

Минобрнауки России
Федеральное государственное
бюджетное учреждение науки
Федеральный исследовательский центр
«Карельский научный центр
Российской академии наук»
(КарНЦ РАН)

УТВЕРЖДАЮ

Врио председателя КарНЦ РАН
член-корр. РАН

_____ О.Н. Бахмет

« ____ » _____ 2018 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Математические основы криптологии»

Основной образовательной программы высшего образования –
программы подготовки научно-педагогических кадров в аспирантуре
по направлению подготовки

01.06.01 «Математика и механика»,
профиль: Дискретная математика и математическая кибернетика

Петрозаводск
2018

Рабочая программа дисциплины разработана в соответствии с ФГОС ВО, утвержденным приказом Министерства образования и науки Российской Федерации от 30.07.2014 г. № 866 и учебным планом по направлению подготовки аспирантуры 01.06.01 Математика и механика, профиль «Дискретная математика и математическая кибернетика».

Разработчики:

Павлов Юрий Леонидович, главный научный сотрудник ИПМИ КарНЦ РАН, доктор физико-математических наук, профессор

Эксперт:

Реттеева Анна Николаевна, ведущий научный сотрудник ИПМИ КарНЦ РАН, доктор физико-математических наук, доцент

Рабочая программа дисциплины рассмотрена и одобрена на заседании Ученого совета ИПМИ КарНЦ РАН (протокол № 5 от «24» мая 2018 г.) и рекомендована к утверждению на заседании Ученого совета КарНЦ РАН (протокол № 7 от «25» мая 2018 г.)

1. Цели и задачи дисциплины

1.1. *Целью дисциплины является:* получение базовых знаний математических основ криптографии и криптоанализа; формирование навыков использования методов криптологии в научно-исследовательской и педагогической деятельности; повышение квалификации в области научных основ и применения методов криптологии для решения фундаментальных и прикладных научно-технических проблем.

1.2. *Виды профессиональной деятельности:*

- научно-исследовательская деятельность;
- проектная деятельность.

Выпускник, освоивший программу аспирантуры в соответствии с данными видами профессиональной деятельности, готов решать следующие профессиональные задачи:

- подготовка научных и научно-технических публикаций;
- разработка алгоритмов с использованием методов криптологии;
- использование математических методов криптологии в научно-исследовательской, педагогической и производственно-технологической деятельности, включая разработку алгоритмических и программных решений в области прикладного программирования.

2. Место дисциплины в структуре ООП аспиранта

Дисциплина «Математические основы криптологии» является вариативной согласно учебному плану ООП по направлению подготовки 01.06.01 «Математика и механика», профиль – Дискретная математика и математическая кибернетика. Дисциплина изучается в 1-м и 2-м семестрах, направлена на формирование компетенций УК1, УК3, УК4, ОПК1, ОПК2, ПК1, ПК4.

3. Требования к уровню подготовки аспиранта, завершившего изучение дисциплины

В результате освоения дисциплины аспирант приобретает следующие компетенции.

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	<p>Знать: классические методы криптологии и текущее состояние современных научных достижений, фундаментальные основы криптологии.</p> <p>Уметь: генерировать новые идеи при решении исследовательских и практических задач, в том числе в междисциплинарных областях.</p> <p>Владеть: способностью к анализу и оценке современных научных достижений</p>
УК3	Готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач	<p>Знать: общее состояние современных научных достижений</p> <p>Уметь: вести научно-исследовательскую деятельность.</p> <p>Владеть: организационными, коммуникативными навыками, позволяющими осуществлять работу в исследовательских коллективах.</p>
УК4	Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках	<p>Знать: текущее состояние современных научных достижений.</p> <p>Уметь: принимать мотивированное решение.</p> <p>Владеть: навыками принятия решений и способностью нести ответственность за принятые решения</p>
ОПК1	Способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной	<p>Знать: текущее состояние современных научных достижений в области криптологии.</p> <p>Уметь: использовать основные методы криптологии.</p> <p>Владеть: навыками и основными методами криптологии.</p>

