МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Судебные компьютерно-технические экспертизы»

Специальность:	40.05.03 – Судебная экспертиза
Специализация:	Инженерно-технические экспертизы
Квалификация выпускника:	Судебный эксперт
Форма обучения:	очная
Год начала подготовки	2017

1. Цели освоения учебной дисциплины

Цель преподавания дисциплины состоит в подготовке специалистов, способных квалифицированно и на современном уровне решать задачи использования специальных познаний в целях установления фактических данных, способствующих расследованию, раскрытию и предупреждению «компьютерных преступлений» и преступлений других видов, обладающих основами знаний и умений в области исследования средств обеспечения автоматизированных информационных систем и их технологий.
Задачи преподавания дисциплины заключаются в получении студентами теоретических знаний научных и правовых основ судебной компьютерно-технической экспертизы, изучении системы методов и средств судебной компьютерно-технической экспертизы, овладении специальной терминологией, изучении основных методов поиска и фиксации криминалистически значимой информации, закономерностей следообразования, ознакомление с работой специалистов в области информационных технологий по обеспечению оперативно-розыскных мероприятий и следственных действий, ознакомление с деятельностью государственных судебно-экспертных учреждений по производству компьютерно-технической (информационно-технологической) экспертизы. В содержании учебной дисциплины присутствуют новейшие концепции криминалистики и судебной экспертологии, отражен передовой опыт экспертных подразделений и следственных аппаратов органов внутренних дел по раскрытию и расследованию преступлений.

2. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Судебные компьютерно-технические экспертизы" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОК-7	способностью к логическому мышлению, аргументированно и ясно строить устную и письменную речь, вести полемику и дискуссии
ОК-12	способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
ОПК-2	способностью применять естественнонаучные и математические методы при решении профессиональных задач, использовать средства измерения
ПК-1	способностью использовать знания теоретических, методических, процессуальных и организационных основ судебной экспертизы, криминалистики при производстве судебных экспертиз и исследований
ПК-2	способностью применять методики судебных экспертных исследований в профессиональной деятельности
ПК-3	способностью использовать естественнонаучные методы при исследовании вещественных доказательств
ПК-4	способностью применять технические средства при обнаружении, фиксации и исследовании материальных объектов - вещественных доказательств в процессе производства судебных экспертиз
ПК-5	способностью применять познания в области уголовного права и уголовного процесса
ПК-7	способностью участвовать в качестве специалиста в следственных и

	других процессуальных действиях, а также в непроцессуальных действиях
ПСК - 2.2	способностью при участии в процессуальных и непроцессуальных действиях применять инженерно-технические методы и средства поиска, обнаружения, фиксации, изъятия и предварительного исследования материальных объектов для установления фактических данных (обстоятельств дела) в гражданском, административном, уголовном судопроизводстве, производстве по делам об административных правонарушениях

4. Общая трудоемкость дисциплины составляет

7 зачетных единиц (252 ак. ч.).

5. Образовательные технологии

С целью формирования и развития профессиональных знаний, умений и навыков обучающихся предусмотрено проведение лекций с активным применением мультимедийных средств, проведение практических занятий с использованием современных технико-криминалистических средств, решение типовых задач в диалоговом режиме, проблемные вопросы разрешать в виде научных дискуссий, подготовка и обсуждение эссе, докладов и рефератов, участие студентов в вузовских конференциях в сочетании с внеаудиторной работой, приглашение на занятия практиков из следственных, оперативно-розыскных и экспертных аппаратов. .

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

Тема: Уголовно-правовая квалификация и криминалистическая характеристика преступлений совершенных с использованием средств электронно-вычислительной техники и радиоэлектронных устройств.
Тестирование

Тема: Уголовно-правовая квалификация и криминалистическая характеристика преступлений совершенных с использованием средств электронно-вычислительной техники и радиоэлектронных устройств.
Преступления в сфере компьютерной информации. Составы преступлений УК России, связанные с использованием компьютерных технологий.
Подготовка и совершение преступления с использованием компьютерных технологий. Механизм и инструменты совершения компьютерных преступлений. Последствия несанкционированного доступа (блокирование информационных систем, модификация и уничтожение информации, копирование). Использование компьютерных технологий для подделки документов. Компьютер как источник криминалистически значимой информации.
Современные формы преступлений в сфере информационных технологий. Объект, предмет и субъект таких преступлений.
Угрозы информационной безопасности. Каналы утечки информации из средств компьютерной техники. Понятие несанкционированного и неправомерного доступа. Использование уязвимостей программного обеспечения и достижений информационных технологий для совершения преступлений.

