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
Основы 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-3 Применяет программные средства прикладного назначения, в том числе отечественного производства для решения профессиональных задач

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Общая характеристика типовых киберпреступлений (Реферат)

Форма реализации: Выступление (доклад)

1. Изучение понятия, целей, методов, предмета, задач и сферы применения форензики (Семинар)

Форма реализации: Письменная работа

1. Организация оперативно-розыскных мероприятий методами форензики (Контрольная работа)

БРС дисциплины

3 семестр

Раздел дисциплины	Веса контрольных мероприятий, %			
	Индекс КМ:	КМ-1	КМ-2	КМ-3
	Срок КМ:	5	10	15
Введение в форензику				
Понятие, цель, методы, предмет, задачи и сфера применения форензики		+		
Система обеспечения форензики		+		
Типовые киберпреступления: общая характеристика, способ реализации, преступник и потерпевший, следы преступления.				
Общая характеристика типовых киберпреступлений			+	
Общая характеристика криминалистического процесса и анализ его этапов.				+

Организация оперативно-розыскных мероприятий методами форензики.			
Технология исследования трафика	+		
Информативность, значение, технология исследования содержания лог-файлов (логов)		+	
Общая характеристика следственных действий методами форензики	+		
Вес КМ:	30	30	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-З$_{ОПК-2}$ Применяет программные средства прикладного назначения, в том числе отечественного производства для решения профессиональных задач	Знать: технологию и этапы цифрового криминалистического процесса; актуальность, перечень и механизм реализации типовых киберпреступлений; Уметь: выполнять практические мероприятия по расследованию киберпреступлений и компьютерных инцидентов; правильно фиксировать цифровые "следы" киберпреступлений и компьютерных инцидентов.	Изучение понятия, целей, методов, предмета, задач и сферы применения форензики (Семинар) Общая характеристика типовых киберпреступлений (Реферат) Организация оперативно-розыскных мероприятий методами форензики (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Изучение понятия, целей, методов, предмета, задач и сферы применения форензики

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия: Семинар
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Проводится на семинарском занятии (круглом столе) в виде индивидуального выступления студента с последующим обсуждением в учебной группе

Краткое содержание задания:
Раскрыть сущность форензики, как прикладной науки: понятие, методы, предмет, задачи и сферы применения.

Контрольные вопросы/задания:

Уметь: выполнять практические мероприятия по расследованию киберпреступлений и компьютерных инцидентов;	1.Особенности добывания цифровых доказательств компьютерных инцидентов и киберпреступлений.
Уметь: правильно фиксировать цифровые "следы" киберпреступлений и компьютерных инцидентов.	1.Формы компьютерной криминалистики

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: На вопрос дан правильный и непротиворечивый ответ. Допустимы отдельные неточности.

Оценка: не зачтено
Описание характеристики выполнения знания: На вопрос дан неправильный ответ.

КМ-2. Общая характеристика типовых киберпреступлений

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Реферат
Вес контрольного мероприятия в БРС: 30
Процедура проведения контрольного мероприятия: Задание выполняется в форме реферата по выбранной (определенной преподавателем) теме из перечня тем

Краткое содержание задания:
Студент проводит обзор литературных источников по выбранной теме, комплексно освещает вопрос в соответствии с темой реферата, готовит презентацию для выступления.
Темы реферата:
1. Общая характеристика on-line мошенничества: способ, обстановка, преступник, потерпевший, следы;
2. Общая характеристика экстремистских действий в сети: способ, обстановка,

преступник, потерпевший, следы;
3. Общая характеристика DoS и DDoS атаки: способ, обстановка, преступник, потерпевший, следы;
4. Общая характеристика дефейса: способ, обстановка, преступник, потерпевший, следы;
5. Общая характеристика распространения вредоносного кода: способ, обстановка, преступник, потерпевший,
следы;
6. Общая характеристика кардерства: способ, обстановка, преступник, потерпевший, следы;
7. Общая характеристика мошенничества с трафиком: способ, обстановка, преступник, потерпевший, следы;
8. Общая характеристика нарушения авторских прав в офлайне: способ, преступник, потерпевший,
следы;
9. Общая характеристика нарушения авторских прав в сети: способ, преступник, потерпевший,
следы;
10. Общая характеристика фишинга: способ, преступник, потерпевший;
11. Общая характеристика кибersквоттинга;
12. Общая характеристика терроризма и кибервойн: сценарии, методы реализации и противодействие.

Контрольные вопросы/задания:

Знать: актуальность, перечень и механизм реализации типовых киберпреступлений;	1.Что такое способ совершения киберпреступления? 2.Что является обстановкой при совершении киберпреступления? 3.Что может относиться к следам киберпреступления?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Реферат написан полно, понятным языком, источники информации указаны корректно.

Оценка: не зачтено
Описание характеристики выполнения знания: Реферат содержит неправильную и некорректную информацию, нет ссылок на источники.

КМ-3. Организация оперативно-розыскных мероприятий методами форензики

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 40
Процедура проведения контрольного мероприятия: Выполняется в виде контрольной письменной работы по индивидуальному заданию для каждого студента.

Краткое содержание задания:
Организация оперативно-розыскных мероприятий методами форензики;

1. 1. Порядок организации перехвата трафика.
2. 2. Порядок исследования трафика. Данные трафика,
3. 3. Исследование статистики трафика с использованием специального программного обеспечения.

