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

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Оценочные материалы
по дисциплине
Технологии защиты информационных систем от кибератак

Москва
2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Дратвяк А.В. Идентификатор: R1a0ecc29-DratviakAV-b9b11303	А.В. Дратвяк
(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. ПК-7 способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений

2. ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации

3. ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

4. ПСК-1 Способность администрировать подсистемы информационной безопасности объектов, объекты энергетики КВО РФ, эксплуатирующие АСУ ТП

5. ПСК-2 Способность применять программные средства системного и специального назначения, в том числе для обеспечения безопасносго функционирования объектов энергетики с элементами АСУ ТП

6. ПСК-3 Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности в том числе и на объектах энергетики, эксплуатирующих АСУ ТП

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 № 4 (Контрольная работа)
5. Контрольное мероприятие № 5 (Контрольная работа)
6. Контрольное мероприятие № 6 (Контрольная работа)
7. Контрольное мероприятие № 7 (Контрольная работа)
8. Контрольное мероприятие № 8 (Контрольная работа)

БРС дисциплины

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %							
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8
	Срок КМ:	2	4	6	8	10	12	14	16
Основы защиты информационных систем от кибератак								
Введение в защиту от кибератак	+							
Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах	+							
Структура кибератаки на информационную систему объекта информатизации								
Атаки на корпоративные информационные системы компаний (КИС)		+						
Атаки на промышленные предприятия (АСУ ТП)		+						
Обнаружение атак на ИС			+		+			
Атаки на ИС. DoS/DDoS			+		+			
Атаки на ИС. Социальная инженерия				+		+		
Структура кибератаки на веб-приложения и ресурсы сети "Интернет"								
Выявление и эксплуатация SQL-инъекций в приложениях								+
Защита веб-приложений от инъекций команд								+
Защита веб-приложений от атак типа XSS				+		+		
Меры предотвращения stored и reflected XSS. CSRF. SSRF.							+	
Применение подхода DevSecOps в современных системах разработки программного обеспечения							+	
Вес КМ:	10	10	15	15	15	15	10	10

$Общая часть/Для промежуточной аттестации$

БРС курсовой работы/проекта

6 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Титульный лист		+			

Содержание	+	+		
Введение		+		
Первый раздел			+	
Второй раздел			+	
Заключение				+
Список использованной литературы				+
Вес КМ:	25	25	25	25

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
ПК-7	ПК-7(Компетенция)	Знать: типовые алгоритмы атаки и механизмы защиты от кибератак на информационные системы Уметь: анализировать исходные данные для проектирования систем обеспечения информационной безопасности объектов информатизации от киберугроз	Контрольное мероприятие № 1 (Контрольная работа)
ПК-12	ПК-12(Компетенция)	Знать: программные и программно-аппаратные средства защиты компьютерных систем от кибератак Уметь: разрабатывать рекомендации по применению программных и программно-аппаратных	Контрольное мероприятие № 2 (Контрольная работа)

		решений для защиты системных и прикладных программных продуктов, а также web-приложений и ресурсов сети "Интернет" от киберугроз	
ПК-13	ПК-13(Компетенция)	Знать: порядок проектирования систем обеспечения информационной безопасности от киберугроз Уметь: проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей	Контрольное мероприятие № 3 (Контрольная работа) Контрольное мероприятие № 5 (Контрольная работа)
ПСК-1	ПСК-1(Компетенция)	Знать: особенности защиты автоматизированных систем управления технологическими процессами от киберугроз, в том числе объектов энергетики КВО РФ Уметь: администрировать компоненты системы информационной безопасности, включая	Контрольное мероприятие № 4 (Контрольная работа) Контрольное мероприятие № 6 (Контрольная работа)

