- Голубенко Н.Б.
- Иванов Г.П.
- Кайнов А.Б.
- Каравдин П.А.
- Миркин В.И.
- Мотков О.И.
- Недосекин Ю.А.
- Петров В.В.
- Хмельник С.И.

ISBN 978-0-557-72797-1
90000
ID: 9487789
www.lulu.com
9 780557 727971

The Papers of independent Authors, volume 16

2010 выпуск №16

Доклады Независимых Авторов

- Гидродинамика
- Гидродинамика
- Криптография
- Педагогика
- Психология
- Физика и астрономия
- Эволюция

Доклады Независимых Авторов

Периодическое многопрофильное научно-техническое издание

Выпуск № 16

Россия - Израиль
2010

The Papers of independent Authors

(volume 16, in Russian)

Russia - Israel
2010

Отправлено в печать **15.10.2010**
Напечатано в США, Lulu Inc., каталожный № **9487789**
ISBN 978-0-557-72797-1
Сайт со сведениями для автора - http://dna.izdatelstwo.com
Контактная информация - publisher-dna@hotmail.com
Факс: ++972-8-8691348
Адрес: POB 15302, Bene-Ayish, Israel, 60860
Форма ссылки: *Автор. Статья*, «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 16, printed in USA, Lulu Inc., ID 9487789, ISBN 978-0-557-72797-1

Истина – дочь времени, а не авторитета.

Френсис Бэкон

Каждый человек имеет право на свободу убеждений и на свободное выражение их; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ.

Организация Объединенных Наций.
Всеобщая декларация прав человека. Статья 19

От издателя

"Доклады независимых авторов" - многопрофильный научно-технический печатный журнал на русском языке. Журнал принимает статьи к публикации из России, стран СНГ, Израиля, США, Канады и других стран. При этом соблюдаются следующие правила:

1) статьи не рецензируются и издательство не отвечает за содержание и стиль публикаций,
2) автор оплачивает публикацию,
3) журнал регистрируется в международном классификаторе книг ISBN, передается и регистрируется в основных библиотеках России, библиотеке Конгресса США, национальной и университетской библиотеке Израиля,
4) приоритет и авторские права автора статьи обеспечиваются регистрацией журнала в ISBN,
5) коммерческие права автора статьи сохраняются за автором,
6) журнал издается в США,
7) журнал продается в интернете и в тех магазинах, которые решат его приобрести, пользуясь указанным международным классификатором.

Этот журнал - для тех авторов, которые уверены в себе и не нуждаются в одобрении рецензента. Нас часто упрекают в том, что статьи не рецензируются. Но институт рецензирования не является идеальным фильтром - пропускает неудачные статьи и задерживает оригинальные работы. Не анализируя многочисленные причины этого, заметим только, что, если плохие статьи может отфильтровать сам читатель, то выдающиеся идеи могут остаться неизвестными. Поэтому мы - за то, чтобы ученые и инженеры имели право (подобно писателям и художникам) публиковаться без рецензирования и не тратить годы на "пробивание" своих идей.

Хмельник С.И.

Содержание

Серия: **ГИДРОДИНАМИКА**

Хмельник С. И.

Существование глобального решения уравнений Навье-Стокса для сжимаемой жидкости

Аннотация

Формулируется и доказывается вариационный принцип экстремума для вязкой сжимаемой жидкости, из которого следует, что уравнения Навье-Стокса являются условиями экстремума некоторого функционала. Формулируются необходимые и достаточные условия существования глобального экстремума этого функционала.

Оглавление

Введение

В [1] автор предложил принцип экстремума полного действия, позволяющий конструировать функционал для диссипативных систем, а затем в [2] и, более подробно, в [3] применил этот принцип для доказательства существования глобального решения уравнений Навье_Стокса для вязкой несжимаемой жидкости. В этой статье данный принцип применяетсч к уравнениям Навье_Стокса для сжимаемой жидкости..

Рассматриваются уравнения Навье-Стокса для вязкой сжимаемой жидкости. Показывается, что эти уравнения являются условиями экстремума некоторого функционала. Описывается метод поиска решения этих уравнений, который состоит в движении по градиенту к экстремуму этого функционала. Формулируются условия достижения этого экстремума, которые являются одновременно

необходимыми и достаточными условиями существования глобального экстремума этого функционала.

1. Уравнения гидродинамики

Уравнения гидродинамики для вязкой несжимаемой жидкости имеют следующий вид [4]:

$$\operatorname{div}(v) = 0, \tag{1}$$

$$\rho \frac{\partial v}{\partial t} + \nabla p - \mu \cdot \Delta v + \rho \cdot G(v) - \rho \cdot F = 0, \tag{2}$$

где

$$G(v) = (v \cdot \nabla) v \tag{3}$$

и

ρ - постоянная плотность, постоянная для сжимаемой жидкости,

μ - коэффициент внутреннего трения,

p - неизвестное давление,

$v = \lfloor v_x, v_y, v_z \rfloor$ - неизвестная скорость, вектор,

$F = \lfloor F_x, F_y, F_z \rfloor$ - известная массовая сила, вектор,

x, y, z, t - пространственные координаты и время.

В отличие от этого уравнения гидродинамики для вязкой сжимаемой жидкости имеют следующий вид [4]:

$$\frac{\partial \rho}{\partial t} + \operatorname{div}(\rho \cdot v) = 0, \tag{4}$$

$$\rho \frac{\partial v}{\partial t} + \nabla p - \mu \cdot \Delta v + \rho \cdot G(v) - \rho \cdot F - \frac{\mu}{3} \Omega(v) = 0, \tag{5}$$

где

$$\Omega(v) = \nabla(\nabla v). \tag{6}$$

В приложении функции (3) и (6) представлены в развернутом виде – см. (p1, p2, p3). Для сжимаемой жидкости плотность является известной функцией давления:

$$\rho = f(p). \tag{7}$$

Далее будем рассуждать по аналогии с [2].

2. Энержиан и квазиэкстремаль

Для сжимаемой жидкости неизвестными являются функции давления и скорости, поскольку давление определяется по (7). Для дальнейшего объединим неизвестные функции в вектор вида

$$q = [p, v] = \lfloor p, v_x, v_y, v_z \rfloor . \quad (11)$$

Этот вектор и все его компоненты являются функциями от (x, y, z, t). Рассматривается поток жидкости в объеме V. Полное действие в представим в виде

$$\Phi = \int_0^T \left\{ \oint_V \Re(q(x, y, z, t) dV \right\} dt . \quad (12)$$

Для несжимаемой жидкости энержиан имеет следующий вид [2]:

$$\Re(q) = \rho \cdot v \frac{dv}{dt} + \mu \cdot v \cdot \Delta v - \operatorname{div}(v \cdot p) + \rho \cdot v \cdot G(v) - \rho F v . \quad (13)$$

Для сжимаемой жидкости энержиан рассмотрим в следующем виде :

$$\Re(q) = \left\{ \begin{array}{l} \rho \cdot v \dfrac{dv}{dt} + \mu \cdot v \cdot \Delta v - \dfrac{1}{\rho} \operatorname{div}(\rho \cdot p \cdot v) + \\ + p \cdot v \cdot G(v) - p \cdot F v - \dfrac{p}{\rho} \dfrac{\partial \rho}{\partial t} - \dfrac{\mu}{3} v \cdot \Omega(v) \end{array} \right\} . \quad (14)$$

Далее будем обозначать производную, вычисляемую по формуле Остроградского (р6), символом $\frac{\partial_o}{\partial v}$, в отличие от обычной частной производной $\frac{\partial}{\partial v}$.

Квазиэкстремаль для несжимаемой жидкости имеет следующий вид [2]:

$$\left\{ \begin{array}{l} \dfrac{\partial}{\partial v}\left(\rho \cdot v \dfrac{dv}{dt} \right) + \mu \cdot \dfrac{\partial}{\partial v}(v \cdot \Delta v) + \dfrac{\partial_o}{\partial q}(\operatorname{div}(p \cdot v)) + \\ + \dfrac{\partial}{\partial v}(\rho \cdot v \cdot G(v)) - \dfrac{\partial}{\partial q}(\rho \cdot v \cdot F) \end{array} \right\} = 0 . \quad (15)$$

По аналогии с этим запишем квазиэкстремаль для сжимаемой жидкости в следующем виде:

$$\left\{\begin{array}{l}\dfrac{\partial}{\partial v}\left(\rho\cdot v\dfrac{dv}{dt}\right)+\mu\cdot\dfrac{\partial}{\partial v}(v\cdot\Delta v)+\dfrac{\partial_o}{\partial q}\left(\dfrac{1}{\rho}\operatorname{div}(\rho\cdot p\cdot v)\right)+\\ +\dfrac{\partial}{\partial v}(\rho\cdot v\cdot G(v))-\dfrac{\partial}{\partial v}(\rho\cdot F\cdot v)-\\ -\dfrac{\partial}{\partial p}\left(\dfrac{p}{\rho}\dfrac{\partial\rho}{\partial t}\right)-\dfrac{\mu}{3}\cdot\dfrac{\partial}{\partial v}(v\cdot\Omega(v)).\end{array}\right\}=0. \quad (16)$$

3. Расщепленный энержиан

Рассмотрим расщепленные функции (11) в виде

$$q'=[p',v']=\lfloor p',v'_x,v'_y,v'_z\rfloor, \quad (21)$$

$$q''=[p'',v'']=\lfloor p'',v''_x,v''_y,v''_z\rfloor. \quad (22)$$

Расщепленный энержиан для несжимаемой жидкости имеет следующий вид [2]:

$$\Re_2(q',q'')=\left\{\begin{array}{l}\rho\cdot\left(v'\dfrac{dv''}{dt}-v''\dfrac{dv'}{dt}\right)-\mu\cdot(v'\Delta v'-v''\Delta v'')\\ +(\operatorname{div}(v'\cdot p'')-\operatorname{div}(v''\cdot p'))+\\ \rho\cdot(v'G(v'')-v''G(v'))-\rho\cdot F(v'-v'')\end{array}\right\}. \quad (23)$$

По аналогии с этим запишем расщепленный энержиан для сжимаемой жидкости в следующем виде:

$$\Re_2(q',q'')=\left\{\begin{array}{l}\rho\cdot\left(v'\dfrac{dv''}{dt}-v''\dfrac{dv'}{dt}\right)-\mu\cdot(v'\Delta v'-v''\Delta v'')\\ +\dfrac{1}{\rho}((\operatorname{div}(\rho\cdot v'\cdot p'')-\operatorname{div}(\rho\cdot v''\cdot p')))+\\ \rho\cdot(v'G(v'')-v''G(v'))-\rho\cdot F(v'-v'')-\\ \dfrac{1}{\rho}\left(p'\dfrac{d\rho}{dt}-p''\dfrac{d\rho}{dt}\right)-\dfrac{\mu}{3}\cdot(v'\Omega(v')-v''\Omega(v''))\end{array}\right\}. \quad (24)$$

Функционалу (12) поставим в соответствие функционал расщепленного полного действия

$$\Phi_2 = \int_0^T \left\{ \oint_V \Re_2(q', q'')dV \right\} dt, \tag{25}$$

По формуле Остроградского (р6) найдем вариации функционала (25) от функций q'

$$\frac{\partial_o \Re_2}{\partial p'} = b_{p'}, \tag{26}$$

$$\frac{\partial_o \Re_2}{\partial v'} = b_{v'}, \tag{27}$$

Эти вариации определяются при варьировании функций p' и v', тогда как функции ρ, p'', v'' не изменяются. При этом получим:

$$1)\ \frac{\partial}{\partial v'}\left[\rho \cdot \left(v'\frac{dv''}{dt} - v''\frac{dv'}{dt}\right)\right] = 2\rho\frac{dv''}{dt},$$

$$2)\ \frac{\partial}{\partial v'}\left[-\mu \cdot \left(v'\Delta v' - v''\Delta v''\right)\right] = -2\mu \cdot \Delta v',$$

$$3)\ \frac{\partial}{\partial v'}\left[\rho\left(v'G(v'') - v''G(v')\right)\right] = 2\rho \cdot \left[G\left(v'', \frac{\partial v''}{\partial X}\right) + G\left(v', \frac{\partial v''}{\partial X}\right)\right],$$

$$4)\ \frac{\partial}{\partial v'}\left[-\rho \cdot F\left(v' - v''\right)\right] = -\rho \cdot F,$$

$$5)\ \frac{\partial}{\partial v'}\left[-\frac{\mu}{3} \cdot \left(v'\Omega(v') - v''\Omega(v'')\right)\right] = -\frac{2\mu}{3} \cdot \Omega(v'),$$

$$6)\ \frac{\partial}{\partial v'}\left[\frac{1}{\rho}\left(\mathrm{div}(\rho \cdot v' \cdot p'') - \mathrm{div}(\rho \cdot v'' \cdot p')\right)\right] = \mathrm{grad}(p''),$$

$$7)\ \frac{\partial}{\partial p'}\left[\frac{1}{\rho}\left(\mathrm{div}(\rho \cdot v' \cdot p'') - \mathrm{div}(\rho \cdot v'' \cdot p')\right)\right] = -\frac{1}{\rho}\mathrm{div}(\rho \cdot v''),$$

$$8)\ \frac{\partial}{\partial p'}\left[-\frac{1}{\rho}\left(p'\frac{d\rho}{dt} - p''\frac{d\rho}{dt}\right)\right] = -\frac{1}{\rho}\frac{d\rho}{dt}. \tag{28}$$

Замечания к этим формулам:

1, 2, 3, 4) – вывод приведен в {2],

5) – аналогчна формуле 2),

6, 7) - вывод приведен в приложении – см. (р11, р10) соответственно.

При этом имеем:

$$b_{p'} = -\frac{d\rho}{dt} - 2\mathrm{div}(\rho \cdot v''), \tag{29}$$

$$b_{v'} = \left\{ \begin{array}{l} 2\rho \cdot \dfrac{dv''}{dt} - 2\mu \cdot \Delta(v') - \dfrac{2\mu}{3} \cdot \Omega(v') + 2\nabla(p'') \\ + 2\rho \cdot \left[G\left(v'', \dfrac{\partial v''}{\partial X}\right) + G\left(v', \dfrac{\partial v''}{\partial X}\right) \right] - \rho \cdot F \end{array} \right\}. \tag{30}$$

Как показано в [2], условие

$$b' = \lfloor b_{p'},\ b_{v'} \rfloor = 0 \tag{31}$$

и аналогичное ему условие

$$b'' = \lfloor b_{p''},\ b_{v''} \rfloor = 0 \tag{32}$$

являются необходимыми условиями для существования седловой линии. Из симметрии этих уравнений следует, что оптимальные функции q'_0 и q''_0, удовлетворяющие уравнениям (31, 32), удовлетворяют также условию

$$q'_0 = q''_0. \tag{33}$$

Вычитая попарно уравнения (31, 32) с учетом (29, 30), получаем

$$-2\frac{\mathrm{d}\rho}{\mathrm{dt}} - 2\mathrm{div}(v' + v'') = 0, \tag{34}$$

$$\left\{ \begin{array}{l} + 2\rho \cdot \dfrac{d(v' + v'')}{dt} - 2\mu \cdot \Delta(v' + v'') - \dfrac{2\mu}{3} \cdot \Omega(v' + v'') + \\ + 2\nabla(p' + p'') - 2\rho \cdot F + 2\rho \cdot \left[\begin{array}{l} G\left(v'', \dfrac{\partial v''}{\partial X}\right) + G\left(v', \dfrac{\partial v''}{\partial X}\right) + \\ + G\left(v', \dfrac{\partial v'}{\partial X}\right) + G\left(v'', \dfrac{\partial v'}{\partial X}\right) \end{array} \right] \end{array} \right\} = 0. \tag{35}$$

В [2] показано, что

$$\left[G(v'') + G\left(v', \frac{\partial v''}{\partial X}\right) + G(v') + G\left(v'', \frac{\partial v'}{\partial X}\right) \right] = G(v' + v'') \tag{36}$$

Учитывая (45) и сокращая (34, 35) на 2, получаем уравнения (4, 5), где

$$q = q'_o + q''_o, \tag{37}$$

т.е. уравнения экстремальной линии являются уравнениями Навье-Стокса для сжимаемой жидкости.

4. О достаточных условиях экстремума

В [2, 3] для несжимаемой жидкости показано, что необходимые условия (31, 32) существования экстремума функционала (34) являются также и достаточными, если величина интеграла

$$I = \int_0^T \left\{ \oint_V \Re_{22} dV \right\} dt \qquad (41)$$

является знакопостоянной, где

$$\Re_{22} = -\mu b_v \Delta(b_v) - 2\rho v'' G(b_v). \qquad (42)$$

Не повторяя приведенные там выкладки отметим, что для сжимаемой жидкости показано, что необходимые условия (31, 32) существования экстремума функционала (25) являются также и достаточными, если величина интеграла (41) является знакопостоянной, где, в отличие от (42),

$$\Re_{22} = -\mu b_v \Delta(b_v) - \frac{\mu}{3} b_v \Omega(b_v) - 2\rho v'' G(b_v). \qquad (43)$$

В [2, 3] среди расчитываемых объемов потока жидкости можно выделяются замкнутые объемы потока жидкости, которые не обмениваются потоком с соседними объемами – т.н. замкнутые системы. Можно утверждать, что системы, описываемые уравнениями Навье-Стокса и имеющие определенные граничные условия (давления или скорости) на всех границах, являются замкнутыми. Для замкнутых систем с потоком несжимаемой жидкости там показано, что величина (42) приобретает вид

$$\Re_{22} = -\mu b_v \Delta(b_v). \qquad (44)$$

Аналогично, для замкнутых систем с потоком сжимаемой жидкости величина (43) приобретает вид

$$\Re_{22} = -\mu b_v \Delta(b_v) - \frac{\mu}{3} b_v \Omega(b_v). \qquad (45)$$

Рассмотрим аналогично [2, 3] интеграл

$$J = \int_0^T \left\{ \oint_V \Re'_{22} dV \right\} dt \qquad (46)$$

где

$$\Re'_{22} = -\mu \cdot v \cdot \Delta(v) - \frac{\mu}{3} v \cdot \Omega(v). \qquad (47)$$

(т.е. в эту формулу вместо функции b_v входит функция скорости). Поскольку доказательство знакопостоянства интеграла должно распространятся на любые функции, достаточно доказать знакопостоянство интеграла (46) со скоростями. Для этого заметим, что

- первое слагаемое в (47) выражает тепловую энергию, выделяемую жидкостью в результате внутреннего трения,
- второе слагаемое в (47) выражает тепловую энергию, выделяемую\поглощаемую жидкостью в результате расширения\сжатия.

Первая энергия положительна вне зависимости от того, какова функция вектора скорости от координат. (Более строгое доказательство этого утверждения для первого сдагаемого дано в [2, 3]). Вторая энергия в сумме рана нулю (поскольку в данной постановке задачи температура не учитывается, т.е. принимается постоянной). Следовательно, интеграл (41, 47) имеет положительное значение на любой итерации, что и требовалось показать.

Таким образом, уравнения Навье-Стокса для сжимаемой жидкости имеют глобальное решение.

Приложение

Некоторые формулы:

$$G = \begin{bmatrix} v_x \dfrac{\partial v_x}{\partial x} + v_y \dfrac{\partial v_x}{\partial y} + v_z \dfrac{\partial v_x}{\partial z} \\ v_x \dfrac{\partial v_y}{\partial x} + v_y \dfrac{\partial v_y}{\partial y} + v_z \dfrac{\partial v_y}{\partial z} \\ v_x \dfrac{\partial v_z}{\partial x} + v_y \dfrac{\partial v_z}{\partial y} + v_z \dfrac{\partial v_z}{\partial z} \end{bmatrix}, \qquad (p1)$$

$$\Omega(v) = \left[\frac{\partial(\mathrm{div}(v))}{\partial x}, \frac{\partial(\mathrm{div}(v))}{\partial y}, \frac{\partial(\mathrm{div}(v))}{\partial z} \right], \qquad (p2)$$

$$\Omega(v)=\begin{bmatrix}\dfrac{\partial^2 v_x}{\partial x^2}+\dfrac{\partial^2 v_y}{\partial x\partial y}+\dfrac{\partial^2 v_z}{\partial x\partial z}\\ \dfrac{\partial^2 v_x}{\partial x\partial y}+\dfrac{\partial^2 v_y}{\partial y^2}+\dfrac{\partial^2 v_z}{\partial y\partial z}\\ \dfrac{\partial^2 v_x}{\partial x\partial z}+\dfrac{\partial^2 v_y}{\partial y\partial z}+\dfrac{\partial^2 v_z}{\partial z^2}\end{bmatrix}, \qquad (р3)$$

Необходимые условия экстремума функционала от функций нескольких независимых переменных – уравнения Остроградского [5] имеют для каждой функции вид

$$\frac{\partial_o f}{\partial v}=\frac{\partial f}{\partial v}-\sum_{a=x,y,z,t}\left[\frac{\partial}{\partial a}\left(\frac{\partial f}{\partial(dv/da)}\right)\right]=0, \qquad (р6)$$

где f – подынтегральное выражение, $v(x,y,z,t)$ – переменная функция, a - независимая переменная.

Если ρ, p — скалярные поля, а v — векторное поле, то

$$\operatorname{div}(\rho\cdot v)=v\cdot\operatorname{grad}(\rho)+\rho\cdot\operatorname{div}(v), \qquad (р7)$$

$$\operatorname{div}(\rho\cdot p\cdot v)=\rho\cdot v\cdot\operatorname{grad}(p)+p\cdot\operatorname{div}(\rho\cdot v), \qquad (р8)$$

т.е.

$$\operatorname{div}(\rho\cdot p\cdot v)=\rho\cdot v\cdot\operatorname{grad}(p)+p\cdot v\cdot\operatorname{grad}(\rho)+p\cdot\rho\cdot\operatorname{div}(v). \qquad (р9)$$

Рассмотрим $\operatorname{div}(\rho\cdot p'\cdot v'')$ и будем полагать, что экстремум некоторого функционала определяется либо при варьировании функции p', либо при варьировании функции v''. Тогда, дифференцируя последнее выражение по формуле Остроградского (р6), найдем:

$$\frac{\partial_o}{\partial p'}\left[\operatorname{div}(\rho\cdot p'\cdot v'')\right]=0+v''\cdot\operatorname{grad}(\rho)+\rho\cdot\operatorname{div}(v''),$$

$$\frac{\partial_o}{\partial v''}\left[\operatorname{div}(\rho\cdot p'\cdot v'')\right]=\rho\cdot\operatorname{grad}(p')+p'\cdot\operatorname{grad}(\rho)-p'\cdot\operatorname{grad}(\rho)$$

или

$$\frac{\partial_o}{\partial p'}\left[\operatorname{div}(\rho \cdot p' \cdot v'')\right] = \operatorname{div}(\rho \cdot v''), \qquad (p10)$$

$$\frac{\partial_o}{\partial v''}\left[\operatorname{div}(\rho \cdot p' \cdot v'')\right] = \rho \cdot \operatorname{grad}(p'). \qquad (p11)$$

Литература

1. Хмельник С.И. Принцип экстремума полного действия, «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 15, printed in USA, Lulu Inc., ID 8976094, ISBN 978-0-557-52134-0.
2. Хмельник С.И. Существование и метод поиска глобального решения для уравнений Навье-Стокса, «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 15, printed in USA, Lulu Inc., ID 8976094, ISBN 978-0-557-52134-0
3. Хмельник С.И. Уравнения Навье-Стокса. Существование и метод поиска глобального решения. Published by "MiC" - Mathematics in Computer Comp., printed in USA, Lulu Inc., ID 8828459. Израиль, 2010, ISBN 978-0-557-48083-8.
4. Н.Е. Кочин, И.А. Кибель, Н.В. Розе. Теоретическая гидромеханика, часть 2. Гос. изд. "Физматлит", Москва, 1963, 727 с.
5. Эльсгольц Л.Э. Дифференциальные уравнения и вариационное исчисление, Эдиториал УРСС, Москва, 2000.

Серия: **КРИПТОГРАФИЯ**

Недосекин Ю.А.

Алгоритм нераскрываемого шифра

Аннотация

Предложен алгоритм нераскрываемого поточного шифра.

В работе [1] были изложены алгоритмы шифрования и дешифрования, в которых на каждом шаге t шифрования знак

$$j_t = j'_{t-1}, \quad (1)$$

где $t = 1, 2, ..., \Delta$, Δ – длина открытого текста.

Знак j_t при шифровании может быть задан и в общей форме

$$j_t = \begin{cases} j'_{t-1} & , \quad t \le \delta \\ j'_{t-l_\gamma} & , \quad \gamma = 1, 2, ..., \delta , \quad t > \delta \end{cases}, \quad (2)$$

где $l_\gamma \ge 1$ – некоторые целые числа последовательности

$$L = l_1 l_2 ... l_\delta \quad (3)$$

длиной δ, начальное состояние системы $j'_0 \in \{0, 1, 2, ..., 2^k - 1\}$ выбираем произвольно. Номер γ определяет положение числа l_γ в последовательности (3) и его значение связано с шагом t шифрования соотношением

$$\gamma = \begin{cases} t \bmod \delta , & t \bmod \delta \ne 0 \\ \delta & , \quad t \bmod \delta = 0 \end{cases}, \quad t > \delta . \quad (4)$$

Для $t = \delta + 1, \delta + 2, ..., 2\delta$ число l_γ выбираем таким, чтобы получить разные значения $t - l_\gamma$, заполняющие весь отрезок $[1, \delta]$. При этом среди всех чисел l_γ могут быть и совпадающие.

По известному из соотношений (4) номеру γ определяем число l_γ в последовательности (3), которое используется в формуле (2).

Номер γ можно определять также и следующим способом:

начиная с $t = \delta$ фиксируем каждый раз значение t, кратное δ, тогда

$$\gamma = t - t_s, \text{ где } t_s = s\delta, \quad s = 1,2,..., \quad t > t_s, \qquad (5)$$

где t_s – фиксированное значение t.

Последовательности L следует придать статус секретности, в результате чего она будет выполнять роль дополнительного ключа, затрудняющего проведение криптоанализа.

Формулу (2) можно применить к любому алгоритму, рассмотренному в работе [1]. Здесь же мы остановимся на алгоритме 4.В [1] для системы с ключом K_{ij}^{i1}. О значениях верхних и нижних индексах в ключе K_{ij}^{ij} сказано в пункте 3 [1]. Для удобства чтения данной работы приведем этот алгоритм полностью с небольшими изменениями, связанными с формулой (2) и ключом K_{ij}^{i1}.

Шифрование и расшифрование при базисе $\mu = q$

Напомним, что i_t, i'_t – m-значные, а j_t, j'_t – k-значные числа, записанные в q-ичной системе счисления.

Алгоритм шифрования.

Исходные данные: открытый текст $I = i_1 i_2 ... i_\Delta$ (Δ – длина текста) и начальное состояние j'_0 системы, произвольно выбираемое из множества $\{0, 1, 2,..., q^k - 1\}$.

1. $v_t = i_t(k<) + j_t$, $t = 1, 2,..., \Delta$, где v_t – содержимое таблицы v с координатами i'_t, j'_t, значение j_t определяем по формуле (2).
2. По таблице v из $v_t \Rightarrow i'_t$, j'_t.

Результатами шифрования являются: шифртекст $I' = i'_1 i'_2 ... i'_\Delta$ и $r = \begin{cases} \gamma_\Delta + \delta, & \gamma_\Delta \neq \delta \\ \delta, & \gamma_\Delta = \delta \end{cases}$ последних значений j_t, где γ_Δ – последнее значение номера последовательности (3), используемое при шифровании.

Алгоритм расшифрования.

Исходные данные: шифртекст $I' = i'_1 i'_2 ... i'_\Delta$ и $r = \begin{cases} \gamma_\Delta + \delta, & \gamma_\Delta \neq \delta \\ \delta, & \gamma_\Delta = \delta \end{cases}$ последних значений j_t, где γ_Δ – последнее значение номера последовательности (3), используемое при шифровании.

1. Для $r = \begin{cases} \gamma_\Delta + \delta, & \gamma_\Delta \neq \delta \\ \delta, & \gamma_\Delta = \delta \end{cases}$ значений j_t из таблицы v однозначно определяем по i'_t знак i_t, а по j_t – знак $j'_{t-l_\gamma} = j_t$, где γ находим из соотношений (4) или же по формулам (5), а по нему из (3) находим l_γ, знаки j'_t на данном отрезке шагов знать не надо, $t = \Delta, \Delta - 1, ..., \Delta - r + 1$.
2. По координатам i'_t, j'_t таблицы v определяем содержимое v_t соответствующей ячейки, $t = \Delta - r, \Delta - r - 1, ..., \delta + 1$.
3. Из v_t для $t = \Delta - r, \Delta - r - 1, ..., \delta + 1$ определяем: $i_t = v_t(k>)$, $j'_{t-l_\gamma} = j_t = v_t(m<, m>)$.
4. Для $t = \delta, \delta - 1, ..., 1$ по координатам i'_t, j'_t таблицы v определяем значение v_t, из которого находим $i_t = v_t(k>)$, $j'_{t-1} = j_t = v_t(m<, m>)$.

Результатами расшифрования являются:
открытый текст $I = i_1 i_2 ... i_\Delta$ и начальное состояние j'_0 системы.

Пример. Система $[q, \mu, m, k] = [2, 2, 1, 3]$, $n = m + k = 4$, ключ K_{01}^{01}, длина открытого текста $\Delta = 30$ знаков i_t, $t = 1, 2, ..., 30$, $\delta = 7$ – длина последовательности L.

i_t – однозначные знаки, j_t – трехзначные знаки в двоичной системе счисления. Знаки j_t для удобства восприятия в ключе и в таблицах шифрования и дешифрования записываем в десятичной системе счисления.

Используя формулы (3) и (4) совместно с указанным выше алгоритмом построения последовательности L, запишем ее в виде следующей таблицы.

γ	1	2	3	4	5	6	7
l_γ	5	3	9	4	10	8	10

Номер γ при шифровании будем определять по формулам (5), выделяя фиксированные значения t_s жирным шрифтом.

Из множества $\{0, 1, 2,..., q^k - 1\} = \{0,1,2,3,4,5,6,7\}$ произвольно выбираем значение начального состояния $j'_0 = 5$ системы, записанное в десятичной системе счисления.

Напомним (см. пункт 1 [1]), что для построения ключа любого типа необходимо учитывать, что содержимое каждой его ячейки должно находиться в нем (в таблице v) только один раз.

Таблица v
Ключ $K_{ij}^{ij} = K_{01}^{01}$

i'	0		1	
j'	i	j	i	j
0	0	2	1	5
1	0	5	0	3
2	1	1	1	2
3	0	0	0	1
4	1	4	1	6
5	0	7	1	0
6	0	6	1	7
7	1	3	0	4

Связь между системами счисления								
$q=2$	000	001	010	011	100	101	110	111
$q=10$	0	1	2	3	4	5	6	7

Шифрование						Дешифрование				
t	i_t	j_t	i'_t	j'_t		t	i_t	j_t	i'_t	j'_t
0				5		0				5
1	1	5	1	0		1	1	5	1	0
2	0	0	0	3		2	0	0	0	3

3	0	3	1	1		3	0	3	1	1
4	1	1	0	2		4	1	1	0	2
5	0	2	0	0		5	0	2	0	0
6	1	0	1	5		6	1	0	1	5
7	1	5	1	0		**7**	1	5	1	0
8	1	1	0	2		8	1	1	0	2
9	0	5	0	1		9	0	5	0	1
10	0	0	0	3		10	0	0	0	3
11	1	0	1	5		11	1	0	1	5
12	1	3	0	7		12	1	3	0	7
13	0	0	0	3		13	0	0	0	3
14	1	2	1	2		**14**	1	2	1	2
15	1	3	0	7		15	1	3	0	7
16	1	3	0	7		16	1	3	0	7
17	1	2	1	2		17	1	2	1	2
18	0	2	0	0		18	0	2	0	0
19	0	1	1	3		19	0	1	1	3
20	0	7	0	5		20	0	7	0	5
21	1	5	1	0		**21**	1	5	1	0
22	1	2	1	2		22	1	2	1	
23	0	5	0	1		23	0	5	0	
24	1	7	1	6		24	1	7	1	
25	0	0	0	3		25	0	0	0	
26	1	7	1	6		26	1	7	1	
27	1	3	0	7		27	1	3	0	
28	0	0	0	3		**28**	0	0	0	
29	1	6	1	4		29	1	6	1	
30	1	7	1	6		30	1	7	1	

Результатами шифрования являются:

шифртекст – в столбце i'_t , $\gamma_\Delta = \gamma_{30} = 30 - 28 = 2$,

$r = \gamma_\Delta + \delta = 2 + 7 = 9$ последних значений j_t:

t	30	29	28	27	26	25	24	23	22
j_t	7	6	0	3	7	0	7	5	2

Для расшифрования полученного шифртекста исходными данными являются результаты шифрования.

Результатами выполненного дешифрования являются:

открытый текст в столбце i_t и начальное состояние $j'_0 = 5$ системы.

Криптоанализ, изложенный в пункте 8 [1], остается в силе и для описанного в данной работе алгоритма. К тому же он еще сильнее

усложняется из-за последовательности L, введенной в процесс шифрования. В итоге все это делает невозможным раскрытие шифра, составленного по описанному в данной работе алгоритму. Если кто-то думает иначе, то пусть попробует.

Литература

1. Недосекин Ю.А. Преобразование и защита информации. «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 16.

Недосекин Ю.А.

