Контрольно-оценочные средства для проведения текущего контроля
по МДК.09.03 Обеспечение безопасности веб-приложений
(3 курс, 5 семестр 2023-2024 уч. г.)

Текущий контроль №1

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

- Что понимается под несанкционированным воздействием на защищаемую информацию?
- Дайте понятие конфиденциальности, целостности и доступности информации.
- Дайте определение информационной безопасности.

Оценка	Показатели оценки
3	Дан ответ на 1 вопрос из 3.
4	Дан ответ на 2 вопроса из 3.
5	Дан ответ на все 3 вопроса.

Задание №2

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

Оценка	Показатели оценки
3	Дан ответ на 1 вопрос из 3.
4	Дан ответ на 2 вопроса из 3.
5	Дан ответ на все 3 вопроса.

Текущий контроль №2

Форма контроля: Письменный опрос (Опрос)
Описательная часть: Письменный опрос с применением ИКТ
Задание №1

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

3	Дан ответ на 1 вопрос из 3.
4	Дан ответ на 2 вопроса из 3.
5	Дан ответ на все 3 вопроса.

Задание №2

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
3	Дан ответ на 1 вопрос из 3.
4	Дан ответ на 2 вопроса из 3.
5	Дан ответ на все 3 вопроса.

Текущий контроль №3

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

1. Для веб-приложения, уязвимого к атаке CSRF, написать эксплоит, отправляющий данные типа

multipart/form-data.

2. Для веб-приложения, уязвимого к атаке XSS, написать на языке JavaScript эксплоит, извлекающий CSRF-токен.

3. Показать, как, используя уязвимость к атаке CSRF, можно выполнить атаку XSS.

Оценка	Показатели оценки
3	Выполнено 1 задание из 3.
4	Выполнено 2 задания из 3.
5	Выполнены все 3 задания.

Задание №2

1. Как автоматически идентифицировать уязвимости, связанные с загрузкой файлов на сервер?

2. Изучить рекомендации по реализации защищенной загрузки файлов на сервер.

3. Загрузить на сервер и использовать PHP шелл-код c99.

Оценка	Показатели оценки
3	Выполнено 1 задание из 3.
4	Выполнено 2 задания из 3.
5	Выполнены все 3 задания.