Утверждено

Директор Астрелин И.С.

ООО «ЭЦ «Сателлит»

«31» октября 2023

Программа повышения квалификации по специальности
«Исследование информационных компьютерных средств»

Москва, 2023

Программа повышения квалификации по специальности «Исследование информационных компьютерных средств»

I. Общая часть

1. Процессуальные основы назначения и производства судебной компьютерно-технической экспертизы

Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации». Обязанности и права эксперта. Основания производства судебных экспертиз (далее - СЭ) в государственных судебно-экспертных учреждениях (далее - ГСЭУ). Производство дополнительной, повторной, комплексной и комиссионной СЭ в ГСЭУ. Заключение эксперта или комиссии экспертов и его содержание. Финансовое, организационное, научно-методическое, информационное обеспечение деятельности ГСЭУ.

Уголовно-процессуальный кодекс Российской Федерации. Порядок назначения судебной экспертизы. Постановление (определение) о назначении судебной компьютерно-технической экспертизы (далее - СКТЭ). Права подозреваемого, обвиняемого, потерпевшего, свидетеля при назначении и производстве судебной экспертизы. Особенности назначения следователем (судом) дополнительной, повторной, комиссионной и комплексной экспертиз. Материалы, необходимые для проведения экспертизы. Ходатайство эксперта о предоставлении дополнительных материалов, необходимых для дачи заключения. Участие эксперта в различных следственных действиях (осмотре, допросах и др.). Допрос эксперта.

Заключение эксперта. Его структура и содержание. Изложение исходных данных. Исследовательская и синтезирующая части заключения. Формулировка выводов. Особенности проведения повторных и дополнительных экспертиз и составления заключений по ним. Комиссионная и комплексная экспертизы, особенности их проведения и подготовки заключения по ним. Роль ведущего эксперта в организации и проведении этих экспертиз.

Процессуальный порядок проведения экспертизы в суде. Порядок исследования в судебном заседании заключения эксперта, данного на стадии предварительного следствия.

Особенности производства СКТЭ в суде. Назначение и проведение экспертизы в суде. Постановка вопросов. Подбор и оформление материалов для исследования. Дача заключения в судебном заседании после производства СКТЭ на предварительном следствии. Допрос эксперта в суде. Отличие его от заключения, данного в стадии предварительного расследования.

Гражданский процессуальный кодекс Российской Федерации. Назначение экспертизы. Содержание определения суда о назначении экспертизы. Комплексная и комиссионная экспертизы. Порядок проведения экспертизы. Обязанности и права эксперта. Заключение эксперта. Дополнительная и повторная экспертизы. Исследование заключения эксперта. Назначение дополнительной или повторной экспертизы.

Арбитражный процессуальный кодекс Российской Федерации. Права и обязанности эксперта. Назначение экспертизы. Порядок проведения экспертизы. Заключение эксперта. Экспертная инициатива.

Литература: [1-7, 13, 18, 22].

2. Научные и методические основы судебной компьютерно-технической экспертизы

Тема 1. Правовые аспекты судебно-экспертных исследований компьютерных средств и систем

Общая характеристика преступлений в сфере информационных технологий. Законодательство по вопросам информатизации и защиты информации.

Особенности квалификации преступлений и административных правонарушений, сопряженных с применением компьютерных средств. Особенности гражданско-правовых споров, связанных с оборотом компьютерных средств.

Механизм и инструменты совершения «компьютерных преступлений». Правовые основы производства СКТЭ.

Тема 2. Сущность СКТЭ: предмет, задачи и объекты

СКТЭ как форма использования специальных знаний. Предмет СКТЭ. Цели и задачи СКТЭ. Место СКТЭ в общей классификации судебных экспертиз. Понятие и общая характеристика объектов СКТЭ.

Тема 3. Методы и методики экспертного исследования средств обеспечения автоматизированных информационных систем и их технологий

Общенаучные и специальные методы, используемые при производстве СКТЭ.

Принцип некомпрометации доказательств. Неразрушающие методы исследования информации: перенос файловой структуры на тестовый винчестер, использование технологии виртуальных машин, использование образов разделов и дисков для исследования. Анализ и восстановление информации, не подлежащей автоматическому восстановлению. Использование виртуальных машин для моделирования работы и исследования программного обеспечения (далее-ПО).

Современные методические подходы к исследованию объектов СКТЭ. Общая методика исследования компьютерной информации на носителях данных. Общая методика исследования признаков несанкционированного доступа к компьютерной информации.

Тема 4. Средства вычислительной техники и связи, реализующие информационные процессы как объект СКТЭ

Типы технических устройств, реализующих информационные процессы. Их классификация и общая характеристика. Современные схемы коммуникаций.