Генерирование псевдослучайных чисел

Аннотация

Рассмотрен алгоритм построения непериодической последовательности псевдослучайных чисел и приведено пять примеров такого построения. Для периодических последовательностей псевдослучайных чисел предложены программы на языке Си с иллюстрациями их работ.

Оглавление

На основе описанных в работе [1] алгоритмов и свойств криптосистем можно образовать достаточно много программных генераторов псевдослучайных чисел (ГПСЧ).

1. Непериодическая последовательность псевдослучайных чисел

Изложим способ построения генерирования непериодической последовательности псевдослучайных чисел. Для этого используем системы с произвольным ключом K_{ij}^{ij} без замкнутых циклов. Применяем однократное шифрование по алгоритмам **2.A** и **2.E** (**4.A**, **4.B**) [1], в которых открытый текст I состоит из знаков $i_t = i'_{t-\delta}$, $\delta \geq 1$ – целое положительное число. Последовательность псевдослучайных чисел, образуемая ГПСЧ, состоит из знаков i'_t: для фиксированного t последовательность $L_\delta^t = i'_{t-(\delta-1)} i'_{t-(\delta-2)} ... i'_{t-1} i'_t$ имеет длину δ, $t = 0, 1, 2, ..., \Delta$, где Δ – длина всей последовательности, начальная последовательность L_δ^0 длины δ из m-битовых знаков задается произвольно.

Алгоритм ГПСЧ.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 3$.

1. Шифрование на шаге t, знак открытого текста $i_t = i'_{t-\delta}$.

2. Сравнение:

$$L_\delta^{t_p} = L_\delta^{t_{p-1}}, \quad j'_{t_p} = j'_0, \quad (x_l^{t_p}) = (x_l^0) \text{ äëÿ } \mu > q, \qquad (1)$$

где все равенства выполняются одновременно;

если ДА, то переход к пункту 3;

если НЕТ, то переход к пункту 1: $t \to t+1$;

в (1): $t_p = t$ – номер шага шифрования; $p \geq 1$ целое положительное число – номер сравнения, при котором выполняются все равенства (1) одновременно; $t_0 = 0$, начальное значение $p = 1$.

3. $L_\delta^{t_p} \to L_{\delta+1}^{t_p} = i'_{t_p-\delta} L_\delta^{t_p}$, $\delta \to \delta + 1$, $p \to p + 1$.

Результатом работы ГПСЧ является бесконечная непериодическая последовательность $L = i'_1 i'_2 ... i'_t ...$ псевдослучайных чисел i'_t. Последовательность L может быть восстановлена при шифровании, исходя из L_δ^0, j'_0, (x_l^0), а также в обратном порядке

при дешифровании, исходя из известных $L_{\delta}^{t_p}$, j'_{t_p}, $(x_l^{t_p})$, $t_p = \Delta$.

Пример 1. Система $[q, \mu, m, k] = [2, 2, 1, 1]$, $n = m + k = 2$, K_{21}^{11}, $\delta = 1$, $L_{\delta}^{0} = i'_0 = 0$, $j'_0 = 0$.

Образуемые последовательности $L_{\delta+1}^{t_p}$ вместе с $j'_{t_p} = j'_0 = 0$ в общей последовательности L выделены жирным шрифтом с указанием номера p. Так как в примерах мы берем достаточно длинные последовательности L, то таблицы шифрования в них полностью не приводятся. Желающие при необходимости могут заполнить пробелы в этой таблице. В полученной последовательности L длиной $\Delta = 1261$ знак выделим группы последовательных знаков i'_t и подсчитаем их частоты ω, таблица 1.

Пример 2. Система $[q, \mu, m, k] = [2, 2, 1, 2]$, $n = m + k = 3$, K_{21}^{01}, $\delta = 1$, $L_{\delta}^{0} = i'_0 = 0$, $j'_0 = 0$.

Длина полученной последовательности $\Delta = 1348$ знаков. Частотное распределение в таблице 1.

Пример 3. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, $n = m + k = 4$, K_{21}^{11}, $\delta = 1$, $L_{\delta}^{0} = i'_0 = 0$, $j'_0 = 0$.

Длина полученной последовательности $\Delta = 744$ знака. Частотное распределение в таблице 2.

Пример 4. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, $n = m + k = 4$, K_{01}^{01}, $\delta = 1$, $L_{\delta}^{0} = i'_0 = 0$, $j'_0 = 0$.

Длина полученной последовательности $\Delta = 995$ знаков. Частотное распределение в таблице 2.

Таблица 1

Пример	1	2	5
Группа i'_t	ω	ω	ω
0	643	692	290
1	618	656	303
00	161	188	71
01	125	172	79
10	194	144	68

Таблица 2

Пример	3	4
Группа i'_t	ω	ω
0	257	248
1	171	250
2	139	249
3	177	248
00	54	29

11	150	170	78
000	66	72	21
001	44	48	20
010	48	52	30
011	39	41	21
100	59	63	30
101	53	56	29
110	50	52	16
111	61	65	30
0000	24	28	9
0001	12	26	11
0010	28	21	9
0011	16	20	7
0100	11	16	7
0101	9	24	7
0110	26	18	10
0111	17	17	11
1000	27	14	7
1001	20	20	14
1010	25	22	6
1011	15	12	11
1100	20	35	12
1101	18	27	12
1110	30	15	5
1111	17	22	10

01	37	37
02	26	32
03	14	30
10	22	35
11	20	25
12	11	30
13	21	35
20	14	28
21	25	37
22	17	33
23	11	25
30	36	27
31	15	26
32	18	31
33	31	37

Пример 5. Система $[q, \mu, m, k] = [2, 10, 1, 1]$, $n = m + k = 2$, K_{21}^{11}, $\delta = 1$, $L_{\delta}^{0} = i'_0 = 0$, $j'_0 = 0$, $(x_l^0) = (x_1^0, x_2^0) = (0, 0)$.

Длина полученной последовательности $\Delta = 593$ знака. Частотное распределение в таблице 1.

Примеры 1 ÷ 5. Шифрование.

Пример 1

Таблица v Ключ $K_{ij}^{ij} = K_{21}^{11}$				
i'	0		1	
j'	i	j	i	j
0	1	0	1	1
1	0	1	0	0

t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t
0	0	0	- - -	- - -	- - -	117	0	1	p=7		
1	1	1	- - -	- - -	- - -	118	0	1	300	0	0
2	**1**	0	41	1	0	119	0	1	301	0	0
3	**0**	**0**	42	**1**	1	120	0	1	302	0	0
p=1			43	**1**	0	121	1	0	- - -	- - -	- - -
4	0	0	44	**1**	1	- - -	- - -	- - -	- - -	- - -	- - -
5	1	1	45	**1**	0	- - -	- - -	- - -	361	1	1
6	0	1	46	**0**	**0**	227	1	1	362	0	1
7	1	0	p=4			228	0	1	363	1	0
8	**1**	1	47	0	0	229	1	0	364	**1**	1
9	**1**	0	48	0	0	230	**1**	1	365	**1**	0
10	**0**	**0**	49	0	0	231	**1**	0	366	**1**	1
p=2			50	0	0	232	**1**	1	367	**1**	0
11	0	0	51	1	1	233	**1**	0	368	**1**	1
12	0	0	52	0	1	234	**1**	1	369	**1**	0
13	1	1	- - -	- - -	- - -	235	**1**	0	370	**1**	1
14	0	1	- - -	- - -	- - -	236	**0**	**0**	371	**1**	0
15	0	1	101	1	0	p=6			372	**0**	**0**
16	1	0	102	0	0	237	0	0	p=8		
17	1	1	103	1	1	238	0	0	373	0	0
18	0	1	104	**1**	0	239	0	0	374	0	0
19	1	0	105	**1**	1	- - -	- - -	- - -	- - -	- - -	- - -
20	0	0	106	**1**	0	- - -	- - -	- - -	- - -	- - -	- - -
21	1	1	107	**1**	1	289	1	0	1252	**1**	0
22	**1**	0	108	**1**	0	290	0	0	1253	**1**	1
23	**1**	1	109	**0**	**0**	291	1	1	1254	**1**	0
24	**1**	0	p=5			292	1	0	1255	**1**	1
25	**0**	**0**	110	0	0	293	1	1	1256	**1**	0
p=3			111	0	0	294	1	0	1257	**1**	1
26	0	0	112	0	0	295	1	1	1258	**1**	0
27	0	0	113	0	0	296	1	0	1259	**1**	1
28	0	0	114	0	0	297	1	1	1260	**1**	0
29	1	1	115	1	1	298	1	0	1261	**0**	**0**
30	0	1	116	0	1	299	0	0	p=9		

Пример 2

Таблица v

Ключ $K_{ij}^{ij} = K_{21}^{01}$

i'	0		1	
j'	i	j	i	j
0	1	0	1	1
1	0	1	0	2
2	1	2	1	3
3	0	3	0	0

t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t
0	0	0	66	**1**	3	261	0	0	462	0	0
1	1	3	67	**1**	2	262	0	0	- - -	- - -	- - -
2	1	2	68	**1**	1	263	0	0	1336	1	2
3	0	2	69	**1**	0	- - -	- - -	- - -	1337	0	2
4	1	1	70	**0**	**0**	376	1	0	1338	1	1
5	**1**	0	p=4			377	0	0	1339	**1**	0
6	**0**	**0**	71	0	0	378	1	3	1340	**1**	3
p=1			72	0	0	379	**1**	2	1341	**1**	2
7	0	0	73	0	0	380	**1**	1	1342	**1**	1
8	1	3	- - -	- - -	- - -	381	**1**	0	1343	**1**	0
9	0	3	125	1	2	382	**1**	3	1344	**1**	3
10	1	2	126	0	2	383	**1**	2	1345	**1**	2
11	**1**	1	127	1	1	384	**1**	1	1346	**1**	1
12	**1**	0	128	**1**	0	385	**1**	0	1347	**1**	0
13	**0**	**0**	129	**1**	3	386	**0**	**0**	1348	**0**	**0**
p=2			130	**1**	2	p=7			p=9		
14	0	0	131	**1**	1	387	0	0			
15	0	0	132	**1**	0	388	0	0			
16	1	3	133	**0**	**0**	389	0	0			
- - -	- - -	- - -	p=5			- - -	- - -	- - -			
22	1	0	134	0	0	448	1	1			
23	0	0	135	0	0	449	0	1			
24	1	3	136	0	0	450	1	0			
25	**1**	2	- - -	- - -	- - -	451	**1**	3			
26	**1**	1	251	1	3	452	**1**	2			
27	**1**	0	252	0	3	453	**1**	1			
28	**0**	**0**	253	1	2	454	**1**	0			

p=3			254	**1**	1	455	**1**	3			
29	0	0	255	**1**	0	456	**1**	2			
30	0	0	256	**1**	3	457	**1**	1			
31	0	0	257	**1**	2	458	**1**	0			
- - -	- - -	- - -	258	**1**	1	459	**0**	**0**			
63	1	1	259	**1**	0	p=8					
64	0	1	260	**0**	**0**	460	0	0			
65	1	0	p=6			461	0	0			

Пример 3

Таблица v. Ключ $K_{ij}^{ij} = K_{21}^{11}$								
i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	3	0	3	1	3	2	3	3
1	2	1	2	2	2	3	2	0
2	1	2	1	3	1	0	1	1
3	0	3	0	0	0	1	0	2

Связь между системами счисления				
$q=2$	00	01	10	11
$q=10$	0	1	2	3

t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t
0	0	0	47	**3**	2	214	**3**	1	589	0	0
1	1	3	48	**3**	3	215	**3**	2	590	3	1
2	1	2	49	**3**	0	216	**3**	3	591	**3**	2
3	0	2	50	**0**	**0**	217	**3**	0	592	**3**	3
4	3	3	p=3			218	**0**	**0**	593	**3**	0
5	**3**	0	51	0	0	p=5			594	**3**	1
6	**0**	**0**	52	0	0	219	0	0	595	**3**	2
p=1			53	0	0	220	0	0	596	**3**	3
7	0	0	- - -	- - -	- - -	221	0	0	597	**3**	0
8	1	3	85	1	3	- - -	- - -	- - -	598	**0**	**0**
9	0	3	86	0	3	463	1	1	p=7		
- - -	- - -	- - -	87	3	0	464	0	1	599	0	0
15	1	1	88	**3**	1	465	3	2	600	0	0
16	0	1	89	**3**	2	466	**3**	3	601	0	0

17	3	2	90	**3**	3	467	**3**	0	- - -	- - -	- - -
18	**3**	3	91	**3**	0	468	**3**	1	735	3	0
19	**3**	0	92	**0**	**0**	469	**3**	2	736	**3**	1
20	**0**	**0**	p=4			470	**3**	3	737	**3**	2
p=2			93	0	0	471	**3**	0	738	**3**	3
21	0	0	94	0	0	472	**0**	**0**	739	**3**	0
22	0	0	95	0	0	p=6			740	**3**	1
23	1	3	- - -	- - -	- - -	474	0	0	741	**3**	2
- - -	- - -	- - -	210	1	2	474	0	0	742	**3**	3
44	1	0	211	0	2	475	0	0	743	**3**	0
45	0	0	212	3	3	- - -	- - -	- - -	744	**0**	**0**
46	3	1	213	**3**	0	588	1	0	p=8		

Пример 4

Таблица v. Ключ $K_{ij}^{ij} = K_{01}^{01}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	3	0	1	1	3	2	2	3
1	2	1	0	2	3	3	0	0
2	1	2	0	3	1	0	3	1
3	1	3	2	0	0	1	2	2

Связь между системами счисления				
$q=2$	00	01	10	11
$q=10$	0	1	2	3

t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t	t	i'_t	j'_t
0	0	0	18	3	1	50	3	1	271	0	0
1	3	1	19	2	3	- - -	- - -	- - -	- - -	- - -	- - -
2	3	2	- - -	- - -	- - -	262	3	1	988	3	0
3	2	0	42	1	2	263	2	3	989	2	2
- - -	- - -	- - -	43	2	0	264	2	1	990	2	0
12	2	1	44	2	2	265	**3**	2	991	**3**	1
13	0	1	45	**3**	3	266	**3**	3	992	**3**	2
14	2	3	46	**3**	0	267	**3**	0	993	**3**	3
15	**3**	0	47	**0**	**0**	268	**0**	**0**	994	**3**	0
16	**0**	**0**	p=2			p=3			995	**0**	**0**
p=1			48	0	0	269	0	0	p=4		
17	0	0	49	0	0	270	0	0			

Пример 5

Таблица v Ключ $K_{ij}^{ij} = K_{21}^{11}$				
i'	0		1	
j'	i	j	i	j
0	1	0	1	1
1	0	1	0	0

t	y_1	y_2	i'_t	j'_t	x_1	x_2
0			0	0	0	0
1	0	0	1	1	0	0
2	1	1	1	1	2	2
3	3	3	1	1	6	6
- - -	- - -	- - -	- - -	- - -	- - -	- - -
66	8	3	0	0	6	6
67	6	6	1	0	2	2
68	3	2	1	1	6	4
69	7	5	**1**	0	4	0
70	5	0	**0**	**0**	**0**	**0**
p=1						
71	1	0	1	1	2	0
72	2	1	1	1	4	2
73	5	3	0	0	0	6
- - -	- - -	- - -	- - -	- - -	- - -	- - -
252	9	4	0	0	8	8
253	8	8	1	0	6	6
254	6	6	1	0	2	2
255	3	2	**1**	1	6	4
256	7	5	**1**	0	4	0
257	5	0	**0**	**0**	**0**	**0**
p=2						
258	1	0	1	1	2	0
259	3	1	1	1	6	2
260	6	3	0	0	2	6
- - -	- - -	- - -	- - -	- - -	- - -	- - -
587	4	9	0	1	8	8
588	9	9	1	0	8	8
589	8	8	1	0	6	6
590	6	6	**1**	0	2	2

591	3	2	**1**	1	6	4
592	7	5	**1**	0	4	0
593	5	0	**0**	**0**	**0**	**0**
p=3						

2. Периодические последовательности псевдослучайных чисел

2.1. Вычисление периода последовательности псевдослучайных чисел

Для генерирования периодических последовательностей псевдослучайных чисел будем использовать систему с ключом K_{21}^{11}.

Таблица v
Ключ $K_{ij}^{ij} = K_{21}^{11}$

i'	0		1	
j'	i	j	i	j
0	1	0	1	1
1	0	1	0	0

Исходные данные возьмем в виде:

$$i_t = i'_{t-\delta}, \quad j_t = j'_{t-1}, \quad j'_0 = 0, \qquad (2)$$

где j'_0 – начальное состояние системы, i_t – символы открытого текста, i'_t – символы шифртекста, δ – длина начального вектора I'_0 шифртекста, j'_t – состояние системы, $t = 1, 2, ..., T$, T – период последовательности псевдослучайных чисел, зависящий от вектора I'_0, который возьмем в виде последовательности из δ нулей:

$$I'_0 = 00...0. \qquad (3)$$

Элементами таблицы v (ключа K_{21}^{11}) являются двоичные числа $l = i(1<) + j$, где $i(1<)$ обозначает сдвиг числа i на 1 разряд влево. Координатами числа l в таблице v являются числа i', j', принимающие значения 0 и 1. Образуем число

$$l_t = i_t(1<) + j'_{t-1}, \quad j'_{t-1} = j_t. \qquad (4)$$

Числа l_t являются элементами таблицы v, по значениям которых определяем их координаты i', j'.

Описанный процесс является алгоритмом шифрования открытого текста i_t, определяемого формулой (2). Получаемый при этом шифртекст i'_t образует последовательность псевдослучайных чисел. Для того, чтобы было удобнее использовать этот алгоритм в компьютерной программе, образуем массив из четырех ячеек, содержимым которых являются числа $l' = i'(1<) + j'$, а их индексами будут числа $l = i(1<) + j$.

Для рассматриваемого ключа K_{21}^{11} такой массив запишется в виде

$$n[4] = \{3,1,0,2\}. \qquad (5)$$

Для небольших значений δ описанный алгоритм получения последовательности псевдослучайных чисел легко может быть реализован вручную. Этот и последующие алгоритмы записаны в программах на языке Си.

Программа 1. Вычисление периода последовательности псевдослучайных чисел

```
#include <stdio.h>
#include <conio.h>
int mas[1000];
main(){
  unsigned long k,t,T=0;
  int N,p,l,s,x,u,m;
  static int i,j,I[31];
  int n[4]={3,1,0,2};
  FILE *per;
  printf("Dlina nachalnogo vektora 1<=N<=30 \n");
  printf("N=");
  fflush(stdin);
  scanf("%d",&N);
  while(1){
     l=(i<<1)+j;
     x=n[l];
     i=x>>1;
     j=x&1;
     for(s=0;s<N-1;++s)
        I[N-1-s]=I[N-2-s];
     I[0]=i;
```

```
      ++T;
      if(N<10)
         mas[T]=i;
      u=0;
      for(s=0;s<N;++s){
         u+=I[s];
         if(u)
            break;
      }
      if(!u && !j)
         break;
      i=I[N-1];
   }
   t=1;
   for(s=0;s<N+1;++s)
      t*=2;
   --t;
   p=0;
   if(T==t)
      p=1;
   per=fopen("scree_period.cpp","a+");
   fprintf(per,"Dlina nachalnogo vektora N=%d \n",N);
   fprintf(per,"Period T=%ld    prisnak p=%d \n",T,p);
   if(N<10){
      fprintf(per,"\n");
      fprintf(per,"                    posledovatelnost \n");
      for(k=1;k<=T;++k){
         m=mas[k];
         fprintf(per,"%d ",m);
         if(!(k%40))
            fprintf(per,"\n");
      }
      fprintf(per,"\n\n");
   }
   else
      fprintf(per,"\n");
   fclose(per);
   return(0);
}
```

Некоторые пояснения к программе.

Длина начального вектора $N = \delta$. Программа заканчивает работу, когда последовательность конечной части шифртекста, состоящая из одних нулей, достигнет длины δ и конечное состояние системы станет равным ее начальному состоянию: $j'_T = j'_0 = 0$.

Для некоторых значений δ период последовательности вычисляется по формуле

$$T = 2^{\delta+1} - 1. \qquad (6)$$

Когда период T последовательности псевдослучайных чисел, вычисленный программой совпадает с периодом, вычисленным по формуле (6), программа записывает признак $p = 1$, иначе $p = 0$.

Приведем некоторые результаты работы этой программы.

Dlina nachalnogo vektora N=1
Period T=3 prisnak p=1 posledovatelnost 1 1 0

Dlina nachalnogo vektora N=2
Period T=7 prisnak p=1 posledovatelnost 1 0 1 1 1 0 0

Dlina nachalnogo vektora N=3
Period T=15 prisnak p=1
posledovatelnost 1 0 0 1 1 0 1 0 1 1 1 1 0 0 0

Dlina nachalnogo vektora N=4
Period T=21 prisnak p=0
posledovatelnost 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0

Dlina nachalnogo vektora N=5
Period T=63 prisnak p=1
posledovatelnost 1 0 0 0 0 1 1 0 0 0 1 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1 0 0 1
0 0 1 0 1 1 0 1 1 1 0 1 1 0 0 1 1 0 1 0 1 0 1 1 1 1 1 1 0 0 0 0 0

Dlina nachalnogo vektora N=6
Period T=127 prisnak p=1
posledovatelnost
1 0 0 0 0 0 1 1 0 0 0 0 1 0 1 0 0 0 1 1 1 1 0 0 1 0 0 0 1 0 1 1 0 0 1 1 1 0 1 0
1 0 0 1 1 1 1 1 0 1 0 0 0 0 1 1 1 0 0 0 1 0 0 1 0 0 1 1 0 1 1 0 1 0 1 1 0 1 1 1
1 0 1 1 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 1 1 1 1 1
1 0 0 0 0 0 0

Dlina nachalnogo vektora N=7
Period T=63 prisnak p=0
posledovatelnost
1 0 0 0 0 0 0 1 1 0 0 0 0 0 1 0 1 0 0 0 0 1 1 1 1 0 0 0 1 0 0 0 1 0 0 1 1 0 0 1
1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0

Dlina nachalnogo vektora N=8
Period T=73 prisnak p=0
posledovatelnost
1 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 0 1 0 0 0 0 0 1 1 1 1 0 0 0 0 1 0 0 0 1 0 0 0
1 1 0 0 1 1 0 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

Dlina nachalnogo vektora N=9
Period T=889 prisnak p=0
posledovatelnost
1 0 0 0 0 0 0 0 0 1 1 0 0 0 0 0 0 0 1 0 1 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 1 0 0 0
1 0 0 0 0 1 1 0 0 1 1 0 0 0 1 0 1 0 1 0 1 0 0 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 0 0 0
1 1 1 0 0 0 0 0 0 1 0 0 1 0 0 0 0 0 1 1 0 1 1 0 0 0 0 1 0 1 1 0 1 0 0 0 0 1 1 1 0
1 1 1 0 0 1 0 0 1 1 0 0 1 0 1 1 0 1 0 1 0 1 1 1 0 1 1 1 1 1 1 1 0 0 1 1 0 0 0 0 0
1 0 1 0 1 0 0 0 0 1 1 1 1 1 1 0 0 0 1 0 0 0 0 0 0 1 0 0 1 1 0 0 0 0 1 1 0 1 0 1 0
0 0 1 0 1 1 1 1 1 0 0 1 1 1 0 0 0 0 1 0 1 0 0 1 0 0 0 1 1 1 1 0 1 1 0 0 1 0 0 0
1 1 0 1 0 1 1 0 0 1 0 1 1 1 1 0 1 0 1 1 1 0 0 0 1 1 1 1 0 0 1 0 0 1 0 0 0 1 0 1
1 0 1 1 0 0 1 1 1 0 1 1 0 1 0 1 0 0 1 1 0 1 1 1 1 1 0 1 0 1 1 0 0 0 0 1 1 1 1 0
1 0 0 0 1 0 0 0 1 1 1 0 0 1 1 0 0 1 0 0 1 0 1 0 1 0 1 1 1 0 1 1 1 1 1 1 1 0 1 1 0
0 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 1 1 0 0 0 0 1 1 1 0 0 1 0 0 0 1 0 0 1 0 1 1 0
0 1 1 0 1 1 1 0 1 0 1 0 1 1 0 0 1 1 1 1 1 1 0 1 0 1 0 0 0 0 0 1 1 1 1 1 0 0 0 0
1 0 0 0 0 1 0 0 0 1 1 0 0 0 1 1 0 0 1 0 1 0 0 1 0 1 0 1 1 1 1 0 1 1 1 1 1 0 0 0
1 1 0 0 0 0 1 0 0 1 0 1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 1 1 0 0 0 1 0 1 1 1 0 1 0 0
1 1 1 0 0 1 1 1 0 1 0 0 1 0 1 0 0 1 1 1 0 1 1 1 1 0 1 0 0 1 1 0 0 0 1 1 1 0 1 0
1 0 0 1 0 0 1 1 1 1 1 0 1 1 0 1 0 0 0 0 1 1 0 1 1 1 0 0 0 1 0 1 1 0 0 1 0 0 1 1
1 0 1 0 1 1 0 1 0 0 1 1 1 1 0 1 1 1 0 1 0 0 0 1 1 0 0 1 1 1 0 0 1 0 1 0 1 0 0 1
0 1 1 1 1 1 1 0 1 1 1 0 0 0 0 0 1 1 0 0 1 0 0 0 0 1 0 1 0 1 1 0 0 0 1 1 1 1 1 0
1 0 0 1 0 0 0 0 1 1 1 0 1 1 0 0 0 1 0 0 1 1 0 1 0 0 1 1 0 1 0 1 1 1 0 1 0 1 1 1
1 0 0 1 1 1 1 0 0 0 1 0 1 0 0 0 1 0 0 1 1 1 1 0 0 1 1 0 1 0 0 0 1 0 1 0 1 1 1 0
0 1 1 1 1 1 0 0 1 0 1 0 0 0 0 1 0 1 1 1 1 0 0 0 1 1 1 0 0 0 1 0 0 1 0 0 1 0 0 1
1 0 1 1 0 1 1 0 1 0 1 1 0 1 1 0 1 1 1 1 0 1 1 0 1 1 0 0 0 1 1 0 1 1 0 1 0 0 1 0
1 1 0 1 1 1 0 1 1 1 0 1 1 0 0 1 1 0 0 1 1 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 1 1 1
0 0 0 0 0 0 0 0 0

Остальные значения периодов T запишем в таблице 3.

Таблица 3

N	T	p
10	1533	0
11	3255	0
12	7905	0
13	11811	0
14	32767	1
15	255	0
16	273	0
17	253921	0
18	413385	0
19	761763	0
20	5461	0
21	4194303	1
22	2088705	0
23	2097151	0
24	10961685	0
25	298935	0
26	125829105	0
27	17895697	0
28	402653181	0
29	10845877	0
30	2097151	0

Программа 2. Вычисление периода последовательности псевдослучайных чисел

В предложенном алгоритме можно обойтись без начального вектора I'_0 (в программе 1– массив I[31]), заменив его переменной z. Новая программа работает примерно в 10 раз быстрее, результаты те же, что и по программе 1.

```
#include <stdio.h>
#include <conio.h>
int mas[1000];
main(){
  unsigned long k,t,T=0,z=0;
  int N,p,l,s,x,u,m;
  int n[4]={3,1,0,2};
  static int i,j;
```

```
FILE *per;
printf("Dlina nachalnogo vektora 1<=N<=30 \n");
printf("N=");
fflush(stdin);
scanf("%d",&N);
t=1;
for(s=0;s<N-1;++s)
   t*=2;
while(1){
   l=(i<<1)+j;
   x=n[l];
   i=x>>1;
   j=x&1;
   z>>=1;
   if(i)
      z|=t;
   ++T;
   if(N<10)
      mas[T]=i;
   if(!z && !j)
      break;
   i=z&1;
}
t=1;
for(s=0;s<N+1;++s)
   t*=2;
--t;
p=0;
if(T==t)
   p=1;
per=fopen("scree_period_.cpp","a+");
fprintf(per,"Dlina nachalnogo vektora N=%d \n",N);
fprintf(per,"Period T=%ld    prisnak p=%d \n",T,p);
if(N<10){
   fprintf(per,"\n");
   fprintf(per,"                    posledovatelnost \n");
   for(k=1;k<=T;++k){
      m=mas[k];
      fprintf(per,"%d ",m);
      if(!(k%40))
```

```
            fprintf(per,"\n");
      }
      fprintf(per,"\n\n");
   }
   else
      fprintf(per,"\n");
   fclose(per);
   return(0);
}
```

Если использовать один и тот же ключ K_{21}^{11} (можно и несколько разных), обратное выражение которого записано в виде массива (5), последовательно для разных переменных z, меняя их при каждом новом вычислении знака i, то последовательность псевдослучайных чисел, вырабатываемая такой программой, при одинаковых значениях N будет иметь значительно больший период (возможны редкие исключения), чем вычисленный по программе 1. Кратность использования ключа реализована в программе 3.

Программа 3. Вычисление периода последовательности псевдослучайных чисел

```
#include <stdio.h>
#include <conio.h>
main(){
  unsigned long w,t,T=0,z,mz[11];
  int R,N,p,q=0,r,l,s,x;
  int n[4]={3,1,0,2};
  static int i,j;
  FILE *per;
  for(s=0;s<11;++s)
     mz[s]=0;
  printf("Kratnost ispolzovaniya klyucha 1<=R<=10 \n");
  printf("R=");
  fflush(stdin);
  scanf("%d",&R);
  printf("Dlina N nachalnogo vektora \n");
  printf("R=1: 1<=N<=30 \n");
  printf("R=2: 1<=N<=15 \n");
  printf("R=3: 1<=N<=11 \n");
```

```
printf("R=4: 1<=N<=8 \n");
printf("R=5: 1<=N<=6 \n");
printf("R=6: 1<=N<=5 \n");
printf("R=7–8: 1<=N<=4 \n");
printf("R=9–10: 1<=N<=3 \n");
printf("N=");
fflush(stdin);
scanf("%d",&N);
t=1;
for(s=0;s<N-1;++s)
   t*=2;
while(1){
   for(r=1;r<=R;++r){
      z=mz[r];
      i=z&1;
      l=(i<<1)+j;
      x=n[l];
      i=x>>1;
      j=x&1;
      z>>=1;
      if(i)
         z|=t;
      mz[r]=z;
      ++T;
      p=0;
      for(s=1;s<=R;++s){
         w=mz[s];
         if(!w)
            ++p;
      }
      if(p==R && !j){
         q=1;
         break;
      }
   }
   if(q)
      break;
}
per=fopen("scree_period_r.cpp","a+");
fprintf(per,"Kratnost ispolzovaniya klyucha R=%d \n",R);
```

```
  fprintf(per,"Dlina nachalnogo vektora N=%d \n",N);
  fprintf(per,"Period T=%ld \n\n",T);
  fclose(per);
  return(0);
}
```

Вычислим по этой программе периоды T последовательностей псевдослучайных чисел для кратностей $1 <= R <= 10$ использования ключа K_{21}^{11}. При этом ограничимся периодами, не превышающими максимального значения unsigned long. Результаты вычислений приведены в сводной таблице 4.

Таблица 4

R	1	2	3	4	5
N	T	T	T	T	T
1	3	7	15	21	63
2	7	21	127	73	1533
3	15	127	889	7905	255
4	21	73	7905	273	5461
5	63	1533	255	5461	298935
6	127	7905	413385	10961685	2097151
7	63	32767	4194303	402653181	
8	73	273	10961685	1057	
9	889	413385	17895697		
10	1533	5461	2097151		
11	3255	2088705	255652815		
12	7905	10961685			
13	11811	125829105			
14	32767	402653181			
15	255	2097151			
R	6	7	8	9	10
N	T	T	T	T	T
1	127	63	73	889	1533
2	7905	32767	273	413385	5461
3	413385	4194303	10961685	17895697	2097151
4	10961685	402653181	1057		
5	2097151				

2.2. Частотное распределение двоичных чисел в последовательности псевдослучайных чисел

Подсчитаем количество каждого n-значного $(n = 1,2,...,6)$ двоичного числа, содержащегося в последовательностях псевдослучайных чисел с периодами $T = 889$ и $T = 402653181$, при помощи программы 4. Результаты вычислений приведены в таблицах 5, 6 и 7, в которых двоичные n-значные числа записаны в десятичной системе счисления. Результаты вычислений по программе 4 для периода $T = 889$ могут быть проверены вручную, используя последовательность псевдослучайных чисел, вычисленную программой 1 в пункте 2.1 при $N = 9$.

Таблица 5

Частотное распределение двоичных n-значных чисел в последовательности с периодом $T = 889$

$n=1$		$n=2$		$n=3$		$n=4$		$n=5$		$n=6$	
0–1	ω	0–3	ω	0–7	ω	0–15	ω	0–31	ω	0–63	ω
0	445	0	105	0	34	0	15	0	5	0	3
1	444	1	103	1	33	1	10	1	5	1	3
		2	133	2	48	2	12	2	3	2	2
		3	104	3	39	3	10	3	6	3	2
				4	41	4	10	4	4	4	0
				5	31	5	9	5	7	5	0
				6	31	6	22	6	1	6	3
				7	40	7	13	7	4	7	2
						8	21	8	3	8	3
						9	16	9	5	9	1
						10	14	10	3	10	4
						11	10	11	2	11	1
						12	13	12	5	12	2
						13	14	13	4	13	1
						14	24	14	7	14	3
						15	10	15	9	15	3
								16	13	16	0
								17	10	17	3
								18	10	18	4
								19	7	19	6
								20	5	20	0

								21	7	21	1
								22	9	22	4
								23	5	23	5
								24	4	24	2
								25	4	25	1
								26	9	26	5
								27	5	27	2
								28	5	28	2
								29	2	29	1
								30	4	30	2
								31	6	31	4
										32	3
										33	3
										34	6
										35	3
										36	1
										37	3
										38	4
										39	5
										40	5
										41	2
										42	2
										43	3
										44	3
										45	3
										46	1
										47	0
										48	1
										49	0
										50	1
										51	1
										52	0
										53	2
										54	2
										55	2
										56	3
										57	2
										58	1
										59	2
										60	5

										61	1
										62	3
										63	1

Из таблицы 5 видно, что частотное распределение чисел близко к равномерному. Небольшие колебания частот ω для фиксированного значения n вызваны небольшой длиной последовательности. С увеличением ее длины относительные колебания частот ω для всех чисел при данном n уменьшатся.

