

УТВЕРЖДЕНО

Решением Президиума Союза
лиц, осуществляющих
деятельность в сфере судебной
экспертизы и судебных
экспертных исследований
«Палата судебных экспертов
имени Ю.Г. Корухова»
(«СУДЭКС»)
Протокол № 138
от 18 ноября 2016 г.

УЧЕБНЫЙ ПЛАН

повышения квалификации судебных экспертов по специальности
«Исследование информационных компьютерных средств»¹

№ п/п	Наименование и темы занятий	Краткое содержание	Форма проведения занятий	Кол-во часов
1	Основы судебной экспертизы	Основные вопросы правового регулирования судебной экспертизы. Объекты судебной экспертизы. Права и обязанности судебного эксперта. Заключение судебной экспертизы. Классификация судебных экспертиз. Характеристика судебных экспертиз по классам, родам и видам. Судебно-экспертные учреждения России.	очная - лекции очно - заочная с использованием ДОТ ²	10
2	Криминалистические основы судебной экспертизы	Криминалистическая идентификация в экспертных исследованиях		8
3	Информационное обеспечение судебной экспертизы.	Проблемы автоматизации и информационного обеспечения в судебной экспертизе.		4
4	Математические методы в	Применение математических методов и		8

¹ Данный план разработан на основании программы подготовки экспертов по специальности 21.1 «Исследование информационных компьютерных средств», утвержденной приказом Минюста России от 13.10.2004 № 169

² самостоятельная работа слушателя по изучению рекомендованных и раздаточных материалов при постоянном консультировании и информационно - справочной поддержке преподавателя в дистанционном режиме

	судебной экспертизе	ЭВМ при решении задач судебной экспертизы.		
5	Процессуальные основы назначения и производства судебной компьютерно - технической экспертизы (СКТЭ)	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.	<p style="text-align: center;">очная - лекции</p> <hr style="width: 50%; margin: auto;"/> <p style="text-align: center;">очно - заочная с использованием ДОТ</p>	2
6	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.		2
7	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.		2
8	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).		2
9	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.		2

10	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.		2
11	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.	очная - лекции очно - заочная с использованием ДОТ	2
12	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.		2
13	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		2

		стол, Send To, Recent), структура файлов данных прикладных программ (обработки графической информации, офисных пакетов, архиваторов и т.д.).		
14	Программные способы защиты информации	Защита шифрованием, паролем, технология использования открытого ключа Хэши. Способы аутентификации. Программные продукты для защиты информации. Защита сетей: понятие межсетевое экрана и брандмауэра.	очная - лекции очно - заочная с использованием ДОТ	2
15	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.		2
16	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.		2
17	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.		2
18	Особенности исследования информационных	Предмет судебно-товароведческой экспертизы (далее - СТЭ). Основы		4

	компьютерных средств в рамках комплексной компьютерно-технической и товароведческой экспертизы (в соответствии с программой подготовки экспертов по специальности 19.1.)	товароведения.		
19	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. Установление наличия дефектов, их характера и влияния на качество изделий применительно к объектам СКТЭ. Особенности производства судебно-товароведческой экспертизы по документам применительно к объектам СКТЭ. Товароведческие исследования с целью определения стоимости изделий применительно к объектам СКТЭ.	очная - лекции очно - заочная с использованием ДОТ	2
20	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.		2
21	Основы слепообразования в сфере компьютерной информации	Природа информационных следов и их классификация. Способы сокрытия следов неправомерного воздействия на информацию.		2
22	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.		2
23	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.		2

24	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.	очная - лекции очно - заочная с использованием ДОТ	2
25	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.		2
26	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.		2
27	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.		2
28	Курсовая работа			8
29	Практическая работа по выполнению экспертного исследования		10	
30	Разбор, анализ и защита курсовой работы и практической работы		4	
31	Итоговый комплексный экзамен		4	
32	Общая трудоемкость дисциплины		104	

Генеральный директор
«СУДЭКС»

С.Е.Киселев