

Министерство науки и высшего образования Российской Федерации

ЧИТИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ  
Первый заместитель директора  
Н.В. Раевский  
26 февраля 2025 г.  
М.П.

Рабочая программа дисциплины  
Б1.Э.1 Особенности расследования преступлений в сфере компьютерной  
информации

Специальность: 40.05.04 Судебная и прокурорская деятельность

Специализация: Судебная деятельность

Квалификация выпускника: юрист

Форма обучения: очная

	очная ФО
Курс	5
Семестр	5.2
Лекции (час)	14
Практические (сем., лаб.) занятия (час)	14
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	44
Курсовая работа (час)	-
Всего часов	72
Зачет (семестр)	-
Экзамен (семестр)	5.2

Рабочая программа обсуждена и утверждена на заседании кафедры гражданского и уголовного права и процесса

24 февраля 2025 г. протокол № 6

Зав. кафедрой  
Е.В. Ракитина  
24 февраля 2025 г.

  
(подпись)

Рабочая программа согласована:  
Зав. кафедрой гражданского и уголовного права и процесса  
Е.В. Ракитина  
26 февраля 2025 г.

  
(подпись)

Чита, 2025

Программа составлена в соответствии с ФГОС ВО по специальности *40.05.04 Судебная и прокурорская деятельность*

Автор (ы)

к.юр.н. , доцент

Е.В. Ракитина

### 1. Цели изучения дисциплины

Целями освоения дисциплины «Особенности расследования преступлений в сфере компьютерной информации» является получение студентами необходимых знаний при раскрытии и расследовании преступлений в сфере компьютерной информации.

### 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

#### Компетенции обучающегося, формируемые в результате освоения дисциплины

<i>Код компетенции по ФГОС ВО</i>	<i>Компетенция</i>
<b>ПК-6</b>	Способен применять методы проведения прикладных научных исследований, анализа и обработки их результатов

#### Структура компетенции

<i>Компетенция</i>	<i>Формируемые ЗУНы</i>
ПК-6 Способен применять методы проведения прикладных научных исследований, анализа и обработки их результатов	З. Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации У. Уметь анализировать и обрабатывать результаты прикладных научных исследований при расследовании преступлений в сфере компьютерной информации Н. Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации

### 3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.Э.1 «Особенности расследования преступлений в сфере компьютерной информации» входит в Блок «Б1 дисциплины (модули)»

Необходимые для изучения дисциплины знания, умения и навыки формируются в ходе изучения уголовного права и криминалистики. Изучение дисциплины готовит обучающихся к прохождению производственной практики, выполнению ВКР.

### 4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зач. ед., 72 часов.

Вид учебной работы	Количество часов (очная ФО)
Контактная (аудиторная) работа	
Лекции	14
Практические (сем., лаб.) занятия	14

Самостоятельная работа, включая подготовку к экзаменам и зачетам	44
Всего часов	72

**5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**5.1. Содержание разделов дисциплины**

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат.Пра ктич.	Самостоят. раб.	В интеракти вной форме	Формы текущего контроля успеваемости и
<b>1</b>			<b>14</b>	<b>14</b>	<b>44</b>		<b>Уо, СЗ</b>
1.1	Уголовно-правовая и криминалистическая характеристика преступлений в сфере компьютерной информации.	5.2	2	2	6,5		Уо, СЗ
1.2	Характеристика личности преступника, совершающего преступления в сфере компьютерной информации.	5.2	2	2	6,5		Уо, СЗ
1.3	Типичные способы совершения преступлений в сфере компьютерной информации.	5.2	2	2	6,5		Уо, СЗ
1.4	Особенности организации и планирования расследования на первоначальном этапе	5.2	2	2	6,5		Уо, СЗ
1.5	Система специальных средств собирания и исследования следов преступлений, совершенных с использованием	5.2	2	2	6		Уо, СЗ

	компьютерных технологий						
1.6	Участие специалиста и эксперта при расследовании преступлений в сфере компьютерной информации.	5.2	2	2	6		Уо, СЗ
1.7	Противодействие преступности в сфере компьютерных технологий	5.2	2	2	6		Уо, СЗ
	<b>ИТОГО</b>		<b>14</b>	<b>14</b>	<b>44</b>		

