

**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  
2024**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик

|  |                                                    |                               |
|--|----------------------------------------------------|-------------------------------|
|  | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» |                               |
|  | Сведения о владельце ЦЭП МЭИ                       |                               |
|  | Владелец                                           | Дратвяк А.В.                  |
|  | Идентификатор                                      | R1a0ecc29-DratviakAV-b9b11303 |

А.В. Дратвяк

## 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

Заведующий  
выпускающей кафедрой

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

А.Ю.  
Невский

## 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-2 Способен администрировать средства защиты информации в компьютерных системах и сетях

ПК-3.2 Администрирует программно-аппаратные средства защиты информации в компьютерных сетях

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   | 15   |
| 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:                                                                                 | 12,5 | 12,5 | 12,5 | 12,5 | 12,5 | 12,5 | 12,5 | 12,5 |

\$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-2               | ПК-3.2 <sub>ПК-2</sub><br>Администрирует программно-аппаратные средства защиты информации в компьютерных сетях | Знать:<br>программные и программно-аппаратные средства защиты компьютерных систем от кибератак<br>типовые алгоритмы атаки и механизмы защиты от кибератак на информационные системы<br>классификацию киберугроз<br>информационной безопасности в соответствии нормативными документами регуляторов<br>Уметь:<br>разрабатывать рекомендации по применению программных и программно-аппаратных решений для защиты системных и прикладных программных продуктов, а | Контрольное мероприятие № 1 (Контрольная работа)<br>Контрольное мероприятие № 2 (Контрольная работа)<br>Контрольное мероприятие № 3 (Контрольная работа)<br>Контрольное мероприятие № 4 (Контрольная работа)<br>Контрольное мероприятие № 5 (Контрольная работа)<br>Контрольное мероприятие № 6 (Контрольная работа)<br>Контрольное мероприятие № 7 (Контрольная работа)<br>Контрольное мероприятие № 8 (Контрольная работа) |

|  |  |                                                                                                                                                                                                                                                                                                                                                   |  |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
|  |  | <p>также web-приложений и ресурсов сети "Интернет" от киберугроз</p> <p>применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах</p> <p>проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей</p> |  |
|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

## 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:** 12,5

**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 киберугроз информационной безопасности в соответствии нормативными документами регуляторов                  | <b>1.1 вариант</b><br>Что такое Command and Control server?<br>Что такое Payload?<br>Указать домен второго уровня из api.tiktok.com<br>Дайте описание тактики "Initial Access"<br>Что такое SSH?<br><br><b>2 вариант</b><br>Что такое "уязвимость"?<br>Что такое exploit?<br>Указать домен третьего уровня из api.tiktok.com<br>Дайте описание тактики "Persistence"<br>Что такое SSL/TLS? |
| Уметь: применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах | <b>1.1 вариант</b><br>Отфильтруйте матрицу Mittra по тактике атаки "Initial Access"<br><br><b>2 вариант</b><br>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

*Оценка:* 2

*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

## **КМ-2. Контрольное мероприятие № 2**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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                                                 | <b>1.1 вариант</b><br>Преимущества сканеров уязвимостей<br>Перечень видов сетевых атак<br>Средства ОБ ОС<br>Суть средства защиты Air Gap<br>Хар-ка "статического тестирования" ПО<br><br><b>2 вариант</b><br>Недостатки сканеров уязвимостей<br>Перечень средства защиты от сетевых атак<br>Средства ОБ приложений (App Sec)<br>Суть средства защиты Honeypots<br>Хар-ка "динамического тестирования" ПО |
| Уметь: проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей | <b>1.1 вариант</b><br>Постройте mind-карту программных продуктов, применяемых для "статического тестирования" ПО<br><br><b>2 вариант</b><br>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

*Оценка:* 2

*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

### **КМ-3. Контрольное мероприятие № 3**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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:**

|                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Знать:</b> программные и программно-аппаратные средства защиты компьютерных систем от кибератак                                                 | <b>1.1 вариант</b><br>Команда для получения списка установленных пакетов<br>Команда для получения содержимого файла<br>Команда создания архива<br>Что такое Persistence?<br>Что такое Defense Evasion?<br><br><b>2 вариант</b><br>Как выглядит команда с флагами (опциями)<br>Можно ли на сервисе CVE Details посмотреть ущерб для КЦД?<br>Приведите пример идентификатора уязвимостей в базе данных CVE (из чего состоит идентификатор)<br>Что такое Lateral Movement?<br>Что такое Privilege Escalation? |
| <b>Уметь:</b> проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей | <b>1.1 вариант</b><br>Продемонстрируйте применение команды для получения содержимого файла в ОС Kali Linux<br><br><b>2 вариант</b><br>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*

