Бауманский учебный центр «Специалист»

Программа курса Расследование хакерских инцидентов. Основы форензики

Код курса: **CEH3**

Тема	Ак. часов
Модуль 1. Компьютерная криминалистика в современном мире • Что такое компьютерная криминалистика • Применение компьютерной криминалистики • Виды компьютерных преступлений • Case Study. Примеры расследования компьютерных преступлений • Сложности криминалистической экспертизы • Расследование киберпреступлений ◦ Гражданское расследование ◦ Уголовное расследование ◦ Административное расследование ◦ Case Study. Примеры типов расследований • Правила судебно-медицинской экспертизы • Расследование преступлений, совершенных организованными преступными группами (Enterprise Theory of Investigation) • Цифровые улики • Что такое цифровые улики • Типы цифровых улик • Характеристики цифровых улик • Роль цифровых улик • Источники потенциальных улик • Правила сбора доказательств ◦ Требование представления наилучших доказательств ◦ Кодекс доказательственного права ◦ Производные доказательства • Научная рабочая группа по цифровым уликам (SWGDE) • Готовность к криминалистическому расследованию • Компьютерная криминалистика как часть плана реагирования на инциденты • Необходимость компьютерной криминалистики • Роли и обязанности следователя судебной экспертизы • Проблемы криминалистического расследования ◦ Правовые вопросы ◦ Вопросы конфиденциальности • Правила этики • Ресурсы по компьютерной криминалистике **Лабораторная работа:** • Изучение основ расследования компьютерных преступлений • Подготовка лаборатории для практических экспериментов	**2**
Модуль 2. Процесс расследования компьютерных инцидентов • Важность процесса расследования • Фазы процесса расследования • Этап предварительного расследования ◦ Подготовка криминалистической лаборатории ◦ Построение следственной группы ◦ Обзор политик и законов ◦ Создание процессов обеспечения качества ◦ Знакомство со стандартами уничтожения данных ◦ Оценка риска • Этап расследования ◦ Процесс расследования ◦ Методология расследования: оперативное реагирование	

◦ Методология расследования: досмотр и изъятие ◦ Проведение предварительных интервью ◦ Планирование досмотра и изъятия ◦ Ордер на обыск и изъятие ◦ Вопросы здоровья и безопасности ◦ Защита и оценка сцены преступления: контрольный список • Методология расследования: сбор улик ◦ Сбор вещественных доказательств ◦ Форма сбора вещественных доказательств ◦ Сбор и сохранение электронных улик ◦ Работа с включенными компьютерами ◦ Работа с выключенными компьютерами ◦ Работа с сетевым компьютером ◦ Работа с открытыми файлами и файлами автозагрузки ◦ Процедура выключения операционной системы ◦ Работа с рабочими станциями и серверами ◦ Работа с портативными компьютерами ◦ Работа с включенными портативными компьютерами • Методология расследования: защита улик ◦ Управление уликами ◦ Порядок передачи и хранения улик ◦ Упаковка и транспортировка электронных улик ◦ Нумерация вещественных доказательств ◦ Хранение электронных вещественных доказательств • Методология расследования: сбор данных ◦ Руководство по сбору данных ◦ Дублирование данных ◦ Проверка целостности образа ◦ Восстановление данных • Методология расследования: анализ данных ◦ Процесс анализа данных ◦ Программное обеспечение для анализа данных • Этап после расследования • Методология расследования: оценка улик ◦ Оценка найденных доказательств ◦ Приобщение улик к делу ◦ Обработка оценки месторасположения ◦ Сбор данных из социальных сетей ◦ Рекомендации по исследованию социальных сетей ◦ Рекомендации по оценке улик • Методология расследования: документация и отчетность ◦ Документация по каждой фазе расследования ◦ Сбор и упорядочивание информации ◦ Написание отчета об исследовании • Методология расследования: экспертное свидетельствование ◦ Выступление в качестве эксперта-свидетеля ◦ Закрытие дела • Профессиональное поведение **Лабораторная работа:** • Изучение и практическое применение программных средств, необходимых в процессе криминалистического расследования	**2**

