

**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ  
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ, НАУЧНО-ТЕХНОЛОГИЧЕСКОЙ ПОЛИТИКИ  
И РЫБОХОЗЯЙСТВЕННОГО КОМПЛЕКСА  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ  
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
ВЫСШЕГО ОБРАЗОВАНИЯ  
«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**

**ЮРИДИЧЕСКИЙ ИНСТИТУТ  
КАФЕДРА СУДЕБНЫХ ЭКСПЕРТИЗ**

**СОГЛАСОВАНО:**

Директор ЮИ Е. А. Ерахтина

«28» 03 2024 г.

**УТВЕРЖДАЮ:**

Ректор Н.И. Пыжикова

«31» 03 2024 г.

**РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ  
КРИМИНАЛИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ОПЕРАЦИОННЫХ  
СИСТЕМ В ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗАХ**

ФГОС ВО

Специальность: 40.05.03 «Судебная экспертиза»

Специализация: «Инженерно-технические экспертизы»

Курс: 5

Семестр (ы): 9

Форма обучения: очная

Квалификация выпускника: судебный эксперт

Красноярск, 2024



ДОКУМЕНТ ПОДПИСАН  
УСИЛЕННОЙ КВАЛИФИЦИРОВАННОЙ  
ЭЛЕКТРОННОЙ ПОДПИСЬЮ  
ВЫДАННОЙ: ФГБОУ ВО КРАСНОЯРСКИЙ ГАУ  
ВЛАДЕЛЕЦ: РЕКТОР ПЫЖИКОВА Н.И.  
ДЕЙСТВИТЕЛЕН: 15.05.2025 - 08.08.2026

Составитель: А.А. Рябикин, канд. филос. наук, доцент кафедры судебных экспертиз

\_\_\_\_\_ « 10 » \_\_\_\_\_ 03 \_\_\_\_\_ 2024 г.

Программа разработана в соответствии с ФГОС ВО по специальности 40.05.03 «Судебная экспертиза», специализация: «Инженерно-технические экспертизы».

Программа обсуждена на заседании кафедры:  
протокол № 13 от « 14 » \_\_\_\_\_ 03 \_\_\_\_\_ 2024 г.

Зав. кафедрой судебных экспертиз, канд.юрид.наук. \_\_\_\_\_ М.Э. Червяков

« 14 » \_\_\_\_\_ 03 \_\_\_\_\_ 2024 г.

## **Лист согласования рабочей программы**

Программа принята методической комиссией Юридического института  
Протокол №7 от «28» марта 2024 г.

Председатель Методической комиссии: Широких С.В.

---

«28» марта 2024 г.

Заведующий выпускающей кафедрой по направлению подготовки  
40.05.03 «Судебная экспертиза», направленность (профиль): «Инженерно-  
технические экспертизы»,

Червяков М.Э канд. юрид. наук, доцент

---

«28» марта 2024 г.

<b>Аннотация</b> .....	<b>5</b>
<b>1. Место дисциплины в структуре образовательной программы</b> .....	<b>6</b>
<b>2. Цели и задачи дисциплины. Компетенции, формируемые в результате освоения дисциплины</b> .....	<b>6</b>
<b>3. Организационно-методические данные дисциплины</b> .....	<b>9</b>
<b>4. Структура и содержание дисциплины</b> .....	<b>9</b>
<b>4.1. Трудоёмкость модулей и модульных единиц дисциплины</b> .....	<b>9</b>
<b>4.2. Содержание модулей дисциплины</b> .....	<b>10</b>
<b>4.3. Лекционные / лабораторные/ практические/ семинарские занятия</b> .....	<b>12</b>
<b>4.4. Самостоятельное изучение разделов дисциплины и виды самоподготовки к текущему контролю знаний</b> .....	<b>15</b>
<b>5. Взаимосвязь видов учебных занятий</b> .....	<b>17</b>
<b>6. Учебно-методическое и информационное обеспечение дисциплины</b> .....	<b>17</b>
<b>6.1. Карта обеспеченности литературой</b> .....	<b>18</b>
<b>6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»)</b> .....	<b>18</b>
<b>6.3. Программное обеспечение</b> .....	<b>18</b>

## Аннотация

Дисциплина «Криминалистическое исследование операционных систем в инженерно-технических экспертизах» относится к части дисциплин, формируемой участниками образовательных отношений Блока №1 подготовки обучающихся по специальности 40.05.03 Судебная экспертиза, специализация: «Инженерно-технические экспертизы».

Дисциплина реализуется в Юридическом институте кафедрой Судебных экспертиз.

Дисциплина нацелена на формирование профессиональных компетенций:

- ПК-3 - Способен применять методики инженерно-технических экспертиз и исследований в профессиональной деятельности;
- ПК-5 Способность консультировать субъектов правоприменительной деятельности по вопросам назначения и производства инженерно-технических экспертиз при расследовании преступлений и иных правонарушений.

Содержание дисциплины охватывает круг вопросов, связанных с формированием у обучающихся представления об общих принципах структурно-функциональной организации современных компьютерных сетей и средств телекоммуникаций, а также методики их осмотра на месте происшествия.

Изучение дисциплины осуществляется с использованием электронной информационно-образовательной среды Университета (LMS Moodle, сайт <http://e.kgau.ru/>).

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, коллоквиумы, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме устного опроса, тестирования, коллоквиумы и промежуточная аттестация успеваемости в форме зачета с оценкой (9 семестр).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы (108 час.). Программой дисциплины предусмотрены лекционные (28 часов), практические (28 часов) занятия и 54 часа самостоятельной работы обучающихся.

