$$Z_t = \sum_{i=1}^{14} \omega_i Y_{i,t}\ ,\ \sum_{i=1}^{14} \omega_i = 1, \qquad (3)$$

где $\{\omega_i\}$ – весовые коэффициенты, в качестве которых выступают доли добавленной стоимости в ВВП для рассматриваемых видов экономической деятельности. На последнем шаге рассчитывается сам индекс экономических настроений *ESI* посредством преобразования масштабирования значений $\{Z_t\}$:

$$ESI_t = \frac{Z_t - \bar{Z}}{S_z} \cdot 10 + 100, \text{ где } \bar{Z} = \frac{1}{T}\sum_{t=1}^{T} Z_t\ ,\ S = \sqrt{\frac{1}{T-1}\sum_{t=1}^{T}(Z_t - \bar{Z})^2}. \qquad (4)$$

В качестве иллюстрации опережающего характера построенного индекса экономических настроений в табл. 1 приводятся результаты тестирования причинной зависимости по Грейнджеру [3] между совместно моделируемыми на основе модели VAR(2) переменными: темпом роста ВВП и построенным ИЭН. На основании табл. 1 можно сделать вывод о том, что нулевая гипотеза: «ИЭН не является причиной изменения темпов прироста ВВП» отклоняется (правая панель таблицы), а гипотеза «изменение темпов прироста ВВП не является причиной для изменения ИЭН» не отклоняется (левая панель таблицы).

Таблица 1 – Результаты теста причинности по Грейнджеру

Лаг тестируемой модели	ВВП не является причиной для ИЭН		ИЭН не является причиной для ВВП	
	F-Statistic	Prob.	F-Statistic	Prob.
2	0.06295	0.9391	3.24571	0.0470

Приведенные результаты статистического анализа дают основания говорить о построенном индексе ИЭН как об опережающем индикаторе.

Список цитированных источников

1. Демидов, О. Различные индексы прогнозирования экономической активности в России / О. Демидов // Квантиль. – 2008. – № 5. – С. 83–102.
2. Малюгин, В.И. Об использовании векторных авторегрессионных моделей с переключающимися состояниями для анализа и прогнозирования циклов экономической активности / В.И. Малюгин // Экономика. Моделирование. Прогнозирование / Редкол.: М.К. Кравцов (гл. ред.) [и др.]. – Минск: НИЭИ Министерства экономики Республики Беларусь, 2015. – Вып. 9. – С. 183–196.
3. OECD Composite Leading Indicators – a Tool for Short-term Analysis. – Электронный ресурс: http://www.oecd.org/std/li1.htm

УДК 004.4

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ КАНАЛА СВЯЗИ

Меньших Т.Ю.
Брестский государственный технический университет, г. Брест
Научный руководитель: Дереченник С.С., к.т.н., доцент

В настоящее время вопрос защиты информации, которая передается по каналам связи, является неделимой частью общей проблемы сферы информационной безопасности. Это связано с тем, что в различных отраслях (например, обороны и связи, финансов, транспорта, управления и производства, науке, образовании и многих других) интенсивность информационного обмена велика, что без защиты дает злоумыш-ленникам и несанкционированным пользователям возможность использовать инфор-мацию в своих целях. Актуальность темы исследования определяется необходимостью развития защищенности каналов связи, так как большинство криптографических систем взламываются и становятся общеизвестными. Именно генераторы псевдослучайных чисел

(ГПСЧ) определяют степень защищенности канала связи в схеме синхронного поточного шифрования. Новизна работы состоит в программной разработке генераторов псевдослучайных последовательностей ПСЧ-1, ПСЧ-2 и разработке программы шифрования в среде Matlab с помощью данных ГПСЧ, что позволит в дальнейшем использовать полученные программы в практических целях.

Достоинством поточных шифров является высокая скорость шифрования, которая и определяет область их использования – шифрование данных, требующих оперативной доставки потребителю, например аудио- и видеоинформации [1]. К преимуществам поточных шифров также относятся отсутствие размножения ошибок, простая реализация системы криптографической защиты.

Недостатком является необходимость передачи информации синхронизации перед заголовком сообщения, которая должна быть принята до расшифрования любого сообщения. Это связано с тем, что если два различных сообщения шифруются на одном и том же ключе, то для расшифрования этих сообщений должна использоваться одна и та же псевдослучайная последовательность. Такое положение может создать опасную угрозу криптостойкости системы и поэтому часто используется дополнительный, случайно выбираемый ключ сообщения, который передается в начале сообщения и используется для модификации ключа шифрования. В результате разные сообщения будут шифроваться с использованием различных последовательностей.

На рисунке 1 изображена схема алгоритма работы ГСЧ-1. Рядом приведена таблица 1, полученная с помощью программы Matlab, первых десяти значений для случая N = 16 и начального числа 33.