Модуль 3. Жесткие диски и файловые системы • Обзор жестких дисков ◦ Жесткие диски (HDD) ◦ Твердотельные накопители (SSD) ◦ Физическая структура жесткого диска ◦ Логическая структура жесткого диска ◦ Типы интерфейсов жестких дисков ◦ Интерфейсы жестких дисков ◦ Треки ◦ Секторы ◦ Кластеры ◦ Плохие секторы ◦ Бит, байт и полубайт ◦ Адресация данных на жестком диске ◦ Плотность данных на жестком диске ◦ Расчет емкости диска ◦ Измерение производительности жесткого диска • Разделы диска и процесс загрузки ◦ Дисковые разделы ◦ Блок параметров BIOS ◦ Главная загрузочная запись (MBR) ◦ Глобальный уникальный идентификатор (GUID) ◦ Что такое процесс загрузки? ◦ Основные системные файлы Windows ◦ Процесс загрузки Windows ◦ Идентификация таблицы разделов GUID ◦ Анализ заголовка и записей GPT ◦ Артефакты GPT ◦ Процесс загрузки Macintosh ◦ Процесс загрузки Linux • Файловые системы ◦ Общие сведения о файловых системах ◦ Типы файловых систем ◦ Файловые системы Windows ◦ Файловые системы Linux ◦ Файловые системы Mac OS X ◦ Файловая система Oracle Solaris 11: ZFS ◦ Файловая система CD-ROM / DVD ◦ Файловая система компакт-дисков (CDFS) ◦ Виртуальная файловая система (VFS) ◦ Файловая система универсального диска (UDF) • Система хранения RAID ◦ Уровни RAID ◦ Защищенные области хоста (HPA) • Анализ файловой системы ◦ Выделение однородных массивов данных ◦ Анализ файла изображения (JPEG, BMP, шестнадцатеричный вид форматов файлов изображений) ◦ Анализ файла PDF ◦ Анализ файлов Word ◦ Анализ файлов PPT ◦ Анализ файлов Excel ◦ Шестнадцатеричный вид популярных форматов файлов (видео, аудио) ◦ Анализ файловой системы с использованием Autopsy ◦ Анализ файловой системы с использованием The Sleuth Kit (TSK) **Лабораторная работа:** • Восстановление удаленных файлов • Анализ файловых систем	**4**

Модуль 4. Сбор и дублирование данных • Концепции сбора и дублирования данных ◦ Общие сведения о сборе данных ▪ Типы систем сбора данных • Получение данных в реальном времени ◦ Порядок волатильности ◦ Типичные ошибки при сборе изменчивых данных ◦ Методология сбора изменчивых данных • Получение статических данных ◦ Статические данные ◦ Эмпирические правила ◦ Дубликаты образов ◦ Побитовая копия и резервная копия ◦ Проблемы с копированием данных ◦ Шаги по сбору и дублированию данных ▪ Подготовка формы передачи улик ▪ Включение защиты от записи на носителях уликах ▪ Подготовка целевого носителя: руководство NIST SP 800-88 ▪ Определение формата сбора данных ▪ Методы сбора данных ▪ Определение лучшего метода сбора данных ▪ Выбор инструмента для сбора данных ▪ Сбор данных с RAID-дисков ▪ Удаленное получение данных ▪ Ошибки при сборе данных ▪ Планирование нештатных ситуаций • Рекомендации по сбору данных **Лабораторная работа:** • Применение программных средств для извлечений данных с жестких дисков	**2**

Модуль 5. Техники, затрудняющие криминалистическую экспертизу • Что такое антифорензика? ◦ Цели антифорензики • Техники антифорензики ◦ Удаление данных / файлов ▪ Что происходит при удалении файла в Windows? ◦ Корзина Windows ▪ Место хранения корзины в FAT и NTFS-системах ▪ Как работает корзина ▪ Повреждение файла INFO2 ▪ Повреждение файлов в корзине ▪ Повреждение каталога корзины ◦ Восстановление файлов ▪ Средства восстановления файлов в Windows ▪ Средства восстановления файлов в MAC OS X ▪ Восстановление файлов в Linux ▪ Восстановление удаленных разделов ◦ Защита паролем ▪ Типы паролей ▪ Работа взломщика паролей ▪ Техники взлома паролей ▪ Пароли по умолчанию ▪ Использование радужных таблиц для взлома хэшей ▪ Аутентификация Microsoft ▪ Взлом системных паролей ▪ Обход паролей BIOS ▪ Инструменты для сброса пароля администратора ▪ Инструменты для взлома паролей приложений ▪ Инструменты для взлома системных паролей ◦ Стеганография и стеганализ ◦ Скрытие данных в структурах файловой системы ◦ Обфускация следов ◦ Стирание артефактов ◦ Перезапись данных и метаданных ◦ Шифрование ▪ Шифрующая файловая система (EFS) ▪ Инструменты восстановления данных EFS ◦ Шифрованные сетевые протоколы ◦ Упаковщики ◦ Руткиты ▪ Обнаружение руткитов ▪ Шаги для обнаружения руткитов ◦ Минимизация следов ◦ Эксплуатация ошибок криминалистических инструментов ◦ Детектирование криминалистических инструментов • Меры противодействия антифорензике • Инструменты, затрудняющие криминалистическую экспертизу **Лабораторная работа:** • Применение программных средств для взлома паролей приложений • Обнаружение стеганографии	**2**
Модуль 6. Криминалистическая экспертиза операционных систем • Введение в криминалистическую экспертизу ОС • Криминалистическая экспертиза WINDOWS • Методология криминалистической экспертизы Windows ◦ Сбор энергозависимой информации ▪ Системное время ▪ Зарегистрированные пользователи ▪ Открытые файлы ▪ Информация о сети ▪ Сетевые подключения ▪ Информация о процессах	

