

Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем (продвинутый уровень)

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
WINDOWS- И LINUX ОРИЕНТИРОВАННЫЕ ИНСТРУМЕНТЫ
ФОРЕНЗИКИ

Блок:	Блок 1 «Дисциплины (модули)»
Часть образовательной программы:	Часть, формируемая участниками образовательных отношений
№ дисциплины по учебному плану:	Б4.Ч.03
Трудоемкость в зачетных единицах:	4 семестр - 2;
Часов (всего) по учебному плану:	72 часа
Лекции	4 семестр - 16 часов;
Практические занятия	4 семестр - 16 часов;
Лабораторные работы	не предусмотрено учебным планом
Консультации	проводится в рамках часов аудиторных занятий
Самостоятельная работа	4 семестр - 39,7 часа;
в том числе на КП/КР	не предусмотрено учебным планом
Иная контактная работа	проводится в рамках часов аудиторных занятий
включая: Доклад Домашнее задание Контрольная работа	
Промежуточная аттестация:	
Зачет	4 семестр - 0,3 часа;

Москва 2023

ПРОГРАММУ СОСТАВИЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskeyAY-0b6e493d

(подпись)

А.Ю. Невский

(расшифровка
подписи)

СОГЛАСОВАНО:

Руководитель
образовательной программы

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка
подписи)

Заведующий выпускающей
кафедры

(должность, ученая степень, ученое звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskeyAY-0b6e493d

(подпись)

А.Ю. Невский

(расшифровка
подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: Формирование знаний и навыков по применению программных Windows и Linux-ориентированных приложений для решения основных задач форензики.

Задачи дисциплины

- на основе изучения перечня и содержания основных задач форензики и анализа программных приложений определить их перечень для практического применения;;
- на основе анализа особенностей операционных систем типа Windows и Linux, которые они накладывают на решение задач форензики изучить правила, технологию и особенности применения программных приложений для их решения;;
- сформировать готовность и способность студентов к практическому применению программных приложений при решении задач форензики..

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Запланированные результаты обучения
ОПК-2 способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ИД-2 _{ОПК-2} Применяет программно-аппаратные средства и средства системного назначения, инструментальные средства, в том числе отечественного производства для решения профессиональных задач	знать: - перечень программных приложений под Windows и Linux для решения основных задач форензики;; - особенности решения основных задач форензики при исследовании информационных систем под управлением ОС типа Windows и Linux;. уметь: - практически использовать программные приложения под Windows и Linux при решении основных задач форензики;; - правильно интерпретировать результаты исследования (задач форензики), полученные с использованием программных приложений под ОС Windows и Linux.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к факультативным дисциплинам основной профессиональной образовательной программе Безопасность компьютерных систем (продвинутый уровень) (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа							СР			
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
КПР	ГК	ИККП	ТК											
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Особенности решения основных задач форензики в Windows и Linux системах	20	4	4	-	4	-	-	-	-	-	12	-	<p><u>Подготовка к аудиторным занятиям:</u> Проработка лекции, выполнение и подготовка к защите лаб. работы</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Особенности решения основных задач форензики в Windows и Linux системах"</p> <p><u>Подготовка реферата:</u> В рамках реферативной части студенту необходимо провести обзор интернет-источников по выбранной теме, подготовить презентацию для выступления по результатам работы на семинарском занятии. В качестве тем реферата студенту предлагаются следующие варианты: - анализ особенностей работы с файлами и дисками в ОС Windows при решении задач форензики; - анализ особенностей работы с файлами и дисками в ОС Linux при решении задач форензики; - анализ особенностей работы с приложениями ОС Windows при решении задач форензики; - анализ особенностей работы с приложениями ОС Linux при решении задач форензики; - анализ особенностей работы с памятью в Windows-системах при решении задач форензики; - анализ особенностей работы с памятью в</p>
1.1	Особенности решения основных задач форензики в системах типа Windows	10		2	-	2	-	-	-	-	-	6	-	
1.2	Особенности решения основных задач форензики в системах Linux	10		2	-	2	-	-	-	-	-	6	-	

