Программа спецкурса для аспирантов по специальности 05.13.19
«Криптографические методы защиты информации»
(полугодовой курс, 36 часов)
Подготовили: д.ф.-м.н., проф. В.А.Васенин, к.ф.-м.н., с.н.с. А.В.Галатенко, к.ф.-м.н., с.н.с. К.А.Шапченко, к.ф.-м.н., с.н.с. Ф.М.Пучков

Лекция 1. Введение в криптографию, часть 1 (2 часа).
Криптография и криптоанализ. Обзор решаемых задач и основных методов. Понятия криптографической системы, криптографического алгоритма, криптографического протокола. Обзор нормативной базы в области криптографии.

Лекция 2. Введение в криптографию, часть 2 (2 часа).
Обзор типовых областей применения криптографических систем, алгоритмов и протоколов. Криптографическая стойкость. Обзор распространенных методов атак.

Лекция 3. Обзор и применение методов криптографической защиты информации (2 часа).
Обзор методов криптографии с симметричным ключом и криптографии с открытым ключом. Виды блочных и поточных шифров.

Лекция 4. Симметричные криптосистемы, часть 1 (2 часа).
Примеры традиционных симметричных криптосистем: шифры перестановки; шифр перестановки «скитала»; шифрующие таблицы; применение магических квадратов; шифры простой замены; полибианский квадрат; система шифрования Цезаря; система шифрования Вижинера; шифр «двойной квадрат» Уитстона; одноразовая система шифрования; шифрование методом Вернама; роторные машины; шифрование методом гаммирования.

Лекция 5. Симметричные криптосистемы, часть 2 (2 часа).
Применение симметричных криптосистем для защиты компьютерной информации в информационных системах. Обзор основных принципов и режимов работы алгоритма шифрования данных DES.

Лекция 6. Криптосистема AES (2 часа).
Обзор основных принципов и режимов работы алгоритма шифрования данных AES.

Лекция 7. Обзор стандарта симметричного шифрования данных ГОСТ 28147-89 (2 часа).
Общие положения отечественного стандарта шифрования данных на примере режимов простой замены, гаммирования, гаммирования с обратной связью, выработки имитовставки.

Лекция 8. Асимметричные криптосистемы. Общие положения (2 часа).
Применение асимметричных криптосистем для защиты компьютерной информации в информационных системах. Концепция криптосистемы с открытым ключом. Однонаправленные функции. Комбинированные методы шифрования.

Лекция 9. Асимметричные криптосистемы. Криптосистема RSA (2 часа).
Криптосистема шифрования данных RSA на примере алгоритмов шифрования и расшифрования в этой системе.

Лекция 10. Асимметричные криптосистемы. Криптосистема Полига-Хеллмана. Криптосистема эль-Гамаля (2 часа).
Схема шифрования Полига—Хеллмана. Схема шифрования эль-Гамаля.

Лекция 11. Криптографические методы идентификации и аутентификации в компьютерных системах (2 часа).
Криптографические методы идентификации и аутентификации в компьютерных системах. Взаимная аутентификация.

Лекция 12. Протоколы идентификации с нулевой передачей знаний (2 часа).
Протоколы идентификации с нулевой передачей знаний.

Лекция 13. Генераторы псевдослучайных чисел (2 часа).
Роль генераторов псевдослучайных чисел в криптосистемах. Методы генерации псевдослучайных последовательностей чисел. Криптографически стойкие генераторы псевдослучайных чисел.

Лекция 14. Методы построения хеш-функций (2 часа).
Методы реализации хеш-функций. Однонаправленные хеш-функции. Однонаправленные хеш-функции на основе симметричных блочных алгоритмов.

Лекция 15. Алгоритмы хеширования MD, SHA (2 часа).
Обзор алгоритмов хеширования семейств MD и SHA.

Лекция 16. Обзор отечественного стандарта функции хэширования (2 часа).
Отечественный стандарт хеш-функции.

Лекция 17. Методы реализации электронной цифровой подписи.
Методы реализации электронной цифровой подписи. Электронная цифровая подпись на примере алгоритмов RSA, EGSA, DSA.

Лекция 18. Обзор отечественного стандарта электронной цифровой подписи (2 часа).
Отечественный стандарт цифровой подписи.

Рекомендуемая литература

1. Основы информационной безопасности: учебное пособие. / В. А. Галатенко. Под редакцией академика РАН В. Б. Бетелина – 4-е изд. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. – 205 с.: ил. – (Серия «Основы информационных технологий»).

2. Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений. / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. – М.: Издательский центр «Академия», 2009. – 272 с.

3. Б. Шнайер. Прикладная криптография: протоколы, алгоритмы и исходные тексты на языке С. 2-е изд. / Под редакцией П. В. Семьянова. – М.: Триумф, 2002.

4. Методы дискретной математики в криптологии. / В. М. Фомичев. – М.: Диалог-МИФИ, 2010. – 424 с.

5. Введение в криптографию. 3-е изд., дополненное. / Под редакцией Ященко В.В. - М.: МЦНМО, 2000.

6. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО, 2008. – 398 с.

7. Критически важные объекты и кибертерроризм. Часть 2. Аспекты программной реализации средств противодействия. / О. О. Андреев и др. Под ред. В. А. Васенина. — М.: МЦНМО, 2008. – 607 с.