**\*Формы текущего контроля успеваемости (оценочные средства):**

**Уо** -устный опрос, собеседование

**КО** -коллоквиум, конференция

**Л** -лабораторная работа

**ДИ** -деловая игра

**СЗ** -ситуационные задания

**К** -контрольные работы

**Т** -тестирование

**РЗ** -решение задач

**РГ** -расчетно-графическая работа

**ЭС** -эссе

**Р** -реферат

**УИ** -учебное исследование

**П** -прочие

**Э** -экзамен

**З** -зачет

**КР** -курсовая работа

**О** -отчет

**Г** -государственный итоговый экзамен

**ВКР** -выпускная квалификационная работа

**По** -письменный опрос

**5.2. Лекционные занятия, их содержание**

№ п/п	Наименование разделов и тем	Содержание
1.	Уголовно-правовая и криминалистическая характеристика преступлений в сфере компьютерной информации.	1. Характеристика составов преступлений в сфере компьютерной информации. 2. Понятие, содержание и основные элементы криминалистической характеристики преступлений в сфере компьютерной информации. 3. Компьютерная информация, вредоносные программы, средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных

		сетей и окончного оборудования, как предмет преступления. 4. 4. Критическая информационная инфраструктура Российской Федерации 5. Особенности обстановки совершения компьютерных преступлений, иные обстоятельства совершения преступлений в сфере компьютерной информации.
2.	Характеристика личности преступника, совершающего преступления в сфере компьютерной информации.	Социально-демографическая и социально-психологическая, характеристика личности преступника, совершающего преступления в сфере компьютерной информации. Типология личности преступника, совершающего преступления в сфере компьютерной информации.
3.	Типичные способы совершения преступлений в сфере компьютерной информации.	Механизмы и способы совершения компьютерных преступлений. Понятие и классификация следов компьютерного преступления. Следы относительно простых способов совершения компьютерных преступлений. Следы типичных высокотехнологичных способов совершения компьютерных преступлений. Способы сокрытия следов преступлений. Идентификация преступника
4.	Особенности организации и планирования расследования на первоначальном этапе	Особенности организации и планирования расследования на первоначальном этапе Установление достаточных данных, указывающих на признаки преступления. Возбуждение уголовного дела. Выдвижение следственных версий. Планирование расследования. Создание следственной группы и налаживание взаимодействия в ней
5.	Система специальных средств собирания и исследования следов преступлений, совершенных с использованием компьютерных технологий	Понятие, сущность и задачи обыска и выемки по делам о компьютерных преступлениях. Основания для производства обыска и выемки. Тактика обыска в помещении. Применение научно-технических средств. Фиксация хода и результатов обыска протоколом.
6.	Участие специалиста и эксперта при расследовании преступлений в сфере компьютерной информации.	Участие специалиста при проведении отдельных следственных действий. Назначение экспертиз при расследовании преступлений в сфере компьютерной информации. Помощь специалистов и экспертов по делам о компьютерных преступлениях. Ограничения при использовании помощи специалиста. Понятие и содержание компьютерно технической экспертизы. Назначение судебной компьютерно-технической экспертизы. Техническая экспертиза компьютеров, их отдельных устройств и комплектующих и техническая экспертиза компьютерных данных и программного обеспечения. Вопросы, подлежащие рассмотрению.
7.	Противодействие преступности в сфере	Содержание и структура криминалистического предупреждения компьютерных преступлений.

	компьютерных технологий	Причины и условия, способствующие преступлениям в сфере компьютерной информации. Организационные и правовые основы противодействия преступлениям в сфере компьютерной информации. Меры обеспечения криминалистического предупреждения.
--	-------------------------	--