## 1. Место дисциплины в структуре образовательной программы

Дисциплина «Криминалистическое исследование операционных систем в инженерно-технических экспертизах» включена в ОПОП части дисциплин, формируемой участниками образовательных отношений Блока №1 подготовки обучающихся по специальности 40.05.03 Судебная экспертиза, специализация: «Инженерно-технические экспертизы».

Предшествующими курсами, на которых непосредственно базируется дисциплина «Криминалистическое исследование операционных систем в инженерно-технических экспертизах» являются «Информатика», «Логика»,» и др. Является основополагающей для изучения следующих дисциплин: «Судебная компьютерно-техническая экспертиза».

Особенностью дисциплины является изучение следующих модулей:

- 1-й модуль – «Операционные системы семейства WINDOWS»;
- 2-й модуль - «Операционные системы семейства Unix».

## 2. Цели и задачи дисциплины. Компетенции, формируемые в результате освоения дисциплины

Цель дисциплины «Криминалистическое исследование операционных систем в инженерно-технических экспертизах» состоит в формировании целостного представления, обучающегося об основных тенденциях в криминалистическом исследовании наиболее популярных операционных систем, а также уголовно-правовых и процессуальных основ использования специальных познаний в данной области IT-технологий.

Задачи дисциплины «Криминалистическое исследование операционных систем в инженерно-технических экспертизах»:

- изучение обучающимися функционального предназначения и характеристик основных элементов операционных систем;
- освоение обучающимися методов поиска, обнаружения, анализа и оценки криминалистически-значимой информации, образующейся в ходе эксплуатации операционных систем;
- изучение обучающимися методов работы с фактами и обстоятельствами, имеющими значение для уголовного или гражданского дела, которые устанавливаются в процессе исследования операционных систем;
- получить базовые навыки применения методов экспертно-криминалистического исследования операционных систем;
- сформировать у обучающихся практические навыки работы с использованием программных продуктов общего и специализированного экспертного назначения.

Таблица 1

Перечень планируемых результатов обучения по дисциплин

<p>ПК-3. Способен применять методики инженерно-технических экспертиз и исследований в профессиональной деятельности</p>	<p>ИД-1 ПК-3. Обладает знаниями о типовых методиках исследования объектов судебных инженерно-технических экспертиз.</p> <p>ИД-2 ПК-3 Применяет, путем модифицирования, типовую методику для решения конкретных экспертных задач.</p> <p>ИД-3 ПК-3. Выбирает методическое и технологическое обеспечение экспертной деятельности в целях объективного и всестороннего установления обстоятельств, подлежащих доказыванию по конкретному делу, при подготовке и производстве судебных экспертиз.</p>	<p><b>Знать:-</b> современные возможности судебных инженерно-технических экспертиз, методов и методик их производства в части исследования операционных систем; особенности использования специальных инженерно-технических знаний в целях получения розыскной и доказательственной информации при производстве различных процессуальных действий;</p> <ul style="list-style-type: none"> <li>- общие принципы работы с фактами и обстоятельствами, имеющими значение для уголовного или гражданского дела, и устанавливаемые на основе исследования закономерностей разработки и эксплуатации операционных систем;</li> <li>- функциональное предназначение, характеристики и методы применения специализированного программного обеспечения для исследования операционных систем.</li> </ul> <p><b>Уметь:-</b> производить судебные инженерно-технические исследования операционных систем с использованием современных экспертных технологий; применять при участии в процессуальных и не процессуальных действиях инженерно-технические методы и средства поиска, обнаружения, фиксации, изъятия и предварительного исследования материальных и информационных объектов;</p> <ul style="list-style-type: none"> <li>- оказывать методическую помощь субъектам правоприменительной деятельности по вопросам назначения и производства инженерно-технических экспертиз в части исследования операционных</li> </ul>
---	---	---

		<p>систем, использовать специальные знания по криминалистическому исследованию операционных систем при производстве различных процессуальных действий</p> <p><b>Владеть:-</b> навыками применения инженерно-технических методов и средств экспертного исследования операционных систем;</p> <p>- навыками применять инженерно-технические методы и средства поиска, обнаружения, фиксации, изъятия и предварительного исследования операционных систем как следообразующих и следовоспринимающих объектов для установления фактических данных (обстоятельств дела) в гражданском, административном, уголовном судопроизводстве, производстве по делам об административных правонарушениях</p>
<p>ПК-5 Способность консультировать субъектов правоприменительной деятельности по вопросам назначения и производства инженерно-технических экспертиз при расследовании преступлений и иных правонарушений</p>	<p>ИД-1 ПК-5. Знает характеристики технических средств используемых при производстве инженерно-технических экспертиз</p> <p>ИД-2 ПК-5. Владеет навыками определения круга потенциальных объектов судебных инженерно-технических экспертиз и способностью разъяснить субъектам правоприменительной деятельности возможности их предварительного и экспертного исследования с применениями современных методов и методик.</p> <p>ИД-3 ПК-5. Консультирует субъектов правоприменительной деятельности по вопросам назначения и производства судебных инженерно-технических экспертиз</p>	<p><b>Знать:</b> характеристики технических средств используемых при производстве инженерно-технических экспертиз</p> <p><b>Уметь:</b> консультировать субъекты правоприменительной деятельности по вопросам назначения и производства судебных инженерно-технических экспертиз</p> <p><b>Владеть:</b> навыками определения круга потенциальных объектов судебных инженерно-технических экспертиз и способностью разъяснить субъектам правоприменительной деятельности возможности их предварительного и экспертного исследования</p>

### 3. Организационно-методические данные дисциплины

Общая трудоёмкость дисциплины составляет 3 зач. ед. (108 час.), их распределение по видам работ и по семестрам представлено в таблице 2.

