**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ имени И.Т. ТРУБИЛИНА»**

Юридический факультет

Кафедра криминалистики

**КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

**Методические указания**

для организации контактной работы собучающимися по

направлению подготовки 40.04.01 Юриспруденция,

Краснодар

КубГАУ

2021

*Составители:*В. В. Помазанов, С. И. Грицаев.

**Криминалистическое обеспечение защиты и исследования компьютерной информации:** метод. указания / сост. В. В. Помазанов, С. И. Грицаев. – Электронный ресурс, 2021. – 37 с.

Методические указания содержат краткую характеристику основных аспектов контактной работы (аудиторной и внеаудиторной) преподавателя с обучающимися при изучении дисциплины «Криминалистическое обеспечение защиты и исследования компьютерной информации», требования по ее выполнению.

Предназначены для обучающихся по направлению подготовки 40.04.01 Юриспруденция, направленность «Теория и практика расследования преступлений»

© В. В. Помазанов,

С. И. Грицаев

составление, 2021

© ФГБОУ ВО «Кубанский

государственный аграрный   
университет имени   
И. Т. Трубилина», 2021

**ВВЕДЕНИЕ**

Цель организации контактной работы преподавателя с обучающимся по дисциплине «Криминалистическое обеспечение защиты и исследования компьютерной информации» – обеспечение качества общекультурной и профессиональной подготовки обучающихся по направлению подготовки 40.04.01 Юриспруденция, что позволяет выпускнику успешно работать в избранной сфере деятельности, обладать компетенциями, способствующими его социальной мобильности и конкурентоспособности в современных условиях.

Контактная работа преподавателя с обучающимся по дисциплине «Криминалистическое обеспечение защиты и исследования компьютерной информации» может быть аудиторной и внеаудиторной. Объем контактной работы отражается в учебных планах.

Контактная работа преподавателя с обучающимся по дисциплине «Криминалистическое обеспечение защиты и исследования компьютерной информации» включает в себя: занятия лекционного типа, семинары, практические, индивидуальную работу обучающихся с преподавателем, в том числе индивидуальные консультации и проведение зачета.

Качество освоения обучающимся материала по дисциплине «Криминалистическое обеспечение защиты и исследования компьютерной информации» оценивается преподавателем в ходе контактной работы (аудиторная и внеаудиторная) с обучающимся посредством текущего контроля успеваемости и промежуточной аттестации обучающихся (период сдачи зачета).

Текущий контроль, осуществляемый преподавателем, обеспечивает выполнение обучающимся всех видов работ, предусмотренных рабочей программой дисциплины (устный опрос, решение компетентностно-ориентированных задач (ситуационных), участие в дискуссиях, тестирование)*,* активность обучающегося в ходе учебной деятельности, посещаемость занятий, научно-исследовательскую работу и т.д.

Формой промежуточной аттестации обучающихся по дисциплине «Криминалистическое обеспечение защиты и исследования компьютерной информации» является зачет.

**1. АУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИН «Криминалистическое обеспечение защиты и исследования компьютерной информации»**

1.1 ПЛАНЫ ПРАКТИЧЕСКИХ (СЕМИНАРСКИХ)

ЗАНЯТИЙ

# Тема 1. Компьютерные преступления

**План занятия:**

1. Понятие компьютерной информации.

2. Понятие «компьютерного преступления».

3. Компьютерные преступления.

**Задания:**

**1. Доклад**

Тема доклада:

Борьба с преступлениями в сфере высоких технологий.

**2. Реферат**

Тема реферата:

Уголовный кодекс РФ о преступлениях в сфере компьютерной информации.

**3. Дискуссия**

Тема дискуссии: Информатизация современного общества: риски и вызовы цифровизации.

Перечень вопросов для проведения дискуссии:

Соотношение информатизации и цифровизации в уголовном судопроизводстве.

**4. Компетентностно-ориентированная задача (ситуационная)**

# Адвокат Хорошавин, работая в юридической фирме «Лига А» в качестве помощника генерального директора, получил несанкционированный доступ к программам других людей и постоянно использовал их. Более того, часть информации, полученной в базах данных, адвокат Хорошавин продал заинтересованным людям. В то же время, из-за несанкционированного проникновения помощника генерального директора в вышеупомянутые программы, в них начали появляться сбои, после чего владельцы источников информации, чтобы найти причину сбоя программного обеспечения провели экспертизу и установили причину сбоев. Владельцы программ и баз данных потребовали строгого наказания Хорошавина.

# Задание. Оцените сложившуюся ситуацию с точки зрения действующего законодательства.

# Тема 2. Следственные действия при расследовании преступлений в информационной сфере

**План занятия:**

1. Особенности осмотра и выемки средств компьютерной техники и носителей информации.

2. Подготовка к осмотру компьютерных средств.

3. Предварительная ориентировка перед обыском или осмотром компьютерной техники.

4. Исследование носителей и хранящейся информации.

5. Исследование программного обеспечения.

**Задания:**

**1. Доклад**

Тема доклада:

Исследование и экспертиза по компьютерной аппаратуре и информации.

**2. Реферат**

Тема реферата:

Виды хранящейся компьютерной информации.

**3. Дискуссия**

Тема дискуссии: Идентификация компьютеров и данных.

Перечень вопросов для проведения дискуссии:

Исследование, анализ и восстановление компьютерных данных.

**4. Компетентностно-ориентированная задача (ситуационная)**

Петровский получил на телефон сообщение, в котором был прислан единоразовый пароль для входа в личный кабинет банковских транзакций его подруги Ивановской. Однажды Ивановская просила его телефон для проведения транзакций и, по-видимому, «привязала» номер к личному профилю интернет-банка. Петровский помнил номер карты Ивановской и, воспользовавшись единоразовым паролем, перевел часть денежных средств с банковской карты Ивановской на свой расчетный счет.

Задание. Оцените действия Петровского и Ивановской с точки зрения норм права.

**Тема 3. Криминалистическая значимость данных в реестре**

**План занятия:**

1. Структура реестра: понятие куста, ветви, ключа, значения ключа.

2. Типы данных.

3. Логическая организация данных в реестре.

4. Изменения содержимого реестра при изменении аппаратной конфигурации компьютера, установке программного обеспечения, операциях с файлами.

**Задания:**

**1. Доклад**

Тема доклада:

Программное обеспечение для работы с данными в реестре.

**2. Реферат**

Тема реферата:

Виды программного обеспечения, его функциональные возможности и особенности применения при производстве компьютерной экспертизы.

**3. Дискуссия**

Тема дискуссии: Изменения содержимого реестра при изменении аппаратной конфигурации компьютера.

Перечень вопросов для проведения дискуссии:

Возможности использования информационных и телекоммуникационных технологий в профессиональной деятельности.

