УДК 004.056: 061.068

КОНТРОЛЬ ХАОТИЧНОСТИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ АЛГОРИТМА ШИФРОВАНИЯ НА ОСНОВЕ ДИНАМИЧЕСКОГО ХАОСА

А.В. СИДОРЕНКО

Белорусский государственный университет
пр. Независимости, 4, 220050, Минск, Беларусь

Поступила в редакцию 17 февраля 2014

Рассматриваются два подхода для контроля хаотического режима в выходных последовательностях алгоритма шифрования с использованием динамического хаоса путем применения метода задержанной координаты и метода сингулярного спектрального анализа. Проводится сравнительный анализ параметров входных и выходных последовательностей разработанного алгоритма шифрования на основе динамического хаоса и алгоритмов AES (Advanced Encryption Standard), DES (Data Encryption Standard). Установлено, что параметры, характеризующие выходные последовательности алгоритма шифрования с использованием динамического хаоса не хуже параметров, полученных для стандартных шифров.

Ключевые слова: шифрование, информация, контроль, хаотическое отображение, хаос.

Введение

На современном уровне развития информационных технологий существенное значение приобретают вопросы защиты информации в телекоммуникационных системах различного назначения. Развивается направление, связанное с шифрованием информации в хаотических системах [1]. Использование динамического хаоса для систем защиты информации обусловлено способностью хаотических отображений обеспечивать скрытость передачи зашифрованной информации в блочных или поточных шифрах. Детерминизм хаоса способствует шифрованию информации, а его случайность делает систему стойкой к вскрытию [2, 3]. Такие свойства как спутанность и распыление, характерные для традиционных криптоалгоритмов, в хаотических реализуются с помощью хаотических отображений и последующих итераций.

В работе [4] показано, что традиционные криптографические системы могут рассматриваться в рамках синергетического подхода, то есть как нелинейные динамические системы. Под криптосистемой тогда можно понимать динамическую систему $\langle f, X, K \rangle$ с нелинейной функцией f, пространством состояний X и пространством параметров K. Нелинейная функция f задается с помощью алгоритма, X – множество исходных состояний, K – множество ключей.

При рассмотрении алгоритмов с использованием динамического хаоса существенным является обеспечение хаотического режима, что проявляется в получении хаотических последовательностей алгоритма шифрования, и обусловлено обеспечением требований безопасности схемы шифрования.

Как известно, показатель экспоненты Ляпунова λ является признаком хаотического режима функционирования динамической системы [5]. В ряде работ предлагается использовать показатель экспоненты Ляпунова λ для определения хаотичности динамической системы в криптографии [6, 7]. Однако при использовании, например, логистического отображения, вычисление среднего значения показателя экспоненты является недостаточно точным, либо не

охватывает «окна периодичности», где динамическая система является детерминированной. Поэтому следует рассмотреть иные методы анализа зашифрованных сообщений.

Целью работы является определение количественных параметров и визуализация зашифрованных с использованием динамического хаоса выходных последовательностей алгоритма шифрования.

В данной работе предлагаются и рассматриваются два подхода определения хаотичности выходных последовательностей зашифрованной информации. Первый из них основан на подходе методов нелинейной динамики, позволяющем определять параметры динамической системы и их изменений в процессе шифрования. Второй вариант, обусловленный наличием в исследуемых последовательностях детерминированной составляющей, дает возможность использовать подход на базе сингулярного спектрального анализа с определением динамики интенсивности главных компонент.

Методика проведения исследований

Для проведения исследований использованы выходные последовательности, полученные для разработанного нами алгоритма шифрования с применением динамического хаоса и алгоритмами AES (Advanced Encryption Standard), DES (Data Encryption Standard), а также входные последовательности открытого текста. В основу разработанного нами алгоритма шифрования на основе динамического хаоса положена обобщенная схема блочного симметричного алгоритма шифрования [8]. В качестве базового преобразования используется сеть Фейстеля, в которой нелинейная функция задается в виде хаотического отображения.