Таблица 2

Распределение трудоёмкости дисциплины по видам работ по семестрам

Вид учебной работы	Трудоёмкость		
	зач. ед.	час.	по семестрам
			№9
<b>Общая трудоёмкость</b> дисциплины по учебному плану	<b>3</b>	<b>108</b>	<b>108</b>
<b>Контактная работа</b>	<b>1,6</b>	<b>56</b>	<b>56</b>
в том числе:			
Лекции (Л) / в том числе в интерактивной форме	0,85	28	28
Практические занятия (ПЗ) / в том числе в интерактивной форме	0,8	28	28
Семинары (С) / в том числе в интерактивной форме			
Лабораторные работы (ЛР) / в том числе в интерактивной форме			
<b>Самостоятельная работа (СРС)</b>	<b>1,4</b>	<b>52</b>	<b>52</b>
в том числе:			
самостоятельное изучение тем и разделов	1,15	43	43
подготовка к коллоквиуму и тестированию			
подготовка к зачету	0,25	9	9
<b>Подготовка и сдача экзамена</b>			
<b>Вид контроля:</b>			зачет с оценкой

### 4. Структура и содержание дисциплины

#### 4.1. Трудоёмкость модулей и модульных единиц дисциплины

Таблица 3

Трудоёмкость модулей и модульных единиц дисциплины\*

Наименование модулей и модульных единиц дисциплины	Всего часов на модуль	Контактная работа		Внеаудиторная работа (СРС)
		Л	ЛЗ/ПЗ/С	
<b>Модуль 1. Операционные системы семейства WINDOWS</b>	<b>54</b>	<b>14</b>	<b>14</b>	<b>26</b>
Модульная единица 1.1. Исследование информации, идентифицирующей установленные операционные системы семейства WINDOWS и программные продукты в ОС.	14	4	4	6

Наименование модулей и модульных единиц дисциплины	Всего часов на модуль	Контактная работа		Внеаудиторная работа (СРС)
		Л	ЛЗ/ЛЗ/С	
Модульная единица 1.2. Защита программных продуктов от несанкционированного использования	14	4	4	6
Модульная единица 1.3. Процессуальные особенности исследования ОС семейства WINDOWS	14	2	2	6
Модульная единица 1.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства WINDOWS и ее криминалистическая значимость	8	2	2	4
Модульная единица 1.5. Информация, содержащаяся в системном реестре ОС семейства WINDOWS и ее криминалистическая значимость	8	2	2	4
<b>Модуль 2. Операционные системы семейства Unix</b>	<b>54</b>	<b>14</b>	<b>14</b>	<b>26</b>
Модульная единица 2.1. Основные понятия об ОС Unix	14	4	4	6
Модульная единица 2.2. Методические подходы предварительного исследования ОС семейства Unix на месте происшествия	14	4	4	6
Модульная единица 2.3. Журналы регистрации событий в ОС семейства Unix	10	2	2	6
Модульная единица 2.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства Unix и ее криминалистическая значимость	8	2	2	4
Модульная единица 2.5. Особенности исследования ОС семейства Mac OS X	8	2	2	4
<b>ИТОГО</b>	<b>108</b>	<b>28</b>	<b>28</b>	<b>52</b>

\* 9 часов на самоподготовку к зачету (зачет с оценкой) входят в общее количество часов, отведенных на самостоятельную работу в учебном семестре

## 4.2. Содержание модулей дисциплины

### Модуль 1. Операционные системы семейства WINDOWS

### **Модульная единица 1.1. Исследование информации, идентифицирующей установленные операционные системы семейства WINDOWS и программные продукты в ОС.**

Информация, идентифицирующая программные продукты корпорации Microsoft. Методика получения идентификационной информации о программных продуктах, установленных в ОС семейства Windows. Криминалистическая значимость служебной информации в

программной среде под управлением ОС семейства Windows.

### **Модульная единица 1.2. Защита программных продуктов от несанкционированного использования**

Типы лицензий программных продуктов корпорации Microsoft. Система активации в ОС семейства Windows. Программные и аппаратные средства защиты программных продуктов от несанкционированного использования. Основные способы обхода защиты

программных продуктов от несанкционированного использования. Следы использования

программных средств обхода защиты программных продуктов от несанкционированного

использования в ОС семейства Windows. Типовые вопросы, разрешаемые экспертом при производстве СКТЭ, связанные с исследованием программных продуктов, содержащих признаки их контрафактного использования.

### **Модульная единица 1.3. Процессуальные особенности исследования ОС семейства WINDOWS**

Снятие ограничений доступа к информации об ОС семейства WINDOWS. Особенности определения соответствия системного времени ПК с реальным временем часового пояса. Методика контрольной установки программных продуктов, содержащих следы обхода защиты от несанкционированного использования. Методика извлечения энергозависимых данных с компьютера под управлением ОС семейства Windows.

### **Модульная единица 1.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства WINDOWS и ее криминалистическая значимость**

Общие принципы следообразования в служебных каталогах ОС семейства WINDOWS. Философия документирования информации о состоянии систем и доступность такой информации. Служебная информация в каталогах Users, Recent, History, Application data, Prefetch. Файлы журналов ОС и программ. Файлы инициализации. Файлы системного реестра. Методика снятия ограничений доступа на исследование информации в профиле пользователя ОС семейства Windows.