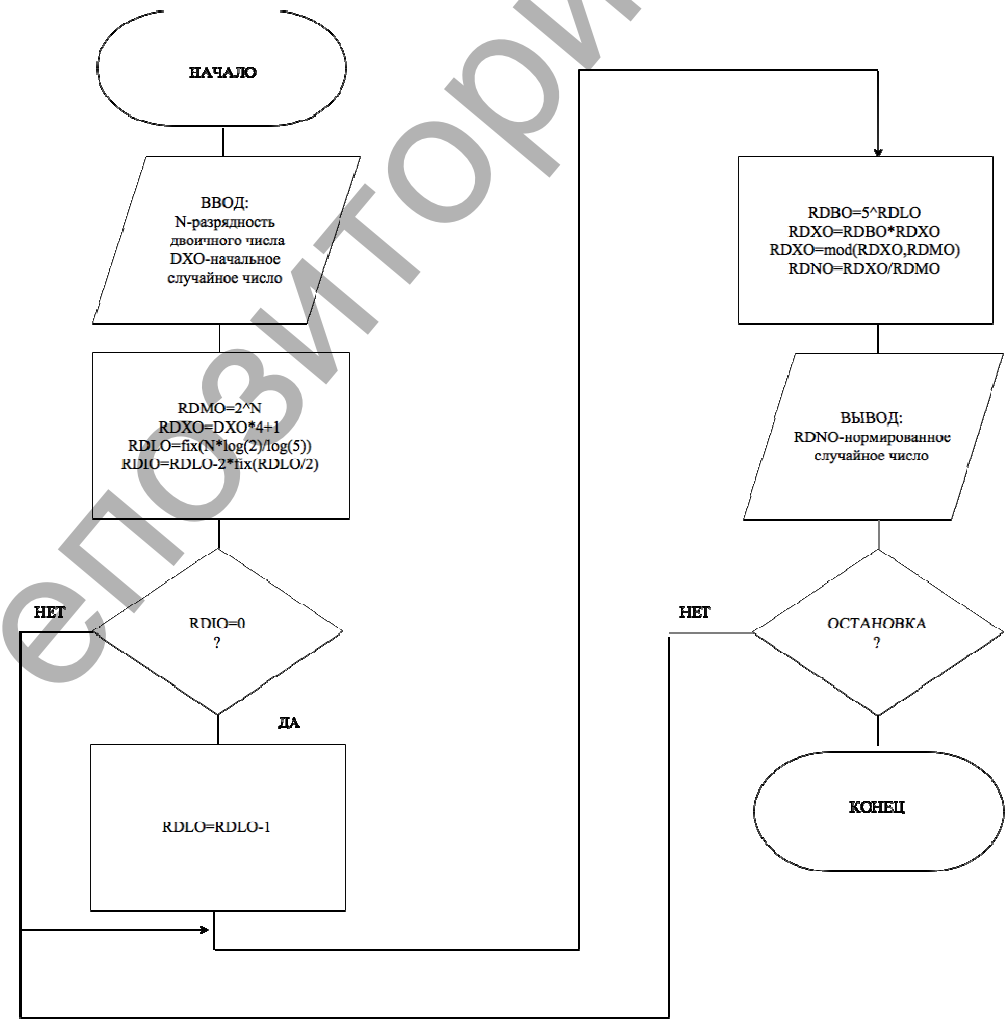

Рисунок 1 – Схема алгоритма ПСЧ-1

В вышеприведенном алгоритме операция X(n) = mod(X(n - 1),M) не дает возможности получить при имеющейся разрядности ЭВМ максимально возможное количество случайных чисел. На многих ПЭВМ вводимая разрядность двоичного числа не может быть более чем 16. Поэтому в тех случаях, когда необходимо увеличить период генерации случайных чисел, жертвуя временем, можно воспользоваться другим алгоритмом, приведенным на рисунке 2, в котором операция деления заменена на операцию последовательного вычитания. Данный алгоритм уникален в своем роде и подробно описан в источнике [2]. Благодаря этому алгоритму возможно увеличить разрядность двоичного числа до 53, что позволяет получать на обычных современных ПЭВМ 2251799813685248 случайных чисел. Значения первых десяти полученных чисел приведены в таблице 2. В таком случае весь период программа реализует примерно за 5 дней (процессор компьютера Intel Core i5-3317U, базовая тактовая частота 1.7 ГГц).