Тема 5. Архитектура и устройство компьютерных систем

Архитектура компьютера, порядок взаимодействия процессора и периферийных устройств. Модули и компоненты компьютерных систем. Понятие конфигурации системы. Установка и удаление аппаратных компонентов. Роль системного программного обеспечения в управлении устройствами. Совместимость аппаратных компонентов друг с другом и с программным обеспечением, аппаратные проблемы, конфликты ресурсов и способы их разрешения.

Тема 6. Основы хранения информации

Файловые системы и системы управления базой данных (далее - СУБД) как средства упорядочения и хранения информации.

Наиболее распространенные операционные системы и используемые ими файловые системы. Журналируемые файловые системы и моментальные снимки. Кластеризация и фрагментация, алгоритмы размещения информации. Удаление и перезапись файлов. Оптимизация операций с файлами, поиск файлов. Файловые системы FAT, HPFS/NTFS, UFS/FSS, ext2/3, IBM JFS, SGI XFS, Novell NWFS. Свойства и атрибуты файлов.

Тема 7. Основные принципы работы сетей

Понятие и разновидности компьютерных сетей. Среда передачи данных. Каналы и каналообразующее оборудование. Уровни OSI. Инкапсуляция. Протоколы. Адресация.

Коммутация и маршрутизация. Службы. Понятие стека протоколов, реализация протоколов. TCP/IP. Сеансы связи.

Тема 8. Архитектура операционных систем (далее - ОС)

Назначение и архитектура операционных систем. Функции операционной системы. Семейства операционных систем: *NIX, DOS/Windows 9x, Windows NT, OS/2, BeOS. Интерфейс прикладных программ (API). Конфигурационная информация операционной системы. Управление доступа в многопользовательских системах. Прикладное программное обеспечение. Виды и типы компьютерной информации. Основные виды информации и их машинное представление, основы кодирования. Структура файлов программ и данных. Структура и содержание файлов программ различных операционных систем и средства для работы с ними. Структура служебной информации (Temporary Internet Files, Downloaded Program Files, Главное меню, Рабочий стол, Send To, Recent), структура файлов данных прикладных программ (обработки графической информации, офисных пакетов, архиваторов и т.д.).

Тема 9. Программные способы защиты информации

Защита шифрованием, паролем, технология использования открытого ключа Хэши. Способы аутентификации. Программные продукты для защиты информации. Защита сетей: понятие межсетевого экрана и брандмауэра.

Тема 10. Основы программирования

Различия между аппаратными платформами с точки зрения программирования ядра операционной системы. Процессоры без PMMU (процессоры Intel в реальном режиме). Процессоры с PMMU, защищенный режим работы процессоров Intel, начиная с модели 386. Шины, мосты и контроллеры. Управление внешними устройствами. Основы объектно-ориентированного программирования (Visual Basic). Неклассические языки программирования: сценариев, разметки. Основы HTML и JavaScript. Программное воздействие на параметры операционной системы. Программирование операций с файловой системой.

Литература: [8-12, 14-17, 19-21, 23-24, 30-33].

3. Организационные основы судебной компьютерно-технической экспертизы

Тема 1. Формы использования специальных знаний в сфере информационных технологий

Порядок и формы участия специалиста в области информационных технологий при проведении оперативно-розыскных мероприятий и следственных действий. Участие лица, обладающего специальными познаниями в области информационных технологий, в следственных действиях в качестве эксперта.

Тема 2. Особенности исследования информационных компьютерных средств в рамках комплексной экспертизы.

Специфика назначения комплексной экспертизы в случае включения в комиссию экспертов разных специальностей эксперта по производству СКТЭ. Порядок исследования объектов СКТЭ и судебно-технической экспертизы документов: документы, подготовленные с использованием компьютерных технологий; анализ признаков используемого ПО и его настройки; определение режимов работы печатающего устройства; ситуационный анализ; установление источника происхождения печатного документа. СКТЭ и товароведческая экспертиза. СКТЭ и бухгалтерская экспертиза.

Тема 3. Особенности исследования информационных компьютерных средств в рамках комплексной компьютерно-технической и товароведческой экспертизы (в соответствии с программой подготовки экспертов по специальности 19.1.)

Предмет судебно-товароведческой экспертизы (далее - СТЭ)

Задачи судебно-товароведческой экспертизы. Вопросы, относящиеся к компетенции эксперта-товароведа.

Объекты исследования. Классификация объектов СТЭ по процессуальной и вещной природе. Документы как носители информации о фактических данных, установленных с помощью специальных товароведческих познаний. Классификация видов СТЭ промышленных (непродовольственных) товаров.

Стандарты, технические условия и другие нормативные документы как составная часть специальных познаний эксперта-товароведа при исследовании объектов.