При использовании первого из подходов определения хаотичности анализ степени хаотичности выходных (зашифрованных) последовательностей проводится построением фазовых портретов и применением метода задержанной координаты. Применение метода задержанной координаты, как одного из методов нелинейной динамики, позволяет определить количественные параметры в виде корреляционной размерности d и энтропии Колмогорова K каждой из исследуемых последовательностей [9]. Корреляционная размерность определяет область локализации динамической системы в фазовом пространстве или число степеней свободы указанной системы. Энтропия Колмогорова характеризует устойчивость работы системы, измеряемую скоростью расходимости ее траекторий в фазовом пространстве. Визуальный анализ проводится по построенным фазовым портретам системы. Построение фазовых портретов дает возможность визуально определять степень заполнения фазового пространства.

При использовании второго из подходов определения хаотичности, основанного на методе сингулярного спектрального анализа, оценивается количественный параметр – уровень главных компонент I. Для получения визуальной информации используется построение фазовых диаграмм, когда по осям x и y откладываются различные пары собственных векторов или главных компонент.

Метод задержанной координаты

Согласно метода задержанной координаты [9], выходная последовательность алгоритма шифрования представляется в виде

$$x_1, x_2, \ldots x_n, \qquad (1)$$

где $x_n = x(np)$, p – шаг дискретизации, n – целое число.

Эта последовательность порождает m-мерные векторы, лежащие в m-мерном фазовом пространстве

$$\vec{x}_i^{\,T} = \left(x_i, \cdots x_{i+m-1}\right), \qquad (2)$$

где T – знак транспонирования.

Состояние системы в реконструированном m-размерном фазовом пространстве определяется m-размерными точками для каждой реализации $x(p)$

$$x_i^m = \left(m^{-1/2}\right)(x_i, x_{i+1}, ...x_{i+m-1}). \quad (3)$$

Корреляционный интеграл $C_m(l)$ – это функция, равная вероятности того, что расстояние между двумя реконструированными векторами $\vec{x}_i$ меньше l.

Корреляционная размерность d определяется

$$d = \lim_{r\to 0}\left[\lg C_m(r) / \lg r\right], \quad (4)$$

где $C_m(r)$ – корреляционный интеграл, r – размер ячейки разбиения или коэффициент подобия.

Корреляционный интеграл записывается

$$C_m(r) = \lim_{N\to\infty} \frac{1}{N^2} \sum_{i,j=1}^{N} \theta\left(r - \left|\vec{x}_i - \vec{x}_j\right|\right), \quad (5)$$

где $\theta = 0$ при $t \le 0$, $\theta = 0{,}5$ при $t = 0$, $\theta = 1$ при $t \ge 0$, θ – функция Хевисайда, N – число точек, используемых для оценки размерности.

Найдено, что для малых значений r поведение функции $C_m(r)$ может быть описано

$$C_m(r) = r^d, \quad (6)$$

где d – параметр, близкий к фрактальной размерности странного аттрактора, r – параметр подобия.

Для достоверной оценки корреляционной размерности d размерность соответствующих фазовых пространств должна удовлетворять условию Мане

$$m \ge 2d + 1. \quad (7)$$

Для снижения объема вычислений используется алгоритм И. Арансона, позволяющий оперировать с целыми числами и существенно снизить временные затраты.

Энтропия Колмогорова определяется выражением

$$K = \lim_{r\to 0} \lim_{\tau\to 0} \frac{1}{\tau} \lg\left[C_m(r) / C_{m+1}(r)\right]. \quad (8)$$

Метод сингулярного спектрального анализа

Для исследования реализаций открытого и зашифрованного текстовых сообщений используется метод сингулярного спектрального анализа, алгоритм которого сводится к следующему [10].

Пусть задан временной ряд $\{x_i\}_{i=1}^N$, образованный последовательностью N равноотстоящих значений некоторой функции $f(t)$.

1. *Развертка одномерного ряда в многомерный*. В качестве первой строки матрицы X используется M (длина гусеницы) значений последовательности, начиная с первого члена. В качестве второй строки матрицы используются значения последовательности, начиная с x_2 до x_{M+1}. Последнюю строку матрицы с номером $k = N - M + 1$ образуют последние M элементов последовательности. Эту матрицу, элементы которой $x_{ij} = x_{i+j-1}$, можно рассматривать как M-мерный временной ряд, которому соответствует M-мерная траектория в M-мерном пространстве из $k-1$ звена.

2. *Анализ главных компонент: сингулярное разложение выборочной ковариационной матрицы.* Вычисляется матрица $V = (\frac{1}{k}) X^T X$, которая является нецентрированной ковариационной матрицей.

