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.

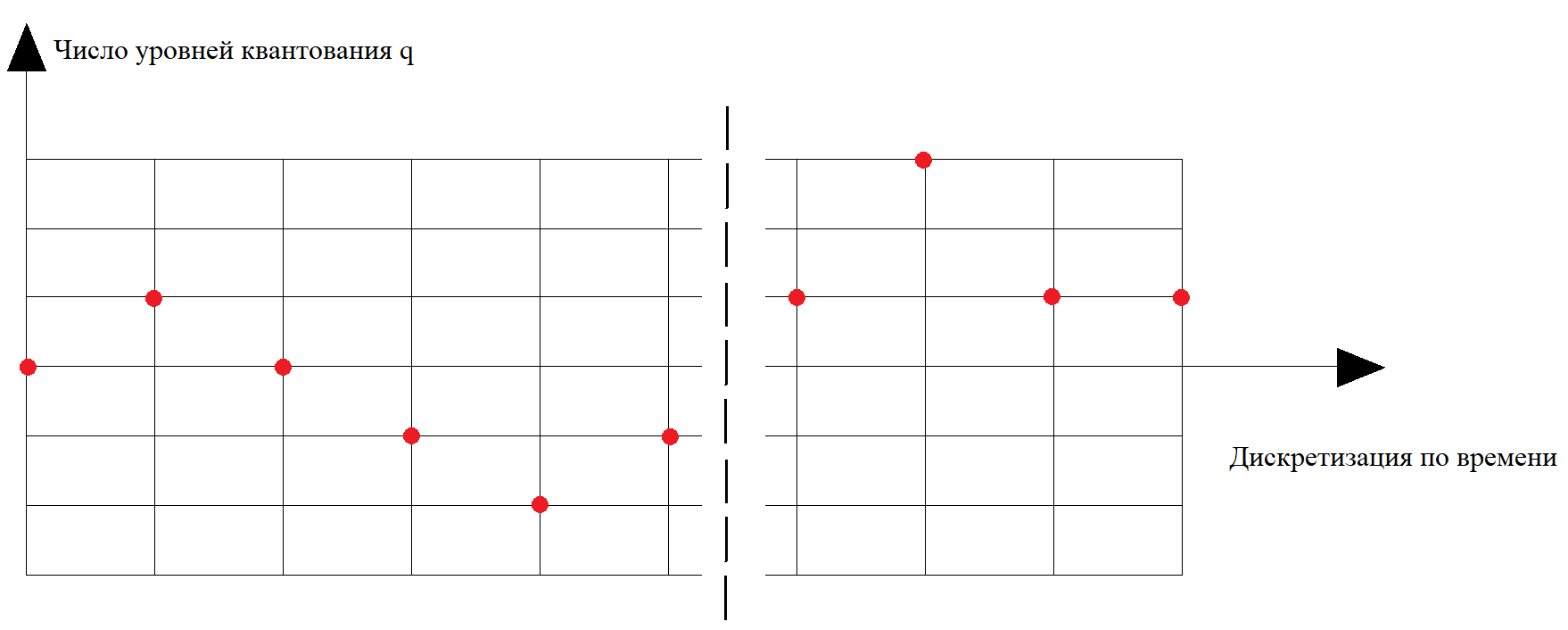
(подпись)

Н. Новгород, 2018

**1. Введение.**

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.



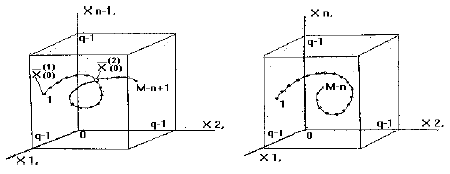
Для оценки численных значений БП требуются только сами «сигналы» источника данных и минимальная априорная информация (например, алфавит).

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.

**2. Поиск БП. Участки стационарности.**

По своей сути q – размерность алфавита сигнала, а n – минимальная длина неповторяющейся подпоследовательности сигнала, состоящей из n последовательных выборок.

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.

**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