Методы исследования, применяемые при производстве судебно-товароведческих экспертиз. Возможность и допустимость использования в судебно-товароведческой экспертизе органолептических методов исследования.

Основы товароведения

Предмет и задачи товароведения. Понятие о товаре.

Связь товароведения с другими научными дисциплинами: экономикой и технологией производства товаров, с химией, физикой, биологией, микробиологией и др.

Классификация товарных групп.

Потребительские свойства товаров.

Понятие качества и уровня качества товара.

Факторы, влияющие на качество товара. Виды и качество сырья, способы и условия производства. Условия сохранности качества товара: упаковка, транспортировка, хранение. Маркировка товаров.

Нормативно-техническая документация на товары: стандарты, технические условия, контракты, договоры и др. Виды стандартов и их основное содержание.

Методы определения качества товаров: органолептический, измерительный, регистрационный, расчетный, экспертный, лабораторный. Отбор проб, образцов для определения качества товаров.

Показатели качества товаров: по числу характеризуемых свойств, характеризуемым свойствам, методу определения, способу выражения, применению для оценки уровня качества.

Тема 4. Специальные знания и алгоритмы решения типовых задач судебно-товароведческой экспертизы применительно к объектам СКТЭ

Особенности проведения судебно-товароведческих экспертиз в целях установления принадлежности двух или нескольких объектов к одной модели или марке применительно к объектам СКТЭ.

Формирование совокупности свойств объектов СКТЭ, ориентированных на задачу. Исходные материалы. Стандарты. Выбор методов исследования.

Раздельное исследование объектов СКТЭ. Выявление свойств (признаков) объектов СКТЭ, характеризующих товарную принадлежность. Оценка совокупности свойств исследуемых объектов СКТЭ в целях отнесения к конкретной товарной группе. Вывод о товарной принадлежности объектов СКТЭ.

Сравнительное исследование (сопоставление) классификационных свойств исследуемых объектов СКТЭ. Вывод о различии (сходстве) отдельных свойств или группы свойств исследуемых объектов СКТЭ.

Установление соответствия (несоответствия) товарных свойств исследуемых объектов стандартным и эталонным требованиям; базовым характеристикам, изложенным в договорах, контрактах и др. применительно к объектам СКТЭ

Документы: стандарты, контракты как исходные данные.

Вопросы, решаемые экспертом.

Методы исследования объектов СКТЭ.

Исследование объектов СКТЭ. Выявление свойств объектов. Анализ результатов исследования и их оценка. Вывод о товарной принадлежности объектов СКТЭ. Вывод о фактическом состоянии объектов СКТЭ. Сопоставление результатов исследования и исходных данных. Вывод о соответствии (несоответствии) товарных свойств исследуемых объектов СКТЭ базовым стандартным, эталонным данным, базовым характеристикам договоров, контрактов и т.д.

Установление наличия дефектов, их характера и влияния на качество изделий применительно к объектам СКТЭ.

Формирование программы исследования. Система методов научно-технических документов (далее - НТД) (стандарты, ТУ, ТО, сертификат качества), специальная литература.

Определение фактического состояния изделий. Выделение признаков повреждений объектов СКТЭ. Вывод (промежуточный) о наличии дефектов. Установление характера дефектов (сырьевой, производственный, эксплуатационный) в зависимости от типов негативных воздействий: механических, биологических, атмосферных и т.д. Вывод о причине возникновения дефектов.

Установление соответствия (несоответствия) отдельных свойств изделий стандартным и эталонным требованиям (базовым характеристикам). Вывод.

Оценка уровня качества (формирование совокупности показателей свойств (одного свойства) с точки зрения их влияния на качество). Вывод о степени снижения качества изделий и возможности дальнейшего использования.

Особенности производства судебно-товароведческой экспертизы по документам применительно к объектам СКТЭ.

Предмет и задачи судебно-товароведческой экспертизы применительно к объектам СКТЭ. Вопросы, решаемые экспертом при производстве экспертизы по документам.

Объекты исследования. Схема документообеспечения при решении задач судебно-товароведческой экспертизы.

Методы экспертного исследования (их особенности).

Программа проведения исследования. Осмотр документов. Установление достаточности данных. Заявление ходатайства о предоставлении недостающих материалов. Установление пригодности материалов для исследования.

Установление соблюдения (несоблюдения) правил исследования. Выводы.

Установление соответствия (несоответствия) качества объектов СКТЭ базовым данным (требованиям НТД, контрактов, сертификатов). Вывод.

Установление уровня качества (снижение, порча объекта СКТЭ). Выводы.

Установление соответствия (несоответствия) условий упаковки, маркировки, транспортировки, хранения нормативным требованиям. Выводы.

