МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «СГУ имени Н.Г. Чернышевского»

Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ

«13» 04 2017 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,
2017

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 вариативной части Блока 1 «Дисциплины (Модули)» ООП и направлена на формирование у обучающихся общепрофессиональных и профессиональных 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. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен обладать следующими общепрофессиональными и профессиональными компетенциями:

- способностью использовать нормативные правовые акты в своей профессиональной деятельности (ОПК-5);
- способностью проводить анализ безопасности компьютерных систем на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности (ПК-3);
- способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа (ПК-14).

В рамках указанных компетенций обучающийся должен

- Знать:

– современные методы и средства исследования компьютерной информации;

– современные методы и средства расследования компьютерных инцидентов;

- Уметь:

– осуществлять фиксацию следов компьютерных инцидентов;

– организовывать исследование компьютерной информации;

- Владеть:

– навыками проведения расследований компьютерных инцидентов;

– навыками работы со средствами экспертного исследования информации.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 часов.

№ 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)
				Всего часов	Лекции	Лабораторные занятия	Самостоятельная работа	
1	2	3	4	5	6	7	8	9
1	Теоретические основы судебной компьютерной экспертизы	7	1-11	68	22	22	24	Контрольная работа на 10-й неделе
2	Правовые и методические основы судебной компьютерной экспертизы		12-14	36	6	6	24	
3	Практические основы экспертного исследования компьютерной информации		15-18	40	8	8	24	
	Промежуточная аттестация							Экзамен
	ИТОГО			**180**	**36**	**36**	**72**	**36**

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	Теоретические основы судебной компьютерной экспертизы. Значимые области следообразования в системных структурах ОС.	№6
9	Теоретические основы судебной компьютерной экспертизы. Области следообразования в файлах различных форматов.	№7
10-12	Правовые и методические основы судебной компьютерной экспертизы. Законодательство РФ по охране компьютерной информации. Правовой статус эксперта, структура и правила оформления заключения эксперта.	№8

№ занятия	Тема	Задания для лабораторного практикума
1	2	3
13-14	Правовые и методические основы судебной компьютерной экспертизы. Методические основы компьютерной экспертизы.	№9
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
18	Практические основы экспертного исследования компьютерной информации. Установление обстоятельств работы в сети и исследование предположительно вредоносных программ.	№12

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.

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; увеличивается время на самостоятельное освоение материала.

Основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья и инвалидов, 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 (зачет). Фонд оценочных средств дисциплины приведён в приложении 1.

7. Данные для учета успеваемости студентов в БАРС

Таблица 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 – 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) основная 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 (дата обращения: 02.01.2017). Загл. с экрана. Яз. рус.

б) дополнительная литература:

1) Криминалистика [Текст] : учебник / В. В. Агафонов [и др.] ; под ред. А. Г. Филиппова. - Москва : Высш. образование, 2007. - 441, [7] с. : табл. - (Основы наук) (Высшее образование). - ISBN 5-9692-0096-4 (в пер.).

2) Таненбаум, Э. С. Современные операционные системы [Текст] = Modern Operating Systems / Э. С. Таненбаум ; пер. на рус. яз. А. Леонтьева. - 2-е изд. - Москва ; Санкт-Петербург [и др.] : Питер, 2007. - 1037, [3] с. : рис. - (Классика Computer Science). - Библиогр.: с. 998-1020. - Алф. указ.: с. 1021-1037. - ISBN 978-5-318-00299-1 (в пер.). - ISBN 0-13-031358-0 (анг.).

в) Интернет-ресурсы:

1) Национальный центр по борьбе с преступлениями в сфере высоких технологий [Электронный ресурс]. URL: http://www.nhtcu.ru/jur (дата обращения: 02.01.2017) Загл. с экрана. Яз. рус.

2) Компьютерно-техническая экспертиза [Электронный ресурс]. URL: http://computer-forensics-lab.org (дата обращения: 02.01.2017) Загл. с экрана. Яз. рус.

г) программное обеспечение:

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.

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 и специализации «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Авторы

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

Старший преподаватель кафедры теоретических основ компьютерной безопасности и криптографии  И.Ю. Юрин

Программа разработана в 2012 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «25» мая 2012 года, протокол № 18).

Программа актуализирована в 2017 г. (одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «09» января 2017 года, протокол № 10).

Заведующий кафедрой теоретических основ компьютерной безопасности и криптографии, профессор, к.ф.-м.н.  В.Н. Салий

Декан факультета компьютерных наук и информационных технологий, к.ф.-м.н., доцент  А.Г. Федорова