

Аннотация рабочей программы дисциплины (модуля)

Математические основы защиты информации и информационной безопасности

Цели дисциплины

Целью дисциплины «Криптографические методы защиты информации» является формирование у студентов общих представлений о криптографических методах защиты информации, о применении криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности и об основных принципах, лежащих в основе функционирования криптографических средств защиты информации.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

1. дать представление о криптографических методах защиты информации.
2. изучить математические основы современной криптографии.
3. изучить современные стандарты симметричного шифрования.
4. изучить основные криптографические алгоритмы с открытым ключом.
5. изучить криптографические функции хеширования.
6. сформировать умение применять полученные знания для компьютерной реализации криптографических алгоритмов.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ОПК-1	Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте;	ОПК-1.1. Знает методы самостоятельного приобретения, развития и применения математических, естественнонаучных, социально-экономических и профессиональных знаний для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте. ОПК-1.2. Умеет приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте. ОПК-1.3. Владеет навыками самостоятельного приобретения, развития и применения математических, естественнонаучных, социально-экономических и профессиональных знаний для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.
ОПК-7.	Способен использовать методы научных исследований и математического моделирования в области проектирования и управления информационными системами	ОПК-7.1. Знает методы научных исследований и математического моделирования в области проектирования и управления информационными системами. ОПК-7.2. Умеет применять методы научных исследований и математического моделирования в области

		проектирования и управления информационными системами. ОПК-7.3. Владеет навыками применения методов научных исследований и математического моделирования в области проектирования и управления информационными системами
--	--	--

Содержание разделов дисциплины

Тема 1 Математические основы криптографии

Криптографические методы защиты информации: шифрование, хеширование, электронная подпись.

Тема 2 Основные цели и задачи криптографии

Алгебраические структуры. Группы. Циклические группы. Кольца, кольца классов вычетов. Конечные поля. Поля Галуа. Эллиптические кривые. Понятие наибольшего общего делителя. Алгоритм Евклида, расширенный алгоритм Евклида. Сравнение первой степени с одним неизвестным. Китайская теорема об остатках. Генерация простых чисел. Тест на простоту. Алгоритмы работы с большими числами.

Тема 3 Историческая криптография

Математическая модель шифра. Классические шифры: подстановочный, перестановочный, шифр Хилла, шифры гаммирования

Тема 4. Симметричное шифрование

DES. ГОСТ 28147-89. ГОСТ Р 34.12-2015. ГОСТ Р 34.13-2015. Режимы шифрования, эммитовставка. AES.

Тема 5 Хеширование

Криптографические хеш-функции. ГОСТ Р 34.11- 2012. SHA-3.

Тема 6. Поточное шифрование

Принципы поточного шифрования. Типы поточного шифрования. Синхронные и самосинхронизирующиеся шифры. Шифр RC-4 как пример поточного алгоритма шифрования.

Тема 7 ГСПЧ и проверка их качества

Генерация случайных чисел. Псевдослучайные числа и их отличия от истинно случайных чисел. Подходы к получению псевдослучайных чисел. Критерии качества псевдослучайных чисел. Виды тестов псевдослучайных последовательностей. Тесты NIST.

Тема 8. Криптография с открытым ключом

Концепция криптографии с открытым ключом. Протокол Диффи-Хеллмана. Криптосистема RSA. Криптосистема Эль-Гамала. Криптосистема Рабина.

Тема 9. Электронная подпись.

Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.

Тема 10. Протоколы

Протокол раздельного вручения бита. Протоколы доказательства знания с нулевым разглашением. Протоколы простановки "слепых" подписей. Протоколы голосования. Протоколы безопасных вычислений