Усовершенствование алгоритма шифрования текстовых сообщений основанного на полиалфавитном методе

Голубничий Артем Александрович
ассистент кафедры инженерной экологии и основ производства Хакасского государственного университета им. Н.Ф. Катанова
E-mail: artem@golubnichij.ru
Тюкалов Павел Александрович
студент кафедры программного обеспечения вычислительной техники и автоматизированных систем Хакасского государственного университета им. Н.Ф. Катанова
E-mail: ajibtopuyc@mail.ru
Литюк Татьяна Сергеевна
студентка кафедры инженерной экологии и основ производства Хакасского государственного университета им. Н.Ф. Катанова
E-mail: tskotya@mail.ru

В связи с широким распространением глобальных компьютерных сетей, все более актуальной становится проблема защиты информации [1]. Основой защиты информации – является ее тайная передача.

Все методы тайной передачи информации относительно способов передачи информации и выбора типа канала связи можно разделить на три категории [2]:

1. Создание абсолютно надежных и недоступных для других пользователей каналов связи;

2. Использование общедоступных каналов связи, но при скрытии самого факта передачи информации (стенография);

3. Использование общедоступных каналов связи, но передачи по нему информации в таком преобразованном виде, что восстановление ее может осуществить только получатель.

Выбор того или иного метода осуществляется, как правило, при ответе на следующие вопросы:

1) является ли информация более ценной для противника, чем стоимость ее атаки?;

2) является ли информация более ценной, чем затраты на ее защиту? [2].

Наиболее оптимальным с точки зрения материальных затрат, с учетом того, что передаваемая информация не обладает особой важностью, является способ передачи основанный на преобразовании информации в такой вид при котором осуществить ее чтение может только получатель.

Системы защиты информации (СЗИ), характеризуются тем, что не существует однозначных тестов, позволяющих убедится в их стойкости. Задача определения эффективности СЗИ при использовании криптографических методов защиты зачастую более трудоемкая, чем разработка самих СЗИ [3].

Выбор полиалфавитного метода шифрования обусловлен одним из самых основных методов криптоанализа – вскрытие с помощью метода частотного анализа (основывающегося на предположении о существовании нетривиального статистического распределения отдельных символов и их последовательностей, как в открытом тексте, так и в шифротексте, которое, с точностью до замены символов, будет сохраняться в процессе шифрования и дешифрования) [2].

В ходе работы был разработан алгоритм полиалфавитного метода шифрования. Основой для применения данного алгоритма шифрования является квадратная сетка, размер которой задается произвольно с учетом требования о минимальном значении ячеек (общее количество ячеек должно быть не меньше чем размерность алфавита умноженная на два).

Алгоритм шифрования включает следующие этапы:

1. Символы алфавита записываются слева на право, при записи последнего символа, запись алфавита начинается сначала, пока не закончится сетка.

2. Выбирается «начальный алфавит» и производится смещение по горизонтали и вертикали на n ячеек.

В отличии от ранее разработанных алгоритмов полиалфавитного метода [4, с 61] предлагается усложнить алгоритм следующим способом: направление смещения для каждого символа алфавита задается случайно. Тем самым сложность вскрытия шифра будет увеличена за счет случайности замены

символов. Т.е. даже если злоумышленник знает алгоритм, из-за случайности замены символов время на вскрытие шифра может значительно увеличится. Увеличение времени напрямую зависит от хаотичности замены символов, чем хаотичнее замена, тем больше времени потребуется на вскрытие шифра.

Список литературы

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум [Текст] учеб. пособие/ А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников.- М.: КНОРУС, 2012.-136с
2. Ященко В.В. Введение в криптографию [Текст]: учеб. пособие/ под ред. В.В Ященко – М.: МЦНМО, 2001.-288с
3. Авдошин С.М. Криптоанализ: современное состояние и перспективы развития./ С.М. Авдошин, А.А. Савельева. Приложение к журналу «Информационные технологии». – 03/2007. – N3.
4. Тюкалов П.А. Разработка алгоритма шифрования текстовых сообщений многоалфавитным методом/ П.А. Тюкалов. Материалы 50-й международной студенческой научной конференции «Студент и научно-технический прогресс»// Новосибирский государственный университет. – Новосибирск: Изд-во НГУ, 2012. – С. 61.