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

Оценочные материалы
по дисциплине
Windows- и Linux ориентированные инструменты форензики

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. 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 Применяет программно-аппаратные средства и средства системного назначения, инструментальные средства, в том числе отечественного производства для решения профессиональных задач

и включает:

для текущего контроля успеваемости:

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)

БРС дисциплины

4 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	5	10	15
Особенности решения основных задач форензики в Windows и Linux системах				
Особенности решения основных задач форензики в системах типа Windows		+		
Особенности решения основных задач форензики в системах Linux		+		
Windows ориентированные инструменты для решения задач форензики				
Возможности встроенных средств ОС Windows для решения задач форензики			+	
Возможности программных приложений под ОС Windows для решения задач форензики			+	

Linux ориентированные инструменты для решения задач форензики			
Решение задач форензики с использованием Kali Linux.			+
Другие инструменты для решения задач форензики под ОС Linux			+
Вес КМ:	25	35	40

$Общая часть/Для промежуточной аттестации$

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ОПК-2	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	Особенности решения задач форензики в Windows и Linux системах (Доклад) Windows ориентированные инструменты для решения задач форензики. (Домашнее задание) Linux-ориентированные инструменты для решения задач форензики (Контрольная работа)

		под ОС Windows и Linux	

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Особенности решения задач форензики в Windows и Linux системах

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия: Доклад
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Студент готовит доклад по выбранной теме и выступает с ним на семинаре (практическом занятии).

Краткое содержание задания:

На основе обзора интернет-источников по выбранной теме студент готовит доклад, 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 Linux-системах при решении задач форензики;

Контрольные вопросы/задания:

Знать: особенности решения основных задач форензики при исследовании информационных систем под управлением ОС типа Windows и Linux;	1. • Каковы особенности работы с файлами и дисками в ОС Windows при решении задач форензики? Каковы особенности работы с файлами и дисками в ОС Linux при решении задач форензики? Каковы особенности работы с приложениями ОС Windows при решении задач форензики? Каковы особенности работы с приложениями ОС Linux при решении задач форензики? Каковы особенности работы с памятью в Windows-системах при решении задач форензики? Каковы особенности работы с памятью в Linux-системах при решении задач форензики?
Уметь: практически использовать программные приложения под Windows и Linux при решении основных задач форензики;	1.Какова последовательность работы с файлами и дисками в ОС Windows при решении задач форензики? Какова последовательность работы с файлами и дисками в ОС Linux при решении задач форензики? Какова последовательность работы с приложениями ОС Windows при решении задач форензики? Какова последовательность работы с приложениями ОС Linux при решении задач форензики?

	Какова последовательность работы с памятью в Windows-системах при решении задач форензики? Какова последовательность работы с памятью в Linux-системах при решении задач форензики?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Доклад выполнен полно, правильно и непротиворечиво. Могут быть отдельные неточности

Оценка: не зачтено
Описание характеристики выполнения знания: Не выполнены требования на "зачтено".

КМ-2. Windows ориентированные инструменты для решения задач форензики.

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Домашнее задание
Вес контрольного мероприятия в БРС: 35
Процедура проведения контрольного мероприятия: Студент выполняет практическое задание по выбранной теме и представляет его преподавателю.

Краткое содержание задания:
Выполнить практическое задание по выбранной теме и представить его результаты преподавателю:
- Порядок практической работа с образами дисков с использованием утилиты Arsenal Image Mounter;
- Технология создания дампа физической памяти с использованием утилиты DumpIt;
- Последовательность создания доказательных файлов EnCase с использованием утилиты EnCase Forensic Imager;
- Порядок выявления зашифрованных томов TrueCrypt, PGP, Bitlocker с использованием утилиты Encrypted Disk Detector;
- Технология захвата веб-страниц для проведения расследований с использованием браузера Forensics Acquisition of Websites;
- Технология просмотра и клонирования носителей данных с использованием утилиты FTK Imager.

