

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»  
Институт математики, физики и информационных технологий  
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:  
Директор института



Н. Л. Королева  
«05» июля 2021 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.В.3 Компьютерная экспертиза

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2021

**Автор программы:**

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «18» мая 2021 г. Протокол № 9

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «05» июля 2021 г. № 5.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	8
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	40
6. Учебно-методическое и информационное обеспечение дисциплины.....	41
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	42

## 1. Цели и задачи дисциплины

1.1 Цель дисциплины – формирование компетенций:

ПК-4 Способен организовывать технологический процесс защиты информации в компьютерных системах

1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сфере: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере)

1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-4 Способен организовывать технологический процесс защиты информации в компьютерных системах	На основе результатов компьютерной экспертизы организует технологический процесс защиты информации в компьютерных системах

1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-4 Способен организовывать технологический процесс защиты информации в компьютерных системах

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения					
		Очная (семестр)					
		3	4	5	6	7	8
1	Аудит и аттестация объектов информатизации				+	+	
2	Защита информации от утечки по техническим каналам		+	+			
3	Микропроцессорная техника	+					
4	Основы электро- и радиоизмерений	+					
5	Преддипломная практика						+
6	Расследование компьютерных инцидентов					+	
7	Электроника и схемотехника	+					

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Компьютерная экспертиза» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Компьютерная экспертиза» изучается в 5 семестре.

## 3.Объем и содержание дисциплины

3.1.Объем дисциплины: 3 з.е.

Очная: 3 з.е.

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>108</b>
Контактная работа	64
Лекции (Лекции)	32
Лабораторные (Лаб. раб.)	32
Самостоятельная работа (СР)	44
Зачет	-

3.2.Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
5 семестр					
1	Компьютерные преступления.	6	4	8	Собеседование; выполнение практических заданий; Тестирование
2	Расследование инцидентов информационной безопасности.	6	4	8	Собеседование; выполнение практических заданий; Тестирование
3	Общая схема расследования преступления.	6	8	8	Собеседование; выполнение практических заданий; Тестирование
4	Сбор доказательств.	6	8	10	Собеседование; выполнение практических заданий; Тестирование

5	Действия правоохранительных органов по делам о преступлениях в сфере компьютерной информации.	8	8	10	Собеседование; выполнение практических заданий; Тестирование
---	---	---	---	----	--

### Тема 1. Компьютерные преступления. (ПК-4)

#### Лекция.

Понятие компьютерного преступления. Процедура компьютерной экспертизы. Правовая оценка преступления, определение к какой статье уголовного кодекса можно отнести данное преступление и дальнейшая передача материалов расследования данного дела в прокуратуру РФ.

#### Лабораторные работы.

1. Восстановление данных
2. Анализ файлов

#### Задания для самостоятельной работы.

1. Выделите предметы и задачи компьютерной экспертизы.
2. Что такое инцидент информационной безопасности.
3. Проведите анализ законодательной базой регулирования компьютерного преступления.
4. Какое деяние может считаться уголовно наказуемым.
5. Перечислите этапы компьютерной экспертизы.
6. На какие группы классифицируются лица совершившие компьютерные преступления.
7. Перечислите причины инцидента компьютерного преступления.
8. Что является объектами программно-компьютерной экспертизы.
9. На какие группы делятся методы исследования программного обеспечения.

### Тема 2. Расследование инцидентов информационной безопасности. (ПК-4)

#### Лекция.

Комиссия по расследованию инцидента информационной безопасности. Контекстный поиск информации на диске. Алгоритмы поиска данных. Программное обеспечение по сбору доказательств. Анализ истории и файлов браузера.

#### Лабораторные работы.

1. Просмотр и клонирование носителей данных.
2. Редактор двоичных файлов.
3. Сканирование локальной сети.

#### Задания для самостоятельной работы.

1. С помощью каких алгоритмов осуществляется поиск данных.
2. Какие файловых менеджеров используются и как они применяются.
3. Какие угрозы могут быть связаны с cookie файлами.
4. Способы получения злоумышленником информации из cookie файлов.
5. Перечислите методы предотвращения возникновения угрозы инцидента информационной безопасности.

### Тема 3. Общая схема расследования преступления. (ПК-4)

#### Лекция.

Установление факта и способа создания вредоносной программы для ЭВМ. Установление факта использования и распространения вредоносной программы. Установление лиц, виновных в создании, использовании и распространении вредоносных программ для ЭВМ. Установление вреда, причиненного данным преступлением.

#### **Лабораторные работы.**

1. Анализ времени активности компьютера.
2. Анализ локальной сети.
3. Восстановление данных.
4. Восстановление потерянных разделов.

#### **Задания для самостоятельной работы.**

1. Постройте схему организации взлома защитных механизмов информационных систем.
2. Какими законодательными актами регулируются наказания за неправомерный доступ к охраняемой законом информации.
3. Распишите общую схему расследования преступления.
4. Какие существуют признаки несанкционированного доступа.
5. Как определяется место и время совершения преступления.
6. Опишите последовательность действий расследования, создания и распространения вредоносного ПО.
7. Каким наказанием является за нарушение законодательства о «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»
8. Как доказать факты нарушения правил пользования ЭВМ.

### **Тема 4. Сбор доказательств. (ПК-4)**

#### **Лекция.**

Анализ файловых систем и файлов. Сбор доказательств в сетях. Анализ информации проходящей по проводной, радио, оптической и другим электромагнитным системам связи (электросвязи). Вопрос целесообразности и законности хранения информации о действиях пользователя. Сбор доказательств в социальных сетях.

#### **Лабораторные работы.**

1. Сбор данных о USB устройствах.
2. Блокировка и запрет работы с USB портами.

#### **Задания для самостоятельной работы.**

1. Как осуществляется поиск доказательств преступлений в файловой системе.
2. На что подразделяются следы в системных областях файловой системы.
3. Какие существуют методы сбора данных о пользователе.
5. Какой закон регулирует законодательный уровень накопления данных в сетях.
6. Какие самые популярные преступления в социальных сетях.

### **Тема 5. Действия правоохранительных органов по делам о преступлениях в сфере компьютерной информации. (ПК-4)**

#### **Лекция.**

Обыск и выемка компьютерных объектов. Осмотр отдельных видов компьютерных объектов. Назначение компьютерных экспертиз. Допрос. Подготовка и проведение следственного эксперимента.

#### **Лабораторные работы.**

1. Информация о зарегистрированных доменах.
2. Аудит компьютерной системы.

#### **Задания для самостоятельной работы.**

1. Какие объекты способны по своим физико-техническим свойствам содержать информацию, имеющую отношение к расследуемому преступлению.

2. Как различают обыск по последовательности проведения.
3. На какие группы разделяются объекты следственного действия (компьютерная техника и компьютерная информация).
4. Что относится к объектам компьютерно-технической экспертизы.
5. Какие задачи решаются с помощью компьютерно-технической экспертизы.
6. Какой перечень вопросов может выноситься на разрешения компьютерно-технической экспертизы.
7. Что нужно для проведения следственного эксперимента.

#### 4. Контроль знаний обучающихся и типовые оценочные средства

##### 4.1. Распределение баллов:

5 семестр

- посещаемость – 10 баллов
- текущий контроль – 70 баллов
- контрольные срезы – 2 среза по 10 баллов каждый
- премиальные баллы – 20 баллов

##### Распределение баллов по заданиям:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
---------------	--	--	--------------------------	--------------------------------------



1.	Компьютерные преступления.	Собеседование	3	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>3 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>1 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		выполнение практических заданий	6	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>6 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестирование	10	<p>10 баллов – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

2.	Расследование инцидентов информационной безопасности.	Собеседование	3	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>3 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>1 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		выполнение практических заданий	4	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>
		Тестирование(контрольный срез)	10	<p>10 баллов – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

3.	Общая схема расследования преступления.	Собеседование	3	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>3 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>1 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		выполнение практических заданий	3	<p>Практические работы выполняются самостоятельно или в малой группе (2-3 студента) на оборудовании или компьютерных классах по текущему разделу или темы дисциплины.</p> <p>Основные качества выполненного практического задания подлежащего оценке: полнота и точность выявления характеристик; оригинальность практического решения; полнота достигнутых показателей; детальность описания и наглядность схем и алгоритмов; наличие тестовых примеров, качество работы.</p>
		Тестирование	10	<p>10 баллов – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

4.	Сбор доказательств.	Собеседо вание	3	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>3 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>1 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		выполнен ие практичес ких заданий	6	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>6 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенны ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестиров ание(кон трольны й срез)	10	<p>10 баллов – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

5.	Действия правоохранительных органов по делам о преступлениях в сфере компьютерной информации.	Собеседование	3	<p>Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.</p> <p>Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:</p> <ul style="list-style-type: none"> <li>- правильность ответа по содержанию;</li> <li>- полнота и глубина ответа;</li> <li>- сознательность ответа;</li> <li>- логика изложения материала;</li> <li>- рациональность использованных приемов и способов решения поставленной учебной задачи;</li> <li>- своевременность и эффективность использования наглядных пособий и технических средств при ответе;</li> <li>- использование дополнительного материала;</li> <li>- рациональность использования времени, отведенного на задание.</li> </ul> <p>3 баллов – студент умеет сопоставить полученную при подготовке к практическому занятию информацию, сравнивать разные точки зрения на анализируемую проблему, уметь четко формулировать свои вопросы и отвечать на задаваемые ему вопросы</p> <p>2 баллов - студент умеет применять полученную при подготовке к практическому занятию информацию, отвечать на большинство вопросов, вести дискуссию .</p> <p>1 балла – студент владеет теоретическим материалом по теме практического занятия, иногда затрудняется при ответе на вопросы, не умеет сформулировать свою точку зрения на обсуждаемую проблему</p> <p>Если студент не владеет проблематикой практического занятия, не может отвечать на вопросы, зачитывает ответ по напечатанному тексту – ответ баллами не оценивается.</p>
		выполнение практических заданий	6	<p>Лабораторные работы выполняются по тематике практических занятий.</p> <p>6 баллов – лабораторная работа выполнена в полном объеме, студент свободно владеет материалом, демонстрирует глубокие, систематизированные знания, свободно отвечает на вопросы используя профессиональную терминологию</p> <p>4 балла – лабораторная работа выполнена, но имеет некоторые неточности выполнения, студент владеет представленным материалом, отвечает на заданные вопросы</p> <p>2 балла - лабораторная работа в целом выполнена, однако в процессе выполнения лабораторной работы допущены существенные ошибки, студент слабо владеет информацией по теме, при ответе использует заготовленный текст, затрудняется с ответами на задаваемые вопросы</p>
		Тестирование	10	<p>10 баллов – студент правильно отвечает на 50-100% вопросов в тесте</p> <p>5 баллов - студент правильно отвечает на 25-50% вопросов в тесте.</p> <p>Менее 25% правильных ответов баллов не дает</p>

6.	Посещаемость	10	10 баллов – стопроцентное посещение занятий студентом 8 баллов – посещаемость студента составляет не менее 80 % занятий 5 балла – посещаемость студента составляет не менее 50 % занятий 2 балл – посещаемость студента составляет не менее 25 % занятий
7.	Премияльные баллы	20	Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции / журнале из перечня ВАК – 10 / 15 / 20
8.	Индивидуальные задания, с помощью которых можно набрать дополнительные баллы	20	Решение кейса (10 баллов) Прохождение тестирования (30 вопросов) по всему курсу дисциплины (10 баллов)
9.	Итого за семестр	100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

#### 4.2 Типовые оценочные средства текущего контроля

##### **выполнение практических заданий**

##### **Тема 1. Компьютерные преступления.**

Лабораторная работа. Восстановление данных.