**4. Компетентностно-ориентированная задача (ситуационная)**

Гавриков, обладая специальными познаниями в области работы с электронными вычислительными машинами (далее - ЭВМ) и компьютерными программами, используя принадлежащую ему ЭВМ, имеющую подключение к сети Интернет, приобрел путем копирования с сайта «Fishki» компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации. Впоследствии посредством принадлежащего ему компьютерного оборудования, а также находящихся в его пользовании хостинговых сервисов с доменными именами использовал указанные вредоносные компьютерные программы для заражения 50 ЭВМ пользователей сети Интернет и построения из них контролируемой сети. Построив контролируемую сеть, Гавриков без ведома и согласия пользователей скопировал хранящуюся в памяти зараженных ЭВМ компьютерную информацию, содержащую сведения о логинах и паролях авторизации пользователей на различных Интернет-ресурсах.

Задание. Оцените действия Гаврикова, приведите правовые нормы в обосновании своих доводов.

**5. Лабораторная работа**

**Работа с реестром Windows**

Цель: изучить назначение и возможности реестра, научиться выпол­нять настройки в системном реестре.

Реестр - это база данных в Windows, которая содержит важную инфор­мацию об оборудовании системы, установленных программах и настройках, а также о профиле учетных записей компьютера.

Реестр заменяет собой большинство текстовых ini-файлов, которые ис­пользовались в Windows 3.x, а также файлы конфигурации MS-DOS (напри­мер, Autoexec.bat и Config.sys).

Windows постоянно обращается к информации в реестре.

Версии реестра для разных версий операционных систем семейства Windows имеют определенные различия.

При запуске операционной системы происходит до тысячи обращений к реестру, а при работе на ПК в течение одного сеанса работы - до 10 тысяч!

Отдельные компоненты реестра хранятся в оперативной памяти ПК в течение всего сеанса работы.

Запись (считывание) информации в реестр (из реестра) происходит по­стоянно: например, при установке какой-нибудь программы вся информация, необходимая для запуска и работы этой программы, записывается в реестр. Если мы устанавливаем новое устройство, в реестре будет отмечено, где на­ходится его драйвер и т.д. Если же мы запускаем какую-то программу или устройство, то из реестра считывается вся необходимая для запуска про­граммы (устройства) информация.

Значение реестра

Значение реестра для Windows трудно переоценить - это основная часть операционной системы. От корректности данных реестра зависит эф­фективность работы как программного обеспечения (операционной системы и приложений), так и аппаратной части ПК. С помощью реестра можно за­ставить ПК или работать с максимально возможным быстродействием, или «тормозить».

Появление всевозможных «глюков» в работе ОС говорит о том, что ка­кие-либо настройки реестра стали некорректными. При серьезном поврежде­нии реестра операционную систему загрузить невозможно. Поэтому вирусы зачастую стараются испортить реестр или заблокировать доступ к реестру пользователя.

Реестр Windows состоит из 5-ти ветвей:

1. HKEY\_CLASSES\_ROOT (HKCR) - в этой ветви содержатся сведе­ния о расширении всех зарегистрированных в системе типов файлов (храня­щиеся здесь сведения отвечают за запуск необходимой программы при от­крытии файла с помощью Проводника Windows);
2. HKEY\_CURRENT\_USER (HKCU) - в этой ветви содержится ин­формация о пользователе, вошедшем в систему в данный момент (здесь хра­нятся папки пользователя, цвета экрана и параметры панели управления);
3. HKEY\_LOCAL\_MACHINE (HKLM) - в этой ветви содержится ин­формация об аппаратной части ПК, о драйверах устройств, сведения о за­грузке Windows;
4. HKEY\_USERS (HKU) - в этой ветви содержится информация о всех активных загруженных профилях пользователей данного ПК;
5. HKEY\_CURRENT\_CONFIG (HKCC) - в этой ветви содержится информация о профиле оборудования, используемом локальным компьюте­ром при запуске системы.

Реестр Windows хранится в папке Windows\System32\config в двоич­ных файлах.

Как управлять Реестром

Основным и наиболее известным инструментом администрирования Реестра Windows является утилита Редактор реестра (Registry Editor), вхо­дящая в состав любой копии ОС Windows (дисковый адрес утилиты - Windowsregedit.exe). Утилита имеет небольшой размер - около 130 КБ.

Для запуска утилиты Редактор реестра:

1. Выполните команду Пуск - Выполнить ...
2. В поле Открыть: введите regedit.

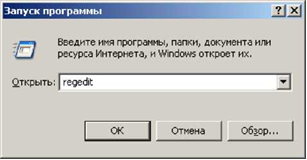


Рис. 1. Диалоговое окно Выполнить Интерфейс

Редактора реестра представляет собой обычное окно со строкой заголовка, строкой меню (Файл, Правка, Вид, Избранное, Справ­ка).

Рабочее окно Редактора реестра разделено на две части:

1. в левой (Панель разделов) отображаются ветви, разделы и под­разделы,
2. в правой (Панель параметров) - параметры выбранного элемен­та реестра.

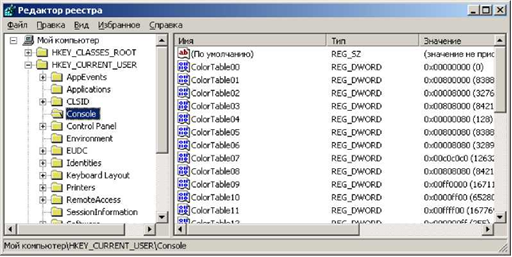


Рис. 2. Диалоговое окно Редактор реестра

Так называемые «точки восстановления» - это копии реестра Windows. Они широко используются пользователями при возникновении различных проблем, как с операционной системой, так и с прикладным про­граммным и аппаратным обеспечением. Точки восстановления позволяют выполнить откат на тот момент, когда система работала нормально.

Обычно не нужно изменять реестр вручную, поскольку программы и приложения вносят все необходимые изменения автоматически. Неправиль­ное изменение реестра может привести нерабочее состояние компьютера. Однако если в реестре появляется поврежденный файл, возможно, вам по­требуется осуществить изменения.

Рекомендуется сделать резервную копию реестра перед внесением изменений.

Нужно изменять только те значения в реестре, которые вы понимаете или если вы получили указания из источника, которому доверяете.

Установка разрешений на разделы реестра

Как для других объектов Windows ХР, можно назначить разрешения разделам реестра, чтобы указать действия, которые определенные пользова­тели или группы могут совершать с выбранным разделом.

Например, предотвратить возможность удаленного доступа пользова­телей к реестру, изменив разрешения на раздел winreg.

Установка разрешений оказывает действие не только на других пользо­вателей, но и на вас. Например, можно предотвратить автоматическое откры­тие редактором реестра последнего использовавшегося ключа при следую­щем запуске, установив права на раздел, где хранится эта информация. То есть если редактор реестра не сможет прочесть этот раздел, он не сможет от­крыть последний использованный раздел, а вместо этого откроет корень рее­стра.

Внимание: будьте аккуратны при установке разрешений в реестре. Не­верное назначение прав перекроет вам доступ к важным ключам реестра или даже лишит систему возможности функционирования.

Для установки разрешений на раздел реестра можно использовать один и тот же метод как в Professional, так и в Home Edition. Откройте редактор реестра, выберите раздел, на который нужно установить разрешения, и вы­полните команду Правка - Разрешения, чтобы открыть диалоговое окно Разрешения.