Определяются собственные числа и собственные вектора матрицы V, т.е. ее разложение $V = P\Lambda P^T$, где Λ – диагональная матрица, на диагонали которой стоят

упорядоченные по убыванию собственные числа, а P – ортогональная матрица собственных векторов матрицы V.

Матрицу P можно рассматривать как матрицу перехода к главным компонентам $XP = Y = (y_1, y_{2,}, ... y_M)$.

Если используется временной ряд из случайных чисел, то собственные числа матрицы V являются выборочными дисперсиями соответствующих главных компонент, а квадратные корни из них – выборочными средними. Графическое представление собственных чисел и некоторых функций при анализе главных компонент традиционно используется для выявления структуры исследуемого ряда, отбора и интерпретации главных компонент.

3. *Отбор главных компонент.* С учетом свойств матрицы P можно матрицу ряда X представить в виде $X = YP^T$. Получаем разложение матрицы ряда по ортогональным составляющим (главным компонентам).

В то же время преобразование $y_j = X\, p_j$ является линейным преобразованием исходного процесса с помощью дискретного преобразования свертки, т. е.

$$y_j[l] = \sum_{q=1}^{M} x_{lq} p_{jq} = \sum_{q=1}^{M} x_{l+q-1} p_{jq}. \qquad (9)$$

Алгоритм порождает набор линейных фильтров, настроенных на составляющие исходного процесса. Собственные векторы матрицы V выступают в роли переходных функций соответствующих фильтров.

Визуальное и аналитическое изучение собственных векторов и главных компонент, полученных в результате линейной фильтрации, дает информацию о структуре изучаемого процесса и его свойствах.

Для получения визуальной информации используется построение фазовых диаграмм, когда по осям x и y откладываются различные пары собственных векторов или главных компонент. Из ортогональности собственных векторов и главных компонент следует, что сдвиг фаз между такими парами равен $\pm\pi/2$.

4. *Восстановление одномерного ряда.* Процедура восстановления основана на разложении $X = YP^T$.

Восстановление проводится по главным компонентам, если при применении формулы $X = Y^* \cdot P$ матрица Y^* получена из матрицы Y обнулением всех, не входящих в набор компонент. Таким образом, мы можем получить интересующее нас приближение матрицы ряда или интерпретируемую часть этой матрицы.

Результаты и обсуждение

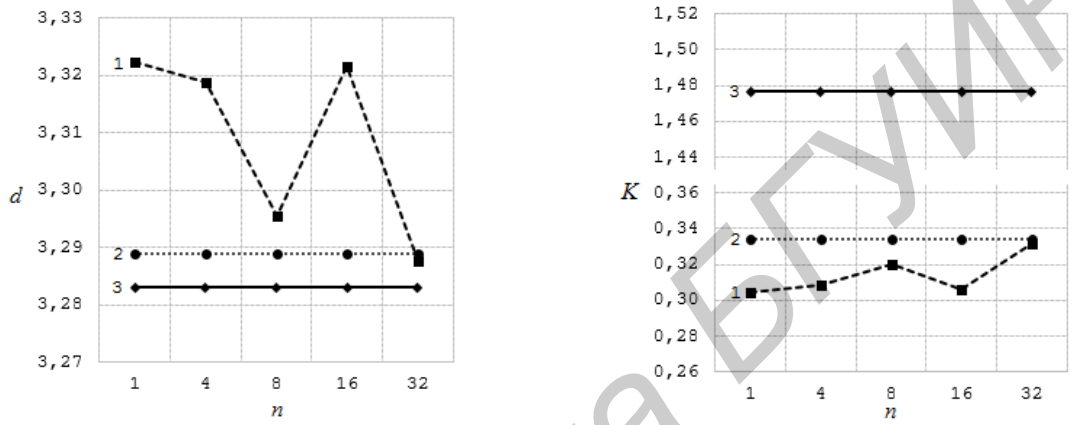
В процессе проведения вычислительного эксперимента при использовании метода задержанной координаты и метода сингулярного спектрального анализа получены параметры выходных последовательностей разработанного нами алгоритма шифрования, алгоритмов AES и DES. На рис.1 приведены графики зависимости корреляционной размерности d и энтропии Колмогорова K входных и выходных последовательностей (полученных путем зашифрования произвольного фрагмента открытого текста) от количества раундов базового преобразования n при использовании разработанного алгоритма шифрования и алгоритма AES в режиме работы CBC (сцепление блоков шифра).

