1	Название модуля, учебной дисциплины, учебной дисциплины по выбору студента	Модуль «Информационная безопасность», дисциплина «Защита информации в компьютерных системах и сетях»
2	Специальность	1-40 05 01 «Информационные системы и технологии (по направлениям) 1-40 05 01-10 Информационные системы и технологии (в бизнес-менеджменте)
3	Курс обучения	3
4	Семестр обучения	5
5	Степень, звание, фамилия, имя, отчество преподавателя	магистр, Киселёва Светлана Владимировна
6	Трудоемкость в зачетных единицах	3
7	Количество аудиторных часов и часов самостоятельной работы	54
8	Требования к текущей и промежуточной аттестации и ее формы	Текущая аттестация обучающихся проводится в течение семестра. Формами текущей аттестации являются тест, опрос, отчет о выполнении практической работы, защита расчетно-графической работы. Промежуточная аттестация обучающихся проводится в целях оценки результатов их учебной деятельности за семестр по учебной дисциплине. Форма промежуточной аттестации – зачет (5 семестр)
9	Краткое содержание	ТЕМА 1. Основные понятия и терминология защиты информации ТЕМА 2. Угрозы информационной безопасности компьютерных систем и сетей ТЕМА 3. Методы и средства защиты информации в компьютерных системах и сетях ТЕМА 4. Криптографические методы защиты информации в компьютерных системах и сетях

		ТЕМА 5. Средства аутентификации и управления доступом к информации в компьютерных системах и сетях ТЕМА 6. Вредоносное программное обеспечение ТЕМА 7. Защита информации в распределенных компьютерных системах
10	Формируемые компетенции	СК-22 Диагностировать виды угроз информационной безопасности компьютерных систем, применять основные методы и средства защиты информации субъекта хозяйствования
11	Результаты обучения (знать, уметь, иметь навык)	В результате изучения дисциплины студент должен *знать:* – системную методологию, правовое и нормативное обеспечение защиты информации; – организационные и технические методы защиты информации; – алгоритмы криптографического преобразования информации; *уметь:* – проводить анализ вероятных угроз и уязвимостей информационной безопасности для заданных объектов; – определять риски нарушения информационной безопасности компьютерных систем; – использовать протоколы сетевой безопасности и анализировать особенности их использования; *владеть:* методами защиты распределенных компьютерных систем.
12	Пререквизиты	Разработка программных приложений для бизнес-анализа