Факультет компьютерных технологий и прикладной математики

Направление и код подготовки/специальности (профиль): 01.03.02 Прикладная математика и информатика (Программирование и информационные технологии) / ОФО

Наименование и код дисциплины: Б1.В.ДВ.03.02«Математические методы защиты информации»	
Количество академических часов (аудиторные/внеаудиторные): 34/37,8	Количество зачетных единиц: 2
Предварительные требования для изучения дисциплины: нет	Уровень подготовки: бакалавриат
Язык обучения: русский	Вид занятий по дисциплине: лабораторные занятия– 34 ак.час., самостоятельная работа – 37,8 ак.час
Курс/семестр: 4/весенний	Вид аттестации: зачет
Образовательные технологии: коммуникативного обучения, разноуровневого (дифференцированного) обучения, модульного обучения, информационно-коммуникационные технологии, использования компьютерных программ, Интернет-технологии, проектная технология, игровая технология, развития критического мышления.	
Краткая аннотация к содержанию дисциплины: изучение основ обеспечения компьютерной и сетевой безопасности; основ безопасности информационных экономических систем предприятия; знание федеральных законов по обеспечения информационной безопасности, обработки персональных данных; владение основными алгоритмами математики криптографии; знание и использование различных криптосистем шифрования. . Важным является приобретения навыков оперирования с объектами изучаемых областей.	
Темы лекционных и семинарских занятий: 1. Базовые понятия и история развития информационной безопасности. 2. Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем. 3. Шифры замены. Шифры перестановки. Шифры гаммирования. 4. Блочные системы шифрования. 5. Поточные системы шифрования. 6. Идентификация. Цифровые подписи.	
Полученные компетенции: – Знание основы алгоритмизации и программирования безопасного кода – Знание принципов построения и виды архитектуры безопасного компьютерного программного обеспечения – Знание стандартов оформления безопасного кода для используемых языков программирования – Знание техники тестирования безопасности данных, базирующиеся на условиях использования криптозащиты – Умение применять методы и средства проектирования безопасного компьютерного программного обеспечения, структур данных, баз данных, программных интерфейсов – Умение применять существующие стандарты для разработки технической документации на компьютерное программное обеспечение с применением алгоритмов криптозащиты – Владениями навыками проектирования защищенных структур данных – Владениями навыками разработки, изменения архитектуры защищенного компьютерного программного обеспечения и ее согласование с системным аналитиком и архитектором программного обеспечения – Владениями навыками составления новых тестовых случаев и повторение тестирования при необходимости	