**Литература**

1. С. Хайкин, Нейронные сети: полный курс, 2-е изд., испр. : Пер. с англ. – М.: ООО «И.Д. Вильямс», 2006, 1104 стр.

УДК 004.056.55

## АЛГОРИТМЫ ШИФРОВАНИЯ, ОСНОВАННЫЕ НА ДАННЫХ

Стухальский А.Л. Романенко Р.А.
Научный руководитель – Федосик Е.А., физ.-мат. наук, доцент.

Существует большое количество алгоритмов шифрования. Многие из них устарели и не пригодны для использования. Причина в том, что производительность вычислительных систем растет экспоненциально (ЗаконМура). Причем проблемы возникают последовательно и со всех сторон: с увеличением производительности уменьшается время взлома, а для усиления алгоритмов применяются все более сложные методы, которые требуют больших вычислительных затрат.

Самым востребованным и распространенным алгоритмом шифрования на протяжении длительного периода времени является Advanced Encryption Standard (AES). Тем не менее надежность AES вызывает сомнения в связи с его простым математическим описанием.

Для решения возникающих проблем, авторами разработана концепция динамических алгоритмов. Для простоты понимания концепции можно воспользоваться теорией систем (ЧерныйЯщик). Всю систему можно представить, как «черный ящик» со входом и выходом. Сама реализация «черного ящика» также представляется в виде набора «черных ящиков». Анализируя каждую часть в отдельности можно обнаружить элементы с простой зависимостью по отношению к другим. Авторы предлагают представлять подобные элементы в качестве самостоятельных логических частей. Такой подход имеет много преимуществ, главным из которых является гибкость системы. Заменяя один или несколько элементов системы либо их порядок на выходе получаем новую систему. Примечательно, что наличие нескольких заменяемых элементов увеличивает сложность взлома. Несмотря на то, что структура системы не изменилась, результат полученной криптосистемы будет кардинально отличатся от предыдущего. Теория систем позволяет рассмотреть альтернативный подход: вместо замены частей системы можно внести в систему изменчивые элементы. Поведение такого элемента зависит от его текущего состояния.

Моментально изменяющаяся криптосистема исключает возможность использования дифференциального и интегрального методов взлома. Суть данных методов сводится к обнаружению зависимостей в ходе работы системы, путём изменения входных данных и анализа изменения в выходных данных. Сбор и анализ поведения изменчивой системы ни к чему не приведет.

Совокупность всех возможных состояний элементов системы можно представить в виде линейного пространства *N*. Совокупность входных данных представим в виде линейного пространства M (см. рис. 1).

