Интернет»

1. Официальный Интернет-портал правовой информации: URL: http://pravo.gov.ru/.

2. Официальный Интернет-сайт Верховного Суда Российской Федерации: URL: http://www.vsrf.ru/.

3. Официальный Интернет-сайт Генеральной Прокуратуры Российской Федерации: URL: http://genproc.gov.ru/.

4. Официальный Интернет-сайт Государственной Думы Федерального Собрания Российской Федерации: URL: http://www.duma.gov.ru/.

5. Официальный Интернет-сайт Конституционного Суда Российской Федерации: URL: http://www.ksrf.ru.

6. Официальный Интернет-сайт МВД России: URL: http://www.mvd.ru/.

7. Официальный Интернет-сайт Московского городского суда: URL: http://www.mos-gorsud.ru/.

8. ГАС РФ «Правосудие»: URL: http://www.sudrf.ru/.

9. Электронная библиотека по праву: URL: http://www.allpravo.ru/library/.

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине

1. Справочная правовая система «Консультант Плюс».

2. Справочная правовая система «Гарант».

3. Электронно-библиотечная система Znanium.com.

4. Электронно-библиотечная система «Проспект».

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.

Лист согласований рабочей программы учебной дисциплины
«Противодействие киберпреступности»

Заведующий кафедрой
уголовно-правовых дисциплин
кандидат юридических наук, доцент — Н.Н. Загвоздкин

Декан юридического факультета
доктор юридических наук, профессор — Е.Ю. Антонова

Начальник учебного отдела — Е.М. Дроздова