МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Н.И. ЛОБАЧЕВСКОГО»

РАДИОФИЗИЧЕСКИЙ ФАКУЛЬТЕТ

КАФЕДРА «БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»

Научно-исследовательская работа

Работу выполнил: студент

Группы \_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_ Гусев Ю.С.

(подпись)

Номер зачётной книжки

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Проверил:

\_\_\_\_\_\_\_\_\_\_\_ Горбунов А.А.

(подпись)

Н. Новгород, 2018

**1. Введение.**

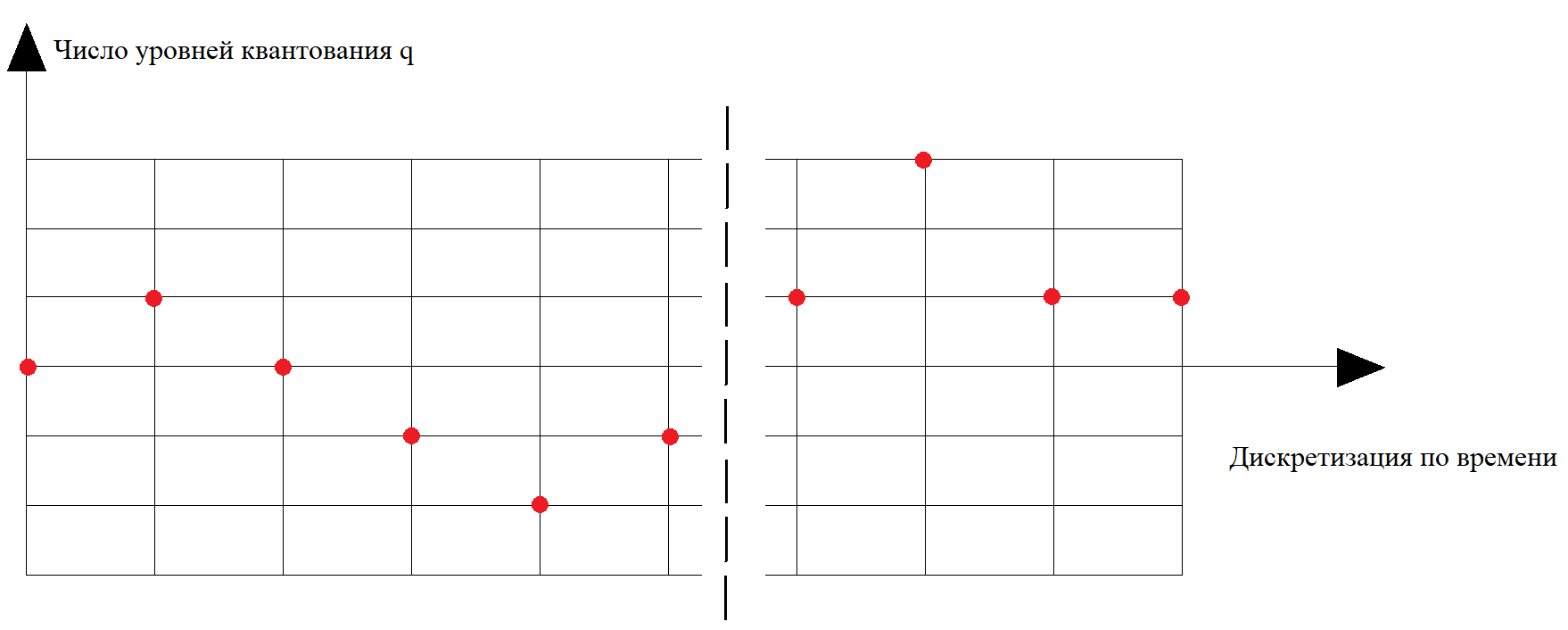
На современном этапе развития системы защиты информации получили довольно широкое распрстранение и задействованы в той или иной степени в жизни каждого человека. Поэтому задачи проверки устойчивости, оценки параметров и сравнения различных криптосистем не теряют своей актуальности.

В данной работе будет рассмотрена тема оценки параметров КС через методы структурной идентификации математической модели КС, базирующиеся на определение характеристик последовательностей, снятых в определенных точках автомата.

**2. Базовые параметры.**

Будем рассматривать текста на входе и выходе шифрующего автомата как сигналы, порождаемые источником экспериментальных данных. На каждом участке стационарности источник обладает набором базовых параметров

{q, n, Δt}. Δt – интервал квантования по времени, q – число уровней квантования, n – «сложность» источника на участке стационарности.

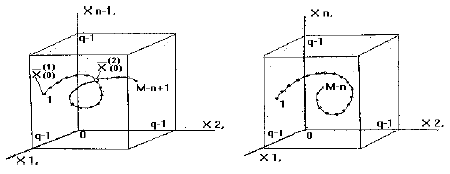


Для оценки численных значений БП требуются только сами «сигналы» источника данных и минимальная априорная информация (например, алфавит).

При определении базовых параметров математической модели источника данных решается задача структурной идентификации источника. После их определения можно перейти к нахождению «свободных» параметров математической модели. К ним относятся, например, коэффициенты матриц, вектора начального состояния.