Контрольные вопросы/задания:

Знать: перечень программных приложений под Windows и Linux для решения основных задач форензики;	1.- Для чего предназначена утилита Arsenal Image Mounter? - Для чего используется утилита DumpIt? - Что такое файл EnCase? - Для чего используется утилит EnCase Forensic Imager; - Для чего осуществляется поиск зашифрованных томов TrueCrypt, PGP, Bitlocker? • - Для чего используется утилита Encrypted Disk Detector? - Для чего необходим захвата веб-страниц для проведения расследований? • - Для чего используется браузер Forensics Acquisition of Websites; - Что такое клонирование и для чего используется в форензике?

	• - Для чего используется утилита FTK Imager?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Практическое задание выполнено полно, технически правильно. Могут иметь место отдельные неточности.

Оценка: не зачтено
Описание характеристики выполнения знания: Не выполнены требования на "зачтено"

КМ-3. Linux-ориентированные инструменты для решения задач форензики

Формы реализации: Защита задания
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 40
Процедура проведения контрольного мероприятия: Индивидуальное задание выполняется студентами в соответствии с выбранной темой и предполагает защиту его результатов в виде контрольной работы.

Краткое содержание задания:
Утилита Guymager - бесплатный криминалистический "тепловизор" с функционалом цветовой идентификации событий безопасности. Описать назначение, основные возможности, приемы работы и результативность;
ProDiscover - утилита для захвата и анализа дисков. Описать назначение, основные возможности, приемы работы и результативность;
SIFT Workstation программы с открытым исходным кодом для служб реагирования на инциденты и проведения криминалистической цифровой экспертизы в различных условиях. Описать назначение, основные возможности, приемы работы и результативность;

Контрольные вопросы/задания:

Уметь: правильно интерпретировать результаты исследования (задач форензики), полученные с использованием программных приложений под ОС Windows и Linux	1.Для чего предназначена утилита ProDiscover? Каковы функции утилиты ProDiscover? Каковы подходы к анализу содержимого дисков? Каковы основные возможности утилиты ProDiscover? Как определить результативность утилиты ProDiscover?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: На вопросы даны полные и исчерпывающие ответы. Могут иметь место отдельные неточности.

Оценка: не зачтено
Описание характеристики выполнения знания: Не выполнены требования на оценку "зачтено"

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

4 семестр

Форма промежуточной аттестации: Зачет

Пример билета

1. Перечислите основные задачи форензики и раскройте их сущность.
2. Опишите порядок создания дампа физической памяти компьютера, для каких задач это делается и с помощью каких утилит.

Процедура проведения

Зачет проводится в письменном виде по билетам в течение 40 минут

I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины

1. Компетенция/Индикатор: ИД-2$_{ОПК-2}$ Применяет программно-аппаратные средства и средства системного назначения, инструментальные средства, в том числе отечественного производства для решения профессиональных задач

Вопросы, задания

1.

1. Перечислите наиболее популярные бесплатные утилиты для решения решения задач форензики и дайте их описание
2. Опишите технологию работы утилит для работы с образами дисков
3. Опишите порядок создания дампа физической памяти компьютера, для каких задач это делается и с помощью каких утилит
4. EnCase файлы - что это такое, порядок получения (создания), какие утилиты для этого предназначены
5. Порядок поиска доказательств (цифровых артефактов) в случае шифрованных томов (дисков, файлов), как в этом случае поступают, какие утилиты могут помочь и как?
6. Технология захвата веб-страниц для проведения расследований: с помощью какого веб-браузера можно выполнить и каким образом использовать;
7. Просмотр и клонирование носителей данных в среде Windows: утилита FTK Imager, основные возможности.

Материалы для проверки остаточных знаний

1.Перечислите основные задачи форензики

Ответы:

Все задачи форензики должны быть перечислены в принятой терминологии и уровнем подробности

Верный ответ: Форензика решает следующие задачи: - разработка тактики оперативно-розыскных мероприятий (ОРМ) и следственных действий, связанных с компьютерной информацией; - создание методов, аппаратных и программных инструментов для сбора и исследования доказательств компьютерных преступлений; - установление криминалистических характеристик правонарушений, связанных с компьютерной информацией.

II. Описание шкалы оценивания

Оценка: зачтено
Описание характеристики выполнения знания: На вопросы даны полные и правильные ответы. Могут иметь место отдельные неточности

Оценка: не зачтено
Описание характеристики выполнения знания: Не выполнены требования на оценку "зачтено"

III. Правила выставления итоговой оценки по курсу

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