ВВЕДЕНИЕ В КРИПТОГРАФИЮ

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. Общая трудоёмкость дисциплины и её распределение

количество зачётных единиц – 4,
общая трудоёмкость дисциплины в часах – 144 ч. (в т. ч. аудиторных часов – 30 ч., СРС – 114 ч.),
распределение по семестрам – 4,
форма и место отчётности – зачёт (4 семестр).

5. Краткое содержание дисциплины

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.

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

6. Разработчик

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