		АСУ ТП объектов энергетики КВО РФ	
ПСК-2	ПСК-2(Компетенция)	Знать: классификацию киберугроз информационной безопасности в соответствии нормативными документами регуляторов Уметь: применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах	Контрольное мероприятие № 7 (Контрольная работа)
ПСК-3	ПСК-3(Компетенция)	Знать: типовые подходы к обеспечению комплексной защиты информации на объектах, эксплуатирующих АСУ ТП Уметь: формировать обоснованные рекомендации по применению комплексного подхода к информационной безопасности на объектах, эксплуатирующих АСУ	Контрольное мероприятие № 8 (Контрольная работа)

		ТП	

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: 10
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: типовые алгоритмы атаки и механизмы защиты от кибератак на информационные системы	1.**1 вариант** Что такое Command and Control server? Что такое Payload? Указать домен второго уровня из api.tiktok.com Дайте описание тактики "Initial Access" Что такое SSH? **2 вариант** Что такое "уязвимость"? Что такое exploit? Указать домен третьего уровня из api.tiktok.com Дайте описание тактики "Persistence" Что такое SSL/TLS?
Уметь: анализировать исходные данные для проектирования систем обеспечения информационной безопасности объектов информатизации от киберугроз	1.**1 вариант** Отфильтруйте матрицу Mittra по тактике атаки "Initial Access" **2 вариант** Отфильтруйте матрицу Mittra по тактике атаки "Persistence"

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: 10
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: программные и программно-аппаратные средства защиты компьютерных систем от кибератак	1.**1 вариант** Преимущества сканеров уязвимостей Перечень видов сетевых атак Средства ОБ ОС Суть средства защиты Air Gap Хар-ка "статического тестирования" ПО **2 вариант** Недостатки сканеров уязвимостей Перечень средства защиты от сетевых атак Средства ОБ приложений (App Sec) Суть средства защиты Honeypots Хар-ка "динамического тестирования" ПО
Уметь: разрабатывать рекомендации по применению программных и программно-аппаратных решений для защиты системных и прикладных программных продуктов, а также web-приложений и ресурсов сети "Интернет" от киберугроз	1.**1 вариант** Постройте mind-карту программных продуктов, применяемых для “статического тестирования” ПО **2 вариант** Постройте mind-карту программных продуктов, применяемых для “динамического тестирования” ПО

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: 15
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: порядок проектирования систем обеспечения информационной безопасности от киберугроз	1.**1 вариант** Команда для получения списка установленных пакетов Команда для получения содержимого файла Команда создания архива Что такое Persistence? Что такое Defense Evasion? **2 вариант** Как выглядит команда с флагами (опциями) Можно ли на сервисе CVE Details посмотреть ущерб для КЦД? Приведите пример идентификатора уязвимостей в базе данных CVE (из чего состоит идентификатор) Что такое Lateral Movement? Что такое Privilege Escalation?
Уметь: проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей	1.**1 вариант** Продемонстрируйте применение команды для получения содержимого файла в ОС Kali Linux **2 вариант** Продемонстрируйте применение команды для создания и распаковки архива в ОС Kali Linux

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 № 4

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: особенности защиты автоматизированных систем управления технологическими процессами от киберугроз, в том числе объектов энергетики КВО РФ	1.**1 вариант** Функциональные возможности NGFW Для чего нужен Burn Suite? Что можно делать с помощью Nmap? Три этапа типовой схемы атаки на АСУ ТП Схема работы DNS-over-HTTPS **2 вариант** Функциональные возможности IDS/IPS Для чего нужен WireShark? Что можно делать с помощью John the Ripper? Три типа моделей АСУ ТП Схема работы DNS-over-HTTPS
Уметь: администрировать компоненты системы информационной безопасности, включая АСУ ТП объектов энергетики КВО РФ	1.**1 вариант** Запустите и продемонстрируйте базовые возможности утилиты Nmap в ОС Kali Linux **2 вариант** Запустите и продемонстрируйте базовые возможности утилиты John the Ripper в ОС Kali Linux

