Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
и.о. заведующего кафедрой
Борисов Дмитрий Николаевич
Кафедра информационных систем
21.04.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.07.02 Компьютерно-техническая экспертиза

1. Код и наименование направления подготовки/специальности:

09.03.03 Прикладная информатика

2. Профиль подготовки/специализация:

Прикладная информатика в экономике

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра информационных систем

6. Составители программы:

Борисов Дмитрий Николаевич (borisov@cs.vsu.ru)

7. Рекомендована:

протокол НМС №5 от 10.03.2021

8. Учебный год:

2024-2025

9.Цели и задачи учебной дисциплины:

Цель дисциплины – формирование у студентов комплексного представления о компьютерно-технической экспертизе, представления об экспертном исследовании, используемых технических средствах и методик экспертного исследования.

Задача дисциплины:

- рассмотрение основных понятий компьютерно-технической экспертизы;

- изучение порядка, основных правил и методов проведения экспертных исследований;

- изучение технических средств, используемых для проведения экспертных исследований и основных методик проведения экспертного исследования;

- формирование навыков компьютерно-технической экспертизы.

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений блока Б1. Для успешного освоения необходимо предварительного

изучение следующих дисциплин: введение в прикладную информатику, правовые основы прикладной информатики, информационные системы и технологии, операционные системы, администрирование ИС, инсталляция и настройка ПО.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-1 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	ПК-1.1 Определение первоначальных требований заказчика к ИС и возможности их реализации в типовой ИС.	знать: алгоритм определения первоначальных требований заказчика к ИС и возможности их реализации в типовой ИС уметь: определять первоначальные требования заказчика к ИС и использовать возможности их реализации в типовой ИС владеть: определением первоначальных требований заказчика к ИС и возможностями их реализации в типовой ИС
ПК-2 Способность составлять технико-экономическое обоснование проектных решений и техническое задание на разработку информационной системы	ПК-2.1 Разработка требований и проектирование программного обеспечения.	знать: алгоритмы разработки требований и проектирования программного обеспечения уметь: разрабатывать требования и проектировать программное обеспечение владеть: разработкой требований и проектированием программного обеспечения
ПК-6 Способность документировать процессы создания информационных систем на стадиях жизненного цикла	ПК-6.1 Создание пользовательской документации к ИС.	знать: алгоритмы создания пользовательской документации к ИС уметь: создавать пользовательскую документацию к ИС владеть: созданием пользовательской документации к ИС

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ПК-6 Способность документировать процессы создания информационных систем на стадиях жизненного цикла	ПК-6.2 Методологическое обеспечение обучения пользователей ИС.	знать: методологическое обеспечение обучения пользователей ИС уметь: использовать методологическое обеспечение обучения пользователей ИС владеть: методологическим обеспечением обучения пользователей ИС
ПК-2 Способность составлять технико-экономическое обоснование проектных решений и техническое задание на разработку информационной системы	ПК-2.2 Разработка требований и проектирование технического обеспечения.	знать: алгоритм разработки требований и проектирования технического обеспечения уметь: разрабатывать требования и проектировать техническое обеспечения владеть: рзработкой требований и проектированием технического обеспечения
ПК-1 Способность проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе	ПК-1.2 Управление ожиданиями заказчика.	знать: алгоритмы управления ожиданиями заказчика уметь: управлять ожиданиями заказчика владеть: управлением ожиданиями заказчика

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	60	60
Лекционные занятия	24	24
Практические занятия	36	36
Лабораторные занятия		0
Самостоятельная работа	12	12

Вид учебной работы	Семестр 8	Всего
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	108	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
Лекции			
1.1	Организационные основы компьютерно-технической экспертизы	Порядок назначения и производства экспертизы. Применение специалистом технических методов и средств с целью обнаружения доказательственной информации. Документальное оформление результатов экспертизы.	-
1.2	Научно-методические основы компьютерно-технической экспертизы	Предмет компьютерно-технической экспертизы. Цели и задачи компьютерно-технической экспертизы. Понятие и характеристика объектов компьютерно-технической экспертизы. Вопросы, решаемые компьютерно-технической экспертизой. Разновидности компьютерных экспертиз, условное деление по объекту исследования. Принципы неразрушающих методов исследования информации. Проверка наличия программно-аппаратных средств защиты информации и следов их применения. Обзор практики производства компьютерно-технических экспертиз.	-

