МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.

«31» августа 2021 г.

Рабочая программа дисциплины
Основы компьютерной экспертизы

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Гортинский А. В.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления	Юшинова И. В.		31.08.2021 г.

1. Цели освоения дисциплины

Целями освоения дисциплины «Основы компьютерной экспертизы» являются знакомство с методами и средствами анализа состояния компьютерных систем и получение навыков расследования компьютерных инцидентов, основанных на использовании уязвимостей.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» учебного плана ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Системы управления базами данных», «Операционные системы» и «Основы информационной безопасности».

Компетенции, сформированные при изучении данной дисциплины, могут быть полезны при изучении дисциплины «Программно-аппаратные средства обеспечения информационной безопасности».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-2. Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.	ОПК-2.1.1 знает общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств и программного обеспечения персонального компьютера; классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей; ОПК-2.1.2 знает принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных	Знать общие принципы построения современных компьютеров, формы и способы представления данных в персональном компьютере; логико-математические основы построения электронных цифровых устройств; состав, назначение аппаратных средств и программного обеспечения персонального компьютера; классификацию современных вычислительных систем, типовые структуры и принципы организации компьютерных сетей; принципы построения современных операционных систем и особенности их применения; принципы разработки специального программного обеспечения, предназначенного для преодоления защиты современных операционных систем с использованием их недокументированных

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	систем с использованием их недокументированных возможностей; основные принципы конфигурирования и администрирования операционных систем; ОПК-2.2.1 умеет применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети интернет; составлять документы, используя прикладные программы офисного назначения; ОПК-2.3.1 владеет средствами управления пользовательскими интерфейсами операционных систем.	возможностей; основные принципы конфигурирования и администрирования операционных систем; Уметь применять типовые программные средства сервисного назначения, информационного поиска и обмена данными в сети интернет; составлять документы, используя прикладные программы офисного назначения; Владеть владеет средствами управления пользовательскими интерфейсами операционных систем.
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации.	ОПК-5.1.2 знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за	Знать основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации; основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации; основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
	разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности; ОПК-5.2.3 умеет анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; ОПК-5.3.2 владеет методами и средствами технической защиты информации.	разглашение защищаемой информации; правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности; Уметь анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами в области технической защиты информации; Владеть методами и средствами технической защиты информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 часа.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
1	Теоретические основы судебной компьютерной экспертизы	7	1-11	22	22	–	2	14	*Контрольная работа* на 10-й неделе
2	Правовые и методические основы судебной компьютер		12-14	6	6	–	1	10	

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	ной экспертизы								
3	Практические основы экспертного исследования компьютерной информации		15-17	6	6	–	1	12	
	Промежуточная аттестация - 36								**Экзамен**
	ИТОГО – 144ч.			**34**	**34**	**–**	**4**	**36**	

Содержание дисциплины

Теоретические основы судебной компьютерной экспертизы. Теоретические основы судебной экспертизы. Теоретические основы экспертного исследования компьютерной информации. Устройство внешней памяти на низком уровне. Технико-криминалистическая характеристика файловых систем ранних ОС (FAT, Ext2fs, Ext3fs). Техико-криминалистическая характеристика NTFS. Значимые области следообразования в системных структурах ОС. Области следообразования в файлах различных форматов.

Правовые и методические основы судебной компьютерной экспертизы. Законодательство РФ по охране компьютерной информации. Правовой статус эксперта, структура и правила оформления заключения эксперта. Методические основы компьютерной экспертизы.

Практические основы экспертного исследования компьютерной информации. Обеспечение, используемое в экспертной практике и фиксация следовой картины. Анализ следов воздействия на информацию в операционной системе Windows при решении задачи поиска по контексту. Установление обстоятельств создания файлов и изготовления документов. Установление обстоятельств работы в сети и исследование предположительно вредоносных программ.