Использование информационных параметров (корреляционной размерности и энтропии Колмогорова) позволяет выявить отличия в выходной последовательности алгоритма шифрования относительно входной. В частности, в режиме работы CBC, значения корреляционной размерности для выходной последовательности превышают значения для входной последовательности на 4,0–4,6 %, а значения энтропии Колмогорова для выходной последовательности составляют, соответственно, 20,0–21,8 % от значений для входной.

Как видно из графиков, приведенных на рис. 1, в режиме CBC, для исследованного интервала значений количества раундов базового преобразования (1–32 раунда) выходные последовательности, полученные разработанным алгоритмом шифрования, демонстрируют

более высокую степень хаотичности, чем выходные последовательности, полученные алгоритмом шифрования AES.

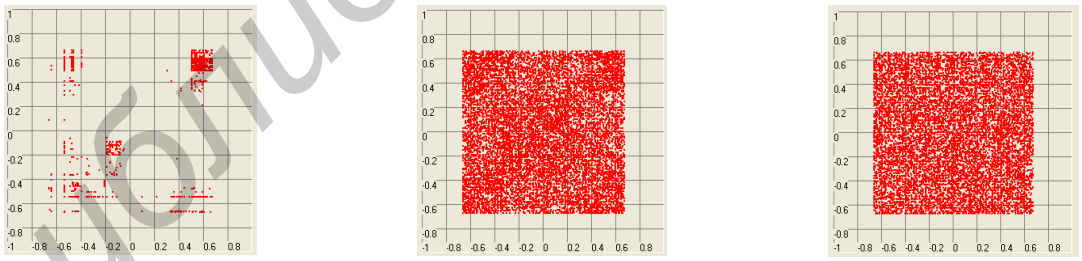
Использование указанных информационных параметров также позволяет выявить участки детерминированности в выходных последовательностях, которые могут быть образованы при нехаотическом поведении элементов алгоритма шифрования, что не может быть выявлено при анализе показателей Ляпунова. В частности, поведение логистического отображения в алгоритме шифрования, описанном в работе [6], при определенных значениях управляющего параметра попадает в область с детерминированной динамикой, что делает данный алгоритм уязвимым к атакам на основе известного открытого текста [6]. Значения корреляционной размерности и энтропии Колмогорова для соответствующих выходных последовательностей будут существенно отличаться от таковых при наличии динамического хаоса.



а *б*

Рис. 1. Графики зависимости значения корреляционной размерности d (*а*), энтропии Колмогорова K (*б*) выходных последовательностей алгоритма шифрования с использованием динамического хаоса (кривая 1), алгоритмом AES (кривая 2), а также входных последовательностей (кривая 3) от количества раундов n базового преобразования в режиме работы СВС

На рис. 2 изображены фазовые портреты открытого текста и соответствующих зашифрованных последовательностей, полученных разработанным алгоритмом шифрования и алгоритмом AES. Количество раундов базового преобразования разработанного алгоритма равняется 16, а для AES – 14.



а *б* *в*

Рис. 2. Фазовые портреты входной (открытого текста) (*а*) и выходных последовательностей, полученных разработанным алгоритмом шифрования (*б*) и алгоритмом AES (*в*), в режиме СВС

Полученные методом задержанной координаты и построением фазовых портретов входных (открытого текста) и выходных (зашифрованных) последовательностей результаты позволяют заключить, что: корреляционная размерность, энтропия Колмогорова могут быть использованы в качестве параметров определения степени хаотичности выходных последовательностей, а фазовые портреты – для визуального анализа при применении алгоритма шифрования с использованием динамического хаоса.