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-5. Контрольное мероприятие № 5

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: порядок проектирования систем обеспечения информационной безопасности от киберугроз</td>
<td>1.Контрольное мероприятие по дисциплине "Технологии защиты информационных систем от кибератак"
<table>
<tr><th>№ п/п</th><th>1 Вариант</th><th>2 Вариант</th></tr>
<tr><td>1</td><td>Что такое и каковы причины возникновения SQL-инъекций?</td><td>Перечислите и раскройте суть техник, применяемых при эксплуатации SQL-инъекций.</td></tr>
<tr><td>2</td><td>Подробно раскройте что такое Blind SQL-инъекция.</td><td>Подробно раскройте что такое Time-Based SQL-инъекция.</td></tr>
<tr><td>3</td><td>Дайте определение ORM, поясните как данная технология используется в контексте кибербезопасности.</td><td>Для каких целей могут быть использованы команды chown и chmod?</td></tr>
<tr><td>4</td><td>Перечислите и поясните методы обнаружения внедрения опасных команд.</td><td>Перечислите и поясните методы предотвращения внедрения опасных команд.</td></tr>
<tr><td>5</td><td>Что такое XSS в контексте информационной безопасности? Раскройте сущность XSS на конкретных примерах.</td><td>Составьте классификацию XSS и раскройте суть каждого из элементов классификации.</td></tr>
</table>
</td>
</tr>
<tr>
<td>Уметь: проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей</td>
<td>1.
<table>
<tr><td>6</td><td>На примере стенда кафедры продемонстрировать реализацию обычной SQL-инъекции</td><td>На примере стенда кафедры продемонстрировать реализацию Blind SQL-инъекции</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-6. Контрольное мероприятие № 6

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

<table>
<tr>
<td>Знать: особенности защиты автоматизированных систем управления технологическими процессами от киберугроз, в том числе объектов энергетики КВО РФ</td>
<td>1.Контрольное мероприятие по дисциплине "Технологии защиты информационных систем от кибератак"
<table>
<tr><th>№ п/п</th><th>1 Вариант</th><th>2 Вариант</th></tr>
<tr><td>1</td><td>Приведите примеры реализации stored XSS атак</td><td>Приведите примеры реализации reflected XSS</td></tr>
<tr><td>2</td><td>Поясните в чём заключатеся отличие следующих видов XSS атак: stored, reflected и DOM-based</td><td>Раскройте суть понятия CSP, опишите порядок его включения и приведите пример её реализации.</td></tr>
<tr><td>3</td><td>Нарусуйте графическую схему атаки типа CSRF.</td><td>Нарусуйте графическую схему атаки типа SSRF.</td></tr>
<tr><td>4</td><td>Дайте характеристику методов защиты от CSRF. Дайте определение "токену" в контексте защиты от CSRF атаки. Опишите суть и порядок использования</td><td>Дайте характеристику методов защиты от CSRF. Дайте определение "токену" в контексте защиты от CSRF</td></tr>
</table>
</td>
</tr>
</table>

			Synchronizer Token и Double Submit Cookie	атаки. Опишите суть и порядок использования Encrypted Token и Same-Site Cookie
		5	Описать методы защиты от SSRF в ситуации "Приложение может отправлять запросы только идентифицированным и доверенным приложениям"	Описать методы защиты от SSRF в ситуации "Приложение может отправлять запросы на ЛЮБОЙ внешний IP-адрес или доменное имя"
Уметь: администрировать компоненты системы информационной безопасности, включая АСУ ТП объектов энергетики КВО РФ		1.		
		6	На примере стенда кафедры продемонстрировать реализацию CSRF атаки. Предложите практические рекомендации по противодействию атаке.	На примере стенда кафедры продемонстрировать реализацию SSRF атаки. Предложите практические рекомендации по противодействию атаке.

