Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Ростовский государственный экономический университет (РИНХ)»

УТВЕРЖДАЮ
Директор Института магистратуры
_____ Иванова Е.А.
«_29_» __августа__ 2022_г.

Рабочая программа дисциплины
Основы компьютерной криминалистики

Направление 10.04.01 Информационная безопасность
магистерская программа 10.04.01.02 "Программно-аппаратные методы расследования компьютерных преступлений"

Для набора 2022 года

Квалификация
магистр

КАФЕДРА **Судебная экспертиза и криминалистика**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
Недель	15 2/6			
Вид занятий	УП	РП	УП	РП
Лекции	14	14	14	14
Практические	22	22	22	22
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	68	68	68	68
Часы на контроль	4	4	4	4
Итого	108	108	108	108

ОСНОВАНИЕ

Учебный план утвержден учёным советом вуза от 22.02.2022 протокол № 7.

Программу составил(и): к.ю.н., доц., Гайбарян О.М.

Зав. кафедрой: к.ю.н., доц. Николаев А.В.

Методическим советом направления: д.э.н., проф., Тищенко Е.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1	Выработать у обучающихся систему знаний, умений и навыков по применению методов исследования и использованию технических средств в раскрытии и расследовании компьютерных преступлений; получение теоретических знаний и практических навыков эффективного применения технико-криминалистических средств и методов при выполнении судебно-компьютерных экспертиз.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-4:Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;

В результате освоения дисциплины обучающийся должен:

Знать:

- порядок планирования своей работы и составления отчетов о выполнении таких планов (соотнесено с индикатором ОПК- 4);
- порядок поиска, обработки и анализа научно-технической информации (соотнесено с индикатором ОПК-4).

Уметь:

- составлять план проведения научных исследований (соотнесено с индикатором ОПК-4);
- вести сбор и систематизацию научно-технической информации (соотнесено с индикатором ОПК-4).

Владеть:

- навыками составления плана своей работы и отчета о его выполнении (соотнесено с индикатором ОПК-4);
- навыками обработки научно-технической информации (соотнесено с индикатором ОПК-4).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература
	Раздел 1. Теоретические основы криминалистики				
1.1	Тема 1.: «Введение в криминалистику. Предмет, система, задачи и функции криминалистики.» 1. Предмет криминалистики. 2. Закономерности объективной действительности, изучаемые криминалистикой. 3. Возникновение и развитие криминалистики в России. 4. Система криминалистики. 5. Общая теория и частные криминалистические теории и учения, их система. 6. Методы, разрабатываемые криминалистикой. Их виды. Использование общенаучных методов в криминалистике. Специальные методы криминалистики, их система. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
1.2	Тема 1.: «Введение в криминалистику. Предмет, система, задачи и функции криминалистики.» 1. Предмет криминалистики. 2. Закономерности объективной действительности, изучаемые криминалистикой. 3. Возникновение и развитие криминалистики в России. 4. Система криминалистики. 5. Общая теория и частные криминалистические теории и учения, их система. 6. Методы, разрабатываемые криминалистикой. Их виды. Использование общенаучных методов в криминалистике. Специальные методы криминалистики, их система. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

1.3	Тема 1.: «Введение в криминалистику. Предмет, система, задачи и функции криминалистики.» Предмет криминалистики. Закономерности объективной действительности, изучаемые криминалистикой. Возникновение и развитие криминалистики в России. Система криминалистики. Общая теория и частные криминалистические теории и учения, их система. Методы, разрабатываемые криминалистикой. Их виды. Использование общенаучных методов в криминалистике. Специальные методы криминалистики, их система. /Ср/	3	6	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
1.4	Тема 2: «Криминалистическая идентификация и диагностика». 1. Понятие криминалистической идентификации, ее методологические и естественно-научные основы. 2. Содержание и задачи криминалистической идентификации. 3. Условия идентификации, субъекты и объекты криминалистической идентификации, ее виды и формы. 4. Идентификация и установление групповой принадлежности. 5. Понятие и сущность криминалистической диагностики. 6. Значение криминалистической диагностики для раскрытия и расследования преступлений. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
1.5	Тема 2: «Криминалистическая идентификация и диагностика». 1. Понятие криминалистической идентификации, ее методологические и естественно-научные основы. 2. Содержание и задачи криминалистической идентификации. 3. Условия идентификации, субъекты и объекты криминалистической идентификации, ее виды и формы. 4. Идентификация и установление групповой принадлежности. 5. Понятие и сущность криминалистической диагностики. 6. Значение криминалистической диагностики для раскрытия и расследования преступлений. Подготовка к практическим занятиям с использованием в LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
1.6	Тема 2: «Криминалистическая идентификация и диагностика». Понятие криминалистической идентификации, ее методологические и естественно-научные основы. Содержание и задачи криминалистической идентификации. Условия идентификации, субъекты и объекты криминалистической идентификации, ее виды и формы. Идентификация и установление групповой принадлежности. Понятие и сущность криминалистической диагностики. Значение криминалистической диагностики для раскрытия и расследования преступлений. /Ср/	3	6	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
1.7	Тема 3. «Криминалистическая фотография и видеозапись». 1. Понятие, назначение и правовые основы применения криминалистической фотографии и видеозаписи, научно- технические средства, приемы и методы, используемые при проведении следственных действий. 2. Устройство и классификация цифровых фотоаппаратов. 3. Особенности фотосъемки отдельных криминалистических объектов. 4. Процессуальные и технические правила оформления результатов криминалистической фотосъемки и видеозаписи. Подготовка к практическим занятиям с использованием в LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6

1.8	Тема 3. «Криминалистическая фотография и видеозапись». Понятие, назначение и правовые основы применения криминалистической фотографии и видеозаписи, научно- технические средства, приемы и методы, используемые при проведении следственных действий. Устройство и классификация цифровых фотоаппаратов. Особенности фотосъемки отдельных криминалистических объектов. Процессуальные и технические правила оформления результатов криминалистической фотосъемки и видеозаписи. /Ср/	3	6	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
1.9	Тема 4. «Криминалистическая трасология». 1. Общие положения криминалистической трасологии как отрасли криминалистической техники. 2. Следы орудий взлома и инструментов,транспортных средств, следов обуви. 3. Криминалистическое исследование запирающих устройств, пломб и запорно- пломбировочных устройств. 4. Понятие и криминалистическое значение следов-предметов и следов – веществ. Подготовка к практическим занятиям с использованием в LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
1.10	Тема 4. «Криминалистическая трасология». Общие положения криминалистической трасологии как отрасли криминалистической техники. Следы орудий взлома и инструментов,транспортных средств, следов обуви. Криминалистическое исследование запирающих устройств, пломб и запорно- пломбировочных устройств. Понятие и криминалистическое значение следов-предметов и следов – веществ. /Ср/	3	6	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
	Раздел 2. Теоретические и организационные основы использования специальных знаний в процессе судопроизводства по делам, сопряженным с применением компьютерных средств				
2.1	Тема 5: «Проблемы противоправного оборота компьютерных систем». 1. Современное состояние проблемы борьбы с преступностью в сфере информационных технологий. 2. Особенности квалификации преступлений и административных правонарушений, сопряженных с применением компьютерных средств. 3. Особенности гражданско-правовых споров, связанных с оборотом компьютерных систем. 4. Формы использования специальных знаний в уголовном и гражданском судопроизводстве по делам, сопряженным с использованием компьютерных систем. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
2.2	Тема 5: «Проблемы противоправного оборота компьютерных систем». 1. Современное состояние проблемы борьбы с преступностью в сфере информационных технологий. 2. Особенности квалификации преступлений и административных правонарушений, сопряженных с применением компьютерных средств. 3. Особенности гражданско-правовых споров, связанных с оборотом компьютерных систем. 4. Формы использования специальных знаний в уголовном и гражданском судопроизводстве по делам, сопряженным с использованием компьютерных систем. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6

