1. АННОТАЦИЯ

к рабочей программе дисциплины
Б1.В.ОД.1.4 – Математические основы защиты информации
Трудоемкость 4 з. е.

1.1. Цель освоения и краткое содержание дисциплины

Целью изучения диципины «Математические основы защиты информации» является: Дать представление о математических основах наиболее значимых алгоритмов, применяемых для защиты информации.

Краткое содержание дисциплины. Шифрование и криптоанализ на простейших примерах. Основы теории информации и кодирования. Делимость и арифметика в кольцах вычетов. Хэширование и односторонние функции. Криптография с открытым ключом..

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1. *Перечень планируемых результатов обучения*

Планируемые результаты освоения программы (содержание и коды компетенций)	Планируемые результаты обучения по дисциплине
ОК-6 : способностью проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности, ОПК-1 : способностью воспринимать математические, естественнонаучные, социально-экономические и профессиональные знания, умением самостоятельно приобретать, развивать и применять их для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте, ОПК-5 : владением методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях, ПК-7 : применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий	В результате изучения дисциплины обучающийся должен: знать: принципы работы алгоритмов Диффи-Хеллмана и RSA; принципы работы блочных шифров; уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретико-сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p.

1.3. Место дисциплины в структуре образовательной программы

Таблица 2. *Содержательно-логические связи дисциплины*

Индекс дисциплины	Наименование дисциплины	Коды учебных дисциплин, практик	
		на которые опирается содержание дисциплины	для которых содержание дисциплины выступает опорой
Б1.В.ОД.1.4	Математические основы защиты информации	Б1.Б.3.2 – Современные проблемы информатики и вычислительной техники	Б1.В.ДВ.4.2 – Сетевое администрирование

1.4. Язык преподавания

Русский.