АННОТАЦИЯ рабочей программы дисциплины
Б1.В.ДВ.03.02«Математические методы защиты информации»

Направление подготовки 01.03.02 Прикладная математика и информатика

Объем трудоемкости: 2 з.е.

Цель дисциплины:

Курс посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель курса – научить студента методам информационной безопасности и их использовании в области защиты информации. Задачей курса является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты.

Задачи дисциплины:

Основные задачи курса на основе системного подхода:

- Описать проблемную область информационной безопасности.
- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о генерации псевдослучайных последовательностях.
- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Место дисциплины в структуре ООП ВО

Дисциплина «Математические методы защиты информации» относится к «Часть, формируемая участниками образовательных отношений» Блока 1 «Дисциплины (модули)» учебного плана.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

ПК-4	**Способен активно участвовать в разработке системного и прикладного программного обеспечения**
ПК-5	**Способен применять основные алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их разработке**

Основные разделы дисциплины:

Базовые понятия и история развития информационной безопасности.
Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.
Шифры замены. Шифры перестановки. Шифры гаммирования.
Блочные системы шифрования.

Поточные системы шифрования.
Идентификация. Цифровые подписи.

Курсовые работы: *не предусмотрено*

Форма проведения аттестации по дисциплине: *зачет*

Автор
В.В. Подколзин, доцент, канд. физ.-мат. наук