- Сопоставление процессов и портов
- Память процесса
- Состояние сети
- Файлы очереди печати
- Другая важная информация

- Сбор энергонезависимой информации
  - Файловые системы
  - Настройки реестра
  - Идентификаторы безопасности (SID)
  - Журналы событий
  - Файл базы данных ESE
  - Подключенные устройства
  - Slack Space
  - Виртуальная память
  - Файлы гибернации
  - Файл подкачки
  - Поисковый индекс
  - Поиск скрытых разделов
  - Скрытые альтернативные потоки
  - Другая энергонезависимая информация
- Анализ памяти Windows
  - Виртуальные жесткие диски (VHD)
  - Дамп памяти
  - Структура EProcess
  - Механизм создания процесса
  - Анализ содержимого памяти
  - Анализ памяти процесса
  - Извлечение образа процесса
  - Сбор содержимого из памяти процесса
- Анализ реестра Windows
  - Устройство реестра
  - Структура реестра
  - Реестр как файл журнала
  - Анализ реестра
  - Системная информация
  - Информация о часовом поясе
  - Общие папки
  - Беспроводные идентификаторы SSID
  - Служба теневого копирования томов
  - Загрузка системы
  - Вход пользователя
  - Активность пользователя
  - Ключи реестра автозагрузки
  - USB устройства
  - Монтируемые устройства
  - Отслеживание активности пользователей
  - Ключи UserAssist
  - Списки MRU
  - Подключение к другим системам
  - Анализ точек восстановления
  - Определение мест запуска
- Кэш, Cookie и анализ истории
  - Mozilla Firefox
  - Google Chrome
  - Microsoft Edge и Internet Explorer
- Анализ файлов Windows
  - Точки восстановления системы
  - Prefetch файлы
  - Ярлыки
  - Файлы изображений
- Исследование метаданных
  - Что такое метаданные
  - Типы метаданных
  - Метаданные в разных файловых системах
  - Метаданные в файлах PDF
  - Метаданные в документах Word

4

        - Инструменты анализа метаданных
    - Журналы
        - Что такое события
        - Типы событий входа в систему
        - Формат файла журнала событий
        - Организация записей событий
        - Структура ELF_LOGFILE_HEADER
        - Структура записи журнала
        - Журналы событий Windows 10
        - Криминалистический анализ журналов событий
    - Инструменты криминалистического анализа Windows
- Криминалистическая экспертиза LINUX
    - Команды оболочки
    - Файлы журнала Linux
    - Сбор энергозависимых данных
    - Сбор энергонезависимых данных
    - Область подкачки
- Криминалистическая экспертиза MAC
    - Введение в криминалистическую экспертизу MAC
    - Данные для криминалистического исследования MAC
    - Файлы журнала
    - Каталоги
    - Инструменты криминалистического анализа MAC

Лабораторная работа:

- Обнаружение и извлечение материалов для анализа с помощью OSForensics
- Извлечение информации о запущенных процессах с помощью Process Explorer
- Анализ событий с помощью Event Log Explorer
- Выполнение криминалистического исследования с использованием Helix
- Сбор энергозависимых данных в Linux
- Анализ энергонезависимых данных в Linux