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.3	Экспертные задачи по исследованию компьютерной информации	Проверка наличия вредоносных программ. Неразрушающие методы исследования информации: перенос файловой структуры на тестовый винчестер, использование технологии виртуальных машин, использование образов разделов и дисков для исследования. Проверка наличия программно-аппаратных средств защиты информации и следов их применения. Контроль правильности установки системной даты в конкретном интервале дат или на протяжении всего времени нахождения информации на носителе. Установление содержания почтовых сообщений.	-
1.4	Частные экспертные задачи	Рекомендации по решению наиболее часто встречающихся в экспертной практике частных задач. Определение отдельных этапов (стадий) события по служебной информации файла. Установление причинной связи событий, действий. Частные экспертные задачи, связанные с исследованием обстоятельств работы пользователя в сети Интернет. Установление факта и параметров подключения компьютера к сети Интернет. Установление периодов работы пользователя в сети Интернет. Установление источника происхождения файлов при работе пользователя в сети Интернет.	-

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.5	Решение диагностических задач в экспертном исследовании аппаратных средств персонального компьютера	Понятие состояния аппаратных компонентов. Порядок подключения дополнительных устройств к компьютерной системе. Средства установления и фиксации состояния аппаратных компонентов компьютерной системы. Описание аппаратных компонентов компьютера при экспертном исследовании или осмотре. Анализ текущего состояния аппаратного обеспечения компьютерной системы по его физическому состоянию, определение физической возможности подключения внешнего периферийного. Особенности программного подключения внешних устройств. Понятие драйвера устройства. Программные следы подключения и использования внешних устройств. Файлы устройств. Загружаемые модули ядра. Сведения, находящиеся в файлах регистрации.	-

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.6	Решение диагностических задач в отношении файлов данных	Отождествление оригинала документа на носителе информации при наличии дубликата, копии или машинограммы. Установление групповой принадлежности. Установление формата файла. Установление первоначального состояния файла. Установление содержания электронного документа. Выявление файлов, изменивших свое первоначальное местоположение. Определение времени (периода) выполнения действия пользователем или хронологической последовательности событий. Проблема определения даты и времени удаленного файла или сохранившихся его фрагментов и пути ее решения. Особенности восстановления содержимого документа при поврежденной структуре файла.	-

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.7	Скрытая информация и особенности ее исследования при решении экспертных задач	Теоретические основы восстановления удаленной информации. Операционные системы, защищенные от восстановления удалённой информации. Выявление информации, скрытой путем модификации системных областей (заголовки разделов, каталоги). Получение доступа к виртуальным дискам и дискам, зашифрованным средствами ОС. Методология и средства стеганографии. Способы обнаружения шифрованных объектов. Ревизия установленного программного обеспечения. Определение назначения установленного программного обеспечения в прикладном и системном аспекте. Классификация программного обеспечения, используемого в целях поиска информации. Проблема кодировок и форматов файлов, ее учет при осуществлении поиска информации. Этапы поиска информации: поиск информации, содержащейся в файлах; поиск информации, содержащейся в удаленных файлах; поиск информации в кластерах	-

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.8	Поиск информация при решении экспертных задач	Использование возможностей пакета программ Microsoft Office для поиска информации. Специализированные программы для поиска текстовой информации. Специализированные программы для поиска графической информации. Особенности файловых систем FAT и NTFS применительно к решению задачи поиска и восстановления информации. Программы для поиска и восстановления удаленных файлов. Программы для поиска и восстановления файловой структуры носителя информации. Поиск и восстановление информации в файловой системе FAT в условиях разрушения связей кластеров файла. Низкоуровневый поиск и восстановление информации в файловой системе NTFS. Проблема определения даты и времени удаленного файла или сохранившихся его фрагментов и пути ее решения. Особенности восстановления содержимого документа при поврежденной структуре файла.	-
Практические занятия			
2.1	Воздействие на информацию в компьютерной системе	Следы воздействия на информацию в локальных компьютерных системах.	-
2.2	Служебная информация BIOS	Служебная информация BIOS и ее использование в экспертных задачах.	-