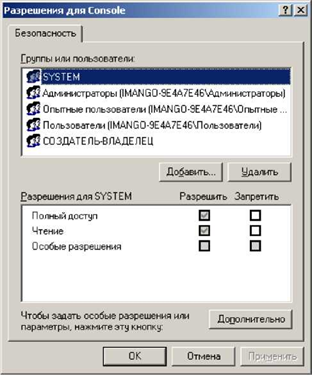


Рис. 3 Диалоговое окно Разрешения

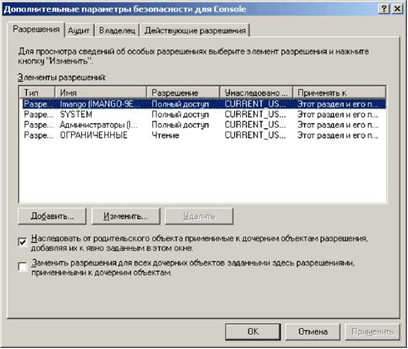


Рис. 4. Диалоговое окно Дополнительные параметры безопасности

Это окно используется для добавления или удаления пользователей и групп, для изменения разрешений пользователей или групп на данный раз­дел. Диалоговое окно Разрешения (Permissions) дает доступ лишь к некото­рым разрешениям. Чтобы назначить дополнительные разрешения, выберите

Дополнительно (Advanced), открыв диалоговое окно Дополнительные па­раметры безопасности (Advanced Security Settings).

Диалоговое окно Дополнительные параметры безопасности содер­жит два варианта, которые определяют применение разрешений:

1. Наследовать от родительского объекта применимые к дочерним объектам разрешения (Inherit from parent the permission entries that apply to child objects). При включении параметра выбранный раздел наследует разре­шения от родительского раздела.
2. Заменить разрешения для всех дочерних объектов, заданными здесь разрешениями, применимыми к дочерним объектам (Replace permission entries on all child objects with entries shown here that apply to the child). Включите этот параметр, чтобы применить выбранные разрешения реестра ко всем подразделам выбранного в данный момент раздела.

Что можно изменить в системном реестре:

1. Отключить Dr.Watson - отладчик, который по умолчанию за­пускается при каждом сбое в работе.

Чтобы его отключить, нужно запустить редактор реестра: в меню Пуск выберите пункт Выполнить. Откроется окно запуска программ. Напишите в нем regedit и нажмите кнопку ОК.

В левой части редактора реестра выбрать последовательно:

HKEY\_LOCAL\_MACHINE - SOFTWARE - Microsoft - Windows NT - CurrentVersion - AeDebug, находим там параметр Auto (появится в правой части редактора реестра).

В контекстном меню параметра Auto нужно выбрать пункт изменить.

В открывшемся окне значение параметра нужно изменить на 0, нажать

ОК.

Dr.Watson отключено. После такого изменения реестра при возникно­вении ошибки система будет предлагать либо закрыть приложение, либо пе­редать отладчику для исправления.

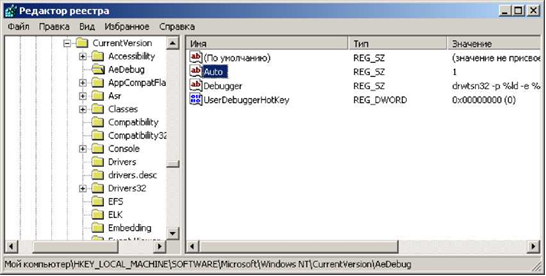


Рис. 5. Выбор параметра Auto

1. Если ваш компьютер отформатирован в NTFS, открытие па­пок с большим количеством файлов, что на нем содержатся, происходит довольно медленно, так как Windows каждый раз обновляет метку по­следнего доступа к файлам и на это тратится определенное время. Эту функцию также можно отключить.

Запустить редактор реестра, в левой его части перейти:

HKEY\_LOCAL\_MACHINE - SYSTEM - CurrentControlSet - Control - FileSystem.

Теперь в правой части редактора создать новый параметр DWord, на­зываем его NtfsDisableLastAccessUpdate и присваиваем ему значение 1. Для этого в правой части редактора реестра в контекстном меню выбрать Соз­дать - Параметр DWORD

В правой части редактора появляется новый параметр.

Далее его нужно переименовать на NtfsDisableLastAccessUpdate, в контекстном меню этого параметра выбрать изменить. В поле Значение ста­вим 1 , в системе исчисления отметить шестнадцатеричная и нажать ОК.

1. Еще один параметр в реестре, который можно изменить - скорость открывания меню Пуск. По умолчанию, оно открывается с за­держкой 400 миллисекунд.

Чтобы уменьшить эту задержку, нужно открыть редактор реестра, в ле­вой части редактора перейти:

HKEY\_CURRENT\_USER - ControlPanel - Desktop.

Теперь в правой части нужно найти параметр MenuShowDelay.

В контекстном меню параметра выбрать пункт изменить. Далее в поле значение отметить 0 и нажать ОК.

Теперь меню Пуск будет открываться без задержек.

1. Установить приоритет запросов на прерывание (IRQ) для «CMOS и часы», что должно увеличить производительность системной платы. Сначала надо определить, какой запрос на прерывание использует это устройство (как правило, IRQ08, но лучше убедиться).

Удерживая Win нажать клавишу Pause Break (Break). В окне Свойст­ва системы на вкладке Оборудование нажать кнопку Диспетчер устройств.

В разделе Системные устройства в контекстном меню пункта CMOS и часы выбрать Свойства.

В появившемся окне перейти на вкладку Ресурсы, найти и запомнить (записать в тетрадь) значение IRQ для устройства, закрыть все окна.

Запустить Редактор реестра (см. выше) и в разделе HKEY\_LOCAL\_MACHTNE \ System \ CurrentControlSet \ Control \ PriorityControl создать новый DWORD-параметр с названием TRQ \*\* Priority (где '\*\*' номер IRQ, который вы запомнили), установить для него значение «1».

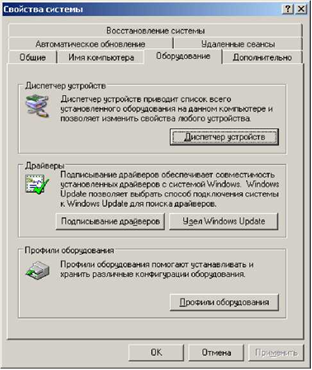


Рис. 6. Диалоговое окно Свойства системы

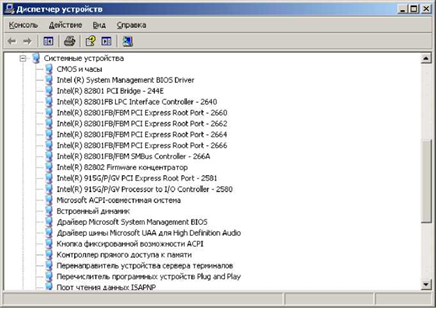


Рис. 7. Диалоговое окно Диспетчер устройств

1. Отключить POSIX:

открыть Редактор реестра и в разделе

HKEY\_LOCAL\_MACHINE\SYSTEM\ CurrentControlSet \ Control Ses- sionManager \ SubSystems удалить параметры Optional и Posix.