Модуль 7. Сетевые расследования, логи и дампы сетевого трафика • Введение в сетевую криминалистику ◦ Что такое сетевая криминалистика ◦ Анализ по журналам и в реальном времени ◦ Сетевые уязвимости ◦ Сетевые атаки ◦ Где искать доказательства • Основные понятия ведения журналов ◦ Лог-файлы как доказательство ◦ Законы и нормативные акты ◦ Законность использования журналов ◦ Записи о регулярно проводимой деятельности в качестве доказательства • Корреляция событий ◦ Что такое корреляция событий ◦ Типы корреляции событий ◦ Пререквизиты для корреляции событий ◦ Подходы к корреляции событий ◦ Обеспечение точности лог-файлов ◦ Записывать все ◦ Сохранение времени ◦ Зачем синхронизировать время компьютеров? ◦ Что такое протокол сетевого времени (NTP)? ◦ Использование нескольких датчиков ◦ Не терять журналы • Управления журналами ◦ Функции инфраструктуры управления журналами ◦ Проблемы с управлением журналами ◦ Решение задач управления журналами ◦ Централизованное ведение журнала ◦ Протокол Syslog ◦ Обеспечение целостности системы ◦ Контроль доступа к журналам ◦ Цифровая подпись, шифрование и контрольные суммы • Анализ журналов ◦ Механизм сетевого криминалистического анализа ◦ Средства сбора и анализа журналов ◦ Анализ журналов маршрутизатора ◦ Сбор информации из таблицы ARP ◦ Анализ журналов брандмауэра ◦ Анализ журналов IDS ◦ Анализ журналов Honeypot ◦ Анализ журналов DHCP ◦ Анализ журнала ODBC • Исследование сетевого трафика ◦ Зачем изучать сетевой трафик? ◦ Сбор улик посредством сниффинга ◦ Wireshark – сниффер N1 ◦ Анализаторы сетевых пакетов • Анализ журналов IDS • Документирование сетевых улик • Реконструкция улик **Лабораторная работа:** • Сбор и анализ журналов с помощью GFI EventsManager • Исследование данных системного журнала с помощью XpoLog Center Suite • Расследование сетевых атак с помощью Kiwi Log Viewer • Исследование сетевого трафика с помощью Wireshark	**4**

Модуль 8. Расследование взлома веб-серверов • Введение в криминалистическую экспертизу веб-приложений ◦ Архитектура веб-приложений ◦ Проблемы криминалистического расследования веб-приложений • Расследование веб-атак ◦ Симптомы атаки на веб-приложение ◦ Обзор угроз для веб-приложений ◦ Исследование веб-атак • Исследование журналов веб-серверов ◦ IIS ◦ Apache • Расследование атак с использованием межсайтовых сценариев (XSS) • Расследование атак с использованием SQL-инъекций • Расследование атак с подделкой межсайтовых запросов (CSRF) • Расследование атак на инъекцию кода • Расследование атак с отравлением Cookies • Средства обнаружения веб-атак **Лабораторная работа:** • Анализ доменов и IP адресов • Расследование атаки на веб-сервер	**2**
Модуль 9. Расследование взлома серверов баз данных • Криминалистическая экспертиза систем управления базами данных (СУБД) • Криминалистическая экспертиза MSSQL ◦ Хранение данных в SQL сервере ◦ Где можно найти улики в СУБД ◦ Сбор энергозависимых данных ◦ Файлы данных и журналы активных транзакций ◦ Сбор журналов активных транзакций ◦ Кэш планов баз данных ◦ События SQL сервера в журналах Windows ◦ Файлы трассировки SQL сервера ◦ Журналы ошибок SQL сервера ◦ Инструменты криминалистической экспертизы MS SQL • Криминалистическая экспертиза MySQL ◦ Архитектура MySQL ◦ Структура каталога данных ◦ Криминалистическая экспертиза MySQL ◦ Просмотр информационной схемы ◦ Инструменты криминалистической экспертизы MySQL • Примеры криминалистического анализа MySQL **Лабораторная работа:** • Извлечение баз данных с Android устройства с использованием Andriller • Анализ баз данных SQLite с использованием DB Browser for SQLite • Выполнение криминалистического анализа базы данных MySQL	**2**