*Оценка: 2*

*Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено*

#### **КМ-4. Контрольное мероприятие № 4**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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                                                                                                                             | <b>1.1 вариант</b><br>Функциональные возможности NGFW<br>Для чего нужен Burn Suite?<br>Что можно делать с помощью Nmap?<br>Три этапа типовой схемы атаки на АСУ ТП<br>Схема работы DNS-over-HTTPS<br><br><b>2 вариант</b><br>Функциональные возможности IDS/IPS<br>Для чего нужен WireShark?<br>Что можно делать с помощью John the Ripper?<br>Три типа моделей АСУ ТП<br>Схема работы DNS-over-HTTPS |
| 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 | <b>1.1 вариант</b><br>Запустите и продемонстрируйте базовые возможности утилиты Nmap в ОС Kali Linux<br><br><b>2 вариант</b><br>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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**КМ-5. Контрольное мероприятие № 5**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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 киберугроз информационной безопасности в соответствии нормативными документами регуляторов | 1.Контрольное мероприятие по дисциплине "Технологии защиты информационных систем от кибератак" |                                                                                                   |                                                                                 |
|                                                                                                                 | № п/п                                                                                          | 1 Вариант                                                                                         | 2 Вариант                                                                       |
|                                                                                                                 | 1                                                                                              | Что такое и каковы причины возникновения SQL-инъекций?                                            | Перечислите и раскройте суть техник, применяемых при эксплуатации SQL-инъекций. |
|                                                                                                                 | 2                                                                                              | Подробно раскройте что такое Blind SQL-инъекция.                                                  | Подробно раскройте что такое Time-Based SQL-инъекция.                           |
|                                                                                                                 | 3                                                                                              | Дайте определение ORM, поясните как данная технология используется в контексте кибербезопасности. | Для каких целей могут быть использованы команды chown и chmod?                  |
|                                                                                                                 | 4                                                                                              | Перечислите и поясните методы обнаружения                                                         | Перечислите и поясните методы                                                   |

|                                                                                                                                  |    |   |                                                                                                          |                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------|----|---|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
|                                                                                                                                  |    |   | внедрения опасных команд.                                                                                | предотвращения внедрения опасных команд.                                         |
|                                                                                                                                  |    | 5 | Что такое XSS в контексте информационной безопасности?<br>Раскройте сущность XSS на конкретных примерах. | Составьте классификацию XSS и раскройте суть каждого из элементов классификации. |
| Уметь: применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах | 1. |   |                                                                                                          |                                                                                  |
|                                                                                                                                  |    | 6 | На примере стенда кафедры продемонстрировать реализацию обычной SQL-инъекции                             | На примере стенда кафедры продемонстрировать реализацию Blind SQL-инъекции       |

#### 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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

#### КМ-6. Контрольное мероприятие № 6

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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.Контрольное мероприятие по дисциплине "Технологии защиты информационных систем от кибератак" |           |           |
|                                                                                             | №                                                                                              | 1 Вариант | 2 Вариант |

|                                                                                                                                             |   |                                                                                                                                    |                                                                                                                                                                                          |                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                             |   | п/п                                                                                                                                |                                                                                                                                                                                          |                                                                                                                                                                                   |
|                                                                                                                                             |   | 1                                                                                                                                  | Приведите примеры реализации stored XSS атак                                                                                                                                             | Приведите примеры реализации reflected XSS                                                                                                                                        |
|                                                                                                                                             |   | 2                                                                                                                                  | Поясните в чём заключаются отличие следующих видов XSS атак: stored, reflected и DOM-based                                                                                               | Раскройте суть понятия CSP, опишите порядок его включения и приведите пример её реализации.                                                                                       |
|                                                                                                                                             |   | 3                                                                                                                                  | Нарусуйте графическую схему атаки типа CSRF.                                                                                                                                             | Нарусуйте графическую схему атаки типа SSRF.                                                                                                                                      |
|                                                                                                                                             |   | 4                                                                                                                                  | Дайте характеристику методов защиты от CSRF. Дайте определение "токену" в контексте защиты от CSRF атаки. Опишите суть и порядок использования Synchronizer Token и Double Submit Cookie | Дайте характеристику методов защиты от CSRF. Дайте определение "токену" в контексте защиты от CSRF 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: проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей |   | 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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