1. Отключить кэширование DLL:

в разделе HKEY\_LOCAL\_MACHINE \ SOFTWARE \ Microsoft \ Windows \ Current Version \ Explorer создать новый DWORD-параметр с названием lwaysUnloadDLL и значением 1.

1. Можно отключить сообщения об окончании свободного места на дисках:

в разделе HKEY\_CURRENT\_USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer создать DWORD-параметр под назва­нием NoLowDiskSpaceChecks и значением 1.

Выполнить практическое задание:

1. Изучить Редактор реестра.
2. Выполнить некоторые настройки (по собственному выбору, не нарушая работы системы) из приведенных в работе.
3. Подготовить отчет по работе.

Контрольные вопросы:

1. Поясните, что такое реестр Windows
2. Как запустить Редактор реестра?
3. Укажите и кратко охарактеризуйте составные части (ветви) сис­темного реестра
4. Какие разрешения можно установить в диалоговом окне Разрешения?
5. Какие параметры можно изменить в системном реестре?

Составьте отчет о выполненной работе.

**Тема 4. Анализ следов воздействия на информацию в операционной системе Windows при решении задачи поиска по контексту**

**План занятия:**

1. Моделирование и анализ искомой информации при решении задачи поиска по контексту.

2. Стандартные и специальные средства кодирования информации для оптимизации ее хранения или предотвращения несанкционированного доступа.

3. Инструментальные средства получения доступа к информации и ее поиска по контексту.

**Задания:**

**1. Доклад**

Тема доклада:

Объекты файловой системы ОС Windows

**2. Реферат**

Классификация следов в компьютерных системах.

**3. Дискуссия**

Тема дискуссии: О природе следов в информационной среде компьютерных систем

Перечень вопросов для проведения дискуссии:

Компьютерная программа как следообразующий объект.

**4. Компетентностно-ориентированная задача (ситуационная)**

Сотрудники банка «Импэкскредит» гр. Свиридов С. С. и гр. Прокофьев П. П. 25 января с. г. указанные лица, по предварительному сговору, с целью сокрытия следов хищения денежных средств, размещенных на депозитах, уничтожили изобличающие их электронные финансовые документы общим числом 143 единицы и информацию из 78 электронных IР-адресов.

Задание. Оцените действия Свиридов С. С. и гр. Прокофьев П. П. с точки зрения норм права.

**5. Лабораторная работа. Выявление скрытых папок и файлов**

Кратко: В сети существует много программ для скрытия отдельных папок и файлов от других пользователей компьютера. Эти программы предлагают простой метод скрытия папок - с помощью фильтрации запросов к файловой системе. Но это не означает 100% защиту данных.

На самом деле скрытые файлы и папки можно увидеть и посмотреть с помощью других средств. Если требуется более надёжная защита, следует обратиться к серьёзным криптографическим пакетам (шифрование).

Как скрыть папку или файл?

Одним из самых больших желаний пользователя зачастую является желание спрятать свои личные документы, программы и прочие данные куда-нибудь подальше от чужих глаз. Самый распространённые способы для этого:

• Использовать программы для скрытия файлов и папок. Таковых сейчас довольно много: Hide Folders XP, Folder Lock и др.

• Использовать стандартные средства в Windows: пометить папку\файл как скрытый, на NTFS томах - запретить доступ к папке/файлу путем указания прав для доступа к объекту.

Директории и файлы, помеченные в Windows как «скрытые»:

• Не видны в Проводнике другим пользователям системы, если у пользователя включен флаг: Не отображать скрытые папки.

• Видны в программах: FAR, Total Commander, и др., которые не используют стандартный диалог для отображения файлов и папок.

Мы намеренно упустили из виду EFS (встроенное шифрование в Windows 2000/XP), поскольку для настройки этой возможности требуются значительные усилия и квалификация.

Удобство этих методов заключается в том, что для скрытия информации не нужно делать ничего лишнего. Всё довольно просто: достаточно одного клика мыши, чтобы скрыть ту или иную папку/файл.

Защита файлов и папок с помощью Hide Folders XP

Hide Folders XP закрывает доступ к папкам и файлам, скрывая или блокируя их. В первом случае папка или файлы не видны, во втором случае - видны, но заблокированы.

Программу можно настроить на автоматический запуск при старте Windows.

**Задание 1.**

1. Создайте на диске D:\ папку с именем Директория.

2. Скопируйте в созданную папку с диска C:\ файл Proba.txt.

Запустите Hide Folders XP (Пуск - Тема - Защита и преодоление - Защита информации - hfxp).

Примечание. В зависимости от установленных настроек программы, запуск Hide Folders XP, возможно, придется повторить еще раз.

В правом нижнем углу экрана появится значок программы с сообщением, что Hide Folders XP уже запущен. Нажмите на значке правую кнопку мыши и выберите Открыть Hide Folders XP...

Порядок работы с программой следующий:

1. Ввести пароль для защиты программы. • Выберите в меню Сервис - Задать пароль и введите пароль.

2. Добавить в список программы папку или файлы. • Выберите в меню Файл - Добавить в список - Добавить в список папку или файлы...

• Выберите диск D:\ папку Директория. Нажмите кнопку ОК. Выбранная папка появится в окне программы.

3. Если необходимо, изменить способ защиты. По умолчанию установлен способ защиты - Скрывать и блокировать. • Нажмите правую кнопку мыши на строке Б:\Директория в окне программы и выберите нужный способ защиты.

4. Настроить программу для более удобной работы с ней. • Установить или отменить автозапуск программы при старте Windows. Меню Сервис - Настройки - Запуск.

• Указать видимость трей-иконки при запуске. Меню Сервис - Настройки - Запуск.

• Указать действия при закрытии окна программы. Меню Сервис - Настройки - Основные.

• Установить Горячие клавиши. Меню Сервис - Настройки - Горячие клавиши.

Примечание. При выборе Горячих клавиш надо установить курсор в нужную строку и нажать на клавиатуре необходимую комбинацию клавиш.

• Выполнить другие, необходимые вам настройки программы.

5. Включить или отключить защиту. • Выберите в меню Файл - Включить или Выключить защиту или нажмите соответствующую кнопку на панели инструментов программы.

6. Закрыть окно программы.

**Задания 2.**

1. Запустите программу.

2. Защитите программу паролем.

3. Настройте программу на сворачивание в трей при закрытии окна.

4. Настройте горячие клавиши для следующих операций: • Открытие программы.

• Включение защиты.

• Выключение защиты.

• Видимость трей-иконки.

5. Скройте папку Директория на диске D:\ .

6. Запустите Мой компьютер и убедитесь в том, что папка не видна.

7. Заблокируйте папку Директория на диске D:\ .

8. Запустите Мой компьютер и убедитесь в том, что папка видна, но не открывается.

