МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ДАГЕСТАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра уголовного права и криминологии

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Кафедра уголовного права и криминологии
Юридического института

Образовательная программа специалитета
40.05.02 «Правоохранительная деятельность»

Направленность (профиль) программы
Оперативно – розыскная деятельность

Форма обучения:
очная, заочная

Статус дисциплины:
Входит в часть, формируемую
участниками образовательных отношений

Махачкала – 2022

Рабочая программа дисциплины «Преступления в сфере высоких технологий» составлена в соответствии с требованиями ФГОС ВО - специалитета по специальности 40.05.02 Правоохранительная деятельность от 28.08.2020 г. № 1131

Разработчики:
доктор юридических наук, профессор Акутаев Р.М.

Рабочая программа дисциплины одобрена:
на заседании кафедры уголовного права и криминологии
от «25» 02 2022 г. протокол № 6

Зав. кафедрой _____профессор Акутаев Р.М.

на заседании Методической комиссии Юридического института
от «21» 03 2022 г. протокол № 7

Председатель комиссии _____д.ю.н., профессор Арсланбекова А.З.

Рабочая программа дисциплины согласована с с учебно-методическим управлением
«31» 03 2022 г.

Начальник УМУ _____Гасангаджиева А.Г.
(подпись)

Аннотация рабочей программы дисциплины

Дисциплина «Преступления в сфере высоких технологий» входит в часть, формируемую участниками образовательной программы специалитета по специальности 40.05.02 Правоохранительная деятельность.

Дисциплина реализуется в юридическом институте кафедрой уголовного права и криминологии.

Содержание дисциплины охватывает круг вопросов, связанных с курсом уголовного права и криминологии как юридических наук и учебных дисциплин, изучающих преступления в сфере высоких технологий и меры противодействия им.

Дисциплина нацелена на формирование следующих компетенций выпускника: *ПК-4, ПК-5*

Преподавание дисциплины предусматривает проведение следующих видов учебных занятий: *лекции, практические занятия и самостоятельная работа.*

Рабочая программа дисциплины предусматривает проведение следующих видов контроля успеваемости в форме *устных опросов пройденной темы, совместного обсуждения проблемных вопросов, проведения контрольных работ;* промежуточный контроль в форме *зачета.*

Объем дисциплины 2 зачетные единицы (модуля), в том по видам учебных занятий 72 часов по очной форме обучения:

Семестры	Учебные занятия							Форма промежуточной аттестации (зачет, дифф. зачет, экзамен)
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС	
	Всего	из них						
		Лекции	Лаборат.занятия	Практические занятия	КСР	Консультации		
7	72	12	-	12		-	48	Зачет

Заочная форма обучения:

Семестры	Учебные занятия							Форма промежуточной аттестации (зачет, дифф. зачет, экзамен)
	в том числе							
	Контактная работа обучающихся с преподавателем						СРС	
	Всего	из них						
		Лекции	Лаборат.занятия	Практические занятия	КСР	Консультации		
9	72	6	-	2		-	60	Зачет

1. Цели освоения дисциплины

Целями освоения дисциплины (модуля) «Преступления в сфере высоких технологий» являются:

- анализ понятия преступности в сфере высоких технологий и противодействия ей;
- формирование знаний и умение проводить анализ составов преступлений в сфере компьютерной информации;
- изучение возможностей использования высоких технологий для совершения иных, не компьютерных, преступлений;
- формирование у обучающихся теоретических знаний о специфике, формах и методах противодействия преступности в сфере высоких технологий;
- выработка у обучающихся практических навыков, необходимых для профессионального выполнения выпускниками служебных обязанностей в области профессиональной деятельности по противодействию преступности в сфере высоких технологий;
- подготовка обучающихся к самостоятельному, квалифицированному и компетентному решению профессиональных задач.

2. Место дисциплины в структуре ОПОП

Дисциплина «Преступления в сфере высоких технологий» входит в часть, формируемую участниками образовательной программы специалитета по специальности 40.05.02 Правоохранительная деятельность.

Программа курса «Проблемы противодействия преступности в сфере высоких технологий» входит в часть, формируемую участниками образовательных отношений подготовки специалистов . В качестве исходных знаний, умений и компетенций, необходимых для освоения данного курса, выступают знания, умения и компетенции, сформированные в процессе изучения курса «Криминология», «Уголовное право», «Уголовный процесс», «Уголовно-исполнительное право», «Криминалистика».