Тема: Правовые, организационные и научно-методические основы судебно-компьютерной экспертизы.
Становление и современная практика организации производства СКЭ. Нормативная база производства компьютерных экспертиз в системе экспертных учреждений. Порядок

назначения и производства экспертизы. Вещественные доказательства по преступлениям, связанным с применением средств вычислительной техники.
Судебно-компьютерная экспертиза как вид судебной экспертизы и направление экспертной деятельности. Предмет СКЭ. Цели и задачи СКЭ. Место СКЭ в общей классификации судебных экспертиз. Понятие и характеристика объектов СКЭ. Вопросы, решаемые СКЭ.

Тема: Общие вопросы следообразования в компьютерных системах.
Реализация информационных процессов в компьютерных системах. Понятие следов в информационной системе.
Криминалистическое значение специальных файлов настройки конфигурации, отчетов и каталогов операционной системы (ОС).
Информационные следы в системных областях, каталогах, файлах: особенности следообразования. Понятие электронного документа и его связь с файлом.
Криминалистически значимая информация, получаемая при исследовании файлов документов.
Следы воздействия на информацию в локальных компьютерных системах. Следы подготовки и выполнения удаленного воздействия. Способы сокрытия следов неправомерного воздействия на информацию.

Тема: Общие вопросы следообразования в компьютерных системах.
Ситуационные задачи

Тема: Криминалистическая значимость служебной информации операционной системы и прикладного программного обеспечения.
Виды служебной информации и их криминалистическая значимость.
Служебная информация BIOS и ее использование в криминалистических целях. Проблема достоверности системной даты и системного времени.
Местоположение характерной служебной информации в Windows-ориентированных программных средах. Реестр Windows.
Служебная информация и ее использование в восстановлении хронологии событий.
Служебная информация об обстоятельствах установки экземпляров программ.
Служебная информация о работе пользователя с пакетом программ Microsoft Office, локальной сетью, сетью Интернет, прикладных программ. Лог-файлы, файлы инициализации программ и их криминалистическая значимость.

Зачет

Тема: Экспертные задачи исследования компьютерной информации и рекомендации по их решению.
Рекомендации по решению общих экспертных задач. 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.
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.
Рекомендации по решению наиболее часто встречающихся в экспертной практике частных задач. Определение отдельных этапов (стадий) события по служебной информации файла. Установление причинной связи событий, действий. Частные экспертные задачи, связанные с исследованием обстоятельств работы пользователя в сети

Интернет. Установление факта и параметров подключения компьютера к сети Интернет. Установление периодов работы пользователя в сети Интернет. Установление источника происхождения файлов при работе пользователя в сети Интернет. Установление содержания почтовых сообщений.

Тема: Решение диагностических задач в экспертном исследовании аппаратных средств персонального компьютера. Признаки подключения внешних устройств к компьютеру. Понятие состояния аппаратных компонентов. Порядок подключения дополнительных устройств к компьютерной системе. Средства установления и фиксации состояния аппаратных компонентов компьютерной системы. Описание аппаратных компонентов компьютера при экспертном исследовании или осмотре.
Анализ текущего состояния аппаратного обеспечения компьютерной системы по его физическому состоянию, определение физической возможности подключения внешнего периферийного оборудования (стандартные порты, дополнительные адаптеры, виды имеющихся или требуемых, для работы с подозреваемым оборудованием, интерфейсных разъёмов, электронные ключи).
Особенности программного подключения внешних устройств. Понятие драйвера устройства. Программные следы подключения и использования внешних устройств. Файлы устройств. Загружаемые модули ядра. Сведения, находящиеся в файлах регистрации.
Принципы программного обеспечения работоспособности периферийного оборудования в MS Windows 9x и Windows NT. Особенности использования драйверов для обеспечения работы устройств в составе аппаратно-программного комплекса. Следы подключения в реестре, среди драйверов и в файлах ini.