	области с использованием современных методов исследования и информационно-коммуникационных технологий	
ОПК2	Готовность к преподавательской деятельности по основным образовательным программам высшего образования	<p>Знать: историю развития криптологии, классические методы и текущее состояние современных научных достижений в области защиты информации.</p> <p>Уметь: использовать основные методы криптологии.</p> <p>Владеть: способностью к критическому анализу учебных программ по криптологии</p>
ПК1	Понимание роли и места дискретной математики и математической кибернетики в математике в целом, их связи с другими разделами математики и другими областями науки	<p>Знать: методы дискретной математики, теории графов, алгебры и теории алгоритмов, применяемые в криптологии и задачи защиты информации, решаемые с помощью криптографических протоколов.</p> <p>Уметь: оценивать методы дискретной математики и математической кибернетики с точки зрения возможности и целесообразности их применения в криптологии.</p> <p>Владеть: навыками использования методов дискретной математики и математической кибернетики в криптологии.</p>
ПК4	Способность применять алгебраические, логические, комбинаторные, вероятностные и алгоритмические методы анализа графов, автоматов, формальных языков, символьных последовательностей	<p>Знать: текущее положение современных научных достижений в дискретной математике и математической кибернетике, классическую и современную методологию криптологии.</p> <p>Уметь: применять алгебраические, логические, комбинаторные, вероятностные, алгоритмические и теоретико-графовые методы при решении задач защиты информации</p> <p>Владеть: . навыками использования методов дискретной математики и математической кибернетики при решении задач защиты информации</p>

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

4.2. Лекционные занятия

№ те мы	Название раздела/темы дисциплины	Технология проведения	Формиру- емые компетен- ции (код)	Форма оценочных средств	Трудоемкость (час.)
1	Понятие криптологии, терминология, исторический очерк	Чтение лекций, использование учебников, методических пособий и УМК	УК 3	коллоквиум	3
2	Алгебра секретных систем. Чистые шифры	Чтение лекций, использование учебников, методических пособий и УМК	ПК 1	собеседование	4
3	Совершенно секретные системы	Чтение лекций, использование учебников, методических пособий и УМК	ОПК 1	коллоквиум	3
4	Современные методы криптологии. Секретные системы с открытым ключом	Чтение лекций, использование учебников, методических пособий и УМК	ОПК 2	собеседование	4

5	Криптографические протоколы	Чтение лекций, презентации с использованием мультимедийного оборудования, использование учебников, методических пособий и УМК	ПК 4	коллоквиум	2
Итого:					16

4.3. Практические (семинарские) занятия

№ темы	Тематика занятий	Технология проведения	Формируемые компетенции (код)	Форма оценочных средств	Трудоемкость (час.)
1	Понятие криптологии, терминология, исторический очерк	Лабораторный практикум, консультация по решению задач	УК 1	Дискуссия	3
2	Алгебра секретных систем. Чистые шифры	Лабораторный практикум, консультация по решению задач	УК 4	Дискуссия	3
3	Совершенно секретные системы	Лабораторный практикум, консультация по решению задач	ОПК 1	Дискуссия	4
4	Современные методы криптологии. Секретные системы с открытым ключом	Лабораторный практикум, консультация по решению задач	ОПК 2	Дискуссия	3
5	Криптографические протоколы	Лабораторный практикум, консультация по решению задач	ПК 1	Дискуссия	3
Итого:					16

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.

6. Учебно-методическое обеспечение самостоятельной работы аспирантов

Формы проведения самостоятельной работы

№	Тема дисциплины	Форма самостоятельной работы	Трудоемкость (час.)
1	Понятие криптологии, терминология, исторический очерк	Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение по основной и дополнительной литературе с использованием интернет-ресурсов	4
2	Алгебра секретных систем. Чистые шифры	Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение по основной и дополнительной литературе с использованием интернет-ресурсов	7
3	Совершенно секретные системы	Выполнение домашних и контрольных работ с привлечением специальной научно-технической литературы и программных средств и интернет-ресурсов. Участие в НИР аспирантов	9
4	Современные методы криптологии. Секретные системы с открытым ключом	Выполнение домашних и контрольных работ с привлечением специальной научно-технической литературы и программных средств и интернет-ресурсов. Участие в НИР аспирантов	9
5	Криптографические протоколы	Проработка конспектов лекций и вопросов, вынесенных на самостоятельное изучение по основной и дополнительной литературе с использованием интернет-ресурсов	7
	Итого:		36

7. Контроль знаний аспирантов

7.1. Формы текущего контроля работы аспирантов:

1) коллоквиум; 2) собеседование; 3) дискуссия.

7.2. Промежуточная аттестация по дисциплине:

проводится в форме зачета.

