Контрольно-оценочные средства для проведения текущего контроля
по МДК.09.03 Обеспечение безопасности веб-приложений
(3 курс, 5 семестр 2025-2026 уч. г.)

Текущий контроль №1 (90 минут)

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Письменный опрос
Задание №1 (30 минут)

Представить ответы на следующие вопросы:

1. Что такое SQL инъекции?
2. На какие два вида делятся HTML инъекции?
3. Перечислите 22 вида уязвимостей веб сайтов.

Оценка	Показатели оценки
5	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
3	Представлен ответ на 1 вопрос.

Задание №2 (30 минут)

Представить ответы на следующие вопросы:

1. Что такое веб-аналитика?

2. Назвать основные методы веб-аналитики.

3. Описать процесс настройки системы веб-аналитики.

Оценка	Показатели оценки
5	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
3	Представлен ответ на 1 вопрос.

Задание №3 (30 минут)

Представить ответы на следующие вопросы:

1. Что такое "Нежелательный контент"?

2. Что такое "Утечки информации"?

3. Что такое "Несанкционированный доступ"?

Оценка	Показатели оценки
5	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
3	Представлен ответ на 1 вопрос.

Текущий контроль №2 (90 минут)

Форма контроля: Практическая работа (Информационно-аналитический)
Описательная часть: Практическая работа с применением ИКТ
Задание №1 (30 минут)

Представить ответы на следующие вопросы:

1. Дайте характеристику 10 видам уязвимостей веб сайтов.

2. Назовите виды сетевых атак.

3. Что является наиболее эффективным средством для защиты от сетевых атак?

Оценка	Показатели оценки
5	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
3	Представлен ответ на 1 вопрос.

Задание №2 (30 минут)

Представить ответы на следующие вопросы:

1. Что понимается под несанкционированным воздействием на защищаемую информацию

2. Дайте понятие конфиденциальности, целостности и доступности информации.

3. Дайте определение информационной безопасности.

Оценка	Показатели оценки
5	Представлены ответы на все вопросы.
4	Представлены ответы на 2 вопроса.
3	Представлен ответ на 1 вопрос.

Задание №3 (30 минут)

1.Найти административные интерфейсы коммуникационного и сетевого оборудования

(видеокамеры, коммутаторы ЛВС, домашние Wi-Fi маршрутизаторы, и т.д.), подключенные к сети Интернет.

2. Известно, что адрес веб-интерфейса системы VMWare Horizon View HTML Access содержит строку portal/webclient/views/mainUI.html. Найти такие системы, доступные из сети Интернет.

3. Оценить количество коммутаторов Cisco Catalyst с административным веб-интерфейсом, подключенным к сети Интернет.

Оценка	Показатели оценки
5	Представлены все пункты задания.
4	Представлены 2 пункта задания.
3	Представлен 1 пункт задания.

Текущий контроль №3 (90 минут)

Форма контроля: Практическая работа (Информационно-аналитический)
Описательная часть: Практическая работа с применением ИКТ
Задание №1 (30 минут)

Привести рабочий алгоритм проверки защищенности механизма управления доступом и сессиями

Оценка	Показатели оценки
5	Выделены основные атаки на механизм управления сессиями (не менее 4), сформулированы основные требования безопасности к реализации механизма управления сессиями (не менее 8) и алгоритм проверки защищенности механизма управления доступом и сессиями
4	Сформулированы основные требования безопасности к реализации механизма управления сессиями (менее 8) и алгоритм проверки защищенности механизма управления доступом и сессиями с незначительными ошибками
3	Приведен алгоритм проверки защищенности механизма управления доступом и сессиями с ошибками

Задание №2 (30 минут)

1. Что такое аутентификация?

2. Что такое авторизация?

3 Написать на php пример защищенной авторизации и регистрации.

Оценка	Показатели оценки
5	Задание выполнено в полном объеме.
4	Выполнено 2 пункта задания.
3	Выполнен 1 пункт задания.

Задание №3 (30 минут)

Определить контекст вывода данных для каждого из нижеприведенных векторов XSS-атаки

<h1>Hello,<img/src=1 onerror=prompt(0)></h1>

<script>var name=";alert(1);";</script>

ClickMe

<div class=""onmouseover="alert(1);">…

…

Указать меры для предотвращения XSS-атаки в зависимости от контекста.

Оценка	Показатели оценки
5	Безошибочно выполнена идентификация уязвимостей к атаке XSS в зависимости от контекста выводимых данных, для каждого XSS-вектора указаны меры по предотвращению угрозы атаки.
4	Идентификация уязвимостей к атаке XSS для каждого XSS-вектора и меры по предотвращению угрозы атаки выполнены с незначительными ошибками.
3	Идентификация уязвимостей к атаке XSS для каждого XSS-вектора и меры по предотвращению угрозы атаки выполнены частично, допущены ошибки