Тема: Решение диагностических задач в отношении файлов данных.
Отождествление оригинала документа на носителе информации при наличии дубликата, копии или машинограммы. Установление групповой принадлежности. Установление формата файла. Установление первоначального состояния файла. Установление содержания электронного документа. Выявление файлов, изменивших свое первоначальное местоположение. Реконструкция вида документа на бумажном носителе по служебной информации файла. Определение отдельных этапов (стадий) события по служебной информации файла. Определение времени (периода) выполнения действия пользователем или хронологической последовательности событий. Определение места действия, локализация его границ. Установление роли и рабочего места каждого из участников события, причинной связи событий, действий по информации в электронных документах и служебной информации.
Проблема определения даты и времени удаленного файла или сохранившихся его фрагментов и пути ее решения. Особенности восстановления содержимого документа при поврежденной структуре файла.

Тема: Решение диагностических задач в отношении файлов данных.
Тестирование

Тема: Поиск информации, восстановление удаленной и поврежденной информации.
Ревизия установленного программного обеспечения. Определение назначения установленного программного обеспечения в прикладном и системном аспекте. Определение типа искомой информации. Определение наличия программ, используемых для сокрытия или ограничения доступа к информации, и следов их применения. Классификация программного обеспечения, используемого в целях поиска информации. Проблема кодировок и форматов файлов, ее учет при осуществлении поиска информации. Этапы поиска информации: поиск информации, содержащейся в файлах; поиск

информации, содержащейся в удаленных файлах; поиск информации в кластерах.
Использование возможностей пакета программ Microsoft Office для поиска информации.
Специализированные программы для поиска текстовой информации.
Специализированные программы для поиска графической информации.
Особенности файловых систем FAT и NTFS применительно к решению задачи поиска и восстановления информации.
Программы для поиска и восстановления удаленных файлов. Программы для поиска и восстановления файловой структуры носителя информации.
Поиск и восстановление информации в файловой системе FAT в условиях разрушения связей кластеров файла. Низкоуровневый поиск и восстановление информации в файловой системе NTFS.
Проблема определения даты и времени удаленного файла или сохранившихся его фрагментов и пути ее решения.
Особенности восстановления содержимого документа при поврежденной структуре файла.

Тема: Поиск информации, восстановление удаленной и поврежденной информации.
Ревизия установленного программного обеспечения. Определение назначения установленного программного обеспечения в прикладном и системном аспекте.
Определение типа искомой информации. Определение наличия программ, используемых для сокрытия или ограничения доступа к информации, и следов их применения.
Классификация программного обеспечения, используемого в целях поиска информации.
Проблема кодировок и форматов файлов, ее учет при осуществлении поиска информации.
Этапы поиска информации: поиск информации, содержащейся в файлах; поиск информации, содержащейся в удаленных файлах; поиск информации в кластерах.
Использование возможностей пакета программ Microsoft Office для поиска информации.
Специализированные программы для поиска текстовой информации.
Специализированные программы для поиска графической информации.
Особенности файловых систем FAT и NTFS применительно к решению задачи поиска и восстановления информации.
Программы для поиска и восстановления удаленных файлов. Программы для поиска и восстановления файловой структуры носителя информации.
Поиск и восстановление информации в файловой системе FAT в условиях разрушения связей кластеров файла. Низкоуровневый поиск и восстановление информации в файловой системе NTFS.
Проблема определения даты и времени удаленного файла или сохранившихся его фрагментов и пути ее решения.
Особенности восстановления содержимого документа при поврежденной структуре файла.

Тема: Особенности назначения и производства судебно-компьютерной экспертизы, составление заключения эксперта при производстве компьютерных экспертиз.
Специфика назначения компьютерно-технических экспертиз (в т.ч. комплексных).
Порядок исследования объектов. Комплексная судебно-компьютерная и технико-криминалистическая экспертиза документов: документы, подготовленные с использованием компьютерных технологий; анализ признаков используемого программного обеспечения и его настроек; определение режимов работы печатающего устройства; ситуационный анализ; установление источника происхождения печатного документа. Комплексная судебно-компьютерная и товароведческая экспертиза. Комплексная судебно-компьютерная и трасологическая экспертиза. Комплексная судебно-компьютерная и бухгалтерская экспертиза. Особенности формулирования

выводов при производстве комплексных экспертиз.

Экзамен