В свою очередь изучение рассматриваемой дисциплины (модуля) необходимо для более глубокого усвоения по квалификации (степени) «магистр» многих дисциплин уголовно-правового цикла, в частности, таких, как «Состояние преступности и ее измерительные показатели», «Проблемы латентной преступности», «Система профилактики преступлений» и др.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (перечень планируемых результатов обучения)

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции выпускника	Результаты обучения	Процедура освоения
ПК-4 Способен соблюдать в профессиональной деятельности требования законодательства в области защиты государственной тайны и информационной безопасности, обеспечить соблюдение режима секретности	ПК-4.1. Способен работать с информационными ресурсами и технологиями, находящимися в доступной сфере правового поля правоохранительных органов в области защиты государственной тайны и информационной безопасности	Знать требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности Уметь обеспечивать соблюдение режима секретности Владеть приемами соблюдения в профессиональной деятельности требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечения соблюдения режима секретности	Устный опрос, тестирование
	ПК-4.2 применять и использовать разработанные методы и средства поиска, получения, хранения необходимой информации; систематизировать, обрабатывать, получать и передавать информацию	Знает: основные методы, способы и средства, используемые для собирания и исследования следов преступлений Умеет: применять и использовать разработанные методы и средства поиска, получения, хранения необходимой информации; систематизировать, обрабатывать, получать и передавать информацию Владеет: навыками и умением обращения с существующими различными ресурсами и технологиями для извлечения необходимой информации со следов преступлений и информации имеющейся в системе МВД и других	

	ПК-4.3. Способен применения в профессиональной деятельности нормативноправовые акты в области защиты государственной тайны и информационной безопасности, обеспечения режима секретности	учреждениях, для раскрытия, расследования и предупреждения преступлений и других правонарушений **Знает:** требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, способы соблюдение и обеспечения режима секретности **Умеет:** правильно определять подлежащие применению в профессиональной деятельности нормативные акты в области защиты государственной тайны и информационной безопасности, обеспечения соблюдение режима секретности **Владеет**: навыками применения в профессиональной деятельности требований нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечения режима секретности	
ПК-5 способен противодействовать злоупотребления в профессиональной деятельности	ПК-5.1. Способен выявлять и предотвращать конфликт интересов и противодействовать коррупции в правоохранительной деятельности ПК-5.2. Способен выявлять, давать оценку коррупционному поведению и содействовать его пресечению в	**Знает:** основные виды запретов и ограничений на службе, понятие конфликта интересов на службе, направления противодействия коррупции в служебной деятельности работников правоохранительных органов **Умеет:** выявлять и противодействовать злоупотреблениям в служебной деятельности, предотвращать возникновение конфликта интересов в деятельности правоохранительных органов, применять методы противодействия коррупции. **Владеет:** способностью противодействовать злоупотреблениям в служебной деятельности, навыками и способами выявления и предотвращения конфликта интересов на службе, навыками противодействия коррупции в деятельности должностных лиц правоохранительных органов РФ Знает: специфику правового регулирования антикоррупционного законодательства и современных подходов к определению коррупции, ее причинам, признакам и видам. Умеет: осуществлять профессиональную деятельность правильно оценивая варианты проявления коррупционного поведения и злоупотребления в профессиональной деятельности. Владеет: навыками анализа различных явлений, юридических фактов, правовых норм и правовых отношений,	Устный опрос, тестирование

	соответствии с антикоррупционным законодательством ПК-5.3. готовность принимать участие в проведении юридической экспертизы проектов нормативных правовых актов, в том числе в целях выявления в них положений, способствующих созданию условий для проявления коррупции	относящихся к коррупции; анализа правоприменительной и правоохранительной практики борьбы с коррупцией. Знает: основные принципы, содержание и этапы антикоррупционного законодательства, теоретические основы работы по противодействию коррупции Умеет: применять полученные знания в практических ситуациях, в том числе вносить и обосновывать предложения по применению зарубежного опыта противодействия коррупции в российских условиях, оценивать результаты реализуемой антикоррупционной политики. Владеет: навыками работы с правовыми антикоррупционными актами, навыками анализа конкретной ситуации и принятия решения в соответствии с законом, навыками по планированию своей деятельности, выбору наиболее эффективных способов и методов противодействия коррупции.	