### **Модульная единица 1.5. Информация, содержащаяся в системном реестре ОС семейства WINDOWS и ее криминалистическая значимость**

Назначение и криминалистическая значимость наиболее характерных ветвей и ключей системного реестра ОС семейства Windows. Методика исследования не активного реестра ОС семейства Windows.

## **Модуль 2. Операционные системы семейства Unix**

### **Модульная единица 2.1. Основные понятия об ОС Unix**

Краткая история развития и многообразие ОС Unix. Дистрибутивы и установка ОС Unix. Консольные оболочки и консольные команды. Основные положения модели безопасности ОС Unix.

## **Модульная единица 2.2. Методические подходы предварительного исследования ОС семейства Unix на месте происшествия**

Подготовка накопителя информации для создания образа исследуемой системы. Документирование действий на МП. Сбор сведений идентифицирующих систему пользователя. Исследование энергозависимой информации. Создание образа энергонезависимых данных. Загрузочные дистрибутивы для исследования \*nix систем.

## **Модульная единица 2.3. Журналы регистрации событий в ОС семейства Unix**

Классификация журналов регистрации событий. «Глобальный системный журнал». Журналы менеджера пакетов. Бинарные журналы учета пользовательских сессий.

## **Модульная единица 2.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства Unix и ее криминалистическая значимость**

Стандартная структура каталогов ОС семейства Unix и их криминалистическое значение. Служебные файлы, обладающие криминалистически-значимой информацией.

## **Модульная единица 2.5. Особенности исследования ОС семейства Mac OS X**

Общие принципы построения программно-аппаратных комплексов корпорации Apple. Файловые системы MacOS. Особенности использования программы Boot Camp. Ветви ресурсов и файлы ресурсов. Файлы программ в ОС семейства Mac OS X

### **4.3. Лекционные / лабораторные/ практические/ семинарские занятия**

Таблица 4

#### **Содержание лекционного курса**

<b>№ модуля и модульной единицы дисциплины</b>	<b>№ и тема лекции</b>	<b>Вид контрольного мероприятия</b>	<b>Кол-во часов</b>
<b>Модуль 1. Операционные системы семейства WINDOWS</b>			<b>14</b>
Модульная единица 1.1. Исследование информации, идентифицирующей установленные операционные системы семейства WINDOWS и программные продукты в ОС.	Лекция №1-2 Исследование информации, идентифицирующей установленные операционные системы семейства WINDOWS и программные продукты в ОС.		4
Модульная единица 1.2. Защита программных продуктов от несанкционированного использования	Лекция №3-4 Защита программных продуктов от несанкционированного использования		4
Модульная единица 1.3. Процессуальные особенности исследования ОС семейства WINDOWS	Лекция №5 Процессуальные особенности исследования ОС семейства WINDOWS		2
Модульная единица 1.4. Информация, содержащаяся в	Лекция №6 Информация, содержащаяся в служебных		2

№ модуля и модульной единицы дисциплины	№ и тема лекции	Вид контрольного мероприятия	Кол-во часов
служебных каталогах и файлах ОС семейства WINDOWS и ее криминалистическая значимость	каталогах и файлах ОС семейства WINDOWS и ее криминалистическая значимость		
Модульная единица 1.5. Информация, содержащаяся в системном реестре ОС семейства WINDOWS и ее криминалистическая значимость	Лекция №7 Информация, содержащаяся в системном реестре ОС семейства WINDOWS и ее криминалистическая значимость		2
<b>Модуль 2. Операционные системы семейства Unix</b>			<b>14</b>
Модульная единица 2.1. Основные понятия об ОС Unix	Лекция №8-9 Основные понятия об ОС Unix		4
Модульная единица 2.2. Методические подходы предварительного исследования ОС семейства Unix на месте происшествия	Лекция №10-11 Методические подходы предварительного исследования ОС семейства Unix на месте происшествия		4
Модульная единица 2.3. Журналы регистрации событий в ОС семейства Unix	Лекция №12 Журналы регистрации событий в ОС семейства Unix		2
Модульная единица 2.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства Unix и ее криминалистическая значимость	Лекция №13 Информация, содержащаяся в служебных каталогах и файлах ОС семейства Unix и ее криминалистическая значимость		2
Модульная единица 2.5. Особенности исследования ОС семейства Mac OS X	Лекция №14 Особенности исследования ОС семейства Mac OS X		2
<b>ИТОГО</b>			<b>28</b>

### Лабораторные/практические/семинарские занятия

Таблица 5

### Содержание занятий и контрольных мероприятий

№ модуля и модульной единицы дисциплины	№ и название лабораторных/практических занятий с	Вид контрольного мероприятия	Кол-во часов
---	--	------------------------------	--------------