На этом работа с Hide Folders XP закончена.

Но какие минусы у такого рода программ? Давайте попробуем разобраться.

Какая степень защиты?

Далеко не все утилиты для скрытия папок надёжно скроют Ваши данные. Ещё меньшее их число кроме того, что скроет их, будет надежно защищать их шифрованием от разных приемов. Множество таких программ скрывают папки и файлы лишь для одной операционной системы. А если на компьютере (ПК) установлено несколько операционных систем (ОС)? Из одной системы данные видно не будет, а из другой - всё, как на ладони!

Простое скрытие папок и ограничение доступа к файлам не спасает в следующих случаях:

• Загрузка ПК в другой операционной системе (если она есть) либо загрузка другой ОС с CD-ROM. Например Linux BLin .

- в другой ОС, которая подключится к вашему HDD диску, все файлы на нем будут видны, поскольку никаких ограничений и защиты не будет.

• Загрузка Windows в SafeMode (безопасный режим).

После такой загрузки все папки будут видны, да же те, которые были скрыты программно. Ведь, при загрузке в безопасном режиме, Windows загружает лишь драйвера, необходимые для работы системы, а все дополнительные пропускает (драйвера-фильтры), чтобы заранее отбросить потенциально возможные сбои.

• Снять HDD диск и подключить его к другому компьютеру.

Если снять жесткий диск (HDD диск) и подключить его к другому компьютеру, то можно увидеть и открыть все скрытые папки и файлы. Будут видны даже те папки, доступ к которым запрещен (на NTFS томах).

Есть ещё одна возможность просмотреть файлы, скрытые различными программами. Для этого необходимо обладать правами Администратора (Учетная запись с Администраторскими полномочиями). Потому что, если Вы являетесь администратором системы, вы можете деинсталлировать (удалить) программы для скрытия папок, или загрузиться в режиме защиты от сбоев, и тогда все скрытые объекты станут видимыми.

**Тема 5. Журналы операционной системы Windows, их криминалистическая значимость.**

**План занятия:**

1. Журнал системы, журнал приложений и журнал безопасности: их назначение, структура, криминалистическая значимость.

2. Журнал программы «Проводник», его назначение, структура, криминалистическая значимость.

3. Журнал сведений о системе, формируемый инструментарием Windows Management Instrumentation (WMI), его назначение, структура, криминалистическая значимость.

4. Иные журналы операционной системы Windows, их структура, криминалистическая значимость.

**Задания:**

**1. Доклад**

Тема доклада:

Программное обеспечение для работы с журналами операционной системы Windows

**2. Реферат**

Тема реферата:

Особенности применения программного обеспечения при производстве компьютерной экспертизы.

**3. Дискуссия**

Тема дискуссии: Программное обеспечение для работы с журналами операционной системы Windows: его функциональные возможности и особенности применения при производстве компьютерной экспертизы.

Перечень вопросов для проведения дискуссии:

Криминалистическая значимость журнала системы, журнала приложений и журнала безопасности.

**4. Компетентностно-ориентированная задача (ситуационная)**

Гуляшов, студент факультета вычислительной математики, организовывал сетевые атаки, заключающиеся в получении обманным путем доступа в сеть посредством имитации соединения. Таким образом он получил доступ к информации о счетах пользователей интернета и номерах некоторых кредитных карт и пин-кодов. Полученную информацию Гуляшов передавал Сорокиной за вознаграждение, которая использовала ее для хищения денежных средств.

Что такое фишинг, спуфинг и фарминг? Признаки какого явления усматриваются в деянии Гуляшова? (фишинга, спуфинга или фарминга). Квалифицируйте содеянное Гуляшовым и Сорокиной.

**5. Лабораторная работа.** Анализ состояния операционной системы и системных событий

В ходе разработки операционных систем семейства Windows представители компании Microsoft всегда уделяли особое внимание надежности и безопасности своих систем, и в этом необходимо отдать им должное. Под «безопасностью системы» подразумевается не только ее защищенность от взлома посторонними лицами (кстати, тут они не всегда были на высоте), но, в первую очередь, защищенность системных файлов и файлов реестра. С целью обеспечения надежности и безопасности операционных систем семейства Windows разработчики включили в их состав систему аудита, позволяющую контролировать, производить оценку и прогнозировать их состояние.

Аудит операционной системы семейства Windows – это процесс, предназначенный для обнаружения и регистрации событий, происходящих в системе, для проведения последующего анализа. Система аудита, встроенная в ОС Windows, позволяет фиксировать большинство событий, происходящих в ней, а сами события регистрируются в специальных журналах Windows. Следует отметить, что информация, которая регистрируется в вышеуказанных журналах, порядок настройки регистрируемых параметров и порядок анализа событий, происходящих в системе, зависят от типа операционной системы. Например, для операционных систем Windows XP фиксация событий, влияющих на безопасность системы, возможна только после активации хотя бы одного из параметров, подлежащих контролю. А в более поздних вариантах операционных систем некоторые события безопасности регистрируются постоянно, независимо от настроек аудита.

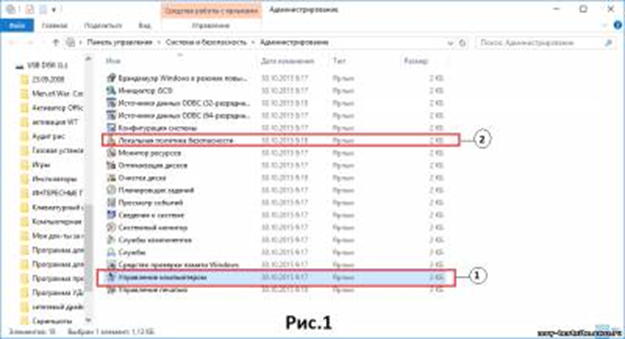
Типы событий операционных систем

В операционных системах семейства Windows существует несколько журналов, в которые записывается большинство событий, происходящих в системе. При этом некоторые события записываются автоматически, а регистрацию других (в основном, касающихся безопасности системы) необходимо активировать и настраивать. Событиями можно назвать любые изменения состояния операционной системы. К ним относятся запуск системы (компьютера), вход в систему любого пользователя, любые процессы, запускаемые или отключаемые в операционных системах, попытка доступа к системным файлам и защищенным файлам реестра и многое другое. События подразделяются на типы, к которым относятся: а) информация, б) предупреждение и в) ошибка. Кроме этого, существуют еще такие события, как «Успешный аудит» и «Неуспешный аудит». Последние два типа событий предназначены для специалистов, обеспечивающих контроль безопасности системы, и в данной статье будут рассмотрены только в части, касающейся активации параметров «Журнала безопасности Windows».

События типа «Информация» (еще этот тип событий называется «Сведения») отображают факт успешной операции. Этим событиям соответствует пиктограмма в журнале событий в виде кружочка с буквой «i» внутри кружочка (см. Рис.1). Справа от пиктограммы текстом отображается тип события «Сведения».