Содержание

Описание продукта

Системные требования

Ход работы

Задание №1. Установка программного продукта

Задание №2. Провести анализ скорости чтения локальных дисков

Задание №3. Провести проверку диска на наличие ошибок файловой системы

Задание №4. Изучить сведения о жестком диске

HardDiskInformation содержит следующую информацию: тип файловой системы, серийное значение диска, кол-во байт в секторе, кол-во всего кластеров, кол-во свободных кластеров, физический номер диска и другое.

Задание №5 Изучить информацию об оптических дисках

Задание №6 Удаление программного продукта

## Описание продукта

DriveManager – программа, позволяющая легко следить за состоянием жестких дисков. Она отображает информацию о каждом разделе жесткого диска, например, размер, метку тома, общий и свободный объем и т.д. Но самая важная функция программы заключается в том, что она содержит тесты на чтение/запись информации и на наличие ошибок, которые можно исправить на ходу.

Данная программа не требовательна к системным ресурсам и позволяет в режиме реального времени получать информацию о вашем жестком диске и всех разделах, находящихся на нём. Поддерживается работа сразу несколькими физическими винчестерами. При необходимости можно посмотреть данные и о CD/DVD приводах, подключённых в системе.

DriveManager автоматически обновляет данные о дисках каждые 20 секунд и показывает следующую информацию: имя диска, букву диска, тип диска, размер, свободное и занятое дисковое пространство, процентное соотношение свободного и занятого пространства, файловую систему и серийный номер. Кроме того, утилита позволяет сделать невидимым из Проводника Windows любой раздел жесткого диска.

### Drive Manager Функциональность

DriveManager будет постоянно отслеживать пространство, доступное для каждого из дисков в системе. Вы также можете открыть диск в проводнике, дважды щелкнув на нем.

Он автоматически обновляется каждые 30 секунд. В этом экономит того, чтобы использовать "Мой компьютер" в windows, а затем изменить представления отчета. Можно принудительно обновить в любой момент, нажав клавишу F5.

### Объемные Наклейки

Метка Тома выводится для всех съемных дисков, а также локальные диски. Это полезно, если у вас много флэш-накопители или smartmedia, compactflash и др.

### Серийные Номера

Серийный номер столбца полезен для того, чтобы отследить, на каком жестком диске или для выхода из вас сайта жесткий диск серийный номер.

### Скрытие дисков

Отдельные диски могут быть скрыты от Windows explorer. Вы можете сделать это, нажав правой кнопкой мыши на диске и выбрав Спрятать Диск из всплывающего меню. Диски по-прежнему будут отображаться в менеджер дисков, так что вы можете сделать потом снова стал видимым и теперь отображаются синим цветом.

### Subst

DriveManager может быть использован в качестве Windows-версию DOS "subst" команда для создания заменить буквы диска для локальных папок как способ ведения локальных дисков. Он также показывает Вам, где subst буквы указывают в колонке "Тип".

### Особенности Drive Manager

1. Процент свободного столбца.
2. Жесткий диск серийный номер
3. CD-ROM двери open + close.
4. Заблокировать / разблокировать CD-ROM / DVD-дисков.
5. Не подключенных дисков, перечисленных в серо-диски не установлена.
6. Время и дата.
7. Карта / отключать сетевые диски.
8. Hide / Unhide диски от проводника.
9. Свойства диска диалоговое меню правой кнопкой мыши.
10. Создать / удалить заменить букву для локальной папке.
11. Скрытые диски отображаются синим цветом.
12. Запуск Windows Search

13. Диски с менее чем 5% свободного отображаются красным цветом.

14. Сведения о поставщике: наименование поставщика, код продукта, ревизию, Спес поставщиков

15. Тип шины: позволяет Вам видеть, как ваши диски подключены к вашей системе

Системные требования

Статус программы - Бесплатная

ОС - Windows 8, 7, Vista, XP

Интерфейс - Английский

Разработчик - AlexNolan

Категории программы - HDD утилиты

Ход работы

Задание №1. Установка программного продукта.

Для выполнения задания необходимо выполнить следующее действие:

1. Зайдите на сайт разработчика <http://www.alexnolan.net/software/driveman.htm> и скачайте новую версию продукта.

2. Следуйте инструкциям процесса установки

3. Запустить программу Drive Manager.

Задание №2. Провести анализ скорости чтения локальных дисков

Для выполнения этого задания, необходимо выполнить следующие действия:

1. В главном окне программы на панели инструментов выбрать кнопку «DiskSpeed»

2. Выбрать локальные диски – поставить галочку напротив «Local»

3. Нажать «Benchmark»

Задание №3. Провести проверку диска на наличие ошибок файловой системы

В главном окне программы выбираем диск. Затем на вкладке «Drives»выбираем «Properties». Потом переходим на вкладку «Сервис» и нажимаем на кнопку «Проверить»

Задание №4. Изучить сведения о жестком диске

Данные жесткого диска экран был полностью переработан, в версии 4.11 DriveManager.

Для выполнения задачи нужно проделать задачи:

1. В главном окне программы выбираем нужный диск

2. На панели инструментов выбираем «DiskInfo»

HardDiskInformationсодержит следующую информацию: тип файловой системы, серийное значение диска, кол-во байт в секторе, кол-во всего кластеров, кол-во свободных кластеров, физический номер диска и другое.

Задание №5. Изучить информацию об оптических дисках

Информация об оптических дисках, таких как CD / DVD дисков отображается в DriveManager. Вы также можете скачать оптический info в виде отдельного файла программы. Для выполнения этого задания, выполните следующие пункты:

1. Вставьте в дисковод диск CD / DVD

2. Навкладке «Optical» выберете «Optical Inforamtion»

Задание №6. Удаление программного продукта

Если нужно удалить DriveManager, следует воспользоваться опцией Установка и удаление программ для Изменения/Удаления программ через Панель управления Windows. Следовать инструкциям деинсталлятора.

Контрольные вопросы и задания

1. Скрыть буквы у логических дисков.

2. Создать логический диск R и при открытие его открывалась папка Мои документы. (По окончании выполнения этого задания не забудьте удалить созданный логический диск)

3. Изучить S.M.A.R.T. информацию всех логических дисков

4. Проанализируйте скорость чтения данных и проверьте на наличие ошибок файловой системы вашей USB- Flash.



5. Скрыть логический диск

6. Просканируйте локальный диск на наличие исправленных ошибок и установленных драйверов.

Лабораторная работа. Анализ файлов.

Содержание

Описание продукта

Системные требования

Ход работы \

Задание №1. Установка программного продукта

Задание №2. Провести аудит установленных программ, ОС, сеть Windows, сеть TCP/IP, службы и драйвера, и автозагрузки программ в ПК

Задание №3. Сохранить результаты аудита в формате pdf с разрешением копировать содержимое

Задание №4. Сохранить результаты аудита в виде PDF-документа с паролем Смит через командную строку

Задание 5 Поиск файлов с расширением \*.exe

Задание №6 Экспорт результатов аудита в БД MicrosoftAccess

Задание №7 Удаление программного продукта

Контрольные задания

Описание продукта

Простая в установке программа: приложение использует интерактивные контроли выбора устройств и папок для того, чтобы позволить пользователю найти устройство или папку для анализа.

Простая в оперировании программа: данное приложение имеет операции Старта и Стопа в один щелчок. Готовая для анализа, щелкните на старт. Если вы хотите быстро выйти из анализа, щелкните на стоп (что может быть проще?!).

Быстрый анализ: результаты производительности варьируются от конфигурации машины, но когда мы запускали данную программу, мы смогли проанализировать более 200000 файлов с общим размером около 80 гигабайт за 39 секунд. Данное приложение работает быстрее, чем вы успеете прочитать статусное сообщение, которое всплывает во время процесса анализа.

Конфигурация: хотите скрыть приложение во время выполнения процесса анализа? Не хотите просматривать отчеты, когда приложение завершит работу? Настройте приложение на то, что вы хотите.

Тихое выполнение: используйте командную строку для ввода путей для анализа, и приложение будет исполнять и завершать все операции без чьего либо ведома. Выполняйте различные операции по анализу и составьте расписание выполнения, используя календарь.

Мощные функции отчетности: когда анализ завершен, приложение выводит отчет в текстовом формате, который автоматически открывается для просмотра. Отчет содержит путь к файлу или папке, размер и дату последнего изменения файла.

Импортируемый вывод: отчеты могут выводиться в CSV формате, что позволяет импортировать данные в практически любые приложения, которые работают с широкоформатными таблицами.

Это приложение декодирует и анализирует некоторые специальные файлы, используемые ОС Windows. В этих файлах интересная информация для судебно-медицинской экспертизы. Каждые результаты анализа могут быть напечатаны в удобной для пользователя форме.

Он создан в многодокументного интерфейса. Здесь описаны отдельные анализаторы:

Windows XP Миниатюра База данных Анализатор

Анализатор считывает Thumbs.db файл и отображает его содержимое с сохраненными данными включают предварительный просмотр изображения.

### ACDSee Миниатюра База данных Анализатор

Анализатор считывает ACDSee \*. FPT файл и отображает его содержимое с сохраненные данные включают предварительный просмотр изображения.

### GooglePicasa Миниатюра База данных Анализатор

Анализатор считывает Picasa \*. db файл и отображает его содержимое с сохраненные данные включают предварительный просмотр изображения.