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-7. Контрольное мероприятие № 7

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: классификацию	1.Контрольное мероприятие по дисциплине

<table>
<tr>
<td>киберугроз информационной безопасности в соответствии нормативными документами регуляторов</td>
<td>"Технологии защиты информационных систем от кибератак"
<table>
<tr><th>№ п/п</th><th>1 Вариант</th><th>2 Вариант</th></tr>
<tr><td>1</td><td>Схематично изобразите жизненный цикл существования идентификатора сеанса веб-приложения. Дайте краткое описание каждому из этапов.</td><td>Какие критерии определяют срок действия сеанса в веб-приложениях, и какие механизмы автоматического истечения сеанса Вам известны?</td></tr>
<tr><td>2</td><td>Перечислите и кратко охарактеризуйте средства защиты, используемые для управления сеансом на стороне клиента.</td><td>Перечислите механизмы обнаружения сессионных атак на веб-приложения.</td></tr>
<tr><td>3</td><td>Раскройте варианты и суть реализации атаки типа "обход пути".</td><td>Опишите суть требований, предъявляемых к структуре и значению идентификатора сеанса в веб-приложениях.</td></tr>
<tr><td>4</td><td>Назовите и раскройте смысл защитных мер, применяемых для защиты от атак типа "обход пути".</td><td>Назовите различия в тестировании методом "чёрного" и "серого ящика" в контексте веб-безопасности.</td></tr>
<tr><td>5</td><td>Дайте определение безопасному и небезопасному перенаправлению/переадресации URL</td><td>Дайте характеристику мер предотвращения Open Redirect.</td></tr>
</table></td>
</tr>
<tr>
<td>Уметь: применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах</td>
<td>1.
<table>
<tr><td>6</td><td>В матрице MITRE ATT&CK отфильтровать техники атаки типа "обход пути". Определить вредоносные программные продукты, применяемые на данном этапе атаки</td><td>В матрице MITRE ATT&CK отфильтровать техники атаки типа "повышения привилегий". Определить вредоносные программные продукты, применяемые на данном этапе атаки</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-8. Контрольное мероприятие № 8

Формы реализации: Письменная работа
Тип контрольного мероприятия: Контрольная работа
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Письменный ответ на вопросы контрольного мероприятия, выполняемый на листах установленного администрацией формата

Краткое содержание задания:
Дайте письменный ответ на 6 вопросов.
Один из двух вариантов контрольного мероприятия выбирается по критерию:
нечётные номера по списку журнала БАСР - 1 вариант, чётные номера - 2 вариант.

Контрольные вопросы/задания:

Знать: типовые подходы к обеспечению комплексной защиты информации на объектах, эксплуатирующих АСУ ТП

1.Контрольное мероприятие по дисциплине "Технологии защиты информационных систем от кибератак"

№ п/п	1 Вариант	2 Вариант
1	Дайте определение и назовите суть применения JSON Web Token	Перечислите части токена JWT и раскройте их назначение в контексте информационной безопасности
2	Перечислите варианты хранения токенов веб-приложения. Назовите достоинства и недостатки этих способов.	Раскройте назначение FIDO и протоколов UAF и U2F. Конкретизируйте различия в работе протоколов.
3	Какой цели служит WebAuthn? Какие виды электронных ключей используются для WebAuthn?	Поясните принцип работы WebAuthn и особенности его применения для целей обеспечения информационной безопасности веб-приложений
4	Раскройте аббревиатуру MFA в	Перечислите варианты реализации технологии