4. Объем, структура и содержание дисциплины

4.1 Объем дисциплины составляет 2 зачетные единицы (модуля), 72 академических часов.
4.2 Структура дисциплины

Очная форма обучения:

№ п/п	Разделы и темы дисциплины	Экзамен	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля и промежуточной аттестации
			Лекции	Практ. занятия	СРС	КСР	Всего	
	Модуль 1.Уголовное право как отрасль российского права и юридическая наука. Предмет и метод уголовного права. Задачи и функции уголовного права.							
1	Ознакомительная лекция с отраслью и наукой уголовного права, его предметом и методом, задачами и функциями.		6	6	24			Текущий контроль: заслушивание и обсуждение научных докладов по теме исследования. Промежуточная аттестация: контрольная работа и зачетная аттестация.
	Итого по модулю 1:		6	6	24		36	
	Модуль 2. Уголовный закон, его особенности. Общая и Особенная части УК РФ. Уголовно-правовая норма, диспозиции и санкции. Применение уголовного закона во времени, в пространстве и по лицам. Основные институты Общей части УК РФ.							

2	Особенности уголовного закона. Структура Уголовного кодекса РФ. Применение уголовного закона. Основные институты Общей части уголовного права		6	6	24			
	Итого по модулю 2:		6	6	24		36	
Общий объем аудиторной нагрузки за 7 семестр			**12**	**12**	**48**		**72**	

Заочная форма обучения:

№ п/п	**Разделы и темы дисциплины**	**Экзамен**	**Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)**					**Формы текущего контроля и промежуточной аттестации**
			Лекции	**Практ. занятия**	**СРС**	**КСР**	**Всего**	
	Модуль 1. Уголовное наказание: понятие, цели, система и виды. Общая характеристика основных разделов Особенной части УК РФ.							Текущий контроль: заслушивание и обсуждение научных докладов по теме исследования.
1	Понятие уголовного наказание, его цели. Система и виды наказаний. Разделы Особенной части УК РФ: общая характеристика.		2	**1**	33			
	Итого по модулю 1:		2	**1**	33		36	
	Модуль 2. Информация как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. Правовые режимы защиты государственной тайны и конфиденциальной информации.							
2	Информация как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. Правовые режимы защиты государственной тайны и конфиденциальной информации.		4	1	27	4		Текущий контроль: заслушивание и обсуждение научных докладов по теме исследования. Промежуточная аттестация: контрольная работа и зачетная аттестация.
	Итого по модулю 2:		4	1	27	4	36	
Общий объем аудиторной нагрузки			**6**	**2**	**60**	**4**	**72**	

4.3. Содержание дисциплины, структурированное по темам (разделам).

<u>Модуль 1.</u>Уголовное право как отрасль российского права и юридическая наука. Предмет и метод уголовного права. Задачи и функции уголовного права.

Тема 1. Уголовное право как отрасль российского права и юридическая наука. Предмет и метод уголовного права. Задачи и функции уголовного права.

Содержание лекционного занятия.

1. Уголовное право как отрасль российского права и юридическая наука, их предмет и различие.

2. Предмет и метод уголовного права. Уголовно-правовые отношения.
3. Задачи и функции уголовного права.

Модуль 2.Уголовный закон, его особенности. Общая и Особенная части УК РФ. Уголовно-правовая норма, диспозиции и санкции. Применение уголовного закона во времени, в пространстве и по лицам. Основные институты Общей части УК РФ.

Тема 2. Уголовный закон, его особенности. Общая и Особенная части УК РФ. Уголовно-правовая норма, диспозиции и санкции. Применение уголовного закона во времени, в пространстве и по лицам. Основные институты Общей части УК РФ.

Содержание лекционного занятия.

1. Уголовный закон, его особенности и характерные черты.
2. Соотношение Общей и Особенной частей УК РФ.
3. Уголовно-правовая норма, диспозиции и санкции.
4. Применение уголовного закона во времени, в пространстве и по лицам.
5. Основные институты Общей части УК РФ.

Содержание практического занятия по 2 модулю

1. Уголовный закон, его особенности и характерные черты.
2. Соотношение Общей и Особенной частей УК РФ.
3. Уголовно-правовая норма, диспозиции и санкции.
4. Применение уголовного закона во времени, в пространстве и по лицам.
5. Основные институты Общей части УК РФ.