2.3	Тема 5: «Проблемы противоправного оборота компьютерных систем». 1. Современное состояние проблемы борьбы с преступностью в сфере информационных технологий. 2. Особенности квалификации преступлений и административных правонарушений, сопряженных с применением компьютерных средств. 3. Особенности гражданско-правовых споров, связанных с оборотом компьютерных систем. 4. Формы использования специальных знаний в уголовном и гражданском судопроизводстве по делам, сопряженным с использованием компьютерных систем. /Ср/	3	6	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
2.4	Тема 6: «Применение специальных знаний при производстве следственных и судебных действий по делам, сопряженным с использованием компьютерных средств». 1. Собирание доказательств по делам,сопряженным с использованием компьютерных средств. 2. Особенности обнаружения, фиксации и изъятия криминалистически значимой информации в вычислительной сети. 3. Требования по изъятию, транспортировке и хранению компьютерных средств. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
2.5	Тема 6: «Применение специальных знаний при производстве следственных и судебных действий по делам, сопряженным с использованием компьютерных средств». 1. Собирание доказательств по делам,сопряженным с использованием компьютерных средств. 2. Особенности обнаружения, фиксации и изъятия криминалистически значимой информации в вычислительной сети. 3. Требования по изъятию, транспортировке и хранению компьютерных средств. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7
2.6	Тема 6: «Применение специальных знаний при производстве следственных и судебных действий по делам, сопряженным с использованием компьютерных средств». 1. Собирание доказательств по делам,сопряженным с использованием компьютерных средств. 2. Особенности обнаружения, фиксации и изъятия криминалистически значимой информации в вычислительной сети. 3. Требования по изъятию, транспортировке и хранению компьютерных средств. /Ср/	3	6	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
2.7	Тема 7: «Предмет, задачи и объекты судебно-компьютерной экспертизы». 1. Предмет и цели судебно-компьютерной экспертизы. 2. Классификация судебно-компьютерной экспертизы. 3. Задачи судебно-компьютерной экспертизы. 4. Понятие объекта судебно-компьютерной экспертизы. Классификация объектов. 5. Общие представления о компьютерных средствах как объектах судебно-компьютерной экспертизы. 6. Комплексный характер СКЭ и ее связь с другими родами и видами судебных экспертиз. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7

2.8	Тема 7: «Предмет, задачи и объекты судебно-компьютерной экспертизы». 1. Предмет и цели судебно-компьютерной экспертизы. 2. Классификация судебно-компьютерной экспертизы. 3. Задачи судебно-компьютерной экспертизы. 4. Понятие объекта судебно-компьютерной экспертизы. Классификация объектов. 5. Общие представления о компьютерных средствах как объектах судебно-компьютерной экспертизы. 6. Комплексный характер СКЭ и ее связь с другими родами и видами судебных экспертиз. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
2.9	Тема 7: «Предмет, задачи и объекты судебно-компьютерной экспертизы». 1. Предмет и цели судебно-компьютерной экспертизы. 2. Классификация судебно-компьютерной экспертизы. 3. Задачи судебно-компьютерной экспертизы. 4. Понятие объекта судебно-компьютерной экспертизы. Классификация объектов. 5. Общие представления о компьютерных средствах как объектах судебно-компьютерной экспертизы. 6. Комплексный характер СКЭ и ее связь с другими родами и видами судебных экспертиз. /Ср/	3	8	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
2.10	Тема 8: «Назначение и производство судебно-компьютерной экспертизы». 1. Особенности назначения судебно-компьютерной экспертизы и подготовки объектов на экспертизу. 2. Типичные следственные ситуации и экспертные пути их разрешения. 3. Производство судебно- компьютерной экспертизы. 4. Судебно-компьютерная экспертиза в суде. Допрос эксперта. 5. Оценка заключения судебно-компьютерной экспертизы следователем и судом. 6 Компетенция эксперта и формы подготовки экспертов СКЭ. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6
2.11	Тема 8: «Назначение и производство судебно-компьютерной экспертизы». 1. Особенности назначения судебно-компьютерной экспертизы и подготовки объектов на экспертизу. 2. Типичные следственные ситуации и экспертные пути их разрешения. 3. Производство судебно- компьютерной экспертизы. 4. Судебно-компьютерная экспертиза в суде. Допрос эксперта. 5. Оценка заключения судебно-компьютерной экспертизы следователем и судом. 6 Компетенция эксперта и формы подготовки экспертов СКЭ. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	4	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
2.12	Тема 8: «Назначение и производство судебно-компьютерной экспертизы». 1. Особенности назначения судебно-компьютерной экспертизы и подготовки объектов на экспертизу. 2. Типичные следственные ситуации и экспертные пути их разрешения. 3. Производство судебно- компьютерной экспертизы. 4. Судебно-компьютерная экспертиза в суде. Допрос эксперта. 5. Оценка заключения судебно-компьютерной экспертизы следователем и судом. 6 Компетенция эксперта и формы подготовки экспертов СКЭ. /Ср/	3	8	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
	Раздел 3. Методические основы судебной компьютерно-технической экспертизы				

3.1	Тема 9: «Система экспертных методов и средств судебно-компьютерной экспертизы». 1. Требования, предъявляемые к методам и средствам судебно-компьютерной экспертизы. 2. Методы диалектической и формальной логики, применяемые при производстве судебно-компьютерной экспертизы. 3. Общенаучные методы, применяемые в судебно-компьютерной экспертизе. 4. Специальные методы решения экспертных задач СКЭ. 5. Экспертные средства СКЭ. Демонстрация презентаций в LibreOffice. /Лек/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
3.2	Тема 9: «Система экспертных методов и средств судебно-компьютерной экспертизы». 1. Требования, предъявляемые к методам и средствам судебно-компьютерной экспертизы. 2. Методы диалектической и формальной логики, применяемые при производстве судебно-компьютерной экспертизы. 3. Общенаучные методы, применяемые в судебно-компьютерной экспертизе. 4. Специальные методы решения экспертных задач СКЭ. 5. Экспертные средства СКЭ. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
3.3	Тема 9: «Система экспертных методов и средств судебно-компьютерной экспертизы». 1. Требования, предъявляемые к методам и средствам судебно-компьютерной экспертизы. 2. Методы диалектической и формальной логики, применяемые при производстве судебно-компьютерной экспертизы. 3. Общенаучные методы, применяемые в судебно-компьютерной экспертизе. 4. Специальные методы решения экспертных задач СКЭ. 5. Экспертные средства СКЭ. /Ср/	3	8	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6
3.4	Тема 10: «Методы и средства решения родовых и видовых задач судебно-компьютерной экспертизы». 1. Диагностические и идентификационные задачи СКЭ с позиции экспертного исследования. 2. Характеристика современных интерфейсов и накопителей данных персональных компьютеров как диагностируемых объектов СКЭ. 3. Совокупность признаков, характеризующих объекты судебно- компьютерной экспертизы. 4. Общая последовательность действий эксперта по изучению объектов СКЭ. 5. Методические особенности производства судебно экспертного исследования информационно-программной продукции на признаки контрафактности. 6. Особенности судебно-экспертного исследования компьютерной информации, сопряженной с работой в сети Интернет. Подготовка к практическим занятиям с использованием LibreOffice. /Пр/	3	2	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6

