**Введение.**

Мой реферат посвящен такой немаловажной теме, как история развития криптографии. Зародившись еще примерно в третьем тысячелетии до нашей эры, она развивалась, проходя множество этапов, что позволило ей находиться на том уровне, в котором мы привыкли видеть ее сегодня. Криптография – наука, позволяющая сохранить аутентичность и конфиденциальность информации – является неотъемлемой и необходимой частью нашей повседневной жизни. Для засекречивания данных криптография использует ключи – секретную информацию, позволяющую шифровать/дешифровать информацию в криптографическом алгоритме.

Из-за высокой востребованности в наши дни, криптография постоянно развивается, модернизируется, и, как следствие, сильно отличается от той, что существовала в древности. Тем не менее, с течением времени основная цель криптографии осталось той же: защитить информацию от прочтения нежелательными получателями и обеспечить ей возможность быть правильно интерпретированной по достижению цели. Особенно сильный скачок в развитии данной науки произошел с появлением первых ЭВМ. Если алгоритмы, написанные человеком, еще можно было дешифровать без использования ключа, даже потратив на это огромное количество времени и средств, то из-за сложности современных алгоритмов, осуществляемых машинами, утраченный ключ может привести к невозможности расшифровки информации.

На данный момент история насчитывает четыре основные периода развития криптографии. В первом из них преобладает принцип моноалфавитного шифрования, заключающийся в замене одних мелких единиц языка, как слово или буква, другими. Во втором люди применяли полиалфавитный шифр, заключающийся в циклическом использовании моноалфавитного. Третий период появился благодаря началу использования электромеханических устройств, при этом шифр так и остался полиалфавитным. В течении этих трех периодов использовалась криптография с закрытым ключом. В четвертом же периоде появилась криптография с использованием открытого ключа.

Проблемой моего реферата является то, что многие люди, пользуясь различными методами шифрования каждый день, не осознают значимость такой науки как криптография и не догадываются о ее богатой истории. Поэтому моей целью является ознакомление с понятием «криптография» в целом и изучение прогресса в ее развитии. Для достижения данной цели мне понадобится выполнить ряд задач:

* Ознакомиться с литературой по теме шифрования данных;
* Разобраться с основами криптографии;
* Подробно изучить историю криптографии;
* Разбить ее на 3 этапа;
* Законспектировать полученные мной результаты в реферат.

При написании данного реферата я планирую собирать данные из различных источников информации. Основными для меня будут такие книги, как:

* "История криптографии. Часть I" А.В. Бабаш, Г.П. Шанкин
* "Книга шифров. Тайная история шифров и их расшифровки" Сингх С.
* "Криптография от папируса до компьютера" Жельников В.

Остальные же послужат дополнительными источниками, направленными на подтверждение полученных сведений и углубление познаний в теме.