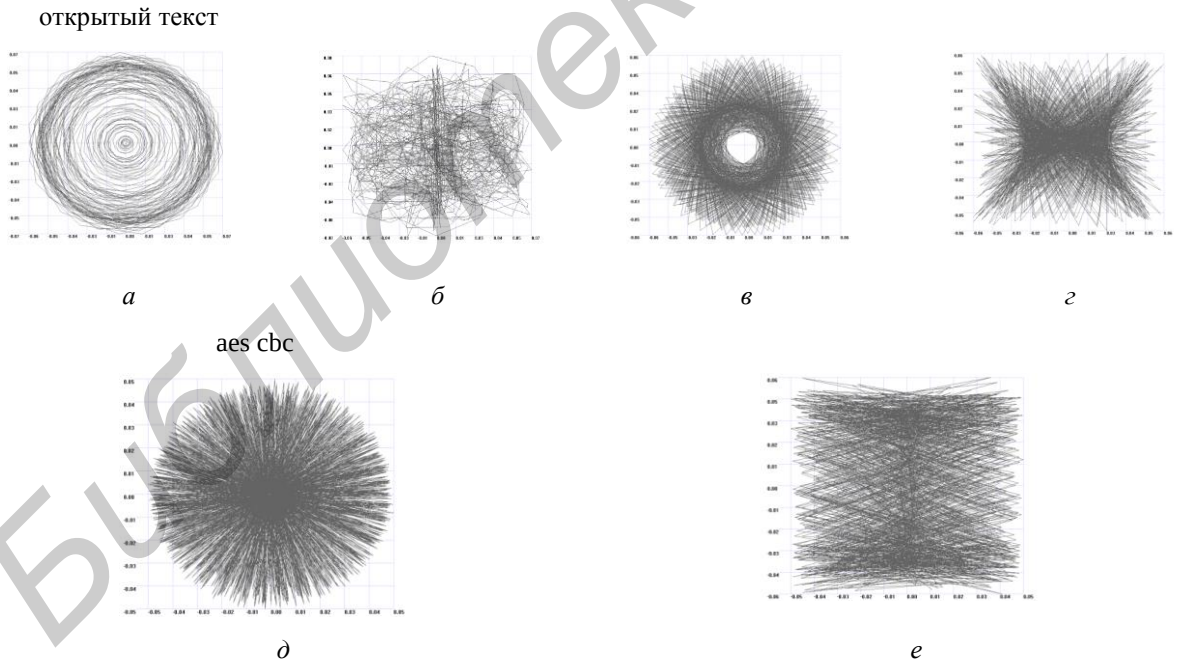
При использовании второго из подходов определения хаотичности, основанного на методе сингулярного спектрального анализа, в процессе исследований проводилась оценка количественного параметра – уровня главных компонент I входных последовательностей,

выходных последовательностей разработанного нами алгоритма шифрования с использованием динамического хаоса, алгоритмов AES, алгоритма DES. Для анализа визуальной информации применяется построение фазовых диаграмм, когда по осям x и y откладываются различные пары собственных векторов или главных компонент. В таблице приведены результаты вычислительного эксперимента при следующих условиях: длина анализируемых последовательностей $N = 10000$, длина гусеницы M = 1000, число итераций изменялось $z = 8$, $z = 64$.

Уровень главных компонент *I*, входных последовательностей (1), выходных последовательностей разработанного алгоритма шифрования с использованием динамического хаоса при числе итераций $z = 8$ (2), $z = 64$ (3), алгоритмов DES (4) и AES (5) в режиме CBC

Номер главной компоненты	1000	999	998	997	996	995	994	993
1	0,3530	0,3530	0,3036	0,3035	0,2989	0,2979	0,2934	0,2934
2	0,2203	0,2202	0,2122	0,2118	0,2081	0,2080	0,2028	0,2027
3	0,226	0,2258	0,2250	0,2250	0,2109	0,2108	0,2015	0,2014
4	0,1899	0,1893	0,1880	0,1879	0,1841	0,1840	0,1821	0,1820
5	0,2287	0,2287	0,2179	0,2177	0,2135	0,2134	0,2083	0,2081

Как видно из таблицы, для входных последовательностей (1) уровень главных компонент *I* превышает значения для показателей исследуемых выходных последовательностей (2–5) более чем на 50 %. Сравнительный анализ показывает, что для выходных последовательностей разработанного алгоритма шифрования с использованием динамического хаоса уровень главных компонент I практически совпадает с показателями алгоритмов шифрования AES и DES в режиме CBC. Фазовые диаграммы пар собственных векторов с номерами 1000 и 999, 1000 и 998 для входных последовательностей, выходных последовательностей разработанного алгоритма (число итераций $z = 8$) и алгоритма AES приведены на рис. 3.