Определение возможности влияния различных факторов на снижение качества объектов СКТЭ. Выводы.

Товароведческие исследования с целью определения стоимости изделий применительно к объектам СКТЭ.

Законодательное обеспечение оценочной деятельности в Российской Федерации. Характеристика нормативных-правовых актов, регулирующих оценочную деятельность.

Виды стоимости.

Цель проведения оценки. Понятие рыночной цены. Виды стоимости объекта, отличные от рыночной стоимости.

Особенности проведения оценки в уголовном, гражданском, арбитражном процессах и в производстве по делам об административных правонарушениях.

Основные факторы, влияющие на величину стоимости объекта.

Понятие аналога объекта оценки. Основные принципы отбора объектов –аналогов. Корректировка цен аналогов с учетом фактических параметров. Источники информации, их достоверность (надежность). Достаточность информации. Конъюнктура рынка (соотношение спроса и предложения на аналогичные объекты).

Этапы проведения оценки.

Установление товарных характеристик объекта СКТЭ. Выбор метода оценки. Анализ рынка, к которому относится объект оценки. Выбор аналога. Установление фактического состояния объекта СКТЭ. Виды износа (физический и моральный).

Литература: [25-29].

II. Специальная часть

Способы и следы негативного воздействия на компьютерную информацию

Тема 1. Объективное и субъективное негативное воздействие на информацию

Понятие намеренного субъективного негативного воздействия на информацию. Способы и средства преднамеренного негативного воздействия на компьютерную информацию. Использование системного и прикладного ПО в деструктивных целях. Вредоносные программы. Меры, способы и средства защиты компьютерной информации, их классификация.

Тема 2. Основы следообразования в сфере компьютерной информации

Природа информационных следов и их классификация. Способы сокрытия следов неправомерного воздействия на информацию.

Литература: [10, 12, 16, 19, 21, 23, 24, 30, 32, 33].

5. Методики судебно-экспертного исследования компьютерной информации

Тема 1. Установление факта и параметров подключения внешних устройств к базовому комплекту

Особенности аппаратного и программного подключения внешних устройств. Программные следы подключения и использования внешних устройств. Эмуляция работы устройств внешней памяти.

Тема 2. Анализ состояния компьютерных систем, установление факта и параметров воздействия на систему

Диагностика установленного ПО. Определение назначения установленного ПО. Определение способа установки прикладного ПО в данной компьютерной системе. Анализ информационных процессов в компьютерных системах по служебным файлам данных.

Тема 3. Поиск и восстановление информации в файловых системах

Принципы поиска информации в файловых системах, Восстановление логической структуры файловой системы. Восстановление удалённых файлов в различных файловых системах. Утилиты восстановления информации: Unerase, Undelete, Easy Recovery, Tiramisu— алгоритм работы, описание применения, особенности использования, основные возможности. Поиск информации на нижнем логическом уровне. Создание инструментария для исследования файловых систем. Использование ядра Linux для неразрушающего чтения информации с NTFS и NWFS. Применение экспертных систем и нечеткой логики для восстановления логической структуры. Определение форматов файлов данных по их заголовкам, источника их происхождения и основных характеристик файлов.

Тема 4. Способы преодоления программной защиты информации

Основы криптоанализа и подбора паролей. Понятие уязвимости. Использование уязвимостей сетевых сервисов для вторжения в систему. Использование отладчиков и декомпиляторов для снятия программной защиты. Клавиатурные шпионы. Способы установления удаленного администрирования. Атаки вида «Отказ в обслуживании». Ресурсы по безопасности в сети Интернет.

Тема 5. Исследование специализированных ЭВМ

Общие сведения о составе, конструкции и классификации специализированных электронных вычислительных машин: контрольно-кассовые машины, микрокалькуляторы и т.д.

Общие сведения о принципах действия специализированных ЭВМ.

Основные методы и методики исследования специализированных ЭВМ.

Тема 6. Исследования в области информационных технологий

Общие сведения о современном состоянии, тенденциях развития и классификации объектов исследования в области информационных технологий.

Основные методы и методики исследования объектов в области информационных технологий.

Литература: [8, 13, 14, 20, 23, 24, 28, 30, 33].

III. Методические рекомендации

В процессе самостоятельной подготовки для изучения вопросов, предусмотренных программой, эксперты должны ознакомиться с рекомендуемой литературой, экспертной практикой отдела, представить заключение эксперта (не менее 5).