5. Образовательные технологии

В соответствии с требованиями ФГОС ВО по специальности 40.04.01. «Правоохранительная деятельность» для реализации компетентностного подхода, в рамках изучения рассматриваемой дисциплины предусмотрено во всех проводимых занятиях, в том числе и при самостоятельной работе студентов, сочетать передовые методические приемы с инновационными образовательными технологиями и достижениями науки и техники. В этой связи при проведении занятий по курсу «Преступления в сфере высоких технологий» предусмотрено применение современных образовательных технологий в виде совместных обсуждений, научных диспутов по спорным вопросам обсуждаемых проблем, в частности, разных мнений относительно определения понятия «противодействие преступности в сфере высоких технологий», масштабов ее латентности, совершенствования законодательства и правоприменительной практики в этой области.

В рамках учебного курса возможна организация встреч с представителями правоохранительных и судебных органов.

6.Учебно-методическое обеспечение самостоятельной работы студентов

Основными видами самостоятельной работы студентов являются:

1. Изучение конспектов лекций и рекомендованной учебной и специализированной литературы (монографических работ, научных статей) по соответствующим темам. Кроме того, самостоятельная работа обучающегося осуществляется в следующих формах:

- подготовка научных докладов по избранной теме;
- выполнение контрольных работ;
- самостоятельная работа с тестами.

Подготовка и выполнение научных докладов (письменных рефератов) и контрольных работ осуществляется по одной из предложенных тем, либо по теме, предложенной самим студентом (по согласованию с преподавателем).

Примерные темы научных докладов

1. Понятие и сущность компьютерной информации. Классификация информации. Свойства и признаки информации.
2. Понятие и сущность преступлений в сфере высоких технологий.

3. Понятие, объекты и субъекты компьютерных преступлений.

4. Особенности квалификации преступлений в сфере компьютерной информации.

5. Теоретические основы классификации преступлений в сфере высоких технологий. Обзор отечественного и международного опыта.

6. Виды компьютерных правонарушений. Ответственность за правонарушения в информационной сфере.

7. Преступления в сфере телекоммуникаций.

8. Национальные законодательства о компьютерных правонарушениях и защите информации.

9. Особенности криминального использования компьютерной техники в экономической сфере и материальном производстве (подлог документированной информации фискальных систем; преступления в сфере безналичных расчетов; преступления в сети Интернет; применение полиграфических компьютерных технологий).

10. Неправомерный доступ к компьютерной информации.

11. Создание, использование и распространение вредоносных программ для ЭВМ.

12. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

13. Контроль над компьютерной преступностью в России.

14. Уголовно-правовой контроль над компьютерной преступностью в России.

15. Особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий.

16. Методика расследования преступлений в сфере компьютерной информации.

17. Особенности тактики расследования преступлений в сфере компьютерной информации.

18. Назначение компьютерно-технических экспертиз при расследовании преступлений в сфере высоких технологий. Опросы, выносимые на их разрешение.

19. Организационно-технические меры предупреждения компьютерных преступлений.

20. Правовые меры предупреждения компьютерных преступлений

7. Фонд оценочных средств для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Типовые контрольные задания

А) Примерные тестовые задания

1. Европейская Конвенция по борьбе с киберпреступностью принята Советом Европы:
а) 23 ноября 2001 г.;
б) 22 ноября 2010 г.;
в) 13 июля 2015 г.

2. Информация по ряду преступлений в сфере высоких технологий выступает в качестве:
а) предмета преступления;
б) состояния «плазменной среды»;
в) объекта преступления.

3. Первый законодательный акт, направленный на правовую охрану программ для ЭВМ и баз данных, в России был принят:
а) 17 октября 1998 г.;
б) 23 сентября 1992 г.;
в) 22 июня 2001 г.

4. Причины преступности, как правило, классифицируются на:
а) частные и личностные;
б) судебно-медицинские и судебно-психиатрические;
в) экономические, социальные, политические и нравственно-психологические.

5. Международные преступления – это:
а) международные преступные деяния, совершаемые транснациональными преступными формированиями;
б) международные преступные деяния, посягающие на интересы отдельных политических и экономических организаций (ООН, БРИГС и т.д.);
в) преступные деяния, затрагивающие интересы всего мирового сообщества и подлежащие юрисдикции Международного уголовного суда.

6. Преступления международного характера – это:

а) преступные деяния, касающиеся ряда отдельных государств и в рамках принципа двойной подсудности подпадающие под регулятивное действие института выдачи (экстрадиции);
б) преступление, совершенное иностранным лицом или лицом без гражданства;
в) международное преступление, совершенное гражданином Российской Федерации.

7. Периодом зарождения компьютерной преступности в мире можно считать:
а) 30-е годы прошлого века;
б) 50- е годы прошлого века;
в) 70-е годы прошлого века.