а *б* *в* *г* *д* *е*

Рис. 3. Фазовые диаграммы пар собственных векторов с номерами 1000 и 999, 1000 и 998: для входных последовательностей (*а*) и (*б*); выходных последовательностей разработанного алгоритма с использованием динамического хаоса при числе итераций $z = 8$ (*в*) и (*г*), выходных последовательностей алгоритма AES (*д*) и (*е*) при анализе последовательностей методом сингулярного спектрального анализа

Для фазовых диаграмм выходных последовательностей разработанного алгоритма шифрования и шифра AES (aes cbc) (рис. 3, *д*, *е*) характерным, в отличие от диаграмм открытого текста (рис. 3, *а*, *б*), является наличие «зашумленности» фигур.

Таким образом, использование метода сингулярного спектрального анализа применительно к входным последовательностям, а также к выходным последовательностям алгоритма шифрования с использованием динамического хаоса, например, в режиме СВС, позволяет установить качественные критерии в виде фазовых диаграмм, а также количественный критерий по уровню главных компонент для определения хаотичности последовательностей алгоритмов шифрования.

Заключение

В результате проведенных исследований установлено, что для контроля хаотичности выходных последовательностей алгоритмов шифрования с использованием хаотических сигналов могут быть использованы метод задержанной координаты и метод сингулярного спектрального анализа. Показано, что такие параметры, как корреляционная размерность, энтропия Колмогорова метода задержанной координаты, могут быть использованы в качестве критериев определения степени хаотичности выходных последовательностей, а фазовые портреты – для визуального анализа при применении алгоритма шифрования с использованием хаотических сигналов. Параметр уровеня главных компонент метода сингулярного спектрального анализа и фазовые диаграммы рекомендуется применять как средства для определения хаотичности выходных последовательностей алгоритма шифрования с использованием хаотических сигналов.

Сравнительный анализ параметров методов задержанной координаты и сингулярного спектрального анализа входных и выходных последовательностей алгоритмов шифрования с использованием хаотических сигналов, DES и AES показал значимые отличия в параметрах входных и выходных последовательностей; практическое совпадение по уровню главных компонент в режиме СВС; улучшение параметров корреляционной размерности и энтропии Колмогорова для алгоритма шифрования с использованием динамического хаоса, что, в целом, может служить основанием для рекомендаций к использованию указанных методов при разработке требований к обеспечению информационной безопасности.

THE CONTROL OF THE CHAOTIC REGIMES IN ENCRYPTION ALGORITHM BASED ON DYNAMIC CHAOS

A.V. SIDORENKO

Abstract

The paper presents two approaches to control of chaotic regimes in encryption algorithm based on dynamic chaos by delayed coordinate methods and singular spectral analyzing methods. The comparative analysis of the parameters for the input and output sets used in encryption algorithms based on a dynamic chaos with standard AES, DES ciphers was performed. It was shown that the parameters characterizing the output sets for the encryption algorithm based on dynamic chaos are not bad relative to those the standard ciphers.

Список литературы

1. *Алферов А.П. Зубов А.Ю., Кузьмин А.С. и др.* Основы криптографии. М., 2005.
2. *Cuomo R.M., Oppenheim A.V.* // Phys. Rev. Let. 1993. P. 65–68.
3. *Dmitriev A.A., Dmitriev A.S., Andreev Y.V.* // Applications of Chaos and Nonlinear Dynamics in Science and Engineering. 2013. Vol. 3.
4. *Птицын Н.* Приложение теории детерминированного хаоса в криптографии. М., 2002.
5. *Анищенко В.С.* Нелинейные эффекты в хаотических и стохастических системах. М., 2003.
6. *Alvares G., Montoya F., Romera M.* // Phys. Lat. A. 2003. Vol. 319. P. 334–339.
7. *Pastor G.A., Romera M., Mentoya F.* // Physica. 1997. Vol. 107. P. 17–22.
8. *Сидоренко А.В., Мулярчик К.С.* // Докл. БГУИР. 2013. № 1. С. 62–67.
9. *Сидоренко А.В.* Информационные аспекты нелинейной динамики. Минск, 2008.
10. Главные компоненты временных рядов: метод «Гусеница» / Под ред. Д.Л. Данилова, А.А. Жиглявского. СПб, 1997.