Код, специальность	6-05-0611-01 Информационные системы и технологии
Модуль	Информационная безопасность
Дисциплина	Математические основы криптографии

Курс / Семестр	Трудоемкость в зачетных единицах (кредитах)	Количество часов		Форма аттестации	
		аудиторных	самостоятельной работы	текущей	промежуточной
2/4	3	60	48		экзамен

Краткое содержание дисциплины (модуля*)
Элементы теории чисел: алгоритм Евклида нахождения наибольшего общего делителя целых чисел; соотношение Безу; диофантовы линейные уравнения; сравнения целых чисел; классы вычетов; функция Эйлера; теорема Эйлера; методы решения линейных сравнений и их систем; китайская теорема об остатках; понятие о первообразных корнях и индексах; задача дискретного логарифмирования, ее применение в криптографии; символы Лежандра и Якоби.
Алгебраические структуры: группа; абелева группа; циклическая группа; теорема Лагранжа о порядке подгруппы; кольцо; делители нуля в кольце; мультипликативная группа кольца; понятие поля; кольцо многочленов над полем; факторизация полиномов в произведение неприводимых множителей в зависимости от поля коэффициентов.
Поля Галуа: построение конечного поля как факторкольца кольца полиномов над полем; существование и единственность конечного поля; задача дискретного логарифмирования в конечных полях.
Эллиптические кривые над полем действительных чисел и над конечными полями, абелева группа точек эллиптической кривой, дискретный логарифм в группе точек эллиптической кривой.

Пререквизиты
Базовыми учебными дисциплинами являются «Математический анализ», «Линейная алгебра и аналитическая геометрия».

Компетенции
СК-5. Понимать математические основы криптографии и криптоанализа.

Результаты обучения (*знать, уметь, иметь навык*)
В результате изучения учебной дисциплины студент должен:
знать:
основы теории чисел, алгоритм Евклида; вычеты, элементы модулярной арифметики; определения группы, кольца, поля; действия в конечных полях (полях Галуа); алгебру над точками эллиптических кривых;

уметь:

применять алгебраические операции над полем вычетов и операции на основе модулярной арифметики для решения прикладных задач в области криптографии;

иметь навык:

владения методами вычислений на основе базовых алгебраических структур; владения основными алгоритмами теории чисел.

Примечание:

Объем описания учебной дисциплины, модуля составляет максимум одну страницу.

Пререквизиты — это учебные дисциплины, модули или навыки, которые необходимо освоить до начала изучения текущей дисциплины (модуля). Это обязательные предварительные знания (предпосылки), гарантирующие наличие базы для успешного обучения по данной учебной дисциплине (модулю).

Пререквизиты, компетенции, результаты обучения, формы текущей аттестации переписываются из учебной программы по учебной дисциплине.

** Краткое содержания модуля указывается, если аттестация, часы, зачетные единицы в учебном плане установлены на модуль.*