3.5	Тема 10: «Методы и средства решения родовых и видовых задач судебно-компьютерной экспертизы». 1. Диагностические и идентификационные задачи СКЭ с позиции экспертного исследования. 2. Характеристика современных интерфейсов и накопителей данных персональных компьютеров как диагностируемых объектов СКЭ. 3. Совокупность признаков, характеризующих объекты судебно- компьютерной экспертизы. 4. Общая последовательность действий эксперта по изучению объектов СКЭ. 5. Методические особенности производства судебно экспертного исследования информационно-программной продукции на признаки контрафактности. 6. Особенности судебно-экспертного исследования компьютерной информации, сопряженной с работой в сети Интернет. /Ср/	3	8	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.4 Л2.5 Л2.6 Л2.7
3.6	/Зачёт/	3	4	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Структура и содержание фонда оценочных средств для проведения текущей и промежуточной аттестации представлены в Приложении 1 к рабочей программе дисциплины.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1		Компьютерная криминалистика: лабораторный практикум: практикум	Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2017	https://biblioclub.ru/index.php?page=book&id=466995 неограниченный доступ для зарегистрированных пользователей
Л1.2	Оливер, Ибе, Синицын, И. В.	Компьютерные сети и службы удаленного доступа	Саратов: Профобразование, 2019	http://www.iprbookshop.ru/87999.html неограниченный доступ для зарегистрированных пользователей
Л1.3	Габдрахманов, А. Ш., Миролюбов, С. Л., Хайруллова, Э. Т.	Назначение традиционных судебных видов экспертиз при расследовании преступлений: учебно-практическое пособие	Казань: Казанский юридический институт МВД России, 2020	https://www.iprbookshop.ru/108595.html неограниченный доступ для зарегистрированных пользователей
Л1.4	Колотушкин, С. М., Кузовлева, О. В., Майлис, Н. П., Моисеева, Т. Ф., Кузовлев, В. Ю., Пискунова, Е. В., Моисеевой, Т. Ф.	Основы криминалистики: учебное пособие	Москва: Российский государственный университет правосудия, 2021	https://www.iprbookshop.ru/117256.html неограниченный доступ для зарегистрированных пользователей

5.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Россинская Е. Р., Усов А. И.	Судебная компьютерно-техническая экспертиза	М.: Право и закон, 2001	50
Л2.2	Щербаков А.	Современная компьютерная безопасность. Теоретические основы. Практические аспекты: учебное пособие	Москва: Книжный мир, 2009	https://biblioclub.ru/index.php?page=book&id=89798 неограниченный доступ для зарегистрированных пользователей

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.3		Право и образование: журнал	Москва: Современный гуманитарный университет, 2018	https://biblioclub.ru/index.php?page=book&id=483901 неограниченный доступ для зарегистрированных пользователей
Л2.4	Докучаев, В. А., Кондратьев, М. Г., Крупнов, И. А., Маклачкова, В. В., Мытенков, С. С., Шведов, А. В., Докучаев, В. А.	Система обнаружения компьютерных атак «Форпост»: учебно-методическое пособие	Москва: Московский технический университет связи и информатики, 2016	http://www.iprbookshop.ru/61543.html неограниченный доступ для зарегистрированных пользователей
Л2.5	Костин, Д. В.	Практикум по выполнению лабораторных работ по дисциплине Системы обнаружения вторжений в компьютерные сети	Москва: Московский технический университет связи и информатики, 2016	http://www.iprbookshop.ru/61546.html неограниченный доступ для зарегистрированных пользователей
Л2.6	Болтава, А. Л.	Бухгалтерские компьютерные программы: практикум для обучающихся по направлению подготовки бакалавриата «экономика»	Краснодар, Саратов: Южный институт менеджмента, Ай Пи Эр Медиа, 2018	http://www.iprbookshop.ru/76918.html неограниченный доступ для зарегистрированных пользователей
Л2.7		Вестник Университета имени О.Е. Кутафина (МГЮА)	, 2014	http://www.iprbookshop.ru/63377.html неограниченный доступ для зарегистрированных пользователей

5.3 Профессиональные базы данных и информационные справочные системы

Справочно-правовая система Консультант Плюс

Справочно-правовая система Гарант

Научный центр правовой информации при Минюсте России

5.4. Перечень программного обеспечения

LibreOffice

5.5. Учебно-методические материалы для студентов с ограниченными возможностями здоровья

При необходимости по заявлению обучающегося с ограниченными возможностями здоровья учебно-методические материалы предоставляются в формах, адаптированных к ограничениям здоровья и восприятия информации. Для лиц с нарушениями зрения: в форме аудиофайла; в печатной форме увеличенным шрифтом. Для лиц с нарушениями слуха: в форме электронного документа; в печатной форме. Для лиц с нарушениями опорно-двигательного аппарата: в форме электронного документа; в печатной форме.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Помещения для проведения всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;

- персональный компьютер / ноутбук (переносной);

- проектор, экран / интерактивная доска.

7. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по освоению дисциплины представлены в Приложении 2 к рабочей программе дисциплины.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

1.1. Показатели и критерии оценивания компетенций:

ЗУН, составляющие компетенцию	Показатели оценивания	Критерии оценивания	Средства оценивания
ОПК-6: способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок			
Знать: порядок планирования своей работы и составления отчетов о выполнении таких планов; порядок поиска, обработки и анализа научно-технической информации.	Знать и объяснять порядок планирования проведения научных исследований; знать порядок работы с научно-технической информацией; подготовка материала доклада и выступление с ним на практическом занятии, с логическим обоснованием своей позиции по рассматриваемому вопросу, анализом актуальных правовых норм по данному вопросу и позиций ученых; ответ на вопросы тестового задания, основные и дополнительные вопросы по сделанному докладу, вопросы вынесенные на зачет.	Верность ответа на тестовые задания. Степень раскрытия проблемы, использование дополнительной литературы и статистических данных при подготовке доклада. Полнота и содержательность ответа на вопросы зачета.	Т-тест 1-63. Д-доклад 1-25. ВЗ – вопросы к зачету 1-19.
Уметь: составлять план проведения научных исследований; вести сбор и систематизацию научно-технической информации.	Проводить исследования компьютерных средств и информации с необходимой точностью; решение кейс-задачи, анализ проблемной ситуации и поиск ее разрешения на основе действующего законодательства о правоохранительных органах.	Решение задач, правильность выводов, их обоснование с ссылками на нормы законодательства.	КЗ – кейс-задача 1-20. ВЗ – 20-39 практическое задание к зачету 61-74.
Владеть: навыками составления плана своей работы и отчета о его выполнении; навыками обработки научно-технической информации.	Способен применять на практике знания методических основ проведения исследований криминалистически значимой информации; грамотно оформлять результаты проведенной экспертизы; решение кейс-задачи, анализ проблемной ситуации и поиск ее разрешения на основе действующего законодательства о правоохранительных органах.	Решение задач, правильность выводов, их обоснование с ссылками на нормы законодательства.	КЗ – кейс-задача 21-41. ВЗ – 40-60 практическое задание к зачету 75-60.