<table>
<tr><td></td><td></td><td><table>
<tr><td></td><td>контексте безопасности веб-приложений. Перечислите основные достоинства и недостатки MFA.</td><td>MFA в веб-приложениях. Дайте характеристику безопасности применения указанных вариантов реализации.</td></tr>
<tr><td>5</td><td>Дайте определение понятию сериализация и десериализация. Что подразумевается под небезопасной сериализацией.</td><td>Раскройте суть концепции хеширования "соль и перец". Какой цели служит добавление "перца" при хешировании?</td></tr>
</table></td></tr>
<tr><td>Уметь: формировать обоснованные рекомендации по применению комплексного подхода к информационной безопасности на объектах, эксплуатирующих АСУ ТП</td><td>1.</td><td><table>
<tr><td>5</td><td>Сформируйте mind-карту уязвимостей веб-приложений (десктопных и мобильных) по критерию типа реализуемой атаки</td><td>Сформируйте mind-карту уязвимостей веб-сайта по критерию типа реализуемой атаки</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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

НИУ МЭИ	**ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1** Кафедра: *Безопасности и информационных технологий* Дисциплина: «Технологии защиты информационных систем от кибератак»	*Утверждаю:* *Зав. каф. БИТ* *А.Ю. Невский* *Протокол кафедры № 3* *«16» декабря 2020г.*
1. Ответственность за киберпреступления, предусмотренная законодательством РФ. 2. Понятие CIA в контексте сетевой безопасности корпоративных информационных систем. 3. В браузере открыть MITRE ATT&CK NAVIGATOR, создать новый уровень, выполнить фильтрацию техник атак по категориям кибергруппировок, а затем дать пояснение возможностям применения навигатора в профессиональной деятельности специалистов по информационной безопасности..		

Процедура проведения

Устный экзамен с практической письменной частью на листах установленного администрацией образца

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

1. Компетенция/Индикатор: ПК-7(Компетенция)

Вопросы, задания

1.Понятие CIA в контексте сетевой безопасности корпоративных информационных систем

2.Классификация видов сетевых атак по трём критериям: защищаемый объект, угроза и меры защиты

3.Сравнение функциональных возможностей и решаемых задач с помощью Firewall и NGFW в корпоративных системах

Материалы для проверки остаточных знаний

1.В чём состоит суть Stored XSS атаки?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 7

Верный ответ: Payload сохраняется в БД. Не требует специально созданного URL. Полезная нагрузка не видна для фильтра XSS браузера. Пользователи могут случайно активировать полезную нагрузку, если они посещают уязвимую страницу.

2.В чем отличие XSS в DOM-модели от других видов XSS?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 8

Верный ответ: При Stored и reflected XSS-атаках сервер вставляет вредоносный скрипт на страницу, которая затем пересылается в ответе к жертве. Когда браузер жертвы получил ответ, он предполагает, что вредоносный скрипт является частью

легитимного содержания страницы, и автоматически выполняет его во время загрузки страницы, как и любой другой сценарий.

3.Назовите 2 механизма управления сеансом, связанных с уязвимостью фиксации сессии

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 10

Верный ответ: Разрешающее управление сеансом - позволяет веб-приложению изначально принимать любое значение идентификатора сеанса, установленное пользователем как действительное, создавая для него новый сеанс. Строгое управление сеансом - позволяет веб-приложению изначально принимать только значения идентификатора сеанса, которые были ранее сгенерированы веб-приложением

2. Компетенция/Индикатор: ПК-12(Компетенция)

Вопросы, задания

1.Суть, варианты реализации и защиты от атаки типа ARP-spoofing, IP Spoofing, DHCP Spoofing и DNS Spoofing

2.Набор практик DevOps и DevSecOps в контексте разработки безопасных компьютерных приложений

3.Понятие и инструменты OSINT, используемые на различных этапах атак и тестирования защиты компьютерных систем

Материалы для проверки остаточных знаний

1.Что такое DOM tree?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 6

Верный ответ: В соответствии с объектной моделью документа («Document Object Model»), каждый HTML-тег является объектом. Вложенные теги являются «детьми» родительского элемента. Текст, который находится внутри тега, также является объектом. DOM — это независящий от платформы и языка программный интерфейс, позволяющий программам и скриптам получить доступ к содержимому HTML-, XHTML- и XML-документов, а также изменять содержимое, структуру и оформление таких документов.

