МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Волгоградский государственный социально-педагогический университет»
Факультет математики, информатики и физики
Кафедра алгебры, геометрии и математического анализа

«УТВЕРЖДАЮ»
Проректор по учебной работе
_____ Ю. А. Жадаев
« 29 » августа 2016 г.

Введение в криптографию

Программа учебной дисциплины

Направление 44.04.01 «Педагогическое образование»

Магистерская программа «Математическое образование»

очная форма обучения

Волгоград
2016

Обсуждена на заседании кафедры алгебры, геометрии и математического анализа
« 31 » 05 2016 г., протокол № 10

Заведующий кафедрой _____ В.К.Карташов « 31 » 05 2016 г.
(подпись) (зав. кафедрой) (дата)

Рассмотрена и одобрена на заседании учёного совета факультета математики, информатики и физики « 30 » 06 2016 г. , протокол № 12

Председатель учёного совета Смыковская Т.К. _____ « 30 » 06 2016 г.
(подпись) (дата)

Утверждена на заседании учёного совета ФГБОУ ВО «ВГСПУ»
« 29 » 08 2016 г. , протокол № 1

Отметки о внесении изменений в программу:

Лист изменений № 1 _____ Карташов ВК 01.09.2017
(подпись) (руководитель ОПОП) (дата)

Лист изменений № _____ _____ _____ _____
(подпись) (руководитель ОПОП) (дата)

Лист изменений № _____ _____ _____ _____
(подпись) (руководитель ОПОП) (дата)

Разработчики:
Карташова Анна Владимировна, кандидат физико-математических наук, доцент кафедры алгебры, геометрии и математического анализа ФГБОУ ВО «ВГСПУ».

Программа дисциплины «Введение в криптографию» соответствует требованиям ФГОС ВО по направлению подготовки 44.04.01 «Педагогическое образование» (утверждён приказом Министерства образования и науки Российской Федерации от 21 ноября 2014 г. № 1505) и базовому учебному плану по направлению подготовки 44.04.01 «Педагогическое образование» (магистерская программа «Математическое образование»), утверждённому Учёным советом ФГБОУ ВПО «ВГСПУ» (от 30 марта 2015 г., протокол № 8).

1. Цель освоения дисциплины

Сформировать систематизированные знания в области криптографии.

2. Место дисциплины в структуре ОПОП

Дисциплина «Введение в криптографию» относится к вариативной части блока дисциплин и является дисциплиной по выбору.

Для освоения дисциплины «Введение в криптографию» обучающиеся используют знания, умения, способы деятельности и установки, сформированные в ходе изучения дисциплин «Введение в теорию колец и модулей», «Графы и их приложения», «Исследование операций», «Логические вопросы алгебры», «Преподавание математики в учреждениях профессионального образования», «Проектирование содержания математических дисциплин в профессиональном образовании», «Теория алгебраических систем», «Теория групп», «Теория решеток», прохождения практики «Практика по получению профессиональных умений и опыта профессиональной деятельности (Педагогическая)».

3. Планируемые результаты обучения

В результате освоения дисциплины выпускник должен обладать следующими компетенциями:

– способностью проводить самостоятельные научные исследования по одному или нескольким направлениям универсальной алгебры, теории чисел, дискретной математики и их приложениям; внедрять в образовательный процесс полученные результаты собственных исследований или наиболее значимые результаты по направлениям, близким к научным интересам магистранта (СК-1).

В результате изучения дисциплины обучающийся должен:

знать
– основные принципы работы симметричных криптосистем;
– основные принципы работы асимметричных криптосистем;

уметь
– шифровать и дешифровать сообщения в симметричных криптосистемах;
– шифровать и дешифровать сообщения в криптосистемах с открытым ключом;

владеть
– навыками реализации алгоритмов шифрования и дешифрования сообщений в классических симметричных криптосистемах;
– навыками реализации алгоритмов шифрования и дешифрования сообщений в криптосистемах рюкзака и RSA.

4. Объём дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Семестры
		4
Аудиторные занятия (всего)	30	30

В том числе:		
Лекции (Л)	–	–
Практические занятия (ПЗ)	30	30
Лабораторные работы (ЛР)	–	–
Самостоятельная работа	114	114
Контроль	–	–
Вид промежуточной аттестации		ЗЧ
Общая трудоемкость часы	144	144
зачётные единицы	4	4

5. Содержание дисциплины

5.1. Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Симметричные криптосистемы	Предмет и задачи криптографии. Понятие открытого и шифрованного текста, ключа, криптосистемы. Классические криптосистемы. Шифр атбаш, шифр Сцитала, табличка Энея, шифр Цезаря, шифровальные диски, шифр Тритемия. Шифры гаммирования. Шифр Вижинера. Одноразовый щит (шифр Вернама), шифр Плэйфера. Шифрующие матрицы. Шифры перестановок. Примеры блочных и поточных шифров.
2	Криптография с открытым ключом	Суть криптографии с открытыми ключом. Общая структура криптосистем с открытыми ключами. Конфиденциальность и цифровая подпись в криптосистемах с открытыми ключами. Примеры криптосистем с открытыми ключами. Система, основанная на методе RSA

5.2. Количество часов и виды учебных занятий по разделам дисциплины

№ п/п	Наименование раздела дисциплины	Лекц.	Практ. зан.	Лаб. зан.	СРС	**Всего**
1	Симметричные криптосистемы	–	16	–	74	90
2	Криптография с открытым ключом	–	14	–	40	54

6. Перечень основной и дополнительной учебной литературы

6.1. Основная литература

1. Басалова Г.В. Основы криптографии [Электронный ресурс]/ Басалова Г.В.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 282 с.— Режим доступа: http://www.iprbookshop.ru/52158.html.— ЭБС «IPRbooks».