	указанием контрольных мероприятий		
<b>Модуль 1. Операционные системы семейства WINDOWS</b>			<b>14</b>
Модульная единица 1.1. Исследование информации, идентифицирующей установленные операционные системы семейства WINDOWS и программные продукты в ОС.	Практическое занятие №1-2 Информация, идентифицирующая программные продукты корпорации Microsoft. Методика получения идентификационной информации о программных продуктах, установленных в ОС семейства Windows.	Устный опрос	4
Модульная единица 1.2. Защита программных продуктов от несанкционированного использования	Практическое занятие №3-4 Типы лицензий программных продуктов корпорации Microsoft. Система активации в ОС семейства Windows. Программные и аппаратные средства защиты программных продуктов от несанкционированного использования. Основные способы обхода защиты программных продуктов от несанкционированного использования.	Устный опрос	4
Модульная единица 1.3. Процессуальные особенности исследования ОС семейства WINDOWS	Практическое занятие №5 Снятие ограничений доступа к информации об ОС семейства WINDOWS. Особенности определения соответствия системного времени ПК с реальным временем часового пояса.	Устный опрос	2
Модульная единица 1.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства WINDOWS и ее криминалистическая значимость	Практическое занятие №6 Общие принципы следообразования в служебных каталогах ОС семейства WINDOWS. Философия документирования информации о состоянии систем и доступность такой информации.	Устный опрос	2
Модульная единица 1.5. Информация, содержащаяся в системном реестре ОС семейства WINDOWS и ее криминалистическая значимость	Практическое занятие №7 Назначение и криминалистическая значимость наиболее характерных ветвей и ключей системного реестра ОС семейства Windows. Методика исследования не активного реестра ОС семейства Windows.	Устный опрос Коллоквиум Тестирование LMS Moodle	2
<b>Модуль 2. Операционные системы семейства Unix</b>			<b>14</b>
Модульная единица 2.1. Основные понятия об ОС Unix	Практическое занятие №8-9 Краткая история развития и многообразие ОС Unix. Дистрибутивы и установка ОС Unix. Консольные оболочки и консольные команды. Основные положения модели безопасности ОС Unix.	Устный опрос	4
Модульная единица 2.2. Методические подходы предварительного исследования ОС семейства Unix на месте происшествия	Практическое занятие №10-11 Подготовка накопителя информации для создания образа исследуемой системы. Документирование действий на МП. Сбор сведений идентифицирующих систему пользователя.	Устный опрос	4
Модульная единица 2.3. Журналы регистрации событий в ОС семейства Unix	Практическое занятие №12 Классификация журналов регистрации событий. «Глобальный системный журнал». Журналы менеджера пакетов. Бинарные журналы учета пользовательских сессий.	Устный опрос	2
Модульная единица 2.4. Информация, содержащаяся в служебных каталогах и	Практическое занятие №13 Стандартная структура каталогов ОС семейства Unix и их криминалистическое значение. Служебные файлы, обладающие	Устный опрос	2

№ модуля и модульной единицы дисциплины	№ и название лабораторных/ практических занятий с указанием контрольных мероприятий	Вид контрольного мероприятия	Кол-во часов
файлах ОС семейства Unix и ее криминалистическая значимость	криминалистически-значимой информацией.		
Модульная единица 2.5. Особенности исследования ОС семейства Mac OS X	Практическое занятие №14 Общие принципы построения программно-аппаратных комплексов корпорации Apple. Файловые системы MacOS. Особенности использования программы Boot Camp. Ветви ресурсов и файлы ресурсов. Файлы программ в ОС семейства Mac OS X.	Устный опрос Коллоквиум Тестирование LMS Moodle	2
<b>ИТОГО</b>			<b>28</b>

#### 4.4. Самостоятельное изучение разделов дисциплины и виды самоподготовки к текущему контролю знаний

Самостоятельная работа студентов (СРС) организуется с целью развития навыков работы с учебной и научной литературой, выработки способности вести научно-исследовательскую работу, а также для систематического изучения дисциплины. При изучении данной дисциплины, самостоятельная работа организована в следующих формах:

- подготовка к коллоквиуму (перечень вопросов приведен в п.5.2. ФОС по данной дисциплине);
- подготовка к тестированию на платформе LMS Moodle (перечень вопросов представлен в п.4.2. настоящей рабочей программы, примерные тестовые задания приведены в п. 5.2. ФОС по данной дисциплине);
- самостоятельное изучение тем и разделов дисциплины (перечень тем и разделов приведен в Таблице №6 настоящей рабочей программы).

##### 4.4.1. Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний

Таблица 6

#### Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний

№ модуля и модульной единицы дисциплины	Перечень рассматриваемых вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний	Кол-во часов
<b>Модуль 1. Операционные системы семейства WINDOWS</b>		<b>26</b>
Модульная единица 1.1. Исследование информации, идентифицирующей установленные операционные	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Криминалистическая значимость служебной информации в программной среде под управлением ОС семейства Windows.	6