8. Киберпреступность - это:
а) преступление, совершенное с помощью компьютерной системы (сети);
б) преступление, совершенное в рамках компьютерной системы (сети);
в) любое преступление, которое может быть совершено в электронной среде.

9. *Объектом компьютерных преступлений являются:*
а) информационная безопасность и системы обработки информации с использованием ЭВМ;
б) информация и компьютерные сети;
в) информационные каналы связи между ЭВМ.

10. *Предупреждение компьютерной преступности направлено на:*
а) устранение фактора, способствовавшее совершению конкретного компьютерного преступления;
б) устранение или нейтрализацию причин и условий, способствующих совершению компьютерных преступлений;
в) создание условий для ликвидации компьютерной преступности.

11. *Субъекты компьютерных преступлений могут быть квалифицированы как:*
а) хакеры, шпионы, вандалы, террористы, корыстные преступники;
б) хакеры, хулиганы, разбойники;
в) хакеры, домушники, технари, лица, испытывающие компьютерные фобии.

12. *Динамика компьютерных преступлений:*
а) относительно стабильна;
б) характеризуется ростом;
в) имеет тенденцию к снижению.

13. *К компьютерным преступлениям, в частности, относятся:*
а) нарушение авторских и смежных прав, изобретательских и патентных прав;
б) самовольные установка или эксплуатация узла проводного вещания;
в) неправомерный доступ к компьютерной информации.

14. *К административному проступку относится:*
а) незаконная деятельность в области защиты информации;
б) создание, использование и распространение вредоносных программ для ЭВМ;
в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

15. *Латентную преступность в сфере высоких технологий можно представить в виде:*
а) не полно раскрытых и полно раскрытых преступлений;
б) ложной и истинной латентности;
в) естественной и искусственной латентности преступлений.

16. *Как классифицируются компьютерные преступления по законодательству Российской Федерации:*
а) преступления в сфере оборота компьютерной информации и телекоммуникаций;
б) преступления в сфере оборота компьютерной информации, в сфере телекоммуникаций; в сфере информационного оборудования; в сфере защиты охраняемой законом информации;
в) преступления в сфере оборота компьютерной информации и в сфере защиты охраняемой законом информации.

17. *Меры контроля над компьютерной преступностью классифицируются:*
а) правовые и научно-технические;
б) правовые, научно-технические и организационные;
в) правовые, организационно-тактические и программно-технические.

18. *Основной целью государственной политики по выявлению и пресечению компьютерных преступлений является:*
а) создание эффективной национальной системы борьбы с правонарушениями в сфере компьютерной информации;
б) создание эффективной национальной системы профилактики и предупреждения компьютерных преступлений;
в) создание эффективной национальной системыконтроля за компьютерными преступлениями.

19. *Снижение уровня латентности компьютерных преступлений предполагает:*
а) расширение штатов сотрудников правоохранительных органов, ведущих борьбу с компьютерными преступлениями;
б) повышение финансирования соответствующих управлений (отделов) правоохранительных органов;
в) обеспечение неотвратимости ответственности лиц, совершивших компьютерные преступления.

20. *Правовые методы борьбы с компьютерными преступлениями включает:*
а) совершенствование уголовного законодательства в этой части;
б) совершенствование административного и уголовного законодательства об ответственности за компьютерные правонарушения;
в) совершенствование международного сотрудничества по борьбе с компьютерными преступлениями.

Б) Контрольные вопросы для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины

1. Как определяются понятия «информационные технологии» и «высокие технологии»?
2. Охарактеризуйте основные подходы к определению понятия «информация».
3. Что такое «компьютерная информация»?
4. По каким признакам классифицируется информация?
5. Каковы основные свойства и признаки информации?
6. Каковы основные аспекты уязвимости информации?
7. Назовите основные виды угроз информационной безопасности.
8. Какие цели должны преследовать подсистемы защиты информации?
9. Перечислите способы предотвращения угроз информационной безопасности.
10. Что такое компьютерное преступление?
11. Каковы субъекты компьютерных преступлений?
12. Каковы особенности квалификации преступлений в сфере компьютерной информации?
13. Какие нормативно-правовые акты предусматривают ответственность за совершение преступлений сфере высоких технологий?
14. Как классифицируются компьютерные преступления в соответствии с законодательством России?
15. Назовите и охарактеризуйте наиболее распространенные виды преступлений в сфере телекоммуникаций?
16. Каковы особенности криминального использования компьютерной техники в экономической сфере и материальном производстве?
17. Приведите примеры противоправных действий в отношении документированной информации фискальных систем.
18. Приведите примеры противоправных действий в сфере безналичных расчетов.
19. Какие виды противоправных действий совершаются в сети Интернет?
20. Какие виды противоправных действий совершаются с применением полиграфических компьютерных технологий?
21. Охарактеризуйте преступные деяния, предусмотренные главой 28 УК РФ «Преступления в сфере компьютерной информации».
22. Какие меры контроля над компьютерной преступностью используются в России?
23. Какие меры уголовно-правового контроля над компьютерной преступностью предусмотрены в законодательстве России?
24. Каковы базовые направления повышения эффективности контроля над компьютерной преступностью в Росси?
25. Каковы особенности оперативно-розыскной деятельности при расследовании преступлений в сфере высоких технологий?
26. В какой последовательности целесообразно решать основные следственные задачи в ходе расследования преступления, связанного с неправомерным (несанкционированным) доступом к компьютерной информации?

