1	Название модуля, учебной дисциплины	Дисциплина «Криптографические технологии», дополнительные виды обучения
2	Специальность	6-05-0611-01 Информационные системы и технологии
3	Курс обучения	4
4	Семестр обучения	7
5	Степень, звание, фамилия, имя, отчество преподавателя	Кожедуб Сергей Сергеевич
6	Трудоемкость в зачетных единицах	3,0
7	Количество аудиторных часов и часов самостоятельной работы	Аудиторных – 54 часов. Самостоятельной работы – 46 часов.
8	Требования к текущей и промежуточной аттестации и ее формы	Промежуточная – зачет. Текущая – контрольные сроки.
9	Краткое содержание	Введение в криптографию. Классические криптосистемы. Симметричные блочные криптосистемы. Симметричные поточные криптосистемы. Асимметричные криптосистемы. Контроль целостности. Электронная цифровая подпись. Эллиптические кривые в криптографии. Протоколы формирования общего ключа. Новые направления в криптографии.
10	Формируемые компетенции	СК-26 Освоить методики шифрования и хэширования информации, применять методы криптоанализа, стеганографические методы скрытия передаваемой информации.
11	Результаты обучения (знать, уметь, иметь навык)	Знать: – основные задачи и понятия криптографии; – требования к шифрам и основные характеристики шифров; – методы построения и блочных и поточных криптосистем, функций хэширования, криптосистем с открытым ключом, систем электронной цифровой подписи, стеганографических систем; – принципы использования современного программного обеспечения для криптографической защиты информации; Уметь: – применять полученные знания для создания защищенных систем и документации; – использовать шифросистемы и стегосистемы для безопасной передачи бинарной и текстовой информации; – проводить простейший анализ стойкости алгоритмов; – применять хэш-функции и электронную цифровую подпись при обмене информацией; Иметь навык: – применения криптографической защитой для собственной и корпоративной информации.
12	Пререквизиты	Основы алгоритмизации и программирования, объектно-ориентированное программирование.