Таблица 6

Частотное распределение двоичных n-значных чисел в последовательности с периодом $T = 402653181$

$n=1$		$n=2$		$n=3$	
0–1	ω	0–3	ω	0–7	ω
0	201326591	0	50331760	0	16777216
1	201326590	1	50331312	1	16777216
		2	50331760	2	16777216
		3	50331759	3	16777216
				4	16777216
				5	16777215
				6	16777216
				7	16777216

Таблица 7

Частотное распределение двоичных n-значных чисел в последовательности с периодом $T = 402653181$

$n=4$		$n=5$		$n=6$	
0–15	ω	0–31	ω	0–63	ω
0	6290564	0	2516455	0	1048352
1	6288638	1	2516560	1	1049407
2	6292836	2	2517048	2	1048260
3	6292171	3	2516389	3	1048248
4	6292171	4	2516695	4	1049411
5	6292836	5	2517409	5	1047876
6	6292904	6	2513908	6	1049355
7	6292311	7	2517697	7	1048458
8	6292339	8	2517545	8	1048700
9	6289774	9	2517083	9	1049330
10	6291813	10	2516713	10	1049801

11	6290507	11	2517050	11	1048166
12	6292478	12	2516753	12	1048120
13	6289842	13	2518078	13	1047705
14	6289774	14	2517044	14	1048864
15	6292338	15	2516259	15	1048777
		16	2517763	16	1047334
		17	2513790	17	1049543
		18	2515281	18	1048333
		19	2517513	19	1049128
		20	2515728	20	1047979
		21	2517151	21	1049260
		22	2516158	22	1048211
		23	2513833	23	1047950
		24	2515271	24	1047918
		25	2515721	25	1047746
		26	2518481	26	1049477
		27	2515507	27	1048629
		28	2517737	28	1049782
		29	2517727	29	1048642
		30	2518315	30	1049373
		31	2515975	31	1047799
				32	1048621
				33	1047210
				34	1048200
				35	1048464
				36	1048278
				37	1049037
				38	1048141
				39	1048406
				40	1049431
				41	1048286
				42	1047913
				43	1048940
				44	1048499
				45	1048968
				46	1047382
				47	1048445
				48	1047938
				49	1048073
				50	1048288

				51	1048823
				52	1049287
				53	1049499
				54	1048915
				55	1047041
				56	1049556
				57	1048158
				58	1049206
				59	1047452
				60	1049503
				61	1048364
				62	1049111
				63	1049495

Значения частот ω в таблицах 6 и 7 свидетельствуют о распределениях, достаточно близких к равномерным.

Программа 4

Частотное распределение двоичных n-значных чисел в последовательности псевдослучайных чисел

```
/* Распределение двоичных n-значных чисел, 1<=n<=6
   в последовательности псевдослучайных чисел периода T */
#include <stdio.h>
#include <conio.h>
unsigned long mas[64];
main(){
  unsigned long u,t,T=0,z=0;
  int N,q=0,a,b,c,p,l,s,x,n;
  int k[4]={3,1,0,2};
  static int i,j;
  FILE *out;
  printf("Dlina nachalnogo vektora 1<=N<=30 \n");
  printf("N=");
  fflush(stdin);
  scanf("%d",&N);
  printf("Kolichestvo rasryadov dvoichnogo chisla 1<=n<=6 \n");
  printf("n=");
  fflush(stdin);
  scanf("%d",&n);
  t=1;
  for(s=0;s<N-1;++s)
```

```
    t*=2;
  while(1){
    c=0;
    b=1;
    for(s=1;s<n;++s)
      b*=2;
    for(p=0;p<n;b>>=1){
      l=(i<<1)+j;
      x=k[l];
      i=x>>1;
      j=x&1;
      z>>=1;
      if(i){
        z|=t;
        c|=b;
      }
      ++T;
      if(!z && !j){
        q=1;
        break;
      }
      i=z&1;
      ++p;
    }
    mas[c]+=1;
    if(q)
      break;
  }
  out=fopen("scree_raspredelenie.cpp","a+");
  fprintf(out,"Dlina nachalnogo vektora N=%d \n",N);
  fprintf(out,"Kolichestvo rasryadov dvoichnogo chisla n=%d \n",n);
  fprintf(out,"Period T=%ld \n",T);
  a=1;
  for(s=1;s<=n;++s)
    a*=2;
  if(n<=2){
    for(s=0;s<a;++s)
      fprintf(out,"%9d ",s);
    fprintf(out,"\n");
    for(s=0;s<a;++s){
```

```
        u=mas[s];
        fprintf(out,"%9ld ",u);
      }
      fprintf(out,"\n");
   }
   else{
      for(s=0;s<a;++s)
        fprintf(out,"%8d ",s);
      fprintf(out,"\n");
      for(s=0;s<a;++s){
        u=mas[s];
        fprintf(out,"%8ld ",u);
      }
      fprintf(out,"\n");
   }
   fprintf(out,"\n");
   fclose(out);
   return(0);
}
```

Запишем теперь программу 5, генерирующую последовательность до 1000000 двоичных n-значных псевдослучайных чисел заданного периода T. Количество выводимых в файл чисел, значения длины начального вектора и разрядности n двоичных чисел выбираются в указанных пределах. Псевдослучайные числа, записанные в файле, просматриваются в редакторе в десятичной системе счисления. Диапазон чисел в десятичной системе счисления в зависимости от разрядности n двоичных чисел выражается в виде $0 \div 2^n - 1$.

Программа 5

Последовательность двоичных n-значных псевдослучайных чисел заданного периода T

```
#include <stdio.h>
#include <conio.h>
int N,n;
unsigned int mas[1000001];
int gan(void);
main(){
  int m;
  long Q;
```

```
  unsigned long T,q;
  unsigned int u;
  FILE *out;
  printf("Vybiraem period T i sootvetstvuyuschyuyu emu dlinu nachalnogo vektora N \n");

printf("T:|3|7|15|21|63|127|63|73|889|1533|3255|7905|11811|32767|255|273| \n");
  printf("N:|1|2| 3| 4| 5| 6 | 7| 8| 9 | 10 | 11 | 12 | 13 | 14 | 15| 16| \n\n");

printf("T:|253921|413385|761763|5461|4194303|2088705|2097151|10961685| \n");
  printf("N:| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | \n\n");

printf("T=|298935|125829105|17895697|402653181|10845877|2097151| \n");
  printf("N:| 25 | 26 | 27 | 28 | 29 | 30 | \n\n");
  printf("T=");
  fflush(stdin);
  scanf("%ld",&T);
  printf("N=");
  fflush(stdin);
  scanf("%d",&N);
  printf("Kolichestvo rasryadov dvoichnogo chisla 1<=n<=16 \n");
  printf("n=");
  fflush(stdin);
  scanf("%d",&n);
  printf("Kolichestvo vyvodimyh chisel \n");
  printf("Q=");
  fflush(stdin);
  scanf("%ld",&Q);
  for(m=1;m<=Q;++m)
     mas[m]=gan();
  out=fopen("scree_n_znachnye.cpp","a+");
  fprintf(out,"Period posledovatelnosti T=%ld \n",T);
  fprintf(out,"Dlina nachalnogo vektora N=%d \n",N);
  fprintf(out,"Kolichestvo rasryadov dvoichnogo chisla n=%d \n",n);
  fprintf(out,"Kolichestvo vyvodimyh chisel Q=%ld \n",Q);
```

```
  q=0;
  for(m=1;m<=Q;++m){
     u=mas[m];
     ++q;
     fprintf(out,"%5d ",u);
     if(q==T){
        fprintf(out,"\n\n");
        q=0;
     }
     else{
        if(!(q%13))
           fprintf(out,"\n");
     }
  }
  fprintf(out,"\n\n");
  fclose(out);
  return(0);
}
int gan(void){
  int p,l,s,x;
  unsigned int b,c;
  unsigned long t;
  int k[4]={3,1,0,2};
  static int i,j;
  static unsigned long z;
  t=1;
  for(s=0;s<N-1;++s)
     t*=2;
  c=0;
  b=1;
  for(s=1;s<n;++s)
     b*=2;
  for(p=0;p<n;b>>=1){
     l=(i<<1)+j;
     x=k[l];
     i=x>>1;
     j=x&1;
     z>>=1;
     if(i){
        z|=t;
```

```
        c|=b;
      }
      i=z&1;
      ++p;
    }
    return(c);
}
```

При $N=9$ (период $T=889$), $n=1$ и $Q=889$ получим последовательность псевдослучайных чисел, совпадающую с ранее записанной в пункте 2.1, что является подтверждением правильности работы программы 5.

Если длина полученной последовательности чисел больше ее периода, то можно проследить периодическую повторяемость чисел, содержащихся в начальной части этой последовательности длиной, равной периоду T.

Приведем результаты некоторых вычислений по программе 5.

```
Period posledovatelnosti T=7
Dlina nachalnogo vektora N=2
Kolichestvo rasryadov dvoichnogo chisla n=3
Kolichestvo vyvodimyh chisel Q=35
Программа выдала 5 повторяющихся групп чисел
   5    6    2    7    1    3    4

Period posledovatelnosti T=63
Dlina nachalnogo vektora N=5
Kolichestvo rasryadov dvoichnogo chisla n=4
Kolichestvo vyvodimyh chisel Q=315
Программа выдала 5 повторяющихся групп чисел
   8     6    2    9   14    8   14    4   11    7    6    6   10
  15    12    1    0   12    5    3   13    1   12    9    6   14
  12    13    5   15    8    2    1    8   10    7   10    3    9
   2    13   13    9   10   11   15    0    4    3    1    4   15
   4     7    2    5   11   11    3    5    7   14    0

Period posledovatelnosti T=73
Dlina nachalnogo vektora N=8
Kolichestvo rasryadov dvoichnogo chisla n=5
Kolichestvo vyvodimyh chisel Q=365
```

Программа выдала 5 повторяющихся групп чисел

16	3	0	10	1	28	4	8	25	18	21	15	31
0	2	0	12	1	8	7	16	17	3	6	10	21
31	28	0	8	1	16	5	0	30	2	4	12	25
10	23	31	16	1	0	6	0	20	3	24	8	17
19	5	10	31	30	0	4	0	24	2	16	15	1
2	6	12	21	11	31	24	0					

Часть программы 5, формирующая двоичные n-значные псевдослучайные числа, оформим в виде функции gan(), которую можно использовать при необходимости в разнообразных программах.

Функция gan()

Генератор двоичных n-значных псевдослучайных чисел

```
int gan(void){
  int N=28,n=5,p,l,s,x;
  unsigned int b,c;
  unsigned long t;
  int k[4]={3,1,0,2};
  static int i,j;
  static unsigned long z;
  t=1;
  for(s=0;s<N-1;++s)
     t*=2;
  c=0;
  b=1;
  for(s=1;s<n;++s)
     b*=2;
  for(p=0;p<n;b>>=1){
     l=(i<<1)+j;
     x=k[l];
     i=x>>1;
     j=x&1;
     z>>=1;
     if(i){
        z|=t;
        c|=b;
     }
     i=z&1;
```

```
    ++p;
  }
  return(c);
}
```

Для использования этой функции необходимо задать значения для переменных N и n. От значения N зависит период T генерируемой последовательности, переменная n определяет разрядность двоичных чисел. В представленной функции gan() эти значения соответственно равны N=28 и n=5 Для N=28 период T=402653181.

При выборе разрядности n следует использовать выражение для диапазона чисел в десятичной системе счисления $0 \div 2^n - 1$, выдаваемых функцией gan().

Значение N выбираем по таблице 8 в зависимости от желаемого периода T генерируемой последовательности.

Таблица 8

N	1	2	3	4	5	6	7	8	9	10	11
T	3	7	15	21	63	127	63	73	889	1533	3255

N	12	13	14	15	16	17	18
T	7905	11811	32767	255	273	253921	413385

N	19	20	21	22	23	24	25
T	761763	5461	4194303	2088705	2097151	10961685	298935

N	26	27	28	29	30
T	125829105	17895697	402653181	10845877	2097151

Литература

1. Недосекин Ю.А. Преобразование и защита информации. «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 16.

Недосекин Ю.А.

Преобразование и защита информации

Аннотация

Предлагаемая в данной работе схема преобразования и защиты информации основана на использовании таблицы, специальным образом составленной из q-ичных чисел (q – значение системы счисления). Представлено шесть разных алгоритмов шифрования и дешифрования, на основе которых построены некоторые криптосистемы и исследованы их свойства. Приведено большое количество примеров, иллюстрирующих работу предложенных алгоритмов. Рассмотрены вопросы аутентификации данных и криптоанализа.

Содержание

1. Основные понятия

Любая информация, представленная в q-ичном коде, может быть зашифрована q-ичными символами предлагаемой системой. Символы q-ичной системы счисления принимают значения

$s = 0,1,2,...,q-1; \quad q > 1$ – произвольное целое число.

Метод шифрования основан на записи q-ичных символов исходной информации I набором целых чисел x_l, кратных q и являющихся носителями q-ичных символов.

Значения x_l $(l = 1,2,...,n; \quad n$ – целое число$)$ принадлежат множеству $\{0, q, 2q, ..., \mu - q\}$, где μ / q – целое число.

Запись и чтение q-ичного символа s_l осуществляем по схеме:

запись $y_l = x_l + s_l$, **чтение** $s_l = y_l \bmod q$, (1)

где $y_l \in \{0,1,2,...,\mu-1\}$ – базис μ; числа x_l и y_l всегда записываем в десятичной системе счисления.

Исходная информация I может быть представлена в виде последовательности m-значных слов (знаков), поступающих по отдельности на вход алгоритма, образуя на его выходе последовательность I' шифрованных m-значных слов такой же длины. Запись информации начинается с использования начального вектора $\overline{x}_0 = (x_l^0) = (x_1^0, x_2^0, ..., x_n^0)$ и заканчивается конечным вектором $\overline{x}_\Delta = (x_l^\Delta) = (x_1^\Delta, x_2^\Delta, ..., x_n^\Delta)$; промежуточная запись на шаге t характеризуется вектором $\overline{x}_t = (x_l^t) = (x_1^t, x_2^t, ..., x_n^t)$.

Введем обозначения для q-ичных слов:

i – m-значное слово; j – k-значное слово;

$v_{j'i'} = i(k<) + j$ – n-значное слово,

где $n = m + k$, $i(k<)$ – сдвиг слова i на k разрядов влево;

$i = v_{j'i'}(k>), \quad j = v_{j'i'} - i(k<) = v_{j'i'} - v_{j'i'}(k>, k<) =$

$= v_{j'i'}(m<, m>)$, где $v_{j'i'}(k>)$ – сдвиг слова $v_{j'i'}$ на k разрядов вправо, $v_{j'i'}(k>, k<)$ – сдвиг $v_{j'i'}$ сначала на k разрядов вправо, а затем на k разрядов влево, $v_{j'i'}(m<, m>)$ – сдвиг $v_{j'i'}$ сначала на m разрядов влево, а затем на m разрядов вправо,

j', i' – координаты слова $v_{j'i'}$ в таблице v;

$i, i' = 0,1,2,...,q^m - 1, \quad j, j' = 0,1,2,...,q^k - 1.$

При сдвигах q-ичных слов на несколько разрядов влево или вправо символы, выходящие за границы первых n разрядов, исчезают.

Из слов $v_{j'i'} = i(k<) + j$ при $i = i'$, $j = j'$ образуем таблицу v_0, в которой числа i, j и i', j' записываем для удобства восприятия в десятичной системе счисления, а числа i, j в словах $v_{j'i'}$ для наглядности отделены друг от друга пунктиром.

Таблица v_0

i'	0		1		2		…….	q^m-1	
j'	i	j	i	j	i	j	…….	i	j
0	0	0	1	0	2	0	…….	q^m-1	0
1	0	1	1	1	2	1	…….	q^m-1	1
2	0	2	1	2	2	2	…….	q^m-1	2
:	:	:	:	:	:	:	…….	:	:
:	:	:	:	:	:	:	…….	:	:
q^k-1	0	q^k-1	1	q^k-1	2	q^k-1	…….	q^m-1	q^k-1

При произвольной перестановке слов $v_{j'i'}$ в таблице v_0 получим таблицу v, в которой координаты j', i' слова $v_{j'i'} = i(k<) + j$ в общем случае не совпадают с числами j, i этого слова.

Элементы таблиц v_0 и v принадлежат одному множеству $A = \{0,1,2,...,q^n - 1\}$. Каждый элемент $v_{j'i'}$ в таблицах v_0 и v отличен от всех других подобных элементов соответствующей таблицы и содержится в ней только один раз.

Из таблицы v_0 видно, что каждое число i содержится в ней q^k раз, а каждое число j – q^m раз. В элементах $v_{j'i'}$ при каждом фиксированном числе j находится q^m разных чисел i, а при каждом фиксированном числе i находится q^k разных чисел j.

Таблицы v_0 и v представим в виде соответствующих подстановок:

$$E = \begin{pmatrix} 0 & 1 & 2\cdots q^n - 1 \\ 0 & 1 & 2\cdots q^n - 1 \end{pmatrix} = \begin{pmatrix} u \\ u \end{pmatrix} \begin{matrix} \leftarrow \text{номер} \\ \leftarrow \text{содержимое} \end{matrix} \Big\} \begin{matrix} \text{ячейки} \\ \text{памяти} \end{matrix}, \quad (2)$$

$$K = \begin{pmatrix} 0 & 1 & 2\cdots q^n - 1 \\ v_0 & v_1 & v_2 \ldots v_{q^n - 1} \end{pmatrix} = \begin{pmatrix} u \\ v_u \end{pmatrix} \begin{matrix} \leftarrow \text{номер} \\ \leftarrow \text{содержимое} \end{matrix} \Big\} \begin{matrix} \text{ячейки} \\ \text{памяти} \end{matrix}, \quad (3)$$

где $u = i'(k<) + j', \quad v_u = i(k<) + j; \quad u, v_u \in A;$

u, v_u – n-значные q-ичные числа.

В подстановке K поменяем местами номера ячеек u с их содержимым v_u, в результате получим обратную подстановку

$$K^{-1}=\begin{pmatrix} v_0 & v_1 & v_2 \dots v_{q^n-1} \\ 0 & 1 & 2 \cdots q^n-1 \end{pmatrix}=\begin{pmatrix} v_u \\ u \end{pmatrix}\begin{matrix} \leftarrow \text{номер} \\ \leftarrow \text{содержимое} \end{matrix}\Big\}\begin{matrix} \text{ячейки} \\ \text{памяти} \end{matrix}. \qquad (4)$$

Подстановка K^{-1} является ключом для шифрования информации, а подстановка K – для ее расшифрования.

Действия ключей: $Ku = v_u$, $K^{-1}v_u = u$.

Слово i_t является входным знаком открытого текста I, а слово i'_t – выходным знаком шифрованного текста I'; t – номер знака открытого текста. Состояние системы определяется знаком:

$$j'_t = j_{t+1} = f(i_t, j'_{t-1}). \qquad (5)$$

Меняя значения параметров q, μ, m, k, получим достаточно большое количество поточных криптографических систем, свойства которых определяются структурой ключа K и модификацией слов i, i', j', входящих в алгоритм.

После записи информации I по формуле (1) q-ичные символы ε_l образуют n-значные слова:

$$v_{j'i'} = \varepsilon_1\varepsilon_2 \dots \varepsilon_m\varepsilon_{m+1} \dots \varepsilon_n = i(k<) + j \ , \qquad (6)$$

где $i = \varepsilon_1\varepsilon_2 \dots \varepsilon_m$, $j = \varepsilon_{m+1}\varepsilon_{m+2} \dots \varepsilon_n$, $\varepsilon_l = \left[y_l \frac{q}{\mu} \right]$ – целая часть, $l = 1, 2, \dots, n$; $n = m + k$. Схематическое расположение символов s_l на числах x_l имеет вид: $\begin{matrix} s_1 & s_2 & \dots & s_m & s_{m+1} & \dots & s_n \\ x_1 & x_2 & \dots & x_m & x_{m+1} & \dots & x_n \end{matrix}$.

Слова $v_{j'i'}$ в таблице v имеют координаты:

$$i' = s'_1 s'_2 \dots s'_m \ , \quad j' = s'_{m+1} s'_{m+2} \dots s'_{m+k} \ , \quad m + k = n. \qquad (7)$$

Тип системы шифрования будем обозначать знаком $[q, \mu, m, k]$.

2. Алгоритмы записи (шифрования) и чтения (расшифрования) информации

Все алгоритмы записаны с учетом возможности многократного шифрования кратности $r = 1, 2, \dots, \bar{r}$ набором ключей K_ξ , ξ – номер ключа, $\xi = 1, 2, \dots, \bar{r}$; $\bar{r}$ – конечное значение r.

Шифрование кратности r производится для каждого знака i_t открытого текста в отдельности с получением шифрованного знака i'_t при фиксированном значении t и может быть выполнено при базисе $\mu > q$ четырьмя способами, а при $\mu = q$ двумя. Первые восемь алгоритмов относятся к базису $\mu > q$, а последние четыре – к базису $\mu = q$.

При базисе $\mu = q$ алгоритмы упрощаются, а носители x_l q-ичных символов s_l исчезают.

Во всех алгоритмах для каждого входного знака i_t при фиксированном t алгоритм прогоняется по всем пунктам для каждого значения r; значения r и ξ изменяются одновременно.

Параметры системы q, μ, m, k – целые положительные числа считаются заданными; μ / q – целое число; $n = m + k$.

Алгоритмы при базисе $\mu > q$

А. Первый способ: шифрование с одним начальным вектором и одним начальным состоянием системы.

Количество вариантов шифрования:

$$z = \left(\frac{\mu}{q}\right)^n q^k (q^n!)^{\bar{r}}. \qquad (8)$$

Алгоритм записи. На вход алгоритма последовательно поступают отдельные знаки i_t исходной информации $I = i_1 i_2 ... i_\Delta$; $t = 1, 2, ..., \Delta$; Δ – конечное значение номера входного знака i_t (длина открытого текста). Ключи шифрования K_ξ^{-1r}, начальный вектор (x_l^0) и начальное состояние j'_0 системы считаются известными; $x_l^0 \in \{0, q, 2q, ..., \mu - q\}$, $j'_0 \in \{0, 1, 2, ..., q^k - 1\}$.

Ключи K_ξ^{-1r} могут быть как одинаковыми, так и разными. В последнем случае они должны иметь одинаковые значения m и k.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 5$.

1. $y_l^{tr} = x_l^{t,r-1} + s_l^{tr}$, где $x_l^{t0} = x_l^{t-1,\bar{r}}$, $x_l^{10} = x_l^{0\bar{r}} = x_l^0$, $s_l^{tr} = s_l'^{t,r-1}$,

$l = 1, 2,..., n$, $r = 1, 2,..., \bar{r}$; q–ичные символы $s_l'^{t,r-1}$ определяем из выражений: $i_t^r = i_t'^{r-1} = s_1'^{t,r-1} s_2'^{t,r-1} ... s_m'^{t,r-1}$, $i_t^1 = i_t'^0 = i_t$;

$j_t^r = j_t'^{r-1} = s_{m+1}'^{t,r-1} s_{m+2}'^{t,r-1} ... s_n'^{t,r-1}$, $j_t^1 = j_t'^0 = j_{t-1}'^{\bar{r}}$, $j_1^1 = j_0'^{\bar{r}} = j_0'$.

2. $\varepsilon_l^{tr} = \left[y_l^{tr} \frac{q}{\mu} \right]$ – целая часть, $v_t^r = \varepsilon_1^{tr} \varepsilon_2^{tr} ... \varepsilon_n^{tr}$.

3. $u_t^r = K_\xi^{-1r} v_t^r$, $\xi = 1, 2,..., \bar{r}$.

4. $i_t'^r = u_t^r(k>)$, $j_t'^r = u_t^r(m<, m>)$.

5. $x_l^{tr} = q y_l^{tr} \bmod \mu$.

Знаки $i_t'^{\bar{r}}$ из пункта 4 образуют последовательность $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ зашифрованной информации. Результатами шифрования являются: шифртекст $I'^{\bar{r}}$, конечный вектор $(x_l^{\Delta\bar{r}})$ и конечное состояние $j_\Delta'^{\bar{r}}$ системы.

Алгоритм чтения. На вход алгоритма последовательно поступают отдельные знаки $i_t'^{\bar{r}}$ зашифрованной информации $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ в обратном порядке с ее конца; $t = \Delta, \Delta - 1,..., 1$.

Ключи расшифрования K_ξ^r, конечный вектор $(x_l^{\Delta\bar{r}})$ и конечное состояние $j_\Delta'^{\bar{r}}$ системы считаются известными.

Цикл для $t = [\Delta, 1]$ с шагом $H = -1$, пункты $1 \div 5$.

1. $u_t^r = i_t'^r(k<) + j_t'^r$, $r = \bar{r}, \bar{r} - 1,..., 1$.

2. $v_t^r = K_\xi^r u_t^r$, $\xi = \bar{r}, \bar{r} - 1,..., 1$, $v_t^r = \varepsilon_1^{tr} \varepsilon_2^{tr} ... \varepsilon_n^{tr}$.

3. $y_l^{tr} = \frac{x_l^{tr}}{q} + \frac{\mu}{q} \varepsilon_l^{tr}$, $l = 1, 2,..., n$.

4. $s_l^{tr} = y_l^{tr} \bmod q$, $s_l'^{t,r-1} = s_l^{tr}$;

$i_t'^{r-1} = i_t^r = s_1'^{t,r-1} s_2'^{t,r-1} ... s_m'^{t,r-1}$, $i_t = i_t^1 = i_t'^0$;

$j_t'^{r-1} = j_t^r = s_{m+1}'^{t,r-1} s_{m+2}'^{t,r-1} ... s_n'^{t,r-1}$, $j_t'^0 = j_t^1 = j_{t-1}'^{\bar{r}}$,

$j_0' = j_1'^0 = j_1^1 = j_0'^{\bar{r}}$.

5. $x_l^{t,r-1} = y_l^{tr} - s_l^{tr}$, $x_l^{t-1,\bar{r}} = x_l^{t0}$, $x_l^0 = x_l^{0\bar{r}} = x_l^{1,0}$.

Знаки i_t из пункта 4 образуют последовательность $I = i_1 i_2 ... i_\Delta$ исходной информации. Результатами расшифрования являются: открытый текст I, начальный вектор (x_l^0) и начальное состояние j_0' системы.

В. Второй способ: шифрование с одним начальным вектором и многими начальными состояниями системы.

Количество вариантов шифрования:

$$z = \left(\frac{\mu}{q}\right)^n q^{k\bar{r}} (q^n!)^{\bar{r}}. \qquad (9)$$

Алгоритм записи. На вход алгоритма последовательно поступают отдельные знаки i_t исходной информации $I = i_1 i_2 ... i_\Delta$; $t = 1, 2, ..., \Delta$. Ключи шифрования K_ξ^{-1r}, начальный вектор (x_l^0) и начальные состояния $j_0'^r$ системы считаются известными; $x_l^0 \in \{0, q, 2q, ..., \mu - q\}$, $j_0'^r \in \{0, 1, 2, ..., q^k - 1\}$; ключи K_ξ^{-1r} имеют одинаковые значения m и k.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 5$.

1. $y_l^{tr} = x_l^{t,r-1} + s_l^{tr}$, где $x_l^{t0} = x_l^{t-1,\bar{r}}$, $x_l^{1,0} = x_l^{0\bar{r}} = x_l^0$,
   $l = 1, 2, ..., n$, $r = 1, 2, ..., \bar{r}$;
   $$s_l^{tr} = \begin{cases} s_l'^{t,r-1}, & l = 1, 2, ..., m \\ s_l'^{t-1,r}, & l = m+1, m+2, ..., n \end{cases};$$
   q–ичные символы $s_l'^{t,r-1}$ и $s_l'^{t-1,r}$ определяем из выражений:
   $i_t^r = i_t'^{r-1} = s_1'^{t,r-1} s_2'^{t,r-1} ... s_m'^{t,r-1}$, $i_t^1 = i_t'^0 = i_t$;
   $j_t^r = j_{t-1}'^r = s_{m+1}'^{t-1,r} s_{m+2}'^{t-1,r} ... s_n'^{t-1,r}$.
2. $\varepsilon_l^{tr} = \left[y_l^{tr} \frac{q}{\mu} \right]$ – целая часть, $v_t^r = \varepsilon_1^{tr} \varepsilon_2^{tr} ... \varepsilon_n^{tr}$.
3. $u_t^r = K_\xi^{-1r} v_t^r$, $\xi = 1, 2, ..., \bar{r}$.

4. $i'^{r}_{t} = u^{r}_{t}(k<), \quad j'^{r}_{t} = u^{r}_{t}(m<, m>)$.

5. $x^{tr}_{l} = q y^{tr}_{l} \bmod \mu$.

Знаки $i'^{\bar{r}}_{t}$ из пункта 4 образуют последовательность $I'^{\bar{r}} = i'^{\bar{r}}_{1} i'^{\bar{r}}_{2} ... i'^{\bar{r}}_{\Delta}$ зашифрованной информации. Результатами шифрования являются: шифртекст $I'^{\bar{r}}$, конечный вектор $(x^{\Delta\bar{r}}_{l})$ и конечные состояния j'^{r}_{Δ} системы.

Алгоритм чтения. На вход алгоритма последовательно поступают отдельные знаки $i'^{\bar{r}}_{t}$ зашифрованной информации $I'^{\bar{r}} = i'^{\bar{r}}_{1} i'^{\bar{r}}_{2} ... i'^{\bar{r}}_{\Delta}$ в обратном порядке с ее конца; $t = \Delta, \Delta - 1, ..., 1$. Ключи расшифрования K^{r}_{ξ}, конечный вектор $(x^{\Delta\bar{r}}_{l})$ и конечные состояния j'^{r}_{Δ} системы считаются известными.

Цикл для $t = [\Delta, 1]$ с шагом $H = -1$, пункты $1 \div 5$.

1. $u^{r}_{t} = i'^{r}_{t}(k<) + j'^{r}_{t}, \quad r = \bar{r}, \bar{r} - 1, ..., 1$.

2. $v^{r}_{t} = K^{r}_{\xi} u^{r}_{t}, \quad \xi = \bar{r}, \bar{r} - 1, ..., 1; \quad v^{r}_{t} = \varepsilon^{tr}_{1} \varepsilon^{tr}_{2} ... \varepsilon^{tr}_{n}$.

3. $y^{tr}_{l} = \dfrac{x^{tr}_{l}}{q} + \dfrac{\mu}{q} \varepsilon^{tr}_{l}, \quad l = 1, 2, ..., n$.

4. $s^{tr}_{l} = y^{tr}_{l} \bmod q$;

$s'^{t,r-1}_{l} = s^{tr}_{l}, \ l = 1, 2, ..., m, \quad s'^{t-1,r}_{l} = s^{tr}_{l}, \ l = m+1, m+2, ..., n$;

$i'^{r-1}_{t} = i^{r}_{t} = s'^{t,r-1}_{1} s'^{t,r-1}_{2} ... s'^{t,r-1}_{m}, \quad i_{t} = i^{1}_{t} = i'^{t0}_{t}$;

$j'^{r}_{t-1} = j^{r}_{t} = s'^{t-1,r}_{m+1} s'^{t-1,r}_{m+2} ... s'^{t-1,r}_{n}$.

5. $x^{t,r-1}_{l} = y^{tr}_{l} - s^{tr}_{l}, \quad x^{t-1,\bar{r}}_{l} = x^{t0}_{l}, \quad x^{0}_{l} = x^{0\bar{r}}_{l} = x^{1,0}_{l}$.

Знаки i_{t} из пункта 4 образуют последовательность $I = i_1 i_2 ... i_{\Delta}$ исходной информации. Результатами расшифрования являются: открытый текст I, начальный вектор (x^{0}_{l}) и начальные состояния j'^{r}_{0} системы.

С. Третий способ: шифрование со многими начальными векторами и одним начальным состоянием системы.

Количество вариантов шифрования:

$$z = \left(\frac{\mu}{q}\right)^{n\bar{r}} q^{k}(q^{n}!)^{\bar{r}}. \qquad (10)$$

Алгоритм записи. На вход алгоритма последовательно поступают отдельные знаки i_t исходной информации $I = i_1 i_2 ... i_\Delta$; $t = 1, 2, ..., \Delta$. Ключи шифрования K_ξ^{-1r}, начальные векторы (x_l^{0r}) и начальное состояние j_0' системы считаются известными; $x_l^{0r} \in \{0, q, 2q, ..., \mu - q\}$, $j_0' \in \{0, 1, 2, ..., q^k - 1\}$; ключи K_ξ^{-1r} имеют одинаковые значения m и k.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 5$.