													Linux-системах при решении задач форензики; <u>Изучение материалов литературных источников:</u> [1], 48-76 [3], 91-128 [5], 17-45	
2	Windows ориентированные инструменты для решения задач форензики	18	4	-	4	-	-	-	-	-	-	10	-	<u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Windows ориентированные инструменты для решения задач форензики" <u>Подготовка домашнего задания:</u>
2.1	Возможности встроенных средств ОС Windows для решения задач форензики	8	2	-	2	-	-	-	-	-	-	4	-	Подготовка домашнего задания направлена на отработку умений решения профессиональных задач. Домашнее задание выдается студентам по изученному в разделе "Windows ориентированные инструменты для решения задач форензики" материалу.
2.2	Возможности программных приложений под ОС Windows для решения задач форензики	10	2	-	2	-	-	-	-	-	-	6	-	Дополнительно студенту необходимо изучить литературу и разобрать примеры выполнения подобных заданий. Проверка домашнего задания проводится по представленным письменным работам. В качестве тем домашнего задания студентам предлагаются следующие варианты: - практическая работа с образами дисков Arsenal Image Mounter; - создание дампа физической памяти с использованием утилиты DumpIt; - создание доказательных файлов EnCase с использованием утилиты EnCase Forensic Imager; - выявление зашифрованных томов TrueCrypt, PGP, Bitlocker с использованием утилиты Encrypted Disk Detector; - захват веб-страниц для проведения расследований с использованием браузера Forensics Acquisition of Websites; - просмотр и клонирование носителей данных с использованием утилиты FTK Imager.

													<p><u>Подготовка к практическим занятиям:</u> Изучение материала по разделу "Windows ориентированные инструменты для решения задач форензики" подготовка к выполнению заданий на практических занятиях: - Практическая работа с образами дисков Arsenal Image Mounter; - создание дампа физической памяти с использованием утилиты DumpIt; - создание доказательных файлов EnCase с использованием утилиты EnCase Forensic Imager; - выявление зашифрованных томов TrueCrypt, PGP, Bitlocker с использованием утилиты Encrypted Disk Detector; - захват веб-страниц для проведения расследований с использованием браузера Forensics Acquisition of Websites; - просмотр и клонирование носителей данных с использованием утилиты FTK Imager.</p> <p><u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Windows ориентированные инструменты для решения задач форензики"</p> <p><u>Изучение материалов литературных источников:</u> [2], 51-72</p>
3	Linux ориентированные инструменты для решения задач форензики	33.7	8	-	8	-	-	-	-	-	17.7	-	<p><u>Подготовка к текущему контролю:</u> Повторение материала по разделу "Linux ориентированные инструменты для решения задач форензики": Guymager - бесплатный криминалистический "тепловизор".</p>
3.1	Решение задач форензики с использованием Kali Linux.	17.7	4	-	4	-	-	-	-	-	9.7	-	<p>Назначение, описание, основные возможности и приемы работы; ProDiscover - утилита для захвата и анализа дисков.</p>
3.2	Другие инструменты для решения задач форензики под ОС	16	4	-	4	-	-	-	-	-	8	-	<p>Назначение, описание, основные возможности и приемы работы; SIFT Workstation программы с открытым исходным кодом для служб реагирования на</p>

	Linux												инциденты и проведения криминалистической цифровой экспертизы в различных условиях. Назначение, описание, основные возможности и приемы работы; <u>Самостоятельное изучение теоретического материала:</u> Изучение дополнительного материала по разделу "Linux ориентированные инструменты для решения задач форензики". Kali Linux - описание дистрибутива и решение задач: - тестирование на проникновение - исследование безопасности - компьютерная криминалистика - реверс-инжиниринг. <u>Подготовка к контрольной работе:</u> Изучение материалов по разделу Linux ориентированные инструменты для решения задач форензики и подготовка к контрольной работе <u>Изучение материалов литературных источников:</u> [4], 115-248
	Зачет	0.3	-	-	-	-	-	-	-	0.3	-	-	
	Всего за семестр	72.0	16	-	16	-	-	-	-	0.3	39.7	-	
	Итого за семестр	72.0	16	-	16	-	-	-	-	0.3	39.7	-	