План лабораторных занятий

На лабораторных занятиях студенты исследуют области следообразования в файловой системе и осваивают формальные основы составления экспертного заключения. Для этого на лабораторных занятиях последовательно изучаются системные области файловой системы, служебные файлы ОС, проводятся эксперименты с воздействием различных программ на файловую систему, осуществляется поиск следов в выданных преподавателем файловых системах виртуальных машин. При проведении лабораторных занятий используется ОС Windows и Virtual Box, а так же свободно-распространяемое программное обеспечение, которое выдает преподаватель на одном из первых занятий, всего около 40 программных средств, например таких как: Quick Unpack 0.7, File Analyser, File Decoder, Event Log Explorer, LDE, NTFS Stream explorer, Hexeditor, PE Explorer, SQLiteStudio, XnView, Windows Registry Recovery и т.д.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1	Теоретические основы судебной компьютерной экспертизы. Теоретические основы судебной экспертизы.	№1
2	Теоретические основы судебной компьютерной экспертизы. Теоретические основы экспертного исследования компьютерной информации.	№2
3	Теоретические основы судебной компьютерной экспертизы. Устройство внешней памяти на низком уровне.	№3
4-5	Теоретические основы судебной компьютерной экспертизы. Технико-криминалистическая характеристика файловых систем ранних ОС (FAT, Ext2fs, Ext3fs).	№4
6-7	Теоретические основы судебной компьютерной экспертизы. Техико-криминалистическая характеристика NTFS.	№5
8-9	Теоретические основы судебной компьютерной экспертизы. Значимые области следообразования в системных структурах ОС.	№6
10-11	Теоретические основы судебной компьютерной экспертизы. Области следообразования в файлах различных форматов.	№7
12	Правовые и методические основы судебной компьютерной экспертизы. Законодательство РФ по охране компьютерной информации. Правовой статус эксперта, структура и правила оформления заключения эксперта.	№8
13-14	Правовые и методические основы судебной компьютерной экспертизы. Методические основы компьютерной экспертизы.	№9

№ занятия	Тема	Задания для лабораторного практикума
1	2	3
15	Практические основы экспертного исследования компьютерной информации. Обеспечение, используемое в экспертной практике и фиксация следовой картины. Анализ следов воздействия на информацию в операционной системе Windows при решении задачи поиска по контексту.	№10
16-17	Практические основы экспертного исследования компьютерной информации. Установление обстоятельств создания файлов и изготовления документов.	№11

5. Образовательные технологии, применяемые при освоении дисциплины

Предусматривается широкое использование в учебном процессе образовательных технологий аналогичных творческой мастерской и кейс. На лабораторных занятиях, проводимых методом творческой мастерской студентам предоставляется возможность в очерченных рамках тематики и указанной цели самостоятельно ставить эксперименты по следообразованию и выделять признаки того или иного вида деятельности пользователя в информационной системе компьютера. На лабораторных занятиях, проводимых методом кейса, студентам выдаются срезы файловых систем или накопители виртуальных машин, в которых отразилась деятельность по воздействию на информационную среду компьютера, кроме того выдаются типовые вопросы, которые ставит лицо, проводящее расследование и обстоятельства события. Студент должен найти достаточное количество следов для категорического ответа на поставленные вопросы.

Кроме того, предусматриваются выступления экспертов и специалистов перед студентами, встречи с представителями ведущих отечественных фирм по защите информации, ознакомительные беседы с представителями потенциальных работодателей.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты доделывают лабораторные работы, которые начали на аудиторных занятиях. Как правило либо готовят отчет, где описывают порядок постановки экспериментов и наблюдаемые результаты, либо оформляют элементы экспертизы, проводимой над выданными преподавателем информационными объектами – файловыми системами, подвергшимися воздействию при осуществлении деструктивной деятельности.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольной работы, контрольные вопросы, вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Основы компьютерной экспертизы».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	10	5	0	5	0	40	40	**100**

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 10 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий в течение одного семестра – от 0 до 5 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Контроль результатов самостоятельной работы, которая состоит в доведении до заключительной стадии и оформлении исследований, начатых на аудиторных занятиях. Оформленные работы в электронном виде сдаются преподавателю для дальнейшей проверки.