6.2. Дополнительная литература

1. Гультяева Т.А. Основы теории информации и криптографии [Электронный ресурс]: конспект лекций/ Гультяева Т.А.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2010.— 88 с.— Режим доступа:

http://www.iprbookshop.ru/44987.html.— ЭБС «IPRbooks».
2. Зомор Ж. Курс криптографии [Электронный ресурс]/ Зомор Ж.— Электрон. текстовые данные.— Москва, Ижевск: Регулярная и хаотическая динамика, Ижевский институт компьютерных исследований, 2006.— 256 с.— Режим доступа: http://www.iprbookshop.ru/16547.html.— ЭБС «IPRbooks».

7. Ресурсы Интернета

Перечень ресурсов Интернета, необходимых для освоения дисциплины:

1. Информационно-поисковая и вычислительная система WolframAlpha. – URL: http://www.wolframalpha.com.
2. Википедия – свободная энциклопедия. – URL: http://ru.wikipedia.org и http://en.wikipedia.org.
3. Электронная библиотечная система IPRbooks (http://www.iprbookshop.ru).

8. Информационные технологии и программное обеспечение

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости):

1. Офисный пакет Open Office.

9. Материально-техническая база

Для проведения учебных занятий по дисциплине «Введение в криптографию» необходимо следующее материально-техническое обеспечение:

1. Аудитория с мультимедийной поддержкой для проведения учебных занятий.
2. Аудитория для проведения самостоятельной работы студентов с доступом к сети Интернет.

10. Методические указания для обучающихся по освоению дисциплины

Дисциплина «Введение в криптографию» относится к вариативной части блока дисциплин и является дисциплиной по выбору. Программой дисциплины предусмотрено проведение практических занятий. Промежуточная аттестация проводится в форме зачета.

Практические занятия являются формой организации педагогического процесса, направленной на углубление научно-теоретических знаний и овладение методами работы, в процессе которых вырабатываются умения и навыки выполнения учебных действий в сфере изучаемой науки. Практические занятия предполагают детальное изучение обучающимися отдельных теоретических положений учебной дисциплины. В ходе практических занятий формируются умения и навыки практического применения теоретических знаний в конкретных ситуациях путем выполнения поставленных задач, развивается научное мышление и речь, осуществляется контроль учебных достижений обучающихся.

При подготовке к практическим занятиям необходимо ознакомиться с теоретическим материалом дисциплины по изучаемым темам – разобрать конспекты лекций, изучить литературу, рекомендованную преподавателем. Во время самого занятия рекомендуется активно участвовать в выполнении поставленных заданий, задавать вопросы, принимать участие в дискуссиях, аккуратно и своевременно выполнять контрольные задания.

Контроль за качеством обучения и ходом освоения дисциплины осуществляется на основе рейтинговой системы текущего контроля успеваемости и промежуточной аттестации студентов. Рейтинговая система предполагает 100-балльную оценку успеваемости студента по учебной дисциплине в течение семестра, 60 из которых отводится на текущий контроль, а

40 – на промежуточную аттестацию по дисциплине. Критериальная база рейтинговой оценки, типовые контрольные задания, а также методические материалы по их применению описаны в фонде оценочных средств по дисциплине, являющемся приложением к данной программе.

11. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является неотъемлемой частью процесса обучения в вузе. Правильная организация самостоятельной работы позволяет обучающимся развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, способствует формированию навыков совершенствования профессионального мастерства.

Самостоятельная работа обучающихся во внеаудиторное время включает в себя подготовку к аудиторным занятиям, а также изучение отдельных тем, расширяющих и углубляющих представления обучающихся по разделам изучаемой дисциплины. Такая работа может предполагать проработку теоретического материала, работу с научной литературой, выполнение практических заданий, подготовку ко всем видам контрольных испытаний, выполнение творческих работ.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине представлено в рабочей программе и включает в себя:

– рекомендуемую основную и дополнительную литературу;

– информационно-справочные и образовательные ресурсы Интернета;

– оценочные средства для проведения текущего контроля и промежуточной аттестации по дисциплине.

Конкретные рекомендации по планированию и проведению самостоятельной работы по дисциплине «Введение в криптографию» представлены в методических указаниях для обучающихся, а также в методических материалах фондов оценочных средств.

12. Фонд оценочных средств

Фонд оценочных средств, включающий перечень компетенций с указанием этапов их формирования, описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания, типовые контрольные задания и методические материалы является приложением к программе учебной дисциплины.