### FastStone просмотра Миниатюра База данных Анализатор

Анализатор считывает fsviewer.db файл и отображает его содержимое с сохраненными данными включают предварительный просмотр изображения.

### Цифровой обработки изображений HP Миниатюра База данных Анализатор

Анализатор считывает \*. дБ или \*. DAT-файл и отображает его содержимое с сохраненными данными включают предварительный просмотр изображения.

### Prefetch Анализатор

Она читает файлы, хранящиеся обычно в папке Prefetch и Диггс из хранимой более подробных сведений.

### Ярлык Анализатор

Этот инструмент читает все сочетания файлы в указанной папке и отображает данные, хранящиеся в них.

### Index.dat Analyzer

Анализатор считывает указанный файл index.dat и отображает его содержимое. Index.dat файлы магазин обычно включает данные InternetExplorerкуки, временные файлы или истории.

### Корзина Анализатор

Анализатор декодирует и отображает info2 файлы, которые держат очищение корзины информацию о содержимом.

### Системные требования

1. Целевые платформы - Windows 2000, Windows XP, Windows 2003, Windows Vista, Windows 7, Windows Server 2008, Windows Server 2008 R2
2. Лицензия - Бесплатный в использовании как для частных, так и коммерческих пользователей.
3. Категория - Файловые менеджеры/поиск

### Ход работы

#### Задание №1. Установка программного продукта.

Для выполнения задания необходимо выполнить следующее действие:

1. Зайдите на сайт разработчика <http://www.mitec.cz/> и скачайте новую версию продукта. Windows FileAnalyzer - " готов к работе". Она была составлена так, что вы не должны проходить через процедуру установки.

#### Задание №2. Провести анализ Index.Dat

Для выполнения задания, выполните следующие действия(см. рис.1)

1. Во вкладке «Файл» выберете пункт «Анализ Index.Dat»нажмите «Открыть»
  2. Перейти по следующему адресу: «C:\DocumentsandSettings\Имя пользователя\Cookies\index.dat»
- Для рассмотрения деталей, щелкните по одному из элементов списка два раза

#### Задание №3. Провести анализ папки «C:\Windows\Prefetch»и сделать отчет в масштабе 150%

Для успешного выполнения этого задания, необходимо проделать следующие пункты:

1. Во вкладке «Файл» выберете «AnalyzePrefetch»
2. В появившемся окне выберете папку «Prefetch»
3. В результате появится список файлов с расширением \*.exe
4. В правом верхнем углу нажмите «Report» и выберете масштаб – 150%

#### Задание №4. Проанализировать недавние документы

Вы полните следующие пункты:

1. Во вкладке «Файл» выберете «AnalyzerShortcuts»

2. Выберите папку «Недавние документы»

3. Нажмите «ОК»

Данный анализ показывает когда был создан тот или иной файл, перезаписан и последнее время запуска. А также размер этого файла и откуда он запускался.

Задание №5. Удаление программного продукта

Так как FileAnalyzer не устанавливает какие-либо файлы на компьютер, деинсталлировать его стандартными средствами Windows нет необходимости. Достаточно просто удалить файл программы File Analyzer.exe.

Контрольные вопросы и задания

1. Провести анализ папок «Загрузки» и «Мои документы». Текст отчета выравнивать по ширине страницы.
2. Провести анализ историю cookie-файлов. Предоставить отчет в масштабе 200%.
3. Проанализировать папку Prefetch.
4. Проанализировать папку «Недавние документы»
5. Проанализировать состояние корзины и определить когда был удален последний файл. Текст отчета выравнивать по ширине страницы и в масштабе 150%.

## Тема 2. Расследование инцидентов информационной безопасности.

Лабораторная работа. Просмотр и клонирование носителей данных.

FTK Imager — программа для просмотра и клонирования носителей данных в среде Windows.

Возможности:

- Просмотр файлов и директорий на подключенных носителях данных;
- Создание точных копий подключенных носителей данных (в форматах dd, EnCase, SMART);
- Создание копий отдельных файлов и директорий;
- Экспорт хеш-значений для файлов;
- Обнаружение использования EFS;
- Экспорт файлов реестра с работающей системы.

Для запуска программы необходимо запустить WinTaylor и выбрать соответствующий пункт FTK Imager

Откроется главное окно программы

Добавление источника данных. Для добавления источника данных необходимо выбрать вкладку fail -> Add Evidence item

В появившемся окне нам необходимо выбрать, что будет являться источником для последующих операций: физический носитель, логический, файл образа, выбрать папку.

После выбора соответствующего источника в левой части программы появится источник в виде дерева каталогов

Нам доступны следующие действия над корневым источником, или же мы можем выбрать отдельную папку или файл в источнике: копировать полностью выбранные файлы в новое место, получить хэш-лист файлов в виде .csv формата, создать образ.

Полное копирование

Для полного копирования необходимо выполнить следующие действия: кликнуть по элементу, который нам необходимо скопировать правой кнопкой мыши, выбрать Export Files и затем выбрать папку назначения

В данном примере мы выбрали в качестве примера папку !\_задача 1 и скопировали в папку Taylor на рабочем столе. На следующем скриншоте вы можете увидеть результат выполненной операции

Экспорт хэш-листа в формате.csv

Для экспорта хэш-листа в формате .csv необходимо выполнить следующие действия:

1. Выбрать исходный файл или папку

2. Нажать в программе правой кнопкой на файл / папку и выбрать Export Fail Hash List
3. В появившемся окне выбрать папку назначения и название файла куда будут импортированы все значения

#### Создание образа

Для создания образа необходимо выполнить следующие действия:

1. Выбрать файлы которые мы хотим поместить в образ
2. Нажать правой кнопкой по директории и выбрать Export Logial Driver
3. В появившемся окне ввести всю необходимую информацию о образе.
4. Ввести имя образа и папку назначения.
5. Нажать Start

#### Контрольные вопросы и задания:

1. Для чего служит Ftk Imager
2. Как выбрать источник данных для выполнения задачи
3. Как выполнить полное копирование выбранной папки
4. Поддерживает ли программа копирование образов
5. Как выполнить копирование хэш значения в .csv формате
6. Как создать образ из выбранных файлов
7. Удалите источник данных выбранного на втором этапе

#### Лабораторная работа. Редактор двоичных файлов. Содержание

##### Описание продукта

##### Системные требования

##### Ход работы

Задание №1. Установка программного продукта.

Задание №2. Вывести содержимое System Management BIOS

Задание №3. Вывести содержимое секторов №3,4,5,6 с Flash-носителя

Задание №4. Настроить HexEdit по следующим параметрам: OffsetDisplay – Dec, LineSize – 32 bytes, Grid, MarkZeros

Задание №5 Взлом системы авторизации пользователей при помощи HexEdit

Задание №6 Изменение файла типа \*.exe при помощи HexEdit

Задание №7 Удаление программного продукта

##### Контрольные задания

##### Описание продукта

HexEdit - редактор двоичных файлов. Предназначен для редактирования игр, программ и т.д., и т.п. Запоминает положение окна, неограниченный размер редактируемого файла, новая версия калькулятора, минимизируется в трей, запоминает список файлов. HexEdit является мощным редактором в шестнадцатеричной системе со следующими особенностями:

1. Интерфейс MDI
2. Инспектор данных
3. Калькулятор
4. Сравнение файлов
5. Буфер памяти
6. Хранитель диска (NT только)

##### Системные требования

1. Целевые платформы - Windows 2000 Windows XP Windows 2003 Windows Vista Windows 7
2. Лицензия - Бесплатная в использовании, как для частных, так и коммерческих пользователей.

##### Ход работы

Задание №1. Установка программного продукта.

Для выполнения задания необходимо выполнить следующее действие:

1. Зайдите на сайт разработчика [http://www.skan.ru/software/n355\\_hexedit.html](http://www.skan.ru/software/n355_hexedit.html) и скачайте новую версию продукта.

HexEdit-"готов к работе". Она была составлена так, что вы не должны проходить через процедуру установки.

**Задание №2.** Вывести содержимое System Management BIOS

Для выполнения задания, выполните следующие действия

1. В главном окне программы, выберете вкладку «File»
2. Выберете «Memory»
3. Затем выберете «SMBIOS»
4. Нажмите «OK»

Слева расположена информационная панель, которая отображает всю необходимую информацию – контрольные суммы (CRC 32, MD5), DataSize, Position и т.д. Кроме того, рядом с таблицей можем увидеть:

Слева от матрицы отображается линейка (0x000, 0x010 и т.д.) из чисел: каждой строчке соответствует число, означающее адрес/смещение первого байта этой строчки. Шаг адресов при этом равен количеству колонок.

Сверху от матрицы отображается другая линейка (0001, 0203, 0405 и т.д.) из чисел: над каждой колонкой отображается смещение байта, стоящего в этой колонке, относительно первого байта соответствующей строчки. Сумма числа, соответствующего i-той строке, и числа, соответствующего j-той колонке является адресом/смещением байта (i;j), стоящего на пересечении взятой строки и взятого столбца.

Справа от матрицы могут отображаться те же данные, но в другой интерпретации. Наиболее часто используется альтернативное отображение данных как текста в кодировке ASCII (на рисунке показаны в крайнем правом столбце), при этом байты, значения которых соответствуют непечатаемым символам, отображаются как точки (·).

**Задание №3.** Вывести содержимое секторов №3,4,5,6 с Flash-носителя

Для выполнения, сделайте следующие действия:

1. Вставьте в компьютер Flash-носитель
2. В главном окне программы, во вкладке «File» выберете «Disk»
3. В появившемся окне выберете любой Flash-носитель
4. Внизу введите значение «2» в поле «Starting sector», а в поле «Sector store read» - «4»
5. Нажмите «OK»
6. Результат

**Задание №4.** Настроить HexEdit по следующим параметрам: OffsetDisplay – Dec, LineSize– 32 bytes, Grid, MarkZeros

Для выполнения, сделайте следующие действия в главном окне программы:

1. Во вкладке «Format», в пункте «OffsetDisplay» выберете значение DEC
2. В пункте «LineSize» выберете значение 32 байта
3. Отметьте галочкой пункт GRID
4. Во вкладке «Tools», отметьте галочкой пункт MarkZeros

**Задание №5.** Взлом системы авторизации пользователей при помощи HexEdit

В папке, где находится данный текст находится файл Enter\_Of\_System.exe, которая имитирует процесс авторизации пользователей. Система имеет 2-х пользователей Student и Administrator. После успешной авторизации пользователя система выдает сообщение о том, что пользователь вошел в систему под Student или под Administrator. Наша задача состоит, чтобы узнать логины и пароли этих пользователей.