Выполнение заданий в рамках самостоятельной работы в течение семестра – от 0 до 5 баллов.

0 баллов – работа не сдана

1 балл – работа содержит грубые ошибки, цель поиска не достигнута, оформление не соответствует предъявляемым требованиям.

2 балла – содержит грубые ошибки, цель поиска не достигнута, оформление соответствует предъявляемым требованиям.

3 балла – содержит ошибки, критически не влияющие на получение результата, найдены все присутствующие на объекте следы или поставлены опыты в отношении не всех следообразующих областей, оформление соответствует предъявляемым требованиям.

4 балла – содержит незначительные ошибки, практически все следы найдены, есть неточности в оценке наблюдаемых следов, оформление соответствует предъявляемым требованиям.

5 баллов – не содержит ошибок, все следы найдены, оформление соответствует предъявляемым требованиям.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контрольная работа должна быть аккуратно оформлена по стандарту оформления реферата и экспертного заключения. В ней должны присутствовать описательная, исследовательская и заключительная часть, а также обоснованные выводы.

Контрольная работа оценивается – от 0 до 40 баллов, а именно

работа на «отлично» оценивается от 35 до 40 баллов;

работа на «хорошо» оценивается от 30 до 34 баллов;

работа на «удовлетворительно» оценивается от 20 до 29 баллов;

работа на «неудовлетворительно» оценивается от 0 до 19 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой *экзамен*, проводимый в устной форме с предварительной подготовкой студента к ответу.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 31 до 40 баллов;

ответ на «хорошо» оценивается от 21 до 30 баллов;

ответ на «удовлетворительно» оценивается от 11 до 20 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 10 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за седьмой семестр по дисциплине «Основы компьютерной экспертизы» составляет **100** баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Основы компьютерной экспертизы» в оценку (экзамен)

91-100 баллов	«отлично»
81-90 баллов	«хорошо»
65-80 баллов	«удовлетворительно»
0-64 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Балашов, Д. Н. Криминалистика [Электронный ресурс] : Учебное пособие / Д. Н. Балашов, С. В. Маликов, Н. М. Балашов. - 6. - Москва : Издательский Центр РИОР ; Москва : ООО "Научно-издательский центр ИНФРА-М", 2015. - 241 с. - ISBN 978-5-369-01353-3 : Б. ц. URL: http://znanium.com/go.php?id=460715. Загл. с экрана. Яз. Рус.

2) Россинская, Е. Р. Теория судебной экспертизы (Судебная экспертология) : учебник / Е.Р. Россинская, Е.И. Галяшина, А.М. Зинин ; под ред. Е.Р. Россинской. - 2-е изд., перераб и доп. - Москва : Норма : ИНФРА-М, 2020. - 368 с. - ISBN 978-5-91768-716-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1088918.

3) Таненбаум, Э. Архитектура компьютера. 6-е изд. / Э. Таненбаум, Т. Остин. - Санкт-Петербург : Питер, 2013. - 816 с. : ил. - URL: http://ibooks.ru/reading.php?short=1&isbn=978-5-496-00337-7. - ISBN 978-5-496-00337-7

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: ОС Windows.

2) Свободное программное обеспечение: Virtual Box, Quick Unpack 0.7, File Analyser, File Decoder, Event Log Explorer, LDE, NTFS Stream explorer, Hexeditor, PE Explorer, SQLiteStudio, XnView, Windows Registry Recovery.

3) Национальный центр по борьбе с преступлениями в сфере высоких технологий [Электронный ресурс]. URL: http://www.nhtcu.ru/jur. Загл. с экрана. Яз. рус.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходимы аудитория, оборудованная компьютером с установленным любым программным обеспечением, позволяющим читать следующие форматы файлов данных: pdf, doc, docx, ppt, pptx и подключаемый к нему проектор.

Для проведения лабораторных занятий необходимы аудитории, оборудованные компьютерами класса не ниже Pentium IV, с установленным любым программным обеспечением ОС Windows, Virtual Box.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии к. ю. н., доцент А. В. Гортинский

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.