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПр – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Особенности решения основных задач форензики в Windows и Linux системах

1.1. Особенности решения основных задач форензики в системах типа Windows
Технология и особенности выявления цифровых следов злоумышленной деятельности в Windows-системах.

1.2. Особенности решения основных задач форензики в системах Linux
Технология и особенности выявления цифровых следов злоумышленной деятельности в Linux-системах.

2. Windows ориентированные инструменты для решения задач форензики

2.1. Возможности встроенных средств ОС Windows для решения задач форензики
Программы работы с файлами, памятью, реестром Windows.

2.2. Возможности программных приложений под ОС Windows для решения задач форензики

Возможности бесплатных утилит под Windows для решения задач форензики: Arsenal Image Mounter - утилита для работы с образами дисков; DumpIt - утилита для создания дампа физической памяти; EnCase Forensic Imager - утилита для создания доказательных файлов EnCase; Encrypted Disk Detector - утилита для выявления зашифрованных томов TrueCrypt, PGP, Bitlocker; Forensics Acquisition of Websites - браузер, предназначенный для захвата веб-страниц для проведения расследований; FTK Imager - утилита для просмотра и клонирования носителей данных в среде Windows..

3. Linux ориентированные инструменты для решения задач форензики

3.1. Решение задач форензики с использованием Kali Linux.

Kali Linux - описание дистрибутива, решение задач тестирования на проникновение, исследование безопасности, компьютерная криминалистика, реверс-инжиниринг..

3.2. Другие инструменты для решения задач форензики под ОС Linux

Guymager - бесплатным криминалистический "тепловизор"; ProDiscover - утилита для захвата и анализа дисков; SIFT Workstation программы с открытым исходным кодом для служб реагирования на инциденты и проведения криминалистической цифровой экспертизы в различных условиях..

3.3. Темы практических занятий

не предусмотрено

3.4. Темы лабораторных работ

не предусмотрено

3.5 Консультации

Групповые консультации по разделам дисциплины (ГК)

1. Обсуждение материалов по кейсам раздела "Особенности решения основных задач форензики в Windows и Linux системах"

2. Обсуждение материалов по кейсам раздела "Windows ориентированные инструменты для решения задач форензики": Изучение материала по разделу "Windows ориентированные инструменты для решения задач форензики" подготовка к выполнению заданий на практических занятиях: - практическая работа с образами дисков Arsenal Image Mounter; - создание дампа физической памяти с использованием утилиты DumpIt; - создание доказательных файлов EnCase с использованием утилиты EnCase Forensic Imager; - выявление зашифрованных томов TrueCrypt, PGP, Bitlocker с использованием утилиты Encrypted Disk Detector; - захват веб-страниц для проведения расследований с использованием браузера Forensics Acquisition of Websites; - просмотр и клонирование носителей данных с использованием утилиты FTK Imager.
3. Обсуждение материалов по кейсам раздела "Linux ориентированные инструменты для решения задач форензики": Изучение дополнительного материала по разделу "Linux ориентированные инструменты для решения задач форензики". Kali Linux - описание дистрибутива и решение задач: - тестирование на проникновение - исследование безопасности - компьютерная криминалистика - реверс-инжиниринг.