1. $y_l^{tr} = x_l^{t-1, r} + s_l^{tr}$, $s_l^{tr} = s_l'^{t, r-1}$, $l = 1, 2, ..., n$, $r = 1, 2, ..., \bar{r}$;

   q–ичные символы $s_l'^{t, r-1}$ определяем из выражений:

   $i_t^r = i_t'^{r-1} = s_1'^{t, r-1} s_2'^{t, r-1} ... s_m'^{t, r-1}$, $i_t^1 = i_t'^0 = i_t$;

   $j_t^r = j_t'^{r-1} = s_{m+1}'^{t, r-1} s_{m+2}'^{t, r-1} ... s_n'^{t, r-1}$, $j_t^1 = j_t'^0 = j_{t-1}'^{\bar{r}}$, $j_1^1 = j_0'^{\bar{r}} = j_0'$.

2. $\varepsilon_l^{tr} = \left[y_l^{tr} \frac{q}{\mu} \right]$ – целая часть, $v_t^r = \varepsilon_1^{tr} \varepsilon_2^{tr} ... \varepsilon_n^{tr}$.

3. $u_t^r = K_\xi^{-1r} v_t^r$, $\xi = 1, 2, ..., \bar{r}$.

4. $i_t'^r = u_t^r(k>)$, $j_t'^r = u_t^r(m<, m>)$.

5. $x_l^{tr} = q y_l^{tr} \bmod \mu$.

Знаки $i_t'^{\bar{r}}$ из пункта 4 образуют последовательность $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ зашифрованной информации. Результатами шифрования являются: шифртекст $I'^{\bar{r}}$, конечные векторы $(x_l^{\Delta r})$ и конечное состояние $j_\Delta'^{\bar{r}}$ системы.

Алгоритм чтения. На вход алгоритма последовательно поступают отдельные знаки $i_t'^{\bar{r}}$ зашифрованной информации $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ в обратном порядке с ее конца; $t = \Delta, \Delta - 1, ..., 1$.

Ключи расшифрования K_ξ^r, конечные векторы $(x_l^{\Delta r})$ и конечное состояние $j_\Delta^{\prime\bar{r}}$ системы считаются известными.

Цикл для $t=[\Delta,1]$ с шагом $H=-1$, пункты $1\div 5$.

1. $u_t^r = i_t^{\prime r}(k<) + j_t^{\prime r}$, $r=\bar{r},\bar{r}-1,...,1$.

2. $v_t^r = K_\xi^r u_t^r$, $\xi=\bar{r},\bar{r}-1,...,1$; $v_t^r = \varepsilon_1^{tr}\varepsilon_2^{tr}...\varepsilon_n^{tr}$.

3. $y_l^{tr} = \dfrac{x_l^{tr}}{q} + \dfrac{\mu}{q}\varepsilon_l^{tr}$, $l=1,2,...,n$.

4. $s_l^{tr} = y_l^{tr} \bmod q$; $s_l^{\prime t,r-1} = s_l^{tr}$;

$i_t^{\prime r-1} = i_t^r = s_1^{\prime t,r-1}s_2^{\prime t,r-1}...s_m^{\prime t,r-1}$, $i_t = i_t^1 = i_t^{\prime 0}$;

$j_t^{\prime r-1} = j_t^r = s_{m+1}^{\prime t,r-1}s_{m+2}^{\prime t,r-1}...s_n^{\prime t,r-1}$, $j_t^{\prime 0} = j_t^1 = j_{t-1}^{\prime\bar{r}}$,

$j_0^{\prime} = j_1^{\prime 0} = j_1^1 = j_0^{\prime\bar{r}}$.

5. $x_l^{t-1,r} = y_l^{tr} - s_l^{tr}$.

Знаки i_t из пункта 4 образуют последовательность $I = i_1 i_2 ... i_\Delta$ исходной информации. Результатами расшифрования являются: открытый текст I, начальные векторы (x_l^{0r}) и начальное состояние $j_0^{\prime}$ системы.

D. Четвертый способ: шифрование со многими начальными векторами и многими начальными состояниями системы.

Количество вариантов шифрования:

$$z = \prod_{r=1}^{\bar{r}} \left(\frac{\mu}{q}\right)^{n_r} q^{k_r}\left(q^{n_r}!\right). \qquad (11)$$

Алгоритм записи. На вход алгоритма последовательно поступают отдельные знаки i_t исходной информации $I = i_1 i_2 ... i_\Delta$; $t=1,2,...,\Delta$. Ключи шифрования K_ξ^{-1r}, начальные векторы (x_l^{0r}) и начальные состояния $j_0^{\prime r}$ системы считаются известными;

$x_l^{0r} \in \{0, q, 2q, ..., \mu - q\}$, $j_0'^r \in \{0, 1, 2, ..., q^{k_r} - 1\}$; ключи K_ξ^{-1r} имеют одинаковые значения m и могут иметь разные значения $k = k_r$, $m + k_r = n_r$.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 5$.

1. $y_l^{tr} = x_l^{t-1, r} + s_l^{tr}$, $l = 1, 2, ..., n_r$, $r = 1, 2, ..., \bar{r}$;

$$s_l^{tr} = \begin{cases} s_l'^{t, r-1}, & l = 1, 2, ..., m \\ s_l'^{t-1, r}, & l = m+1, m+2, ..., n_r \end{cases};$$

q–ичные символы $s_l'^{t, r-1}$ и $s_l'^{t-1, r}$ определяем из выражений:

$i_t^r = i_t'^{r-1} = s_1'^{t, r-1} s_2'^{t, r-1} ... s_m'^{t, r-1}$, $i_t^1 = i_t'^0 = i_t$;

$j_t^r = j_{t-1}'^r = s_{m+1}'^{t-1, r} s_{m+2}'^{t-1, r} ... s_{n_r}'^{t-1, r}$.

2. $\varepsilon_l^{tr} = \left[y_l^{tr} \frac{q}{\mu} \right]$ – целая часть, $v_t^r = \varepsilon_1^{tr} \varepsilon_2^{tr} ... \varepsilon_{n_r}^{tr}$.

3. $u_t^r = K_\xi^{-1r} v_t^r$, $\xi = 1, 2, ..., \bar{r}$.

4. $i_t'^r = u_t^r(k_r >)$, $j_t'^r = u_t^r(m <, m >)$.

5. $x_l^{tr} = q y_l^{tr} \bmod \mu$.

Знаки $i_t'^{\bar{r}}$ из пункта 4 образуют последовательность $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ зашифрованной информации. Результатами шифрования являются: шифртекст $I'^{\bar{r}}$, конечные векторы $(x_l^{\Delta r})$ и конечные состояния $j_\Delta'^r$ системы.

Алгоритм чтения. На вход алгоритма последовательно поступают отдельные знаки $i_t'^{\bar{r}}$ зашифрованной информации $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ в обратном порядке с ее конца; $t = \Delta, \Delta - 1, ..., 1$. Ключи расшифрования K_ξ^r, конечные векторы $(x_l^{\Delta r})$ и конечные состояния $j_\Delta'^r$ системы считаются известными.

Цикл для $t = [\Delta, 1]$ с шагом $H = -1$, пункты $1 \div 5$.

1. $u_t^r = i_t'^r(k_r <) + j_t'^r$, $r = \bar{r}, \bar{r} - 1, ..., 1$.

2. $v_t^r = K_\xi^r u_t^r$, $\xi = \bar{r}, \bar{r}-1,..., 1$; $v_t^r = \varepsilon_1^{tr}\varepsilon_2^{tr}...\varepsilon_{n_r}^{tr}$.

3. $y_l^{tr} = \dfrac{x_l^{tr}}{q} + \dfrac{\mu}{q}\varepsilon_l^{tr}$, $l = 1, 2,..., n_r$.

4. $s_l^{tr} = y_l^{tr} \bmod q$;

$s_l'^{t,r-1} = s_l^{tr}$, $l = 1, 2,..., m$, $s_l'^{t-1,r} = s_l^{tr}$, $l = m+1, m+2,..., n_r$;

$i_t'^{r-1} = i_t^r = s_1'^{t,r-1}s_2'^{t,r-1}...s_m'^{t,r-1}$, $i_t = i_t^1 = i_t'^0$;

$j_{t-1}'^r = j_t^r = s_{m+1}'^{t-1,r}s_{m+2}'^{t-1,r}...s_{n_r}'^{t-1,r}$.

5. $x_l^{t-1,r} = y_l^{tr} - s_l^{tr}$.

Знаки i_t из пункта 4 образуют последовательность $I = i_1 i_2 ... i_\Delta$ исходной информации. Результатами расшифрования являются: открытый текст I, начальные векторы (x_l^{0r}) и начальные состояния $j_0'^r$ системы.

Алгоритмы при базисе $\mu = q$

Е. Первый способ: шифрование с одним начальным состоянием системы.

Количество вариантов шифрования:

$$z = q^k (q^n!)^{\bar{r}}. \qquad (12)$$

Алгоритм записи. На вход алгоритма последовательно поступают отдельные знаки i_t исходной информации $I = i_1 i_2 ... i_\Delta$; $t = 1, 2,..., \Delta$. Ключи шифрования K_ξ^{-1r} и начальное состояние j_0' системы считаются известными; $j_0' \in \{0, 1, 2,..., q^k - 1\}$; ключи K_ξ^{-1r} имеют одинаковые значения m и k.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 3$.

1. $v_t^r = i_t'^{r-1}(k<) + j_t'^{r-1}$, $i_t'^{r-1} = i_t^r$, $j_t'^{r-1} = j_t^r$,

$i_t'^0 = i_t$, $j_t'^0 = j_{t-1}'^{\bar{r}}$, $j_1'^0 = j_0'^{\bar{r}} = j_0'$, $r = 1, 2,..., \bar{r}$.

2. $u_t^r = K_\xi^{-1r} v_t^r$, $\xi = 1, 2,..., \bar{r}$.

3. $i_t'^r = u_t^r(k>)$, $j_t'^r = u_t^r(m<, m>)$.

Результатами шифрования являются: последовательность $I'^{\bar{r}} = i'^{\bar{r}}_1 i'^{\bar{r}}_2 ... i'^{\bar{r}}_\Delta$ зашифрованной информации и конечное состояние $j'^{\bar{r}}_\Delta$ системы.

Алгоритм чтения. На вход алгоритма последовательно поступают отдельные знаки $i'^{\bar{r}}_t$ зашифрованной информации $I'^{\bar{r}} = i'^{\bar{r}}_1 i'^{\bar{r}}_2 ... i'^{\bar{r}}_\Delta$ в обратном порядке с ее конца; $t = \Delta, \Delta - 1, ..., 1$.

Ключи расшифрования K^r_ξ и конечное состояние $j'^{\bar{r}}_\Delta$ системы считаются известными.

Цикл для $t = [\Delta, 1]$ с шагом $H = -1$, пункты $1 \div 3$.

1. $u^r_t = i'^r_t (k <) + j'^r_t$, $\quad r = \bar{r}, \bar{r} - 1, ..., 1$.

2. $v^r_t = K^r_\xi u^r_t$, $\quad \xi = \bar{r}, \bar{r} - 1, ..., 1$.

3. $i'^{r-1}_t = i^r_t = v^r_t (k >)$, $\quad j'^{r-1}_t = j^r_t = v^r_t (m <, m >)$;

$i_t = i'^0_t = i^1_t$, $\quad j'^0_t = j^1_t = j'^{\bar{r}}_{t-1}$, $\quad j'_0 = j'^0_1 = j^1_1 = j'^{\bar{r}}_0$.

Результатами расшифрования являются: последовательность $I = i_1 i_2 ... i_\Delta$ исходной информации и начальное состояние j'_0 системы.

F. Второй способ: шифрование со многими начальными состояниями системы.

Количество вариантов шифрования:

$$z = \prod_{r=1}^{\bar{r}} q^{k_r} \left(q^{n_r} ! \right). \qquad (13)$$

Алгоритм записи. На вход алгоритма последовательно поступают отдельные знаки i_t исходной информации $I = i_1 i_2 ... i_\Delta$; $t = 1, 2, ..., \Delta$. Ключи шифрования K^{-1r}_ξ и начальные состояния j'^r_0 системы считаются известными; $j'^r_0 \in \{0, 1, 2, ..., q^{k_r} - 1\}$; ключи K^{-1r}_ξ имеют одинаковые значения m и могут иметь разные значения $k = k_r$, $\quad m + k_r = n_r$.

Цикл для $t = [1, \Delta]$ с шагом $H = 1$, пункты $1 \div 3$.

1. $v^r_t = i'^{r-1}_t (k_r <) + j'^r_{t-1}$, $\quad i'^0_t = i_t$, $\quad r = 1, 2, ..., \bar{r}$.

2. $u_t^r = K_\xi^{-1r} v_t^r$, $\xi = 1, 2, ..., \bar{r}$.

3. $i_t'^r = u_t^r(k_r >)$ $j_t'^r = u_t^r(m <, m >)$.

Результатами шифрования являются: последовательность $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ зашифрованной информации и конечные состояния $j_\Delta'^r$ системы.

Алгоритм чтения. На вход алгоритма последовательно поступают отдельные знаки $i_t'^{\bar{r}}$ зашифрованной информации $I'^{\bar{r}} = i_1'^{\bar{r}} i_2'^{\bar{r}} ... i_\Delta'^{\bar{r}}$ в обратном порядке с ее конца; $t = \Delta, \Delta - 1, ..., 1$.

Ключи расшифрования K_ξ^r и конечные состояния $j_\Delta'^r$ системы считаются известными.

Цикл для $t = [\Delta, 1]$ с шагом $H = -1$, пункты $1 \div 3$.

1. $u_t^r = i_t'^r(k_r <) + j_t'^r$, $r = \bar{r}, \bar{r} - 1, ..., 1$.

2. $v_t^r = K_\xi^r u_t^r$, $\xi = \bar{r}, \bar{r} - 1, ..., 1$.

3. $i_t'^{r-1} = i_t^r = v_t^r(k_r >)$, $i_t = i_t'^0 = i_t^1$; $j_{t-1}'^r = j_t^r = v_t^r(m <, m >)$.

Результатами расшифрования являются: последовательность $I = i_1 i_2 ... i_\Delta$ исходной информации и начальные состояния $j_0'^r$ системы.

3. Классификация ключей

Структура ключа (3) определяется расположением знаков i, j в таблице v и соответствует определенному типу ключа, обозначаемому как K_{ij}^{ij}. Верхние индексы ij в этом обозначении определяют характер распределения знаков i и j в каждом столбце таблицы v, а нижние индексы ij определяют соответственно то же самое в каждой строке этой таблицы. Для индексов ij в K_{ij}^{ij} введем следующие обозначения:

0 – произвольные, 1– разные, 2 – одинаковые значения i и j в столбцах и строках таблицы v.

В ключах типа K_{i1}^{1j} имеет место равенство $m = k$. Для однократного шифрования при базисе $\mu = q$ зависимость (5) состояния системы от типа ключа имеет вид:

$$j'_t = \begin{cases} f(i_t) \text{ для } K_{21}^{1j} \\ f(j'_{t-1}) \text{ для } K_{12}^{i1} \\ f(i_t, j'_{t-1}) \text{ для всех других } K_{ij}^{ij} \end{cases} . \qquad (14)$$

При базисе $\mu > q$ состояние j'_t системы зависит также и от носителей (x_l^t) q-ичных символов s_l^t.

Аналогичные зависимости имеют место и для многократного шифрования.

Так как каждый элемент $v_{j'i'}$ в таблице v содержится только один раз, то возможны следующие 30 типов ключей, приведенных в таблице 1.

Таблица 1

K_{ij}^{ij}	0 0 0 0	0 1 0 0	1 0 0 0	1 1 0 0	0 0 0 1	0 1 0 1	1 0 0 1	1 1 0 1	0 0 1 0	0 1 1 0	1 0 1 0	1 1 1 0	0 0 1 1	0 1 1 1	1 0 1 1	1 1 1 1
K_{ij}^{ij}	0 0 2 1	0 1 2 1	1 0 2 1	1 1 2 1	1 2 2 1	2 1 1 0	2 1 1 1	2 1 1 2	1 2 0 0	1 2 0 1	1 2 1 0	1 2 1 1	0 1 1 2	1 1 1 2		

Ключ K_{11}^{11} существует только для нечетных q.

4. Иллюстрация работы алгоритмов

Простота алгоритмов шифрования и расшифрования позволяет проиллюстрировать их работу вручную без применения технических средств. Этим ручным способом можно быстро зашифровать, а затем и расшифровать достаточно большие сообщения высокостойким алгоритмом, что может найти применение в разведывательных службах. Для этой цели воспользуемся таблицей v, в которой при базисе $\mu = q$ знаки i, i', j, j' записаны для удобства в десятичной системе счисления, $q = 10$.

Содержимым этой таблицы являются слова $v = i(k<) + j$ с координатами j', i'; $v \in A = \{0, 1, 2, ..., q^n - 1\}$. В некоторых

случаях этого пункта и в дальнейшем для удобства восприятия m-значные знаки i, i' и k-значные знаки j, j' таблицы v, записанные через символы q-алфавита, будут выражены в алфавите $q = 10$.

Шифрование и расшифрование для каждого конкретного случая производится при помощи одной и той же таблицы v, выполняющей роль соответствующих ключей.

В этом пункте остановимся только на иллюстрации работы алгоритмов при однократном шифровании; многократное шифрование будет использовано в дальнейшем.

А. Шифрование и расшифрование при базисе $\mu > q$

Напомним, что i_t, i'_t – m-значные, а j_t, j'_t – k-значные числа, записанные в q-ичной системе счисления.

Алгоритм шифрования.

Исходные данные: открытый текст $I = i_1 i_2 ... i_\Delta$ (Δ – длина текста), начальный вектор $(x_l^0) = (x_1^0, x_2^0, ..., x_n^0)$ задается произвольным образом, где $x_l^0 \in \{0, q, 2q, ..., \mu - q\}$ – целые десятичные числа, μ / q – целое число, начальное состояние j'_0 системы произвольно выбираем из множества $\{0, 1, 2, ..., q^k - 1\}$.

1. $y_l^t = x_l^{t-1} + s_l^t$, $l = 1, 2, ..., n$, $t = 1, 2, ..., \Delta$,

$$s_l^t = \begin{cases} s_l^t, & l = 1, 2, ..., m \\ s_l'^{t-1}, & l = m+1, m+2, ..., n, \quad n = m + k \end{cases},$$

где q-ичные символы s_l^t и $s_l'^t$ определяем из выражений:

$i_t = s_1^t s_2^t ... s_m^t$, $j_t = j'_{t-1} = s_{m+1}'^{t-1} s_{m+2}'^{t-1} ... s_n'^{t-1}$.

2. $\varepsilon_l^t = \left[y_l^t \frac{q}{\mu} \right]$ – целая часть, $v_t = \varepsilon_1^t \varepsilon_2^t ... \varepsilon_n^t$.

3. Из $v_t \Rightarrow i'_t$, j'_t по таблице v.

4. $x_l^t = q y_l^t \bmod \mu$.

Результатами шифрования являются: шифртекст $I' = i'_1 i'_2 ... i'_\Delta$, конечный вектор $(x_l^\Delta) = (x_1^\Delta, x_2^\Delta, ..., x_n^\Delta)$, конечное состояние j'_Δ системы.

Алгоритм расшифрования.

Исходные данные: шифртекст $I' = i'_1 i'_2 ... i'_\Delta$, конечный вектор $(x_l^\Delta) = (x_1^\Delta, x_2^\Delta, ..., x_n^\Delta)$ и конечное состояние j'_Δ системы. Знаки i'_t поступают на вход алгоритма с конца шифртекста.

1. По координатам j'_t, i'_t таблицы v определяем $v_t = \varepsilon_1^t \varepsilon_2^t ... \varepsilon_n^t$, где $t = \Delta, \Delta - 1, ..., 1$

2. $y_l^t = \dfrac{x_l^t}{q} + \dfrac{\mu}{q} \varepsilon_l^t$, $\quad l = 1, 2, ..., n$.

3. $s_l^t = y_l^t \bmod q \Rightarrow i_t = s_1^t s_2^t ... s_m^t$, $\quad j'_{t-1} = j_t = s'^{t-1}_{m+1} s'^{t-1}_{m+2} ... s'^{t-1}_n$,
$s'^{t-1}_l = s_l^t$, $\quad l = m+1, m+2, ..., n$.

4. $x_l^{t-1} = y_l^t - s_l^t$.

Результатами расшифрования являются: открытый текст $I = i_1 i_2 ... i_\Delta$, начальный вектор $(x_l^0) = (x_1^0, x_2^0, ..., x_n^0)$ и начальное состояние j'_0 системы.

Пример 1. Система $[q, \mu, m, k] = [2, 10, 1, 1]$, ключ K_{21}^{11}, $n = m + k = 2$, длина открытого текста $\Delta = 10$ знаков i_t, $l = 1, 2$.

Шифрование

Из значений $x_l^0 \in \{0, q, 2q, ..., \mu - q\} = \{0, 2, 4, 6, 8\}$

произвольно образуем начальный вектор $(x_l^0) = (x_1^0, x_2^0) = (2, 6)$.

Из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1\}$ произвольно выбираем значение начального состояния $j'_0 = 1$ системы.

Таблица v Ключ $K_{ij}^{ij} = K_{21}^{11}$				Шифрование										
					i_t	y_l^t		v_t		i'_t	j'_t	x_l^t	
i'	0		1	t	s_1^t	y_1^t	y_2^t	ε_1^t	ε_2^t		s'^t_2	x_1^t	x_2^t
j'	i	j	i	j	0							1	2	6

0	0	0	0	1	1	1	3	7	0	1	1	0	6	4
1	1	1	1	0	2	0	6	4	1	0	1	1	2	8
					3	1	3	9	0	1	1	0	6	8
					4	1	7	8	1	1	0	1	4	6
					5	0	4	7	0	1	1	0	8	4
					6	0	8	4	1	0	1	1	6	8
					7	0	6	9	1	1	0	1	2	8
					8	1	3	9	0	1	1	0	6	8
					9	1	7	8	1	1	0	1	4	6
					10	0	4	7	0	1	1	0	8	4

Результаты шифрования: шифртекст – знаки i'_t, конечный вектор $(x_l^{\Delta}) = (x_1^{\Delta}, x_2^{\Delta}, ..., x_n^{\Delta}) = (x_1^{10}, x_2^{10}) = (8, 4)$, конечное состояние $j'_{\Delta} = j'_{10} = 0$ системы.

Расшифрование

Исходными данными для расшифрования являются результаты шифрования. Знаки i'_t поступают на вход алгоритма с конца шифртекста, $t = \Delta, \Delta - 1, ..., 1 = 10, 9, ..., 1$.

Таблица v Ключ $K_{ij}^{ij} = K_{21}^{11}$					Расшифрование									
						i'_t	v_t		y_l^t		i_t	j'_t	x_l^t	
i'	0		1		t		ε_1^t	ε_2^t	y_1^t	y_2^t	s_1^t	$s_2'^t$	x_1^t	x_2^t
j'	i	j	i	j	0							1	2	6
0	0	0	0	1	1	1	0	1	3	7	1	0	6	4
1	1	1	1	0	2	1	1	0	6	4	0	1	2	8
					3	1	0	1	3	9	1	0	6	8
					4	0	1	1	7	8	1	1	4	6
					5	1	0	1	4	7	0	0	8	4
					6	1	1	0	8	4	0	1	6	8
					7	0	1	1	6	9	0	1	2	8
					8	1	0	1	3	9	1	0	6	8
					9	0	1	1	7	8	1	1	4	6
					10	1	0	1	4	7	0	0	8	4

Результатами расшифрования являются исходные данные для шифрования.

Пример 2. Система $[q, \mu, m, k] = [2, 10, 1, 2]$, ключ K_{21}^{01}, $n = m + k = 3$, длина открытого текста $\Delta = 10$ знаков i_t, $l = 1, 2, 3$.

Таблица v Ключ $K_{ij}^{ij} = K_{21}^{01}$				
i'	0		1	
j'	i	j	i	j
00	0	00	0	01
01	1	01	1	10
10	0	10	0	11
11	1	11	1	00

Шифрование

Из значений $x_l^0 \in \{0, q, 2q, ..., \mu - q\} = \{0, 2, 4, 6, 8\}$ произвольно образуем начальный вектор $(x_l^0) = (x_1^0, x_2^0, x_3^0) = (2, 4, 6)$.

Из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3\}$ произвольно выбираем значение начального состояния $j_0' = 1 = 01$ системы, записанного в десятичной и двоичной системах счисления.

Шифрование													
	i_t	y_l^t			v_t			i_t'	j_t'		x_l^t		
t	s_1^t	y_1^t	y_2^t	y_3^t	ε_1^t	ε_2^t	ε_3^t		$s_2'^t$	$s_3'^t$	x_1^t	x_2^t	x_3^t
0									0	1	2	4	6
1	0	2	4	7	0	0	1	1	0	0	4	8	4
2	1	5	8	4	1	1	0	1	0	1	0	6	8
3	1	1	6	9	0	1	1	1	1	0	2	2	8
4	0	2	3	8	0	0	1	1	0	0	4	6	6
5	1	5	6	6	1	1	1	0	1	1	0	2	2
6	0	0	3	3	0	0	0	0	0	0	0	6	6
7	0	0	6	6	0	1	1	1	1	0	0	2	2
8	1	1	3	2	0	0	0	0	0	0	2	6	4
9	1	3	6	4	0	1	0	0	1	0	6	2	8
10	0	6	3	8	1	0	1	0	0	1	2	6	6

Результаты шифрования: шифртекст – знаки i_t', конечный вектор $(x_l^\Delta) = (x_1^\Delta, x_2^\Delta, ..., x_n^\Delta) = (x_1^{10}, x_2^{10}, x_3^{10}) = (2, 6, 6)$, конечное состояние $j_\Delta' = j_{10}' = 01$ системы.

Расшифрование

Исходными данными для расшифрования являются результаты шифрования. Знаки i_t' поступают на вход алгоритма с конца шифртекста, $t = \Delta, \Delta - 1, ..., 1 = 10, 9, ..., 1$.

Расшифрование													
	i'_t	v_t			y_l^t			i_t	j'_t		x_l^t		
t		ε_1^t	ε_2^t	ε_3^t	y_1^t	y_2^t	y_3^t	s_1^t	$s_2''^t$	$s_3''^t$	x_1^t	x_2^t	x_3^t
0									0	1	2	4	6
1	1	0	0	1	2	4	7	0	0	0	4	8	4
2	1	1	1	0	5	8	4	1	0	1	0	6	8
3	1	0	1	1	1	6	9	1	1	0	2	2	8
4	1	0	0	1	2	3	8	0	0	0	4	6	6
5	0	1	1	1	5	6	6	1	1	1	0	2	2
6	0	0	0	0	0	3	3	0	0	0	0	6	6
7	1	0	1	1	0	6	6	0	1	0	0	2	2
8	0	0	0	0	1	3	2	1	0	0	2	6	4
9	0	0	1	0	3	6	4	1	1	0	6	2	8
10	0	1	0	1	6	3	8	0	0	1	2	6	6

Результатами расшифрования являются исходные данные для шифрования.

Пример 3. Система $[q, \mu, m, k] = [2, 10, 2, 1]$, ключ K_{10}^{12}, $n = m + k = 3$, длина открытого текста $\Delta = 10$ знаков i_t, $l = 1, 2, 3$.

Таблица v Ключ $K_{ij}^{ij} = K_{10}^{12}$								
i'	00		01		10		11	
j'	i	j	i	j	i	j	i	j
0	00	0	01	1	10	0	11	1
1	01	0	10	1	11	0	00	1

Шифрование

Из значений $x_l^0 \in \{0, q, 2q, ..., \mu - q\} = \{0, 2, 4, 6, 8\}$ произвольно образуем начальный вектор $(x_l^0) = (x_1^0, x_2^0, x_3^0) = (0, 0, 0)$.

Из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1\}$ произвольно выбираем значение начального состояния $j'_0 = 0$ системы.

Шифрование														
	i_t		y_l^t			v_t			i'_t		j'_t	x_l^t		
t	s_1^t	s_2^t	y_1^t	y_2^t	y_3^t	ε_1^t	ε_2^t	ε_3^t			$s_3''^t$	x_1^t	x_2^t	x_3^t
0											0	0	0	0

1	0	1	0	1	0	0	0	0	0	0	0	0	2	0
2	1	1	1	3	0	0	0	0	0	0	0	2	6	0
3	0	0	2	6	0	0	1	0	0	0	1	4	2	0
4	1	0	5	2	1	1	0	0	1	0	0	0	4	2
5	0	1	0	5	2	0	1	0	0	0	1	0	0	4
6	0	0	0	0	5	0	0	1	1	1	1	0	0	0
7	1	1	1	1	1	0	0	0	0	0	0	2	2	2
8	1	1	3	3	2	0	0	0	0	0	0	6	6	4
9	0	0	6	6	4	1	1	0	1	0	1	2	2	8
10	1	0	3	2	9	0	0	1	1	1	1	6	4	8

Результаты шифрования: шифртекст – знаки i'_t, конечный вектор $(x_l^{\Delta}) = (x_1^{\Delta}, x_2^{\Delta}, ..., x_n^{\Delta}) = (x_1^{10}, x_2^{10}, x_3^{10}) = (6, 4, 8)$, конечное состояние $j'_{\Delta} = j'_{10} = 1$ системы.

Расшифрование

Исходными данными для расшифрования являются результаты шифрования. Знаки i'_t поступают на вход алгоритма с конца шифртекста, $t = \Delta, \Delta - 1, ..., 1 = 10, 9, ..., 1$.

Расшифрование															
	i'_t		v_t			y_l^t			i_t		j'_t	x_l^t			
t			ε_1^t	ε_2^t	ε_3^t	y_1^t	y_2^t	y_3^t	s_1^t	s_2^t	$s_3'^t$	x_1^t	x_2^t	x_3^t
0											0	0	0	0
1	0	0	0	0	0	0	1	0	0	1	0	0	2	0
2	0	0	0	0	0	1	3	0	1	1	0	2	6	0
3	0	0	0	1	0	2	6	0	0	0	1	4	2	0
4	1	0	1	0	0	5	2	1	1	0	0	0	4	2
5	0	0	0	1	0	0	5	2	0	1	1	0	0	4
6	1	1	0	0	1	0	0	5	0	0	1	0	0	0
7	0	0	0	0	0	1	1	1	1	1	0	2	2	2
8	0	0	0	0	0	3	3	2	1	1	0	6	6	4
9	1	0	1	1	0	6	6	4	0	0	1	2	2	8
10	1	1	0	0	1	3	2	9	1	0	1	6	4	8

Результатами расшифрования являются исходные данные для шифрования.

Пример 4. Система $[q, \mu, m, k] = [2, 10, 2, 2]$, ключ K_{01}^{11}, $n = m + k = 4$, длина открытого текста $\Delta = 10$ знаков i_t, $l = 1, 2, 3, 4$.

Таблица v Ключ $K_{ij}^{ij} = K_{01}^{11}$								
i'	00		01		10		11	
j'	i	j	i	j	i	j	i	j
00	00	00	10	01	00	10	10	11
01	01	01	11	10	01	11	11	00
10	10	10	00	11	10	00	00	01
11	11	11	01	00	11	01	01	10

Шифрование

Из значений $x_l^0 \in \{0, q, 2q,..., \mu - q\} = \{0, 2, 4, 6, 8\}$ произвольно образуем начальный вектор

$(x_l^0) = (x_1^0, x_2^0, x_3^0, x_4^0) = (0, 2, 4, 6)$.

Из множества $\{0, 1, 2,..., q^k - 1\} = \{0, 1, 2, 3\}$ произвольно выбираем значение начального состояния $j'_0 = 2 = 10$ системы, записанного в десятичной и двоичной системах счисления.

Шифрование																		
	i_t		y_l^t				v_t				i'_t		j'_t		x_l^t			
t	s_1^t	s_2^t	y_1^t	y_2^t	y_3^t	y_4^t	ε_1^t	ε_2^t	ε_3^t	ε_4^t			$s_3'^t$	$s_4'^t$	x_1^t	x_2^t	x_3^t	x_4^t
0													1	0	0	2	4	6
1	1	0	1	2	5	6	0	0	1	1	0	1	1	0	2	4	0	2
2	0	1	2	5	1	2	0	1	0	0	0	1	1	1	4	0	2	4
3	0	0	4	0	3	5	0	0	0	1	1	1	1	0	8	0	6	0
4	1	1	9	1	7	0	1	0	1	0	0	0	1	0	8	2	4	0
5	0	1	8	3	5	0	1	0	1	0	0	0	1	0	6	6	0	0
6	0	0	6	6	1	0	1	1	0	0	1	1	0	1	2	2	2	0
7	0	0	2	2	2	1	0	0	0	0	0	0	0	0	4	4	4	2
8	1	0	5	4	4	2	1	0	0	0	1	0	1	0	0	8	8	4
9	1	1	1	9	9	4	0	1	1	0	1	1	1	1	2	8	8	8
10	0	1	2	9	9	9	0	1	1	1	1	0	0	1	4	8	8	8

Результаты шифрования: шифртекст – знаки i'_t,

конечный вектор

$(x_l^\Delta) = (x_1^\Delta, x_2^\Delta,..., x_n^\Delta) = (x_1^{10}, x_2^{10}, x_3^{10}, x_4^{10}) = (4, 8, 8, 8)$,

конечное состояние $j'_\Delta = j'_{10} = 01$ системы.

Расшифрование

Исходными данными для расшифрования являются результаты шифрования. Знаки i'_t поступают на вход алгоритма с конца шифртекста, $t = \Delta, \Delta - 1, ..., 1 = 10, 9, ..., 1$.