Для этого выполните следующие пункты в главном окне программы:

1. Откройте файл Enter\_Of\_System.exe
2. Для более быстрого поиска необходимого воспользуемся поиском текста в файле. Для этого нажмем «Ctrl+F» и введем Form и нажмем ОК. После слова Form видим название программы Enter\_Of\_System.

3. Прodelайте несколько раз шаг 2 до тех пор пока не найдете строку «FormBorderStyle».
4. Чуть ниже находим строки (t.e.x.t.B.o.x.l. и т.д.) и в них находим интересные строки (S.t.u.d.e.n.t. . 5.5.5. . = .. .....A.d.m.i.n. i.n.t.e.r.8.g.t.6... = A.d.m.i.n). Вот и нашли логины и пароли от пользователей системы. Осталось проверить они ли это.(см. рис. 8)
5. Запустите программу Enter\_Of\_System.exe и введите по очереди: Student – 555; Admin – inter8gt6;Как видно они правильные.

Задание №6. Изменение файла типа \*.exe при помощи HexEdit

Выполните следующие действия в главном окне программы:

1. Откройте файл Enter\_Of\_System – копия.exe
2. Найдите строку, где хранится имя формы (Welcome)
3. Измените это название на «Systems»
4. Сохраните (см. рис. 13)

Задание №7 Удаление программного продукта

Так как HexEdit не устанавливает какие-либо файлы на компьютер, деинсталлировать его стандартными средствами Windows нет необходимости. Достаточно просто удалить файл программы HexEdit.exe.

Контрольные вопросы и задания

1. Проанализировать содержимое DiskDumpFlash-носителя.
2. Проанализировать содержимое MemoryDumpBIOSи VideoBIOS.
3. В папке, где находится данная лабораторная работа есть файл (Enter\_Of\_System2.exe), который имитирует вход пользователей в систему. Система имеет 2-х пользователей. Узнайте логины и пароли этих пользователей и войдите в систему под каждым пользователем.
4. Настройте HexEdit последующим параметрам: OffsetDisplay – Oct, LineSize – 64 bytes, Grid, MarkZeros, Unicode Chars.
5. Измените в файле Enter\_Of\_System2.exe название формы на EnterSys

Лабораторная работа. Сканирование локальной сети.

LAN Scanner - это программа для сканирования локальной сети, которая использует метод многопоточного сканирования, позволяя осуществлять сканирование более 1000 элементов в секунду. При использовании программы для сканирования портов, можно осуществлять сканирование всех 65536 портов менее чем за минуту.

Кроме сверхбыстрого сканирования, программа обладает также рядом других отличительных черт: получение детальной информации об удаленных компьютерах без установки на них дополнительного ПО; сканирование под указанными правами; широкие возможности экспорта и импорта результатов сканирования, включая поддержку скриптов для пользовательских форматов экспорта.

Операционные системы:

Windows 95/98/ME/NT4.0/2000/XP/2003/Vista/2008 и Windows 7 (32 бит, 64 бит)

I. Запуск программы

Для запуска программы необходимо выбрать соответствующую кнопку главного окна программы. После нажатия кнопки «LanScanner» откроется главное окно программы.

II. Scan Ports

В окне ScanPorts осуществляется сканирование портов. Для того чтобы провести сканирование необходимо указать начальный IP–адрес (или имя сервера) и конечный IP–адрес.

В этом же окне указываются параметры сканирования.

Для запуска сканирования необходимо нажать «Scan», чтобы сохранить полученный результат «Save» и указать путь сохранения результата.

III. Search Devices

В окне SearchDevices можно произвести поиск устройств, таких как принтеры, маршрутизаторы, другие какие-либо сетевые устройства, даже если не знаем их IP-адрес.

Чтобы сохранить результат сканирования необходимо нажать «Save» и указать путь сохранения результата.

#### IV. Ping Devices

В окне PingDevices можно пропинговать устройства, указав их IP-адрес (имя сервера)

Чтобы сохранить результат сканирования необходимо нажать «Save» и указать путь сохранения результата.

#### V. Контрольные вопросы и задания

1. Для чего служит программа LanScanner?
2. Какими свойствами обладает программа LanScanner?
3. В каком окне можно произвести поиск устройств, даже не зная их IP-адресов?
4. Проведите сканирование наиболее распространенных портов и сохраните результат сканирования
5. Проведите сканирование, выбрав отдельные порты, и сохраните результат
6. Проведите поиск устройств (принтеры, маршрутизаторы) и сохраните результат
7. Пропингуйте устройство с помощью увеличенных пакетов
8. Проверьте связь с устройством

### Тема 3. Общая схема расследования преступления.

Лабораторная работа. Анализ времени активности компьютера.

Анализ времени активности компьютера помогает определить сколько и в какой день компьютер был в рабочем состоянии. Графическое оформление позволяет определить общее количество времени работы компьютера за день и за все время, среднее количество времени включения, промежутки времени работы.

Это необходимо при компьютерной экспертизе, если нужно определить в какое время компьютер работал и мог ли использоваться в противоправных действиях.

Для анализа необходимо запустить PC On/Off. Для этого в окне Wintaylor нажать кнопку PC On/Off.

В появившемся окне представлен график работы компьютера. Вверху указаны часы, а слева число месяца и день недели.

Провести выбор компьютера

При анализе сети компьютеров необходимо узнать время активности других компьютеров. Это используется для проведения компьютерной экспертизы.

При нажатии кнопки Browse откроется окно с выбором компьютера в Сетевом окружении

Настройка визуального оформления

Изменение цвета для отображения времени работы компьютера способствует улучшению визуального восприятия.

Для этого необходимо щелкнуть левой кнопкой мыши на графике. Появится окно настройки цвета визуального отображения активности компьютера.

Отчет

Общее количество времени, а также время за сутки позволяют использовать эти данные как доказательства в судебном процессе.

#### Контрольные вопросы и задания

1. Для чего используется утилита PC On/Off?
2. Как можно узнать общее количество времени работы компьютера за последние три недели?
3. Каким образом можно изменить графическое представление времени работы компьютера?
4. Как использовать утилиту при анализе сети?
5. Как определить среднее время работы компьютера за последние три недели?
6. С помощью утилиты как можно узнать имя компьютера?
7. Определить в какой день компьютер был активен больше всего.

Лабораторная работа. Анализ локальной сети.

Программа сканирует компьютеры в сети и позволяет получить различную информацию, например: пинг, доменное имя, NETBIOS имена, MAC адрес и т.п.

В качестве параметров сканирования можно использовать:

- диапазон IP адресов;
- имя компьютера;
- имена компьютеров, перечисленные через запятую.

После сканирования с любым из перечисленных параметров будет выведена вся доступная информация об удаленном компьютере. Для получения информации используются функции API Windows.

Таким образом, можете приступать к сканированию сети на предмет наличия разделяемых ресурсов.

Программа позволяет:

Анализировать наличие компьютеров в локальной сети в заданном IP диапазоне адресов. Список найденных компьютеров хранится в памяти, поэтому в любой момент его можно пересканировать тем самым сэкономить время при сканировании всей подсети;

Анализировать ресурсы компьютеров в локальной сети по заданному критерию. В качестве критерия могут выступать папки с определённым именем, проверка наличия FTP и HTTP серверов. При этом содержимое корневой директории FTP сервера может показываться полностью.

Эти возможности позволяют говорить о программе как о незаменимом инструменте для поиска нужной информации в локальных сетях за минимальное время.

Необязательно каждый раз определять имя компьютера при сканировании, т.к. программа запоминает его и далее вы можете уже не определять имя компьютера, программой будет автоматически подставлено последнее известное имя.

Сканирование портов:

PortScan показывает все открытые порты и дополнительную информацию, как имя хоста, MAC-адрес, HTTP, SMB, FTP, iSCSI, SMTP и SNMP. Поддерживает до 100 потоков для просмотра больших диапазонов IP-адресов. Имеет возможность просматривать открытые SMB ресурсы (папки или диски общего доступа). А также стандартные порты.

Search Devices:

Есть возможность искать UPnP устройства, типа Bonjour, маршрутизаторов, принтеров, принтер (SLP / Service Location Protocol) и сетевых устройств устройств. Можно найти их, даже если нет информации об IP адресе.

Контрольные вопросы и задания:

1. Определить какие девайсы расположены в вашей локальной сети.
2. Пропингуйте сервер ya.ru
3. Определите MAC адрес любого известного вам IP адреса.
4. Проведите сканирование всего диапазона своей локальной сети.
5. Проведите анализ открытых ресурсов на любом известном вам IP адресе.

Лабораторная работа. Восстановление данных. Содержание

Описание продукта

Системные требования

Ход работы

Задание №1. Установка программного продукта

Задание №2. Провести анализ логического диска и результат сохранить в txt формате

Задание №3. Провести анализ логического диска на восстановление файлов документов и вывести результат в режиме древовидного показа

В главном окне программы выбираем нужный логический диск. Затем в списке файлов выберете «Документы».

Задание №4. Восстановить файлы графики на логическом диске

Задание №5 Настроить Recuva по следующим параметрам: показывать файлы из скрытых/системных папок, файлы с нулевым размером, показывать надежно удаленные файлы.

Задание №6 Удаление программного продукта

Контрольные задания



## Описание продукта

Recuva — бесплатная утилита, которая предоставляет пользователям мощный и простой в использовании инструмент для восстановления потерянных (в результате программного сбоя или удаленных) данных. Утилита была создана британской частной фирмой Piriform Limited и написана на C++. У большинства программ технического толка – всевозможных оптимизаторов, "очистителей" реестра и

подобных - есть одна серьезная проблема – слишком сложный интерфейс, в котором неискушенному пользователю порой достаточно трудно разобраться. Recuva создавалась для простых пользователей, поэтому пользоваться программой может любой человек, знакомый с системой Windows.