№ модуля и модульной единицы дисциплины	Перечень рассматриваемых вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний	Кол-во часов
системы семейства WINDOWS и программные продукты в ОС.		
Модульная единица 1.2. Защита программных продуктов от несанкционированного использования	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Типовые вопросы, разрешаемые экспертом при производстве СКТЭ, связанные с исследованием программных продуктов, содержащих признаки их контрафактного использования.	6
Модульная единица 1.3. Процессуальные особенности исследования ОС семейства WINDOWS	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Методика извлечения энергозависимых данных с компьютера под управлением ОС семейства Windows.	6
Модульная единица 1.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства WINDOWS и ее криминалистическая значимость	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Файлы журналов ОС и программ. Файлы инициализации. Файлы системного реестра. Методика снятия ограничений доступа на исследование информации в профиле пользователя ОС семейства Windows.	4
Модульная единица 1.5. Информация, содержащаяся в системном реестре ОС семейства WINDOWS и ее криминалистическая значимость	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Назначение и криминалистическая значимость наиболее характерных ветвей и ключей системного реестра ОС семейства Windows. Методика исследования не активного реестра ОС семейства Windows.	4
<b>Модуль 2. Операционные системы семейства Unix</b>		<b>26</b>
Модульная единица 2.1. Основные понятия об ОС Unix	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Краткая история развития и многообразие ОС Unix. Дистрибутивы и установка ОС Unix. Консольные оболочки и консольные команды. Основные положения модели безопасности ОС Unix.	6
Модульная единица 2.2. Методические подходы предварительного исследования ОС семейства Unix на месте происшествия	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Исследование энергозависимой информации. Создание образа энергонезависимых данных. Загрузочные дистрибутивы для исследования *nix систем.	6
Модульная единица 2.3. Журналы регистрации событий в ОС семейства Unix	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Классификация журналов регистрации событий. «Глобальный системный журнал». Журналы менеджера пакетов. Бинарные журналы учета пользовательских сессий.	6
Модульная единица 2.4. Информация, содержащаяся в служебных каталогах и файлах ОС семейства Unix и ее криминалистическая значимость	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Стандартная структура каталогов ОС семейства Unix и их криминалистическое значение. Служебные файлы, обладающие криминалистически-значимой информацией.	4
Модульная единица 2.5. Особенности исследования ОС	1. Подготовится к коллоквиуму и тестированию (вопросы указаны в ФОС и в LMS Moodle). 2. Самостоятельно изучить следующие вопросы: Общие принципы построения программно-аппаратных	4

№ модуля и модульной единицы дисциплины	Перечень рассматриваемых вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний	Кол-во часов
семейства Mac OS X	комплексов корпорации Apple. Файловые системы MacOS. Особенности использования программы Boot Camp. Ветви ресурсов и файлы ресурсов. Файлы программ в ОС семейства Mac OS X.	
<b>ИТОГО</b>		<b>52</b>

#### 4.4.2. Курсовые проекты (работы)/ контрольные работы/ расчетно-графические работы

Не предусмотрены учебным планом

### 5. Взаимосвязь видов учебных занятий

Таблица 7

#### Взаимосвязь компетенций с учебным материалом и контролем знаний студентов

Компетенции	Лекции	ЛЗ/ ПЗ/С	СРС	Другие виды	Вид контроля
ПК-3. Способен применять методики инженерно-технических экспертиз и исследований в профессиональной деятельности	Модуль 1, 2	Модуль 1, 2	Модуль 1, 2		коллоквиум, тестирование в LMS Moodle по итогам изучения дисциплинарных модулей, зачет с оценкой в 9 семестре
ПК-5 Способность консультировать субъектов правоприменительной деятельности по вопросам назначения и производства инженерно-технических экспертиз при расследовании преступлений и иных правонарушений	Модуль 1, 2	Модуль 1, 2	Модуль 1, 2		коллоквиум, тестирование в LMS Moodle по итогам изучения дисциплинарных модулей, зачет с оценкой в 9 семестре

### 6. Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Сорокотягин, И. Н. Судебная экспертиза: учебник и практикум для вузов / И. Н. Сорокотягин, Д. А. Сорокотягина. — Москва : Издательство Юрайт, 2021. — 288 с. — (Высшее образование). — ISBN 978-5-534-05399-9. — Текст :

- электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/469229>
2. Судебные экспертизы в уголовном процессе : учебное пособие для вузов / Н. Н. Ильин [и др.]; ответственный редактор Н. Н. Ильин. — Москва : Издательство Юрайт, 2022. — 212 с. — (Высшее образование). — ISBN 978-5-534-14303-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519807>
  3. Криминалистика в 5 т. Том 2. Методология криминалистики и криминалистический анализ : учебник для вузов / И. В. Александров, В. Я. Колдин, О. А. Крестовников, С. А. Смирнова ; под общей редакцией И. В. Александрова ; ответственный редактор В. Я. Колдин. — Москва : Издательство Юрайт, 2022. — 167 с. — (Высшее образование). — ISBN 978-5-534-08439-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/474674>
  4. Криминалистика в 5 т. Том 3. Криминалистическая техника : учебник для вузов / И. В. Александров [и др.]; под общей редакцией И. В. Александрова ; ответственный редактор Н. Н. Егоров. — Москва : Издательство Юрайт, 2020. — 216 с. — (Высшее образование). — ISBN 978-5-534-08834-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/455740>
  5. Гостев, И. М. Операционные системы : учебник и практикум для вузов / И. М. Гостев. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 164 с. — (Высшее образование). — ISBN 978-5-534-04520-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/470010>

### **6.1. Карта обеспеченности литературой**

### **6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»)**

У обучающихся и преподавателей имеется индивидуальный неограниченный доступ к нескольким ЭБ (ЭБ «Web-Ирбис64+ Электронная библиотека», ЭБС «AgriLib», ЭБС «Лань», ЭБС «Юрайт», ИБС «Статистика», НЭБ «Национальная электронная библиотека», НЭБ «eLIBRARY.RU» и др.), электронной информационно-образовательной среде (LMS Moodle, сайт <http://e.kgau.ru/>), СПС «Консультант плюс», иным информационным Интернет-ресурсам (<https://sudact.ru/>, <https://sudrf.ru/> и др.) из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее.

