СОДЕРЖАНИЕ И МЕТОДИКА ПОСТРОЕНИЯ КУРСА «МЕТОДЫ АЛГЕБРАИЧЕСКОЙ ГЕОМЕТРИИ В КРИПТОГРАФИИ» ДЛЯ СТУДЕНТОВ СПЕЦИАЛЬНОСТИ 090301.65 «КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ»

Отрыванкина Т.М., Фомина Т.А.
Оренбургский государственный университет, г. Оренбург

Получение высшего образования в современном мире предполагает самостоятельный выбор студентом образовательной траектории в соответствии с интересами, желаниями, профессиональными потребностями. Учебные планы специальностей и направлений бакалавриата содержат в том или ином количестве курсы по выбору, которые призваны расширить, углубить общие или профессиональные познания студента и развить его профессиональные компетенции. Целесообразно делать перечень спецкурсов как можно более широким для того, чтобы заинтересованные в повышении уровня и качества образования студенты могли реализовать свои потребности.

Анализ основной образовательной программы и учебного плана по специальности 090301 Компьютерная безопасность, показал, что имеет смысл рассмотреть дисциплину «Методы алгебраической геометрии в криптографии» в качестве дисциплины по выбору в подготовке студентов данной специальности. Этот курс, имея разносторонние связи со всеми основными и специальными математическими дисциплинами, будет базироваться на обязательных для изучения дисциплинах: «Алгебра», «Геометрия», «Теоретико-числовые методы в криптографии», «Криптографические протоколы», «Криптографические методы защиты информации». По этой причине считаем целесообразным изучение данной дисциплины на 4 курсе в 8 семестре. Знания и навыки, приобретенные в результате изучения данного курса, дополнят, углубят и расширят знания, накопленные при изучении дисциплин профессионального цикла.

Включение дисциплины в список изучаемых требует составления рабочей программы. Для этого необходима проработка содержания курса и разработка его методического обеспечения [3].

Мы видим цель учебной дисциплины «Методы алгебраической геометрии в криптографии» в развитии и совершенствовании у обучающихся следующих профессионально-специальных компетенций:

- способности ориентироваться в современных и перспективных математических методах защиты информации, оценивать возможность и эффективность их применения в конкретных задачах защиты информации [1, 13];
- способности моделировать алгоритмы в системах компьютерной математики, оценивать их работоспособность и эффективность [1, 14];
- способности на основе анализа применяемых математических методов и алгоритмов оценить эффективность средств защиты информации [1, 14].

В результате изучения дисциплины, обучающиеся будут: знать принципы применения эллиптических и гиперэллиптических кривых в криптографии; уметь проводить предварительное оценивание временной сложности разрабатываемых алгоритмов; владеть навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых, использования систем компьютерной математики для решения профессиональных задач; методами построения быстрых вычислительных алгоритмов алгебры и теории чисел [3].

Предполагаемая общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа). Примерное содержание дисциплины может включать следующие разделы (некоторые – на уровне повторения) :

1. Алгебраические основы: Поля, подполя. Простые поля. Характеристика поля. Расширения полей. Их строение. Расширения конечной степени. Теорема о башне полей для расширений конечной степени. Алгебраические и трансцендентные элементы поля относительно его подполя. Минимальный полином алгебраического элемента, некоторые его свойства. Строение расширения поля, полученное присоединением алгебраического элемента. Алгебраические расширения полей. Теорема о башне полей для алгебраических расширений. Конечные поля. Теорема о числе элементов конечного поля. Цикличность мультипликативной группы конечного поля. Дискретное логарифмирование в циклической группе. Автоморфизм Фробениуса. Группа автоморфизмов конечного поля.

Неприводимые полиномы над конечными полями, некоторые их свойства. Число неприводимых полиномов данной степени над конечным полем с данным числом элементов. Реализация основных операций конечного поля: сложение, умножение, возведение в степень, обращение. Алгебраическое замыкание поля. Теорема о существовании алгебраического замыкания счетного поля.

2. Эллиптические кривые: Алгебраические и эллиптические кривые. Дискриминант и инвариант эллиптической кривой. Группа точек эллиптической кривой. Эллиптические кривые над полями действительных и рациональных чисел. Эллиптические кривые над полем комплексных чисел. Эллиптические кривые над конечными полями. Точки конечного порядка. Порядок эллиптической кривой. Неравенство Хассе и его применение.

3. Некоторые приложения эллиптических кривых в криптографии: Проверка чисел на простоту при помощи эллиптических кривых. Разложение чисел на простые множители при помощи эллиптических кривых.

Некоторые протоколы эллиптической криптографии. Распределение ключей по протоколу Диффи-Хеллмана. Распределение ключей по протоколу Massey-Omura. Использование группы точек эллиптической кривой. Протокол распределения ключей Менезеса-Кью-Ватсона (MQV-протокол).

Электронная подпись Эль-Гамаля и ее обобщения. Схема электронной подписи Эль Гамаля с возвратом сообщения (Nyberg-Rueppel-алгоритм) с использованием группы точек эллиптической кривой.

Реализация курса предполагает комбинирование лекций, практических занятий, лабораторных работ и различных форм самостоятельной работы студентов.

Выбирая наиболее подходящие интерактивные методы и технологии обучения для реализации данной программы, можно остановиться на следующих: лекция-визуализация; лекция-диалог; проблемная лекция; работа в малых группах; выполнение индивидуальных заданий в рамках внеаудиторной работы.

Список литературы

1. *Федеральный государственный образовательный стандарт высшего профессионального образования по специальности 090301 Компьютерная безопасность. Утвержден приказом Минобрнауки РФ от 17 января 2011 №69 [Электронный ресурс]: Оренбургский государственный университет, 1999-2012. – Режим доступа: http://www.osu.ru/doc/2436 – 10.12.2012*

2. ***Фомина, Т.А.*** *Роль математического образования в формировании профессиональных компетенций специалистов в области компьютерной безопасности [Электронный ресурс] / Т.А. Фомина // Университетский комплекс как региональный центр образования, науки и культуры: материалы Всероссийской научно-методической конференции, 30 января – 1 февраля 2013г. / Оренбургский гос. ун-т. — Оренбург: ООО ИПК «Университет», 2013. - С.1297-1299.*

3. ***Фомина, Т.А.*** *Дисциплина «Методы алгебраической геометрии в криптографии» в профессиональной подготовке студентов специальности 090301 Компьютерная безопасность / Т.А. Фомина // Наука, образование, общество: проблемы и перспективы развития: материалы международной заочной научно-практической конференции, 29 марта 2013г.: тез. докл. / - Тамбов: Изд-во ТРОО «Бизнес-наука-общество». – Часть 7. – С. 139-140.*