Возможности Recuva :

1. Сканировать ваш жесткий диск, карты памяти, usb носители, а также ipod, чтобы найти и попытаться восстановить удаленные файлы.
2. Быстро предоставить данные насколько полно и качественно возможно восстановление.
3. Восстановить файлы, которые Windows не может.
4. Надежно удалить файлы, так чтобы их никто не смог восстановить.
5. Восстановить удаленную из корзины почту в Microsoft Outlook Express, Mozilla Thunderbird и Windows Live Mail.
6. Восстановить музыку на iPod, iPod Nano и iPod Shuffle. (Пока правда нельзя это сделать iPhone и iPod Touch)
7. Восстановить файлы формата Canon RAW. (\*.CRW)

Recuva не может:

1. Восстановить идеально вообще все файлы. К сожалению, такая ситуация на данный момент не осуществима. Утерянные документы воссоздаются из их остатков на жестком диске. Но со временем они также затираются, поэтому не всегда все можно восстановить.
2. Воссоздать файлы после безопасного удаления. (Безопасно удаляет, например, сама Recuva)

Системные требования

Утилита работает в операционных системах семейства Microsoft Windows, в частности на Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 и Windows 8.1 включая 32-битных и 64-разрядных версий платформ.

Recuva работает только с дисковыми системами следующих типов: NTFS, FAT, а также exFAT.

Ход работы

Задание №1. Установка программного продукта.

Для выполнения задания необходимо выполнить следующее действие:

1. Зайдите на сайт разработчика <http://getrecuva.ru/> и скачайте новую версию продукта.
2. Следуйте инструкциям процесса установки
3. Запустить программу Recuva.

Задание №2. Провести анализ логического диска и результат сохранить в txt формате

Для выполнения задания, необходимо выполнить следующие действия:

1. В главном окне программы выберете нужный логический диск
2. Нажимаем на кнопку «Анализ»

После того как был выполнен анализ логического диска, нажимаем ПКМ в поле, где отображены файлы и выбираем «Сохранить список файлов как текст»

Задание №3. Провести анализ логического диска на восстановление файлов документов и вывести результат в режиме древовидного показа

В главном окне программы выбираем нужный логический диск. Затем в списке файлов выберете «Документы».

Для того чтобы результат показывался в режиме древовидного показа нужно: Зайти в настройки и выбрать режим показа – «Древовидный»

Задание №4. Восстановить файлы графики на логическом диске

Для выполнения задания, необходимо выполнить следующие действия:

1. В главном окне программы выбрать нужный логический диск или съемное запоминающее устройство
2. Выбрать маску файлов под названием «Графика»
3. Нажать кнопку «Анализ»
4. После того выберете те файлы, которые могут успешно восстановить. Обратите внимание, иконки, слева от имени файла, показывают вероятность полного восстановления. Зеленый - очень высокая, желтый - средняя, красный - низкая.
5. Нажать кнопку восстановить
6. Выберете папку или диск, куда хотите восстановить файл или файлы

Задание №5. Настроить Rescuva по следующим параметрам: показывать файлы из скрытых/системных папок, файлы с нулевым размером, показывать надежно удаленные файлы.

Для выполнения этого задания выполните следующее:

1. Зайдите в настройки Rescuva
2. Затем перейдите на вкладку «Действия»
3. Поставьте галочки напротив «Показывать файлы из скрытых/системных папок», «Показывать файлы с нулевым размером», «Показывать надежно удаленные файлы»
4. Нажмите «ОК»

Задание №6. Удаление программного продукта

Если нужно удалить Rescuva, следует воспользоваться опцией Установка и удаление программ для Изменения/Удаления программ через Панель управления Windows. Следовать инструкциям деинсталлятора.

Контрольные вопросы и задания

1. Провести анализ файлов музыки на USB-флэш-накопителе. Результат отобразить в режиме показа «В виде миниатюр» и сохранить в как текст.
2. Настроить Rescuva по следующим параметрам: восстанавливать структуру папок (простая перезапись), добавить «Поиск удаленных файлов» в контекстное меню Проводника и Корзины, открывать мастер при запуске. Хранить все настройки в INI-файле
3. Провести поиск по содержимому файла по следующим параметрам: Иск.строка – OCWindows; Файл. Маска - \*.doc
4. Провести восстановление сжатых файлов в Корзине через запуск мастера. А также настроить автоматически, проверять обновление программы Rescuva.
5. Провести анализ логического диска C на восстановление файлов писем. Результат должен отображаться в режиме списка файлов.

Лабораторная работа. Восстановление потерянных разделов.

Описание:

TestDisk — свободная программа для восстановления данных, предназначенная прежде всего для восстановления потерянных разделов на носителях информации, а также для восстановления загрузочного сектора, после программных или пользовательских ошибок.

Данная программа поможет вам в большинстве случаев восстановить удалённые разделы жёсткого диска, случайно это у вас произошло или в силу каких-либо посторонних причин, к примеру неумелого использования программ менеджеров разделов - Acronis или Paragon, аварийного отключения компьютера и так далее.

Возможности программы:

Восстановление удалённых разделов

Перестройка таблицы разделов

Перезапись MBR

FAT

FAT12 и FAT16

Поиск параметров файловой системы для перезаписи загрузочного сектора

FAT32

Поиск параметров файловой системы для перезаписи загрузочного сектора  
загрузочного сектора из резервной копии

Восстановление

## NTFS

Поиск параметров файловой системы для перезаписи загрузочного сектора

Восстановление загрузочного сектора из резервной копии

Восстановление MFT из резервной копии

Системные требования:

Поддерживаемые платформы:

DOS (either real or in a Windows 9x DOS-box),

Windows (NT4, 2000, XP, 2003, Vista, 2008, Windows 7 (x86 & x64),

Linux,

FreeBSD, NetBSD, OpenBSD,

SunOS and

MacOS X

Работа с программой

1) Запуск программы. Запустите «Wintaylor» и выберите «TestDisk».

2) Создание или выбор log-файла для записи информации о работе. Так же можно обойтись и без log-файла («No Log»). Выберите Create если вы не хотите добавить новый лог к существующему и вы не запускаете TestDisk с накопителя только для чтения на котором невозможно создать лог. Нажмите Enter для продолжения.

3) Выбор анализируемого диска. Все жесткие диски должны быть определены TestDisk'ом и перечислены, их размер должен быть указан правильно. Используйте кнопки стрелок вниз/вверх для выбора "проблемного" жесткого диска.

4) Выбор типа таблицы разделов. TestDisk отображает типы Таблицы Разделов (Partition Table types). Выберите нужный тип Таблицы Разделов. Обычно правильное значение уже выбрано "по умолчанию", поскольку TestDisk при анализе определяет тип таблицы автоматически

5) Выбор опции по работе с выбранным диском.

a) Analyse – анализ раздела и поиск удалённых разделов;

b) Advanced – файловые утилиты;

c) Geometry – Выбор геометрии диска;

d) Options – опции изменения;

e) MBRCode – запись MBR-кода на первый сектор;

f) Delete – удаление всей информации в таблице разделов;

g) Quit – возвращение к выбору диска.

6) Поиск удаленных разделов. Выберите пункт «Analyse» для поиска удалённых разделов и TestDisk просматривает начальные сектора цилиндров, первичные разделы находятся начиная с первого сектора цилиндра, а логические разделы - со второго сектора. Другими словами программа TestDisk сканирует жёсткий диск на наличие заголовков файловых систем, каждый обнаруженный во время такого сканирования заголовок, TestDisk расценивает как найденный раздел, затем она определяет его объём и добавляет в список найденных разделов.

В этом окне отображена текущая структура разделов нашего жёсткого диска, нажмите «Quick Search». Происходит более тщательный поиск удалённых разделов, он может занять некоторое время, которое зависит от мощности вашего компьютера.

7) Выбор раздела. Используйте кнопки стрелок для выбора

8) Проверка потерянных папок на удалённом разделе. Зайдите внутрь удалённого раздела с помощью нажатия клавиши клавиатуры в английской раскладке (P) чтобы увидеть потерянные папки.

9) Чтобы выйти из режима отображения файлов, нажмите (Q). Нужный для восстановления раздел уже выбран, здесь выбираем с помощью стрелок на клавиатуре «Write» и вся информация о найденном разделе будет записана в таблицу разделов жёсткого диска.

10) Нажмите (Y) для создания раздела с удаленной информацией.

11) Закройте программу и перезагрузите компьютер. Должен появиться удалённый раздел с нужными нам папками.

Контрольные вопросы и задания:

- 1) Для чего предназначена программа «TestDisk»?
- 2) Работает ли данная программа с системой MacOS?
- 3) Возможно ли восстановление загрузочного сектора из резервной копии на файловой системе FAT32?
- 4) Запустите «TestDisk».
- 5) Создайте Log-файл для записи информации о работе.
- 6) Удалите и найдите нужный раздел, используя программу «TestDisk».
- 7) Восстановите удаленный раздел с помощью программы «TestDisk».

#### Тема 4. Сбор доказательств.

Лабораторная работа. Сбор данных о USB устройствах. Содержание

Описание продукта

Системные требования

Ход работы

Задание №1. Установка программного продукта

Задание №2. Провести тестирования скорости чтения – записи подключенного флэш-накопителя

Задание №3. Сформировать отчет HTML по всем устройствам

Задание №4. Настроить USBDeview v2.30 по следующим параметрам: поместить иконку программы в трей, открывать программу USBDeview при подключении флэш-накопителя, показывать сетку.

Задание 5 Очистить реестр от usb-устройств

Задание №6 Удаление программного продукта

Контрольные задания

Описание продукта

USBDeview - небольшая программа, которая выведет список всех USB устройств (флеш-карта, мобильный телефон, фотоаппарат, принтер и т.д.), когда-либо подключаемых к Вашему компьютеру.

При этом по каждому устройству, подключено оно в данный момент или нет, USBDeview предоставит исчерпывающую информацию: дату и время, когда устройство было добавлено и время последнего подключения,

наименование/описание устройства, тип, серийный номер, идентификационные номера продукта и производителя и многое другое. Полученную информацию можно экспортировать в Text/HTML или XML файл.

USBDeview включает в себя несколько полезных инструментов. Например SpeedTestfor USB FlashDrives, который протестирует скорость чтения – записи подключенного флэш-накопителя. Имейте в виду вам нужно, минимум 100 Мб свободного дискового пространства для того, чтобы успешно сделать этот тест скорости. С помощью USBDeview, вы можете управлять свойствами автозапуска для USB-устройств хранения данных. Есть возможность работы на удаленном компьютере, но для этого необходимо войти в систему с правами администратора.

Кроме этого, USBDeview также может деинсталлировать USB устройства, которые вы использовали ранее, или отключить те, что подключены к вашему компьютеру в данный момент.

Имеется русификатор для USBDeview, он находится в той же папке что и лабораторная работа (распаковать в ту же папку, где находится сама программа)

Системные требования

Статус программы - Бесплатная

Операционная система:

Windows 2000

Windows XP

Windows 2003

Windows Vista

Windows Server 2008

Windows 7

Windows 8.