Общая часть

По разделу 1

Изучение тем этого раздела предполагает освоение основ государственной экспертной деятельности - Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации», Уголовно-процессуального кодекса Российской Федерации, Гражданского процессуального кодекса Российской Федерации, Арбитражного процессуального кодекса Российской Федерации, Кодекса Российской Федерации об административных правонарушениях, Таможенного кодекса Российской Федерации, Налогового кодекса Российской Федерации, знание федеральных законов, касающихся экспертной деятельности, а также нормативных правовых актов Минюста России, регулирующих организацию и производство судебной экспертизы.

Наряду с изучением правовых основ судебно-экспертной деятельности необходимо уяснить основные принципы построения методических схем решения задач экспертизы. При этом следует обратить внимание на многоступенчатый характер процесса исследования при решении классификационных, диагностических и идентификационных задач. Для каждого вида (типа) конкретной задачи необходимо проанализировать систему промежуточных задач, комплекс методов исследования; определить последовательность их применения.

Особое внимание следует уделить изучению требований нормативных актов, предъявляемых к заключению эксперта как источнику доказательств, критериев оценки заключения эксперта, а также правилам обращения с вещественными доказательствами.

По разделу 2

При изучении тем данного раздела особое внимание следует обратить на теоретические вопросы СКТЭ и их связь с практической деятельностью, пределы компетенции эксперта, круг исследуемых объектов, уяснить специфику предмета СКТЭ, обусловленную характером решаемых задач, спецификой свойств объектов исследования и методами, применяемыми для изучения этих свойств. При изучении правовых вопросов следует обратить внимание на новое российское законодательство, регулирующее вопросы судебной экспертизы, а также ведомственные нормативные-правовые акты.

Кроме того, необходимо более детально изучить и освоить на практике следующие разделы:

Тема 5

Устройство и назначение компонентов системного блока. Шины, контроллеры, устройства. Основные функции BIOS. Содержание Setup BIOS. Подключение и отключение внешних устройств. Получение информации о параметрах системных устройств. Влияние настроек BIOS на производительность системы. Порядок добавления устройств в операционную систему с использованием технологии Plug&Play и без неё. Перекомпиляция ядра системы с монолитным ядром. Изменение порядка просмотра самозагружаемых устройств.

Тема 6

Форматирование разделов под разные файловые системы. Поиск файлов в различных файловых системах средствами ОС GNU/Linux по имени и содержимому. Использование низкоуровневых средств, шестнадцатеричных редакторов и специальных программ для исследования

файловых систем. Работа в ОС GNU/Linux с различными файловыми системами, исследование исходного текста драйверов файловых систем.

Тема 7

Практические основы Ethernet. Назначение сетевых устройств, соединительные разъёмы. Алгоритмы работы сетей CSMA/CD, коллизии. Анализ эффективности работы сети. Использование сниффера Ethernet. Анализаторы пакетов. Обращение к адресам ресурсов по протоколу TCP/IP на примере Intranet. Работа с Http и Ftp протоколами. Предоставление и использование сетевых ресурсов для одноранговых сетей и сетей с выделенным сервером. Основы администрирования пользователей и предоставление прав на различные виды доступа в сетях с выделенным сервером.

Тема 8

Конфигурирование Windows. Реестр Windows. Обеспечение автозапуска программ под Windows при старте системы. Настройки аппаратной части системы: даты и времени, клавиатуры, мыши, параметров сети. Установка принтера. Формирование паролей пользователей. Доступ к удалению инсталлированных программ. Аппаратная настройка видеосистемы. Просмотр параметров основных системных устройств. Изменения в файлах сетевых протоколов, а также каталога ROOT\Windows\Temporary Internet Files после осуществления сеансов связи. Изменение в каталоге ROOT\Windows\Recent после открытия файлов с зарегистрированными типами данных. Создание bat-файлов.

Конфигурирование *NIX-подобных операционных систем на примере GNU\Linux и FreeBSD. Права пользователей. Ошибки в аппаратных компонентах и реакция на них ОС и прикладных программ, основы диагностики аппаратной части.

Система безопасности Windows NT. Службы каталогов Active Directory. Создание и исследование резервных копий.

Дамп исполняемых файлов. Инструментарий для анализа файлов данных. Заголовки графических файлов (bmp, tiff, gif), структура файлов html. Структура doc, rtf, xls, mdb, dbf - файлов. Анализ служебной информации. Изучение кодовых таблиц MS DOS (CP 866) и Windows (CP 1251). Иные кодировки - koi8, unicode. Просмотр различных кодировок.

Не-Windows системы. Анализ форматов файлов под различными ОС. Структура и анализ файла подкачки Windows (swp). Структура swap-разделов различных операционных систем. Создание архивов. Структура архивов. Современные программы сжатия информации.

Тема 9

Установка паролей на архивы, шифрование файлов данных. Установка прав доступа и уровня приоритета в сети. Использование специального программного обеспечения для защиты данных на локальном уровне в ОС, не обладающих собственными средствами и на ОС, не поддерживающей данную функцию (Invisible Files 2000, File Protection), достоинства и недостатки данного способа, создание виртуальных защищенных дисков.

