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
Технологии обнаружения уязвимостей в автоматизированных системах

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

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

1. Контрольное мероприятие № 1 (Контрольная работа)
2. Контрольное мероприятие № 2 (Контрольная работа)
3. Контрольное мероприятие № 3 (Контрольная работа)
4. Контрольное мероприятие № 3 (Контрольная работа)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	14
Подготовительный этап исследования автоматизированной системы на наличие уязвимостей информационной безопасности					
Порядок сбора данных об уязвимостях автоматизированных систем и создания триаж-копий		+	+		
Анализ артефактов журналов событий, реестра и файловой системы		+	+		
Подходы к анализу вредоносного кода в процессе обратной разработки		+	+		
Динамический и статический анализ вредоносного кода, используемый специалистами по информационной безопасности		+	+		
Особенности анализа и толкования информации из открытых источников с целью формулирования гипотез и выявления деятельность злоумышленников		+	+		
Порядок идентификации следов инцидентов ИБ в журналах событий Windows.		+	+		

Обзор средств защиты ядра Linux	+	+		
Порядок обнаружения уязвимостей в автоматизированных системах и подходы к их устранению				
Оценка уровня защищенности наиболее распространённых операционных систем			+	+
Общая характеристика уязвимостей системного программного обеспечения операционных систем			+	+
Программные решения для обнаружения уязвимостей в операционных системах			+	+
Перечень наиболее опасных слабых мест программного обеспечения по данным CWE			+	+
Изучение подхода к эксплуатации уязвимостей Stack Buffer Overflow и UAF.			+	+
Методы и алгоритмы управления задачами, процессами, памятью и внешними устройствами			+	+
Комплексный подход к выбору технологий обнаружения уязвимостей в автоматизированных системах			+	+
Вес КМ:	25	25	25	25

$Общая часть/Для промежуточной аттестации$

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: типовые уязвимости операционных систем и прикладных программных продуктов критерии выбора и порядок применений технологий обнаружения уязвимостей в автоматизированных системах	Контрольное мероприятие № 1 (Контрольная работа) Контрольное мероприятие № 2 (Контрольная работа) Контрольное мероприятие № 3 (Контрольная работа) Контрольное мероприятие № 3 (Контрольная работа)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Контрольное мероприятие № 1

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия на бланке задания

Краткое содержание задания:
Дать письменный ответ на вопросы в соответствии с вариантов

Контрольные вопросы/задания:

Знать: критерии выбора и порядок применений технологий обнаружения уязвимостей в автоматизированных системах	1.

Контрольное мероприятие № 1 по дисциплине		
Программно-аппаратные средства защиты информации		
Студента:		группы №
№ п/п	1 Вариант	2 Вариант
1	Дайте характеристику триаж-копий, применяемых специалистами в области ИБ для описания атаки	Приведите классификацию этапов сбора данных об уязвимости типовой автоматизированной системы на базе ОС Windows
2	Перечислите программные продукты и варианты самописных скриптов для сбора исходных данных об уязвимостях АС	Назовите исходные данные, получаемые об уязвимости АС из журнала событий, реестра и файловой системы

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-2. Контрольное мероприятие № 2

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия на бланке задания

Краткое содержание задания:
Дать письменный ответ на вопросы в соответствии с вариантов

Контрольные вопросы/задания:

Знать: критерии выбора и порядок применений технологий обнаружения уязвимостей в автоматизированных системах	1.

Контрольное мероприятие № 2 по дисциплине		
Программно-аппаратные средства защиты информации		
Студента:		группы №
№ п/п	1 Вариант	2 Вариант
1	Дайте характеристику динамического анализа вредоносного кода, применяемого в процессе обратной разработки	Дайте характеристику статистического анализа вредоносного кода, применяемого в процессе обратной разработки
2	Назовите ключевые отличия динамического и статистического анализа кода	Перечислите программные продукты, применяемые специалистами по ИБ для динамического и статистического анализа кода

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-3. Контрольное мероприятие № 3

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия на бланке задания

Краткое содержание задания:
Дать письменный ответ на вопросы в соответствии с вариантов

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: типовые уязвимости операционных систем и прикладных программных продуктов</td>
<td>1.
<table>
<tr><td colspan="3">Контрольное мероприятие № 3 по дисциплине</td></tr>
<tr><td colspan="3">Программно-аппаратные средства защиты информации</td></tr>
<tr><td colspan="2">Студента:</td><td>группы №</td></tr>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
<tr><td>1</td><td>Каков порядок идентификации следов инцидентов ИБ в журналах событий Windows?</td><td>Какие встроенные в ОС Windows инструменты для анализа уязвимостей в АС Вам известны?</td></tr>
<tr><td>2</td><td>Перечислите встроенные в ОС Linux инструменты для анализа уязвимостей в АС</td><td>Перечислите встроенные в ядро Linux средства защиты</td></tr>
</table>
</td>
</tr>
</table>

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

КМ-4. Контрольное мероприятие № 3

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия на бланке задания

Краткое содержание задания:
Дать письменный ответ на вопросы в соответствии с вариантов