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
2.3	Восстановление хронологии событий на компьютере	Служебная информация и ее использование в восстановлении хронологии событий.	-
2.4	Подключение компьютера к сети Интернет	Установление факта, периодов работы, пользователя и параметров подключения компьютера к сети Интернет, а также содержания почтовых сообщений.	-
2.5	Исследование реестра	Следы подключения в реестре, среди драйверов и в файлах ini.	-
2.6	Характеристики удаленной информации	Проблема определения даты и времени удаленного файла или сохранившихся его фрагментов и пути ее решения.	-
2.7	Восстановление информации	Особенности восстановления содержимого документа при поврежденной структуре файла.	-

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Организационные основы компьютерно-технической экспертизы	3	4		2	9
2	Научно-методические основы компьютерно-технической экспертизы	3	4		1	8
3	Экспертные задачи по исследованию компьютерной информации	3	4		2	9
4	Частные экспертные задачи	3	5		2	10

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
5	Решение диагностических задач в экспертном исследовании аппаратных средств персонального компьютера	3	5		1	9
6	Решение диагностических задач в отношении файлов данных	3	5		1	9
7	Скрытая информация и особенности ее исследования при решении экспертных задач	3	4		1	8
8	Поиск информация при решении экспертных задач	3	5		2	10
		24	36	0	12	72

14. Методические указания для обучающихся по освоению дисциплины

К лабораторным занятиям студенты должны изучить теоретический материал предметной области, основы работы в операционных системах Windows и Linux.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Хныкина, А.Г. Информационные технологии : учебное пособие / А.Г. Хныкина, Т.В. Минкина ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 126 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book_view_red&book_id=494703

б) дополнительная литература:

№ п/п	Источник
1	Бегларян, М.Е. Судебная компьютерно-техническая экспертиза: научно-практическое пособие / М.Е. Бегларян. – Москва : Юнити, 2015. – 71 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book_view_red&book_id=446544
2	Моисеева, Т.Ф. Основы судебно-экспертной деятельности: конспект лекций / Т.Ф. Моисеева ; Российский государственный университет правосудия. – Москва : Российский государственный университет правосудия (РГУП), 2016. – 191 с. — Университетская библиотека онлайн : электронно-библиотечная система. — Режим доступа : https://biblioclub.ru/index.php?page=book_view_red&book_id=439610

№ п/п	Источник
3	Скитер, Н. Н. Информационные технологии : учебное пособие / Н. Н. Скитер, А. В. Костикова, Ю. А. Сайкина. — Волгоград : ВолгГТУ, 2019. — 96 с. — ISBN 978-5-9948-3203-5. — Лань : электронно-библиотечная система. — Режим доступа: https://e.lanbook.com/book/157200

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	www.lib.vsu.ru ЗНБ ВГУ

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Операционные системы Windows, Linux.

18. Материально-техническое обеспечение дисциплины:

Компьютерные классы факультета компьютерных наук, проектор для демонстрации теоретического материала.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Организационные основы компьютерно-технической экспертизы Научно-методические основы компьютерно-технической экспертизы Экспертные задачи по исследованию компьютерной информации Частные экспертные задачи	ПК-1	ПК-1.1	Контрольная работа 1 Контрольная работа 2
2	Организационные основы компьютерно-технической экспертизы Научно-методические основы компьютерно-технической экспертизы Экспертные задачи по исследованию компьютерной информации Частные экспертные задачи	ПК-2	ПК-2.1	Контрольная работа 1 Контрольная работа 2

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
3	Решение диагностических задач в экспертном исследовании аппаратных средств персонального компьютера Решение диагностических задач в отношении файлов данных Скрытая информация и особенности ее исследования при решении экспертных задач Поиск информация при решении экспертных задач	ПК-6	ПК-6.1	Контрольная работа 3 Контрольная работа 4
4	Решение диагностических задач в экспертном исследовании аппаратных средств персонального компьютера Решение диагностических задач в отношении файлов данных Скрытая информация и особенности ее исследования при решении экспертных задач Поиск информация при решении экспертных задач	ПК-6	ПК-6.2	Контрольная работа 3 Контрольная работа 4
5	Организационные основы компьютерно-технической экспертизы Научно-методические основы компьютерно-технической экспертизы Экспертные задачи по исследованию компьютерной информации Частные экспертные задачи	ПК-2	ПК-2.2	Контрольная работа 1 Контрольная работа 2
6	Решение диагностических задач в экспертном исследовании аппаратных средств персонального компьютера Решение диагностических задач в отношении файлов данных Скрытая информация и особенности ее исследования при решении экспертных задач Поиск информация при решении экспертных задач	ПК-1	ПК-1.2	Контрольная работа 3 Контрольная работа 4