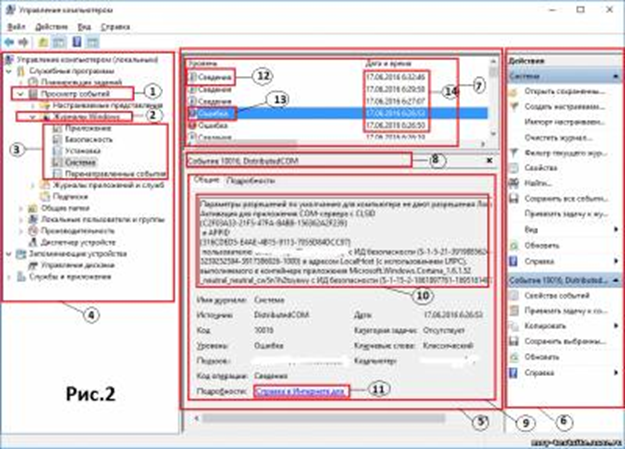
Событие типа «Предупреждение» отображает некоторые проблемы, имеющие место в работе операционной системы. Данное событие свидетельствует о незначительной проблеме в работе системы (приложения) и не требует немедленного вмешательства пользователя, но регулярное появление одного и того же события может со временем привести к ошибкам. Этим событиям соответствует пиктограмма в журнале событий в виде желтого треугольника с восклицательным знаком внутри (не показано). Справа от пиктограммы текстом отображается тип события «Предупреждение».

Событие «Ошибка» отображает проблемы, которые могут привести к потере работоспособности системы или потере информации. Этим событиям соответствует пиктограмма в журнале событий в виде красного кружочка с восклицательным знаком внутри кружочка (см.Рис.1). Справа от пиктограммы текстом отображается тип события «Ошибка».



Журналы событий и их включение

Как уже отмечалось выше, все события регистрируются в специальных журналах. Чтобы запустить любой из журналов, необходимо воспользоваться утилитой «Администрирование» из панели управления. Для этого необходимо последовательно нажать кнопки Пуск\ Панель управления\ Система и безопасность\ Администрирование, и перед вами откроется окно Рис.1. В случае с Windows XP вам необходимо запустить Панель управления, перейти к классическому виду отображения Панели управления и из перечня утилит выбрать «Администрирование». Если вы обладатель ОС Windows 10, воспользуйтесь рекомендациями, выложенными в статье «КУДА ДЕЛАСЬ ПАНЕЛЬ УПРАВЛЕНИЯ В WINDOWS 10?», либо кнопкой «Поиск», с последующим введением в поле поиска поискового слова «Администрирование». В любом случае, результатом ваших действий должно быть открытие окна Рис.1. Чтобы открыть необходимый вам журнал, вы должны выбрать оснастку «Управление компьютером» (см.1 Рис.1), после чего перед вами откроется окно Рис.2.



В окне Рис. 2 откройте вкладку «Просмотр событий» (см.1 Рис.2). Выберите «Журналы Windows» (см.2 Рис.2) и в открывшемся перечне существующих журналов (см.3 Рис.2) выберите тот, который вас интересует. Но, если вы пытаетесь найти причину проблемной работы вашего ПК, вам наверняка придется анализировать все журналы.

Существует три основных журнала, в которые записываются наиболее важные события. Это: а) Система, б) Приложения и в) Безопасность. Кроме этого, есть еще и такие журналы, как «Установка» и «Перенаправленные события» (см.3 Рис.2). Названия вышеуказанных журналов отображают события, которые в них фиксируются (системные события, события приложений и т.д.).

Все события, имевшие место на вашем компьютере, записываются в ключе реестра HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog, который имеет подключи, соответствующие имеющимся журналам (Система, Безопасность и т.д.). А это значит, что пользователь ПК имеет возможность создавать новые журналы, адаптированные под его запросы.

И еще несколько слов об окне Рис.2. При открытии любого из журналов событий Windows, окно делится на три вертикальных подокна. Первое (левое) подокно (см.4 Рис.2) служит для выбора соответствующего журнала. Второе (среднее) подокно (см.5 Рис.2) служит для анализа событий. И третье (правое подокно) содержит набор органов управления для выполнения определенных действий со стороны пользователя компьютера. Среднее окно (см.5 Рис.2) является основным источником проведения анализа.

Анализ событий в операционных системах Windows

Если на вашем ПК периодически проявляются сбои, то эти факты однозначно должны послужить причиной проведения анализа. Если же внешних проявлений сбоев не отмечается, то пользователям все равно периодически необходимо открывать журналы событий и оценивать их с целью выявления повторяющихся ошибок и предупреждений, т.к. эти ошибки могут привести к полному отказу вашего компьютера. Кроме этого, Журнал безопасности может помочь вам выявить случаи злонамеренных или неумышленных, но опасных действий пользователей, имеющих доступ к вашему ПК.

Все события, зарегистрированные в соответствующем журнале, отображаются в среднем вертикальном подокне (см.5 Рис.2), которое делится на три горизонтальных части. В верхней части отображается перечень зафиксированных событий (см.7 Рис.2). Под ней расположен раздел с информацией о коде события и источнике события (см.8 Рис.2), а ниже – детальная информация о событии с его описанием, если оно есть в перечне событий Windows.

Как отмечалось выше, основными событиями являются Информация (Сведения) (см.12 Рис.2), Предупреждения и Ошибки (см.13 Рис.2). Событие типа «Предупреждение» не показано на Рис.2, но внешний вид его детально описан в начале статьи.

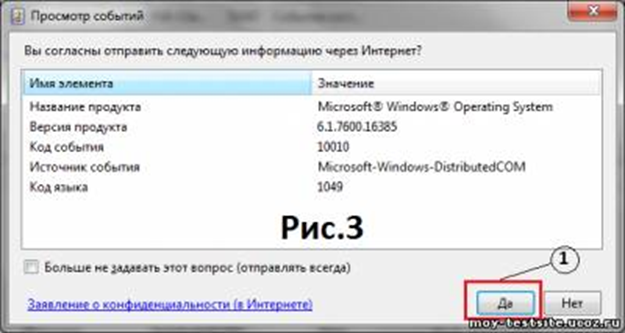
Для проведения анализа событий, имевших место на вашем ПК, необходимо открыть соответствующие журналы событий и найти события, которые предшествовали неустойчивой работе (сбоям) компьютера. При этом делается привязка по времени внешнего проявления неустойчивой работы (сбоя) компьютера и событий, зафиксированных в Журналах событий. Если все зафиксированные в Журналах события четко привязываются к системному времени (см.14 Рис.2), то внешнее проявление (сбой, зависание и т.п.) вам необходимо зафиксировать самостоятельно.

Если неустойчивой работы ПК не отмечалось, то целесообразно просто просмотреть события за определенный период во всех имеющихся журналах.

Среди зафиксированных системой событий необходимо искать в первую очередь события типа «Ошибка». Что касается событий типа «Информация» («Сообщение»), то обычному пользователю нет смысла анализировать эти события, т.к. они информируют об успешном выполнении какой-либо задачи. К примеру, успешный переход системы в режим «Сон», выход из режима «Сон» и т.п. Но, если у кого-нибудь возникнет желание или необходимость, он сможет самостоятельно выбрать событие типа «Информация», выделить его и посмотреть его описание в разделе с детальной информацией (см.9 Рис.2).

