Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Сибирский институт управления – филиал РАНХиГС
Кафедра информатики и математики

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

(Б1.В.ДВ.04.02)
краткое наименование дисциплины – не устанавливается
по направлению подготовки: 38.03.04 Государственное муниципальное управление
направленность (профиль): «Информационные технологии в государственном и муниципальном управлении»
квалификация: Бакалавр
формы обучения: очная

Год набора – 2022

Автор – составитель:
канд. техн. наук, доцент кафедры информатики и математики Осипов А.Л.

Новосибирск, 2021

1. Цель освоения дисциплины:

формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации безопасного использования программных средств.

2.План курса:

Тема 1. Введение и история криптографии

Актуальность задач, решаемых в криптографии. Классическая схема Шеннона с секретным ключом. История криптографии. Исторические шифры. Шифр Цезаря. Взлом шифра Цезаря.

Тема 2. Основы криптографии с открытым ключом

Односторонние функции. Задача дискретного логарифмирования. Быстрый алгоритм возведения в степень и его сложность. Задача хранения паролей в компьютере. Система «свой – чужой» в авиации. Задача, возникающая в сетях с удаленным доступом.

Тема 3. Элементы теории чисел

Простые числа. Основная теорема арифметики. Разложение числа на простые множители. Функция Эйлера. Теоремы Эйлера и Ферма. Алгоритм Евклида. Обобщенный алгоритм Евклида и решение диофантова уравнения. Нахождение инверсий по заданному модулю.

Тема 4. Системы с открытым ключом

Система Диффи-Хеллмана. Шифр Шамира. Шифр Эль-Гамаля. Односторонняя функция с лазейкой и шифр RSA.

Тема 5. Криптографические протоколы

Протоколы аутентификации и электронной подписи. Электронные деньги. Подбрасывание монеты по телефону. Ментальный покер. Доказательства с нулевым знанием. Электронные деньги. Голосование через Интернет.

Тема 6. Общие методы взлома систем с открытым ключом

«Шаг младенца, шаг великана». Теоретико-числовые алгоритмы. Алгоритм исчисления порядка.

Тема 7. Блоковые шифры

Принципы построения блоковых шифров и требования, предъявляемые к ним. Режимы функционирования блоковых шифров: ECB, CBC, OFB, CTR. Сеть Фейстеля. Шифры DES, ГОСТ, AES. Криптоанализ блоковых шифров. Сценарии атак на шифры. Основные атаки на блоковые шифры: линейный и дифференциальный криптоанализ. Связь блоковых шифров и генераторов псевдослучайных чисел.

Тема 8. Потоковые шифры

Принципы построения и современные требования к потоковым шифрам. Криптографически стойкие генераторы псевдослучайных чисел и потоковые шифры. Классификация потоковых шифров. Основные потоковые шифры.

Тема 9. Криптографические хеш-функции

Принципы построения и современные требования к хеш-функциям. Применение хеш-функций в криптографии. Хеш-функция MD5 и семейство SHA. Хеш-функции, базирующиеся на блоковых шифрах.

3.Формы текущего контроля и промежуточной аттестации

Тема (раздел)		Методы текущего контроля успеваемости
Тема1.	Введение и история криптографии	Устный ответ на вопросы
Тема 2.	Основы криптографии с открытым ключом	Устный ответ на вопросы Выполнение практического задания на

		компьютере
Тема 3.	Элементы теории чисел	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 4.	Системы с открытым ключом	Устный ответ на вопросы
Тема 5.	Криптографические протоколы	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 6.	Общие методы взлома систем с открытым ключом	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 7.	Блоковые шифры	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 8.	Потоковые шифры	Устный ответ на вопросы Выполнение практического задания на компьютере
Тема 9.	Криптографические хеш-функции	Устный ответ на вопросы Выполнение практического задания на компьютере

Промежуточная аттестация проводится в форме: зачета и экзамена. Экзамен (зачет) проводится в форме собеседования по билету.

4.Основная литература.

1. Рябко Б. Я. Основы современной криптографии для специалистов по информационным технологиям / Б. Я. Рябко, А. Н. Фионов. – М.: Науч. мир, 2004.

2. Введение в криптографию. Новые мат. дисциплины: [учебник] / [В. В. Ященко, Н. П. Варновский, Ю. В. Нестеренко и др.]; под ред. В. В. Ященко. – СПб.: МЦНМО : Питер, 2001.

3. Бабаш А. В. Криптография / А. В. Бабаш, Г. П. Шанкин. – М.: Солон-Пресс, 2007.

4. Основы криптографии: учеб. пособие для высш. учеб. заведений по гр. специальностям в обл. информ. безопасности / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 3-е изд., испр. и доп. – М.: Гелиос АРВ, 2005.