Модуль 10. Расследование облачных технологий • Концепции облачных вычислений ◦ Типы облачных вычислений ◦ Разделение ответственности в облаке ◦ Модели облачного развертывания ◦ Угрозы облачных технологий ◦ Атаки на облачные решения • Облачная криминалистика • Преступления в облаке ◦ Case Study: облако как субъект ◦ Case Study: облако как объект ◦ Case Study: облако как инструмент • Облачная криминалистика: заинтересованные стороны и их роли • Проблемы криминалистической экспертизы в облаке ◦ Архитектура и идентификация ◦ Сбор данных ◦ Журналы ◦ Юридические аспекты ◦ Анализ ◦ Категории проблем криминалистической экспертизы • Исследование облачных хранилищ • Криминалистическое расследование службы Dropbox ◦ Артефакты веб-портала Dropbox ◦ Артефакты клиента Dropbox в Windows • Криминалистическое расследование службы Google Диска ◦ Артефакты веб-портала Google Drive ◦ Артефакты клиента Google Диска в Windows • Инструменты криминалистической экспертизы облачных вычислений **Лабораторная работа:** • Криминалистический анализ DropBox • Криминалистический анализ Google Drive	**2**

Модуль 11. Расследование зловредного программного обеспечения • Концепции вредоносного ПО ◦ Типы вредоносного ПО ◦ азличные способы проникновения вредоносного ПО в систему ◦ Обычные методы, используемые злоумышленниками для распространения вредоносного ПО в Интернете ◦ Компоненты вредоносного ПО • Криминалистическая экспертиза вредоносных программ ◦ Зачем анализировать вредоносное ПО ◦ Идентификация и извлечение вредоносных программ ◦ Лаборатория для анализа вредоносных программ ◦ Подготовка тестового стенда для анализа вредоносных программ • Инструменты для анализа вредоносных программ • Общие правила анализа вредоносных программ • Организационные вопросы анализа вредоносных программ • Типы анализа вредоносных программ • Статический анализ ◦ Статический анализ вредоносных программ: отпечатки файлов ◦ Онлайн-службы анализа вредоносных программ ◦ Локальное и сетевое сканирование вредоносных программ ◦ Выполнение поиска строк ◦ Определение методов упаковки / обфускации ◦ Поиск информации о переносимых исполняемых файлах (PE) ◦ Определение зависимостей файлов ◦ Дизассемблирование вредоносных программ ◦ Средства анализа вредоносных программ • Динамический анализ ◦ Мониторинг процессов ◦ Мониторинг файлов и папок ◦ Мониторинг реестра ◦ Мониторинг активности сети ◦ Мониторинг портов ◦ Мониторинг DNS ◦ Мониторинг вызовов API ◦ Мониторинг драйверов устройств ◦ Мониторинг программ автозагрузки ◦ Мониторинг служб Windows • Анализ вредоносных документов • Проблемы анализа вредоносных программ **Лабораторная работа:** • Выполнение статического анализа подозрительного файла • Динамический анализ вредоносного ПО • Анализ вредоносного PDF файла • Сканирование PDF файлов с использованием сетевых ресурсов • Сканирование подозрительных офисных документов	**4**

Модуль 12. Криминалистическая экспертиза электронной почты • Система электронной почты ◦ Почтовые клиенты ◦ Сервер электронной почты ◦ SMTP сервер ◦ POP3 сервер ◦ IMAP сервер ◦ Важность управления электронными документами • Преступления, связанные с электронной почтой ◦ Спам ◦ Взлом почты ◦ Почтовый шторм ◦ Фишинг ◦ Подмена электронной почты ◦ Противозаконные сообщения ◦ Мошенничество с идентификационной информацией ◦ Письма счастья ◦ Криминальная хроника • Сообщение электронной почты ◦ Заголовки сообщения электронной почты ◦ Список типичных почтовых заголовков • Шаги по расследованию преступлений, связанных с электронной почтой 1. Получение разрешения на досмотр, изъятие и расследование 2. Исследование сообщений электронной почты 3. Копирование сообщений электронной почты 4. Просмотр заголовков сообщений ▪ в Microsoft Outlook ▪ в AOL ▪ в Apple Mail ▪ в Gmail ▪ в Yahoo Mail 5. Анализ заголовков сообщений электронной почты ▪ Проверка дополнительных файлов (.pst / .ost) ▪ Проверка валидности электронной почты ▪ Исследование IP адресов 6. Отслеживание происхождения электронной почты ▪ Проверка информации заголовка ▪ Отслеживание веб-почты 7. Сбор архивов электронной почты ▪ Архивы электронной почты ▪ Содержание архивов электронной почты ▪ Локальный архив ▪ Архив сервера ▪ Восстановление удаленных электронных писем 8. Исследование журналов электронной почты ▪ Журналы сервера электронной почты Linux ▪ >Журналы сервера электронной почты Microsoft Exchange ▪ Журналы сервера электронной почты Novell • Инструменты криминалистической экспертизы • Законы о преступлениях связанных с электронной почтой **Лабораторная работа:** • Восстановление удаленной электронной почты с помощью Recover My Email • Исследование кибер преступления с помощью Paraben Email Examiner • Трассировка электронного сообщения с помощью eMailTrackerPro	**2**