Итак, как вы, наверное, уже догадались, выделение любого события из списка событий (см.13 Рис.2) приводит к появлению соответствующей информации в разделах «Код события» (см.8 Рис.2) и «Детальная информация о событии» (см.9 Рис.2). Вам только остается внимательно изучить эту детальную информацию и, в первую очередь, текстовую информацию в подокне «Описание события» (см.10 Рис.2). Но, если этой информации недостаточно и вам не понятно, что вы должны предпринять, то воспользуйтесь кнопкой «Справка в Интернете для…» (см.11 Рис.2).

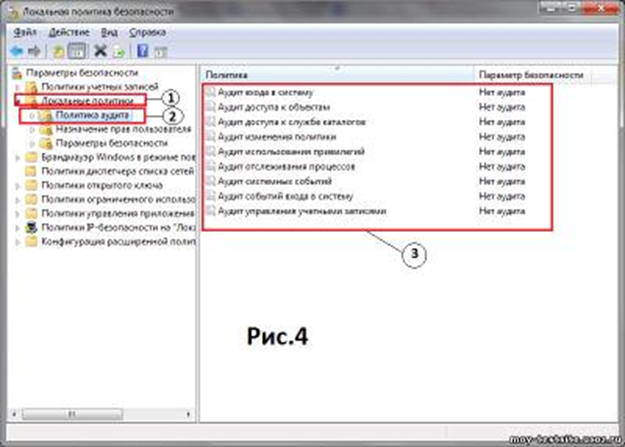
Примечание: В разных операционных системах кнопка «Справка в Интернете для…» (см.11 Рис.2) может называться по-другому. В Windows 7 эта кнопка называется «Веб-справка журнала».



После нажатия на кнопку «Справка в Интернете для…» (см.11 Рис.2) система запросит у вас разрешения на отправку в компанию Microsoft информации о вашем событии. Это проявится в появлении окна Рис.3, в котором вам необходимо будет нажать кнопку «Да» (см.1 Рис.3).

После того, как вы нажмете кнопку «Да» (см.1 Рис.3), ваш браузер, установленный по умолчанию, откроет окно на официальном сайте Microsoft, где должно быть описание ошибки и рекомендации об ее устранении. Вот только для операционных систем Windows 10 это не всегда работает, видимо, потому, что для данной системы накоплено недостаточное количество статистического материала. А вот что касается Windows 7, то тут все нормально. Для большинства ошибок есть и описание, и рекомендации.

Теперь несколько слов о журнале «Безопасность». Как я уже говорил, по умолчанию в Windows XP этот журнал не активирован, т.е. в нем не фиксируется ни одно событие. В операционных системах Windows 7 и выше фиксируется несколько событий, причем для разных систем они различны. Чтобы активировать этот журнал для Windows XP или расширить список событий для других систем, необходимо произвести настройку аудита параметров безопасности. Для этого в окне «Администрирование» необходимо выбрать «Локальная политика безопасности» (см.2 Рис.1).



В новом окне Рис.4 откройте вкладку «Локальные политики» (см.1 Рис.4) и выберите «Политика аудита» (см.2 Рис.4), после чего в правой части этого окна у вас появится перечень событий, которые подлежат аудиту (см. 3 Рис.4). Выбрав любое из событий, для которого вы хотите назначить аудит, выполните настройку этого аудита. Вы можете настраивать аудит таким образом, чтобы фиксировались все удачные попытки или только неудачные попытки совершения события («Успех» или «Отказ»). Вы можете задать перечень объектов, доступ к которым ограничен определенным представителям пользователей компьютера. Вы можете включить и настроить аудит отслеживания определенных процессов и многое другое. Единственное, что не следует забывать, так это то, что для настройки параметров аудита безопасности необходимо зайти на компьютер как представитель группы «Администраторы».

Составьте отчет о выполненной работе.

**6. Тесты**

**2. ВНЕАУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИНЕ «КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»**

В течение периода изучения дисциплины преподаватель обеспечивает процесс освоения материла обучающимся не только в аудиторное время (лекции, практические (семинарские) занятия), но и во внеаудиторное время.

Виды внеаудиторной работы соответствуют учебному плану и рабочей программе дисциплины на текущий учебный год.

С этой целью преподаватель проводит консультации обучающихся по дисциплине «Криминалистическое обеспечение защиты и исследования компьютерной информации» и по результатам ее изучения – зачет. При этом преподавателем учитываются степень освоения обучающимся знаний, полученных как при его контактной работе с преподавателем, так и при его самостоятельной работе, в том числе ответы на практических занятиях, решения компетентностно-ориентированных задач, активность в дискуссиях, качество подготовки рефератов, посещаемость.

Зачет служит формой проверки успешного усвоения обучающимся учебного материала лекционных, семинарских (практических) занятий. Преподаватель оценивает степень сформированности компетенций на этапе изучения данной дисциплины. Зачет для обучающихся всех форм обучения могут проводится в письменной или устной форме. Допускается проводить зачет в форме тестирования. На зачете обучающемуся могут быть заданы дополнительные вопросы в рамках рабочей учебной программы дисциплины.

Вопросы к зачету соответствуют рабочей программе дисциплины на текущий учебный год.

Знания, полученные при освоении дисциплины «Криминалистическое обеспечение защиты и исследования компьютерной информации», могут быть применены обучающимся при подготовке выпускной квалификационной работы

**Приложение 1**

**РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА**

**Основная учебная и научная литература**

1. Проблемы криминалистики: монография /Меретуков Г.М.,Зеленский В.Д. и др. Краснодар,КубГАУ, 2018.-171с. Образовательный портал КубГАУ [Электронный ресурс]: Режим доступа: <https://edu.kubsau.ru/file.php/125/Problemy_kriminalistiki_-_monografija_421248_v1_.PDF>
2. Криминалистика : учебное наглядное пособие / Л. Ю. Аксенова, А. Т. Анешева, Н. И. Герасименко [и др.] ; под редакцией А. А. Кузнецова, К. В. Муравьева. — Омск : Омская академия МВД России, 2020. — 224 c. — ISBN 978-5-88651-752-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <https://www.iprbookshop.ru/108816.html>
3. Ручкин, В. Н. Современные компьютерные технологии и криминалистика : учебное пособие / В. Н. Ручкин, В. В. Фомин. - Рязань : Академия ФСИН России, 2019. - 101 с. - ISBN 978-5-7743-0920-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1254336>
4. Тюнис, И. О. Криминалистика : учебное пособие / И. О. Тюнис. — 4-е изд. — Москва : Университет «Синергия», 2019. — 224 c. — ISBN 978-5-4257-0384-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/101348.html