1.2 Шкалы оценивания:

Текущий контроль успеваемости и промежуточная аттестация осуществляется в рамках накопительной балльно-рейтинговой системы в 100-балльной шкале:

50-100 баллов (зачет)

0-49 баллов (незачет)

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Вопросы к зачету

1. Информационное пространство как объект национальной безопасности. Доктрина информационной безопасности Российской Федерации. Основные положения.
2. Понятие и сущность информации и информационных процессов.
3. Понятие и функции электронного документа и электронной цифровой подписи.
4. Классификация электронных документов и их использование в уголовном судопроизводстве.
5. Основы правового регулирования в сфере информационных технологий.
6. Факторы, угрожающие информационной безопасности. Информационная война и информационное оружие.
7. Преступления, совершаемые с использованием информационных технологий, и основные элементы их криминалистической характеристики.
8. Механизм совершения преступлений в сфере информационных технологий.
9. Способы совершения и сокрытия преступлений в сфере информационных технологий. Их классификация.
10. Методы несанкционированного доступа к компьютерной информации. Методы манипуляций компьютерной информацией.
11. Следовая информационная картина совершения преступлений в сфере информационных технологий. Классификация следов при совершении преступлений в сфере информационных технологий.
12. Объекты осмотра места происшествия по делам о преступлениях в сфере компьютерной информации и особенности подготовки к производству этого следственного действия.
13. Тактика производства осмотра места происшествия по делам о преступлениях в сфере компьютерной информации.
14. Особенности фиксации результатов осмотра места происшествия по делам о преступлениях в сфере компьютерной информации и изъятия следов преступления. Рекомендации по корректному завершению сотрудниками следственно-оперативной группы действия различных компьютерных программ в ходе производства осмотра места происшествия.
15. Особенности подготовки и проведения осмотра места происшествия по делам о преступлениях в сфере телекоммуникации и связи, и изъятия следов преступления.
16. Особенности подготовки и проведения осмотра места происшествия по делам о преступлениях в сфере оборота платежных пластиковых карт и изъятия следов преступления.
17. Применение специальных знаний при расследовании преступлений, сопряженных с применением информационных средств и технологий.
18. Отличительные черты современных операционных систем с точки зрения выявления криминалистически значимой информации.
19. Сетевая операционная система MS Windows и ее особенности при выявлении и собирании криминалистически значимой информации.
20. Базовые настройки программы SETUP BIOS и их значение для выявления и собирания криминалистически значимой информации.
21. Ресурсы персонального компьютера. Понятие, состав, функциональное предназначение. Важность установления системного времени.
22. Аппаратные компоненты персонального компьютера. Виды носителей компьютерной информации.
23. Логическая и физическая структура жесткого магнитного диска. Логическая и физическая структура гибкого магнитного диска.
24. Классификация нештатных состояний жесткого магнитного диска.
25. Физические дефекты и логические ошибки накопителя на жестком магнитном диске. Методы исследования накопителя на жестком магнитном диске. Программное обеспечение, необходимое для исследования.
26. Алгоритм восстановления данных на диске, находящемся в нештатном состоянии.
27. Компьютерные сети – понятие, виды, функциональное предназначение.
28. Принципы действия и используемые протоколы глобальной сети Интернет.
29. Понятие, структура, виды IP-адресов (в зависимости от класса сети), особенности с точки зрения возможности получения криминалистически значимой информации.
30. Основные направления обеспечения сетевой безопасности.
31. Компьютерные вирусы. Понятие, способы и следы негативного воздействия на информацию, способы распространения и внедрения. Принцип действия антивирусных программ.
32. Классификация компьютерных вирусов. Жизненный цикл вируса.
33. Загрузочные вирусы. Понятие, локализация, способ действия программы.
34. Файловые вирусы. Понятие, виды, локализация, способ действия программы.
35. Макровирусы. Понятие, виды, локализация, способ действия программы.

36. Сетевые вирусы. Понятие, виды, локализация, способ распространения и действия программы.
37. Понятие судебно-компьютерной экспертизы, ее предмет и специальные познания. Классификация судебно-компьютерных экспертиз.
38. Основные задачи, решаемые судебно-компьютерной экспертизой. Идентификационные и диагностические задачи.
39. Аппаратные, программные и информационные объекты судебно-компьютерной экспертизы. Типичные объекты судебно-компьютерной экспертизы.
40. Сущность, цели и задачи аппаратно-компьютерной экспертизы.
41. Сущность, цели и задачи программно-компьютерной экспертизы.
42. Сущность, цели и задачи информационно-компьютерной экспертизы (данных).
43. Сущность, цели и задачи компьютерно-сетевой экспертизы.
44. Комплексный характер судебно-компьютерной экспертизы.
45. Особенности назначения и производства комплексной судебно-компьютерной экспертизы и технико-криминалистической экспертизы документов.
46. Особенности назначения и производства комплексных судебно-компьютерной экспертизы и судебно-экономических экспертиз.
47. Комплексные судебно-компьютерные экспертизы и инженерно-технические экспертизы.
48. Подготовительный этап судебно-компьютерной экспертизы – содержание и особенности.
49. Содержание и особенности исследовательского этапа судебно-компьютерной экспертизы. Экспертный инструментарий.
50. Диагностирование системного блока персонального компьютера.
51. Экспертное исследование носителей компьютерной информации. Диагностическое исследование файлов.
52. Поиск признаков выполнения несанкционированных действий или использования специальных программ удаленного администрирования.
53. Особенности экспертной диагностики защищенной компьютерной информации.
54. Особенности производства исследований по признакам контрафактности.
55. Особенности исследования информации, сопряженной с работой в сети Интернет.
56. Особенности назначения судебно-компьютерной экспертизы и подготовки объектов на экспертизу. Структура заключения эксперта и его оценка.
57. Типичные следственные ситуации и экспертные пути их разрешения.
58. Общенаучные и специальные методы, применяемые в судебно-компьютерной экспертизе.
59. Основные системы сотовой связи. Методы исследования мобильных телефонов. Экспертный инструментарий.
60. Тенденции и перспективы развития судебно-компьютерной экспертизы.

Перечень практических заданий к зачету по дисциплине:

61. Определить данные о времени записи оптических дисков при непосредственном доступе к операционной системе.
62. Определить данные об операционной системе «Windows» при непосредственном доступе к операционной системе.
63. Определить данные о программных продуктах «MicrosoftOffice» при непосредственном доступе к операционной системе.
64. Определить данные о программных продуктах «MicrosoftOffice» при удаленном и непосредственном доступе к операционной системе.
65. Определить данные об операционной системе «Windows» при удаленном и непосредственном доступе к операционной системе.
66. Определить данные о подключении мобильных (внешних) устройств через порты USB в операционных системах семейства «Windows NT» при удаленном и непосредственном доступе к операционной системе.
67. Определить данные о подключении мобильных (внешних) устройств через порты USB в операционных системах семейства «Windows NT» при непосредственном доступе к операционной системе.
68. Произвести блокировку записи через порты USB в операционных системах семейства «Windows NT».
69. Выполнить по секторное копирование данных с цифрового носителя информации.
70. Произвести изъятие информации с сетевого источника. Произвести изъятие носителей информации с соблюдением необходимых методик.
71. Получить данные о работе пользователя в сети «Internet» для операционных систем семейства «Windows NT».
72. Определить данные об использовании программного обеспечения.
73. Составить языковый запрос на поиск информации в сети «Internet».
74. Обойти парольную защиту «Windows NT» и скопировать служебные файлы.
75. С помощью специализированных программных продуктов получить файл подкачки и гибернации операционной системы «Windows».
76. Выполнить действия по созданию побитовой копии с помощью программно-аппаратного комплекса «дубликатор».