Расшифрование																			
	i'_t		v_t				y_l^t				i_t		j'_t		x_l^t				
t			ε_1^t	ε_2^t	ε_3^t	ε_4^t	y_1^t	y_2^t	y_3^t	y_4^t	s_1^t	s_2^t	$s_3'^t$	$s_4'^t$	x_1^t	x_2^t	x_3^t	x_4^t	
0													1	0	0	2	4	6	
1	0	1	0	0	1	1	1	2	5	6	1	0	1	0	2	4	0	2	
2	0	1	0	1	0	0	2	5	1	2	0	1	1	1	4	0	2	4	
3	1	1	0	0	0	1	4	0	3	5	0	0	1	0	8	0	6	0	
4	0	0	1	0	1	0	9	1	7	0	1	1	1	0	8	2	4	0	
5	0	0	1	0	1	0	8	3	5	0	0	1	1	0	6	6	0	0	
6	1	1	1	1	0	0	6	6	1	0	0	0	0	1	2	2	2	0	
7	0	0	0	0	0	0	2	2	2	1	0	0	0	0	4	4	4	2	
8	1	0	1	0	0	0	5	4	4	2	1	0	1	0	0	8	8	4	
9	1	1	0	1	1	0	1	9	9	4	1	1	1	1	2	8	8	8	
10	1	0	0	1	1	1	2	9	9	9	0	1	0	1	4	8	8	8	

Результатами расшифрования являются исходные данные для шифрования.

Пример 5. Система $[q, \mu, m, k] = [3, 15, 1, 1]$, ключ K_{11}^{11}, $n = m + k = 2$, длина открытого текста $\Delta = 10$ знаков i_t, $l = 1, 2$.

Таблица v Ключ $K_{ij}^{ij} = K_{11}^{11}$						
i'	0		1		2	
j'	i	j	i	j	i	j
0	0	0	2	1	1	2
1	1	1	0	2	2	0
2	2	2	1	0	0	1

Шифрование

Из значений

$x_l^0 \in \{0, q, 2q, ..., \mu - q\} = \{0, 2, 4, 6, 8, 10, 12\}$ произвольно

образуем начальный вектор $(x_l^0) = (x_1^0, x_2^0) = (6, 9)$.

Из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2\}$ произвольно выбираем значение начального состояния $j'_0 = 2 = 2$ системы, записанного в десятичной и троичной системах счисления.

Шифрование									
	i_t	y_l^t		v_t		i'_t	j'_t	x_l^t	
t	s_1^t	y_1^t	y_2^t	ε_1^t	ε_2^t		$s_2'^t$	x_1^t	x_2^t
0							2	6	9
1	1	7	11	1	2	2	0	6	3
2	0	6	3	1	0	1	2	3	9
3	2	5	11	1	2	2	0	0	3
4	1	1	3	0	0	0	0	3	9
5	2	5	9	1	1	0	1	0	12
6	0	0	13	0	2	1	1	0	9
7	1	1	10	0	2	1	1	3	0
8	2	5	1	1	0	1	2	0	3
9	2	2	5	0	1	2	2	6	0
10	0	6	2	1	0	1	2	3	6

Результаты шифрования: шифртекст – знаки i'_t, конечный вектор $(x_l^{\Delta}) = (x_1^{\Delta}, x_2^{\Delta}) = (x_1^{10}, x_2^{10}) = (3, 6)$, конечное состояние $j'_{\Delta} = j'_{10} = 2$ системы.

Расшифрование

Исходными данными для расшифрования являются результаты шифрования. Знаки i'_t поступают на вход алгоритма с конца шифртекста, $t = \Delta, \Delta - 1, ..., 1 = 10, 9, ..., 1$.

Расшифрование									
	i'_t	v_t		y_l^t		i_t	j'_t	x_l^t	
t		ε_1^t	ε_2^t	y_1^t	y_2^t	s_1^t	$s_2'^t$	x_1^t	x_2^t
0							2	6	9
1	2	1	2	7	11	1	0	6	3
2	1	1	0	6	3	0	2	3	9
3	2	1	2	5	11	2	0	0	3
4	0	0	0	1	3	1	0	3	9
5	0	1	1	5	9	2	1	0	12
6	1	0	2	0	13	0	1	0	9
7	1	0	2	1	10	1	1	3	0
8	1	1	0	5	1	2	2	0	3
9	2	0	1	2	5	2	2	6	0
10	1	1	0	6	2	0	2	3	6

Результатами расшифрования являются исходные данные для шифрования.

В. Шифрование и расшифрование при базисе $\mu = q$

Напомним, что i_t, i'_t – m-значные, а j_t, j'_t – k-значные числа, записанные в q-ичной системе счисления.

Алгоритм шифрования.

Исходные данные: открытый текст $I = i_1 i_2 ... i_\Delta$ (Δ – длина текста) и начальное состояние j'_0 системы, произвольно выбираемое из множества $\{0, 1, 2, ..., q^k - 1\}$.

1. $v_t = i_t(k<) + j'_{t-1}$, $t = 1, 2, ..., \Delta$, где v_t – содержимое таблицы v, имеющее координаты i'_t, j'_t.
2. По таблице v из $v_t \Rightarrow i'_t$, j'_t.

Результатами шифрования являются: шифртекст $I' = i'_1 i'_2 ... i'_\Delta$ и конечное состояние j'_Δ системы.

Алгоритм расшифрования.

Исходные данные: шифртекст $I' = i'_1 i'_2 ... i'_\Delta$ и конечное состояние j'_Δ системы.

1. По координатам i'_t, j'_t таблицы v определяем содержимое v_t соответствующей ячейки, $t = \Delta, \Delta - 1, ..., 1$.
2. Из v_t определяем: $i_t = v_t(k>)$, $j'_{t-1} = j_t = v_t(m<, m>)$.

Результатами расшифрования являются: открытый текст $I = i_1 i_2 ... i_\Delta$ и начальное состояние j'_0 системы.

Пример 1. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, ключ K_{01}^{11}, $n = m + k = 4$, длина открытого текста $\Delta = 10$ знаков i_t, $t = 1, 2, ..., 10$. Из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3\}$ произвольно выбираем значение начального состояния $j'_0 = 0 = 00$ системы, записанного в десятичной и двоичной системах счисления соответственно.

Расшифрование осуществляем в обратном порядке от конца шифртекста, $t = 10, 9, ..., 1$.

Все знаки i, i' и j, j' выражаем через символы q-ичной системы счисления, но для удобства восприятия записываем их в десятичной системе счисления.

Таблица v Ключ $K_{ij}^{ij} = K_{01}^{11}$								
i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	0	0	2	1	0	2	2	3
1	1	1	3	2	1	3	3	0
2	2	2	0	3	2	0	0	1
3	3	3	1	0	3	1	1	2

Связь между системами счисления				
$q=2$	00	01	10	11
$q=10$	0	1	2	3

Шифрование			
t	i_t	i'_t	j'_t
0			0
1	2	2	2
2	0	2	0
3	1	1	3
4	3	0	3
5	2	3	0
6	3	3	1
7	1	0	1
8	0	3	2
9	2	0	2
10	1	3	3

Пример 2. Система $[q, \mu, m, k]=[3, 3, 2, 2]$, ключ K_{11}^{11}, $n = m + k = 4$, длина открытого текста $\Delta = 10$ знаков i_t, $t = 1, 2,..., 10$.

Из множества $\{0, 1, 2,..., q^k - 1\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ произвольно выбираем значение начального состояния $j'_0 = 5 = 12$ системы, записанного в десятичной и троичной системах счисления соответственно.

Расшифрование осуществляем в обратном порядке от конца шифртекста, $t = 10, 9,..., 1$.

Таблица v Ключ $K_{ij}^{ij} = K_{11}^{11}$																		
i'	0		1		2		3		4		5		6		7		8	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	0	0	2	1	4	2	6	3	8	4	1	5	3	6	5	7	7	8
1	1	1	3	2	5	3	7	4	0	5	2	6	4	7	6	8	8	0
2	2	2	4	3	6	4	8	5	1	6	3	7	5	8	7	0	0	1
3	3	3	5	4	7	5	0	6	2	7	4	8	6	0	8	1	1	2
4	4	4	6	5	8	6	1	7	3	8	5	0	7	1	0	2	2	3
5	5	5	7	6	0	7	2	8	4	0	6	1	8	2	1	3	3	4
6	6	6	8	7	1	8	3	0	5	1	7	2	0	3	2	4	4	5
7	7	7	0	8	2	0	4	1	6	2	8	3	1	4	3	5	5	6
8	8	8	1	0	3	1	5	2	7	3	0	4	2	5	4	6	6	7

Связь между системами счисления									
$q=3$	00	01	02	10	11	12	20	21	22
$q=10$	0	1	2	3	4	5	6	7	8

Шифрование			
t	i_t	i'_t	j'_t
0			5
1	2	6	8
2	7	8	0
3	4	4	5
4	0	4	1
5	1	0	1
6	3	2	8
7	5	6	2
8	2	0	2
9	6	4	7
10	8	1	6

5. Свойства криптографических систем

А. Отображение входного знака открытого текста в выходные знаки шифртекста

Из алгоритма шифрования и зависимости (5) следует, что найдутся криптосистемы, для которых каждый знак шифртекста является сложной функцией текущего входного знака, всех предыдущих входных знаков открытого текста, всех элементов ключа (3) и начального состояния j'_0 системы.

Свойство 1. Одинаковые последовательности открытого текста отображаются при шифровании во всевозможные последовательности той же длины шифрованного текста.

Из этого свойства следует, что работа ключа эквивалентна работе ленты одноразового использования. Для разных систем в большей или меньшей степени свойство 1 выполняется, исключая вырожденные случаи в системах с ключом K_{ij}^{21}, дающих одно отображение. Наиболее подходящими для этой цели являются системы с базисом $\mu = q$ и ключом K_{10}^{11}, в котором знаки j, расположенные на строке j', не равны j'.

Последовательность $I_\delta = i_1 i_2 ... i_\delta$ длиной δ знаков i отображается при шифровании в q^k образов $I'_\delta = i'_1 i'_2 ... i'_\delta$.

Степень такого отображения:

$$\varkappa = \frac{N'}{N} = \frac{q^k}{q^{m\delta}} = q^{k-m\delta}, \qquad (15)$$

где N' – количество образов I'_δ последовательности I_δ, N – количество всех последовательностей I_δ. При $\varkappa = 1$ работа ключа полностью эквивалентна работе ленты одноразового использования. Так как количество элементов ключа равно q^{m+k}, то при $\varkappa = 1$ и последовательности I_δ практически значимой длины размеры ключа могут оказаться достаточно большими, $k = m\delta$. Однако значение $\varkappa = 1$ может быть достигнуто в системах K_{10}^{11} с меньшими значениями m и k для последовательностей I_δ любой длины. Для этого в пункте 1 алгоритма **4.В** надо произвести модификацию знака:

$$i_t \to i_t \oplus i'_{t-\delta}, \qquad (16)$$

осуществляющую обратную связь по шифртексту; символ $\oplus$ означает поразрядное сложение по модулю q. В результате указанной модификации последовательность I_δ отображается при шифровании в $q^{m\delta}$ образов I'_δ, что соответствует работе ленты одноразового использования. Для осуществления такого

шифрования вводим начальный вектор $I'^{0}_{\delta} = i'_{-(\delta-1)} i'_{-(\delta-2)} ... i'_{-1} i'_{0}$. Если в (16) величина δ выбираемого знака $i'_{t-\delta}$ периодически принимает значения из некоторой последовательности:

$$L_{\delta} = \delta_1 \delta_2 ... \delta_d \qquad (17)$$

длиной d, то эта последовательность может выполнять роль дополнительного ключа. С учетом модификации (16) свойство 1 легко доказывается. Для последовательности $I_{\delta} = i_t i_{t+1} ... i_{t+\delta-1}$ и состояния j'_{t-1} системы, многократно повторяющихся при шифровании, существует множество последовательностей $I'_{t-\delta} = i'_{t-1} i'_{t-2} ... i'_{t-\delta}$, принимающих $q^{m\delta}$ различных образов ввиду разнообразия открытого текста. Воздействие последовательности $I'_{t-\delta}$ на последовательность I_{δ} по схеме (16) преобразует последовательность I_{δ} во множество $q^{m\delta}$ различных последовательностей, которые при одинаковом состоянии j'_{t-1} системы образуют такое же количество образов I'_{δ}.

Проверим свойство 1 на простой системе $[q, \mu, m, k] = [2, 2, 1, 1]$, ключ K_{12}^{11}, $n = m + k = 2$. Из однобитовых знаков i открытого текста образуем 4-х битовые слова $a = i_1 i_2 i_3 i_4 \in \{0, 1, 2, ..., 15\}$, соответствующие словам $a' = i'_1 i'_2 i'_3 i'_4 \in \{0, 1, 2, ..., 15\}$ шифртекста. Открытый текст составим так, чтобы каждое слово $a = i_1 i_2 i_3 i_4$ из множества $\{0, 1, 2, ..., 15\}$ входило в него 36 раз. В результате получим открытый текст длиной $\Delta = 16 \times 36 = 576$ слов $a = i_1 i_2 i_3 i_4$. По результатам шифрования этого текста составим таблицу 2, показывающую число отображений каждого слова $a = i_1 i_2 i_3 i_4$ в соответствующее слово $a' = i'_1 i'_2 i'_3 i'_4$. В таблице 2 слова a и a' записаны в десятичной системе счисления. Начальный вектор $I'^{0}_{\delta} = 0000$ выбираем произвольно, $\delta = 4$, $j'_0 = 0$.

Таблица v Ключ $K_{ij}^{ij} = K_{12}^{11}$				
i'	0		1	
j'	i	j	i	j
0	0	1	1	1
1	1	0	0	0

Связь между системами счисления								
$q=2$	0000	0001	0010	0011	0100	0101	0110	0111
$q=10$	0	1	2	3	4	5	6	7
$q=2$	1000	1001	1010	1011	1100	1101	1110	1111
$q=10$	8	9	10	11	12	13	14	15

a – в столбце, a' – в строке Таблица 2

$a\backslash a'$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	3	1	3	3	0	5	3	3	3	1	1	2	2	2	3	1
1	2	3	1	1	2	1	4	3	3	5	4	1	2	1	2	1
2	2	4	3	3	2	1	2	2	2	4	1	3	4	2	1	0
3	1	1	4	3	3	3	3	1	1	2	2	1	4	1	3	3
4	2	1	5	2	3	2	1	1	2	2	2	1	3	4	3	2
5	1	1	3	1	1	2	0	1	4	4	7	5	0	3	2	1
6	1	3	2	1	3	1	1	2	2	4	4	4	2	1	3	2
7	2	4	0	4	1	1	3	3	3	2	1	3	3	1	2	3
8	4	2	1	3	1	1	0	1	1	2	4	3	1	2	6	4
9	4	1	2	2	2	1	1	5	2	0	2	4	2	3	1	4
10	5	1	2	2	0	5	1	1	3	4	2	4	2	2	2	0
11	2	4	0	1	2	5	1	1	2	1	2	5	2	2	4	2
12	2	0	5	2	1	3	1	2	3	2	2	3	4	1	3	2
13	1	4	6	4	1	3	1	2	0	0	4	3	2	2	1	2
14	1	2	3	2	6	5	2	1	0	1	3	3	1	1	1	4
15	3	1	0	3	1	2	1	2	0	2	5	6	1	3	1	5

Из таблицы 2 следует, что для рассмотренного примера свойство 1 выполняется.

В. Распространение ошибки

Изменения в ключе, потеря знака при передаче зашифрованных сообщений, изменения в знаках i, i', j'_0, j'_Δ и векторах (x_l^0), (x_l^Δ) приводят к появлению и распространению ошибки в

открытом и шифрованном текстах. Наибольшее распространение ошибки происходит в системах с ключами K_{11}^{11} и K_{11}^{01}. В системах с базисом $\mu > q$ распространение ошибки происходит в большей степени, чем при базисе $\mu = q$, из-за влияния вектора (x_l^t). Рассматриваемые ниже системы относятся к базису $\mu = q$. При однократном изменении одного из указанных выше знаков длина распространения ошибки в открытом и шифрованном текстах определяется структурой ключа и может быть равна всей оставшейся части соответствующего текста.

В синхронных поточных системах K_{12}^{i1} при одном нарушении знака шифртекста возникает один ошибочно дешифрованный знак. В поточных системах с самосинхронизацией, определяемых ключом K_{ij}^{12}, при одном нарушении знака шифртекста возникает не более двух ошибочно дешифрованных знаков, а при потере знака шифртекста – один ошибочно дешифрованный знак.

В системах K_{i1}^{i1} одно нарушение знака шифртекста приводит со следующего шага в зависимости от значения верхнего индекса i к следующим ситуациям:

$i = 1$ – весь текст дешифрован неправильно;

$i = 0$ – произвольное чередование правильно и неправильно дешифрованных знаков;

$i = 2$ – весь текст дешифрован правильно.

Во всех этих случаях дешифрованное значение $j'_{0d} \neq j'_0$, что может служить контролем подлинности шифртекста. В дальнейшем это свойство будет использовано для аутентификации данных.

Повторное нарушение шифртекста может привести к равенству:

$$j'_{0d} = j'_0, \qquad (18)$$

реализация которого зависит от значений всех измененных знаков шифртекста и от значений параметров m и k, определяющих размеры ключа K_{i1}^{i1}. Выполнение равенства (18) более затруднительно в системах при $k >> m$.

Рассмотрим множество $\{L'_{j'_\Delta}\}$ всех последовательностей, порождаемых системой K_{i1}^{i1} с $m = k$ при шифровании с

начальным состоянием j'_0 соответствующих последовательностей одинаковой длины $\Delta \geq 2$ знаков i множества $\{L_{j'_\Delta}\}$ и относящихся к одному конечному состоянию j'_Δ. Последовательности $L'_{j'_\Delta}$ и $L_{j'_\Delta}$ взаимно однозначно отображаются друг в друга.

Теорема 1. В системах K_{i1}^{i1} с $m = k$ и $q^k \geq 3$ при базисе $\mu = q$ для любой последовательности $L'_{j'_\Delta} \in \{L'_{j'_\Delta}\}$ найдется последовательность $\widetilde{L}'_{j'_\Delta} \in \{L'_{j'_\Delta}\}$, отличающаяся от взятой в $2, 3, ..., \Delta$ знаках i' шифртекста.

Доказательство. Пусть $L'_{j'_\Delta} = i'_1 i'_2 ... i'_\Delta$ взятая последовательность, в которой могут быть нарушены любые знаки i'_t. Последовательность $L'_{j'_\Delta} \in \{L'_{j'_\Delta}\}$, если при ее дешифровании выполняется равенство (18). При дешифровании $L'_{j'_\Delta}$ на шаге t для правильного знака i'_t получим правильный знак $j_t = j'_{t-1}$, а для измененного знака $\widetilde{i}'_t$ получим ошибочный знак $\widetilde{j}_t = \widetilde{j}'_{t-1}$, принимающий одно из $(q^k - 1)$ значений. На следующем шаге $(t-1)$ при правильном знаке i'_{t-1} получим:

$$j_{t-1} \neq \widetilde{j}_{t-1}, \qquad (19)$$

так как в ключе K_{i1}^{i1} для каждого столбца все знаки j различны.

Неравенство (19) выполняется для $(q^k - 2)$ измененных знаков $\widetilde{i}'_{t-1}$ и нарушается для одного знака $\widetilde{i}'_{t-1}$, при котором выполняется равенство:

$$j_{t-1} = \widetilde{j}_{t-1}. \qquad (20)$$

На каждом $(t-h)$ шаге $(h \geq 2)$ возможен выбор либо неравенства:

$$j_{t-h} \neq \widetilde{j}_{t-h}, \qquad (21)$$

либо равенства:

$$j_{t-h} = \widetilde{j}_{t-h}. \qquad (22)$$

При выборе неравенства (21) знак i'_{t-h} либо верный, либо нарушенный; при выборе равенства (22) знак i'_{t-h} нарушен.

Если после $(t-h)$-го шага нарушений знаков i' нет, то равенство (22) приведет к выполнению равенства (18), вследствие чего $\widetilde{L}'_{j'_\Delta} \in \{L'_{j'_\Delta}\}$. Здесь $\widetilde{L}'_{j'_\Delta}$ последовательность, отличающаяся от $L'_{j'_\Delta}$ некоторым количеством знаков i'. Из (19) и (20) следует, что наименьшее количество нарушений знака i', при котором равенство (18) выполняется, равно двум. Аналогично из (21) и (22) следует, что наибольшее количество нарушений знака i' во взятой последовательности равно Δ. Теорема доказана.

С. Многократное шифрование при базисе $\mu > q$

Свойство 2. Многократное шифрование с использованием разных ключей некоммутативно.

Доказательство. Рассмотрим двухкратное шифрование по алгоритму **2.А** с ключами $K_1^{-1} \neq K_2^{-1}$.

Для открытого текста I докажем, что:

$$K_2^{-1,2}(K_1^{-1,1} I) \neq K_1^{-1,2}(K_2^{-1,1} I). \qquad (23)$$

Различие в действиях ключей проявляется в пункте 3 алгоритма.

Шифрование в обоих случаях начинается с одинаковых значений (x_l^0) и j'_0. Из алгоритма в общем случае получим:

$$u_{11}^1 \neq u_{12}^1,\ y_{l1}^{12} \neq y_{l2}^{12},\ v_{11}^2 \neq v_{12}^2,\ u_{11}^2 \neq u_{12}^2 \Rightarrow$$
$$\Rightarrow\ K_2^{-1,2}(K_1^{-1,1} i_1) \neq K_1^{-1,2}(K_2^{-1,1} i_1),\ x_{l1}^{12} \neq x_{l2}^{12},$$

где второй нижний индекс у знаков означает номер комбинации ключей.

Аналогичные результаты получим и для знака i_2 при значениях: $(x_{l1}^{12}, j_{11}'^2) \neq (x_{l2}^{12}, j_{12}'^2)$. Для некоторых знаков i_t возможно выполнение равенства $K_2^{-1,2}(K_1^{-1,1} i_t) \neq K_1^{-1,2}(K_2^{-1,1} i_t)$, но для всего текста I выполняется неравенство (23), следовательно свойство 2 доказано.

Пример 1. Система $[q, \mu, m, k] = [2, 10, 1, 1]$, $n = m + k = 2$, ключи $K_1 = K_{21}^{11}$, $K_2 = K_{11}^{21}$, длина открытого текста I: $\Delta = 10$ знаков i_t, $t = 1, 2, ..., 10$, $l = 1, 2$.

Из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1\}$ произвольно выбираем значение начального состояния $j'_0 = 0$ системы. Из значений $x_l^0 \in \{0, q, 2q, ..., \mu - q\} = \{0, 2, 4, 6, 8\}$ произвольно образуем начальный вектор $(x_l^0) = (x_1^0, x_2^0) = (2, 8)$.

Напомним, что для каждого входного знака i_t при фиксированном t алгоритм **2.A** прогоняется по всем пунктам для каждого значения r, где r – номер шифрования.

Выполним двухкратное шифрование, $r = 1, 2$.

Из-за недостатка ширины страницы при каждом типе шифрования двумя ключами K_1 и K_2 для каждого фиксированного t последовательно используем две таблицы с номерами шифрования $r = 1$ и $r = 2$.

Таблица v Ключ $K_1 = K_{ij}^{ij} = K_{21}^{11}$						Таблица v Ключ $K_2 = K_{ij}^{ij} = K_{11}^{21}$					
i'	0		1			i'	0		1		
j'	i	j	i	j		j'	i	j	i	j	
0	0	0	0	1		0	0	1	1	0	
1	1	1	1	0		1	0	0	1	1	

Шифрование $K_2(K_1 I) = K_2^{-1,2}(K_1^{-1,1} I)$									
$r = 1$									
	i_t	y_l^{t1}		v_t^1		$i_t'^1$	$j_t'^1$	x_l^{t1}	
t	s_1^{t1}	y_1^{t1}	y_2^{t1}	ε_1^{t1}	ε_2^{t1}	$s_1'^{t1}$	$s_2'^{t1}$	x_1^{t1}	x_2^{t1}
0									
1	0	2	8	0	1	1	0	4	6
2	1	1	3	0	0	0	0	2	6
3	1	5	2	1	0	1	1	0	4
4	0	2	0	0	0	0	0	4	0
5	1	9	1	1	0	1	1	8	2

6	0	8	6	1	1	0	1	6	2
7	0	2	6	0	1	1	0	4	2
8	1	1	4	0	0	0	0	2	8
9	1	5	6	1	1	0	1	0	2
10	0	0	7	0	1	1	0	0	4

Шифрование $K_2(K_1 I) = K_2^{-1,2}(K_1^{-1,1} I)$								
$r = 2$								
	y_l^{t2}		v_t^2		$i_t'^2$	$j_t'^2$	x_l^{t2}	
t	y_1^{t2}	y_2^{t2}	ε_1^{t2}	ε_2^{t2}		$s_2'^{t2}$	x_1^{t2}	x_2^{t2}
0						0	2	8
1	5	6	1	1	1	1	0	2
2	2	6	0	1	0	0	4	2
3	1	5	0	1	0	0	2	0
4	4	0	0	0	0	1	8	0
5	9	3	1	0	1	0	8	6
6	6	3	1	0	1	0	2	6
7	5	2	1	0	1	0	0	4
8	2	8	0	1	0	0	4	6
9	0	3	0	0	0	1	0	6
10	1	4	0	0	0	1	2	8

Шифрование $K_1(K_2 I) = K_1^{-1,2}(K_2^{-1,1} I)$									
$r = 1$									
	i_t	y_l^{t1}		v_t^1		$i_t'^1$	$j_t'^1$	x_l^{t1}	
t	s_1^{t1}	y_1^{t1}	y_2^{t1}	ε_1^{t1}	ε_2^{t1}	$s_1'^{t1}$	$s_2'^{t1}$	x_1^{t1}	x_2^{t1}
0									
1	0	2	8	0	1	0	0	4	6
2	1	9	2	1	0	1	0	8	4
3	1	9	9	1	1	1	1	8	8
4	0	8	9	1	1	1	1	6	8
5	1	5	9	1	1	1	1	0	8
6	0	2	8	0	1	0	0	4	6
7	0	8	2	1	0	1	0	6	4
8	1	5	9	1	1	1	1	0	8
9	1	3	8	0	1	0	0	6	6
10	0	2	3	0	0	0	1	4	6

Шифрование $K_1(K_2 I) = K_1^{-1,2}(K_2^{-1,1} I)$								
$r = 2$								
	y_l^{t2}		v_t^2		$i_t'^2$	$j_t'^2$	x_l^{t2}	
t	y_1^{t2}	y_2^{t2}	ε_1^{t2}	ε_2^{t2}		$s_2'^{t2}$	x_1^{t2}	x_2^{t2}
0						0	2	8
1	4	6	0	1	1	0	8	2
2	9	4	1	0	1	1	8	8
3	9	9	1	1	0	1	8	8
4	7	9	1	1	0	1	4	8
5	1	9	0	1	1	0	2	8
6	4	6	0	1	1	0	8	2
7	7	4	1	0	1	1	4	8
8	1	9	0	1	1	0	2	8
9	6	6	1	1	0	1	2	2
10	4	7	0	1	1	0	8	4

Результаты двух шифрований $K_2(K_1 I)$ и $K_1(K_2 I)$, расположенные в столбцах $i_t'^2$, различны, что соответствует свойству 2.

Шифртекст шифрования $K_2(K_1 I) = K_2^{-1,2}(K_1^{-1,1} I)$ обозначим через I'^2, который расшифруем действием ключей в следующем порядке $K_1(K_2 I'^2) = K_1^1(K_2^2 I'^2)$, где верхние индексы обозначают номер выполненного шифрования. Как всегда расшифрование начинаем с конца шифртекста I'^2, см. алгоритм чтения **2.А**. Здесь также, как и при шифровании, из-за недостатка ширины страницы при каждом типе расшифрования двумя ключами K_1 и K_2 для каждого фиксированного t последовательно используем две таблицы с номерами шифрования $r = 2$ и $r = 1$. При этом необходимо при $r = 2$ использовать x_l^{t2}, записанный в таблице $r = 1$, а при $r = 1$ использовать x_l^{t1}, записанный в таблице $r = 2$.

Таблица v Ключ $K_1 = K_{ij} = K_{21}^{11}$						Таблица v. Ключ $K_2 = K_{ij} = K_{11}^{21}$					
i'	0		1			i'	0		1		
j'	i	j	i	j		j'	i	j	i	j	
0	0	0	0	1		0	0	1	1	0	
1	1	1	1	0		1	0	0	1	1	

Расшифрование $K_1(K_2I'^2)=K_1^1(K_2^2I'^2)$									
$r=2$									
	$i_t'^2$	v_t^2		y_l^{t2}		$i_t'^1$	$j_t'^1$	x_l^{t1}	
t		ε_1^{t2}	ε_2^{t2}	y_1^{t2}	y_2^{t2}	$s_1'^{t1}$	$s_2'^{t1}$	x_1^{t1}	x_2^{t1}
0									
1	1	1	1	5	6	1	0	4	6
2	0	0	1	2	6	0	0	2	6
3	0	0	1	1	5	1	1	0	4
4	0	0	0	4	0	0	0	4	0
5	1	1	0	9	3	1	1	8	2
6	1	1	0	6	3	0	1	6	2
7	1	1	0	5	2	1	0	4	2
8	0	0	1	2	8	0	0	2	8
9	0	0	0	0	3	0	1	0	2
10	0	0	0	1	4	1	0	0	4

Расшифрование $K_1(K_2I'^2)=K_1^1(K_2^2I'^2)$								
$r=1$								
	v_t^1		y_l^{t1}		i_t	$j_t'^2$	x_l^{t2}	
t	ε_1^{t1}	ε_2^{t1}	y_1^{t1}	y_2^{t1}	s_1^{t1}	$s_2'^{t2}$	x_1^{t2}	x_2^{t2}
0						0	2	8
1	0	1	2	8	0	1	0	2
2	0	0	1	3	1	0	4	2
3	1	0	5	2	1	0	2	0
4	0	0	2	0	0	1	8	0
5	1	0	9	1	1	0	8	6
6	1	1	8	6	0	0	2	6
7	0	1	2	6	0	0	0	4
8	0	0	1	4	1	0	4	6
9	1	1	5	6	1	1	0	6
10	0	1	0	7	0	1	2	8

Результаты расшифрования – текст в столбце i_t, состояние $j_0'^2$ системы и значения x_l^{02} в строке $t=0$ таблицы $r=1$ – совпадают с соответствующими исходными данными для шифрования.

Свойство 3. Результаты многократного шифрования разными ключами или одним ключом при базисе $\mu > q$ не могут быть получены однократным шифрованием.

Доказательство. Рассмотрим многократное шифрование по алгоритму **2.A** с одним ключом. Из пунктов 1 и 5 алгоритма следует, что для каждого шага t знаки y_l^{tr} в пункте 5 $\bar{r}$ раз умножались на q и столько же раз в пункте 1 знаки $x_l^{t,r-1}$ учитывались как слагаемые для y_l^{tr}. Числа $y_l^{tr} \in \{0, 1, 2, ..., \mu - 1\}$ и при одинаковом начальном векторе (x_l^0) однократное шифрование с любым ключом в общем случае не позволяет получить те же самые значения y_l^{tr}, что при многократном шифровании. Достаточно, хотя бы, это установить для одного шага $t = 1$, что очевидно. Следовательно свойство 3 доказано.

D. Многократное шифрование при базисе $\mu = q$

В этом случае многократное шифрование также некоммутативно; доказательство то же самое, что и в пункте **5.C** (свойство 2).

1. Эквивалентные ключи I типа

При многократном шифровании по алгоритму **2.E** разными или одинаковыми ключами существует эквивалентный ключ $K_э$ такой, что выполняется равенство:

$$K_{\bar{r}}^{-1,\bar{r}} K_{\bar{r}-1}^{-1,\bar{r}-1} ... K_1^{-1,1} I = K_э^{-1} I . \qquad (24)$$

Пусть i', j' – координаты элемента $v_{j'i'}$ в таблице v для ключа $K_э$, тогда построение таблицы v для этого ключа осуществим по формулам:

$$\begin{aligned} & i' = i_t'^{\bar{r}}, \quad j' = j_t'^{\bar{r}} \\ & u = i_t'^{\bar{r}}(k <) + j_t'^{\bar{r}}, \quad v = i_t(k <) + j_{t-1}'^{\bar{r}} \end{aligned} , \qquad (25)$$

где u – номер ячейки ключа $K_э$, v – содержимое этой ячейки;

$i_t'^{\bar{r}}, j_t'^{\bar{r}}$ – результат многократного шифрования на шаге t.

Эквивалентный ключ имеет те же самые размеры, что и ключи $K_1, K_2, ..., K_{\bar{r}}$. Эквивалентный ключ будем условно обозначать в виде $K_э = K_{\bar{r}} K_{\bar{r}-1} ... K_1$, соответствующему выражению (24).

Пример 1. Система $[q, \mu, m, k] = [2, 2, 1, 1]$, $n = m + k = 2$, длина открытого текста $\Delta = 15$ знаков i_t.

Начальное состояние $j'_0 = 0$ системы произвольно выбираем из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1\}$.

Возьмем следующие ключи K_1 и K_2.