Тема 10

Понятие ассемблера. CISC и RISC. Современные компиляторы. Язык С как основное средство для написания ядра ОС. Изучение исходных текстов операционных систем.

Основы объектно-ориентированного языка VB. Простейшие линейные программы. Использование классов для управления представлением форм. Использование классов для работы с файловой системой и сложными стандартными форматами файлов. Написание низкоуровневых программ.

Семейство Microsoft Office на языке VBA. Создание макросов на VB для файлов «офисов»: управление представлением данных в документе, автоматическое редактирование текста документа, размножение и рассылка документов.

Получение системной информации из реестра Windows: чтение login-ов, структуры диска, поиск и копирование системных файлов (pwl, dat), HTML, XML. Управление представлением информации.

Языки сценариев, использование сценариев для автоматизации повторяющихся задач. ActiveX scripting, VBScript, Jscript, Per!, Python. Java и ActiveX, их использование в WWW.

По разделу 3

Верное решение организационных вопросов назначения экспертизы является необходимым условием ее успешного проведения. Необходимо обратить внимание на порядок назначения комиссионной комплексной экспертизы, включения в комиссию экспертов разных специальностей; на взаимодействие эксперта с лицом (органом), назначающим экспертизу, при постановке вопросов,

отборе образцов и др; соблюдение процессуальных норм (в части заявления ходатайств, присутствия сторон и др.), а также на изучение вопросов о проведении экспертизы в суде и допрос эксперта.

При изучении тем 3 и 4 следует не только обратить внимание на основные положения и понятия материнской науки (товар, потребительские свойства, меновая стоимость, качество, уровень качества, факторы, влияющие на снижение качества товара, дефект и др.), но и проанализировать их практическое применение исходя из потребностей судебно - экспертной практики. Следует уяснить, что именно основы товароведения являются основой специальных познаний эксперта-товароведа и методологической базой экспертных товароведческих исследований.

Специальная часть

По разделу 1

При изучении тем данного раздела необходимо освоить способы и средства преднамеренного негативного воздействия на компьютерную информацию, вредоносные программы, меры, способы и средства защиты компьютерной информации.

По разделу 2

Необходимо более детально изучить и освоить на практике следующие темы:

Тема 1

Параметр реестра HKEY_LOCAL_MACHINE\Enum и его ключи. Поиск среди драйверов по названию и заголовкам файлов dll, drv, vxd, 386. Поиск аналогичных следов в других операционных системах.

Тема 2

Параметр реестра HKEY_LOCAL_MACHINE\Software - для определения ПО, которое когда-либо устанавливалось. Параметр реестра HKEY_LOCAL_MACHINE\System - для определения системных параметров компьютера. Определение формата файлов по фрагментам, куда входит заголовок. Исследование служебных файлов (pwl, log, err, swp, ini, tmp, wbm) на предмет установления действий, совершавшихся с файловой системой и обстоятельств создания документов.

Тема 3

Поиск информации в различных кодировках (CP 866 и CP 1251) средствами NC, FF, WindowsExplorer. Использование для эффективного поиска специальных средств поиска. Работа с файловой системой FAT. Восстановление удаленной информации средствами Unerase, Undelete.

Восстановление информации специальными средствами: Easy Recovery, Tiramisu. Внесение изменений в файловую систему на нижнем логическом уровне. Восстановление работоспособности файловой системы средствами Scandisk и NDD. Другие файловые системы с точки зрения восстановления удалённой информации. Восстановление сбойных разделов. Нарушения логической структуры.

Прямой поиск информации в кластерах с учетом кодировки и шифрования. Создание специальных средств доступа к иным файловым системам из ОС GNU\Linux. Средства просмотра NTFS и FS Novell.

Тема 4

Криптование и декриптование содержимого файлов. Использование стандартных средств и алгоритмов.

Использование стандартных средств для вскрытия сетевых паролей Windows, содержащихся в файлах pwl. Получение паролей на доступ к компьютерам через сеть. Использование средств удаленного администрирования. «Взлом» паролей различных многопользовательских ОС. Подбор паролей для типов файлов: doc, xls, arj, rar. Стандартные пароли для BIOS.

IV. Список литературы

1. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации».

2. Федеральный закон от 20.02.1995 N 24-ФЗ «Об информации, информатизации и защите информации».

3. Федеральный закон от 09.07.1993 № 5351-1 «Об авторском праве и смежных правах».

4. Федеральный закон от 24.12.2002 № 177-ФЗ «О правовой охране программ для электронных вычислительных машин и баз данных».