2.Чем внедрение кода отличается от внедрения команд?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 6

Верный ответ: Внедрение кода - злоумышленник ограничен только функциональностью самого внедренного языка и среды выполнения. Внедрение команд - внедрение состоит из использования существующего кода для выполнения команд, обычно в контексте оболочки, как например bash.

3.Чем атаки типа межсайтовый скриптинг отличаются от инъекция кода?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 7

Верный ответ: Злоумышленник не атакует жертву напрямую, но использует уязвимость веб-сайта, который посещает жертва и внедряет вредоносный JavaScript код. В браузере жертвы вредоносный JavaScript отображается как легитимная часть веб-сайта, а сам веб-сайт выступает в качестве непосредственного соучастника атакующего.

3. Компетенция/Индикатор: ПК-13(Компетенция)

Вопросы, задания

1.Порядок работы с базой данных известных киберуязвимостей CVE и специализированными сервисами типа CVE Details

2.Рекомендации ФСБ о порядке реагирования на кибератаки в отношении критической информационной инфраструктуры

3.Суть и назначение JSON Web Token для целей обеспечения безопасности в процессе прохождения аутентификации в веб-приложениях

Материалы для проверки остаточных знаний

1.Назовите уровни информационной безопасности в АСУ ТП в соответствии с МЭК 62443

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 4

Верный ответ: Уровни безопасности в соответствии с рекомендациями МЭК 62433 можно разделить на: – Security Level 0 (No specific requirements or security protection necessary); определение уровня, для которого не нужны меры обеспечения ИБ, порождает некоторую неопределенность, поскольку непонятно, можно ли вообще отказаться от обеспечения ИБ; – Security Level 1 (Protection against casual or coincidental violation); защита от случайных или совпадающих нарушений ИБ обеспечивается, в первую очередь, процедурным путем; – Security Level 3 (Protection against intentional violation using sophisticated means with moderate resources, ICS specific skills and moderate motivation); на данном уровне необходимо обеспечить защиту от злоумышленников, обладающих достаточными знаниями и ресурсами, чтобы совершить атаку на целевую систему – Security Level 4 (Protection against intentional violation using sophisticated means with extended resources, ICS specific skills and high motivation); данный уровень отличается от предыдущего тем, что здесь злоумышленник привлекает значительные ресурсы, например, организованная группа может использовать кластер компьютеров с высокой вычислительной мощностью на продолжении длительного времени

2.Назовите 4 метода обнаружения атак на информационные системы на базе АСУ ТП

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 4

Верный ответ: Методы обнаружения атак: - Сопоставление с образцом - Статистическая аномалия - Метрическая модель - Сигнатурный и эвристический анализ

3.Перечислите компоненты гибридной системы IDS

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 4

Верный ответ: Компоненты гибридной системы: - Предпроцессор данных - Алгоритм обнаружения - Фильтр оповещений - Алгоритм обнаружения - Фильтр оповещений

4. Компетенция/Индикатор: ПСК-1(Компетенция)

Вопросы, задания

1.Понятие, структура и этапы компьютерной атаки на информационную систему предприятия

2.Классификация уязвимостей компьютерных систем на основе матрицы MITRE ATT&CK

3.Задачи и функции "красной", "синей" и "фиолетовой" команд аудита информационной безопасности компьютерных систем

Материалы для проверки остаточных знаний

1.Какие задачи решают сетевые сканеры угроз в контексте защиты от кибератак на АС?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 2

Верный ответ: Сетевые сканеры направлены на решение задач: • идентификация и анализ уязвимостей; • инвентаризация ресурсов: ОС, ПО и устройства сети; • формирование отчетов, содержащих описание уязвимостей и варианты их устранения.