Таблица v Ключ $K_1 = K_{ij}^{ij} = K_{21}^{11}$						Таблица v Ключ $K_2 = K_{ij}^{ij} = K_{21}^{11}$					
i'	0		1			i'	0		1		
j'	i	j	i	j		j'	i	j	i	j	
0	1	0	1	1		0	0	1	0	0	
1	0	1	0	0		1	1	0	1	1	

Шифрование $K_2^{-1,2} K_1^{-1,1} I$						Шифрование $K_1^{-1,2} K_2^{-1,1} I$					
	r	1		2			r	1		2	
t	i_t	$i_t'^1$	$j_t'^1$	$i_t'^2$	$j_t'^2$	t	i_t	$i_t'^1$	$j_t'^1$	$i_t'^2$	$j_t'^2$
0					0	0					0
1	0	1	1	1	1	1	0	1	0	0	0
2	1	1	0	0	1	2	1	0	1	0	1
3	0	0	1	0	0	3	0	0	0	1	1
4	1	0	0	1	0	4	1	1	1	1	0
5	1	0	0	1	0	5	1	0	1	0	1
6	1	0	0	1	0	6	1	1	1	1	0
7	0	1	1	1	1	7	0	1	0	0	0
8	0	0	1	0	0	8	0	1	0	0	0
9	1	0	0	1	0	9	1	0	1	0	1
10	0	1	1	1	1	10	0	0	0	1	1
11	1	1	0	0	1	11	1	1	1	1	0
12	1	1	0	0	1	12	1	0	1	0	1
13	1	1	0	0	1	13	1	1	1	1	0
14	0	0	1	0	0	14	0	1	0	0	0
15	1	0	0	1	0	15	1	0	1	0	1

Верхние индексы 1 и 2 у знаков i'_t, j'_t и ключей в таблицах шифрования означают номер шифрования $r = 1, 2$.

Результаты двух типов двухкратного шифрования (столбцы $i_t'^2$) некоммутативны $K_2^{-1,2} K_1^{-1,1} I \neq K_1^{-1,2} K_2^{-1,1} I$.

Эти результаты шифрования могут быть получены при однократном шифровании по алгоритму **4.В** соответствующими эквивалентными ключами $K_э = K_2K_1$ и $K_э = K_1K_2$, построенными по формулам (25) на основе соответствующих таблиц двухкратного шифрования.

Таблица v Эквивалентный ключ $K_э = K_2K_1 = K_{ij}^{ij} = K_{11}^{12}$						Таблица v Эквивалентный ключ $K_э = K_1K_2 = K_{ij}^{ij} = K_{11}^{12}$					
i'	0		1			i'	0		1		
j'	i	j	i	j		j'	i	j	i	j	
0	0	1	1	0		0	0	0	1	1	
1	1	1	0	0		1	1	0	0	1	

Пример 2. Система $[q, \mu, m, k] = [2, 2, 1, 2]$, $n = m + k = 3$, длина открытого текста $\Delta = 15$ знаков i_t.

Начальное состояние $j'_0 = 0$ системы произвольно выбираем из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3\}$.

Возьмем следующие ключи $K_1 = K_2$.

Таблица v Ключи $K_1 = K_2 = K_{ij}^{ij} = K_{21}^{01}$				
i'	0		1	
j'	i	j	i	j
0	0	0	0	1
1	1	1	1	2
2	0	2	0	3
3	1	3	1	0

Шифрование $K_2^{-1,2}K_1^{-1,1}I$					
	r	1		2	
t	i_t	$i_t'^1$	$j_t'^1$	$i_t'^2$	$j_t'^2$
0					0
1	0	0	0	0	0
2	1	1	3	0	3
3	1	0	3	1	2

4	1	1	1	0	1
5	0	1	0	1	3
6	0	1	2	1	1
7	1	0	1	1	0
8	0	0	0	0	0
9	1	1	3	0	3
10	1	0	3	1	2
11	0	0	2	0	2
12	1	1	1	0	1
13	0	1	0	1	3
14	1	0	3	1	2
15	1	1	1	0	1

На основе этой таблицы шифрования по формулам (25) строим эквивалентный ключ $K_э = K_2 K_1$.

Таблица v

Эквивалентный ключ

$K_э = K_2 K_1 = K_{ij}^{ij} = K_{11}^{00}$

i'	0		1	
j'	i	j	i	j
0	0	0	1	1
1	1	2	0	3
2	0	2	1	3
3	1	0	0	1

Пример 3. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, $n = m + k = 4$, длина открытого текста $\Delta = 25$ знаков i_t.

Начальное состояние $j'_0 = 0$ системы произвольно выбираем из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3\}$.

Возьмем следующие ключи $K_1 = K_2$.

Таблица v

Ключи $K_1 = K_2 = K_{ij}^{ij} = K_{01}^{11}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	0	0	2	1	0	2	2	3
1	1	1	3	2	1	3	3	0
2	2	2	0	3	2	0	0	1
3	3	3	1	0	3	1	1	2

Шифрование $K_2^{-1,2}K_1^{-1,1}I$					
	r	1		2	
t	i_t	$i_t'^1$	$j_t'^1$	$i_t'^2$	$j_t'^2$
0					0
1	2	2	2	0	2
2	1	3	3	0	3
3	0	1	2	3	3
4	3	0	3	1	2
5	2	0	2	2	0
6	1	1	3	2	1
7	1	0	1	3	2
8	3	1	1	0	1
9	3	2	3	3	0
10	2	2	2	0	2
11	0	2	0	2	2
12	1	3	3	0	3
13	1	2	1	1	0
14	0	0	0	0	0
15	3	3	1	2	3
16	2	3	0	3	1
17	1	0	1	3	2
18	1	3	3	0	3
19	1	2	1	1	0
20	1	1	3	2	1
21	1	0	1	3	2
22	1	3	3	0	3
23	2	3	0	3	1
24	0	3	2	1	1
25	2	1	0	1	3

На основе этой таблицы шифрования по формулам (25) строим эквивалентный ключ $K_э = K_2K_1$.

Таблица v

Эквивалентный ключ $K_э = K_2K_1 = K_{ij}^{ij} = K_{11}^{10}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	0	0	1	3	2	2	3	1
1	3	2	0	1	1	0	2	3
2	2	0	3	3	0	2	1	1
3	1	2	2	1	3	0	0	3

Пример 4. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, $n = m + k = 4$, длина открытого текста $\Delta = 20$ знаков i_t.

Начальное состояние $j'_0 = 2$ системы произвольно выбираем из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3\}$.

Возьмем три разных ключа K_1, K_2, K_3.

Таблица v

Ключ $K_1 = K_{ij}^{ij} = K_{01}^{11}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	0	0	2	1	0	2	2	3
1	1	1	3	2	1	3	3	0
2	2	2	0	3	2	0	0	1
3	3	3	1	0	3	1	1	2

Таблица v

Ключ $K_2 = K_{ij}^{ij} = K_{00}^{11}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	1	1	3	2	3	1	0	1
1	3	3	1	0	2	0	1	2
2	0	0	0	3	1	3	3	0
3	2	2	2	1	0	2	2	3

Таблица v

Ключ $K_3 = K_{ij}^{ij} = K_{00}^{11}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	3	3	3	2	2	0	0	1
1	0	0	2	1	0	2	2	3
2	2	2	1	0	1	3	1	2
3	1	1	0	3	3	1	3	0

Шифрование $K_3^{-1,3}K_2^{-1,2}K_1^{-1,1}I$							
	r	1		2		3	
t	i_t	$i_t'^1$	$j_t'^1$	$i_t'^2$	$j_t'^2$	$i_t'^3$	$j_t'^3$
0							2
1	3	1	1	0	0	0	1
2	0	3	2	1	0	1	2
3	1	3	3	0	1	3	0
4	2	2	2	0	3	1	3
5	2	3	0	3	2	1	0
6	3	3	1	2	0	2	0
7	1	1	3	2	2	0	2
8	1	3	3	0	1	3	0
9	0	0	0	0	2	2	1
10	2	1	0	1	1	0	3
11	3	0	3	1	2	3	2
12	2	0	2	2	3	3	1
13	3	2	3	3	3	0	0
14	1	1	3	2	2	0	2
15	0	2	0	2	1	1	1
16	1	0	1	3	0	3	3
17	1	2	1	1	3	2	2
18	1	3	3	0	1	3	0
19	2	2	2	0	3	1	3
20	0	1	2	3	1	2	3

На основе этой таблицы шифрования по формулам (25) строим эквивалентный ключ $K_э = K_3K_2K_1$.

Таблица v

Эквивалентный ключ

$$K_э = K_3K_2K_1 = K_{ij}^{ij} = K_{00}^{00}$$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	3	1	2	3	3	0	1	2
1	3	2	0	2	0	0	2	2
2	1	0	0	1	1	3	3	3
3	2	1	2	0	0	3	1	1

2. Эквивалентные ключи II типа

При многократном шифровании по алгоритму **2.F** разными или одинаковыми ключами существует эквивалентный ключ $K_э$, для которого выполняется равенство (24). Эквивалентный ключ имеет:

1) значение m то же самое, что и у ключей шифрования;

2) состояние системы на шаге t равно $j'_t = j'^1_t j'^2_t ... j'^{\bar{r}}_t$, $t = 0, 1, 2, ..., \Delta$, j'^r_t записываем в q-алфавите, $r = 1, 2, ..., \bar{r}$;

3) $i'_t = i'^{\bar{r}}_t$. Из пункта 2) следует значение $k = \sum_{r=1}^{\bar{r}} k_r$.

Таблица v для эквивалентного ключа строится по формулам:

$$\begin{aligned} &i' = i'^{\bar{r}}_t, \quad j' = j'_t = j'^1_t j'^2_t ... j'^{\bar{r}}_t \\ &u = i'^{\bar{r}}_t (k <) + j'_t, \quad v = i_t (k <) + j'_{t-1} \end{aligned}, \qquad (26)$$

где i', j' – координаты элемента $v_{j'i'}$ в таблице v, u – номер ячейки ключа $K_э$, v – содержимое этой ячейки, состояния j'^r_t в выражении для j'_t сдвинуты на соответствующее количество разрядов влево, т.е. выражение j'_t не является произведением j'^r_t ($r = 1, 2, ..., \bar{r}$).

Пример 1. Система $[q, \mu, m, k] = [2, 2, 1, k_r]$, $n_r = m + k_r$, длина открытого текста $\Delta = 43$ знака i_t, $r = 1, 2, 3$.

Ключи шифрования $K_ξ^{-1r}$ имеют одинаковые значения m и могут иметь разные значения $k = k_r$, $m + k_r = n_r$.

Возьмем три разных ключа K_1, K_2, K_3, для которых: $m = 1, k_1 = 1, k_2 = 2, k_3 = 1$.

Начальные состояния j'^r_0 выбираем произвольно из множеств $\{0, 1, 2, ..., q^{k_r} - 1\} : \{0, 1\}, \{0, 1, 2, 3\}, \{0, 1\}$ соответственно для $k_1 = 1, k_2 = 2, k_3 = 1$: $j'^1_0 = 0, j'^2_0 = 3, j'^3_0 = 1$.

Таблицы v и таблицы ключей K_1, K_2, K_3

$m=1,\ k_1=1$ $K_1=K_{ij}^{ij}=K_{21}^{11}$					$m=1,\ k_2=2$ $K_2=K_{ij}^{ij}=K_{21}^{01}$					$m=1,\ k_3=1$ $K_3=K_{ij}^{ij}=K_{21}^{11}$				
i'	0		1		i'	0		1		i'	0		1	
j'	i	j	i	j	j'	i	j	i	j	j'	i	j	i	j
0	1	0	1	1	0	1	0	1	1	0	1	1	1	0
1	0	1	0	0	1	0	1	0	2	1	0	0	0	1
					2	1	2	1	3					
					3	0	3	0	0					

Связь между системами счисления								
$q=2$	0000	0001	0010	0011	0100	0101	0110	0111
$q=10$	0	1	2	3	4	5	6	7
$q=2$	1000	1001	1010	1011	1100	1101	1110	1111
$q=10$	8	9	10	11	12	13	14	15

Шифрование $K_3^{-1,3}K_2^{-1,2}K_1^{-1,1}I$									
	r	1		2		3		$K_{\text{ý}}$	
t	i_t	$i_t'^1$	$j_t'^1$	$i_t'^2$	$j_t'^2$	$i_t'^3$	$j_t'^3$	i_t'	j_t'
0			0		3		1		7
1	1	0	0	0	3	1	1	1	7
2	0	1	1	1	2	0	0	0	12
3	1	1	0	0	2	0	1	0	5
4	1	0	0	1	1	0	0	0	2
5	0	1	1	1	0	1	0	1	8
6	0	0	1	1	3	1	0	1	14
7	0	0	1	0	3	0	1	0	15
8	1	1	0	1	2	0	0	0	4
9	0	1	1	0	2	0	1	0	13
10	1	1	0	0	2	1	1	1	5
11	0	1	1	0	2	1	1	1	13
12	0	0	1	1	1	0	0	0	10
13	1	1	0	1	0	1	0	1	0
14	0	1	1	0	0	0	1	0	9
15	1	1	0	0	0	1	1	1	1
16	1	0	0	1	3	0	0	0	6
17	1	0	0	0	3	0	1	0	7

18	0	1	1	1	2	0	0	0	12
19	0	0	1	1	1	1	0	1	10
20	0	0	1	0	1	0	1	0	11
21	1	1	0	1	0	0	0	0	0
22	1	0	0	1	3	1	0	1	6
23	0	1	1	1	2	1	0	1	12
24	1	1	0	0	2	0	1	0	5
25	1	0	0	1	1	0	0	0	2
26	1	0	0	0	1	0	1	0	3
27	0	1	1	1	0	0	0	0	8
28	1	1	0	0	0	0	1	0	1
29	0	1	1	0	0	1	1	1	9
30	0	0	1	1	3	0	0	0	14
31	1	1	0	1	2	1	0	1	4
32	1	0	0	1	1	1	0	1	2
33	1	0	0	0	1	0	1	0	3
34	1	0	0	0	1	1	1	1	3
35	0	1	1	1	0	0	0	0	8
36	0	0	1	1	3	1	0	1	14
37	0	0	1	0	3	0	1	0	15
38	0	0	1	0	3	1	1	1	15
39	1	1	0	1	2	0	0	0	4
40	0	1	1	0	2	0	1	0	13
41	0	0	1	1	1	0	0	0	10
42	0	0	1	0	1	0	1	0	11
43	0	0	1	0	1	1	1	1	11

На основе этой таблицы шифрования по формулам (26) строим эквивалентный ключ $K_э = K_3K_2K_1$, $k = k_1 + k_2 + k_3$, $k = 1 + 2 + 1 = 4$, $n = m + k = 1 + 4 = 5$. В последних двух столбцах этой таблицы приведены результаты однократного шифрования эквивалентным ключом $K_э$. Шифртекст $i_t'^3$ при $r = 3$ для трехкратного шифрования совпадает с шифртекстом i_t' при шифровании эквивалентным ключом $K_э$.

Таблица v

Эквивалентный ключ

$K_э = K_3K_2K_1 = K_{ij}^{ij} = K_{21}^{01}$

i'	0		1	
j'	i	j	i	j
0	1	11	1	10
1	1	8	1	9

2	1	5	1	4
3	1	2	1	3
4	1	15	1	14
5	1	12	1	13
6	1	1	1	0
7	1	6	1	7
8	0	3	0	2
9	0	0	0	1
10	0	13	0	12
11	0	10	0	11
12	0	7	0	6
13	0	4	0	5
14	0	9	0	8
15	0	14	0	15

E. Замкнутые циклы состояний системы

Замкнутые циклы состояний j'_t возможны только в системах с базисом $\mu = q$. После шифрования каждого знака i_t меняется состояние j'_t системы и в зависимости от структуры ключа $K = K_{ij}^{ij}$ некоторое множество $\{j'_t\}$ состояний системы может оказаться ограниченным по сравнению с их полным количеством, равным q^k. Ограниченное множество состояний, возникающих в системе, будем называть циклом состояний системы. В системе может существовать несколько различных независимых друг от друга циклов. Если количество состояний системы равно Γ, то при шифровании используется только $q^m\Gamma$ элементов таблицы v (ключа), поскольку для каждого состояния j'_t системы знак i_t может принимать одно из q^m своих значений.

Цикл из Γ состояний системы существует, если на строках $\{j'_1, j'_2, ..., j'_\Gamma\}$ таблицы v множество знаков $\{j_1, j_2, ..., j_\Gamma\}$, входящих в состав элементов $v_{j'i'}$ этой таблицы, совпадает с множеством знаков $\{j'_1, j'_2, ..., j'_\Gamma\}$; каждый знак из множества $\{j_1, j_2, ..., j_\Gamma\}$ на этих строках повторяется q^m раз. При этом на каждой строке $j'_g \in \{j'_1, j'_2, ..., j'_\Gamma\}$ должен находиться хотя бы

один знак $j \neq j'_g$. Знаки $\{j_1, j_2, ..., j_\Gamma\}$ на строках $\{j'_1, j'_2, ..., j'_\Gamma\}$ должны быть расположены так, чтобы при записи произвольной информации i_t система проходила через все Γ состояний цикла. Если на какой-либо строке j'_g все q^m знаков $j = j'_g$, то система имеет цикл с одним состоянием j'_g.

Существование циклов состояний $J' = \{j'\}$ системы уменьшает количество используемых элементов $v_{j'i'}$ ключа и поэтому улучшает криптоанализ системы. Выход из цикла состоит в модификации знаков j'_t. Последовательность обхода состояний в цикле может быть заданной по определенному закону (синхронные системы) или свободной, зависящей от входной информации i_t. Время возврата системы в начальное состояние в последнем случае определяется входной информацией i_t и структурой ключа. Количество всевозможных циклов с нужными свойствами определяется структурой ключа. В системе с несколькими циклами возможен переход с одного цикла на другой, если в каждом из этих циклов будет находиться несколько элементов $v_{j'i'}$ других циклов; такие циклы назовем квазизамкнутыми циклами. Управление переходами на разные циклы может осуществляться знаками i входной информации, состояниями j' циклов и их совместным действием. Использование таких систем возможно окажется полезным в кибернетике и системах искусственного интеллекта.

Пример 1. Система $[q, \mu, m, k] = [2, 2, 2, 3]$, $n = m + k = 5$, K_{00}^{00}.

Таблица v

Ключ $K = K_{ij}^{ij} = K_{00}^{00}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	3	4	0	3	2	0	1	6
1	**0**	**2**	**0**	**1**	**0**	**5**	**2**	**1**
2	**2**	**5**	**1**	**5**	**1**	**1**	**3**	**2**
3	0	0	3	7	3	3	1	4
4	1	3	1	0	1	7	0	6
5	**3**	**5**	**1**	**2**	**2**	**2**	**3**	**1**

6	0	4	2	7	3	6	2	3
7	2	6	2	4	0	7	3	0

В этой системе существует два цикла: $J'_1 = \{1, 2, 5\}$ – выделен жирным шрифтом, $J'_2 = \{0, 3, 4, 6, 7\}$. Режим работы системы в заданном цикле определяется начальным состоянием j'_0, принадлежащим этому циклу.

Примеры 2, 3, 4. Система $[q, \mu, m, k] = [2, 2, 2, 4]$, $n = m + k = 6$, K_{00}^{00}.

Таблицы v и ключей $K = K_{ij}^{ij} = K_{00}^{00}$

	Пример 2								Пример 3								Пример 4							
i'	0		1		2		3		0		1		2		3		0		1		2		3	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	0	1	3	12	1	5	2	9	0	1	3	12	1	5	2	9	0	1	3	12	1	5	2	9
1	1	14	0	15	3	0	0	13	1	14	0	15	3	0	0	13	1	14	0	15	3	0	0	13
2	**1**	**3**	**1**	**2**	**0**	**6**	**3**	**8**	**3**	**8**	**1**	**2**	**0**	**6**	**3**	**2**	**1**	**3**	**2**	**10**	**0**	**6**	**3**	**2**
3	**2**	**6**	**0**	**3**	**2**	**2**	**3**	**10**	**0**	**8**	**2**	**8**	**1**	**8**	**3**	**6**	**2**	**6**	**0**	**3**	**2**	**2**	**3**	**3**
4	1	13	1	1	1	9	3	7	1	13	1	1	1	9	3	7	1	13	1	1	1	9	3	7
5	3	4	3	14	0	5	1	12	3	4	3	14	0	5	1	12	3	4	3	14	0	5	1	12
6	**0**	**2**	**1**	**6**	**2**	**3**	**3**	**11**	**2**	**6**	**2**	**2**	**0**	**2**	**1**	**6**	**0**	**2**	**1**	**6**	**2**	**3**	**3**	**6**
7	0	7	2	0	2	1	2	4	0	7	2	0	2	1	2	4	0	7	2	0	2	1	2	4
8	**2**	**8**	**0**	**10**	**1**	**11**	**3**	**2**	**2**	**3**	**0**	**3**	**1**	**3**	**0**	**10**	**2**	**8**	**0**	**10**	**1**	**11**	**3**	**8**
9	2	5	0	9	0	4	0	14	2	5	0	9	0	4	0	14	2	5	0	9	0	4	0	14
10	**1**	**10**	**0**	**8**	**2**	**11**	**3**	**3**	**1**	**11**	**1**	**10**	**2**	**11**	**3**	**3**	**1**	**10**	**0**	**8**	**2**	**11**	**3**	**10**
11	**0**	**11**	**2**	**10**	**1**	**8**	**3**	**6**	**0**	**11**	**2**	**10**	**3**	**10**	**3**	**11**	**0**	**11**	**1**	**2**	**1**	**8**	**3**	**11**
12	0	0	1	15	2	13	3	1	0	0	1	15	2	13	3	1	0	0	1	15	2	13	3	1
13	3	13	2	12	2	7	2	15	3	13	2	12	2	7	2	15	3	13	2	12	2	7	2	15
14	3	9	1	7	3	15	3	5	3	9	1	7	3	15	3	5	3	9	1	7	3	15	3	5
15	0	12	1	4	2	14	1	0	0	12	1	4	2	14	1	0	0	12	1	4	2	14	1	0

В каждом примере 2, 3, 4 система имеет три цикла:

$J'_1 = \{2, 3, 6\}$ – выделен жирным шрифтом;

$J'_2 = \{8, 10, 11\}$ – выделен более крупным жирным шрифтом;

$J'_3 = \{0, 1, 4, 5, 7, 9, 12, 13, 14, 15\}$.

В системе (пример2) управляющим сигналом $i = 3$ входной информации можно переходить с цикла J'_1 на цикл J'_2 и наоборот.

В системе (пример3) переходы между циклами J'_1 и J'_2 осуществляются состояниями $j' = 3$ и $j' = 8$ этих циклов.

В системе (пример4) переходы между циклами J'_1 и J'_2 осуществляются элементами таблицы v: $v = 1|2$ и $v = 2|10$ этих циклов.

Переход с J'_1 на J'_2: в цикле J'_1 входная информация $i = 1$, состояние $j' = 2$.

Переход с J'_2 на J'_1: в цикле J'_2 входная информация $i = 2$, состояние $j' = 10$.

Во всех трех примерах 2, 3, 4 объединение циклов J'_1 и J'_2 образует замкнутый цикл.

F. Спектральные системы

Рассмотрим системы с базисом $\mu = q = 2$, в шифртекстах которых при первом очередном появлении состояния $j'_t = j'_{t+h} \neq j'_{t+h-1}$ на отрезке шагов $[t+1, t+h]$, количество знаков i'_t или их сумма принимают дискретные значения.

1. Квазисинхронная система: m, k – любые; знаки i в таблице v распределены произвольно в соответствии с правилами ее построения; в столбцах $i' = 0,1,2,...,\overline{m}$, $\overline{m} \in \{0,1,2,...,2^m - 2\}$, знаки $j = j'$; в столбцах $i' = \overline{m}+1, \overline{m}+2,..., 2^m - 1$ на каждой строке j' знаки j одинаковы и $j \neq j'$.

Система имеет ключ типа $K_{i\overline{2}}^{i1}$, где индекс $\overline{2}$ означает, что на каждой строке j' знаки j одинаковы для двух групп столбцов i'.

При шифровании произвольного текста по алгоритму **2.E** система обладает следующими свойствами:

1) для каждого состояния j'_t последовательности $J' = j'_0, j'_1,..., j'_\Delta$

знак $i'_t \in \begin{cases} \{\overline{m}+1, \overline{m}+2,..., 2^m - 1\}, & j'_t \neq j'_{t-1} \\ \{0, 1, 2,..., \overline{m}\}, & j'_t = j'_{t-1} \end{cases}$;

2) очередное появление состояния $j'_t = j'_{t+h} \neq j'_{t+h-1}$ произойдет, если количество знаков $i'_t \in \{\overline{m}+1, \overline{m}+2,..., 2^m - 1\}$ на отрезке шагов $[t+1, t+h]$ окажется равным $2^k\theta$, где $\theta = 1, 2, 3,...$ – целое положительное число;

3) переход $j'_t \to j'_{t+1} \neq j'_t$ определяется рекуррентным соотношением $j'_{t+1} = j'\big|_{j=j'_t}$, где j' – номер строки таблицы v, на которой расположен знак $j = j'_t$ столбцов $i' = \overline{m}+1, \overline{m}+2,..., 2^m - 1$;

4) количество знаков $i'_t \in \{\overline{m}+1, \overline{m}+2,..., 2^m - 1\}$ от состояния j'_t до состояния $j'_{t-h} \neq j'_{t-h+1}$ определяется выражением

$$N_{j'_t\, j'_{t-h}} = a + 2^k\theta, \quad \theta = 0, 1, 2,..., [(h-a)/2^k],$$

где a – количество переходов по пункту 3) от состояния j'_{t-h} до первого появления состояния j'_t и равное количеству знаков $i'_t \in \{\overline{m}+1, \overline{m}+2,..., 2^m - 1\}$ по $\bmod 2^k$ на отрезке шагов $[t-h+1, t]$; $[(h-a)/2^k]$ – целая часть.

Последовательность $L_{j'_0}$ 2^k состояний j' системы, определяемая переходами от состояния j'_0 по пункту 3), повторяется в последовательности $J' = j'_0, j'_1, j'_2,..., j'_\Delta$ с периодом $T = 2^k$, если следующие друг за другом одинаковые состояния j' принимать за одно состояние. Последовательность $L_{j'_0}$ совместно с последовательностью номеров расположения состояний j' в ней назовем спектром системы $C_{j'_0}$.

Полагая в пункте 4): $j'_{t-h} = j'_0$, $a = a_N$ – номер расположения состояния j'_t в последовательности $L_{j'_0}$, спектр системы запишем в виде $C_{j'_0} = \begin{matrix} L_{j'_0} & j'_0 & j'_1 & j'_2 & \cdots & j'_{2^k-1} \\ a_N & 0 & 1 & 2 & \cdots & 2^k-1 \end{matrix}$;

обратный спектр $C_{j'_0}^{-1} = \begin{matrix} L_{j'_0} & 0 & 1 & 2 & \cdots & 2^k-1 \\ a_N & a_0 & a_1 & a_2 & \cdots & a_{2^k-1} \end{matrix}$.

Пример 1. Система $[q, \mu, m, k] = [2, 2, 1, 3]$, $n = m + k = 4$, K_{01}^{01}, $\overline{m} = 0$, длина открытого текста $\Delta = 30$ знаков i_t.

Начальное состояние $j'_0 = 0$ системы произвольно выбираем из множества $\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Символы i, i' – однозначные, j, j' – трехзначные.

Таблица v

Ключ $K_{ij}^{ij} = K_{01}^{01}$

i'	0		1	
j'	i	j	i	j
0	0	0	1	3
1	1	1	0	4
2	0	2	1	5
3	0	3	1	2
4	1	4	1	7
5	0	5	1	6
6	0	6	0	1
7	0	7	1	0

Связь между системами счисления

$q=2$	000	001	010	011	100	101	110	111
$q=10$	0	1	2	3	4	5	6	7

Шифрование

t	i_t	i'_t	j'_t		t	i_t	i'_t	j'_t
0			0		16	0	1	1
1	1	1	7		17	1	0	1
2	0	0	7		18	0	1	6
3	1	1	4		19	0	0	6
4	1	0	4		20	1	1	5
5	0	1	1		21	1	1	2
6	0	1	6		22	0	0	2
7	1	1	5		23	1	1	3
8	0	0	5		24	1	1	0
9	1	1	2		25	0	0	0

10	1	1	3		26	1	1	7
11	0	0	3		27	1	1	4
12	1	1	0		28	0	1	1
13	1	1	7		29	0	1	6
14	0	0	7		30	1	1	5
15	1	1	4					

Легко проверить по этой таблице, что свойство 2) выполняется. Пусть, например, $j'_t = j'_1 = 7$, $t = 1$; первое очередное появление этого состояния произойдет при $t = 13$: $j'_{t+h} = j'_{13} = 7$, при этом $j'_{t+h} \neq j'_{t+h-1}$, на отрезке шагов $[t+1, t+h] = [2, 13]$, на котором количество знаков $i'_t = i'_1 = 1 \in \{\overline{m}+1, ..., 2^m - 1\} = \{1\}$ равно $2^k \theta = 2^3 \cdot 1 = 8$, где $\theta = 1, 2, 3, ...$ – целое положительное число. Такое свойство выполняется в соответствии с пунктом 2) для любого состояния j'_t данной таблицы шифрования.

Состояния системы, расположенные в столбце j'_t этой таблицы, повторяются с периодом $T = 2^k = 2^3 = 8$, если идущие подряд одинаковые состояния j'_t считать за одно.

Таблица спектров $C_{j'_0}$								
a_N	0	1	2	3	4	5	6	7
$j'_0 \setminus L_{j'_0}$	j'_0	j'_1	j'_2	j'_3	j'_4	j'_5	j'_6	j'_7
0	0	7	4	1	6	5	2	3
1	1	6	5	2	3	0	7	4
2	2	3	0	7	4	1	6	5
3	3	0	7	4	1	6	5	2
4	4	1	6	5	2	3	0	7
5	5	2	3	0	7	4	1	6
6	6	5	2	3	0	7	4	1
7	7	4	1	6	5	2	3	0

Как видно из этой таблицы спектров все спектры $C_{j'_0}$ для $j'_0 \neq 0$ получаются циклическим сдвигом влево на $a_{Nj'}$ позиций последовательности $L_{j'_0}$ в спектре $C_{j'_0}$ для $j'_0 = 0$, где $a_{Nj'}$ – значение a_N для j', взятого в качестве нового j'_0 , в спектре C_0. Поэтому достаточно иметь спектр $C_0 = C_{j'_0}$ для $j'_0 = 0$.

Спектр C_0								
$L_{j'_0}$	0	7	4	1	6	5	2	3
a_N	0	1	2	3	4	5	6	7

Пример 2. Система $[q, \mu, m, k] = [2, 2, 3, 4]$, $n = m + k = 7$, $K_{0\bar{2}}^{01}$, $\overline{m} = 2$, длина открытого текста $\Delta = 40$ знаков i_t. Начальное состояние $j'_0 = 0$ системы произвольно выбираем из множества $\{0,1,2,...,q^k - 1\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$

.

Символы i, i' – трехзначные, j, j' – четырехзначные.

Таблица v

Ключ $K_{ij}^{ij} = K_{0\bar{2}}^{01}$

i'	0		1		2		3		4		5		6		7	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	5	0	1	0	2	0	5	11	0	11	3	11	7	11	1	11
1	2	1	1	1	7	1	2	4	3	4	0	4	4	4	1	4
2	6	2	3	2	0	2	3	5	4	5	5	5	6	5	7	5
3	0	3	6	3	3	3	2	9	6	9	1	9	4	9	3	9
4	5	4	7	4	6	4	1	8	6	8	0	8	3	8	4	8
5	2	5	0	5	1	5	1	14	6	14	5	14	0	14	3	14
6	7	6	6	6	5	6	0	0	3	0	4	0	6	0	7	0
7	2	7	1	7	0	7	7	2	4	2	1	2	5	2	2	2
8	7	8	2	8	5	8	4	13	1	13	3	13	2	13	0	13
9	5	9	7	9	0	9	4	6	3	6	2	6	1	6	0	6
10	4	10	5	10	2	10	5	3	7	3	1	3	4	3	2	3
11	2	11	6	11	4	11	6	1	0	1	4	1	3	1	5	1
12	0	12	3	12	5	12	5	7	6	7	7	7	4	7	3	7
13	7	13	6	13	5	13	7	15	1	15	5	15	2	15	4	15
14	2	14	7	14	4	14	7	10	0	10	6	10	3	10	1	10
15	3	15	0	15	6	15	4	12	1	12	6	12	2	12	7	12

Из этой таблицы видно, что состояния j на каждой строке j' имеют одни одинаковые значения $j = j'$ для столбцов $i' = 0, 1, 2,..., \overline{m} = 0, 1, 2$ и другие одинаковые значения $j \neq j'$ для столбцов $i' = \overline{m} + 1, \overline{m} + 2,..., 2^m - 1 = 3, 4, 5, 6, 7$.

Связь между системами счисления								
$q=2$	0000	0001	0010	0011	0100	0101	0110	0111
$q=10$	0	1	2	3	4	5	6	7
$q=2$	1000	1001	1010	1011	1100	1101	1110	1111
$q=10$	8	9	10	11	12	13	14	15

Шифрование								
t	i_t	i'_t	j'_t		t	i_t	i'_t	j'_t
0			0		21	1	1	1
1	6	6	6		22	4	5	11
2	0	7	9		23	5	3	0
3	1	5	3		24	7	7	6
4	5	3	10		25	2	5	9
5	3	6	14		26	6	4	3
6	7	1	14		27	2	7	10
7	4	2	14		28	3	6	14
8	2	0	14		29	1	3	5
9	5	5	5		30	6	6	2
10	0	1	5		31	5	6	7
11	1	2	5		32	7	5	12
12	3	3	2		33	2	6	15
13	3	1	2		34	5	5	13
14	7	3	7		35	0	7	8
15	4	6	12		36	3	6	4
16	1	4	15		37	1	7	1
17	7	3	13		38	6	3	11
18	3	5	8		39	1	7	0
19	3	6	4		40	0	3	6
20	2	3	1					

Состояния системы, расположенные в столбце j'_t этой таблицы, повторяются с периодом $T=2^k=2^4=16$, если идущие подряд одинаковые состояния j'_t считать за одно.