77. Выполнить получение дампа памяти мобильного телефона с помощью программно комплекса «Мобильный Криминалист».
78. Выполнить разблокировку мобильного телефона с помощью программного комплекса «Мобильный Криминалист».
79. Произвести получение и анализ данных, хранящихся в MFT файле.
80. Произвести поиск графической информации по заданным критериям.
81. Произвести анализ данных EXIF.
82. Определить данные о времени использования операционных систем семейства «Windows NT».
83. Определить данные, хранящиеся в SQLite файлах.
84. Выполнить восстановление удаленных SMS сообщений из памяти мобильного телефона с помощью программно комплекса «Мобильный Криминалист».
85. Выполнить восстановление удаленных SMS сообщений из памяти мобильного телефона с помощью программно-аппаратного комплекса «UFED».
86. Получить данные о выходе в сеть Internet в операционных системах «MAX OS».
87. Получить данные о выходе в сеть Internet в операционных системах «Linux».
88. Определить данных об операционной системе «Mac OS» при удаленном доступе к операционной системе.
89. Выполнить получение дампа памяти мобильного телефона с помощью программно-аппаратного комплекса «UFED».
90. Выполнить разблокировку мобильного телефона с помощью программно-аппаратного комплекса «UFED».

К комплекту билетов прилагаются разработанные преподавателем и утвержденные на заседании кафедры критерии оценивания по дисциплине.

Критерии оценивания:

1) оценка «зачет» (50-100 баллов) ставится если: в полном объеме раскрыто содержание материала, показано общее понимание вопроса; демонстрируются уверенные знания, умения и навыки по изучаемой дисциплине;

2) оценка «незачет» (0-49 баллов) ставится если: материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине, не раскрыто его основное содержание; допущены грубые ошибки в определениях и понятиях, при использовании терминологии, которые не исправлены после наводящих вопросов; демонстрирует незнание и непонимание существа экзаменационных вопросов; не даны ответы на дополнительные или наводящие вопросы преподавателя.

Тесты

1. Что такое IP-адрес:
а) это номер телефонной станции в системе IP-телефонии;
б) это уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP;
в) это уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet;
г) это уникальный идентификатор подключения канального уровня в компьютерной сети, построенной по протоколу FrameRelay.

2. Что такое MAC-адрес:
а) это уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP;
б) это номер платы сетевого коммуникационного оборудования;
в) это уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet;
г) это адрес канального уровня в сетях FrameRelay.

3. IP-адрес состоит из:
а) 8 бит;
б) 16 бит;
в) 32 бит;
г) 64 бит.

4. Команда запуска подпрограммы (Assembler):
а) Call;
б) Go to;
г) JCXZ;
д) ни одно из названных.

5. Назначение дизассемблера:
а) декомпиляция исполняемого файла;
б) преобразование в ассемблерный код исполняемого файла без его запуска;
г) преобразование в ассемблерный код запущенного приложения.

6. Что такое аппаратное прерывание:
а) адрес блока оперативной памяти, содержащегося в начальном участке оперативной памяти;
б) инструкция для обращения к аппаратному устройству в компьютере;
г) технология взаимодействия программных и аппаратных элементов компьютера.

7. Команда запуска exploits (Assembler):
а) JCXZ;
б) Call;
г) Go to;
д) ни одно из названных.

8. Назначение отладчика:
а) преобразование в ассемблерный код запущенного приложения;
б) редактирования бинарных файлов;
г) преобразование а ассемблерный код исполняемого файла без его запуска;
д) тестирование PE файлов.

9. Что такое программное прерывание:
а) технология взаимодействия программных и аппаратных элементов компьютера;
б) точка останова программы;
г) адрес блока оперативной памяти, содержащегося в начальном участке оперативной памяти.

10. Назначение системных мониторов:
а) сканирование выполняемых процессов;
б) преобразование в ассемблерный код запущенного приложения;
г) преобразование в ассемблерный код исполняемого файла без его запуска.

11. Назначение HEX редакторов:
а) изменение ассемблерных инструкций в исполняемом файле;
б) сканирование обращений к файловой системе;
г) преобразование в ассемблерный код исполняемого файла без его запуска;
д) восстановление зашифрованных ассемблерных инструкций в исполняемом файле.

12. Назначение WinAPI:
а) команда для взаимодействия программного средства с элементами ОС;
б) вызов системной инструкции операционной системы;
в) оба варианта.

13. Команда безусловного перехода (Assembler):
а) Go to;
б) JCXZ;
г) JMP;
д) ни одно из названных.

14. Система управления базами данных (СУБД) это:
а) программный комплекс поддержки интегрированной совокупности данных, предназначенный для создания, ведения и использования базы данных многими пользователями;
б) система языковых, алгоритмических, программных, технических и организационных средств поддержки интегрированной совокупности данных, а также сами эти данные, представленные в виде баз данных;
в) совокупность таблиц с данными.

15. Банк данных это:
а) программный комплекс поддержки интегрированной совокупности данных, предназначенный для создания, ведения и использования базы данных многими пользователями;
б) система языковых, алгоритмических, программных, технических и организационных средств поддержки интегрированной совокупности данных, а также сами эти данные, представленные в виде баз данных;
в) совокупность таблиц с данными.

16. Назначение языка SQL:
а) манипулирование данными;
б) определение данных;
в) определение параметров запуска сервера баз данных;
г) наделение пользователей привилегиями;
д) резервирование данных.

17. Какие операторы не входят в состав языка манипулирования данными (DML):
а) SELECT;
б) CREATE;
в) UPDATE;
г) DELETE;
д) ALTER.

18. Какие операторы входят в состав языка определения данными(DDL):
а) CREATE;
б) SELECT;
в) UPDATE;
г) DELETE;
д) ALTER;
е) DROP.

19. Какие операторы входят в состав языка управления данными
(DCL):
а) REVOKE;
б) SELECT;
в) GRANT
г) DELETE;
д) ALTER.

20. Назначение выражения ORDER BY:
а) позволяет наложить условие на выборку;
б) позволяет произвести группировку данных;
в) позволяет произвести сортировку данных в выборке.

21. Назначение выражения GROUP BY:
а) позволяет наложить условие на выборку;
б) позволяет произвести группировку данных;
в) позволяет произвести сортировку данных в выборке;

22. Какие номера строк выведутся при использовании выражении LIMIT 4,2:
а) 2-4;
б) 4,5;
в) 5,6.

23. Назначение групповой функции COUNT:
а) определяет среднее арифметическое значение в группе;
б) определяет количество записей в группе;
в) выполняет конкатенацию.

24. Ветвь реестра «HKEY_LOCAL_MACHINE\Software» формируется из файла:
а) «%SystemRoot%\system32\config\software»;
б) «%SystemRoot%\system32\config\system»;
г) «%SystemRoot%\system32\config\SAM».

25. В журнале безопасности содержатся события:
а) записанные системными компонентами Windows;
б) удачные и неудачные попытки входа в систему, а также события,
связанные с использованием ресурсов;
г) записанные программами.

26. Идентификатор безопасности «SID» можно определить:
а) путем просмотра ветвей реестра

«HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\ProfileList»;
б) путем просмотра содержимого файла «setupapi.log»;
в) оба варианта.

27. Имя компьютера «ComputerName», соответствующее сетевому идентификационному имени – «COMP», можно определить:
а) путем просмотра ветвей реестра «[HKEY_LOCAL_MACHINE\
SYSTEM\ControlSet001\Control\Computer Name\ ComputerName»;
б) путем просмотра ветвей реестра «HKEY_LOCAL_MACHINE\
SOFTWARE\Microsoft\Windows NT\CurrentVersion»;
г) содержится в обоих ключах реестра.

28. Данные об использовании ОС Windows можно выявить:
а) путем просмотра журнала событий ОС;
б) путем просмотра реестра;
г) оба варианта.

29. Данные о времени получения IP-адресов для сетевого адаптера можно определить:
а) путем просмотра журнала событий ОС;
б) путем просмотра реестра ОС;
в) путем просмотра сведений из \Documents andSettings\LocalService\Application Data\».