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: типовые уязвимости операционных систем и прикладных программных продуктов</td>
<td>1.
<table>
<tr><td colspan="3">Контрольное мероприятие № 4 по дисциплине</td></tr>
<tr><td colspan="3">Программно-аппаратные средства защиты информации</td></tr>
<tr><td colspan="2">Студента:</td><td>группы №</td></tr>
<tr><td>№ п/п</td><td>1 Вариант</td><td>2 Вариант</td></tr>
</table>
</td>
</tr>
</table>

		1	Назовите наиболее опасные слабые мест программного обеспечения по данным CWE	Охарактеризуйте структуру базы данных уязвимостей CWE с точки зрения её применения специалистами по ИБ
		2	Укажите взаимосвязь уязвимостей в программном коде прикладных программных продуктов и системного программного обеспечения нижних уровней ОС	Приведите перечень программных решений, применяемых для обнаружения уязвимостей в АС, по виду ОС и критерию эффективности

Описание шкалы оценивания:

Оценка: 5
Нижний порог выполнения задания в процентах: 70
Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

Оценка: 4
Нижний порог выполнения задания в процентах: 60
Описание характеристики выполнения знания: Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

Оценка: 3
Нижний порог выполнения задания в процентах: 50
Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Зачет

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра *Безопасности и информационных технологий* Дисциплина «Технологии обнаружения уязвимостей в автоматизированных системах»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю.Невский* *Протокол кафедры* *№ ___* *«___»декабря* *20___г.*
1. Порядок проведению обратной разработки вредоносного кода на примере АС на базе ОС Windows 2. Динамический и статический анализ вредоносного кода, используемый специалистами по информационной безопасности 3. Основные программные инструменты Threat Intelligence и Threat hunting для обнаружения уязвимостей ОС		

Процедура проведения

Устный зачёт по билетам с учётом результатов по контрольным неделям

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.Поясните, почему Threat Intelligence — это не киберразведка, но часто называется так?
2.Какой из четырёх уровней Threat Intelligence чаще других выбирают российские предприятия?
3.Какие наборы потоков материала (фидов) необходимо использовать для выявления киберинцидентов?
4.Как осуществляется управление фидами и как их применяют совместно со средствами защиты информации?
5.Как часто индикаторы Threat Intelligence дают ложные срабатывания и как с этим борются специалисты ИБ?
6.Какой уровень зрелости в ИБ нужен компании для корректного внедрения Threat Intelligence в СОИБ?

Материалы для проверки остаточных знаний

1.Дайте определение термина “Threat Intelligence”

Ответы:

Для ответа на вопрос рекомендуется воспользоваться материалами лекции № 2

Верный ответ: Дословный перевод термина Threat Intelligence — «знания об угрозах». hreat Intelligence — это вся информация, которая даёт возможность понять

угрозу. Это могут быть как низкоуровневые данные (хеш, IP-адрес), так и данные о конкретном злоумышленнике, заинтересованном в атаке на целевую систему.

2.Зачем компании нужен Threat Intelligence, если у неё есть другие системы безопасности и сбора данных, такие как IDS, NGFW, SIEM и другие?

Ответы:

Для ответа на вопрос рекомендуется воспользоваться материалами лекции № 4

Верный ответ: Threat Intelligence может увязать всю картину безопасности воедино и отойти от атомарности отдельных решений или вендоров. Особенно это важно для компаний, которые практикуют Threat Response. Кроме того, при помощи методов кибербразведки компания может получить информацию об угрозах за периметром безопасности, которые пока не детектированы инструментами защиты. Ещё один важный момент — многие ИБ-решения имеют «слепые зоны», которыми могут воспользоваться злоумышленники. Threat Intelligence позволяет закрывать эти пробелы.

3.Для каких целей на техническом уровне применяется Threat Intelligence?

Ответы:

Для ответа на вопрос рекомендуется воспользоваться материалами лекции № 5

Верный ответ: На техническом уровне Threat Intelligence применяется для: реагирования на инциденты, проактивного поиска угроз (Threat Hunting), мониторинга безопасности, анализа вредоносного кода, обнаружения вторжений. На стратегическом уровне кибербразведка способна помочь в принятии решений топ-менеджменту компании.

4.Каковы критерии выбора источников для Threat Intelligence в типовой организации?

Ответы:

Для ответа на вопрос рекомендуется воспользоваться материалами лекции № 6

Верный ответ: Критерии выбора источников для Threat Intelligence могут быть следующими: возможности автоматизации, интеграция и интероперабельность, частота обновлений, обогащение метаданными, рейтинг сложности, покрытие, видимость даркнета, аккуратность в геолокации, число и спектр источников, качество.

II. Описание шкалы оценивания

Оценка: 5

Нижний порог выполнения задания в процентах: 70

Описание характеристики выполнения знания: Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

Оценка: 4

Нижний порог выполнения задания в процентах: 60

Описание характеристики выполнения знания: Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

Оценка: 3

Нижний порог выполнения задания в процентах: 50

Описание характеристики выполнения знания: Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

III. Правила выставления итоговой оценки по курсу

Оценка проставляется по результатам ответа на вопрос билета. Результаты контрольных мероприятий № 1, 2, 3, 4 учитываются.