### **6.3. Программное обеспечение**

#### **Наименование программного обеспечения и его назначение**

Windows Vista Business Russian Upgrade OpenLicense Академическая лицензия №44937729 от 15.12.2008;
--

Лицензия Windows Vista Starter 32-bit Russian Академическая лицензия №44937729 от 15.12.2008;
Microsoft Windows Server CAL 2008 Russian Academic OPEN; Академическая лицензия №44937729 от 15.12.2008
Office 2007 Russian OpenLicensePack Академическая лицензия №44937729 от 15.12.2008;
ABBYY FineReader 10 Corporate Edition 30 Лицензия сертификат №FCRC-1100-1002-2465-8755-4238 22.02.2012;
Программная система для обнаружения текстовых заимствований в учебных и научных работах - Лицензионный договор №158 от 03.04.2019 «Антиплагиат ВУЗ»;
Moodle 3.5.6a (система дистанционного образования) - Бесплатно распространяемое ПО;
Библиотечная система «Ирбис 64» (web версия) - Договор сотрудничества.
Офисный пакет Libre Office 6.2.1 - Бесплатно распространяемое ПО;
Яндекс (Браузер / Диск) - Бесплатно распространяемое ПО;
Справочная правовая система «Консультант+» - Договор сотрудничества №20175200206 от 01.06.2016;
Справочная правовая система «Гарант» - Учебная лицензия;
Информационно-аналитическая система «Статистика» <a href="http://www.ias-stat.ru">www.ias-stat.ru</a>
Информационно-аналитическая система Росстат <a href="https://rosstat.gov.ru">https://rosstat.gov.ru</a>

## 7. Критерии оценки знаний, умений, навыков и заявленных компетенций

**Виды текущего контроля:** устный опрос.

**Виды промежуточного контроля:** коллоквиумы и тестирование в LMS Moodle по итогам изучения дисциплинарных модулей.

**Виды промежуточной аттестации:** зачет с оценкой (9 семестр) в форме собеседования по предложенным вопросам.

**Таблица 9**

Рейтинг-план по модулям (9-й семестр)**				
Виды контроля	Дисциплинарный модуль 1 (ДМ1) (от 0 до 30 баллов)	Дисциплинарный модуль 2 (ДМ2) (от 0 до 30 баллов)	Промежуточная аттестация (зачет с оценкой)	Итого баллов

	Кол-во баллов по итогам текущего контроля (МЕ 1.1-1.5)					Промежуточный контроль (М.Е. 1.1-1.5)	Кол-во баллов по итогам текущего контроля (МЕ 2.1-2.5)					Промежуточный контроль (М.Е. 2.1-2.5)		
	1.1	1.2	1.3	1.4	1.5		2.1	2.2	2.3	2.4	2.5			
Устный опрос	0-2	0-2	0-2	0-2	0-2		0-2	0-2	0-2	0-2	0-2			0-20
Тестирование в LMS Moodle						0-15						0-15		0-30
Коллоквиум						0-5						0-5		0-10
Итоговое собеседование (зачет с оценкой)													0-40	0-40
Итого баллов	0-2	0-2	0-2	0-2	0-2	0-20	0-2	0-2	0-2	0-2	0-2	0-20	0-40	0-100

\*\* Критерии оценивания по видам контроля успеваемости обучающихся в процессе изучения дисциплины имеются в Фонде оценочных средств дисциплины и в LMS Moodle.

## 8. Материально-техническое обеспечение дисциплины

В рамках освоения дисциплины «Криминалистическое исследование операционных систем в инженерно-технических экспертизах», обучающимся предоставляется возможность пользования аудиторным фондом: лекционные залы, Учебная аудитория 4-07 (компьютерный класс) Учебная аудитория 4-16 (Инженерно-технический криминалистический полигон), библиотека юридического института, помещения для самостоятельной работы. Библиотека юридического института располагает учебно-методической, научной и справочной литературой по данной дисциплине. Помещение для самостоятельной работы и практических занятий оборудовано компьютеризированными рабочими местами с доступом к сети Интернет и справочно-правовым электронным базам локальной сети вуза. Лекционные залы и аудитории для практических занятий оборудованы современным мультимедийным оборудованием.

Таблица 10

<p align="center"><b>Наименование специальных* помещений и помещений для самостоятельной работы</b></p>	<p align="center"><b>Оснащенность специальных помещений и помещений для самостоятельной работы</b></p>	<p align="center"><b>Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа</b></p>
<p><b>Учебная аудитория 5-05</b> для проведения лекционных занятий, практических (семинарских) занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации г. Красноярск, Ленина, 117</p>	<p>Общая площадь 40,6 кв.м. Посадочных мест – 46. Рабочее место преподавателя, комплект специализированной мебели, доска магнитно-маркерная 90*180см INFILD инв.№ 2101060728, кафедра напольная инв. № 21026211, комплект стационарного мультимедийного оборудования инв. № 4342019079 (системный блок, монитор, экран, проектор), общая локальная компьютерная сеть Интернет.</p>	<p>Windows Vista Business Russian Upgrade OpenLicense Академическая лицензия №44937729 от 15.12.2008; Лицензия Windows Vista Starter 32-bit Russian Академическая лицензия №44937729 от 15.12.2008; Microsoft Windows Server CAL 2008 Russian Academic OPEN; Академическая лицензия №44937729 от 15.12.2008 Office 2007 Russian OpenLicensePack Академическая лицензия №44937729 от 15.12.2008; ABBYY FineReader 10 Corporate Edition 30 Лицензия сертификат №FCRC- 1100-1002-2465-8755-4238 22.02.2012; Программная система для обнаружения текстовых заимствований в учебных и научных работах - Лицензионный договор №158 от 03.04.2019 «Антиплагиат ВУЗ»; Moodle 3.5.6a (система дистанционного образования) - Бесплатно распространяемое ПО; Библиотечная система «Ирбис 64» (web версия) - Договор сотрудничества. Офисный пакет Libre Office 6.2.1 - Бесплатно распространяемое ПО; Яндекс (Браузер / Диск) - Бесплатно распространяемое ПО; Справочная правовая система «Консультант+» - Договор сотрудничества №20175200206 от 01.06.2016; Справочная правовая система «Гарант» - Учебная лицензия; Информационно-аналитическая система «Статистика» www.ias-stat.ru Информационно-аналитическая система Росстат <a href="https://rosstat.gov.ru">https://rosstat.gov.ru</a></p>
<p><b>Учебная аудитория 4-16 (Инженерно-технический криминалистический полигон)</b> для проведения занятий</p>	<p>Общая площадь – 38,9 кв.м. Посадочных мест –30. Рабочее место преподавателя, комплект специализированной мебели, наглядные пособия; камеры видеонаблюдения 2 шт., цифровой видеорегистратор, комплект приспособлений и устройств для изъятия</p>	