Таблица 1 – Значения первых десяти случайных чисел ПСЧ-1

Номер числа	Значение числа
1	0.341934204101563
2	0.544387817382813
3	0.211929321289063
4	0.279129028320313
5	0.278213500976563
6	0.417190551757813
7	0.720474243164063
8	0.482009887695313
9	0.280899047851563
10	0.809524536132813

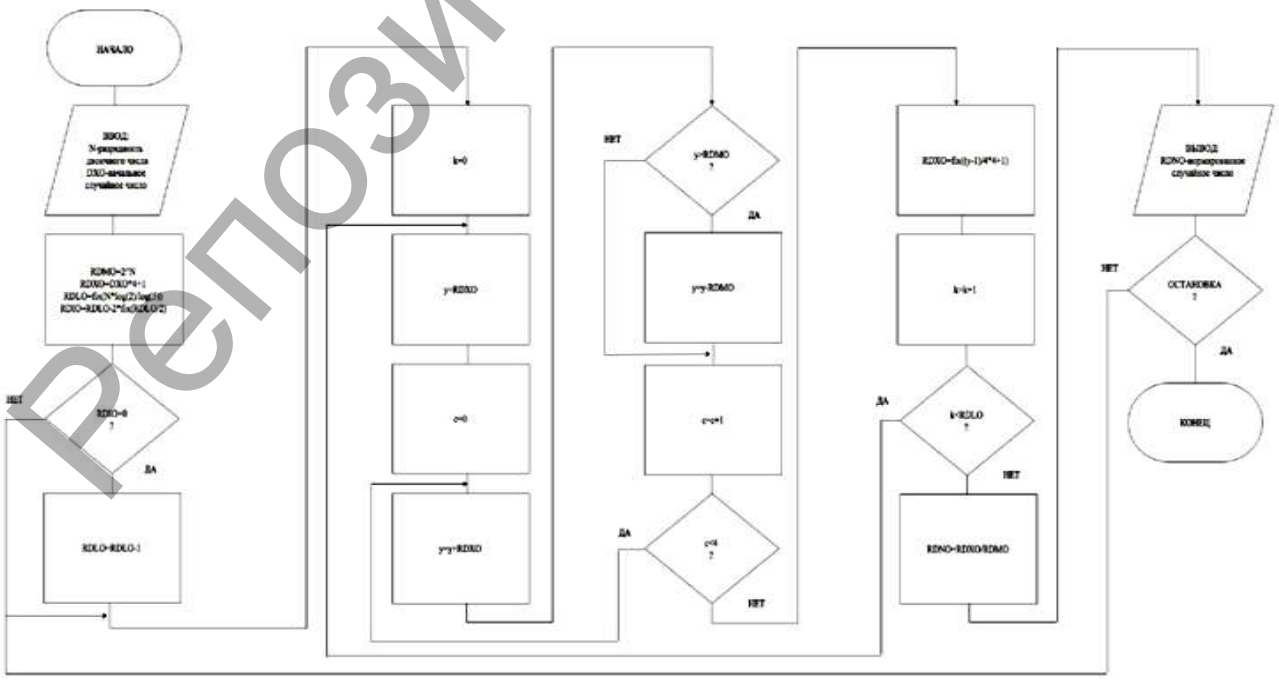

Рисунок 2 – Схема алгоритма ПСЧ-2

Таблица 2 – Значения первых десяти случайных чисел ПСЧ-2

Номер числа	Значение числа
1	0.040961374051372
2	0.235294224665242
3	0.683044209239244
4	0.030477757100518
5	0.027146390407054
6	0.425155767481531
7	0.849325928266710
8	0.216123950798070
9	0.563811995159878
10	0.500688790530220

Проведя статистическое тестирование ПСЧ-1 и ПСЧ-2, получили результаты, удовлетворяющие теоретическим данным. Результаты тестов позволили оценить равномерность распределения символов. Генераторы ПСЧ-1 и ПСЧ-2 прошли тесты на равномерность. Статистический тест показал численную характеристику последовательности и для точности 15 знаков после запятой, для выборки 500 значений чисел полученные характеристики удовлетворяют требованиям и сравнимы с теоретическими значениями для равномерного закона распределения. Для наглядного примера реализации поточного шифрования показано сообщение, которое преобразуется в битовую последовательность и суммируется по модулю два с псевдослучайными битами. Зашифрованное слово «привет» вбитовой последовательности имеет вид:

00000011111111110111111000111101100111 10101001111101111 0111.

В символьном виде зашифрованному слову “привет” соответствует “πoχύïv”. Расшифрование происходит аналогичным образом.

В дальнейшем планируется разработка алгоритмов и программ для большего периода генерации псевдослучайных чисел посредством комбинации ПСЧ-1 и ПСЧ-2.

Список цитированных источников

1. Иванов, М.А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: Кудиц - Образ, 2001. – 363 с.
2. Хазан, В.Л. Математические модели дискретных каналов связи декаметрового диапазона волн: учебное пособие. – Омск, 1998. – 107 с.