27. Какие обстоятельства могут указывать на признаки несанкционированного доступа или подготовки к нему?
28. Какую последовательность действий целесообразно применять при расследовании компьютерных преступлений, связанных с созданием, использованием и распространением вредоносных программ для ЭВМ?
29. Что необходимо установить и доказать при расследовании нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети?
30. Какие особенности должны учитываться при производстве следственных действий по расследованию преступлений в сфере компьютерной информации?
31. Какие неблагоприятные факторы следует принять во внимание при производстве следственных действий?
32. Каких рекомендаций должен придерживаться следователь в целях недопущения вредных последствий неблагоприятных факторов?
33. Каковы типичные следственные ситуации и действия следователя на первоначальном этапе расследования преступлений в сфере компьютерной информации?
34. Какие основные особенности должны учитываться при проведении следственных действий по делам о преступлениях в сфере компьютерной информации?
35. Каков должен быть состав следственно-оперативной группы при осмотре места происшествия?
36. Каковы особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг сети Интернет?
37. Что фиксируют в протоколе осмотра средств вычислительной техники?
38. Что необходимо зафиксировать в протоколе при осмотре документов и их носителей?
39. Что относится к объектам компьютерно-технической экспертизы?
40. Какие вопросы выносятся на разрешение компьютерно-технической экспертизы?
41. Какие вопросы разрешаются при исследовании носителей машинной информации?
42. Какие вопросы разрешаются при исследовании баз данных?
43. Какие вопросы разрешаются при исследовании аппаратного обеспечения ЭВМ?
44. Перечислите и охарактеризуйте организационно-технические меры предупреждения компьютерных преступлений.
45. Каковы наиболее эффективные направления в предупреждении компьютерных преступлений?
46. Какие меры необходимо принимать для уменьшения опасности вирусных посягательств на средства вычислительной техники?
47. Каковы правовые меры предупреждения компьютерных преступлений?
48. Проведите анализ состава преступления, предусмотренного ст. 272 УК РФ – «Неправомерный доступ к компьютерной информации».
49. Проведите анализ состава преступления, предусмотренного ст. 273 УК РФ – Создание, использование и распространение вредоносных программ для ЭВМ».
50. Проведите анализ состава преступления, предусмотренного ст. 274 УК РФ – Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

7.4. Методические материалы, определяющие процедуру оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.
Общий результат выводится как интегральная оценка, складывающаяся из текущего контроля – 50 % и промежуточного контроля – 50 %
Текущий контроль по дисциплине включает:
- посещение занятий – 5 баллов,
- участие на практических занятиях – 20 баллов,
- выполнение домашних (аудиторных) контрольных работ - 15 баллов.
Промежуточный контроль по дисциплине включает:
- устный опрос - 15 баллов,
- письменная контрольная работа - 35 баллов,
- тестирование - 10 баллов.

8. Перечень основной и дополнительной учебной литературы и нормативных правовых актов, необходимых для освоения дисциплины

Нормативные правовые акты:

1. Всеобщая декларация прав человека. Международная защита прав и свобод человека. Сборник документом.- М.: Юридическая Литература, 1990.
2. Конституция Российской Федерации от 12 декабря 1993г. М., 2021.
3. Уголовный кодекс Российской Федерации. М., 2021.