Спектр C_0																
$L_{j'_0}$	0	6	9	3	10	14	5	2	7	12	15	13	8	4	1	11
a_N	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Пример 3. Система $[q,\mu,m,k]=[2,2,4,3]$, $n=m+k=7$, $K_{0\bar{2}}^{01}$, $\overline{m}=5$, длина открытого текста $\Delta=30$ знаков i_t. Начальное

состояние $j'_0 = 0$ системы произвольно выбираем из множества $\{0,1,2,...,q^k - 1\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Символы i, i' – четырехзначные, j, j' – трехзначные.

Таблица v

Ключ $K_{ij}^{ij} = K_{0\overline{2}}^{01}$

i'	0		1		2		3		4		5		6		7	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	12	0	7	0	1	0	0	0	6	0	4	0	14	4	8	4
1	4	1	13	1	11	1	8	1	1	1	5	1	7	3	8	3
2	0	2	9	2	12	2	2	2	5	2	1	2	15	7	9	7
3	5	3	12	3	14	3	13	3	4	3	1	3	13	2	4	2
4	6	4	10	4	7	4	1	4	4	4	0	4	15	6	5	6
5	12	5	13	5	9	5	11	5	8	5	14	5	9	0	14	0
6	8	6	0	6	12	6	7	6	4	6	1	6	15	1	3	1
7	4	7	5	7	6	7	13	7	0	7	1	7	2	5	6	5

Продолжение таблицы v

i'	8		9		10		11		12		13		14		15	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	15	4	2	4	9	4	5	4	13	4	11	4	3	4	12	4
1	10	3	2	3	15	3	9	3	11	3	3	3	6	3	0	3
2	14	7	8	7	12	7	2	7	3	7	10	7	7	7	11	7
3	15	2	3	2	7	2	10	2	6	2	14	2	8	2	11	2
4	14	6	10	6	6	6	3	6	13	6	9	6	2	6	11	6
5	5	0	10	0	2	0	13	0	15	0	11	0	3	0	8	0
6	7	1	12	1	10	1	0	1	14	1	9	1	6	1	2	1
7	7	5	3	5	0	5	10	5	4	5	15	5	5	5	1	5

Из этой таблицы видно, что состояния j на каждой строке j' имеют одинаковые значения $j = j'$ для столбцов $i' = 0, 1, 2,..., \overline{m} = 0, 1, 2, 3, 4, 5$ и одинаковые значения $j \neq j'$ для столбцов $i' = \overline{m} + 1, \overline{m} + 2,..., 2^m - 1 = 6, 7, 8, 9, 10, 11, 12, 13, 14, 15$.

Связь между системами счисления								
$q = 2$	0000	0001	0010	0011	0100	0101	0110	0111
$q = 10$	0	1	2	3	4	5	6	7
$q = 2$	1000	1001	1010	1011	1100	1101	1110	1111
$q = 10$	8	9	10	11	12	13	14	15

Шифрование								
t	i_t	i'_t	j'_t		t	i_t	i'_t	j'_t
0			0		16	0	4	7
1	12	0	0		17	11	15	2
2	2	10	5		18	8	14	3
3	0	10	7		19	2	9	1
4	3	12	2		20	5	5	1
5	14	13	3		21	7	8	6
6	7	6	1		22	12	2	6
7	1	4	1		23	10	9	4
8	8	3	1		24	4	4	4
9	15	6	6		25	9	10	0
10	2	14	4		26	13	11	5
11	3	14	0		27	0	10	7
12	3	14	5		28	15	6	2
13	9	2	5		29	11	15	3
14	6	7	7		30	7	6	1
15	13	3	7					

Состояния системы, расположенные в столбце j'_t этой таблицы, повторяются с периодом $T = 2^k = 2^3 = 8$, если идущие подряд одинаковые состояния j'_t считать за одно.

Спектр C_0								
$L_{j'_0}$	0	5	7	2	3	1	6	4
a_N	0	1	2	3	4	5	6	7

2. Система: $m \le k$, K_{i1}^{i1}, знаки i в таблице v распределены произвольно в соответствии с правилами ее построения; в столбце $i' = 0$ на строке j' знак $j = j'$; в столбце i' знаки j смещены циклически вверх относительно знаков j столбца $(i'-1)$ на $\Delta j = (j_{i'} - j_{i'-1}) \bmod 2^k$, где $j_{i'}$, $j_{i'-1}$ расположены на одной строке j', $i' = 1, 2, ..., 2^m - 1$, $\Delta j = 1, 3, 5, ..., 2^k - 1$ принимает только нечетные значения.

Система обладает следующими свойствами:

1) для каждого состояния j'_t последовательности $J' = j'_0, j'_1, ..., j'_\Delta$

$$\text{знак } i'_t \in \begin{cases} \{1, 2, ..., 2^m - 1\}, & j'_t \neq j'_{t-1} \\ 0, & j'_t = j'_{t-1} \end{cases};$$

2) очередное появление состояния $j'_t = j'_{t+b} \neq j'_{t+b-1}$ произойдет, если $\sum_{t'=t+1}^{t+b} i'_{t'} = 2^k \theta$, $\theta = 1, 2, 3, ...$ – целое положительное число;

3) переход $j'_t \to j'_{t+1} \neq j'_t$ определяется рекуррентным соотношением $j'_{t+1} = j' \Big|_{j=j'_t}$, где j' – номер строки таблицы v, на которой расположены знаки $j = j'_t$ и $i = i_{t+1}$ одного из столбцов $i' = 1, 2, ..., 2^m - 1$;

4) сумма знаков i'_t от состояния j'_t до состояния $j'_{t-b} \neq j'_{t-b+1}$ определяется выражением: $S_{j'_t\, j'_{t-b}} = a + 2^k \theta$, $a = \sum_{t'=t-b+1}^{t} i'_{t'} \bmod 2^k$, $\theta = 0, 1, 2, ...$ – целое положительное число; a – количество переходов по пункту 3) от состояния j'_{t-b} до первого появления j'_t, где все состояния от j'_{t-b} до j'_t перебираются в столбце $i' = 1$ без внимания на соответствующие знаки i;

5) для $\Delta j = 1$ выполняется равенство

$$i'_t + j'_t = \begin{cases} j'_{t-1} \text{ или } j'_{t-1} + 2^k \text{ для } j'_{t-1} = 0, 1, 2, ..., 2^m - 2 \\ j'_{t-1} \text{ для } j'_{t-1} = 2^m - 1, 2^m, ..., 2^k - 1 \end{cases};$$

6) j'_{t-1} – четное $\Rightarrow$

а) j'_{t+b} – четное, $\sum_{t'=t}^{t+b} i'_{t'}$ – четная;

j'_{t+b} – нечетное, $\sum_{t'=t}^{t+b} i'_{t'}$ – нечетная;

б) i'_{t+b}, j'_{t+b} – оба четные или оба нечетные, $\sum_{t'=t}^{t+b-1} i'_{t'}$ – четная;

i'_{t+h} , j'_{t+h} – один четный, другой нечетный, $\sum_{t'=t}^{t+h-1} i'_{t'}$ – нечетная;

7) j'_{t-1} – нечетное $\Rightarrow$

а) j'_{t+h} – четное, $\sum_{t'=t}^{t+h} i'_{t'}$ – нечетная;

j'_{t+h} – нечетное, $\sum_{t'=t}^{t+h} i'_{t'}$ – четная;

б) i'_{t+h} , j'_{t+h} – оба четные или оба нечетные, $\sum_{t'=t}^{t+h-1} i'_{t'}$ – нечетная;

i'_{t+h} , j'_{t+h} – один четный, другой нечетный, $\sum_{t'=t}^{t+h-1} i'_{t'}$ – четная.

Полагая в пункте 4) $j'_{t-h} = j'_0$ и a – номер расположения состояния j'_t в образующейся последовательности $L_{j'_0}$, спектр системы и способы его получения для $j'_0 \neq 0$ будут те же самые, что и в пункте 1. Отличие состоит лишь только в смысловом значении величины a: в пункте 1 величина a обозначает количество соответствующих знаков i'_t на данном отрезке шагов t, а в пункте 2 величина a обозначает $\sum i'_t$ на данном отрезке шагов t. Поэтому в спектрах $C_{j'_0}$ величину a будем писать в виде a_N и a_Σ для систем, определенных в пунктах 1 и 2 соответственно.

Пример 4. Система $[q, \mu, m, k] = [2, 2, 2, 3]$, $n = m + k = 5$, K_{01}^{01}, длина открытого текста $\Delta = 30$ знаков i_t. Рассмотрим системы с $\Delta j = 1, 3, 5, 7$, для которых начальные состояния $j'_0 = 0$ произвольно выбираем из множества

$\{0, 1, 2, ..., q^k - 1\} = \{0, 1, 2, 3, 4, 5, 6, 7\}$.

Символы i, i' –двухзначные, j, j' – трехзначные.

Таблицы v

	$\Delta j = 1$ Ключ $K_{ij}^{ij} = K_{01}^{01}$								$\Delta j = 3$ Ключ $K_{ij}^{ij} = K_{01}^{01}$							
i'	0		1		2		3		0		1		2		3	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	0	0	2	1	0	2	2	3	3	0	0	3	3	6	0	1
1	1	1	3	2	1	3	3	4	1	1	2	4	3	7	3	2
2	2	2	0	3	2	4	0	5	0	2	3	5	0	0	3	3
3	3	3	1	4	3	5	1	6	2	3	0	6	2	1	1	4
4	0	4	2	5	0	6	2	7	3	4	2	7	2	2	0	5
5	1	5	3	6	1	7	3	0	2	5	1	0	1	3	2	6
6	2	6	0	7	2	0	0	1	1	6	3	1	0	4	1	7
7	3	7	1	0	3	1	1	2	0	7	1	2	1	5	2	0

	$\Delta j = 5$ Ключ $K_{ij}^{ij} = K_{01}^{01}$								$\Delta j = 7$ Ключ $K_{ij}^{ij} = K_{01}^{01}$							
i'	0		1		2		3		0		1		2		3	
j'	i	j	i	j	i	j	i	j	i	j	i	j	i	j	i	j
0	1	0	0	5	1	2	3	7	2	0	2	7	2	6	0	5
1	0	1	0	6	1	3	2	0	1	1	1	0	1	7	0	6
2	3	2	2	7	3	4	3	1	0	2	2	1	0	0	0	7
3	0	3	3	0	3	5	0	2	2	3	1	2	0	1	3	0
4	2	4	1	1	1	6	2	3	0	4	3	3	3	2	3	1
5	1	5	2	2	1	7	1	4	3	5	1	4	0	3	2	2
6	2	6	3	3	0	0	2	5	1	6	2	5	2	4	1	3
7	0	7	0	4	2	1	3	6	3	7	3	6	1	5	3	4

Связь между системами счисления								
$q = 2$	000	001	010	011	100	101	110	111
$q = 10$	0	1	2	3	4	5	6	7

Шифрование									
Δj		1		3		5		7	
t	i_t	i'_t	j'_t	i'_t	j'_t	i'_t	j'_t	i'_t	j'_t
0			0		0		0		0
1	1	1	7	1	5	0	0	1	1
2	3	0	7	1	2	1	3	3	4
3	0	1	6	0	2	0	3	0	4
4	2	0	6	2	4	3	4	2	6
5	3	1	5	0	4	2	2	1	7
6	2	1	4	1	1	1	5	1	0
7	2	2	2	2	3	3	6	0	0

8	0	2	0	1	0	1	1	2	2
9	0	0	0	2	2	0	1	0	2
10	1	1	7	1	7	1	4	1	3
11	2	3	4	1	4	0	4	0	3
12	3	3	1	0	4	2	2	1	4
13	3	2	7	0	4	0	2	3	7
14	0	1	6	2	6	3	3	3	2
15	1	3	3	0	6	2	1	1	3
16	0	1	2	1	3	0	1	2	5
17	0	2	0	1	0	0	1	3	0
18	1	1	7	1	5	1	4	1	1
19	2	3	4	0	5	0	4	1	2
20	3	3	1	1	2	2	2	2	4
21	3	2	7	3	1	0	2	3	7
22	1	2	5	0	1	2	0	2	1
23	1	0	5	0	1	0	0	0	1
24	1	0	5	0	1	0	0	0	1
25	1	0	5	0	1	0	0	0	1
26	0	3	2	3	0	2	6	2	3
27	3	1	1	0	0	3	7	1	4
28	3	2	7	0	0	3	0	3	7
29	2	3	4	3	7	3	1	1	0
30	0	0	4	0	7	0	1	2	2

Проверим по этой таблице выполнение свойства 2) для $\Delta j = 1$. Пусть, например, $j'_t = j'_1 = 7$, $t = 1$; первое очередное появление этого состояния произойдет при $t = 10$: $j'_{t+h} = j'_{10} = 7$, при этом $j'_{t+h} \neq j'_{t+h-1}$, на отрезке шагов $[t+1, t+h] = [2, 10]$, на котором сумма всех знаков $\sum_{t'=t+1}^{t+h} i'_{t'} = 2^k \theta$, $\theta = 1, 2, 3, ...$ – любое целое положительное число, $\sum_{t'=t+1}^{t+h} i'_{t'} = \sum_{t=2}^{10} i'_t = 1+1+1+2+2+1 =$

$= 2^k \theta = 2^3 \cdot 1 = 8$. Такое свойство выполняется в соответствии с пунктом 2) для любого состояния j'_t данной таблицы шифрования.

Таблицы спектров $C_{j'_0}$

$\Delta j = 1$								
a_Σ	0	1	2	3	4	5	6	7
$j'_0 \setminus L_{j'_0}$	j'_0	j'_1	j'_2	j'_3	j'_4	j'_5	j'_6	j'_7

0	0	7	6	5	4	3	2	1
1	1	0	7	6	5	4	3	2
2	2	1	0	7	6	5	4	3
3	3	2	1	0	7	6	5	4
4	4	3	2	1	0	7	6	5
5	5	4	3	2	1	0	7	6
6	6	5	4	3	2	1	0	7
7	7	6	5	4	3	2	1	0

$\Delta j = 3$								
a_Σ	0	1	2	3	4	5	6	7
$j'_0 \setminus L_{j'_0}$	j'_0	j'_1	j'_2	j'_3	j'_4	j'_5	j'_6	j'_7
0	0	5	2	7	4	1	6	3
1	1	6	3	0	5	2	7	4
2	2	7	4	1	6	3	0	5
3	3	0	5	2	7	4	1	6
4	4	1	6	3	0	5	2	7
5	5	2	7	4	1	6	3	0
6	6	3	0	5	2	7	4	1
7	7	4	1	6	3	0	5	2

$\Delta j = 5$								
a_Σ	0	1	2	3	4	5	6	7
$j'_0 \setminus L_{j'_0}$	j'_0	j'_1	j'_2	j'_3	j'_4	j'_5	j'_6	j'_7
0	0	3	6	1	4	7	2	5
1	1	4	7	2	5	0	3	6
2	2	5	0	3	6	1	4	7
3	3	6	1	4	7	2	5	0
4	4	7	2	5	0	3	6	1
5	5	0	3	6	1	4	7	2
6	6	1	4	7	2	5	0	3
7	7	2	5	0	3	6	1	4

$\Delta j = 7$								
a_Σ	0	1	2	3	4	5	6	7
$j'_0 \setminus L_{j'_0}$	j'_0	j'_1	j'_2	j'_3	j'_4	j'_5	j'_6	j'_7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1

3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Спектры C_0								
$\Delta j \setminus a_\Sigma$	0	1	2	3	4	5	6	7
1	0	7	6	5	4	3	2	1
3	0	5	2	7	4	1	6	3
5	0	3	6	1	4	7	2	5
7	0	1	2	3	4	5	6	7

В ячейках этой таблицы находятся значения состояний j'_0.

6. Модификация

Модификация знаков i_t, i'_t, j'_t в алгоритмах шифрования и дешифрования позволяет расширить свойства криптосистем, которые могут быть использованы в приложениях.

1. Модификация знака i_t: $i_t \to i_t^* = i_t \oplus i'_{t-\delta}$,

где $\oplus$ – поразрядное сложение по модулю q, $\delta \geq 1$ – целое положительное число, модификатор $M_1(\delta)$.

Этот модификатор был уже ранее использован в (16). Вводится начальный вектор $I_\delta'^0 = i'_{-(\delta-1)} i'_{-(\delta-2)} \ldots i'_{-1} i'_0$. Модификация знака i_t приводит к распространению ошибки при шифровании.

При расшифровании делаем переход $i_t^* \to i_t = i_t^* \Theta i'_{t-\delta}$, где Θ – поразрядное вычитание по модулю q; Θ эквивалентно $\oplus$ для $q = 2$.

2. Модификация знака i'_t: $i'_t \to i_t'^* = i'_t \oplus i_{t+\delta}$, $\delta \geq 1$, $M_2(\delta)$ – модификатор; вводится конечный вектор $I_\delta^\Delta = i_{\Delta+1} i_{\Delta+2} \ldots i_{\Delta+\delta}$,

где Δ – длина открытого текста I. При расшифровании делаем переход $i_t'^* \to i'_t = i_t'^* \Theta i_{t+\delta}$. Модификация знака i'_t приводит к распространению ошибки при расшифровании.

В пунктах 1 и 2 число δ можно сделать переменным, периодически принимающим свои значения на каждом шаге t из некоторой произвольной последовательности $L_\delta = \delta_1\delta_2...\delta_p$ длиной p. В этом случае последовательность L_δ может выполнять роль дополнительного ключа.

3. Модификация знака j'_t:

$j'_t \to j'^*_t = j'_t \oplus i'_t \oplus i'_{t-1}(m<) \oplus i'_{t-2}(2m<) \oplus ... \oplus i'_{t-\lambda}(\lambda m<)$ – модификатор $M_3(\lambda)$; вводится начальный вектор $I'^0_\lambda = i'_{-(\lambda-1)}i'_{-(\lambda-2)}...i'_{-1}i'_0$, где $\lambda = \frac{k}{m} - 1$, k кратно m.

При расшифровании делаем переход

$j'^*_t \to j'_t = j'^*_t \Theta i'_t \Theta i'_{t-1}(m<)\Theta i'_{t-2}(2m<)\Theta...\Theta i'_{t-\lambda}(\lambda m<)$.

Модификация знака j'_t выводит состояние системы из замкнутого цикла и приводит к распространению ошибки при шифровании и дешифровании.

4. Модификация знака j'_t:

$j'_t \to j'^*_t = j'_t \oplus i_{t+1} \oplus i_{t+2}(m<) \oplus i_{t+3}(2m<) \oplus ...$

$... \oplus i_{t+\lambda}((\lambda-1)m<)$ – модификатор $M_4(\lambda)$; вводится конечный вектор $I^\Delta_\lambda = i_{\Delta+1}i_{\Delta+2}...i_{\Delta+\lambda}$, где $\lambda = \frac{k}{m}$, k кратно m.

При расшифровании делаем переход

$j'^*_t \to j'_t = j'^*_t \Theta i_{t+1}\Theta i_{t+2}(m<)\Theta i_{t+3}(2m<)\Theta...$

$...\Theta i_{t+\lambda}((\lambda-1)m<)$.

Модификатор $M_4(\lambda)$ обладает теми же свойствами, что и $M_3(\lambda)$.

7. Аутентификация данных

1. Установление подлинности информации после ее передачи по линиям связи или хранения можно осуществить при помощи многократного шифрования по алгоритму **2.F**. Для этого возьмем систему с ключом K^{01}_{11}, $m = k$; все ключи шифрования K^{-1r}_ξ одинаковые; $j'^r_0 = 0$ для всех $r = 1, 2,..., \bar{r}$. Вероятность

необнаруживаемых изменений в шифртексте $I'^{\bar{r}}$ и конечных состояниях j'^{r}_{Δ} системы определяется по формуле:

$$P = q^{-m\bar{r}}. \qquad (27)$$

Критерием подлинности шифртекста $I'^{\bar{r}}$ и конечных состояний j'^{r}_{Δ} системы является выполнение всех равенств:

$$j'^{r}_{0d} = j'^{r}_{0}, \quad r = 1, 2, ..., \bar{r} \qquad (28)$$

после дешифрования; j'^{r}_{0d} – состояния системы при $t = 0$, полученные при дешифровании.

Если изменения были сделаны только в j'^{r}_{Δ} или в $I'^{\bar{r}}$ для одного какого-либо знака $i'^{\bar{r}}_{t}$, то это обнаружится после дешифрования абсолютным образом в виде нарушения одного или нескольких равенств (28).

2. Аутентификацию данных можно осуществить также и при помощи однократного шифрования по алгоритму **2.Е**, используя системы с ключами K_{11}^{01} и K_{01}^{11}, $m = k$. При шифровании используем модификацию знаков шифртекста $i'_t = i'_t \oplus i_{t+\delta}$ $(\delta \geq 1)$ знаками $i_{t+\delta}$ открытого текста. Перед шифрованием открытого текста шифруем знаки аутентификатора, состоящего из последовательности m-битовых знаков длиной l. В качестве аутентификатора возьмем последовательность из нулевых битов. Данные шифртекста будут считаться подлинными, если при дешифровании получим нулевые m-битовые знаки аутентификатора и $j'_{0d} = j'_0$.

Последовательность m-битовых знаков аутентификатора можно взять произвольной. Вероятность необнаруживаемых изменений в шифртексте при дешифровании равна

$$P = 2^{-n\,l}. \qquad (29)$$

8. Криптоанализ

Определение секретного ключа криптосистемы, построенной на предложенных алгоритмах, на основе анализа известного шифртекста и соответствующей ему некоторой (небольшой) части открытого текста возможно лишь только при полном переборе

вариантов распределения знаков j в таблице v. Доказательство этого утверждения вытекает из необходимости знать распределение знаков i и j в таблице v, являющихся составной частью элементов

$$v_{j'i'} = i(k<) + j \qquad (30)$$

этой таблицы (см. пункт **1**). Кроме этого, для успешного криптоанализа, необходимо знать значения m и k, определяющие размеры таблицы v и являющиеся секретными.

Дальнейший анализ построим на допущении, что криптоаналитику известны значения m и k, что облегчает его задачу, которая однако все же остается весьма и весьма сложной.

Допустим также, что криптоаналитику известны весь шифртекст I', некоторая концевая часть открытого текста $I = i_\Delta i_{\Delta-1} i_{\Delta-2} ... i_{\Delta-\delta+1}$ длиной δ и конечное состояние j'_Δ системы, где Δ – длина открытого текста.

После шифрования открытого текста на выходе алгоритма шифрования имеем шифртекст $I' = \{i'\}$, состоящий из совокупности m-битовых знаков i', и конечное k-битовое состояние $j' = j'_\Delta$ системы. По последнему знаку i' шифртекста и конечному состоянию j'_Δ мы можем однозначно определить по алгоритму дешифрования расположение в таблице v лишь только одного известного m-битового знака i открытого текста. Соответствующий же этому знаку k-битовый знак j не определяется однозначно. Оба знака i и j входят в соответствующий элемент $v_{j'i'}$ таблицы v согласно выражению (30). Для каждой пары i' и j' таблицы v имеется единственный элемент $v_{j'i'}$, отличный от других, в котором возможным знаком j может быть одно из 2^k значений

$$j \in \{0, 1, 2, ..., 2^k - 1\} \qquad (31)$$

при одном и том же знаке i. Поэтому, зная шифртекст и часть соответствующего ему открытого текста, построить правильное распределение знаков j таблицы v возможно лишь только при

полном переборе знаков j из множества (31) для каждого элемента $v_{j'i'}$ этой таблицы. Для всех элементов $v_{j'i'}$ таблицы v (ключ K_{i1}^{i1}, $m \le k$) количество вариантов распределения знаков j определяется выражением

$$Z_{m,k}(j) = \prod_{r=0}^{2^m-1}(2^k - r)! \ , \qquad (32)$$

являющимся заниженной оценкой для рассматриваемого распределения знаков j при учете вариантов с $j = j'$ (знак j расположен на строке j' таблицы v). Полагая $n = m + k = 8$, вычислим некоторые значения выражения (32):

$$Z_{1,7}(j) = 128! \times 127! \approx 1.164 \cdot 10^{429}$$

$$Z_{2,6}(j) = 64! \times 63! \times 62! \times 61! \approx 4.018 \cdot 10^{345} \quad . \qquad (33)$$

$$Z_{4,4}(j) = 16! \times 15! \times 14! \times ... \times 1! \approx 1.892 \cdot 10^{90}$$

Выбранный вариант распределения знаков j будет считаться ложным, если при длине шифртекста, превышающим в несколько раз количество элементов ключа, в процессе дешифрования обнаружится несовпадение некоторого знака открытого текста с соответствующим дешифрованным m-битовым знаком i, расположенным в таблице v. Поскольку значения $Z_{m,k}(j)$ из (33) достаточно велики, то криптоанализ на этой основе требует практически невыполнимых больших временных затрат.

Недосекин Ю.А.

Шифрование со скрытой рандомизацией

Аннотация

Для поточных шифрсистем предложен алгоритм введения в открытый текст рандомизирующей последовательности длиной, кратной длине исходного открытого текста. Из расширенного шифртекста оставляем только ту его часть, которая соответствует части введенной рандомизирующей последовательности длиной, равной длине исходного открытого текста. Оставшаяся часть расширенного шифртекста восстанавливается при его дешифровании.

Используем системы с ключом $K_{i1}^{1,j}$, $m = k$, с базисом $\mu = q$ для шифрования по алгоритму **4.Е** [1] произвольного текста I с, введенной в него, рандомизирующей последовательностью R длины δ. О значениях верхних и нижних индексах в ключе K_{ij}^{ij} сказано в пункте 3[1]. Рандомизирующая последовательность (рандомизатор) $R = \varrho_1 \varrho_2 ... \varrho_\delta$, где ϱ_γ – m-битовые знаки $(\gamma = 1, 2, ..., \delta)$, задается произвольно; при необходимости ее можно использовать в качестве дополнительного ключа.

1. Простая рандомизация

Составим расширенный открытый текст, чередуя один знак ϱ_γ рандомизатора R с одним знаком i открытого текста I (информационной последовательности L), в результате чего знаки ϱ_γ будут расположены на нечетных местах, а знаки i – на четных. Знаки ϱ_γ рандомизатора R используются циклически и в расширенном открытом тексте периодически повторяются, если его длина δ меньше длины Δ информационной последовательности L. Полученный таким образом расширенный открытый текст имеет длину 2Δ.

На выходе алгоритма шифрования оставляем часть I'_R расширенного шифртекста, соответствующую последовательности R. Другая часть I'_L расширенного шифртекста, соответствующая

информационной последовательности L, восстанавливается при дешифровании.

Результатами шифрования со скрытой рандомизацией являются: шифртекст I'_R, конечное состояние $j'_{2\Delta}$ системы и значение номера последнего знака $\varrho_{2\Delta-1}$ последовательности R, используемого при шифровании.

Шифртекст I'_R состоит из знаков i'_t расширенного шифртекста при $t = 1 + 2r$, где $r = 0,1,2,...,\Delta - 1$.

Длина шифртекста I'_R равна длине шифртекста I' без рандомизации для той же последовательности L.

Алгоритм дешифрования по таблице v.

Цикл для $t = [2\Delta, 2]$ с шагом $H = -2$, пункты 1, 2.

1. По известным знакам $i' = i'_{t-1}$ и $i = \varrho_{t-1} = i_{t-1}$ из таблицы v определяем $j'_{t-2} = j_{t-1} = j$ и $j_t = j'_{t-1} = j'$, где i, i', j, j' – знаки таблицы v, t – четные значения шагов, $t = 2\Delta, 2\Delta - 2,..., 2$, ϱ_{t-1} – значение ϱ_γ на шаге $(t-1)$.

2. По известным знакам j_t и j'_t из таблицы v определяем $i = i_t$.

Полученный при дешифровании открытый текст I состоит из знаков i_t расширенного текста при $t = 2r$, где $r = 1,2,...,\Delta$.

Таблица v. Ключ $K_{ij}^{ij} = K_{11}^{10}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	0	0	1	1	2	2	3	3
1	1	2	2	1	3	0	0	3
2	2	0	3	1	0	2	1	3
3	3	2	0	1	1	0	2	3

Пример 1. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, $n = m + k = 4$, K_{11}^{10}, рандомизатор $R = \varrho_1\varrho_2\varrho_3\varrho_4 = 1203$, информационная последовательность $L = 2012321003$ из $\Delta = 10$ двухзначных знаков i двоичной системы счисления.

Начальное состояние $j'_0 = 0$ произвольно выбираем из множества $\{0, 1, 2,..., q^k - 1\} = \{0, 1, 2, 3\}$.

Связь между системами счисления				
$q=2$	00	01	10	11
$q=10$	0	1	2	3

Шифрование					Дешифрование				
t	i_t	i'_t	j'_t		t	i_t	j_t	i'_t	j'_t
0			0		0				0
1	1	2	3		1	1	0	2	3
2	2	3	3		2	2	3	3	3
3	2	3	3		3	2	3	3	3
4	0	3	1		4	0	3	3	1
5	0	1	3		5	0	1	1	3
6	1	3	2		6	1	3	3	2
7	3	0	3		7	3	2	0	3
8	2	3	3		8	2	3	3	3
9	1	3	2		9	1	3	3	2
10	3	0	3		10	3	2	0	3
11	2	3	3		11	2	3	3	3
12	2	3	3		12	2	3	3	3
13	0	3	1		13	0	3	3	1
14	1	1	0		14	1	1	1	0
15	3	2	1		15	3	0	2	1
16	0	1	3		16	0	1	1	3
17	1	3	2		17	1	3	3	2
18	0	2	2		18	0	2	2	2
19	2	2	0		19	2	2	2	0
20	3	2	1		20	3	0	2	1

Результаты шифрования:

конечное состояние $j'_{20}=1$ системы;

последний номер знака рандомизации при $t=19$ равен $\gamma=2$, которому соответствует знак рандомизации $\varrho_\gamma=\varrho_2=2$;

шифртекст в столбце i'_t при нечетных t: $I'_R=2310333232$.

Шифртекст при четных t не запоминается, он восстанавливается при дешифровании согласно приведенному выше алгоритму.

Дешифрованный текст $I=2012321003$, совпадающий с исходной информационной последовательностью L, находится в столбце i_t при четных t.

2. Сложная рандомизация

Скрытую рандомизацию можно вводить в открытый текст I группами из s последовательных знаков ϱ_γ рандомизатора R, чередуя эти группы с одним знаком i информационной последовательности L. Знаки ϱ_γ рандомизатора R используются циклически. В этом случае шифртекст I'_R будет соответствовать только первым знакам ϱ_γ каждой группы из s знаков и его длина по-прежнему будет равна длине информационной последовательности L. Составленный таким образом расширенный открытый текст имеет длину $(s+1)\Delta$.

На выходе алгоритма шифрования оставляем часть I'_R расширенного шифртекста, соответствующую последовательности R. Другая часть расширенного шифртекста восстанавливается при дешифровании.

Количество s знаков ϱ_γ в группе назовем глубиной рандомизации.

Результатами шифрования со скрытой рандомизацией при $s>1$ являются: шифртекст I'_R, конечное состояние $j'_{(s+1)\Delta}$ системы и последнее значение номера знака $\varrho_{(s+1)\Delta-1}$ последовательности R, используемого при шифровании.

Шифртекст I'_R состоит из знаков i'_t расширенного шифртекста при $t=1+r(s+1)$, где $r=0,1,2,...,\Delta-1$.

Длина шифртекста I'_R равна длине шифртекста I' без рандомизации для той же последовательности L.

Дешифрование по таблице v с $s>1$.

Цикл для $t=[(s+1)\Delta,(s+1)]$ с шагом $H=-(s+1)$, пункты 1–3.

1) по известным i'_{t-s}, $\varrho_{t-s}=i_{t-s}$ из таблицы v определяем $j_{t-s}=j'_{t-s-1}$ и $j'_{t-s}=j_{t-s+1}$;

2) далее на всех последующих шагах $t-s+1, t-s+2,..., t-1$ по известным j и ϱ_γ из таблицы v определяем j'; на шаге $(t-1)$ определяем $j'_{t-1}=j_t$;

3) на шаге t по известным j_t и j'_t из таблицы v определяем $i = i_t$.

Полученный при дешифровании открытый текст I состоит из знаков i_t расширенного текста при $t = (s+1)r$, где $r = 1,2,...,\Delta$.

Пример 2. Система $[q, \mu, m, k] = [2, 2, 2, 2]$, $n = m + k = 4$, K_{21}^{10}, рандомизатор $R = \varrho_1\varrho_2\varrho_3\varrho_4\varrho_5 = 03021$, глубина рандомизации $s = 2$, информационная последовательность $L = 0031120332$ из $\Delta = 10$ двухзначных знаков i двоичной системы счисления.

Начальное состояние $j'_0 = 3$ произвольно выбираем из множества $\{0, 1, 2,..., q^k - 1\} = \{0, 1, 2, 3\}$.

