АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОЛОГИИ

Направление подготовки: 01.06.01 «Математика и механика»
Профиль: Дискретная математика и математическая кибернетика
Квалификация: Исследователь. Преподаватель-исследователь

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной образовательной программы (ООП) аспирантуры

Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код компетенции. Этап формирования компетенции	**Формулировка компетенции**	**Планируемые результаты обучения** (индикаторы достижения компетенции)
УК1	Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях	Знать: классические методы криптологии и текущее состояние современных научных достижений, фундаментальные основы криптологии. Уметь: генерировать новые идеи при решении исследовательских и практических задач, в том числе в междисциплинарных областях. Владеть: способностью к анализу и оценке современных научных достижений.
УК3	Готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач	Знать: общее состояние современных научных достижений Уметь: вести научно-исследовательскую деятельность Владеть: организационными, коммуникативными навыками, позволяющими осуществлять работу в исследовательских коллективах

УК4	Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	Знать: текущее состояние современных научных достижений Уметь: принимать мотивированное решение Владеть: навыками принятия решений и способностью нести ответственность за принятые решения
ОПК1	Способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий	Знать: текущее состояние современных научных достижений в области криптологии Уметь: использовать основные методы криптологии Владеть: навыками и основными методами криптологии
ОПК2	Готовность к преподавательской деятельности по основным образовательным программам высшего образования	Знать: историю развития криптологии, классические методы и текущее состояние современных научных достижений в области защиты информации Уметь: применять полученные теоретические знания в преподавательской деятельности Владеть: способностью к критическому анализу учебных программ по криптологии
ПК1	Понимание роли и места дискретной математики и математической кибернетики в математике в целом, их связи с другими разделами математики и другими областями науки	Знать: методы дискретной математики, теории графов, алгебры и теории алгоритмов, применяемые в криптологии и задачи защиты информации, решаемые с помощью криптографических протоколов Уметь: оценивать методы дискретной математики и математической кибернетики с точки зрения возможности и целесообразности их применения в криптологии Владеть: навыками использования методов дискретной математики и математической кибернетики в криптологии

ПК4 Основной	Способность применять алгебраические, логические, комбинаторные, вероятностные и алгоритмические методы анализа графов, автоматов, формальных языков, символьных последовательностей	Знать: текущее положение современных научных достижений в дискретной математике и математической кибернетике, классическую и современную методологию криптологии Уметь: применять алгебраические, логические, комбинаторные, вероятностные, алгоритмические и теоретико-графовые методы при решении задач защиты информации Владеть: навыками использования методов дискретной математики и математической кибернетики при решении задач защиты информации

4. Объем дисциплины и виды учебной работы

4.1. *Объем дисциплины*

Общая трудоемкость дисциплины составляет 2 зачетных единицы, 72 часа.

Вид учебной работы	**Объем часов / зачетных единиц**
Обязательная аудиторная учебная нагрузка (всего)	32
в том числе:	
лекции	16
семинары	-
практические занятия	16
Самостоятельная работа аспиранта (всего)	36
Вид контроля по дисциплине	зачет, 4

.

5. Содержание дисциплины

Тема №1. Понятие криптологии, терминология, исторический очерк.

Понятие криптологии и ее структура (криптография, криптоанализ, стеганография). История криптографии от древности до нашего времени. Примеры шифров. Понятие секретной системы по Шеннону. Представление секретных систем в виде графов. Критерии качества секретных систем

Тема №2. Алгебра секретных систем. Чистые шифры.

Операции над секретными системами (взвешенное суммирование и произведение). Ассоциативность операций. Коммутирующие шифры. Эндоморфные шифры. Множество эндоморфных шифров как ассоциативная алгебраическая система с двумя операциями. Определение чистого шифра. Смешанные шифры. Свойства чистых шифров. Остаточные классы сообщений и криптограмм. Методы криптоанализа чистых шифров. Подобие секретных систем.

Тема №3. Совершенно секретные системы.

Определение и свойства совершенно секретных систем. Доказательство существования совершенно секретных систем. Гаммирование. Энтропия. Ненадежность. Энтропийные методы криптоанализа и примеры. Стандарты криптосистем.

Тема №4. Современные методы криптологии. Секретные системы с открытым ключом.

Элементы теории алгоритмов, сложность алгоритма. Односторонние функции. Функции с секретом. Понятие секретной системы с открытым ключом. Секретная система RSA. Примеры функций, похожих на функции с секретом. Разложение натурального числа на простые сомножители. Дискретное логарифмирование. Изоморфизм графов. Рюкзачный метод шифрования.

Тема №5. Криптографические протоколы.

Понятие криптографического протокола. Протокол выработки общего ключа. Протоколы аутентификации. Подписание контракта. Подбрасывание монеты. Электронная подпись. Электронные деньги. Протокол византийского соглашения. Разделение секрета. Функции хэширования.

Разработчик:
Павлов Юрий Леонидович, г.н.с., д.ф.-м.н., профессор