Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Кафедра прикладной математики и компьютерных наук

ОДОБРЕНО:
Руководитель ОП
_____ Е.В. Соколов
(подпись)
«19» июня 2019 г.

Рабочая программа дисциплины
Алгебраическая криптография

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	02.03.02 Фундаментальная информатика и информационные технологии
Направленность (профиль) образовательной программы:	Фундаментальная информатика и информационные технологии

Иваново

1. Цели освоения дисциплины

подготовить бакалавров для научно-исследовательской деятельности в области алгебраической криптографии, а также в областях, использующих аппарат области алгебраической криптографии.

2. Место дисциплины в структуре ОП

Дисциплина входит в часть, формируемую участниками образовательных отношений.

Для освоения данной дисциплины обучающийся должен:

Знать: основные понятия, утверждения и методы алгебры и геометрии, языков программирования.

Уметь: решать типовые задачи алгебры и геометрии, языков программирования.

Иметь: практический опыт и навыки применения методов алгебры и геометрии, языков программирования.

Практики, для которых освоение данной дисциплины необходимо как предшествующее: производственная практика, практика по получению навыков применения компьютерных наук и информационных технологий в профессиональной деятельности.

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) профессиональные (ПК):

ПК-1: Способен применять в научно-исследовательской деятельности знания в области прикладной математики и (или) информационных технологий.

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

обладать расширенными знаниями, полученными в области алгебраической криптографии (ПК-1.1).

Уметь:

применять полученные в области алгебраической криптографии знания при решении стандартных задач в собственной научно-исследовательской деятельности (ПК-1.2).

Иметь практический опыт/Иметь навыки:

практический опыт научно-исследовательской деятельности в области алгебраической криптографии (ПК-1.3).

4. Объем и содержание дисциплины

Объем дисциплины составляет 4 зачетные единицы (144 академических часа).

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак.часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения) Формы промежуточной аттестации
			Занятия лекционного типа	Занятия семинарского типа	
1.	Криптография, основанная на группах.	7	12	10 лабор. занятие	Выступления на занятиях семинарского типа.
2.	Алгебраическое шифрование.	7	12	10 лабор. занятие	Выступления на занятиях семинарского типа.
3.	Анализ схем криптографии, основанной на группах.	7	12	12 лабор. занятие	Выступления на занятиях семинарского типа.
Итого за семестр:			36	32	Экзамен
Итого по дисциплине:			36	32	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

1. Криптография, основанная на группах.
   1.1. Платформы шифрования.
   1.2. Бесконечные группы и алгоритмические проблемы.
   1.3. Неразрешимые и трудноразрешимые алгоритмические проблемы как основа для построения криптографических схем.
2. Алгебраическое шифрование.
   2.1. Группы кос Артина.
3. Анализ схем криптографии, основанной на группах.
   3.1. Протоколы, базирующиеся на сопряжении.
   3.2. Протоколы, базирующиеся на умножениях.
   3.3. Протоколы, использующие автоморфизмы.

5. Образовательные технологии

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: технологии смешанного обучения, технология проблемного обучения.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Специфика компетентностно-ориентированного подхода, лежащего в основе действующих образовательных стандартов, обусловливает необходимость правильной и эффективной организации самостоятельной работы студентов. Для успешного изучения курса студентам следует не только посещать все лекционные занятия и занятия семинарского типа, но и как можно больше работать самостоятельно с учебниками, учебными и учебно-методическими пособиями, монографиями, научными журналами, сборниками статей, материалами конференций, в научных, в том числе электронных, библиотеках. В связи с этим студентам рекомендуется обратить особое внимание на список литературы по дисциплине. В нем указана учебная и научная литература, ресурсы Интернета, которые могут быть использованы как для подготовки к занятиям, так и при подготовке к итоговой отчетности по дисциплине.

Для эффективного формирования знаний, умений и навыков, предусмотренных программой курса, студентам важно правильно организовать подготовку к аудиторным занятиям.

Лекции – форма учебного занятия, цель которого состоит в рассмотрении теоретических вопросов излагаемой дисциплины в логически выдержанной форме. Весьма полезной для овладения материалом является «система опережающего чтения», когда студент предварительно про-

читывает по темам лекций материал, содержащийся в учебниках, учебных и учебно-методических пособиях, что позволяет более глубоко воспринимать лекции преподавателя. Поможет получить новые знания и систематизировать их составление студентами конспектов прочитанных работ в соответствии с содержанием программы и примерным перечнем контрольных вопросов. Это также существенно облегчит подготовку к аттестации по дисциплине.