Индивидуальные консультации по курсовому проекту /работе (ИККП)

1. Консультации проводятся по разделу "Особенности решения основных задач форензики в Windows и Linux системах" - анализ особенностей работы с файлами и дисками в ОС Windows при решении задач форензики; - анализ особенностей работы с файлами и дисками в ОС Linux при решении задач форензики; - анализ особенностей работы с приложениями ОС Windows при решении задач форензики; - анализ особенностей работы с приложениями ОС Linux при решении задач форензики; - анализ особенностей работы с памятью в Windows-системах при решении задач форензики; - анализ особенностей работы с памятью в Linux-системах при решении задач форензики;

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Windows ориентированные инструменты для решения задач форензики": Изучение материала по разделу "Windows ориентированные инструменты для решения задач форензики" подготовка к выполнению заданий на практических занятиях: - Практическая работа с образами дисков Arsenal Image Mounter; - последовательность создания дампа физической памяти с использованием утилиты DumpIt; - последовательность создания доказательных файлов EnCase с использованием утилиты EnCase Forensic Imager; - технология выявления зашифрованных томов TrueCrypt, PGP, Bitlocker с использованием утилиты Encrypted Disk Detector; - последовательность захвата веб-страниц для проведения расследований с использованием браузера Forensics Acquisition of Websites; - технология просмотра и клонирования носителей данных с использованием утилиты FTK Imager.
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Linux ориентированные инструменты для решения задач форензики": Guymager - бесплатный криминалистический "тепловизор". Назначение, описание, основные возможности и приемы работы; ProDiscover - утилита для захвата и анализа дисков. Назначение, описание, основные возможности и приемы работы; SIFT Workstation программы с открытым исходным кодом для служб реагирования на инциденты и проведения криминалистической цифровой экспертизы в различных условиях. Назначение, описание, основные возможности и приемы работы;

3.6 Тематика курсовых проектов/курсовых работ

Курсовой проект/ работа не предусмотрены

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
особенности решения основных задач форензики при исследовании информационных систем под управлением ОС типа Windows и Linux;	ИД-2ОПК-2	+			Доклад/Особенности решения задач форензики в Windows и Linux системах
перечень программных приложений под Windows и Linux для решения основных задач форензики;	ИД-2ОПК-2		+		Домашнее задание/Windows ориентированные инструменты для решения задач форензики.
Уметь:					
правильно интерпретировать результаты исследования (задач форензики), полученные с использованием программных приложений под ОС Windows и Linux	ИД-2ОПК-2			+	Контрольная работа/Linux-ориентированные инструменты для решения задач форензики
практически использовать программные приложения под Windows и Linux при решении основных задач форензики;	ИД-2ОПК-2			+	Доклад/Особенности решения задач форензики в Windows и Linux системах

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

4 семестр

Форма реализации: Выполнение задания

1. Windows ориентированные инструменты для решения задач форензики. (Домашнее задание)

Форма реализации: Выступление (доклад)

1. Особенности решения задач форензики в Windows и Linux системах (Доклад)

Форма реализации: Защита задания

1. Linux-ориентированные инструменты для решения задач форензики (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.

4.2 Промежуточная аттестация по дисциплине

Зачет (Семестр №4)

Итоговая оценка выставляется исходя из оценок семестровой и зачетной. Семестровая оценка должна быть не ниже 3,0 и зачетная - не ниже "зачет".

В диплом выставляется оценка за 4 семестр.