4. Уголовно-процессуальный кодекс Российской Федерации. М., 2021.
5. Кодекс Российской Федерации об административных правонарушениях. М., 2021.
6. Федеральный закон от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».
7. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» // СПС «КонсультантПлюс».
8. Закон Российской Федерации от 23 сентября 1992 г. № 3523–1. «О правовой охране программ для электронных вычислительных машин и баз данных» // СПС «КонсультантПлюс».
9. Закон Российской Федерацииот 21июля 1993 г. №5485–1. «О государственной тайне» // СПС «КонсультантПлюс».

А) Основная литература:

Информационные технологии в юридической деятельности : учебник и практикум для академического магистратуры / В. Д. Элькин [и др.] ; под ред. В. Д. Элькина. — 2-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 403 с. — (Серия : Магистр. Академический курс)

Мельников В. П., Клейменов С.А., Петра-ков А.М. Информационная безопасность и защита информации : учеб.пособие для студентов вузов. - 2е изд.,стер. - Москва :Academia, 2007.

Казанцев С.Я и др. Правовое обеспечение информационной безопасности : учеб. пособие для студентов вузов. - 3-е изд.,стер. -Москва : Academia, 2008.

Пальцева Е.С. Информационная прозрачность правосудия: пределы и ограничения. // Информационное право, № 4(35), 2013.

Информационные технологии в юридической деятельности : учебное пособие / сост. И.П. Хвостова, А.А. Плетухина ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального обра-зования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2015. - 222 с. : ил. - Библиогр. в кн.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457972 (10.10.2018).

Капинус О.С. Уголовное право России. Особенная часть в 2 томах. Том 2. Учебник для академическогомагистратуры. — М.: Юрайт. 2017.

Наумов А.В. Российское уголовное право. Общая часть. Курс лекций.-6-е изд. — М.: Проспект. 2020.

Рарог А. И. Уголовное право России. Части общая и особенная. Учебник для магистров. — М.: Проспект. 2020.

Российское уголовное право. Общая часть. Учебник. / под ред. Есакова Г.А. — М.: Проспект. 2020.

Уголовное право России. Общая часть. Учебник для магистров. / под ред. Непомнящая Т. В., Гринберг М. С. — М.: Проспект. 2020.

Уголовное право России. Общая часть. Учебник. / под ред. Круковского В.Е., ЧучаеваА.И. -М.: Проспект, 2020.

Б) Дополнительная литература

Беляева Т.М., Кудинов А.Т., Пальянова Н.В., Чубукова С.Г., Элькин А.Д. Информационные технологии в юридической деятельности. /Учебник и практикум / Москва, 2016. Сер. 68 Профессиональное образование (3-е изд., пер. и доп.)

Бурняшов Б.А. Информационные технологии в юридической деятельности. Учебно-методическое пособие / Саратов, 2014.

Воронин С.А. Практика и перспективы применения информационных технологий в судебной экспертизе. //Международное научное издание Современные фундаментальные и прикладные исследования. 2016. Т. 2. № 2 (21). С. 109-114.

Информационные технологии в юридической деятельности : учебник для академического магистратуры / П. У. Кузнецов [и др.]. — 3-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 325 с. — (Серия : Магистр. Академический курс).

Макарова, Наталья Владимировна. Информатика : учеб.для вузов: [для магистров] / Макарова, Наталья Владимировна, В. Б. Волков. - СПб. [и др.] : Питер, 2013, 2011. - 573 с. - (Учебник для вузов). - Рекомендовано УМО. - ISBN 978-5-496-00001-7: 441-00.

9.Перечень ресурсов информационно –телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

При изучении курса «Преступления в сфере высоких технологий» рекомендуется пользоваться информационно-правовыми системами «Гарант» и «КонсультантПлюс», из которых можно извлечь полезную для изучения данного курса информацию.

Не менее важным в плане информационного обеспечения учебного процесса является использование Интернет ресурса как источника информации, не доступной в иных формах публикации. Имеются в виду, в частности, ежегодные доклады Генерального прокурора Российской Федерации о состоянии законности в стране, ежегодные доклады Уполномоченного по правам человека об обеспечении прав человека в стране и т.д.

