# Программа зачета:

# 1. Основные сетевые уязвимости. Уровни модели OSI, на которых возможна эксплуатация уязвимостей.

# 2. Понятие угрозы ИБ, классификация угроз. Угрозы, связанные с сетевым взаимодействием.

# 3. Анализ сетевого трафика. Возможные пути реализации и способы защиты.

# 4. Подмена доверенного объекта сети. Возможные пути реализации и способы защиты.

# 5. Навязывание ложного маршрута. Возможные пути реализации и способы защиты.

# 6. Внедрение ложного DNS-сервера. Возможные пути реализации и способы защиты.

# 7. Внедрение ложного ARP-сервера. Возможные пути реализации и способы защиты.

# 8. Понятие угрозы, реализуемой на прикладном уровне. Классификация сетевых угроз, реализуемых на уровне приложений.

# 9. SQL-инъекции. Возможные пути реализации и способы защиты.

# 10. Межсайтовый скриптинг. Возможные пути реализации и способы защиты.

# 11. Доступ по прямым ссылкам. Возможные пути реализации и способы защиты.

# 12. Непроверенный переход и редирект. Возможные пути реализации и способы защиты.

# 13. Межсайтовая подделка запроса. Возможные пути реализации и способы защиты.

# 14. Обход аутентификации. Возможные пути реализации и способы защиты.

# 15. DoS, DDoS. Возможные пути реализации и способы защиты.

# 16. Классификация технических средств защиты информации, используемых в целях противодействия сетевым угрозам.

# 17. Межсетевые экраны. Классификация по способу фильтрации.

# 18. Межсетевые экраны. Способы размещения в ЛВС.

# 19. Web application firewall.

# 20. Виртуальные частные сети. Принципы работы.

# 21. Средства обнаружения и предотвращения вторжений. Принципы работы.

# 22. Honeypot-системы. Принципы работы.

# 23. Средства анализа защищенности.

# 24. Защищённые протоколы обмена информацией, работающие на транспортном уровне и уровне приложений. Варианты аутентификации в сети.