2.Какие механизмы используют сканеры уязвимости сети для обнаружения признаков кибератак?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 2

Верный ответ: Сканеры уязвимостей сети используют механизмы: - Зондирование — не слишком оперативен, но точен. Механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. - Сканирование — более быстрый, но менее точный. Механизм пассивного анализа, при котором сканируются уязвимости без подтверждения ее наличия, используя косвенные признаки (определяются открытые порты, собираются заголовки для сравнения с таблицей правил)

3.Раскройте суть средства защиты типа Honeypots

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 3

Верный ответ: Honeypot - программно реализованная ловушка, которая имитирует серверы организации и анализирует обращения пользователей к имитируемым ресурсам. Анализируя входящий трафик ловушки, можно: - выяснить местонахождение киберпреступников; - оценить степень угрозы; - изучить методы злоумышленников; - узнать, какие данные или приложения их интересуют; - оценить эффективность используемых мер защиты от кибератак.

5. Компетенция/Индикатор: ПСК-2(Компетенция)

Вопросы, задания

1.Ответственность за киберпреступления, предусмотренная законодательством РФ

2.Техники атаки на компьютерную систему категории Reconnaissance в соответствии с матрицей MITRE ATT&CK

3.Характеристика базы данных CVE и банка данных угроз безопасности информации ФСТЭК России

Материалы для проверки остаточных знаний

1.Опишите типовой алгоритм работы сетевых сканеров в процессе обнаружения угроз безопасности веб-ресурсов компании

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 2

Верный ответ: Алгоритм работы сканеров: 1) Проверка заголовков. Например, проверяя FTP-сервер, сканер узнает версию обеспечения и на основе этой информации сообщает о возможных уязвимостях. Это оптимальное решение, не приводящее к нарушению работы сети. 2) Активные зондирующие проверки (active probing check). Проверяется не версия ПО, а сравнивается «цифровой слепок» фрагмента программы со «слепком» уязвимости (сигнатура). 3) Имитация атак (exploit check) – это зондирование, которое эксплуатирует дефекты в ПО. Подается «импульс» некоторым уязвимостям, но вероятна ситуация, когда даже имитируемая атака просто отключит проверяемый узел сети.

2.Что включает в себя Информационно-технологическая архитектура КИС?

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 3

Верный ответ: Компоненты ИТА КИС: 1. аппаратно-программную платформу реализации КИС; 2. организационную форму БД; 3. архитектуру и топологию компьютерной сети; 4. средства телекоммуникации; 5. комплекс технических средств обработки данных

3.Дайте описание сетевой атаки типа DHCP Spoofing

Ответы:

Для корректного ответа на вопрос рекомендуется обратиться к содержанию лекции № 3

Верный ответ: DHCP Spoofing - злоумышленник настраивает в сети ненастоящий DHCP-сервер, чтобы выдавать для клиентов DHCP-адреса. Цель атаки — заставить клиентов использовать ложную службу доменных имен (DNS) и Windows-службу имён Internet (сервер WINS), а также использовать узел или устройство злоумышленника в качестве шлюза по умолчанию.

6. Компетенция/Индикатор: ПСК-3(Компетенция)

Вопросы, задания

1.Характеристика открытого проекта обеспечения безопасности веб-приложений OWASP и инструмента OWASP Cheat Sheet Series

2.Базовая модель кибернарушителя информационной безопасности компьютерной системы. Его квалификация и применяемые инструменты.

3.Виды сканеров безопасности и их способы применения для реализации кибератак на компьютерные системы

Материалы для проверки остаточных знаний

1.Что из себя представляет и для каких целей используется матрица Mitre Att&ck?