### КМ-7. Контрольное мероприятие № 7

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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.Контрольное мероприятие по дисциплине "Технологии защиты информационных систем от кибератак" |                                                                                                                                    |                                                                                                                                    |
|                                                                                             | № п/п                                                                                          | 1 Вариант                                                                                                                          | 2 Вариант                                                                                                                          |
|                                                                                             | 1                                                                                              | Схематично изобразите жизненный цикл существования идентификатора сеанса веб-приложения. Дайте краткое описание каждому из этапов. | Какие критерии определяют срок действия сеанса в веб-приложениях, и какие механизмы автоматического истечения сеанса Вам известны? |
|                                                                                             | 2                                                                                              | Перечислите и кратко охарактеризуйте средства защиты, используемые для управления сеансом на стороне клиента.                      | Перечислите механизмы обнаружения сессионных атак на веб-приложения.                                                               |
|                                                                                             | 3                                                                                              | Раскройте варианты и суть реализации атаки типа "обход пути".                                                                      | Опишите суть требований, предъявляемых к структуре и значению идентификатора сеанса в веб-приложениях.                             |
|                                                                                             | 4                                                                                              | Назовите и раскройте смысл защитных мер, применяемых для защиты от атак типа "обход                                                | Назовите различия в тестировании                                                                                                   |

|                                                                                                                                             |  |    |                                                                                                                                                      |                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------|--|----|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                             |  |    | пути".                                                                                                                                               | методом "чёрного" и "серого ящика" в контексте веб-безопасности.                                                                                               |
|                                                                                                                                             |  | 5  | Дайте определение безопасному и небезопасному перенаправлению/переадресации URL                                                                      | Дайте характеристику мер предотвращения Open Redirect.                                                                                                         |
| Уметь: проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей |  | 1. |                                                                                                                                                      |                                                                                                                                                                |
|                                                                                                                                             |  | 6  | В матрице MITRE ATT&CK отфильтровать техники атаки типа "обход пути". Определить вредоносные программные продукты, применяемые на данном этапе атаки | В матрице MITRE ATT&CK отфильтровать техники атаки типа "повышения привилегий". Определить вредоносные программные продукты, применяемые на данном этапе атаки |

#### 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

Оценка: 2

Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

#### КМ-8. Контрольное мероприятие № 8

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Контрольная работа

**Вес контрольного мероприятия в БРС:** 12,5

**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.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 контексте безопасности веб-приложений. Перечислите основные достоинства и недостатки MFA. | Перечислите варианты реализации технологии MFA в веб-приложениях. Дайте характеристику безопасности применения указанных вариантов реализации. |
|                                                                                                                                                                                                                      | 5                                                                                              | Дайте определение понятию сериализация и десериализация. Что подразумевается под небезопасной сериализацией.           | Раскройте суть концепции хеширования "соль и перец". Какой цели служит добавление "перца" при хешировании?                                     |
| 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.                                                                                             |                                                                                                                        |                                                                                                                                                |
|                                                                                                                                                                                                                      | 5                                                                                              | Сформируйте mind-карту уязвимостей веб-приложений (desktopных и мобильных) по критерию типа реализуемой атаки          | Сформируйте mind-карту уязвимостей веб-сайта по критерию типа реализуемой атаки                                                                |

#### 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*

*Оценка: 2*

*Описание характеристики выполнения знания: Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

6 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

|                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                       |                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>НИУ<br/>МЭИ</b>                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1</b><br>Кафедра:<br><i>Безопасности и информационных технологий</i><br>Дисциплина: «Технологии защиты информационных систем от кибератак» | <i>Утверждаю:<br/>Зав. каф. БИТ<br/>А.Ю. Невский<br/>Протокол кафедры №<br/>3<br/>«16» декабря 2020г.</i> |
| 1. Ответственность за киберпреступления, предусмотренная законодательством РФ.<br>2. Понятие CIA в контексте сетевой безопасности корпоративных информационных систем.<br>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

### ***1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

**1. Компетенция/Индикатор:** ПК-3.2<sub>ПК-2</sub> Администрирует программно-аппаратные средства защиты информации в компьютерных сетях

### **Вопросы, задания**

1. Ответственность за киберпреступления, предусмотренная законодательством РФ
2. Понятие, структура и этапы компьютерной атаки на информационную систему предприятия
3. Классификация уязвимостей компьютерных систем на основе матрицы MITRE ATT&CK
4. Задачи и функции "красной", "синей" и "фиолетовой" команд аудита информационной безопасности компьютерных систем
5. Техники атаки на компьютерную систему категории Reconnaissance в соответствии с матрицей MITRE ATT&CK
6. Характеристика базы данных CVE и банка данных угроз безопасности информации ФСТЭК России
7. Порядок работы с базой данных известных киберуязвимостей CVE и специализированными сервисами типа CVE Details
8. Характеристика открытого проекта обеспечения безопасности веб-приложений OWASP и инструмента OWASP Cheat Sheet Series
9. Базовая модель кибернарушителя информационной безопасности компьютерной системы. Его квалификация и применяемые инструменты.
10. 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 АРТ-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 security 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

*Оценка: 2*

*Описание характеристики выполнения знания:* Работа не выполнена или выполнена преимущественно неправильно

## ***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

*Оценка: 2*

*Описание характеристики выполнения знания:* Работа не выполнена или выполнена преимущественно неправильно

### ***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