**3. Поиск БП. Участки стационарности.**

Графически поиск БП можно изобразить в виде фазовой траектории, находящейся в гиперкубе со сторонами из q дискрет. Каждой точке этой ФТ будут соответствовать n последовательных выборок данных из сигнала. Так как число точек в дискретном фазовом пространстве ограничено, то траектория может замкнуться, тем самым выделяя участок стационарности. В таком случае при фиксированном q увеличивается n, то есть размерность гиперкуба, и процесс повторяется, до тех пор, вся ФТ не перестанет зацикливаться, а весь текст станет «q-n стационарным».

****

Если сигнал является не стационарным, то таким методом можно точно определить границы участков стационарности и БП для каждого из них. Помимо основных БП, сложный нестационарный сигнал обладает расширенным набором базовых параметров:

t(i) – координата конца i-го участка траектории,

s(i) – число точек до входа в цикл на i-м участке ФТ,

c(i) – число точек в цикле i-го участка ФТ,

cc(i) – полное число точек на цикле i-го участка ФТ.

После определения БП можно перейти к определению рабочих параметров, то есть к решению задачи параметрической идентификации ММ источника экспериментальных данных.

**4. Методы вычисления БП.**

Обозначим открытый текст ut, а шифрованный yt.

По своей сути q – размерность алфавита сигнала, а n – минимальная длина неповторяющейся подпоследовательности сигнала, состоящей из n последовательных выборок. Значит, вычислять q не нужно, так как он заранее известен.

Для вычисления параметра n есть несколько способов, например:

- Алгоритмы, основанные на последовательном переборе всех возможных последовательностей длины n. То есть, берется выборка последовательных n символов и сравнивается со всеми следующими выборками последовательных n символов. Если «двойник» не обнаружен, то берется следующая n-выборка и процесс повторяется. В итоге либо повторяющихся выборок не будет и данное n является базовым параметром текста, либо обнаружится «двойник», что приведет к увеличению n на 1 и повторению алгоритма. Алгоритм обладает небольшими затратами памяти, а время его работы подобного оценивается как О(М2), то есть он применим для относительно коротких текстовых последовательностей или в случаях, когда время не важно.

- Алгоритм бинарного поиска среди отсортированных по определенному правилу n-последовательностей. Общее время работы оценивается как

*.* Таким образом, данный алгоритм применим для более больших объемов текста, но при высокой скорости работы он затрачивает больше ресурсов памяти на хранение упорядоченного списка последовательностей.

- Алгоритмы, использующие деревья для поиска повторяющихся строк. Например, алгоритм Укконена с использованием суффиксального дерева или алгоритм Ахо-Корасик. Оба алгоритма выполняют свою работу за линейное относительно длины обрабатываемой текстовой последовательности. Ограничивают применение подобных алгоритмов большие затраты памяти при большой размерности алфавита q и большой длине самой последовательности.

В данной работе остановимся на первом методе, так как он является наиболее простым в реализации, а временные затраты на данный момент не играют особой роли.

**5. Связь БП и энтропии.**

Понятие энтропии сообщения введено Шеноном через вероятность появления различных вариантов текста.

– энтропия, или мера неопределенности, выходного сообщения.

Аналогично для входного сообщения u(i) :

Суммирование осуществляется по всем возможным вариантам сообщения.

Так же вводится понятие совместной энтропии входного и выходного сообщений:

Средняя условная энтропия исходного сообщения

получила название *функции ненадежности текста сообщения*.

Энтропия текста выражается через его базовые параметры как

Также Шеноном введено понятие «расстояние единственности», то есть длина криптограммы, при которой вероятность только одного варианта расшифровки близка к 1.

- энтропия ключа шифрования, где - средняя длина участка стационарности.

- оценка величины избыточности текста.

**Список литературы.**

1) Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин – «Защита информации в компьютерных системах и сетях» издание второе, дополненное – Москва, «Радио и связь», 2001 г.

2) С.П. Панасенко – «Алгоритмы шифрования. Специальный справочник» – Санкт-Петербург, «БХВ-Петербург, 2009 г.

3) К.Г. Кирьянов – «Выбор оптимальных базовых параметров источников экспериментальных данных при их идентификации – Труды III Международной конференции «Идентификация систем и задач управления» SICPRO ’04 Москва 28-30 января 2004 г.

4) А.А. Горбунов, К.Г. Кирьянов – «Связь “Функции ненадежности” и “Расстояния единственности” криптосистем с базовыми параметрами шифратора в форме математической модели синхронного автомата Хаффмана»

5) А.А. Горбунов, К.Г. Кирьянов – «Динамические модели криптосистем с закрытым ключом. Синтез дешифраторов»

6) А.А. Горбунов – «Алгоритмы структурной идентификации математических моделей криптосистем на основе определения базовых параметров» – Доклады ТУСУРа, № 1 (19), часть 2, июнь 2009

7) К. Шенон – «Работы по теории информации и кибернетике»