Модуль 13. Расследование взлома мобильных устройств • Криминалистическая экспертиза мобильных устройств 1. Необходимость криминалистической экспертизы 2. Основные угрозы для мобильных устройств • Мобильные устройства и криминалистика • Мобильные ОС и криминалистика 1. Архитектурные уровни мобильных устройств 2. Архитектурный стек Android 3. Процесс загрузки Android 4. Архитектура iOS 5. Процесс загрузки iOS 6. Загрузка в обычном режиме и в режиме DFU 7. Загрузка iPhone в режиме DFU 8. Мобильное хранилище и места для улик • Что нужно сделать перед расследованием? 1. Подготовить рабочую станцию для криминалистической экспертизы 2. Построить следственную команду 3. Учесть политики и законы 4. Получить разрешение на исследование 5. Оценить риски 6. Создать набор инструментов для криминалистической экспертизы • Анализ улик мобильного телефона • Процесс криминалистической экспертизы мобильных устройств 1. Сбор улик 2. Документирование сцены преступления ▪ Документирование улик ▪ Сохранение улик ▪ Набор правил обращения с мобильным телефоном ▪ Сдерживание сигнала мобильного телефона ▪ Упаковка, транспортировка и хранение доказательств 3. Снятие образа ▪ Средства создание образа диска мобильных устройств ▪ Обход блокировки телефона ▪ Обход пароля блокировки телефона Android ▪ Обход кода iPhone ▪ Включение USB отладки ▪ Техники снятия защиты платформы 4. Сбор и анализ информации ▪ Сбор улик с мобильных устройств ▪ Методы сбора данных ▪ Сотовая сеть ▪ Модуль идентификации абонента (SIM) ▪ Логический сбор данных ▪ Физический сбор данных ▪ Выделение однородных массивов данных ▪ Извлечение базы данных SQLite ▪ Инструменты сбора данных с мобильных устройств 5. Создание отчета о расследовании ▪ Шаблон отчета об исследовании мобильного устройства **Лабораторная работа:** • Криминалистический анализ образа мобильного устройства и извлечение удаленных файлов с помощью Autopsy • Исследование Android устройства с помощью Andriller	**2**

Модуль 14. Подготовка отчета о расследовании • Подготовка отчета об исследовании ◦ Отчет о криминалистическом исследовании ◦ Важные аспекты хорошего отчета ◦ Шаблон отчета криминалистической экспертизы ◦ Классификация отчетов ◦ Руководство по написанию отчета ◦ Рекомендации по написанию отчета • Показания эксперта-свидетеля ◦ Кто такой «Эксперт-свидетель»? ◦ Роль эксперта-свидетеля ◦ Технический свидетель и эксперт-свидетель ◦ Стандарт Дьюберта ◦ Стандарт Фрайе ◦ Правила хорошего эксперта-свидетеля ◦ Важность резюме ◦ Профессиональный кодекс свидетеля-эксперта ◦ Подготовка к даче свидетельских показаний • Свидетельство в суде ◦ Общий порядок судебных разбирательств ◦ Общая этика при свидетельстве ◦ Значение графики в показаниях ◦ Как избежать проблем с показаниями ◦ Свидетельствование во время прямой экспертизы ◦ Свидетельствование во время перекрестного допроса ◦ Показания, приобщенные к материалам дела • Работа со СМИ **Практическая работа:** • Составление отчета о расследовании инцидента	**2**
Модуль 15. Обзор изменений в 10 версии курса	
Модуль 16. Итоговая контрольная работа	**4**
Аудиторная нагрузка в классе с преподавателем	**40 ак.ч. + 40 ак.ч. самостоятельно**

По окончании обучения на курсе проводится итоговая аттестация. Аттестация проводится в виде теста на последнем занятии или на основании оценок практических работ, выполняемых во время обучения на курсе.

Контакты центра

Для частных лиц
+7 (495) 232-32-16

Для организаций
+7 (495) 780-48-44

E-mail
info@specialist.ru