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Васильев, В. И. Интеллектуальные системы защиты информации : учебное пособие для вузов по специализациям специальности "Комплексное обеспечение информационной безопасности автоматизированных систем" / В. И. Васильев . – 2-е изд., испр . – М. : Машиностроение, 2013 . – 172 с. – (Для вузов) . - ISBN 978-5-94275-667-3 .;
2. Capture the Flag [CTF]. Игровые модели подготовки специалистов в сфере компьютерной безопасности : [учебно-методическое пособие для преподавателей] / А. Ю. Егоров, А. С. Минзов, А. Ю. Невский, О. Р. Баронов, Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ", Кафедра "Безопасности и Информационных Технологий" (БИТ) . – М. : ВНИИГеосистем, 2018 . – 72 с. - ISBN 978-5-8481-0232-1 .;
3. Анашкина, Н. В. Технологии и методы программирования : учебное пособие для вузов по направлению 090900 "Информационная безопасность", специальностям 090301 "Компьютерная безопасность", 090303 "Информационная безопасность автоматизированных систем" / Н. В. Анашкина, Н. Н. Петухова, В. Ю. Смольянинов . – М. : Академия, 2012 . – 384 с. – (Высшее профессиональное образование . Бакалавриат) . - ISBN 978-5-7695-8429-9 .;
4. OpenOffice.org. Теория и практика / И. Хахаев, и др. – М. : ALT Linux : БИНОМ. Лаборатория знаний, 2013 . – 318 с. + CD-ROM . – (Библиотека ALT Linux) . - ISBN 978-5-94774-891-8 .;

5. В. С. Пелешенко, С. В. Говорова, М. А. Лапина- "Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления", Издательство: "Северо-Кавказский Федеральный университет (СКФУ)", Ставрополь, 2017 - (86 с.)

<https://biblioclub.ru/index.php?page=book&id=467139>.

5.2 Лицензионное и свободно распространяемое программное обеспечение:

1. СДО "Прометей";
2. Office / Российский пакет офисных программ;
3. Windows / Операционная система семейства Linux;
4. Майнд Видеоконференции;
5. Windows Server / Серверная операционная система семейства Linux;
6. Kali Linux;
7. Libre Office;
8. ОС Linux.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:

1. ЭБС Лань - <https://e.lanbook.com/>
2. ЭБС "Университетская библиотека онлайн" - http://biblioclub.ru/index.php?page=main_ub_red
3. Научная электронная библиотека - <https://elibrary.ru/>
4. База данных ВИНТИ online - <http://www.viniti.ru/>
5. База данных журналов издательства Elsevier - <https://www.sciencedirect.com/>
6. Электронные ресурсы издательства Springer - <https://link.springer.com/>
7. База данных Web of Science - <http://webofscience.com/>
8. База данных Scopus - <http://www.scopus.com>
9. Национальная электронная библиотека - <https://rusneb.ru/>
10. ЭБС "Консультант студента" - <http://www.studentlibrary.ru/>

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер

	К-307, Учебная лаборатория "Открытое программное обеспечение"	стол преподавателя, стол компьютерный, стол учебный, стул, вешалка для одежды, тумба, компьютерная сеть с выходом в Интернет, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
	К-302, Учебная лаборатория "Информационно-аналитические технологии"	стол преподавателя, стол компьютерный, стул, мультимедийный проектор, экран, доска маркерная, сервер, компьютер персональный, кондиционер
Помещения для консультирования	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Windows- и Linux ориентированные инструменты форензики

(название дисциплины)

4 семестр

Перечень контрольных мероприятий текущего контроля успеваемости по дисциплине:

- КМ-1 Особенности решения задач форензики в Windows и Linux системах (Доклад)
- КМ-2 Windows ориентированные инструменты для решения задач форензики. (Домашнее задание)
- КМ-3 Linux-ориентированные инструменты для решения задач форензики (Контрольная работа)

Вид промежуточной аттестации – Зачет.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3
		Неделя КМ:	5	10	15
1	Особенности решения основных задач форензики в Windows и Linux системах				
1.1	Особенности решения основных задач форензики в системах типа Windows		+		
1.2	Особенности решения основных задач форензики в системах Linux		+		
2	Windows ориентированные инструменты для решения задач форензики				
2.1	Возможности встроенных средств ОС Windows для решения задач форензики			+	
2.2	Возможности программных приложений под ОС Windows для решения задач форензики			+	
3	Linux ориентированные инструменты для решения задач форензики				
3.1	Решение задач форензики с использованием Kali Linux.				+
3.2	Другие инструменты для решения задач форензики под ОС Linux		+		
Вес КМ, %:			25	35	40