30) Данные о времени отключения сетевого адаптера можно
определить:
а) путем просмотра журнала событий ОС;
б) путем просмотра реестра ОС;
в) путем просмотра сведений из «\\Documents and Settings\LocalService\Application Data\».

31. Данные об использовании MS Office в ОС Windows XP можно выявить:
а) путем просмотра реестра ОС и файлов, расположенных в директории «Мои документы»;
б) путем установления дат создания и изменений файлов, созданных в приложениях MS Office;
в) путем просмотра файлов, расположенных :\Documents andSettings\%username %\Application Data\Microsoft\Office\Последние файлы\ и:\WINDOWS\Prefetch\.

32. Учетные данные об ОС Windows можно выявить:
а) путем просмотра ветви реестра«HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion»;
б) путем просмотра файлов, расположенных :\Documents andSettings\%username %\Application Data\Microsoft\Office\Последние файлы\ и:\WINDOWS\Prefetch\;
в) путем просмотра ветви реестра«HKEY_USERS\S1521164449193765137782768200333010003\Software\Microsoft\Windows NT\CurrentVersion».

33. Данные о времени записи оптических дисков можно определить:
а) путем просмотра реестра ОС;
б) путем просмотра сведений из «\DocumentsandSettings\AllUsers\Главноеменю\Программы\»;
в) путем просмотра журнала событий ОС.

34. Возможно ли определить даты удаления файлов в операционной системе Windows:
а) нет;
б) возможно только в файловой системе NTFS;
в) возможно только в файловой системе FAT.

35. Данные об использовании MS Office в ОС Windows 7 можно выявить:
а) путем просмотра файлов, расположенных: Users\%username%\AppData\Roaming\Microsoft\Office\Последниефайлы\ , :\WINDOWS\Prefetch\и журнала работы ОС;
б) путем просмотра реестра ОС и файлов, расположенных в директории «Мои документы»;
в) путем установления дат создания и изменений файлов, созданных в приложениях MS Office.

36. Время подключении USB в Windows XP можно определить:
а) путем просмотра файла setupapi.log;
б) путем просмотра файлов реестра;
в) путем просмотра журналов работы ОС.

37. Файлы реестра, используемые конкретным пользователем Windows 7 и выше, хранятся:
а) . %SystemDrive%\Documents and Settings\<Username>\ ntuser.dat;
б) %SystemDriv%\Users\<Username>\ntuser.dat;
в) %SystemRoot%\Users\config\default.

38. Журналы работы Windows 7 и выше хранятся?
а) %SystemRoot%\System32\Winevt\Logs\;
б) %SystemRoot%\System32\config\;
в) %SystemRoot%\system32\config\default.

39. Данные реестра для разблокировки записи по USB порту:
а) [HKLM]\SYSTEM\CurrentControlSet\Control\Storage DevicePolicies]"WriteProtect"=dword:00000000;
б) [HKLM]\SYSTEM\CurrentControlSet\Control\Storage DevicePolicies]"WriteProtect"=dword:00000001;
в) [HKLM]\SYSTEM\CurrentControlSet\Control\Storage DevicePolicies]"WriteProtect"=dword:00000010.

40 Данные о подключении USB в Windows XP хранятся?
а) в файле подкачки;
б) в файлах реестра;
в) в журналах работы ОС.

41. Данные о выходе в сеть Internet для ОС Windows можно определить:
а) путем просмотра файлов, содержащих настройки и протоколы работы программ, предназначенных для работы пользователя в сети Интернет;
б) путем просмотра реестра ОС;
в) все перечисленные варианты.

42. Основные файлы реестра Windows хранятся?
а) %SystemRoot%\System32\config\;
б) %SystemDrive%\Documents and Settings\<Username>\;
в) %SystemRoot%\System32\Winevt\Logs\.

43. Журналы работы Windows XP хранятся?
а) %SystemRoot%\System32\config\;
б) %SystemRoot%\System32\Winevt\Logs\;
в) %SystemRoot%\system32\config\default.

44. Файлы, используемые конкретным пользователем реестра Windows XP, хранятся?
а) %SystemRoot%\system32\config\default;
б) %SystemRoot%\System32\config\;
3 %SystemDrive%\Documents and Settings\<Username>\.

45. Данные о времени установки ОС Windows можно определить:
а) в реестре Windows в параметре InstallDate, где указано количество секунд,
прошедших с 1 января 1970 г. до момента установки операционной системы;
б) путем определения даты создания директории Windows;
в) путем определения дат создания файлов boot.ini и ntldr.

46. Возможно ли определить даты удаления файлов в операционных системах Linux:
а) возможно;
б) не возможно;
в) возможно в файловой системе ext4.

47. После по секторного копирование информации с машинных носителей на дополнительные носители возможно:
а) восстановление удаленной информации, как на «оригинале»;
б) восстановление только недавно удаленной информации;
в) восстановление информации невозможно.

48. Судебная экспертиза производится:
а) государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями;
б) любыми лицами, назначенными решением суда для производства судебной экспертизы;
в) только лицами, обладающими специальными знаниями и имеющими свидетельство на самостоятельное производство экспертиз.

49. Возможно ли выявить данные об использовании ОС Windows:
а) возможно только при запущенной ОС;
б) возможно;
в) нет.

50. Время подключения USB в семействе Windows и выше можно определить:
а) путем просмотра файла setupapi.log;
б) путем просмотра файлов реестра;
в) путем просмотра времени создания соответствующего ключа реестра.

51. Данные реестра для блокировки записи по USB порту:
а) [HKLM]\SYSTEM\CurrentControlSet\Control\Storage DevicePolicies]"WriteProtect"=dword:00000001;
б) [HKLM]\SYSTEM\CurrentControlSet\Control\Storage DevicePolicies]"WriteProtect"=dword:00000000;
в) [HKLM]\SYSTEM\CurrentControlSet\Control\Storage DevicePolicies]"WriteProtect"=dword:00000010.

52. Допустимо ли эксперту компьютерной судебной экспертизы отвечать на вопросы справочного характера:
а) нет;
б) допустимо в пределах компетенции эксперта;
в) допустимо при наличии у эксперта соответствующего профильного
образования.

53. Задачами судебной компьютерной экспертизы являются:
а) поиск компьютерной информации по заданным критериям;
б) анализ работы средств вычислительной техники;
в) поиск компьютерной информации по заданным критериям и анализ работы средств вычислительной техники.

54. Допускается ли работа на изымаемом компьютере:
а) допускается;
б) да, но только для составления протокола;
в) нет.

55. Допускается ли в рамках проведения судебной компьютерной экспертизы использование законодательно незакрепленных признаков:
а) допустимо, когда нет иной возможности описать действия программного обеспечения;
б) допустимо, только в случаях, когда эксперт может пояснить суду смысл используемых признаков;
в) допустимо, только в случаях отсутствия терминов, определенных законодательными или нормативными актами, при этом необходимо использовать те термины, которые употребляют разработчики технических средств, программных продуктов в документации, описаниях, справках и т.п.

56. Возможно ли определить имя компьютера «ComputterName», соответствующее сетевому идентификационному имени «COMP» не производя загрузку системы:
а) возможно только с применением оперативных источников;
б) невозможно;
в) возможно путем просмотром ветвей реестра.

57. Возможно ли определить информацию о подключении внешних устройств в ОС Wiindows:
а) возможно только при запущенной ОС;;
б) возможно;
в) нет.

58. Следует ли производить изъятие серверов с хранимой и обрабатываемой на них сетевой информацией:
а) нет, если сервер слишком тяжелый;
б) обязательно во всех случаях;
в)) достаточно изъять только необходимую информацию путем копирования её на внешние носители.

