СПИСОК ЛИТЕРАТУРЫ

1. Лєбєдєва І. Ю. Інформаційні технології та їх вплив на сучасні організації [Електронний ресурс] / І. Ю. Лєбєдєва, М. М. Черненко. – Режим доступу: http://nauka.kushnir.mk.ua/?p=69459.

2. Бузак Н. І. Економічна оцінка інформаційних технологій / Н. І. Бузак // Вісник ЖДТУ. – 2010. – № 3(53). – С. 29–32.

3. Поливана Л. А. Методичні підходи до оцінки ефективності проекту впровадження інформаційних технологій на підприємствах торгівлі [Електронний ресурс] / Л. А. Поливана // Вісник Харківського національного технічного університету сільського господарства імені Петра Василенка. – 2014. – Вип. 149. – С. 247–259. – Режим доступу: http://nbuv.gov.ua/UJRN/Vkhdtusg_2014_149_38.

4. Палагута К. О. Мовна модель сучасного інформаційного простору : навч. посіб. для студ. екон. напрямів підг. ден. та заоч. форм навч. – Донецьк : [ДонНУЕТ], 2010. – 270 с.

5. Євдокимов В. В. Аналіз економічної ефективності впровадження бухгалтерських інформаційних систем [Електронний ресурс] / В. В. Євдокимов, Д. Л. Лозинський. – Режим доступу: http://www.nbuv.gov.ua.

6. Экономическая эффективность информационных систем / К. Г. Скрипкин. – М. : ДМК Пресс, 2002. – 256 с.

7. Анисифоров А. Б. Методики оценки эффективности информационных систем и информационных технологий в бизнесе [Электронный ресурс] : учеб. пособ. / А. Б. Анисифоров, Л. О. Анисифорова. – СПб, 2014. – 97 с.

8. Савенко Р. Г. Ефективність інформаційних систем : навч. посіб. / Р. Г. Савенко, М. В. Лисенко. – Полтава : ПНТУ, 2007 р. – 166 с.

9. Автоматизированные информационные технологии в экономике : учеб. / М. И. Семенов, И. Т. Трубилин, В. И. Лойко, Т. П. Барановская ; под общ. ред. И. Т. Трубилина. – М. : Финансы и статистика, 2000. – 416 с.

10. Волков А. С. Инвестиционные проекты: от моделирования до реализации [Текст] / А. С. Волков. – М. : Вершина, 2006. – 256 с.

11. Леоненков А. В. Самоучитель UML / А. В. Леоненков. – 2-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2004. – 432 с.

ПРИМЕНЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ГЕНЕРАТОРА «СХЕМА ЧУА» ДЛЯ ШИФРОВАНИЯ ДАННЫХ

Левицкая Т. А.
ГВУЗ «ПГТУ», г. Мариуполь

При постоянном росте вычислительных возможностей современных технических средств, вопрос усовершенствования вычислительно стойких криптосистем становится всё более острым. Проблема возможного перехвата и расшифровки, подмены или порчи данных, имеет различные методы своего решения. Шифрование передаваемых данных является одним из методов защиты от атак злоумышленников и непредсказуемости среды и позволяет подтвердить их целостность, обеспечить конфиденциальность и доступность информации для конечного получателя.

В ходе анализа проблем существующих криптосистем, становится очевидным, что с ростом вычислительных мощностей современных компьютеров криптостойкость вычислительно стойких алгоритмов падает [1]. Однако благодаря этому же росту мощностей становится возможной реали-

зация алгоритмов, которые могут быть приближённо сравнимы по надёжности с абсолютно стойкими криптосистемами. Одним из таковых решений является использование модели какого-либо сложного непрерывного физического процесса в качестве генератора шифрующей последовательности. Частным случаем такого процесса являются различные генераторы хаоса. Криптосистемы на генераторах хаоса обладают рядом преимуществ над симметричными системами и системами с открытым ключом (последние при шифровании информации обычно используются в форме гибридных криптосистем), главной проблемой которых является длина ключа, а в результате – его повторяемость. Длина ключа, получаемого при помощи генератора хаоса, практически не ограничена, а в связи с тем, что один и тот же хаотический генератор может создавать совершенно разные процессы при незначительном изменении начальных условий, значительно затрудняется определение структуры генератора и предсказание процесса на какое-нибудь длительное время, что позволяет создать устойчивую к взлому систему с высоким уровнем надёжности. Схема Чуа обладает сложным поведением при общей простоте реализации и способна работать в широком диапазоне значений, поэтому она и была выбрана в качестве объекта моделирования с целью использования её для защиты информации.