### 5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
Раздел 1. Тема 1.	1. Характеристика составов преступлений в сфере компьютерной информации. 2. Понятие, содержание и основные элементы криминалистической характеристики преступлений в сфере компьютерной информации. 3. Компьютерная информация, вредоносные программы, средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и окончного оборудования, как предмет преступления. 4. Критическая информационная инфраструктура Российской Федерации 5. Особенности обстановки совершения компьютерных преступлений, иные обстоятельства совершения преступлений в сфере компьютерной информации.
Раздел 1. Тема 2.	1. Социально-демографическая и социально-психологическая, характеристика личности преступника, совершающего преступления в сфере компьютерной информации. 2. Типология личности преступника, совершающего преступления в сфере компьютерной информации по содержанию антиобщественной направленности. 3. Типология личности преступника, совершающего преступления в сфере компьютерной информации по устойчивости антиобщественной направленности.
Раздел 1. Тема 3.	1. Механизмы и способы совершения компьютерных преступлений. 2. Понятие и классификация следов компьютерного преступления. Следы относительно простых способов совершения компьютерных преступлений. Следы типичных высокотехнологичных способов совершения компьютерных преступлений. 3. Способы сокрытия следов преступлений. 4. Идентификация преступника.
Раздел 1. Тема 4.	1. Особенности организации и планирования расследования на первоначальном этапе 2. Установление достаточных данных, указывающих на признаки преступления. 3. Возбуждение уголовного дела. Выдвижение следственных версий. 4. Планирование расследования. Создание следственной группы и налаживание взаимодействия в ней 5. Взаимодействие следователя (следственной группы) с органами государственной власти, ОМСУ и организациями при расследовании преступлений в сфере компьютерной информации.
Раздел 1. Тема 5.	1. Понятие, сущность и задачи обыска и выемки по делам о компьютерных преступлениях. 2. Основания для производства обыска и выемки. Тактика обыска в помещении. 3. Применение научно-технических средств. 4. Фиксация хода и результатов обыска протоколом.
Раздел 1. Тема 6.	1. Участие специалиста при проведении отдельных следственных действий. 2. Назначение экспертиз при расследовании преступлений в сфере компьютерной информации. 3. Помощь специалистов и экспертов по делам о компьютерных преступлениях. Ограничения при использовании помощи специалиста. 4. Понятие и содержание компьютерно технической экспертизы. Назначение судебной компьютерно-технической экспертизы. 5.

	Техническая экспертиза компьютеров, их отдельных устройств и комплектующих и техническая экспертиза компьютерных данных и программного обеспечения. Вопросы, подлежащие рассмотрению.
Раздел 1. Тема 7.	1. Содержание и структура криминалистического предупреждения компьютерных преступлений. 2. Причины и условия, способствующие преступлениям в сфере компьютерной информации. 3. Организационные и правовые основы противодействия преступлениям в сфере компьютерной информации. 4. Меры обеспечения криминалистического предупреждения.

**6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)**

**6.1. Текущий контроль**

№ п/п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	ЗУНы (З.1...З.п, У.1...У.п, Н.1...Н.п)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	Уголовно-правовая и криминалистическая характеристика преступлений в сфере компьютерной информации.	ПК-6	Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации Уметь	Уо, СЗ	правильный и полный ответ на вопрос - до 5 баллов Правильно выполненное тестовое задание - 1 бал

			анализировать и обрабатывать результаты прикладных научных исследований при расследовании преступлений в сфере компьютерной информации Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации		
2	Характеристика личности преступника, совершающего преступления в сфере компьютерной информации.	ПК-6	Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации Уметь анализировать и	Уо, Т	правильный и полный ответ на вопрос - до 5 баллов Правильно выполненное тестовое задание - 1 бал

			<p>обрабатывать результаты прикладных научных исследований при расследовании преступлений в сфере компьютерной информации</p> <p>Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации</p>		
3	<p>Типичные способы совершения преступлений в сфере компьютерной информации.</p>	ПК-6	<p>Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации</p> <p>Уметь анализировать и обрабатывать результаты</p>	Уо, Т	<p>правильный и полный ответ на вопрос - до 5 баллов</p> <p>Правильно выполненное тестовое задание - 1 бал</p>

			<p>прикладный научных исследований при расследовании преступлений в сфере компьютерной информации</p> <p>Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации</p>		
4	Особенности организации и планирования расследования на первоначальном этапе	ПК-6	<p>Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации</p> <p>Уметь анализировать и обрабатывать результаты прикладных научных</p>	Уо, Т	<p>правильный и полный ответ на вопрос - до 5 баллов</p> <p>Правильно выполненное тестовое задание - 1 бал</p>