**Дополнительная учебная и научная литература**

1. Проблемы криминалистики : учеб. пособие / Г. М. Меретуков, Е. П. Ищенко, И. М. Комаров. – Краснодар : КубГАУ, 2020. – 126 с. Образовательный портал КубГАУ [Электронный ресурс]: Режим доступа: https://edu.kubsau.ru/file.php/125/Uchebnoe\_posobie\_Problemy\_kriminolistiki\_574081\_v1\_.PDF
2. Тюнис, И. О. Криминалистика : учебное пособие / И. О. Тюнис. — 4-е изд. — Москва : Университет «Синергия», 2019. — 224 c. — ISBN 978-5-4257-0384-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/101348.html
3. Волынский, А. Ф. Криминалистика и криминалистическая деятельность. Избранное : научное издание / А. Ф. Волынский. - Москва : ЮНИТИ-ДАНА : Закон и право, 2019. - 426 с. — (Серия «Научные школы Московского университета МВД России имения В.Я. Кикотя»). - ISBN 978-5-238-03287-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1359045
4. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography\_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1137902>
5. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности : учебное пособие / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 431 c. — ISBN 978-5-4497-0935-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/102070.html

**Нормативные и иные правовые акты, официальные акты высших судебных органов (в действующей редакции):**

1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года // Российская газета. 1993. 25 декабря.
2. Федеральный закон от 17 января 1992 г. № 2202-I «О прокуратуре Российской Федерации» // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации от 20 февраля 1992. № 8, Ст. 366.
3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (действующая редакция) // Парламентская газета. № 241-242, 22.12.2001. Российская газета. № 249, 22.12.2001. Собрание законодательства РФ. 24.12.2001. № 52 (ч. I). Ст. 4921. Ведомости Федерального Собрания РФ. 01.01.2002. № 1. ст. 1.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (действующая редакция) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954. Российская газета. № 113. 18.06.1996. № 114. 19.06.1996. № 115. 20.06.1996. № 118. 25.06.1996.

О прокуратуре Российской Федерации (ред. от 28.11.2015) [Электронный ресурс]: Федеральный закон от 17.01.1992 г. № 2202-1-ФЗ. – Режим доступа: www.consultant.ru/document/cons\_doc\_LAW

О Следственном комитете Российской Федерации (ред. от 30.12.2015) [Электронный ресурс]: Федеральный закон от 28 декабря 2010. № 403-ФЗ. – Режим доступа: www.consultant.ru/document/cons\_doc\_LAW\_108565

1. Гражданский кодекс Российской Федерации. (Часть первая) от 30 ноября 1994 года // СЗ РФ. 1994. № 32. Ст. 3301.
2. Гражданский кодекс Российской Федерации. (Часть вторая) от 26 января 1996 г. № 14-ФЗ //СЗ РФ. 1996. № 5. Ст. 410.
3. Федеральный закон от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // СЗ РФ. 2001. № 23. Ст. 2291.
4. Гражданский кодекс Российской Федерации. (Часть третья) от 26 ноября 2001 г. № 146-ФЗ // СЗ РФ 2001. № 49. Ст. 4552.
5. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ // СЗ РФ. 2002. № 1 (часть I). Ст. 3.
6. Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» // СЗ РФ. 2002. № 23. Ст. 2102.
7. Гражданский процессуальный кодекс РФ от 14 ноября 2002 г. № 138-ФЗ // СЗ РФ. 2002. № 46. Ст. 4532.
8. Гражданский кодекс Российской Федерации. (Часть четвёртая) от 18 декабря 2006 г. № 230-ФЗ // СЗ РФ. 2006. № 52 (часть I). Ст. 5496.

**Приложение 2**

**РЕКОМЕНДУЕМЫЕ ИНТЕРНЕТ– САЙТЫ**

1. Официальный интернет-портал правовой информации <http://www.pravo.gov.ru/ips/>.
2. Научно-технический центр правовой информации "Система" Федеральной службы охраны Российской Федерации <http://www1.systema.ru/>.
3. Официальный сайт МВД России – [www.мвд.рф](http://www.мвд.рф)
4. Официальный сайт Следственного комитета Российской Федерации – [www.sledcom.ru](http://www.sledcom.ru)

**Приложение 3**

**Перечень современных профессиональных баз данных и информационных справочных и поисковых систем**

1. Государственная автоматизированная система Российской Федерации «Правосудие» https://sudrf.ru/
2. Справочная информация по делам ВС РФ - <https://vsrf.ru/lk/practice/cases>
3. Справочная информация по жалобам - <https://vsrf.ru/lk/practice/appeals>
4. Правовая система «КонсультантПлюс» // Сайт «Consultant.ru» [Электронный ресурс] – URL: <http://www.consultant.ru>
5. Справочно-правовая система «Гарант» // Сайт «Aero.garant.ru» [Электронный ресурс] – URL: <http://www.aero.garant.ru>
6. Судебные и нормативные акты РФ // Сайт «Sudact.ru» [Электронный ресурс] – URL: <https://sudact.ru>
7. Генеральная прокуратура РФ. Портал правовой статистики <http://crimestat.ru/>
8. Банк данных "Нормативно-правовые акты, зарегистрированные в Министерстве юстиции Российской Федерации" // Сайт Министерства юстиции РФ [Электронный ресурс] – <URL:https://minjust.consultant.ru/>
9. Реферативная и цитируемая база рецензируемой литературы «Scopus» <https://www.scopus.com>
10. Реферативные базы данных публикаций в [научных журналах](https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%83%D1%87%D0%BD%D1%8B%D0%B9_%D0%B6%D1%83%D1%80%D0%BD%D0%B0%D0%BB) и [патентов](https://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%82%D0%B5%D0%BD%D1%82) «Web of Science» <http://apps.webofknowledge.com>
11. Научная электронная библиотека «eLIBRARY.RU» <https://elibrary.ru>
12. Сайт Российской государственной библиотеки <https://www.rsl.ru>
13. Поисковая система «Яндекс» <https://yandex.ru/>
14. Поисковая система «Google» <https://www.google.ru/>

**ОГЛАВЛЕНИЕ**

ВВЕДЕНИЕ ………………………………………………………........3

1. АУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ

С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИНЕ

«КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»….……4

1. ВНЕАУДИТОРНАЯ КОНТАКТНАЯ РАБОТА ПРЕПОДАВАТЕЛЯ С ОБУЧАЮЩИМИСЯ ПО ДИСЦИПЛИНЕ

«КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ»……...30

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА……………………………….31

РЕКОМЕНДУЕМЫЕ ИНТЕРНЕТ–САЙТЫ………………….........34

Перечень современных профессиональных баз данных и информационных справочных и

поисковых систем....................................................................34

**КРИМИНАЛИСТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ И ИССЛЕДОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

*Методические указания*

Составитель: **Помазанов** Виталий Викторович, **Грицаев** Сергей Иванович

Подписано в печать 00.00. Формат 60 × 84 1/16.

Усл. печ. л. – 0. Уч.– изд. л. – 0.

Тираж 000 экз. Заказ №000

Типография Кубанского государственного

аграрного университета.

350044, г. Краснодар, ул. Калинина, 13