Также рекомендуем пользоваться информацией, размещаемой на официальных сайтах органов государственной власти и профессиональных объединений юристов, в частности:

http://www.duma.gov.ru (Государственная Дума);
http://www.council.gov.ru (Совет Федерации);
http://www.government.ru (Правительство Российской Федерации);
http://genproc.gov.ru (Генеральная прокуратура РФ);
http://www.supcourt.ru (Верховный Суд РФ);
http://ksrf.ru/pages/default.aspx (Конституционный Суд РФ);
http://www.mvd.ru (Министерство внутренних дел РФ);
http://www.fsb.ru (Федеральная служба безопасности РФ);
http://www.minjust.ru (Министерство юстиции РФ);
http://www.sledcomproc.ru (Следственный комитет при прокуратуре РФ);
http://www.unionlawyers.ru (Международный союз юристов);
http://www.alrf.ru (Ассоциация юристов России);
http://www.ssrf.ru (Совет судей РФ);
http://www.advpalata.ru (Федеральная палата адвокатов);
http://gra.litsa.ru (Гильдия Российских адвокатов);
http://05.mvd.ru (Министерство внутренних дел по Республике Дагестан)

10. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению дисциплины «Преступления в сфере высоких технологий», рекомендуется ознакомиться с настоящей рабочей программой и с соответствующими разделами учебников по уголовному праву, криминологии и криминалистики. Настоящая учебная программа рекомендована для студентов и имеет своей целью помочь им разобраться в вопросах борьбы с преступлениями в сфере высоких технологий, с их предупреждением. Здесь вы найдете перечень основных тем данного курса по каждому из модулей, приведен список рекомендуемой к изучению уголовно-правовой, криминологической и криминалистической литературы. Кроме того, для умелого противодействия указанным преступлениям необходимо ознакомиться и с основами информационного права, на что также делается упор в представленной рабочей программе.

Рабочую программу целесообразно использовать и в качестве самоконтроля, проверки усвоения изученного материала. Для глубокого и всестороннего изучения теоретических проблем, затронутых в ней, рекомендован довольно широкий перечень нормативных правовых актов и специальной литературы. Следует заметить, что для овладения полным комплексом знаний большое значение имеет самостоятельное изучение рекомендуемых литературных источников и глубокое знание законодательного материала, касающееся, в частности, юридической ответственности за правонарушения, в том числе и преступления, совершаемые с использованием компьютерной информации. В этой связи необходимо отслеживать

публикации периодической печати, относящиеся к проблематике настоящего курса, знать изменения, вносимые в уголовное законодательство.

Мы полагаем, что одна из основных целей-задач, стоящих перед студентами и, одновременно, перед преподавателями в ходе изучения данного курса, как, впрочем, и иных дисциплин, состоит в том, чтобы привить (если это не произошло ранее) студентам криминологическое мышление. Его основа должна быть заложена в процессе изучения курса криминологии и других базовых дисциплин уголовно-правового цикла. Причем, хотелось бы не просто способствовать этому, а по возможности формировать *критическое* криминологическое мышление, которое помогло бы будущим магистрам не принимать на веру те или иные факты, сведения и события правовой действительности, включая в первую очередь статистические данные и решения правоохранительных и судебных органов, а критически осмысливать и оценивать их.

Залогом успешного овладения материалом данной дисциплины является хорошее знание предмета уголовного права и криминологии, а также изучение ряда рекомендуемых нормативных правовых актов.

Хорошим подспорьем в ходе изучении теоретических вопросов, рекомендуемых в представленной рабочей программе, могут явиться содержащиеся здесь планы практических занятий, которые включают контрольные вопросы с разбивкой их по соответствующим темам и рекомендуемые к изучению литературные источники.

Полагаю, что изучение вопросов рассматриваемой дисциплины поможет обучающимся добиться укрепления законности и правопорядка, вести борьбу с правонарушителями и преступностью в сфере высоких технологий на должном профессиональном уровне.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

1. Операционная система MicrosoftWindows 7;
2. Пакет офисных программ MicrosoftOffice 2010;
3. Антивирусные программы;
4. Программы-архиваторы;
5. Справочная правовая система «Консультант Плюс»;
6. Справочная правовая система «Гарант»;
7. Информационные ресурсы научной библиотеки Даггосуниверситета (доступ через платформу Научной электронной библиотеки elibrary.ru) http://elib.dgu.ru
8. Электронные каталоги Научной библиотеки Даггосуниверситета http://elib.dgu.ru/?q=node/256
9. Сайт образовательных ресурсов Даггосуниверситетаhttp://edu.icc.dgu.ru

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Материально-техническое обеспечение дисциплины «Преступления в сфере высоких технологий» составляет учебно-научно-методический кабинет кафедры уголовного права и криминологии, оснащенный компьютерами, содержащими базы данных справочно-правовых систем «Консультант Плюс» и «Гарант», научная и методическая литература, периодика юридических изданий и пр.