Целью исследования является моделирование генератора хаоса, известного как «схема Чуа», для его применения в криптосистеме, надёжно функционирующей на различных распространённых устройствах.

Научной новизной данного исследования является разработанный метод применения математической модели генератора хаоса «схема Чуа» в качестве основного компонента гибридной криптосистемы, где генератор хаоса применён в качестве источника открытого и закрытого ключей асимметричного алгоритма шифрования и ключа симметричного алгоритма, непосредственно использующегося для шифрования данных.

В рамках данной работы рассмотрены требования к генераторам случайных чисел, используемые в криптосистемах для создания шифрующих последовательностей, методы достижения параметров, соответствующих этим требованиям, математическая модель генератора хаоса «схема Чуа», её поведение и режимы работы. В результате была разработана математическая модель для конкретного программного решения задачи о защите данных [2].

Посредством методов объектно-ориентированного анализа и проектирования, разработана проектная модель криптосистемы, описывающая классы и их взаимодействие между собой во времени и реализовано приложение, использующее разработанную криптосистему на базе генератора хаоса «схема Чуа», которое представляет собой удобную модель для проведения экспериментальных исследований конкретной реализации криптосистемы. Разработанная криптосистема реализована, как компонент приложения, содержащего в себе пару практически независимых друг от друга потоков. Каждый поток содержит свой экземпляр криптосистемы. Связь между потоками осуществляется при помощи отслеживания событий и временного бинарного файла, что было выполнено с целью возможности осуществления дальнейшего анализа полученных зашифрованных данных и самих ключей. Приложение обладает простым, наглядным интерфейсом и функционалом, достаточным для выполнения поставленных задач.

Были проведены экспериментальные исследования разработанной системы, в результате которых была доказана статистическая надёжность основы ключа, генерируемого математической моделью, по таким критериям, как равномерность распределения случайных чисел, их повторяемость на различных отрезках сгенерированной выборки, а также повторяемость сочетаний близлежащих чисел. Был проведён статистический анализ шифрующей последовательности, генерируемой самой криптосистемой на базе результатов работы генератора хаоса, в результате которого была доказана статистическая надёжность ключа и зашифрованных данных, как в бинарном, так и в числовом виде. Был проведён тест стабильности работы реализованной математической модели генератора хаоса и самой разработанной криптосистемы. По результатам теста отклонения от ожиданий оказались весьма малы и, учитывая достаточно большую длину тестовых данных, подобными отклонениями можно пренебречь.

Исходя из результатов исследования, преимущества представленной работы заключаются в высокой статистической устойчивости данных, зашифровываемых реализованной системой, к расшифровке третьим лицом, что является очень актуальным в настоящее время.

СПИСОК ЛИТЕРАТУРЫ

1. Левицкая Т. А. Разработка криптосистемы на генераторе хаоса «схема Чуа» / Т. А. Левицкая, Д. И. Ганзина // Университетская наука – 2017: Междунар. научно-техн. конф. (Мариуполь, 18–19 мая 2017 г.) : тез. докл. : в 3 т. / ГВУЗ "ПГТУ". – Мариуполь, 2017. – Т. 2. – С. 194–195.

2. Levitskaya T. O. Data protection by using the «chua's circuit» chaos generator / T. O. Levitskaya, D. I. Ganzina // Вісник Приазовського державного технічного університету : зб. наук. праць. – ПДТУ : Маріуполь, 2017. – Вип. 34. – С. 169–175.

ПРИЛОЖЕНИЕ ДЛЯ ДЕМОНСТРАЦИИ РАБОТЫ АЛГОРИТМОВ СОРТИРОВКИ И ПОИСКА ДАННЫХ

Мельников А. Ю., Сокольский А. С.
ДГМА, г. Краматорск

Разделы, связанные с изучением алгоритмов сортировки и поиска данных, являются неотъемлемой частью ряда дисциплин при подготовке студентов специальностей отрасли знаний «Информационные технологии». Внедрение таких информационно-коммуникативных средств обучения, как демонстрационное приложение, позволит лучше понять суть каждого алгоритма, сравнить их на конкретных примерах.

Была поставлена цель – создание приложения для демонстрации алгоритмов сортировки и поиска данных с целью лучшего понимания принципов их работы. В таком приложении пользователю должен быть доступен интуитивно понятный минимум необходимых элементов управления для выполнения всех функций программы, а именно:

а) выпадающие списки для выбора нужного алгоритма сортировки и (или) поиска данных;