4. 4. Исследование лог-файлов, их содержание, представляющее интерес при расследовании киберпреступлений.
5. 5. Исследование лог-файлов веб-серверов.
6. 6. Исследование лог-файлов мейл-серверов.
7. 7. Исследование системных логов Windows-систем.
8. 8. Исследование системных логов Linux-систем.
9. 9. Исследование заголовков и содержания электронной почты.
10. 10. Установление принадлежности и местоположения IP-адреса.
11. 11. Порядок трассировки IP-адреса.
12. 12. Установление принадлежности доменного имени.
13. 13. Установление принадлежности адреса электронной почты.

Контрольные вопросы/задания:

Знать: технологию и этапы цифрового криминалистического процесса;	1.В чем заключается ценность информации о трафике в интересах оперативно-розыскных мероприятий?

Описание шкалы оценивания:

Оценка: зачтено
Описание характеристики выполнения знания: Работа написана полно, определения и формулировки четкие, есть ссылки на используемые источники информации. Допускаются отдельные неточности.

Оценка: не зачтено
Описание характеристики выполнения знания: Работа написана неполно, определения и формулировки отсутствуют или не корректны, ссылки на используемые источники информации не сделаны.

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

3 семестр

Форма промежуточной аттестации: Зачет

Пример билета

БИЛЕТ №____
Вопрос 1. Дайте понятие и перечислите цели, методы, предмет, задачи и сферы применения форензики.
Вопрос 2. *Системные логи Windows-систем: ценность информации логов, порядок извлечения и анализа.*
Задание 3 (практический). На основе анализа информации о сетевых соединениях сделайте вывод о состоянии и работе компьютера с IP-адресом 10.0.4.224.

bash-2.05b$ sudo tcpdump -i fxp0 -n 'tcp and (net 64.12.0.0/16 or net 205.188.0.0/16)'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode listening on fxp0, link-type EN10MB (Ethernet), capture size 96 bytes
15:53:53.968123 IP 205.188.165.249.80 > 10.0.4.224.1728: . ack 2482877808 win 16384
15:53:54.462314 IP 205.188.165.249.80 > 10.0.4.224.1728: P 0:1122(1122) ack 1 win 16384
15:53:54.514242 IP 10.0.4.224.1728 > 205.188.165.249.80: P 1:617(616) ack 1122 win 64413
15:53:54.521192 IP 10.0.4.224.1729 > 205.188.165.249.80: S 3173139757:3173139757(0) win 65535 <mss 1460,nop,nop,sackOK>
15:53:54.866705 IP 205.188.165.249.80 > 10.0.4.224.1729: S 1561008869:1561008869(0) ack 3173139758 win 16384 <mss 1360>
15:53:54.866882 IP 10.0.4.224.1729 > 205.188.165.249.80: . ack 1 win 65535
15:53:54.867122 IP 10.0.4.224.1729 > 205.188.165.249.80: P 1:261(260) ack 1 win 65535
15:53:55.252895 IP 205.188.165.249.80 > 10.0.4.224.1728: . 1122:2482(1360) ack 617 win 16384
15:53:55.259856 IP 205.188.165.249.80 > 10.0.4.224.1728: . 2482:3842(1360) ack 617 win 16384
15:53:55.260369 IP 10.0.4.224.1728 > 205.188.165.249.80: . ack 3842 win 65535

Процедура проведения

Выполняется по билетам в письменном виде в течение 50 минут. Для выполнения задания 3 используется ПК.

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

1. Компетенция/Индикатор: ИД-З$_{ОПК-2}$ Применяет программные средства прикладного назначения, в том числе отечественного производства для решения профессиональных задач

Вопросы, задания
1.БИЛЕТ №____
Вопрос 1. Кардерство: понятие, способы совершения, варианты реализации, причины отнесения к мошенничеству.
Вопрос 2. Порядок установления принадлежности и расположения Программные средства и порядок трассировки IP-адреса.

Задание 3 (практический). На основе анализа фрагмента системной информации определить владельца доменного имени «internet-law.ru».

$>whois -c ru internet-law.ru
% By submitting a query to RIPN's Whois Service
% you agree to abide by the following terms of use:
% http://www.ripn.net/about/servpol.html#3.2 (in Russian)
% http://www.ripn.net/about/en/servpol.html#3.2 (in English).
domain: INTERNET-LAW.RU
type: CORPORATE
nserver: ns.masterhost.ru.
nserver: ns1.masterhost.ru.
nserver: ns2.masterhost.ru.
state: REGISTERED, DELEGATED
org: ANO "Internet & Law"
phone: +7 495 7860130
e-mail: mail@internet-law.ru
registrar: RUCENTER-REG-RIPN
created: 2001.10.30
paid-till: 2007.10.30 source: TC-RIPN
Last updated on 2006.12.16 14:02:58 MSK/MSD

Материалы для проверки остаточных знаний

1.На каких уровнях системы OSI может быть реализован перехват трафика:

Ответы:

Выбрать правильный ответ: 1. Физическом; 2. Канальном; 3. Сетевом; 4. Сеансовом 5; Прикладном 6. 1 - 4; 7. 1-3, 5

Верный ответ: 7. 1-3, 5

2.Какие типы логов имеются в Windows-системах?

Ответы:

Выбрать правильный ответ: 1. Безопасности; 2. Системные; 3. Приложений; 4. 1-3; 5. 1,2.

Верный ответ: 4. 1-3

II. Описание шкалы оценивания

Оценка: зачтено
Описание характеристики выполнения знания: Выбраны правильные ответы не менее чем на 70% вопросов

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

III. Правила выставления итоговой оценки по курсу

На основе оценок "зачет" по всем практическим заданиям и оценки "зачет" на зачете по дисциплине.