			исследовани й при расследован ии преступлени й в сфере компьютерн ой информации Владеть навыками проведения прикладных научных исследовани й, анализа и обработки их результатов при расследован ии преступлени й в сфере компьютерн ой информации		
5	Система специальных средств собирания и исследования следов преступлений, совершенных с использованием компьютерных технологий	ПК-6	Знать методы проведения прикладных научных исследовани й, анализа и обработки их результатов при расследован ии преступлени й в сфере компьютерн ой информации Уметь анализирова ть и обрабатыват ь результаты прикладный научных исследовани й при	Уо, Т	правильный и полный ответ на вопрос - до 5 баллов Правильно выполненное тестовое задание - 1 бал

			<p>расследовании преступлений в сфере компьютерной информации</p> <p>Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации</p>		
6	<p>Участие специалиста и эксперта при расследовании преступлений в сфере компьютерной информации.</p>	ПК-6	<p>Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации</p> <p>Уметь анализировать и обрабатывать результаты прикладных научных исследований при расследовании</p>	Уо, Т	<p>правильный и полный ответ на вопрос - до 5 баллов</p> <p>Правильно выполненное тестовое задание - 1 бал</p>

			преступлений в сфере компьютерной информации Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации		
7	Противодействие преступности в сфере компьютерных технологий	ПК-6	Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации Уметь анализировать и обрабатывать результаты прикладных научных исследований при расследовании преступлений в сфере	Уо, Т	правильный и полный ответ на вопрос - до 5 баллов Правильно выполненное тестовое задание - 1 бал

			компьютерной информации Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации		
8	Итого по текущей аттестации	ПК-6	Знать методы проведения прикладных научных исследований, анализа и обработки их результатов при расследовании преступлений в сфере компьютерной информации Уметь анализировать и обрабатывать результаты прикладных научных исследований при расследовании преступлений в сфере компьютерной информации		правильный и полный ответ на вопрос - до 5 баллов Правильно выполненное тестовое задание - 1 бал

			информации Владеть навыками проведения прикладных научных исследовани й, анализа и обработки их результатов при расследован ии преступлени й в сфере компьютерн ой информации		
9	Промежуточная аттестация	ПК-6	Знать методы проведения прикладных научных исследовани й, анализа и обработки их результатов при расследован ии преступлени й в сфере компьютерн ой информации Уметь анализирова ть и обрабатыват ь результаты прикладный научных исследовани й при расследован ии преступлени й в сфере компьютерн ой информации Владеть		правильный и полный ответ на вопрос - до 5 баллов Правильно выполненное тестовое задание - 1 бал

			навыками проведения прикладных научных исследовани й, анализа и обработки их результатов при расследован ии преступлени й в сфере компьютерн ой информации		
--	--	--	---	--	--

## 6.2. Промежуточный контроль (зачет, экзамен)

Рабочим учебным планом предусмотрен Экзамен

### ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

Компетенция: ПК-6 Способен применять методы проведения прикладных научных исследований, анализа и обработки их результатов

Знание: Знать методы проведения прикладных научных исследований, анализа и обработки их результатов

1. Изготовление и распространение порнографических материалов с использованием компьютерной техники.
2. Классификация преступления в сфере цифровой информации.
3. Кража, совершенная с банковского счета, а равно в отношении электронных денежных средств.
4. Криминализация посягательств на безопасность компьютерной информации в зарубежных государствах.
5. Криминологическая характеристика преступности в сфере цифровой экономики.

### ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

Компетенция: ПК-6 Способен применять методы проведения прикладных научных исследований, анализа и обработки их результатов

Умение: Уметь анализировать и обрабатывать результаты прикладных научных исследований

Задача № 1. Решить задачу, дать развернутый ответ

18 часов 55 минут 1 марта 2008 года, Петрухин С.А. отправил на электронный почтовый ящик, принадлежащий гр. Горину, письмо ложного содержания с прикрепленным к нему файлом, содержащим в себе программу для ЭВМ, которая определяется антивирусной программой AVP 32 Лаборатории Касперского как вирус "TrojanDropper. Win32 .Joiner.a", имеющий своей функциональной особенностью копирование с инфицированных компьютеров конфиденциальной информации о пароле и логине доступа в сеть Интернет на заранее заданный электронный адрес злоумышленника. Указанное письмо поступило на сервер в Интернете для обработки и отправки на ящик Горину, однако, в ходе проверки антивирусная программа указанного сервера обнаружила в файле, приложенном к письму, программу-вирус и не позволила этим файлам дойти до адресата.