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Формирование оценок:

Лабораторные работы после выполнения оцениваются преподавателем, и выставляется оценка «зачтено» при условии ответа на 80% вопросов преподавателя по предметной области лабораторной работы. По итогам лабораторных работ и устного ответа студента выставляется оценка «зачтено» или «не зачтено» по лабораторным работам всей дисциплины. К сдаче экзамена допускаются студенты, сдавшие 100% лабораторных работ.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом интегрированных информационных технологий (теоретическими основами дисциплины), способен иллюстрировать ответ примерами, применять теоретические знания для решения практических задач в области использования интегрированных информационных технологий	*Повышенный уровень*	*Отлично*
Обучающийся владеет понятийным аппаратом данной области науки (теоретическими основами дисциплины), способен формулировать основные понятия предметной области, но затрудняется приводить примеры, характеризующие особенности предметной области	*Базовый уровень*	*Хорошо*
Обучающийся частично владеет теоретическими основами дисциплины, фрагментарно способен формулировать основные понятия предметной области, но затрудняется приводить примеры и схемы, описывающие информационные системы и применяющиеся в них технологии	*Пороговый уровень*	*удовлетворительно*
Обучающийся демонстрирует отрывочные, фрагментарные знания не понимает основных понятий предметной области и допускает грубые ошибки в предметной области.	–	*Неудовлетворительно*

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью контрольных работ

Контрольная работа 1

Вариант 1

1. Общие и частные экспертные задачи компьютерной экспертизы.

2. Специальные методы решения экспертных задач компьютерной экспертизы. Специфика

общеэкспертных методов, применяемых для решения задач компьютерной экспертизы.

3. Понятие и специфика информационных объектов. Определение групповой принадлежности информационных объектов.

Вариант 2

1. Методы диалектической и формальной логики, используемые при решении экспертных задач компьютерной экспертизы.

2. Этапы экспертного осмотра объектов компьютерной экспертизы.

3. Природа следов в информационных системах, их источники и способы фиксации.

Вариант 3

1. Общенаучные методы решения экспертных задач компьютерной экспертизы.

2. Организационно-технические меры, сопутствующие решению экспертных задач компьютерной экспертизы.

3. Классификация, содержание и место нахождения следов в информационных системах.

Контрольная работа 2

Вариант 1

1. Структура раздела NTFS. Роль файла $MFT в описании размещения данных в разделе.

2. Следообразование в файловой системе NTFS.

3. Структура индекса файла (inode) и его значимые поля. Таблица адресов inode и правила адресации тела файла.

Вариант 2

1. Основные атрибуты файлов в NTFS.

2. Типы разделов файловых систем, используемых операционной системой Linux, их структура. Архитектура главной файловой системы.

3. Классификация программных средств для получения несанкционированного доступа к системным ресурсам.

Контрольная работа 3

Вариант 1

1. Структура индекса файла (inode) и его значимые поля.

2. Закономерности известных способов текстовых описаний формата файлов.

3. Алгоритм решения поисковой задачи в реляционных базах данных, построенных на основе классических DBF-файлов.

Вариант 2

1. Таблица адресов inode и правила адресации тела файла.

2. Формат классических DBF-файлов.

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

Вариант 3

1. Следообразование в файловых системах Ext2fs, Ext3fs, Reiserfs.

2. Служебные файлы и каталоги Linux.

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

Контрольная работа 4

Вариант 1

1. Методические рекомендации по поиску следов использования криптографических программных продуктов.

2. Использование сетевых уязвимостей для нарушения работоспособности компьютерных систем.

3. Служебные каталоги операционной системы Windows.

Вариант 2

1. Методические рекомендации по поиску предположительно вредоносных программ.

2. Принципы стеганографии. Основные способы и средства сокрытия информации методом стеганографии.

3. Методы и средства защиты программных продуктов от неправомерной уста-новки и использования.

Вариант 3

1. Способы шифрования информации с открытым и закрытым ключом.

2. Организация хранения данных на компакт-дисках и на устройствах флэш-памяти.

3. Реестр операционной системы Windows.

20.2 Промежуточная аттестация

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме индивидуального опроса в рамках рубежных аттестаций. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.