Ответы:

Для получения корректного ответа на вопрос рекомендуется использовать одноимённый с матрицей интернет-портал

Верный ответ: Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge — «тактики, техники и общеизвестные факты о злоумышленниках») — основанная на реальных наблюдениях база знаний компании Mitre, содержащая описание тактик, приемов и методов, используемых киберпреступниками. Матрицы Mitre Att&ck объединены в четыре группы: - PRE-ATT&CK — тактики и техники, которые злоумышленники используют на этапе подготовки к кибератаке. - Enterprise — тактики и техники, которые злоумышленники применяют в ходе атаки на предприятия. В этой группе доступна как сводная матрица, так и отдельные матрицы, содержащие тактики и техники кибератак на конкретные операционные системы и облачные сервисы. - Mobile — тактики и техники, которые злоумышленники используют в ходе атаки на мобильные устройства под управлением iOS и Android. - ATT&CK for ICS — тактики и техники, которые используются в атаках на промышленные системы управления. Специалисты по информационной безопасности используют матрицы Mitre Att&ck для решения следующих задач: 1. Анализ существующей защиты на предмет соответствия реальным угрозам и повышение безопасности инфраструктуры компании. С помощью матриц Mitre Att&ck можно определить, к каким техникам уязвимы ресурсы организации, чтобы в перспективе устранить самые критичные проблемы. 2. Своевременное реагирование на инциденты. С помощью матриц Mitre Att&ck можно установить, на каком этапе развития находится атака и какие меры необходимо принять в первую очередь. 3. Расследование киберинцидентов. Матрицы Mitre Att&ck позволяют оперативно определить, на каком этапе обнаружена атака и где стоит в первую очередь искать следы вторжения. 4. Атрибуция атак. По перечню

техник, использованных злоумышленниками, можно определить вероятного исполнителя. 5. Анализ деятельности киберпреступников. Матрицы Mitre Att&ck позволяют отслеживать эволюцию тактик и техник, которые применяют известные APT-группировки. 6. Обмен информацией с коллегами. Единая структурированная система описания кибератаки позволяет специалистам из разных областей находить общий язык.

2.Какие дистрибутивы операционных систем для проведения тестирования на проникновение Вам известны?

Ответы:

Для получения высокого балла необходимо назвать не менее 5 ОС, применяемых специалистами по информационной безопасности для тестирования уязвимостей ИБ

Верный ответ: Существует несколько популярных securty дистрибутивов, содержащих большинство популярных утилит и приложений для проведения тестирования на проникновение. Обычно они основаны на существующих Linux-дистрибутивах и представляют из себя их переработанные версии. К таким дистрибутивам относятся: Kali Linux BlackArch Parrot Security OS BackBox Pentoo Linux DEFT Linux Pentest Box Santoku Linux

3.Перечислите инструменты, встроенные в ОС Kali Linux, применяемые для решения профильных задач специалистами из сферы информационной безопасности

Ответы:

Для верного ответа на вопрос рекомендуется обратиться на официальный сайт ОС Kali Linux)https://www.kali.org/)

Верный ответ: В Kali Linux собрано более 600 программ для проверки безопасности программ, сетевой инфраструктуры и веб-ресурсов К числу наиболее популярных можно отнести следующие встроенные программы: - Armitage - для сбора данных и визуализации целей, что упрощает процесс взлома пентеста. - Nmap - для сканирования IP-сетей с любым числом объектов. - Wireshark помогает сохранить и проанализировать трафик. - John the Ripper – инструмент для восстановления паролей по хешам. - Aircrack-ng позволяет протестировать беспроводные сети. - Burp Suite и OWASP ZAP сканируют безопасность веб-приложений.

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

Для курсового проекта/работы:

6 семестр

Форма проведения: Защита КП/КР

I. Процедура защиты КП/КР

К защите допускаются только курсовые работы, прошедшие рецензирование, сброшюрованные и оформленные в соответствии с требованиями методических рекомендаций. Студент устно защищает курсовую работу перед комиссией с демонстрацией презентационных материалов в формате PowerPoint или PDF

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

Результат работы в семестре оценивается с учётом выполнения сроков поэтапной сдачи разделов курсовой работы, посещения консультаций, а также правильности изложенных в курсовой работе теоретического и практического аспектов темы работы