АННОТАЦИЯ рабочей программы дисциплины
Б1.О.09«Криптография и сетевая безопасность»

Направление подготовки 01.04.02 Прикладная математика и информатика

Направленность (профиль) Технологии программирования и разработки информационно-коммуникационных систем

Объем трудоемкости: 4 зач. ед. (144часов)

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.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией:

методы защиты информации;

области применения защиты информации;

о технологиях анализа шифров.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке магистра.

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

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Студент в рамках курса должен знать области применения задач информационной безопасности; методы защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности. принципы построения и функционирования систем информационной безопасности; классификацию шифров; основы организации идентификации и цифровой подписи; принципы построения и применения паролей; уметь проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

В качестве основной формы итогового контроля по рассматриваемой дисциплине предусмотрен экзамен.

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.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке магистра.

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

Место дисциплины в структуре ОПОП

Дисциплина «Криптография и сетевая безопасность» относится к «Обязательная часть» Блока 1 «Дисциплины (модули)» учебного плана.

Курс «Криптография и сетевая безопасность» входит в вариативную часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области разработки современного программного обеспечения. Курс опирается на знания в области дискретной математики, математической логики, программирования, базы данных. Курс расширяет знания студентов в области создания программных систем, защиты данных и знаний.

Дисциплина тесно связана с дисциплинами «История и методология прикладной математики и информатики», «Дискретные и вероятностные математические модели», «Технологии проектирования и сопровождения программных систем», «Распределенные системы обработки информации и управления данными».

К результатам обучения относятся:

фундаментальная подготовка по основам профессиональных знаний;

способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе; соблюдение основных требований информационной безопасности, в том числе защиты государственной тайны

владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией

способность к анализу и синтезу;

способность определения общих форм, закономерностей, инструментальных средств данной дисциплины;

умение понять поставленную задачу

умение грамотно пользоваться языком предметной области;

умение извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов, сети Интернет

знание математических основ информатики как науки

знание проблемы современной информатики, ее категории и связи с другими научными дисциплинами;

знание содержания, основных этапов и тенденции развития программирования, математического обеспечения и информационных технологий.

Требования к уровню освоения дисциплины

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

ОПК-1 Способен решать актуальные задачи фундаментальной и прикладной математики

ОПК-4 Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности

ПК-3 Способен эффективно применять алгоритмические и программные решения в области информационно-коммуникационных технологий, а также участвовать в их проектировании и разработке

Основные разделы дисциплины:

№	Наименование разделов (тем)
1	**2**
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.

Курсовые работы: *не предусмотрено*

Форма проведения аттестации по дисциплине: *экзамен*

Авторы В.В. Подколзин, доцент, канд. физ.-мат. наук, доцент
О.В. Гаркуша, доцент, канд. физ.-мат. наук, доцент