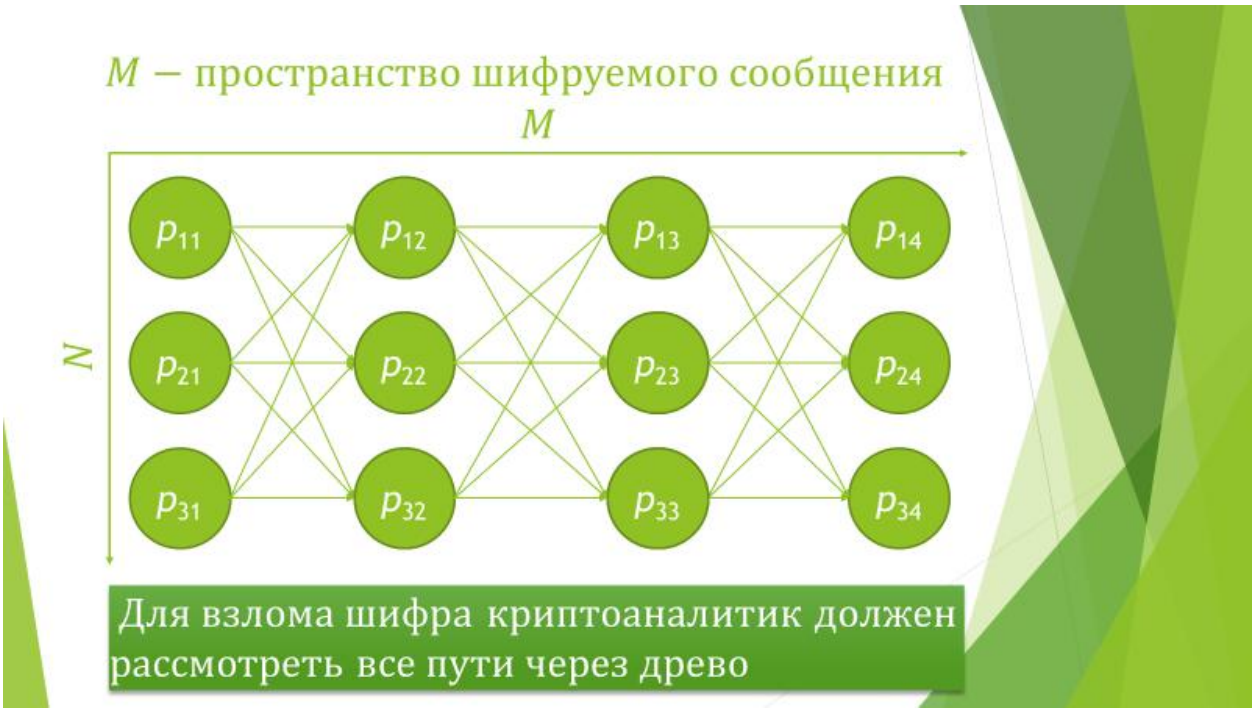


Рисунок 1 Графическое представление гибкой криптосистемы.

В результате получим дерево состояний системы размером $N * M$. Для взлома такой системы необходимо выбрать единственно-верный путь, состоящий из переходов между состояниями, например, $p_{21} \rightarrow p_{32} \rightarrow p_{13} \rightarrow p_{14}$.

## Литература

1. **AES** [В Интернете] // Википедия. - 13 3 2017 г.. - https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard.

2. **Закон Мура** [В Интернете] // Википедия. - 27 4 2017 г.. - https://ru.wikipedia.org/wiki/Закон_Мура.

3. **Черный ящик** [В Интернете] // Википедия. -27.4.2017 г. - https://ru.wikipedia.org/wiki/Чёрный_ящик.

УДК 629.113-585

## ВЫБОР ОПТИМАЛЬНЫХ ПАРАМЕТРОВ КОЛЕБАТЕЛЬНОЙ СИСТЕМЫ

Курьянов П.В.
Научный руководитель – Марцинкевич В.С., ст. преподаватель

Рассмотрим колебательную систему, изображенную ниже, которая состоит из двух одинаковых масс $m_1=m_2=m$, соединенных жесткостями $C_1=C_2=C$ и $C_0$.

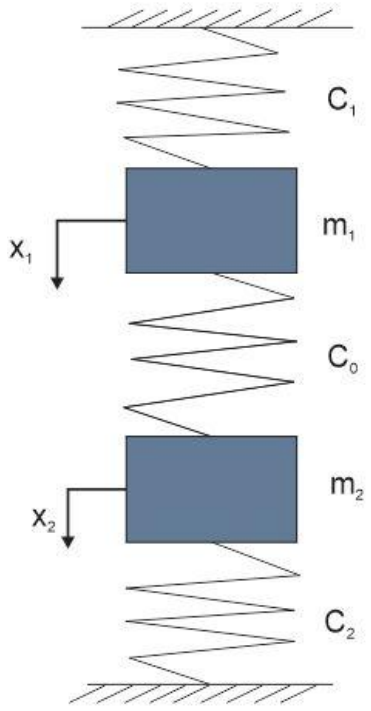


Рисунок 1. Схема конструкции

Такая система зависит от трех параметров C, $C_0$, m.

Предположим, что по техническим условиям эти параметры обязаны находиться в заранее заданных пределах:

$$\begin{cases} C^* \le C \le C^{**} \\ C_0^* \le C_0 \le C_0^{**} \\ m^* \le m \le m^{**} \end{cases} \quad (1)$$