5. Федеральный закон от 23. 09. 1992 № 3526-1 «О правовой охране топологий интегральных микросхем».

6. Федеральный закон от 10. 01. 2002 № 1-ФЗ «Об электронной подписи».

7. Федеральный закон от 19. 02. 1993 № 4524-1 «О федеральных органах правительственной связи и информации».

8. Аверьянова Т.В. Интеграция и дифференциация научных знаний как источники и основы новых методов судебной экспертизы. — М., 1994.

9. Альфред В. Ахо, Джон Э. Хопкрофт, Джеффри Д. Ульман. Структуры данных и алгоритмы. — М., 2000.

10.Вехов В.Б. Особенности расследования преступлений, совершаемых с использованием средств ЭВТ. — УМП.: 1996.

11.Джон Кларк Крейг, Джефф Уэбб. Visual Basic 6,0. Мастерская разработчика. — М., 2001.

12.Защита программного обеспечения. - М., 1992.

13.Зинин А.М., Майлис Н.П. Судебная экспертиза - М., 2002.

14.Зубаха В.С., Усов А.И., Саенко Г.В. и др. Общие положения по назначению и производству компьютерно-технической экспертизы (методические рекомендации).— М., 2001.

15.Карпова И.С. Теоретические и методологические основы судебно-товароведческой экспертизы: Автореф. канд. дис. – М.: РФЦСЭ при Минюсте России, 1997.

16.Компьютерная преступность и информационная безопасность / Под ред. А.П. Леонова. – Минск, 2000.

17.Компьютерные технологии в юридической деятельности / Под ред. Н.С. Полевого, В.В. Крылова. – М., 1994.

18.Криминалистика / Под ред. Р.С. Белкина. - М., 1999.

19.Крылов В.В. Информационные компьютерные преступления. — М., 1996.

20.Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический аспект. – Воронеж, 2001.

21.Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. — М., 2000.

22.Основы судебной экспертизы. Часть 1. Общая теория. / Кол-в авторов. - М., 1997.

23.Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие / Под ред. П.Г. Шурухнова. — М., 1999.

24.Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. - М., 2001.

25.Толмачева С.С. Производство судебно-товароведческой экспертизы по документам: Метод. письмо. – М.: ВНИИСЭ, 1984.

26.Толмачева С.С. Программа экспертного исследования решения типовой задачи о соответствии (несоответствии) фактических свойств изделий маркировочным данным // Экспресс-информация. – М.: ВНИИСЭ, 1991. – Вып. 4.

27.Толмачева С.С. Производство судебно-товароведческих экспертиз по уголовным и гражданским делам // Обзорная информация. – М.: РФЦСЭ при Минюсте России, 1995. – Вып. 1.

28.Толмачева С.С., Карпова И.С. Предмет, объект, задачи судебно-товароведческой экспертизы // Методическое пособие. – М.: РФЦСЭ при Минюсте России, 2002.

29.Толмачева С.С., Карпова И.С. Современные возможности судебно-товароведческой экспертизы // Обзорная информация. – М.: РФЦСЭ при Минюсте России, 1995. – Вып. 1.

30.Усов А.И. Основы методического обеспечения судебно-экспертного исследования компьютерных средств и систем. — М., 2002.

31.Фигурнов В.Э. IBM PC для пользователя. Изд. 7-е. — Уфа, 1997.

32.Щербаков А.Ю. Разрушающие программные воздействия. - М., 1993.

33.Щербаков А.Ю. Введение в теорию и практику компьютерной безопасности. — М., 2001.

34.Экслер А.Б. Архиваторы. - М.: 1992.

Дополнительная литература

35.Брассар Ж. Современная криптология. - М.: Полимед, 1999.

36.Бычкова С.П., Земляная Т.Б., Палий В.М., Черткова Т.Б., Шайдуллин Ф.Т. Судебно-техническая экспертиза документов. Особенная часть. Часть 2. - М., 1993.

37.Волеводз А.Г. Противодействие компьютерным преступлениям.- М.: ООО издательство «Юрлитинформ», 2002.

38.Гавриш Г. Практическое пособие по защите коммерческой тайны. – Симферополь: «Таврида», 1994.

39.Гамма Э., Хелм Р., Джонсон Р. Приемы объектно-ориентированного проектирования. - СПб.: Питер, 2000.

40.Доказывание в уголовном процессе: традиции и современность/ Под ред. В.А. Власихина.- М.: Юристъ, 2000.

41.Касперский Е. Компьютерные вирусы. Что это такое и как с ними бороться. - М.: «СкПресс», 1998.

42.Криминалистическое исследование документов, отпечатанных электрографическим способом. /Под ред. А.А. Гусева. - М.: ВНИИСЭ, 1985.