59. Эксперт это:
а) лицо, обладающее специальными знаниями и назначенное в порядке,, установленном уголовно-процессуальным кодексом для производства судебной экспертизы и дачи заключения;
б)) лицо, обладающее специальными познаниями и назначенное в порядке, установленном Федеральным законом №73 и Конституцией РФ для производства экспертиз;
в)) лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в порядке, установленном Кодексом, для содействия в обнаружении, закреплении и изъятии предметов и документов,

применении технических средств в исследовании материалов уголовного дела, а также для разъяснения сторонам и суду вопросов,, входящих в его профессиональную компетенцию.

60. Эксперт не вправе:
а) проводить без разрешения дознавателя, следователя, суда исследования, могущие повлечь полное или частичное уничтожение объектов, либо изменение их внешнего вида или основных свойств;
б) проводить без разрешения начальника экспертного учреждения исследования, могущие повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств;
в) проводить без консультации с инициатором исследования и разрешения начальника экспертного учреждения исследования, могущие повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств.

61. Руководитель экспертного учреждения вправе возвратить без исполнения постановление о назначении судебной экспертизы и материалы, представленные для ее производства:
а) если в данном учреждении нет эксперта конкретной специальности, либо специальных условий для проведения исследований, указав мотивы, по которым производится возврат;
б) если в постановлении указаны вопросы, требующие привлечения экспертов других специальностей;
в) если в данном учреждении нет эксперта конкретной специальности, либо специальных условий для проведения исследований, указав мотивы, по которым производится возврат.

62. Производство дополнительной судебной экспертизы:
а) назначается в случае недостаточной ясности или полноты ранее данного заключения, поручается тому же или другому эксперту;
б) назначается в случае привлечения эксперта к ответственности за дачу «заведомо ложного заключения»;
в) назначается в случае, если эксперт сделал ошибочные выводы и поручается другому эксперту.

63. Производство повторной судебной экспертизы:
а) назначается в связи с «возникшими у суда, судьи, лица, производящего дознание, следователя или прокурора сомнениями в правильности или обоснованности ранее данного заключения по тем же вопросам», поручается другому эксперту или другой комиссии экспертов;
б) назначается в связи с отсутствием у эксперта, её проводившего, свидетельства на самостоятельное производство экспертиз;
в) назначается в связи с неверным оформлением экспертного заключения.

Инструкция по выполнению

Каждому студенту предлагается комплекс из 35 тестовых заданий, формируемых программой компьютерного тестирования персонально для каждого аттестуемого из общего фонда тестовых заданий.

Каждое тестовое задание предполагает выбор одного правильного ответа из четырех или пяти вариантов. Время, отводимое на тестирование – 30 мин. Время нормируется компьютерной программой тестирования.

Критерии оценки

Количество правильных ответов	Оценка в 35-балльной шкале
30-35	30-35
24-29	24-29
18-23	18-23
17-0	0-17

Алгоритм оценивания является составной частью компьютерной программы тестирования. Результаты тестирования предоставляются преподавателю с указанием ФИО аттестуемого, номера группы, количества баллов в 35-балльной шкале.

Кейс-задачи

Задача 1

Определить данные о времени записи оптических дисков при непосредственном доступе к операционной системе.

Задача 2

Определить данные об операционной системе «Windows» при непосредственном доступе к операционной системе.

Задача 3

Определить данные о программных продуктах «MicrosoftOffice» при непосредственном доступе к операционной

системе.

Задача 4

Определить данные об экономических программных продуктах ЗАО«1С» при непосредственном доступе к операционной системе.

Задача 5

Определить данные о программных продуктах «MicrosoftOffice» при удаленном доступе к операционной системе.

Задача 6

Определить данные об операционной системе «Windows» при удаленном доступе к операционной системе.

Задача 7

Определить данные об экономических программных продуктах ЗАО«1С» при удаленном доступе к операционной системе.

Задача 8

Определить данные о подключении мобильных (внешних) устройств через порты USB в операционных системах семейства «Windows NT» при удаленном доступе к операционной системе.

Задача 9

Определить данные о подключении мобильных (внешних) устройств через порты USB в операционных системах семейства «Windows NT» при непосредственном доступе к операционной системе.

Задача 10

Определить данные о времени записи оптических дисков при непосредственном доступе к операционной системе.

Задача 11

Произвести блокировку записи через порты USB в операционных системах семейства «Windows NT».

Задача 12

Выполнить по секторное копирование данных с цифрового носителя информации.

Задача 13

Произвести изъятие информации с сетевого источника.

Задача 14

Произвести изъятие носителей информации с соблюдением необходимых методик.

Задача 15

Получить данные о работе пользователя в сети «Internet» для операционных систем семейства «Windows NT».

Задача 16

Определить данные об операционной системе «Mac OS» при непосредственном доступе к операционной системе.

Задача 17

Определить данные об использовании программного обеспечения.

Задача 18

Определить валидность платежной карты.

Задача 19

Получить доступ к информации с помощью программно-аппаратного комплекса «PC-3000».

Задача 20

Произвести подключение носителя информации с помощью программно-аппаратного комплекса «PC-3000».

Задача 21

Произвести восстановление информации с помощью программно-аппаратного комплекса «PC-3000».

Задача 22

Составить языковый запрос на поиск информации в сети «Internet».

Задача 23

Обойти парольную защиту «Windows NT» и скопировать служебные файлы.

Задача 24

Определить данных об операционной системе «Mac OS» при удаленном доступе к операционной системе.

Задача 25

Выполнить поиск данных с помощь специализированного программного продукта «Belkasoft».

Задача 26.

С помощью специализированных программных продуктов получить дамп оперативной памяти операционной системы «Windows».

Задача 27

С помощью специализированных программных продуктов получить файл подкачки и гибернации операционной системы «Windows».

Задача 28

Выполнить действия по созданию побитовой копии с помощью программно-аппаратного комплекса «дубликатор».

Задача 29

Выполнить получение дампа памяти мобильного телефона с помощью программно-аппаратного комплекса «UFED».

Задача 30

Выполнить получение дампа памяти мобильного телефона с помощью программно комплекса «Мобильный Криминалист».

Задача 31

Выполнить разблокировку мобильного телефона с помощью программно-аппаратного комплекса «UFED».

Задача 32

Выполнить разблокировку мобильного телефона с помощью программного комплекса «Мобильный Криминалист».

Задача 33

Произвести получение и анализ данных, хранящихся в MFT файле.

Задача 34

Произвести поиск графической информации по заданным критериям.

Задача 35

Произвести анализ данных EXIF.

Задача 36

Определить данные о времени использования операционных систем семейства «Windows NT».

Задача 37

Определить данные, хранящиеся в SQLite файлах.

Задача 38

Выполнить восстановление удаленных SMS сообщений из памяти мобильного телефона с помощью программно комплекса «МобильныйКриминалист».

Задача 39

Выполнить восстановление удаленных SMS сообщений из памяти мобильного телефона с помощью программно-аппаратного комплекса «UFED».

Задача 40

Получить данные о выходе в сеть Internet в операционных системах «MAX OS».

Задача 41

Получить данные о выходе в сеть Internet в операционных системах «Linux»

Критерии оценки:

Максимум по оценочному средству 35 баллов.

Шкала оценивания решения кейс-задачи 5 баллов:

- 5 баллов выставляется обучающемуся, если задача решена верно и полностью, в соответствии с действующим законодательством; в логических рассуждениях и обосновании решения нет пробелов и ошибок; в решении нет процессуальных ошибок (возможна одна неточность, описка, не являющееся следствием незнания или непонимания учебного материала).