Занятия семинарского типа – групповая форма занятий, проходящих при активном участии студентов. Они способствуют углублённому изучению наиболее сложных вопросов дисциплины и служат основной формой подведения итогов самостоятельной работы студентов. На этих занятиях студенты учатся грамотно излагать проблемы, свободно высказывать свои мысли и суждения, вести полемику, убеждать, доказывать, опровергать, отстаивать свои убеждения, рассматривают ситуации, способствующие развитию профессиональной компетентности. Умение выступать перед аудиторией и грамотно обосновывать свою позицию – необходимые навыки. Занятия семинарского типа призваны не только углубить и закрепить теоретические знания студентов, но и научить пользоваться этими знаниями на практике. На занятия семинарского типа выносятся наиболее важные и сложные для изучения темы курса. Качество самостоятельной работы студентов проверяется преподавателем во время занятий семинарского типа путем проведения устного опроса.

Для организации самостоятельной работы студентов по освоению учебного материала практикуется выдача студентам учебной литературы (см. список литературы) и методических указаний (см. приложение 1 к данной РП) в текстовой или электронной форме. Для самоконтроля и подготовки студентов к итоговой отчетности по дисциплине выдается список вопросов.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Форма отчетности по данной дисциплине – экзамен. Экзамен проводится в устной форме. К нему допускаются все студенты.

Все студенты отвечают на вопросы из билета. В билет входят 2 теоретических вопроса. Ответ на каждый из вопросов оценивается максимально до 5 баллов. Итоговый результат за ответ определяется как среднее арифметическое между полученными им баллами за ответы на теоретические вопросы (при необходимости используется округление до ближайшего целого числа). Оценка «отлично» выставляется студенту, если среднее арифметическое (или его округление до целого) между полученными студентом баллами за ответы на теоретические вопросы равно 5. Оценка «хорошо» выставляется студенту, если среднее арифметическое (или его округление до целого) между полученными студентом баллами за ответы на теоретические вопросы равно 4. Оценка «удовлетворительно» выставляется студенту, если среднее арифметическое (или его округление до целого) между полученными студентом баллами за ответы на теоретические вопросы равно 3. Оценка «неудовлетворительно» выставляется студенту, если среднее арифметическое (или его округление до целого) между полученными студентом баллами за ответы на теоретические вопросы равно 2.

Итоговой оценкой по дисциплине служит оценка за экзамен.

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Алгебраические структуры и их приложения / Л.В. Зяблицева, С.Ю. Корабельщикова, И.В. Кузнецова, С.А. Тихомиров ; Министерство образования и науки Российской Федерации, Северный (Арктический) федеральный университет имени М.В. Ломоносова. – Архангельск : САФУ, 2015. – 169 с. : ил., табл. – Режим доступа: по подписке. – URL:

http://biblioclub.ru/index.php?page=book&id=436142 (дата обращения: 30.06.2019). – Библиогр. в кн. – ISBN 978-5-261-01074-6. – Текст : электронный.

2. Басалова, Г.В. Основы криптографии / Г.В. Басалова ; Национальный Открытый Университет 'ИНТУИТ'. – Москва : Интернет-Университет Информационных Технологий, 2011. – 253 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=233689 (дата обращения: 30.06.2019). – Текст : электронный.

Дополнительная литература:

1. Гультяева, Т.А. Основы теории информации и криптографии / Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. – Новосибирск : НГТУ, 2010. – 88 с. : табл., схем. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=228963 (дата обращения: 30.06.2019). – ISBN 978-5-7782-1425-5. – Текст : электронный.

2. Туганбаев, А.А. Линейная алгебра / А.А. Туганбаев. – 2-е изд., стер. – Москва : Издательство «Флинта», 2017. – 75 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=115141 (дата обращения: 30.06.2019). – ISBN 978-5-9765-1407-2. – Текст : электронный.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет» https://uni.ivanovo.ac.ru

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru

Электронная библиотека ИвГУ http://lib.ivanovo.ac.ru

Электронный каталог НБ ИвГУ http://lib.ivanovo.ac.ru/index.php/ek

Программное обеспечение: операционная система Windows, офисный пакет Microsoft Office и(или) LibreOffice, Интернет-браузер Internet Explorer и(или) Microsoft Edge и(или) Yandex Browser, кроссплатформенная среда разработки Code::Blocks.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации.

Основная профессиональная образовательная программа
02.03.02 Фундаментальная информатика и информационные технологии
(Фундаментальная информатика и информационные технологии)

Автор(ы) рабочей программы дисциплины: доцент кафедры прикладной математики и компьютерных наук, канд. физ.-мат. наук, доцент Туманова Е. А.

Программа рассмотрена и утверждена на заседании кафедры прикладной математики и компьютерных наук

«13» июня 2019 г., протокол № 11

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ _____
(подпись)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ _____
(подпись)

Программа обновлена
протокол заседания кафедры № _____ от «_____» _____20 __ г.
Согласовано:
Руководитель ОП _____ _____
(подпись)