Оба 32-битных и 64-битных систем поддерживаются.

Windows 98/ME не поддерживается.

Интерфейс - Английский, Русский

Разработчик - NirSofer

Категория программы - Внешние устройства

Ход работы

Задание №1. Установка программного продукта.

Для выполнения задания необходимо выполнить следующее действие:

1. Зайдите на сайт разработчика <http://www.nirsoft.net/> и скачайте новую версию продукта.

USBDeview работает без установки и имеет русский интерфейс (если загрузить русификатор).

Задание №2. Провести тестирования скорости чтения – записи подключенного флэш-накопителя

Внимание! Нужно, минимум 100 Мб свободного дискового пространства для того, чтобы успешно сделать этот тест скорости. Для выполнения задания, необходимо выполнить следующие пункты в главном окне программы (см. рис. 1):

1. Выберите нужное устройство в списке подключенных флэш-накопителей (отличить от отключенных их можно по значкам) и нажмите ПКМ
2. Выберите пункт «Тест скорости»
3. В появившемся окне нажмите «Запустить тест».

Задание №3. Сформировать отчет HTML по всем устройствам

Для успешного выполнения задания, выполните следующие действия в главном окне программы:

1. Во вкладке «Вид» выберите «Отчет HTML по всем устройствам»

После формирования отчета, он откроется автоматически браузером, который установлен по умолчанию. Также отчет автоматически сохраняется в папке, где находится программа USBDeview v2.30.

Задание №4. Настроить USBDeview v2.30 по следующим параметрам: поместить иконку программы в трей, открывать программу USBDeview при подключении флэш-накопителя, показывать сетку.

В главном окне программы во вкладке «Опции» выберите следующие пункты:

1. Поместить иконку программы в трей
2. Открывать программу USBDeview при подключении флэш-накопителя

Для отображения сетки в USBDeview, во вкладке «Вид» выберите «Показывать сетку»

Задание №5. Очистить реестр от usb-устройств

При подключении к usb-порту нового устройства (флешка, принтер, мобильный телефон и т.д.), информация о нем заносится в реестр. Фактически, получается, что это следы, которые могут пояснить, что совалось в компьютер. Плюс ко всему – это мусор, который копится и со временем большой кучей лежит в реестре. Для выполнения задания, сделайте следующие действия:

1. В главном окне программы выделите те устройства которые отмечены серым значком
2. Нажмите ПКМ и выберите в списке «Деинсталлировать выбранные устройства»
3. Появится окно подтверждающее удаление выбранных устройств, нажмите «Да»

Задание №6. Удаление программного продукта

Так как USBDeview не устанавливает какие-либо файлы на компьютер, деинсталлировать его стандартными средствами Windows нет необходимости. Достаточно просто удалить папку, где хранится данная программа.

Контрольные вопросы и задания

1. Сформировать отчет HTML по отдельным выбранным элементам
2. Настройте по следующим параметрам: показывать только включенные устройства, показывать сообщение в трее при подключении устройства, авто размер столбцов, показывать USB хабы
3. Сформировать отчет нескольких флэш-накопителей и сохранить его в txt формате, а также провести тест скорости этих устройств

4. Провести деинсталляцию нескольких отключенных устройств одновременно.
5. Выполните следующую команду при вставке вашего USB устройства: `C:\Temp\test.exe "%usb_version%".` Примечание! Файл test.exe должен быть создан заранее.

Лабораторная работа. Блокировка и запрет работы с USB портами.

USB Write Blocker – является утилитой для блокировки и запрета работы с USB портами, используется для ограничения доступа к информации посредством подключаемых устройств типа флеш карт, портативных HDD и других подключаемых внешних носителей. При активации программы пользователю позволяет заходить на съёмные носители и просматривать содержимое но запись на них отключена.

В программе содержится 3 различных языка работы (Немецкий, Английский и Итальянский), работа программы может происходить на всех версиях ОС Windows, кроме 8 версии.

USB Device – программа необходима для определения параметров всех подключённых USB устройств. Также программа отображает список когда-либо подключавшихся к USB портам компьютера устройств (флеш-карта, мобильный телефон, принтер и т.д.) , при этом выводятся данные о времени последнего подключения, описания устройств, их серийные номера, VendorID.

Выводимая информация:

- дата и время, когда устройство было добавлено
- время последнего подключения
- наименование/описание устройства
- тип устройства
- серийный номер
- идентификационные номера продукта и производителя

Полученную информацию можно экспортировать в файл форматов Text/HTML/XML и записать на для дальнейшего анализа.

Основное меню программы. Зеленым показывается устройство, которое в данный момент функционирует.

USBDevview позволяет деинсталлировать USB устройства, которые были подключены и отсоединить подключенные в данный момент устройства. Вы можете использовать USBDevview на любом компьютере, на котором есть права администратора.

После запуска перед вами предстанет список всех когда-либо подключившихся по интерфейсу USB девайсов, из которого можно почерпнуть много полезной информации, включая имя устройства, его тип, класс, состояние, версию драйвера, название соответствующей службы Windows и многое другое. Поскольку колонок много, лучше всего кликнуть по интересующему вас пункту в списке и просмотреть все данные по нему в отдельном окне. С помощью контекстного меню можно подключить / отключить устройство, полностью удалить его из системы, сменить букву диска (для накопителей) или же открыть в штатном редакторе реестра соответствующую запись. Из дополнительных функций – генерация отчета в формате HTML. Есть дистрибутивы для 32- и 64-разрядных систем.

Контрольные вопросы и задания:

1. Отключите все usb порты на своём компьютере.
2. Удалите одно из usb устройств установленных на компьютере.
3. Перепишите id пяти последних usb устройств на своём компьютере.
4. Выключите и подключе обратно usb устройства.
5. Сохраните отчёт о созданной конфигурации в формате \*.xml

## Тема 5. Действия правоохранительных органов по делам о преступлениях в сфере компьютерной информации.

Лабораторная работа. Информация о зарегистрированных доменах

WhoisThisDomain - утилита, которая позволяет легко получать информацию о зарегистрированных доменах. Программа автоматически подключается к серверу WHOIS, который служит для получения регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем. В утилите предусмотрена функция сохранения отчёта проведённого сканирования.

Для работы программы необходима операционная система Windows: Любая версия Windows, от Windows 2000 и до Windows 8. Подключение к Интернету. На брандмауэре, необходимо позволить исходящие соединения на порт 43. Данная утилита выпущена как бесплатное программное обеспечение. Утилита не требует установки или дополнительных DLL.

При запуске WhoisThisDomain утилиту, появляется окно “Выбор доменов”. Можно ввести один домен, или несколько доменов через запятую, без пробелов, или их ip адреса. После нажатия кнопки "ОК", WhoisThisDomain начинает извлекать записи регистрации доменов для доменов, которые были указаны.

После ввода и проверки домена программа выдаст всю информацию в нижней части окна на кого был зарегистрирован домен привязанный ip адрес. страну расположения и дату регистрации.

В случае отсутствия доступа в интернет или заблокированного домена программа автоматически будет пытаться возобновить сканирование (красными кругами обозначаются нерабочие домены). Начиная с версии 1.20, есть возможность создать свой собственный список WHOIS серверов для переопределения их по умолчанию

Для того чтобы использовать эту функцию, выполните следующие действия:

Создайте файл с именем 'Whois-Servers.txt' в том же каталоге WhoisTD.exe

Добавьте необходимые серверы в список. Каждая строка должна содержать расширение домена, пробел, а затем и Whois адрес сервера. Например:

```
gov whois.nic.gov
com rs.internic.net
li whois.isoc.org.il
ir whois.nic.ir
```

В следующий раз, при запуске WhoisThisDomain, указанные серверы будут использоваться вместо списка по умолчанию и хранится в папке с WhoisThisDomain.

Также данную утилиту можно запускать в режиме командной строки:

/ Domainsfile <Filename> - Загрузить все домены в заданном текстовом файле и начать сканирование, чтобы получить WHOIS информацию автоматически. Текстовый файл может быть в ASCII, Unicode или UTF8

Пример: WhoisTD.exe / domainsfile "C: \ Temp \ domainslist.txt"

/ Domainslist <Domains List> - Загрузите указанные домены и начать, чтобы получить WHOIS информацию автоматически.

Пример: WhoisTD.exe / domainslist "yahoo.com google.com youtube.com"

Контрольные вопросы и задания :

1. Получите информацию о домене google.com
2. Сохраните отчет о проведенном сканировании.
3. Пропингуйте домен yandex.ru в режиме командной строки используя данную программу.
4. Создайте свой собственный список WHOIS серверов.
5. Соберите информацию о домене своего провайдера или провайдера университета.

Лабораторная работа. Аудит компьютерной системы.

Содержание

Описание продукта

Системные требования

Ход работы

Задание №1. Установка программного продукта.

Задание №2. Провести аудит установленных программ, ОС, сеть Windows, сеть TCP/IP, службы и драйвера, и автозагрузки программ в ПК

Задание №3. Сохранить результаты аудита в формате pdf с разрешением копировать содержимое

Задание №4. Сохранить результаты аудита в виде PDF-документа с паролем Смит через командную строку

Задание 5 Поиск файлов с расширением \*.exe

Задание №6 Экспорт результатов аудита в БД MicrosoftAccess

## Задание №7 Удаление программного продукта

### Контрольные задания

#### Описание продукта

WinAudit - утилита помогает проанализировать всю техническую информацию о компьютере, его возможных слабых местах, что порой необходимо при анализе в расследовании инцидентов, в непринужденной, простой для пользователя форме. Программа проста в использовании и представляет собой один файл, который не требует установки. WinAudit предназначен для подготовки всестороннего аудита с помощью нажатия

одной кнопки, обеспечивая результаты в минимальные сроки. Программа может запускаться с дискеты, USB-flash. Функциональные возможности:

1. Позволяет осуществлять мониторинг аппаратного и программного обеспечения на системе
2. Созданный приложением отчет содержит подробное описание установленного программного обеспечения, информацию о лицензиях, периферийных устройствах, данные об используемой памяти на системе, модель процессора, сетевые настройки и пр.
3. Существует возможность создавать отчеты в csv, xml и html форматах.
4. Приложение снабжено OpenDatabaseConnectivity(ODBC) коннектором, что позволяет осуществлять запись в базу данных. Поддерживает все самые популярные БД (Microsoft Access 2007/2010, Microsoft SQL Server 2005/2008, MySQL® 3.23/4.1/5.5, Парадокс® 5.0 и т.д.).

