Программа спецкурса ЦИФРОВЫЕ ТЕХНОЛОГИИ,

1/2 года, для студентов 1-2 курсов

Специальный курс **Цифровые технологии** будет читаться в течение весеннего семестра, один раз в неделю. Цифровые технологии, возникли сравнительно недавно, в связи с образовавшимися потребностями, и переживают сейчас период становления, они широко обсуждаются, некоторые уже используются, а другие в ближайшее время получат широкое распространение. Деятельность в этой области направлена на создание информации и механизмов её обработки, безопасного хранения и передачи, а в роли инструментов выступают математические алгоритмы, основанные на методах теории чисел, алгебры, дискретной математики. Важную часть цифровых технологий составляет криптография.

Примером таких технологий может служить вопрос, как организовать систему удалённого голосования, с соблюдением некоторых требований: голоса без изменения должны быть переданы по обычным каналам сети Интернет в центральный компьютер; в голосовании могли участвовать только допущенные к этому лица; ни комиссия по проведению выборов, ни участники голосования, ни любые посторонние люди не могли узнать, кто из потенциальных участников голосования и как проголосовал; результаты голосования никому не должны быть известны до окончания голосования и подведения итогов и т.п. Опишем подробнее содержание курса.

1. **Алгоритмы и сложность.**

Алгоритм Евклида и теорема Ламе о сложности этого алгоритма. Быстрый алгоритм возведения в степень. Быстрое умножение целых чисел. Вероятностные алгоритмы и их сложность. Вероятностные методы отсеивания составных чисел. Доказательство простоты чисел. Построение больших простых чисел. Задача разложения целых чисел на множители. Дискретное логарифмирование. Эллиптические кривые над конечными полями, их применения.

1. **Криптографические примитивы.**

Псевдослучайные последовательности чисел. Алгоритм обмена ключами. Алгоритм шифрования RSA. Простейшие булевы функции. Хеш-функции. Алгоритм хеширования SHA-256.Основные алгоритмы шифрования с открытым ключом. Криптосистема Эль-Гамаля. Криптосистема Рабина.

1. **Информационные технологии.**

Электронная подпись. Электронная подпись с помощью эллиптических кривых. Схемы обязательств. Подбрасывание монеты по телефону. Подтверждение выбора (доказательство с нулевым разглашением). Разделение секрета. Протокол аутентификации. Система электронного голосования. Технологии блокчейн. Криптовалюта.