Козырева Е.С.
Научный руководитель: к.т.н., инженер вычислительного центра А. В. Астафьев
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
E-mail: elena.kozireva666@yandex.ru

Разработка алгоритма шифрования текста

Вопрос защиты ценной информации путем ее видоизменения, исключающего ее прочтение незнакомым лицом тревожила лучшие человеческие умы еще с самых древних времён. История шифрования - почти что ровесница истории человеческой речи. Кроме того, изначально письмо само по себе было криптографической системой, поскольку в древних обществах подобным знанием обладали лишь избранные. Священные манускрипты различных древних государств тому примеры[2].

Понятие "Безопасность" охватывает широкий круг интересов как отдельных лиц, так и целых государств. В наше мобильное время видное место отводится проблеме информированной безопасности, обеспечению защиты конфиденциальной информации от ознакомления с ней конкурирующих групп[1].

Целью работы является разработка алгоритма шифрования текста.

Для достижения цели были поставлены следующие задачи:

– разработать свой код шифрования текста;
– выявить недостатки существующих алгоритмов (таблица 1).

Итак шифр Елены – представляет собой матрицу 6х5, столбцы и строки которого нумеруются цифрами от 1 до 5 и 6 соответственно. В каждую клетку этого квадрата записывается одна буква. Буквы расположены в алфавитном порядке. В результате каждой букве соответствует пара чисел, и шифрованное сообщение превращается в последовательность пар чисел. Расшифровывается путём нахождения буквы, стоящей на пересечении строки и столбца.

Сравним три существующих алгоритма и разработанный шифр.

Таблица 1 – Сравнение существующих программ-аналогов

Название	Криптостойкость	Процедура расшифрования	Удобный в использование
Цезарь	-	+	+
Атбаш	-	-	+
АзбукаМорзе	-	+	-
Елена	+	+	+

Проанализировав криптографическую устойчивость трех существующих шифров и разработанного, пришли к выводу, что самый лучший идеальный вариант по всем пунктам: шифр Елены.

Все поставленные цели были выполнены путем решения всех указанных задач.

Литература

1. Бабаш А. В. “Криптографические и теоретико – автоматные аспекты современной защиты информации.” Учебно-методическое пособие. Издательский центр «ЕАОИ» 2011 г , 215 стр.

2. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2012.