<p>семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций</p> <p>г. Красноярск, Ленина, 117</p>	<p>компьютерной информации и работы с ней, комплект элементов "умного дома" Xiaomi Smart Home, Системный блок - инв. № 1360945; Системный блок - инв. № 11014430; Системный блок - инв. № 11014541, Принтер - инв. № 1360211; Системный блок - инв. № 1101040597, Монитор - инв. № 1101040597; Автоматизированное рабочее место ТИП2 - инв. № № 4342019036 - 4342019045;</p> <p>АРМ (MSI H310 PRO, Pentium G5400, мони-тор Benq BL2480, мышка + клавиатура) - инв. № № 4342019152 - 4342019156; комплект мультимедийного оборудования: экран переносной, проектор переносной, акустические колонки переносные, ноутбук переносной, общая локальная компьютерная сеть Интернет.</p>	
---	--	--

## 9. Методические указания для обучающихся по освоению дисциплины

### 9.1. Методические указания по дисциплине для обучающихся

В процессе изучения дисциплины «Криминалистическое исследование операционных систем в инженерно-технических экспертизах» обучающимся настоятельно рекомендуется посещение всех лекционных занятий в соответствии с тематическим планом, т.к. материал, в имеющихся учебных пособиях, не предлагает в полном объеме ответы на рассматриваемые вопросы.

#### Подготовка к лекциям

В ходе лекционных занятий необходимо вести конспектирование учебного материала, обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Необходимо задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Целесообразно дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой.

#### Подготовка к практическим занятиям

Подготовка к практическому занятию включает два этапа. На первом этапе обучающийся планирует свою самостоятельную работу, которая включает: уяснение задания на самостоятельную работу; подбор рекомендованной литературы; составление плана работы, в котором определяются основные пункты предстоящей подготовки. Составление плана дисциплинирует и повышает организованность в работе. Второй этап включает Вашу непосредственную подготовку к занятию. Начинать надо с изучения рекомендованной литературы. Вам необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его часть. Остальная его часть восполняется в процессе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. Особое внимание при этом необходимо обратить на содержание основных положений и выводов, объяснение явлений и фактов, уяснение практического материала по рассматриваемым вопросам. Отдельно стоит отметить, что при подготовке к

практическому занятию каждому обучающемуся нужно обязательно ознакомиться с Фондом оценочных средств и другими учебными материалами, размещенными в LMS Moodle по конкретной модульной единице (-цам). Также можно обращаться за помощью к преподавателю. Перед консультацией, необходимо хорошо продумать вопросы, которые требуют разъяснения.

#### **Подготовка к самостоятельному изучению вопросов**

Самостоятельная работа обучающегося над усвоением учебного материала по учебной дисциплине может выполняться в библиотеке университета, учебных кабинетах, компьютерных классах, а также в домашних условиях. Содержание самостоятельной работы обучающегося определяется рабочей программой дисциплины, методическими материалами, заданиями и указаниями преподавателя. Вы можете дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при подготовке к практическим занятиям.

## **9.2. Методические указания по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья**

В целях освоения учебной программы дисциплины инвалидами и лицами с ограниченными возможностями здоровья в учреждении обеспечивается:

1. Для инвалидов и лиц с ограниченными возможностями здоровья по зрению:
  - 1.1. размещение в доступных для обучающихся местах и в адаптированной форме справочной информации о расписании учебных занятий;
  - 1.2. присутствие ассистента, оказывающего обучающемуся необходимую помощь;
  - 1.3. выпуск альтернативных форматов методических материалов (презентации с крупным шрифтом, аудиофайлы);
2. Для инвалидов и лиц с ограниченными возможностями здоровья по слуху:
  - 2.1. оборудовано надлежащими звуковыми средствами воспроизведение информации;
3. Для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:
  - 3.1. реализована возможность беспрепятственного доступа обучающихся в учебные помещения, туалетные комнаты и другие помещения института, а также пребывание в указанных помещениях.

Образование обучающихся с ограниченными возможностями здоровья организовано совместно с другими обучающимися. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине представлен в настоящей рабочей программе и ФОС к ней. Данные документы размещены в электронном виде в LMS Moodle и адаптивны для изучения посредством возможностей программного обеспечения по проговариванию текста и его зуммированию.

## ПРОТОКОЛ ИЗМЕНЕНИЙ РПД

<b>Дата</b>	<b>Раздел</b>	<b>Изменения</b>	<b>Комментарии</b>