# План проведения практических занятий по дисциплине «Криптографические методы защиты информации»

Занятие 1. Вводное занятие. Методы современной криптографии.

1. Порядок проведения занятий и получения допуска к экзамену.
2. Основные понятия криптографии.
3. Применение криптографических методов защиты информации.

Занятие 2. Понятие криптографического протокола.

1. Понятие и классификация криптографических протоколов.
2. Атаки на криптографические протоколы и методы их анализа.
3. Структура криптографических классов библиотеки Framework Class Library (FCL).

Занятие 3. Протоколы обмена ключами.

1. Требования к распределению ключей.
2. Обмен ключами с помощью центра распределения ключей.
3. Прямой обмен ключами.

Занятие 4. Протоколы обмена ключами.

1. Протоколы передачи и обновления сеансовых ключей.
2. Депонирование ключей.
3. Обсуждение выбора тем рефератов и расчетных заданий.

Занятие 5. Протоколы аутентификации.

1. Односторонняя и взаимная аутентификация.
2. Анонимное распределение ключей.
3. Классы библиотеки FCL для представления сертификатов и цепочек сертификатов.

Занятие 6. Протоколы с нулевой передачей знаний.

1. Протоколы Шнорра и Фиата-Шамира.
2. Протоколы Фейге-Фиата-Шамира и Гиллоу-Куискуотера.
3. Классы библиотеки FCL для хранилищ и коллекций сертификатов, диалогов выбора сертификата.

Занятие 7. Протоколы электронной подписи.

1. Неоспоримая и не отрицаемая электронные подписи.
2. Электронная подпись вслепую.
3. Средства Microsoft Windows для работы с сертификатами (оснастки «Сертификаты», «Шаблоны сертификатов» и «Центр сертификации»).

Занятие 8. Протоколы разделения секрета и скрытого канала.

1. Протоколы разделения секрета и подсознательного канала.
2. Системные средства Microsoft Windows для создания и применения сертификатов (программы MakeCert, MakeCTL, SignTool, CertMgr, pvk2pfx).
3. Заслушивание докладов по темам рефератов.

Занятие 9. Протоколы электронной почты и предсказания бита.

1. Электронная почта с подтверждением и одновременное подписание контракта.
2. Предсказание бита.
3. Заслушивание докладов по темам рефератов.

Занятие 10. Электронная жеребьевка и вычисления с секретными данными.

1. Электронное бросание монеты.
2. Вычисления с секретными данными.
3. Заслушивание докладов по темам рефератов.

Занятие 11. Анонимные вычисления и электронная коммерция.

1. Задача «миллионеров».
2. Протоколы и системы электронных наличных.
3. Заслушивание докладов по темам рефератов.

Занятие 12. Протоколы электронного голосования.

1. Голосование со слепыми подписями.
2. Голосование с центральной избирательной комиссией.
3. Заслушивание докладов по темам рефератов.

Занятие 13. Инфраструктура открытых ключей.

1. Управление сертификатами открытых ключей.
2. Элементы и архитектура инфраструктуры открытых ключей.
3. Заслушивание докладов по темам рефератов.

Занятие 14. Применение инфраструктуры открытых ключей.

1. Сертификация без удостоверяющих центров.
2. Отзыв и распространение сертификатов и списков отозванных сертификатов.
3. Заслушивание докладов по темам рефератов.

Занятие 15. Защита личных ключей.

1. Хранение личных ключей в файлах.
2. Хранение личных ключей на устройствах, защищенных от несанкционированного чтения.
3. Заслушивание докладов по темам рефератов.

Занятие 16. Криптографические средства инфраструктуры открытых ключей.

1. Хранение личных ключей на сервере.
2. Криптографические интерфейсы Microsoft CryptoAPI, Cryptoki и др.
3. Заслушивание докладов по темам рефератов.

Занятие 17. Итоговое занятие.