- 4 балла выставляется обучающемуся, если задача решена полностью, но обоснования шагов решения недостаточны, допущена одна ошибка или два-три недочета в решениях; выполнено без недочетов не менее ¾ задания.

- 3 балла выставляется обучающемуся, если допущены более одной ошибки или более трех недочётов в решении, но обучающийся владеет обязательными навыками и умениями по проверяемой теме; без недочетов выполнено не менее половины задания.

- 2 балла выставляется обучающемуся, если допущены более двух ошибок или более четырех недочётов в решении, но обучающийся владеет основными навыками и умениями по проверяемой теме; без недочетов выполнено не менее одной трети задания.

- 1 балл выставляется обучающемуся, если допущены более трех ошибок или более пяти недочётов в решении, но обучающийся владеет некоторыми навыками и умениями по проверяемой теме; без недочетов выполнено менее одной трети задания.

- 0 баллов выставляется обучающемуся, если допущены существенные ошибки, указывающие, что обучающийся не владеет обязательными навыками и умениями по проверяемой теме; правильно выполнено менее одной пятой задания.

Темы докладов

1. Задачи, решаемые судебными компьютерными экспертизами.
2. Обзор программного обеспечения для производства судебных компьютерных экспертиз.
3. Мировой опыт проведения компьютерных экспертиз.
4. Компьютерная экспертиза средств мобильной связи.
5. Подходы к исследованию компьютерной информации в Российской Федерации.
6. Перспективы развития компьютерных технологий.
7. Компьютерные технологии как предмет экспертных исследований.
8. Специализированные программно-аппаратные комплексы для проведения исследования компьютерной информации.
9. Следообразование в операционных системах.
10. Недокументированные возможности операционных систем Windows.
11. Требования к экспертным подразделениям, проводящим судебно-компьютерные экспертизы.
12. Требования к экспертам, проводящим судебно-компьютерные экспертизы.
13. Реализация информационных процессов в компьютерных системах. Понятие следов в информационной системе.
14. Криминалистическое значение специальных файлов настройки конфигурации, отчетов и каталогов операционной системы (ОС).
15. Информационные следы в системных областях, каталогах, файлах: особенности следообразования.
16. Понятие электронного документа и его связь с файлом. Криминалистически значимая информация, получаемая при исследовании файлов документов.
17. Следы воздействия на информацию в локальных компьютерных системах. Следы подготовки и выполнения удаленного воздействия. Способы сокрытия следов неправомерного воздействия на информацию.
18. Служебная информация BIOS и ее использование в криминалистических целях. Проблема достоверности системной даты и системного времени.
19. Местоположение характерной служебной информации в Windows-ориентированных программных средах. Реестр Windows.
20. Служебная информация и ее использование в восстановлении хронологии событий. Служебная информация об обстоятельствах установки экземпляров программ.
21. Служебная информация о работе пользователя с пакетом программ MicrosoftOffice, локальной сетью, сетью Интернет, прикладных программ. Лог-файлы, файлы инициализации программ и их криминалистическая значимость.
22. Проверка наличия вредоносных программ. Неразрушающие методы исследования информации: перенос файловой структуры на тестовый винчестер, использование технологии виртуальных машин, использование образов разделов и дисков для исследования.
23. Проверка наличия программно-аппаратных средств защиты информации и следов их применения. Контроль правильности установки системной даты в конкретном интервале дат или на протяжении всего времени нахождения информации на носителе.

24. Особенности файловых систем FAT и NTFS применительно к решению задачи поиска и восстановления информации.

25. Программы для поиска и восстановления удаленных файлов. Особенности восстановления содержимого документа при поврежденной структуре файла.

Критерии оценки:

Максимум по оценочному средству 30 баллов.

Шкала оценивания доклада 5 баллов:

- 5 баллов выставляется обучающемуся, если изложенный материал фактически верен, выявлено наличие глубоких исчерпывающих знаний в объеме изучаемой темы, грамотное и логически стройное изложение материала, даны подробные ответы на вопросы. Работа имеет законченный, самостоятельный характер. Оформление соответствует требованиям.

- 4 балла выставляется обучающемуся, если изложенный материал фактически верен, выявлено наличие твердых и достаточно полных знаний в объеме изучаемой темы, грамотное и логически стройное изложение материала, даны ответы на вопросы. Работа имеет законченный, самостоятельный характер. Оформление соответствует требованиям.

- 3 балла выставляется обучающемуся, если материал изложен верно, но не достаточно полно, имеются недостатки в логике и последовательности изложения материала, даны ответы не на все вопросы. Имеются недочеты в оформлении.

- 2 балла выставляется обучающемуся, если материал изложен с незначительными ошибками, недостаточно полно, имеются недостатки в логике и последовательности изложения материала, даны ответы не на все вопросы. Имеются ошибки в оформлении.

- 1 балл выставляется обучающемуся, если материал изложен с ошибками, недостаточно полно, имеются недостатки в логике и последовательности изложения материала, даны ответы не на все вопросы. Имеются грубые ошибки в оформлении.

- 0 баллов выставляется обучающемуся, если материал слабо связан с темой, при наличии грубых ошибок, непонимания сущности излагаемого вопроса, неуверенности и неточности ответов. Работа имеет незаконченный, несамостоятельны характер, присутствует плагиат.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания включают в себя текущий контроль и промежуточную аттестацию.

Текущий контроль успеваемости проводится с использованием оценочных средств, представленных в п. 2 данного приложения. Результаты текущего контроля доводятся до сведения обучающихся до промежуточной аттестации.

Промежуточная аттестация проводится в форме зачета.

Зачет проводится по расписанию промежуточной аттестации. Количество вопросов в зачетном задании – 3 (два теоретических и один практический). Проверка ответов и объявление результатов производится в день проведения зачета. Результаты аттестации заносятся в зачетную ведомость и зачетную книжку студента. Студенты, не прошедшие промежуточную аттестацию по графику сессии, должны ликвидировать задолженность в установленном порядке.

Приложение 2

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Учебным планом предусмотрены следующие виды занятий:

- лекции;
- практические занятия.

В ходе лекционных занятий рассматриваются теоретические вопросы дисциплины и даются рекомендации для самостоятельной работы и подготовке к практическим занятиям.

В ходе практических занятий углубляются и закрепляются знания студентов по ряду рассмотренных на лекциях вопросов, развиваются навыки проведения исследований различных объектов судебно-компьютерной экспертизы.

При подготовке к практическим занятиям каждый студент должен:

– изучить рекомендованную учебную литературу;

– изучить конспекты лекций;

– подготовить ответы на все вопросы по изучаемой теме.

По согласованию с преподавателем студент может подготовить доклад по теме занятия. В процессе подготовки к практическим занятиям студенты могут воспользоваться консультациями преподавателя.

Вопросы, не рассмотренные на лекциях и практических занятиях, должны быть изучены студентами в ходе самостоятельной работы. Контроль самостоятельной работы студентов над учебной программой курса осуществляется в ходе занятий посредством тестирования. В ходе самостоятельной работы каждый студент обязан прочитать основную и по возможности дополнительную литературу по изучаемой теме, дополнить конспекты лекций недостающим материалом, выписками из рекомендованных первоисточников. Выделить непонятные термины, найти их значение в энциклопедических словарях.

Студент должен готовиться к предстоящему практическому занятию по всем, обозначенным в рабочей программе дисциплины вопросам.

Для подготовки к занятиям, текущему контролю и промежуточной аттестации студенты могут воспользоваться электронно-библиотечными системами. Также обучающиеся могут взять на дом необходимую литературу на абонементе университетской библиотеки или воспользоваться читальными залами.