43.Комментарий к Уголовному кодексу Российской Федерации. / Под общ. редакцией Ю.И. Скуратова и В.М. Лебедева. - М.: НОРМА-ИНФРА-М, 1996.

44.Компьютерная преступность и информационная безопасность/ Под общ. ред. А.П. Леонова. - Мн.:АРИЛ, 2000.

45.Компьютерные технологии в юридической деятельности. /Под ред. Н.С. Полевого, В. В. Крылова. - М.: Бек, 1994.

46.Компьютерные технологии в юридической деятельности. Уч. пособ. -М.: ИнтерПракс, 1994.

47.Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. - М.: Новый Юрист, 1998.

48.Кучеренко В. Хитрости, трюки и секреты Visual Basic 5-6. - М.: Познавательная книга, 2000.

49.Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях (изд. 2-е). - СПб., 2001.

50.Палий В.М. Криминалистическое исследование документов, изготовленных на знакопечатающих устройствах. – Киев, 1989.

51.Рассолов М.М. Информационное право. Уч. пособ. М.: «Юристъ». 1999.

52.Толеубекова Б.Х. Криминалистическая характеристика компьютерных преступлений. – Караганда: Высшая школа МВД Республики Казахстан, 1993.

53.Черкасов В.Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. - Саратов: Высшая школа МВД России, 1995.

54.Усов А.И. Методы и средства решения компьютерно-технической экспертизы // Учебное пособие. – М.: ГУ ЭКЦ МВД России, 2002.

55.Нормативная литература по теме - машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования (с изменениями № 1, 2 и 3). Издание официальное. - М.: Издательство стандартов, 1989.

56.Общероссийский классификатор продукции. ОК 005-93. Том 1. Классы \-40. Издание официальное. - М.: ИПК Издательство стандартов, 2000.

57.Новый политехнический словарь. Гл. ред. А. Ю. Ишлинский. - М.: Большая Российская энциклопедия, 2000.

58.Корухов Ю.Г. Соотношение категорий экспертных задач: идентификационных, классификационных, диагностических // Актуальные проблемы теории судебных экспертиз: Сб. науч. тр. ВНИИСЭ. – М., 1984.

59.Методические рекомендации по формированию и применению свободных цен и тарифов на продукцию, товары и услуги (Минэкономики России от 06.12.1995г. № СИ 484/7982).

60.Мирский Д.Я. Некоторые теоретические вопросы классификации объектов судебной экспертизы // Методология судебной экспертизы: Сб. науч. тр. ВНИИСЭ. – М., 1986.

61.Постановление Правительства Российской Федерации от 19 января 1998 г. №55 «Об утверждении Правил продажи отдельных видов товаров, перечня товаров длительного пользования, на которые не распространяется требование покупателя о безвозмездном предоставлении ему на период ремонта или замены аналогичного товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих возврату или обмену на аналогичный товар других размера, формы, габарита, фасона, расцветки или комплектации» (с изм. от 20 октября 1998 г., 2 октября 1999 г., 6 февраля 2002 г.).

62.Постановление Правительства Российской Федерации от 27.03.95. №7 «О мерах по упорядочению государственного регулирования цен (тарифов)».

63.Степутенкова В.К. Проблемы комплексных экономических экспертиз // Мат-лы Всесоюз. науч.-практ. конф. «Проблемы организации и проведения комплексных экспертных исследований» (Рига, 1984). – М.: ВНИИСЭ, 1985.

64.Степутенкова В.К., Толмачева С.С. Судебно-товароведческая экспертиза – структурный элемент системы судебных экономических экспертиз: Мат-лы респ. науч. конф. – Вильнюс, 1986.

65.Степутенкова В.К., Толмачева С.С. К вопросу о предмете судебно-товароведческой экспертизы // Материалы Всесоюз. конф. «Актуальные проблемы теории и практики новых видов судебных экспертиз». – М.: ВНИИСЭ, 1989.

66.Толмачева С.С., Карпова И.С. Сборник комментированных заключений по судебно-товароведческой экспертизе. – М.: РФЦСЭ при Минюсте России, 1996.

Средства обучения

- Операционные системы MS DOS, Windows 9x, Windows NT, Windows 2000, Windows XP
- Пакет Norton Utilities 8.0 for DOS и 200x

- Программы-архиваторы WinRar, WinZip.
- Антивирусные программы AVP LITE, DrWeb
- Easy Recovery, Tiramisu
- NTFS98Pro
- Visual Basic
- Следопыт 2.0, Ищейка, AVSearch
- Remote Administrator
- Norton Ghost, PQ Drive Copy, Drive Image
- Encase, ILOOK Investigator, Vogon International, PC Data Finder
- File Investigator