#### Системные требования

1. ПК с процессором Pentium и ОС Windows 95 или выше.
2. Чтобы отправить отчет аудитана e-mail ваш компьютер должен иметь программу для работы с почтой, например Microsoft Outlook.
3. Должен быть установлен ODBC драйвер базы данных на компьютере.
4. Браузер (IE 6, Safari, Mozilla Firefox, Google Chrome).

#### Ход работы

##### Задание №1. Установка программного продукта.

Для выполнения задания необходимо выполнить следующее действие:

Зайдите на сайт разработчика <http://www.pxserver.com/WinAudit.htm> и скачайте новую версию продукта. WinAudit - "готов к работе". Она была составлена так, что вы не должны проходить через процедуру установки.

##### Задание №2. Провести аудит установленных программ, ОС, сеть Windows, сеть TCP/IP, службы и драйвера, и автозагрузки программ в ПК

Аудит ПК необходимо проводить по несколько причин. Среди них можно отметить:

Проведение инвентаризации компьютерного парка

Проверка технических данных, работоспособности компьютеров

Выбор оптимальных вариантов усовершенствования машин, устранения возможных сложностей в работе, неполадок

Вы сможете в полной мере оценить качество предоставляемого фирмой сервиса, узнать много нового о собственных компьютерах, ознакомиться с проблемами. В итоге наладить полноценную работу с партнерами, клиентами не составит труда.

Для того чтобы провести аудит по конкретным параметрам, необходимо выполнить следующие действия в главном окне программы:

- 1) нажать на кнопку «Параметры»
- 2) Выбрать нужные категории для проведения аудита (в данном случае это Установленные программы, ОС, сеть Windows, сеть TCP/IP, службы и драйвера, Автозагрузка программ) (см. рис. 2). После этого нажимаем на кнопку «Применить»

- 3) Для проведения аудита в главном окне программы нажимаем кнопку «Здесь» (см. рис. 1) Проверка ПК занимает некоторое время, после чего результаты аудита высветятся в главном окне программы

##### Задание №3. Сохранить результаты аудита в формате pdf с разрешением копировать содержимое

Для сохранения результатов в формате pdf аудита ПК необходимо выполнить следующие действия:

- 1) На панели инструментов нажать на кнопку «Сохранить»



2) Выбираем формат pdf и сохраняем в нужном каталоге.

3) После нажатия на кнопку «Сохранить» появляется окно «Сохранение документа», в котором должны указать параметры сохранения документа. В данном окне ставим галочку «Разрешить копировать содержимое» и нажимаем «Сохранить»

После того, как сохранили отчет, вы можете его открыть и просмотреть содержимое

**Задание №4.** Сохранить результаты аудита в виде PDF-документа с паролем Смит через командную строку

Вы можете вызвать WinAudit из командной строки, в этом режиме программа выполняется без показа главного окна. Таким образом, вы можете автоматизировать и аудит компьютеров с помощью пакетных файлов или сценариев входа в систему на контроллере домена. При необходимости, вы можете опубликовать результаты непосредственно к базе данных.

WinAudit собирает данные, связанные с безопасностью, поэтому он не работает в автоматическом режиме. Небольшое окно, информирующее пользователя, что информация была собрана. Такое поведение не изменится. Если это окно закрывается, аудит не остановился, он продолжает выполняться в фоновом режиме. Никаких ассигнований для отправки e-mail в режиме командной строки. Когда WinAudit запускается из пакетного файла, то управление передается асинхронно к следующей строке файла. Вы должны подождать, пока WinAudit, чтобы закончить, если вы намерены пост-обработки выходных данных.

Некоторые советы:

- Попробуйте использовать WinAudit в режиме пользовательского интерфейса, прежде чем активировать его через командную строку. Убедитесь, что вы включили report '/r=' с какой-то категории писем.

- Категория чувствительны к регистру букв

- Использовать только обратные косые черты '\' для файла разделителя пути.

- Не надо цитировать выходной или пути к файлу журнала, даже если есть пробелы.

- WinAudit возвращает код ноль (0) в случае успеха и ненулевое значение, если произошла ошибка.

- Ведение журнала помещение, чтобы помочь в диагностике проблем.

Если вы используете WinAudit через WinTaylor, то необходимо запустить командную строку из следующего каталога: wintaylor2.5.1\Programs\cmd После этого пишем следующую команду: WinAudit.exe /r=Go /o=PDF /p=Смит Результат аудита по умолчанию сохраняется туда, откуда запускали командную строку!!!

Полный список команд для работы с WinAudit-ом через командную строку вы можете найти на сайте <http://www.pxserver.com>

**Задание 5.** Поиск файлов с расширением \*.exe

Для того чтобы выполнить данное задание необходимо выполнить следующие действия:

1) Выбрать категорию для аудита «Поиск файлов» и указать расширение \*.exe

2) Начать аудит

**Задание №6.** Экспорт результатов аудита в БД MicrosoftAccess

Для выполнения этого задания необходимо выполнить следующие действия:

1. Провести аудит ПК

2. Создать БД MicrosoftAccess в отдельной папке

3. На вкладке «Файл» выбрать «Экспорт в базу данных»

4. Нажмите «Создать»

5. Выберите "Пользовательский Источник Данных", затем "Далее"

6. Выберите " MicrosoftAccessDriver (\*.mdb, \*.accdb)", затем " Далее"

7. Нажмите Кнопку " Готово"

8. Нажмите Базы Данных: Выберите. И выберите ту БД, которую создали на шаге 2

9. Нажмите «ОК»

10. Нажмите на «Экспорт»

**Задание №7.** Удаление программного продукта

Так как WinAudit не устанавливает какие-либо файлы на компьютер, деинсталлировать его стандартными средствами Windows нет необходимости. Достаточно просто удалить файл программы WinAudit.exe и, возможно, WinAudit.ini. Если вы создавали ярлык на рабочем столе, вы должны удалить его.

#### Контрольные задания

1. Провести аудит ПК по следующим категориям: Безопасность, Группы и пользователи, Автозагрузка программ и Загруженные модуль. Отчет сохранить в формате xml с паролем «Memory555» и с разрешением печати документа.
2. Выполнить поиск файлов с расширением \*.sysи \*.bat. Отчет сохранить в формате pdf с запретом копирования содержимого и печати документа.
3. Выполнить создание GUID.
4. Провести полный аудит ПК и результат экспортировать в БД MicrosoftAccess
5. Сохранить в одной папке данные о видеоадаптере, свойства модулей UpperMemory, CPIUD и SoftwareDetails в txt формате.

### Собеседование

#### Тема 1. Компьютерные преступления.

- 1.Выделите предметы и задачи компьютерной экспертизы.
- 2.Что такое инцидент информационной безопасности.
- 3.Проведите анализ законодательной базой регулирования компьютерного преступления.
- 4.Какое деяние может считаться уголовно наказуемым.
- 5.Перечислите этапы компьютерной экспертизы.
- 6.На какие группы классифицируются лица совершившие компьютерные преступления.
- 7.Перечислите причины инцидента компьютерного преступления.
- 8.Что является объектами программно-компьютерной экспертизы.
- 9.На какие группы делятся методы исследования программного обеспечения.

#### Тема 2. Расследование инцидентов информационной безопасности.

1. С помощью каких алгоритмов осуществляется поиск данных.
- 2.Какие файловых менеджеров используются и как они применяются.
- 3.Какие угрозы могут быть связаны с cookie файлами.
- 4.Способы получения злоумышленником информации из cookie файлов.
- 5.Перечислите методы предотвращения возникновения угрозыинцидента информационной безопасности.

#### Тема 3. Общая схема расследования преступления.

1. Постройте схему организации взлома защитных механизмов информационных систем.
- 2.Какими законодательными актами регулируются наказания за неправомерный доступ охраняемой законом информации.
- 3.Распишите общую схему расследования преступления.
- 4.Какие существуют признаки несанкционированного доступа.
5. Как определяется место и время совершения преступления.
6. Опишите последовательность действий расследования, создания и распространения вредоносного ПО.
- 7.Каким наказанием является за нарушение законодательно о «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»
- 8.Как доказать факты нарушения правил пользования ЭВМ.

#### Тема 4. Сбор доказательств.

1. Как осуществляется поиск доказательств преступлений в файловой системе.
2. На что подразделяются следы в системных областях файловой системы.
3. Какие существуют методы сбора данных о пользователе.
5. Какой закон регулирует законодательный уровень накопления данных в сетях.
6. Какие самые популярные преступления в социальных сетях.

#### Тема 5. Действия правоохранительных органов по делам о преступлениях в сфере компьютерной информации.

1. Какие объекты способны по своим физико-техническим свойствам содержать информацию, имеющую отношение к расследуемому преступлению.
2. Как различают обыск по последовательности проведения.
3. На какие группы разделяются объекты следственного действия (компьютерная техника и компьютерная информация).
4. Что относится к объектам компьютерно-технической экспертизы.
5. Какие задачи решаются с помощью компьютерно-технической экспертизы.
6. Какой перечень вопросов может выноситься на разрешения компьютерно-технической экспертизы.
7. Что нужно для проведения следственного эксперимента.

### Тестирование

#### Тема 1. Компьютерные преступления.

Типовые вопросы для тестирования

1. Что относится к объектам программно-компьютерной экспертизы?
  - a. Операционные системы, утилиты, прикладные программы
  - b. Операционные системы, утилиты, программные средства для разработки программного обеспечения, прикладные программы.
  - c. программные средства для разработки программного обеспечения, прикладные программы
  - d. Прикладные программы, утилиты
2. Дать определение инцидент информационной безопасности
  - a. Событие, случай, недоразумение, происшествие
  - b. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ.
  - c. Событие, в котором нарушаются файлы
3. Что относится к угрозам связанные с cookie файлами.
  - a. Утечка конфиденциальной информации, несанкционированный доступ злоумышленника к некоторым web-сервисам от имени пользователя.
  - b. Кража логинов с помощью клавиатурных вирусов
  - c. Уничтожение файлов на компьютере
4. Что относится к признакам несанкционированного доступа
  - a. Изменение обоев на рабочем столе компьютера
  - b. Изменение комплектующих системного блока
  - c. Появление в компьютере фальшивых данных, частые сбои в процессе работы компьютеров
5. Какой закон регулирует законодательный уровень накопления данных в сетях
  - a. 149 ФЗ РФ
  - b. 272 УК РФ
  - c. 152 ФЗ РФ

#### Тема 2. Расследование инцидентов информационной безопасности.

### Типовые вопросы для тестирования

1. Что относится к преступлениям в социальных сетях
  - a. Угон машин, кража вещей
  - b. Подделка документов, хищение кредитных карт, клевета
  - c. Нанесение вреда чужому имуществу
  - d. Нанесение вреда здоровью
2. Какие объекты способны по своим физико-техническим свойствам содержать информацию, имеющую отношение к расследуемому преступлению
  - a. Холодильники, микроволновой печи, электрочайники
  - b. Персональные компьютеры, модемы, принтеры
  - c. Клавиатура, компьютерная мышь
  - d. Домашний телефон
3. На какие группы разделяются объекты следственного действия
  - a. Нужные и не нужные
  - b. Рабочие и сломанные
  - c. Предмет традиционных преступных посягательств и орудия совершения преступлений
4. Объектом компьютерно-технической экспертизы является:
  - a. Компьютерная техника и (или) компьютерные носители информации;
  - b. Огнестрельное оружие и боеприпасы;
  - c. Различные документы;
  - d. Самодельные взрывные устройства.
5. Одним из видов компьютерно-технической экспертизы является:
  - a. Информационная экспертиза;
  - b. Аппаратная экспертиза;
  - c. Сетевая экспертиза;
  - d. Информационно-компьютерная экспертиза.

