**Примерные оценочные материалы, применяемые при проведении промежуточной аттестации по дисциплине (модулю) «Безопасность компьютерных систем».**

При проведении промежуточной аттестации обучающемуся предлагается дать ответы на 3 вопроса, из нижеприведенного списка.

1. Классификация угроз информационной безопасности. Нежелательный контент.
2. Классификация угроз информационной безопасности. Несанкционированный доступ.
3. Реверс-инжиниринг. Инструменты для проведения
4. Реверс-инжиниринг. Дизассемблирование, декомпиляция отладка.
5. Средства для анализа сетевого трафика.
6. Анализ сетевого трафика с помощью технологии реверс-инжиниринга. Последовательность действий.
7. Причины возникновения уязвимостей веб-приложений.
8. Уязвимости веб-приложений. Инъекции.
9. Уязвимости веб-приложений. Недостатки аутентификации.
10. Уязвимости веб-приложений. **Межсайтовое выполнение сценариев.**
11. Инструменты поиска уязвимостей. Принципы работы.
12. Инструменты поиска уязвимостей. [Wapiti](https://habr.com/ru/post/510998/),
13. Инструменты поиска уязвимостей. [Nikto](https://cirt.net/Nikto2),
14. Инструменты поиска уязвимостей. [Vega](https://subgraph.com/vega/download/).
15. Инструменты поиска уязвимостей. [SQLmap](http://sqlmap.org/).
16. Использование HTTP-прокси для анализа трафика.
17. Поиск особенностей в поведении приложения на низком уровне.
18. Уязвимости веб-приложений IDOR.
19. Бинарные уязвимости. Вредоносное воздействие.
20. Бинарные уязвимости. Методология и контрольный список для тестирования.
21. Атаки на базы данных.