Задание: 1) Дайте правовую оценку деяния Петрухина С.А. Ответ дайте на основе выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений.

## ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

Компетенция: ПК-6 Способен применять методы проведения прикладных научных исследований, анализа и обработки их результатов

Навык: Владеть навыками проведения прикладных научных исследований, анализа и обработки их результатов

Задание № 1. Дать развернутый ответ на представленную задачу

### ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования Российской Федерации Читинский институт (филиал) Федерального государственного бюджетного образовательного учреждения высшего образования «БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ» (ЧИ ФГБОУ ВО «БГУ»)	Направление - 40.05.04 Судебная и прокурорская деятельность Профиль - Судебная деятельность Кафедра гражданского и уголовного права и процесса Дисциплина - Особенности расследования преступлений в сфере компьютерной информации
--	---

### ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Тест по теме «Характеристика международного и российского законодательства в сфере информации, информатизации и защиты информации» (40 баллов).

2. Дать развернутый ответ на задачу (30 баллов).

3. Решить задачу, дать развернутый ответ (30 баллов).

Составитель \_\_\_\_\_ Е.В. Ракитина

Заведующий кафедрой \_\_\_\_\_ Е.В. Ракитина

#### Перечень вопросов к зачету (экзамену)

1. Характеристика международного и российского законодательства в сфере информации, информатизации и защиты информации.

2. Отличие информации, компьютерной информации, правовой информации.

3. Компьютерные технологии: понятие, значение, сущность.

4. Содержание и особенности уголовно-правовой характеристики преступлений в сфере компьютерной информации

5. . Содержание и особенности криминалистической характеристики преступлений в сфере компьютерной информации.

6. Особенности организации и проведения проверки заявлений и сообщений о преступлениях в сфере компьютерной информации

7. Ситуации, наиболее характерные для этапа проверки сообщений о преступлениях в сфере компьютерной информации

8. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.

9. Социально-демографическая характеристика личности преступника, совершающего компьютерные преступления

10. Типология личности преступника, совершающего компьютерные преступления по содержанию и устойчивости антиобщественно направленности

11. Характеристика международного и российского законодательства в сфере информации, информатизации и защиты информации.

12. Содержание и особенности уголовно-правовой характеристики преступлений в сфере компьютерной информации. Объект и объективная сторона. Субъект и субъективная

сторона. Квалификационные признаки.

13. Содержание и особенности криминалистической характеристики преступлений в сфере компьютерной информации.

14. Особенности организации и проведения проверки заявлений и сообщений о преступлениях в сфере компьютерной информации

15. Ситуации, наиболее характерные для этапа проверки сообщений о преступлениях в сфере компьютерной информации

16. Непосредственный предмет преступного посягательства по делам о компьютерных преступлениях.

17. Особенности обстановки совершения компьютерных преступлений.

18. Характеристика способа совершения компьютерного преступления.

19. Понятие и классификация следов компьютерных преступлений.

20. Регистрационные файлы операционных систем и регистрационные файлы СУБД как доказательства по делу.

21. Поводы и основания для возбуждения уголовных дел в сфере компьютерной информации.

22. Особенности возбуждения уголовного дело при расследовании преступлений в сфере компьютерной информации.

23. Типичные следственные ситуации и версии первоначального этапа расследования преступлений в сфере компьютерной информации.

24. Обстоятельства, подлежащие установлению и доказыванию по делам о преступлениях в сфере компьютерной информации.

25. Особенности организации и проведения допроса свидетеля, потерпевшего по делам о преступлениях в сфере компьютерной информации.

26. Особенности организации и производства обыска по делам о преступлениях в сфере компьютерной информации.

27. Взаимодействие следователя с оперативными подразделениями на первоначальном этапе расследования преступлений в сфере компьютерной информации.