7.3. Вопросы по дисциплине «Математические основы криптологии»

1. Криптология, ее структура, цели и задачи.
2. Шифры Цезаря и Сцитала.
3. Шифры Энея.
4. Шифры Третимия.
5. Дисковые шифры.
6. Шифры Кардано.
7. Шифр Виженера.
8. Шифры Бофора.
9. Шифратор Джеферсона.
10. Шифры Кеплера и Галилея.
11. История отечественной криптографии.
12. Шифровальная машина «Энигма».
13. Шифры подстановки и методы их вскрытия.
14. Шифры транспозиции и методы их вскрытия.
15. Алгебра секретных систем.
16. Чистые и смешанные шифры.
17. Метод характерных слов.
18. Совершенная секретность.
19. Доказательство существования совершенно секретного шифра.
20. Шифр Вернама и гаммирование.
21. Датчики псевдослучайных чисел и криптография.
22. Энтропия и надежность шифров.
23. Криптосистемы с открытым ключом.
24. Односторонние функции и функции с секретом.
25. Система RSA.
26. Сложность криптографических алгоритмов.
27. Дискретное логарифмирование.
28. Задача о рюкзаке.
29. Изоморфизм графов и криптография.
30. Криптографические протоколы.
31. Протоколы аутентификации.
32. Открытое распределения ключей.
33. Математика разделения секрета.
34. Электронная подпись
35. Электронные деньги.

7.4. Критерии оценки промежуточной аттестации аспирантов по дисциплине

Критерии оценки зачета	
«зачтено»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы. При ответе грамотно использует научную лексику, свободно ориентируется в материале курса. Аспирант успешно справляется с практическим заданием.
«не зачтено»	Ставится если, аспирант оказывается неспособным правильно раскрыть содержание основных понятий, плохо ориентируется в материале курса. Ответ содержит ряд серьезных неточностей. Аспирант не способен выполнить практическое задание.

7.5. Фонд оценочных средств

Содержание фонда оценочных средств: см. Приложение №1.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Основная литература

1. Сمارт, Н. Криптография / Н. Смарт ; С. А. Кулешов (пер. с англ.) ; С. К. Ландо (ред.). - М. : Техносфера, 2006. - 525 с.
2. Баричев, С. Г. Основы современной криптографии : Учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - Москва : Горячая линия-Телеком, 2001. - 120 с.
3. Владимиров, С. Н. Нелинейно-динамическая криптология : радиофизические и оптические системы / С. Н. Владимиров, И. В. Измайлов, Б. Н. Пойзнер ; ред. С. Н. Владимиров. - Москва : Физматлит, 2009. - 206 с.
4. Молдовян, Н. А. Введение в криптосистемы с открытым ключом / Молдовян Н. А., Молдовян А. А. - СПб. : БХВ-Петербург, 2005. - 286 с.
5. Мао, В. Современная криптография : теория и практика / Мао Венбо ; [пер. с англ. и ред. Д. А. Ключин]. - М. и др. : Вильямс, 2005. - 763 с.

8.2. Дополнительная литература

1. Рябко, Б. Я. Криптографические методы защиты информации : учеб. пособие для вузов / Б. Я. Рябко, А. Н. Фионов. - М. : Горячая линия - Телеком, 2005. - 226 с.
2. Зубов, А. Ю. Криптографические методы защиты информации. Совершенные шифры : учеб. пособие для вузов / А. Ю. Зубов. - М. : Гелиос АРВ, 2005. - 190 с.
3. Столлингс В. Криптография и защита сетей: Принципы и практика/ Столлингс В.; Пер. с англ. Сивак А.Г., Шпак А.А. - 2-е изд. - М.; СПб.; Киев:Вильямс,2001. - 669 с.
4. Баричев, С. Г. Основы современной криптографии : Учебный курс / С. Г. Баричев, В. В. Гончаров, Р. Е. Серов. - Москва : Горячая линия-Телеком, 2001. - 120 с.

8.3.

Интернет-ресурсы	
www.garant.ru	Базы данных, информационно-справочные и поисковые системы
http://biblioclub.ru	Университетская библиотека Online
http://www.elibrary.ru	Электронная библиотека
http://ndce.edu.ru	Каталог учебников, электронных ресурсов для высшего образования
http://edu.ru	Федеральный портал «Российское образование»
http://window.edu.ru	Портал «Единое окно доступа к образовательным ресурсам»
http://school.edu.ru	Российский общеобразовательный портал

http://www.enlight.ru/crypto/articles/shannon/shann_i.htm	Книга К. Шеннон «Теория связи в секретных системах»
http://cryptography.ru	Сайт МГУ «Математическая криптография»
http://www.youtube.com/watch?v=ZObsnutajAo	Лекция «Введение в криптографию»
http://webofknowledge.com	Библиографическая и реферативная база данных Web of Science
http://www.scopus.com/	Библиографическая и реферативная база данных Scopus

9. Перечень программного обеспечения

Mathematica, PGP, Криптограф, LaTeX, Word

10. Материально-техническое обеспечение дисциплины

Аудитории для проведения лекционных и практических занятий, мультимедийное оборудование, доска, доступ к Интернет-ресурсам.