### Тема 3. Общая схема расследования преступления.

#### Типовые вопросы для тестирования

1. Компьютерно-техническая экспертиза назначается в основном при расследовании:
  - a. Экономических преступлений;
  - b. Компьютерных преступлений;
  - c. Террористических преступлений;
  - d. Всех вышеуказанных преступлений.
2. Компьютерно-техническая экспертиза состоит из следующего исследования:
  - a. Компьютеров и их комплектующих;
  - b. Мобильных телефонов;
  - c. Документации;
  - d. SIM-карт.
3. При производстве выемки изъятие электронных носителей информации производится с участием специалиста:
  - a. Да;
  - b. Нет;
  - c. На усмотрение следователя (дознателя);
  - d. Если получено судебное решение.
4. Копирование информации по ходатайству законного владельца изымаемых электронных носителей

информации или обладателя содержащейся на них информации является:

- a. Обязательным;
  - b. Необязательным;
  - c. На усмотрение следователя (дознателя);
  - d. Если получено судебное решение.
5. Об осуществлении копирования информации и о передаче электронных носителей информации, содержащих скопированную информацию, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации делается запись в:
- a. В постановлении о назначении судебной экспертизы;
  - b. В протоколе следственного действия;
  - c. На пояснительной бирке упаковки;
  - d. Во всех вышеуказанных вариантах.

#### Тема 4. Сбор доказательств.

Типовые вопросы для тестирования

1. В задачи исследования информации (данных) может входить (Выбрать лишнее):
  - a. Технические и содержательные характеристики данных;
  - b. Степень защищенности информации;
  - c. Выявление степени повреждения информации;
  - d. Восстановление удаленных и поврежденных данных;
  - e. Получение доступа к защищенной информации.
2. Тип исполнения техники, объединяющий несколько устройств в одном корпусе, применяется для уменьшения занимаемой оборудованием площади, упрощения сборки конечным пользователем, придания эстетического вида, называется:
  - a. Компьютер;
  - b. Моноблок;
  - c. Планшетный компьютер;
  - d. Мобильный телефон.
3. Мобильный телефон, дополненный функциональностью карманного персонального компьютера, называется:
  - a. Смартфон;
  - b. Моноблок;
  - c. Планшетный компьютер;
  - d. Камерофон.
4. В рамках проведения компьютерно-технической экспертизы могут быть исследованы такие устройства, как (Выбрать лишнее):
  - a. Персональные компьютеры;
  - b. Ноутбуки;
  - c. Планшеты;
  - d. Калькуляторы;
5. Электронная информация может храниться на:
  - a. Оптическом диске;
  - b. Флэш-карте;
  - c. На внешнем накопителе;
  - d. На всех вышеуказанных устройствах.

#### Тема 5. Действия правоохранительных органов по делам о преступлениях в сфере компьютерной информации.

### Типовые вопросы для тестирования

1. Выявление исправности и работоспособности аппаратной составляющей информационной системы с установлением недостатков и причин их возникновения относится к:

- a. Исследование аппаратной составляющей компьютерных систем;
- b. Поиск информации;
- c. Поиск информации о работе в сети Интернет;
- d. Исследование информационной составляющей компьютерных систем;

2. Установление фактов наличия, степени опасности, а также признаков изготовления и распространения вредоносных программ относится к:

- a. Исследование аппаратной составляющей компьютерных систем;
- c. Поиск информации о работе в сети Интернет;
- d. Исследование информационной составляющей компьютерных систем;

b. Поиск информации;

3. Поиск на информационных носителях документов с заданными реквизитами или известным содержанием скрытой (удаленной) информации известного содержания относится к:

- b. Поиск информации;
- a. Исследование аппаратной составляющей компьютерных систем;
- d. Исследование информационной составляющей компьютерных систем;
- c. Поиск информации о работе в сети Интернет;

4. Установление фактов размещения информации на Интернет-ресурсах относится к:

- b. Поиск информации;
- c. Поиск информации о работе в сети Интернет;
- a. Исследование аппаратной составляющей компьютерных систем;
- d. Исследование информационной составляющей компьютерных систем;

5. Относится ли изучение носителей информации, любого типа, постоянных или временных, для обнаружения интересующих вас данных, для извлечения данных в случае повреждения носителей, для анализа повреждений, физических или программных, которые понесены носителями информации к задачам компьютерной экспертизы?

- a. Да
- b. Нет

### 4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

#### Типовые вопросы зачета (ПК-4)

1. Объект и предмет компьютерной экспертизы?
2. Задачи компьютерной экспертизы?
3. Какими законами регулируется деятельность компьютерной экспертизы?
4. Какие организации занимаются компьютерной экспертизой?
5. Какие преступления нуждаются в компьютерной экспертизе?

#### Типовые задания для зачета (ПК-4)

1. Что относится к объектам программно-компьютерной экспертизы?

- a. Операционные системы, утилиты, прикладные программы
- b. Операционные системы, утилиты, программные средства для разработки программного обеспечения, прикладные программы.
- c. программные средства для разработки программного обеспечения, прикладные программы

- d. Прикладные программы, утилиты
2. Дать определение инцидент информационной безопасности
- Событие, случай, недоразумение, происшествие
  - Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий ИБ.
  - Событие, в котором нарушаются файлы
3. Что относится к угрозамсвязанные с cookie файлами.
- Утечка конфиденциальной информации, несанкционированный доступ злоумышленника к некоторым web-сервисам от имени пользователя.
  - Кража логинов с помощью клавиатурных вирусов
  - Уничтожение файлов на компьютере
4. Что относится к признакам несанкционированного доступа
- Изменение обоев на рабочем столе компьютера
  - Изменение комплектующих системного блока
  - Появление в компьютере фальшивых данных, частые сбои в процессе работы компьютеров
- 5.Какой закон регулирует законодательный уровень накопления данных в сетях
- 149 ФЗ РФ
  - 272 УК РФ
  - 152 ФЗ РФ
- 6.Что относится кпреступлениям в социальных сетях
- Угон машин, кража вещей
  - Подделка документов, хищение кредитных карт, клевета
  - Нанесение вреда чужому имуществу
  - Нанесение вреда здоровью
- 7.Какие объекты способны по своим физико-техническим свойствам содержать информацию, имеющую отношение к расследуемому преступлению
- Холодильники, микроволновой печи, электрочайники
  - Персональные компьютеры, модемы, принтеры
  - Клавиатура, компьютерная мышь
  - Домашний телефон
- 8.На какие группы разделяются объекты следственного действия
- Нужные и не нужные
  - Рабочие и сломанные
  - Предмет традиционных преступных посягательств и орудия совершения преступлений

#### 4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
--------	-------------	--

«зачтено» (50 - 100 баллов)	ПК-4	Имеет высокий уровень знаний и обладает навыками и умениями решения задач с использованием методов и теоретических представлений компьютерной экспертизы. Умеет находить цифровые следы в компьютерных системах и сетях. Способен организовывать работы по компьютерной экспертизе как часть технологического процесса защиты информации в компьютерных системах.
«не зачтено» (0 - 49 баллов)	ПК-4	Не имеет знаний и не обладает навыками и умениями решения задач с использованием методов и теоретических представлений компьютерной экспертизы. Не умеет находить цифровые следы в компьютерных системах и сетях. Не способен организовывать работы по компьютерной экспертизе как часть технологического процесса защиты информации в компьютерных системах.

## 5. Методические указания для обучающихся по освоению дисциплины (модуля)

### 5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

### 5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

### 5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.



Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

#### 5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;
- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1 Основная литература:

1. Бегларян М. Е. Судебная компьютерно-техническая экспертиза : научно-практическое пособие. - Москва: Юнити, 2015. - 71 с. - Текст : электронный // ЭБС «Университетская библиотека онлайн» [сайт]. - URL: <http://biblioclub.ru/index.php?page=book&id=446544>
2. Лопатин Д.В. Компьютерная экспертиза : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

## 6.2 Дополнительная литература:

1. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В. Защита компьютерных систем от деструктивных программ : Учеб.-метод. пособие. - Тамбов: Изд-во ТГУ, 2005. - 158 с.
3. Информационные технологии : лабор. практикум : учеб.-метод. пособие, Ч.І. - Тамбов: Изд-во ТГУ, 2008. - 62 с.

## 6.3 Иные источники:

1. Федеральный портал «Российское образование» - <http://www.edu.ru/>

## **7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы**

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

CryptonLock

Crypton Дозор

CryptonFastDisk

CryptonEmulato

Crypton IP Mobile

Terrier 3.0 (средство контроля защищенности от НСД)

Delphi 2007 for Win32 Professional

Фикс 3.0 (программа фиксации и контроля исходного состояния)

Ревизор-2 XP (программа контроля полномочий доступа к информационным ресурсам)

Ревизор-1 XP (средство создания модели системы разграничения доступа)

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Президентская библиотека имени Б.Н. Ельцина. – URL: <https://www.prilib.ru>
3. Российская национальная библиотека. – URL: <http://nlr.ru>
4. Российская государственная библиотека. – URL: <https://www.rsl.ru>
5. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

6. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
7. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>
8. Научная электронная библиотека Российской академии естествознания. – URL: <https://www.monographies.ru>
9. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>

### **Электронная информационно-образовательная среда**

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz)

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.