28. Возможности использования специальных познаний в ходе расследования преступлений в сфере компьютерной информации.

29. Виды судебных экспертиз, проводимых по делам о преступлениях в сфере компьютерной информации.

30. Задачи, решаемые в ходе компьютерных экспертиз.

31. Особенности изъятия и осмотра компьютерной информации и носителей информации.

32. Особенности назначения и производства компьютерных экспертиз.

33. Принципы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений в сфере компьютерной информации.

34. Содержание последующего и заключительного этапов расследования по преступлениям в сфере компьютерной информации.

35. Предъявление обвинения в ходе расследовании преступлений в сфере компьютерной информации.

36. Тактика производства отдельных следственных действий при расследовании преступлений в сфере компьютерной информации на последующем и заключительном этапах.

37. Специальные структуры в правоохранительных органах в борьбе с преступлениями в сфере компьютерной информации.

38. Специализированное программное обеспечения для предупреждения и выявления преступлений в сфере компьютерной информации.

39. Сущность фиксации следовой информации по делам о компьютерных преступлениях.

40. Особенности фиксации следовой информации о попытках зондирования

компьютерных систем или ведения радиоэлектронной разведки.

41. Особенности фиксации следовой информации о действии вредоносных программ в ходе осмотра компьютерных систем и их сети.

42. Особенности фиксации следовой информации при проведении аудита компьютерных систем в ходе осмотра компьютерных систем и их сетей.

## **7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)**

### **а) основная литература:**

1. Организация противодействия преступлениям в сфере информационно-телекоммуникационных технологий : практикум / В. В. Пушкарев, А. В. Константинов, В. Б. Вехов [и др.]. — Москва : Ай Пи Ар Медиа, 2025. — 263 с. — ISBN 978-5-4497-4085-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/147936.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей

2. Кулешов, Ю. Н. Методика расследования преступлений, совершенных с применением цифровых технологий : учебное пособие / Ю. Н. Кулешов, Р. Н. Подольный. — Москва : Ай Пи Ар Медиа, 2025. — 84 с. — ISBN 978-5-4497-3840-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/144743.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей. - DOI: <https://doi.org/10.23682/144743>

3. Расторопов, С. В. Мошенничество в сфере компьютерной информации: уголовно-правовой и криминологический аспекты / С. В. Расторопов, В. К. Барчуков. — Санкт-Петербург : Юридический центр Пресс, 2021. — 228 с. — ISBN 978-5-94201-820-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/133129.html> (дата обращения: 20.02.2025). — Режим доступа: для авторизир. пользователей

### **б) дополнительная литература:**

1. Курс криминалистики. В 3 томах. Т.3. Методика расследования преступлений в сфере экономической деятельности. Методика расследования преступлений против общественной безопасности, других видов и групп преступлений : учебник / М. А. Григорьева, Н. А. Данилова, С. Г. Евдокимов [и др.] ; под редакцией О. Н. Коршуновой. — 3-е изд. — Санкт-Петербург : Юридический центр Пресс, 2024. — 752 с. — ISBN 978-5-94201-729-3 (т.3), 978-5-94201-726-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/137038.html> (дата обращения: 20.02.2025). — Режим доступа: для авторизир. пользователей

2. Шестак, В. А. Ответственность за преступления в сфере экономической деятельности : учебное пособие / В. А. Шестак ; под редакцией А. Г. Волеводза. — Москва : Прометей, 2021. — 314 с. — ISBN 978-5-00172-106-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/125672.html> (дата обращения: 20.02.2025). — Режим доступа: для авторизир. пользователей

3. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суоров. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 368 с. — ISBN 978-5-4497-0931-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146404.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей

4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 543 с. — ISBN 978-5-4488-0074-0. — Текст : электронный // Цифровой образовательный ресурс IPR

SMART : [сайт]. — URL: <https://www.iprbookshop.ru/145909.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей

5. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 3-е изд. — Саратов : Профобразование, 2024. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/145912.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей

6. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 424 с. — ISBN 978-5-4497-2415-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/133955.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей

7. Минин, А. Я. Организация и методика исследовательской деятельности в сфере юриспруденции : учебное пособие для магистрантов / А. Я. Минин, А. В. Орлова ; под редакцией А. Я. Минина. — 2-е изд. — Москва : Московский педагогический государственный университет, 2024. — 128 с. — ISBN 978-5-4263-0515-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/146264.html> (дата обращения: 12.02.2025). — Режим доступа: для авторизир. пользователей

8. Дмитриев, В. Т. Защита информации в инфокоммуникационных системах. Ч.1 : учебное пособие / В. Т. Дмитриев. — Рязань : Рязанский государственный радиотехнический университет, 2023. — 160 с. — ISBN 978-5-7722-0370-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/134852.html> (дата обращения: 13.02.2025). — Режим доступа: для авторизир. пользователей

9. Дмитриев, В. Т. Защита информации в инфокоммуникационных системах. Ч.2 : учебное пособие / В. Т. Дмитриев. — Рязань : Рязанский государственный радиотехнический университет, 2023. — 148 с. — ISBN 978-5-7722-0371-2. — Текст : электронный // Цифровой

#### **в) интернет-ресурсы:**

#### **8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы**

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

Сайт ЧИ ФГБОУ ВО «БГУ», адрес доступа: <http://bgu-chita.ru/>, доступ круглосуточный неограниченный;

Цифровой образовательный ресурс IPR SMART – объединяет новейшие информационные технологии и учебную лицензионную литературу, предназначенный для разных направлений подготовки и специальностей. Контент отвечает требованиям стандартов высшего, среднего профессионального и дополнительного образования. Ресурсом обеспечивается круглосуточный полнотекстовый доступ к учебникам, журналам, статьям и другой литературе для всех зарегистрированных пользователей. Адрес доступа: <http://www.iprbookshop.ru>;

eLIBRARY.RU – крупнейшая в России электронная библиотека научных публикаций, обладающая богатыми возможностями поиска и анализа научной информации. eLIBRARY.RU является разработчиком российского индекса научного цитирования (РИНЦ). Пользование НЭБ eLibrary общедоступно и бесплатно для всех пользователей.

Адрес доступа: [https://www.elibrary.ru/](https://www.elibrary.ru;);

Электронный каталог библиотеки дает возможность поиска литературы, имеющейся в фонде библиотеки, обеспечивает полнотекстовый доступ к учебным пособиям, монографиям, статьям преподавателей и обучающихся, учебно-методическим комплексам и выпускным квалификационным работам. Адрес доступа: <http://lib.bgu-chita.ru/>;

Электронный ресурс цифровой образовательной среды СПО «PROFобразование». Адрес доступа: <https://profspo.ru/>;

Федеральная служба государственной статистики (Росстат). Адрес доступа: <https://rosstat.gov.ru/>;

## **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области \_\_\_\_\_.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Практические (семинарские) занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на практическое (семинарское) занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

- текущие консультации;
- коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);
- прием и разбор домашних заданий (в часы практических занятий);
- прием и защита лабораторных работ (во время проведения занятий);
- выполнение курсовых работ в рамках дисциплин (руководство, консультирование и защита курсовых работ в часы, предусмотренные учебным планом) и др.
- Основными видами самостоятельной работы студентов без участия преподавателей являются:
  - формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
  - самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;
  - написание рефератов, докладов;
  - подготовка к семинарам и лабораторным работам;
  - выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения**

В учебном процессе используется следующее программное обеспечение:

- КонсультантПлюс: Версия Проф - информационная справочная система,
- КонсультантПлюс: Сводное региональное законодательство,

- Гарант платформа F1 7.08.0.163 - информационная справочная система,
- MS Office

#### **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):**

В учебном процессе используются аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения:

учебные аудитории, оснащенные специализированной мебелью, магнитно-маркерной доской, трибуной для выступлений, техническими средствами обучения;

учебные аудитории для групповых и индивидуальных консультаций, оснащенные специализированной мебелью, магнитно-маркерной доской, техническими средствами обучения – ноутбук, проектор;

помещения для самостоятельной работы, оснащенные специализированной мебелью, доской, техническими средствами обучения – мультимедийное оборудование: проектор, компьютерная техника с возможностью подключения к сети Интернет и обеспечением доступа в ЭИОС.

**2025 год набора**