Содержание фонда оценочных средств

Коллоквиум

Вопросы к коллоквиуму по дисциплине «Математические основы криптологии»:

1. Понятие криптологии. Криптография. Криптоанализ. Стеганография.
2. Шифр Цезаря. Шифр сцитала. Шифры Энея. Книжные шифры. N-граммное шифрование. Шифры подстановки. Шифры транспозиции.
3. Дисковые шифры. Блочное шифрование. Шифры Третимия. Многоалфавитное и блочное шифрование.
4. Шифры Виженера, Бофора, Вернаама. Гаммирование. Шифровальная машина «Энигма».
5. Понятие и свойства секретных систем. Критерии оценки секретных систем.
6. Совершенно секретные системы. Энтропия. Ненадежность. Примеры расшифровки энтропийным методом.
7. Экстремальные задачи. Выпуклый анализ. Экстремальные задачи в евклидовых пространствах. Линейное и выпуклое программирование. Задачи на минимум.
8. Криптографические протоколы. Примеры.
9. Протоколы открытого обмена ключами.
10. Протоколы аутентификации и электронной подписи.
11. Электронные деньги. Неотслеживаемость.
12. Протоколы разделения секрета. Примеры.

Критерии оценки коллоквиума

«зачтено»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы.
«не зачтено»	Ставится, если аспирант оказывается неспособным правильно раскрыть содержание основных понятий. Ответ содержит ряд серьезных неточностей. Аспирант не отвечает на дополнительные вопросы.

Собеседование

Тема №2. Алгебра секретных систем. Чистые шифры.

Операции над секретными системами. Взвешенное суммирование. Произведение. Ассоциативность операций. Эндоморфизм шифров. Множество шифров как алгебраическая система. Чистые и смешанные шифры. Свойства чистых шифров. Коммутирующие шифры. Остаточные классы сообщений и криптограмм. Метод характерных слов. Методы криптоанализа шифров транспозиции и Виженера.

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

Односторонние функции. Функции с секретом. Сложность алгоритмов. Идея секретных систем с открытым ключом. Система RSA. Разложение натурального числа на простые сомножители. Дискретное логарифмирование.

Критерии оценки собеседования

«зачтено»	Ставится, если аспирант строит ответ логично в соответствии с планом, обнаруживает глубокое знание теоретических вопросов. Уверенно отвечает на дополнительные вопросы. При ответе грамотно использует научную лексику, способен привести примеры, демонстрирующие эффективность теории.
«не зачтено»	Ставится, если аспирант оказывается неспособным правильно раскрыть содержание основных понятий. Ответ содержит ряд серьезных неточностей. Аспирант не отвечает на дополнительные вопросы и не ориентируется свободно в излагаемом материале.

Дискуссия

Темы дискуссий

1. Криптография и криптоанализ.
2. Криптография и стеганография.
3. Основные идеи древних шифров.
4. Криптография средневековья.
5. Дисковое шифрование.
6. Множество шифров как алгебраическая система.
7. Стойкость чистых шифров.
8. Основная задача криптоаналитика.
9. Можно ли создать абсолютно стойкий шифр?
10. Секретные системы с открытым ключом.
11. Стойкость асимметричных секретных систем.
12. Надежность электронной подписи.
13. Электронные деньги и неотслеживаемость.
14. Протоколы типа византийского соглашения.

Критерии оценки дискуссии:

«зачтено»	Ставится, если аспирант раскрывает тему дискуссии логично, обнаруживает глубокое знание темы. Уверенно отвечает на вопросы, грамотно обосновывает свою позицию. При ответе свободно и уверенно ориентируется в материале.
«не зачтено»	Ставится, если аспирант оказывается неспособным правильно раскрыть содержание основных понятий по теме дискуссии. Ответ содержит ряд серьезных неточностей. Аспирант не раскрывает тему дискуссии, не обосновывает свою позицию по теме дискуссии.