Таблица v. Ключ $K_{ij}^{ij} = K_{11}^{10}$

i'	0		1		2		3	
j'	i	j	i	j	i	j	i	j
0	2	0	2	1	2	2	2	3
1	0	3	0	1	0	0	0	2
2	3	2	3	0	3	3	3	1
3	1	2	1	1	1	0	1	3

Связь между системами счисления				
$q = 2$	00	01	10	11
$q = 10$	0	1	2	3

Шифрование			
t	i_t	i'_t	j'_t
0			3
1	0	0	1
2	3	3	2
3	0	3	1
4	0	1	1
5	2	1	0
6	0	2	1
7	1	1	3
8	0	0	1
9	3	3	2
10	3	0	2

Дешифрование				
t	i_t	j_t	i'_t	j'_t
0				3
1	0	3	0	1
2	3	1	3	2
3	0	2	3	1
4	0	1	1	1
5	2	1	1	0
6	0	0	2	1
7	1	1	1	3
8	0	3	0	1
9	3	1	3	2
10	3	2	0	2

11	0	3	1		11	0	2	3	1
12	1	1	3		12	1	1	1	3
13	2	3	0		13	2	3	3	0
14	1	2	3		14	1	0	2	3
15	1	3	3		15	1	3	3	3
16	0	0	1		16	0	3	0	1
17	3	3	2		17	3	1	3	2
18	2	2	0		18	2	2	2	0
19	0	2	1		19	0	0	2	1
20	2	1	0		20	2	1	1	0
21	0	2	1		21	0	0	2	1
22	1	1	3		22	1	1	1	3
23	0	0	1		23	0	3	0	1
24	3	3	2		24	3	1	3	2
25	3	0	2		25	3	2	0	2
26	0	3	1		26	0	2	3	1
27	3	3	2		27	3	1	3	2
28	2	2	0		28	2	2	2	0
29	1	2	3		29	1	0	2	3
30	2	3	0		30	2	3	3	0

Результаты шифрования:

конечное состояние $j'_{30} = 0$ системы;

последний номер знака рандомизации на шаге $t = 29$ равен $\gamma = 5$, которому соответствует знак рандомизации $\varrho_\gamma = \varrho_5 = 1$;

шифртекст в столбце i'_t при $t = 1 + r(s+1)$, $r = 0,1,2,...,\Delta - 1$: $I'_{\mathrm{R}} = 0110302102$.

Шифртексты при $t = (s+1)r$ и $t = (s+1)r - 1$, где $r = 1,2,...,\Delta$, не запоминаются, они восстанавливается при дешифровании согласно приведенному выше алгоритму.

Дешифрованный текст $I = 0031120332$, совпадающий с исходной информационной последовательностью L, находится в столбце i_t при $t = (s+1)r$, где $r = 1,2,...,\Delta$.

Литература

1. Недосекин Ю.А. Преобразование и защита информации. «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 16.

Серия: **ПЕДАГОГИКА**

Голубенко Н. Б.

Компьютер в детском саду

Воспитание детей в детском саду имеет три цели: сохранить здоровье ребенка, создать условия для полноценного психического развития и дать возможность содержательно прожить детство.

Развитие деятельности у ребенка как мотивированной, целенаправленной, а не случайной активности начинается примерно в возрасте двух лет. В последующие два года развитие деятельности осуществляется по нескольким направлениям. Расширяется и обогащается набор целей, которые самостоятельно ставит перед собой ребенок; интенсивно идет процесс овладения способами, необходимыми для реализации этих целей; возникает способность связывать и соподчинять несколько целей, реализуя цепочки связанных между собой целей.

В возрасте пяти лет в психике ребенка появляются принципиально новые образования. Это произвольность психических процессов - внимания, памяти, восприятия и других - и вытекающая отсюда способность управлять своим поведением, а также изменения в представлениях о себе, в самосознании и в самооценках. Появляется способность на основе достигнутых целей развертывать в течение более или менее длительного времени последующие цели.

На шестом году жизни у ребенка появляется способность ставить цели, касающиеся его самого, собственного поведения и таких психологических процессов, как память, внимание, восприятие и др. Интерес ребенка к себе и своим качествам, получающий дополнительный стимул благодаря развитию представлений о себе, распространяется и на сверстников. Все это порождает в жизни детей два существенных изменения. Во-первых, изменение роли взаимоотношений ребенка со сверстниками в его эмоциональной жизни и усложнение этих взаимоотношений. Во-вторых, появление интереса к личности и личным качествам других детей. Происходит разделение детей на более заметных и популярных, пользующихся симпатией и уважением сверстников, и детей малозаметных, не представляющих на этом фоне интереса для остальных.

После пяти лет контакты в связи с совместной игрой становятся особенно интенсивными и значимыми для ребенка. Для дошкольника игра - это вид деятельности, который в наибольшей степени оказывает влияние на психическое развитие. Произвольность поведения и психических процессов, которая интенсивно развивается в период между пятью и семью годами, имеет решающее значение для готовности ребенка к школьному обучению.

Основное требование школы - делать не то, что тебе в данный момент хочется, а то, что делает весь класс. Это способность сосредотачивать свои умственные усилия на той задаче, которую ставит учитель, является одной из решающих предпосылок готовности к школьному обучению.

Считаю, что для развития и обучения ребенка необходимо иметь в детских садах компьютеры и начинать уже в старших группах проводить уроки компьютерной грамотности.

Конечно, поначалу они должны проводиться в форме игр на компьютере. Это выработает в детях усидчивость и устранит в будущем страх перед компьютером. Играть на компьютере лучше всего в развивающие игры, головоломки, раскраски.

Затем можно начинать осваивать азбуку на компьютере, учиться считать. Можно и нужно разработать специальные программы.

Но надо следить, чтобы ребенок чрезмерно не увлекался работой на компьютере. Компьютерные уроки следует чередовать с подвижными играми, спортивными занятиями.

Компьютер поможет в запоминании слов при помощи картинок, разучивании песенок и стихов, прослушивании музыки. Игры на компьютере способствуют установлению новых контактов между детьми, возникновению дружеских связей.

Активные и общительные дети не всегда самые способные. Так же как и малозаметные и малообщительные дети не всегда на самом деле интеллектуально менее развиты, чем остальные. Компьютер поможет раскрыть и реализовать скрытый интеллектуальный потенциал.

Литература

1. Радуга: Прогр. и метод. Руководство по воспитанию, развитию и образованию детей 5-6 лет в дет. саду/ Т.Н. Доронова, В.В. Гербова, Т.И. Гризик и др.; Сост. Т.Н. Доронова. 2-е изд. М.: Просвещение, 1997, 271 с.

Серия: **ПСИХОЛОГИЯ**

«Чем больше мыслящий наблюдатель теряется перед необозримой массой мелких частностей, тем острее испытывает он потребность в выработке общего взгляда на всю область познания. Но такая философия может покоиться лишь на естественно-научном фундаменте, на критическом сопоставлении всех общих выводов опытных наук. На такую подлинную «натурфилософию» имеет право каждый мыслящий и научно подготовленный человек; она отнюдь не составляет собственности привилегированной касты учёных».

Геккель Э. Мировые загадки. М: Бр. А. и И. ГРАНАТ и К*, 1920. С. 383

Мотков О.И.

Функции и строение психики: свежий взгляд

Аннотация

В статье критически рассматриваются традиционные и альтернативные им подходы к пониманию психики и предлагается авторская точка зрения, основанная на принципах предметности и естественной науки. Психика предстаёт как центральный организатор и регулятор поведения всего живого организма. Эти **управляющие** её **функции** и являются *главными*, а вовсе не "отражение". Ядро психики составляют потребности. Именно наличие жизненных целей и самоорганизации поведения по их осуществлению представляет собой главный признак, отличающий живое от неживого. Психика есть у любого живого существа, в том числе у одноклеточных и растений.

Оглавление

В психологии и сегодня остаётся актуальным отыскание более целостного и ясного понимания сущности, структуры и принципов развития психики живых организмов, стремление глубже разобраться в том, что стоит за устоявшимися и повторяющимися по инерции представлениями. Как традиционное, так и более современные определения психики при вдумчивом чтении вызывают *вопросы*, на которые пытливый ум не находит достаточно правдоподобных удовлетворительных ответов.

Дальнейшее изложение построено следующим образом: даётся традиционное определение, по нему ставятся вопросы, затем та же процедура повторяется с современными представлениями о психике, и далее проводится краткий анализ других альтернативных подходов из иных источников. На основе такого анализа делается попытка дать авторские ответы на поставленные вопросы, представить новое понимание и определение психики, в частности, на основе нового взгляда на приоритетность выделяемых её функций. В конце статьи кратко рассматриваются главные особенности структуры психики.

Анализ традиционных подходов к психике

Рассмотрим пристальнее некоторые традиционные в нашей психологии определения психики. Все они в той или иной мере опирались на доминирующую в то время идеологию марксизма-ленинизма и несли скорее философский и идеологический, нежели естественно-научный характер.

А.Н. Леонтьев в Большой Советской энциклопедии так определял психику:

«**Психика** (от греч. *psychikos* - душевный), свойство высокоорганизованной материи, являющееся особой формой отражения субъектом объективной реальности. Важнейшая особенность психического отражения - его активность. При этом оно не только представляет собой продукт активной деятельности субъекта, но и, опосредствуя её, выполняет функцию ориентации, управления ею. Таким образом, психические явления составляют необходимый внутренний момент предметной деятельности субъекта, и природа психики, её законы могут получить научное объяснение лишь в процессе анализа строения, видов и форм деятельности». (Психика. *Леонтьев А.Н.* / БСЭ, Том 21, с.187. М., 1975. Также http://slovari.yandex.ru/dict/bse/article/00063/69900.htm).

У меня возникает сразу несколько вопросов.

- *Что понимается под «высокоорганизованной материей»?* Если под нею подразумевается мозг, то тогда *почему «точкой отсчёта» наличия психики у живого существа объявляется именно существование у него мозга, а не наличие, например, у него просто жизни как таковой?* Ведь жизнь на порядок более высоко организована, чем любой неживой предмет. *На каких основаниях отказывается в обладании психикой растениям*?

- Это свойство выражается у *А.Н. Леонтьева* в «особой форме отражения субъектом объективной реальности». То есть главной, **приоритетной** функцией психики автор называет «отражение». *Почему именно «отражение» выделяется как ведущая функция психики?* Дальнейшие его рассуждения о том, что рассмотрение «психики как отражения» позволяет преодолеть ложные решения «проблемы о соотношении психологического и физиологического» представляются совершенно не убедительными, так как не затрагивают сути психического.

- На мой взгляд, ближе к сущности психики он интуитивно подходит, когда говорит об активности отражения, являющейся у него фактически одним из выражений активности субъекта. Хотел ли такого поворота автор или нет, но получается, что активность отражению придаёт в ходе развиваемой им деятельности субъект. *Кто же является этим таинственным субъектом? Всякая ли биологическая особь? И в чём суть субъектности этой особи? Что даёт возможность субъекту осуществлять «деятельность»?* Мы не находим в рассматриваемой статье о психике ответа на эти вопросы. По-своему ведь активны и амёба, и растение. Их жизненная активность также включает в себя «отражение» важных для них характеристик среды. *Следует ли из этого, что они - субъекты?* Подчёркивая активность как важнейшую «особенность психического отражения», *А.Н. Леонтьев*, видимо, опирался на факт отличия «отражения» у живого существа от отражения у неодушевлённых предметов, например, у зеркала или камня. *В чем же конкретно заключается это отличие «отражения» у живого и неживого*? Вопрос, возможно, упирается в самую сущность жизни как таковой.

- «Отражение», пишет далее Алексей Николаевич, «не только представляет собой продукт активной деятельности субъекта, но и, опосредствуя её, выполняет функцию ориентации, управления ею». *Кто же выполняет функцию ориентации и управления деятельностью, сам субъект или порождаемое им «отражение*»? Может быть, точнее было бы говорить о том, что живой организм, представляемый как субъект, посредством каких-то внутренних структур и, в частности, отвечающих за «отражение» и наделение этого «отражения»

значимостью, и тем самым - управляющей силой, осуществляет функции ориентации и управления своим поведением?

Теперь обратимся к некоторым разъяснениям позиции А.Н. Леонтьева, даваемым *Ю.Б. Гиппенрейтер* в книге «Введение в общую психологию», в главе 11 о происхождении и развитии психики в филогенезе (Гиппенрейтер Ю.Б., 1996, с. 169-197. http://www.psychology-online.net/articles/doc-37.html). Она пишет: «В качестве *объективного критерия психики* А. Н. Леонтьев предлагает рассматривать способность живых организмов реагировать на биологически нейтральные воздействия. Биологически нейтральные (другой термин "абиотические") воздействия - это те виды энергии или свойства предметов, которые не участвуют непосредственно в обмене веществ. …Почему же оказывается полезным их отражать, или на них реагировать? Потому что они находятся в объективно устойчивой связи с биологически значимыми объектами и, следовательно, являются их потенциальными сигналами. Если живой организм приобретает способность как отражать биологически нейтральные свойства, так и устанавливать их связь с биологически существенными свойствами, то возможности его выживания оказываются несравненно более широкими».

Далее Юлия Борисовна, вслед за А.Н. Леонтьевым, отмечает, что «простейшие реагируют на абиотические воздействия среды, и притом на отдельные ее свойства… Во-вторых, отчетливо выступает *приспособительная функция психики*: здесь она выражается в ориентировании поведения (положительные и отрицательные таксисы), а также, хотя и в самых элементарных формах, в изменении поведения в результате индивидуального опыта».

Резюмируем сказанное автором. Психика у живого существа имеет место, если оно реагирует на абиотические раздражители, у него есть «чувствительность». Она, пусть в виде «элементарной сенсорной психики», уже обнаруживается у простейших, так как у них отмечаются такого рода реакции. Важно, что Ю.Б. Гиппенрейтер подчёркивает *приспособительный* характер реакций на абиотические раздражители, то, что они служат лучшему выживанию в изменяющейся среде. Исходя из этой логики, у растений психики нет, так как у них автору известны только реакции на биологически значимые воздействия, которые называют «раздражимостью». Заметим, что имеется много фактов привыкания растений к определённой воде, почве, уровню освещения, голосу

любящей хозяйки и другим её особенностям. И опять возникают вопросы.

Если психика есть у простейших одноклеточных, то, следовательно, они уже представляют собой «высокоорганизованную материю». А у, казалось бы, более сложных по строению многоклеточных растений её нет, так как у них якобы нет реакций на абиотические раздражители, нет чувствительности. *Можно ли считать главной отличительной чертой и главной функцией психики живых существ возможность совершать абиотические реакции, если они всецело подчинены изначальной цели лучшего выживания и функционирования в изменчивой среде, т.е. несут биологическую приспособительную функцию*? Может быть, мы приблизимся к пониманию важнейшей характеристики психики, если найдём ответ на вопрос, **зачем** *живому организму нужны раздражимость и чувствительность, т.е. зачем им необходимо «отражение»*? Если для лучшего выживания, то, *может быть, целевая (приспособительная к главным требованиям организма) и организующая, короче - управляющая функция психики как раз и является более фундаментальной и главной, подчиняющей себе реакции как на биотические, так и на абиотические раздражители*?

Перейдём к рассмотрению несколько более позднего определения психики, данному *Петровским А.В. и Ярошевским М.Г.* в известном Психологическом словаре (*Петровский А.В.* и *Ярошевский М.Г.* , ред. Психологический словарь. М., 1990).

«ПСИХИКА (от греч. psychikos — душевный) — системное свойство высокоорганизованной материи, заключающееся в активном отражении *субъектом* объективного мира, в построении субъектом неотчуждаемой от него картины этого мира и саморегуляции на этой основе своего поведения и деятельности. В П. представлены и упорядочены события прошлого, настоящего и возможного будущего. …Благодаря активному и опережающему *отражению* …внешних объектов в форме П. становится возможным осуществление *действий*, адекватных свойствам этих объектов, а тем самым — выживание испытывающего в них нужду организма… …Определяющими признаками П. являются: *отражение*, дающее образ предметной среды, в которой действуют живые существа, их *ориентация* в этой среде и *удовлетворение потребности* в контактах с нею. …Активность П. проявляется и при отображении реальности …*и в сфере побуждений*, придающих поведению энергию и стремительность, и при исполнении программы поведения, включающей поиск и выбор вариантов. Возникая на определенном

уровне биологической эволюции, П. сама выступает в качестве одного из ее факторов, обеспечивая возрастающую по сложности *приспособляемость* организмов к условиям их существования».

Что же нового добавляет это определение к предыдущему? Появляется идея построения на основе интеграции отдельных «отражений» «картины этого мира». На психологическом языке это похоже на переход от ощущений к образам восприятия и представлениям и, затем, к их последующему обобщению в единой субъективной картине. Однако, *является ли построение таких обобщённых внутренних «картин» обязательным атрибутом любой психики*? Об участии «отражения» как результата активности субъекта в управлении деятельностью уже говорилось вскользь в определении А.Н. Леонтьева. Здесь используется другой термин – «саморегуляция», содержание которого хоть и не раскрывается подробно авторами, но, с точки зрения современных представлений, указывает на способность живых существ к самоконтролю и самокоррекции своих состояний и поведения с целью приведения параметров организма и его жизнедеятельности к неким желаемым оптимальным характеристикам. Кроме того, к философскому термину «деятельность» добавляется термин «поведение», часто используемый в биологических дисциплинах, что, конечно, позволяет с большим основанием рассматривать психику как общебиологический феномен.

На мой взгляд, наиболее важным дополнением в анализируемом определении является указание такого «определяющего признака» психики как «удовлетворение потребности в контактах» со средой. Это шаг вперёд в понимании предназначения психики в живом организме, понимании того, для чего она собственно нужна живому существу. Вопрос только состоит в том, *какого рода потребности живого существа удовлетворяются с помощью психических и телесных процессов?* Контакт с предметной средой, вероятно, часто важен не сам по себе, а лишь как **средство** удовлетворения целого спектра разнообразных фундаментальных потребностей особи. Кроме того, возникает ещё один существенный вопрос: «*Логично ли рассматривать потребности вне психики, являются ли они её важной составляющей?»*

Судя по разъяснениям авторов определения психики, потребности, наряду с другими психическими процессами, принимают важное участие в психической активности. Они утверждают, что «активность П. проявляется и при отображении реальности …и в сфере побуждений, придающих поведению

энергию и стремительность, и при исполнении программы поведения…». Видимо, под «стремительностью» поведения подразумевается его целенаправленность, устремлённость к какой-то конечной жизненной цели. Нельзя не согласиться с тем, что потребности не только побуждают, включают и обеспечивают энергией поведение, но и задают ему определённое общее направление, требуют от него осуществления определённой жизненной цели.

Если потребности встроены в психический аппарат, то какое функциональное значение и какое место они занимают в нем, соотносительно с механизмами «отражения» и моторного исполнения поведения?

Анализ некоторых современных взглядов на психику

Ниже мы ещё вернёмся к проблеме места и значения потребностей и их мотивационных конкретизаций в психике. Теперь же рассмотрим некоторые современные подходы к пониманию психики.

Н.П. Чуприкова в специальной статье, посвящённой психике и предмету психологии, так определяет психику: «…**психика** – это не что иное, как отражательная и (познавательная) и регулирующая поведение деятельность мозга. …психика животных и человека является функцией их мозга» (*Чуприкова Н.П.*, 2004, с.104). Это определение также вызывает некоторое недоумение.

Если психика есть у одноклеточных простейших, не имеющих мозга (Ю.Б. Гиппенрейтер, 1996; Э. Геккель, 1920, и др.), то правильно ли определять её как функции только мозга? Если «отражательная» и регулирующая функции обнаруживается и у одноклеточных организмов, то, возможно, ими заведуют какие-то молекулы ядра клетки и её протоплазмы?

Можно допустить, что «отражение» и регуляция входят в состав важнейших функций психики. Но за этим определением я не нахожу дальнейшего структурирования, анализа их соподчинения. *Как эти и иные психические функции соотносятся друг с другом?* Косвенно мнение Натальи Ивановны можно усмотреть в дальнейшем её определении, характерном, как она подчёркивает, для отечественной психологии: «…психика – это свойство …обеспечивающее адаптивное взаимодействие живого существа с миром благодаря регуляции поведения на основе результатов отражательной психической деятельности». Суть, видимо, скрывается за словами «адаптивное взаимодействие …благодаря регуляции поведения…». *Но чем это взаимодействие с миром живого существа отличается, скажем, от взаимодействия с миром камня? Может*

быть, наличием целостной самоорганизации и самоуправления поведением организма? На этот вопрос, уходящий в самую сущность живых существ, в статье мы не находим чёткого ответа.

Во многих современных словарях и учебниках российских авторов даются определения психики (П.), почти идентичные определениям А.В. Петровского, М.А. Ярошевского или А.Н. Леонтьева, но с некоторыми вариациями (*Психология: Популярный словарик*, 1997; *Рамендик Д.М., Одинцова О.В.*, 2004, *Шабельников В.К.*, 2004, http://ru.wikipedia.org/wiki/Психика , www.glossary.ru и др.).

В книге *Д.М. Рамендик* и *О.В. Одинцовой* вроде бы даётся, наконец, некий намёк на соподчинение основных функций психики: «Функции П. заключаются в поиске определённых движений и действий, нацеленных на удовлетворение возникшей потребности, опробовании этих действий и контроле за их реализацией…» (*Рамендик Д.М., Одинцова О.В.*, 2004 , с. 10). Поиск, действия организма и контроль осуществляются ради удовлетворения актуальной потребности. И вдруг далее мы читаем: «Первичными являются среда и потребности живого существа, а П. возникает вторично, при их взаимодействии» (там же, с. 10). Мы видим странную вещь – то, ради чего осуществляются психические функции, потребности, рассматриваются вне психики! Они у авторов не встроены в П., а существуют как бы сами по себе. П. оказывается только надстраиваемым над потребностями неким обслуживающим их механизмом, не несущим в себе главных жизненных целей особи. Утрачивается целостное системное понимание психики как аппарата, несущего в себе как целеустремлённые управляющие процессы, так и сервисные исполнительные механизмы, работающие на их реализацию.

Такое «обновление» является скорее шагом назад по сравнению с пониманием П. у А.В. Петровского и М.Г. Ярошевского. Фактически из неё удалили управляющую, регулирующую функцию. Не учитывается важнейший фундаментальный факт организации всей психической жизни и поведения: образ, любой «отражаемый» признак, может стать дополнительным регулятором поведения только за счёт его предварительного *мотивирования*, т.е. придания ему направляющей и силовой, энергетизирующей дальнейший поиск и действия функции, *идущего от актуальной потребности*. Именно потребность или образованная на основе неё мотивация временно передаёт «отражению» эту способность быть управляющей силой, наделяет его *значимостью, «меткой предпочтения»*. Только в этом случае сам

процесс «отражения» становится биологически необходимой психической функцией, «осмысленным» процессом для организации поведения живого организма. Из наших рассуждений следует, что образ вторичен по отношению к актуальной потребности. Исходя из этого, ещё раз спросим, *логично ли выбрасывать первооснову построения любого поведения, потребность, из психики*?

У *В.К. Шабельникова* мы находим традиционное понимание психики: "Известно безусловно правильное понимание психики как идеального отражения материального мира" (*Шабельников В.К.*, 2004, с. 11-12). Но далее у Виталия Константиновича мы встречаем необычную мысль: "Действительным органом психики является не только мозг, а организм как единое целое" (*Шабельников В.К.*, 2004, с. 19). Мы уже знаем, что даже у одноклеточных существует специализация жизненных функций – ядро клетки отвечает за процессы деления и регулирования процессов белкового синтеза. «В цитоплазме большинства клеток находится ядро, координирующее жизнедеятельность клетки…» (*Регуляторные системы организма человека*. 2003. с. 17). Психика – это управляющий, организующий целостное поведение, центр всего живого организма. И эта ее управляющая функция, как и остальные помогающие, исполнительные функции, обеспечиваются у сложно организованного животного не печенью, сердцем или мышцами, а нервной системой и, вероятно, системой гормональной. Психика, конечно, влияет и на мышцы, и на сердце, и на любые другие внутренние и внешние органы тела. И они, безусловно, оказывают воздействие на психику. Но из факта этого взаимовлияния вовсе не следует, что все эти органы являются органами психики. И всё-таки вопрос о том, *что является органом психики, весь организм или его отдельные специализированные системы (или система*), остаётся актуальным и по настоящее время.

Здесь возникает и другой интересный вопрос, выходящий за рамки темы данной статьи: «*Существуют ли пределы, ограничивающие возможности управления, регулирования психикой телесных функций организма*?» Важно учитывать, что далеко не каждую команду психики организм готов выполнить. У него есть, видимо, и своя естественная защита, свои общие «задачи», которые нормальная психика и призвана осуществлять оптимальным образом. Скажите, например, себе "Не буду дышать 10 минут!". И засеките время. Через минуту-две организм заставит вас дышать, или, если вы будете очень упрямиться, просто умрет.

А вот ещё пример попытки современного «системного» определения психики. «В разных отношениях *психическое* открывается и как отражение действительности, и как отношение к ней, и как функция мозга, и как регулятор поведения, деятельности и общения, как природное и социальное, как сознательное и бессознательное» (*Барабанщиков В.А.*, 2004, с.4). У автора всё собрано в одной корзине. Возникают *те же вопросы о приоритетности различных функций психики, о характере их внутренней организации, соподчинения.*

Анализ некоторых альтернативных подходов к психике

Подошло время рассмотреть как сравнительно новые, так и старые представления о психике, альтернативные по отношению к традиционному её пониманию в отечественной психологии. Некоторые из них вносят какие-то новые акценты или особые характеристики в её понимание.

Б.А. Базыма свою статью о природе психики начинает с определения биологического взаимодействия. В его трактовке «современной биологией *жизнь* в самом общем виде рассматривается как система процессов метаболизма жизненного субъекта, то есть как система процессов его обмена с окружающей средой веществом и энергией» (*Базыма Б.А.*, 1999, с.9-18 http://www.colorpsy.boom.ru). На биологическом уровне «процесс жизнедеятельности может быть рассмотрен как процесс взаимодействия жизненного субъекта и различных природных объектов» (там же, http://www.colorpsy.boom.ru). Далее он предлагает рассматривать **психическое** как «взаимодействие *жизненных субъектов* между собой, опосредованное объектом, носителем информации. …Прежде всего, благодаря ему, у животных возникает специализированный аппарат, называемый нервной системой, обеспечивающий физиологическую базу взаимодействий. …Возникновение нервной системы и более-менее специализированных органов чувств может считаться точкой отсчёта и для возникновения *психического субъекта*. Кроме внешнего опосредования, возникает и внутренний опосредователь, главной задачей которого является декодирование-кодирование информации. При этом цель межсубъектного взаимодействия остаётся прежней – взаимная регуляция жизнедеятельности» (там же, http://www.colorpsy.boom.ru).

На мой взгляд, такой подход резко сужает функции психики, сводя их фактически лишь к одной коммуникации между

субъектами, к социальному взаимодействию. Верно, что одной из функций П. можно считать коммуникацию с другими живыми особями. Но это лишь одна из функций П., причём не главная, а, как мы увидим дальше, подчинённая более важной, целевой управляющей функции. Автор *частный* вид взаимодействия субъектов между собой объявил решающим в появлении психики и в её определении. Это очередной уход от фундаментального рассмотрения природы психики. *Неужели взаимодействие с природной средой, с собственным телом, со своими психическими возможностями и личностными особенностями у сложно организованных индивидов не входят в сферу проявлений психического*? Такое утверждение представляется просто абсурдным и не соответствующим очевидным фактам. Все эти виды взаимодействий, в том числе и «взаимодействие субъектов», совершаются с участием психики и преследуют жизненные метацели, общие всем живым существам, т.е. являются по большому счёту биологическими взаимодействиями.

Под «опосредующим объектом» *Б.А. Базыма* понимает тот же абиотический раздражитель, что и А.Н. Леонтьев. Но он трактуется узко как якобы препятствующий жизнедеятельности другого субъекта, предупреждающий его «Осторожно! Я здесь». Первоначально это метки, выделения, хорошо изученные в этологии территориального врождённого поведения животных. *Почему именно и только такого рода социальное коммуникативное взаимодействие между животными объявляется собственно психическим, остаётся непонятным*. Скорее это похоже на прихоть автора - социального психолога, увлечённого очередной, целиком социализирующей психику, идеей.

Важно также отметить, что психика, являясь частью и функцией целостного предмета - организма, сама оказывается встроенным в него внутренним предметом со своими особыми процессами. Взаимодействие с миром и со своими внутренними параметрами является функцией и проявлением, помимо прочего, и психической активности особи. Так что «взаимодействие субъектов» – это всегда результат, проявление действия их психик, а не сама психика. Здесь нужно ещё разбираться, что является первоначальной причиной, а что - следствием. Чтобы произошло психическое взаимодействие, необходимо «предварительное» наличие субъектов с особыми параметрами, с психикой, которая и позволяет в принципе совершать такое взаимодействие.

Целью межсубъектного взаимодействия провозглашается «взаимная регуляция жизнедеятельности». *Что кроется за этой*

«взаимной регуляцией», что она даёт взаимодействующим субъектам, остаётся неясным. А этот вопрос «для чего» остаётся центральным и решающим в понимании сущности психики, её предназначения и устройства.

Жизнь автором также рассматривается однобоко. Возникает концептуально решающий тот же «телеологический» вопрос: «*Зачем живой особи нужны процессы «обмена с окружающей средой веществом и энергией»*?» Автор не останавливает своё внимание на одной из главнейших особенностей живых существ, на том факте, что все виды их целостного поведения всегда **целенаправленны.** Это свойство изначально нести в себе и преследовать определённые жизненные цели является не только сущностным признаком любого живого существа, но и, как мне представляется, является одновременно и важнейшей характеристикой их психики. В подтверждение данного положения уместно привести слова крупнейшего современного биолога *К.Х. Уоддингтона*: «…Каждый данный вид создаёт такую картину внешнего мира, которая помогает этому виду использовать его для своих практических целей – для того, чтобы выжить и оставить потомство» (*Уоддингтон К.Х.* Основные биологические концепции / На пути к теоретической биологии. 1. Пролегомены. М.: Мир, 1970, с. 34. С.11-38). Не могу не привести здесь и ёмкое, красиво сформулированное мнение интересного барнаульского психолога *Д.В. Каширского*, перекликающееся со словами мэтра биологии: «Психика не столько отражает …сколько порождает новую смысловую реальность; она инструмент, трактующий Мир в пользу Организма…» (электронное сообщение мне от 16.12.2003 г.).

Рассмотрим еще один необычный современный подход к психике, представленный в работах *В.Н. Пушкина*. Им были организованы в лаборатории эвристики Психологического института РАО (ОМ - в 70-ые годы он назывался НИИ общей и педагогической психологии АПН СССР) «психолого-ботанические» эксперименты по изучению взаимодействия человек-растение. Испытуемому показывалось растение бегония и внушалось, что он является этим растением. Затем внушались очень позитивные или очень негативные события, происходящие с бегонией. Подбирались испытуемые с богатым воображением и высокой эмоциональностью. Реакция растения на состояние испытуемого и его изменение определялась с помощью электродов на листьях, регистрации его кожно-гальванической реакции КГР по Тарханову на энцефалографе.

Было показано, что прямая линия при «спокойном» состоянии человека сменялась на волны КГР при возникновении интенсивных эмоциональных переживаний у испытуемых, под влиянием внушённых им образов позитивных или резко негативных состояний растения, с которым они идентифицировали себя. «Некоторые факты, полученные в наших экспериментах, позволяют думать о том, что растение способно реагировать не только на момент изменения психологического состояния загипнотизированного человека, но и на внутренние конфликтные процессы, происходящие в его сознании» (*Дубров А.П., Пушкин В.Н.*, 1990, с. 88). В экспериментах сотрудника лаборатории эвристики О.И. Моткова со студентами театрального института, занимавшихся йогой, было доказано, что «субъекты, достигшие высокого уровня управления работой вегетативных систем организма, способны вызывать реакции растений без гипноза» (там же, с. 89).

Далее Вениамин Ноевич подытоживает результаты этих опытов: «…Эксперименты свидетельствуют о том, что лишённый нервной системы, состоящий из совокупности растительных клеток организм откликается на процессы, происходящие в нервной системе человека – существа, находящегося на высшем уровне биологической организации. Это обстоятельство со всей очевидностью свидетельствует об *общности* процессов переработки информации, осуществляющихся в соматических (растительных) и нервных клетках. …Реакции растительной клетки на психические (т.е. информационные) процессы, происходящие в нервных клетках, возможны лишь в том случае, если эти клетки «говорят на одном языке»… Поскольку …нервная клетка существенно моложе клетки растительной, то есть основания заключить, что психика человека и животных, т.е. информационная система поведения, непосредственно возникла из информационной системы жизни, из той системы кодирования и переноса информации, которая имеет место в растительной клетке» (там же, с. 89). «…Возникла необходимость в информационной системе, которая бы позволила таким существам (ОМ – животным) строить необходимые для регуляции поведения модели окружающей среды» (там же, с. 89-90). В другом месте В.Н. Пушкин пишет: «…психика выступает как некоторое свойство, присущее самой жизни, а не привнесённое в жизнь извне» (*Пушкин В.Н. и др.*, 1976, с. 169).

Мы видим, во-первых, что автор считает психику «информационной системой поведения», кодирующей и переносящей информацию, поступающую извне и изнутри, для

организации поведения. Во-вторых, психика выступает у него атрибутом любой жизни. Т.е. она есть и у одноклеточных, и у растений. Он подчёркивает общность и преемственность психических («информационных») механизмов в эволюционном ряду живых существ. Всё живое взаимосвязано и «чувствует» друг друга. С этой экспериментально и логически обоснованной точкой зрения нельзя не согласиться.

Среди психических процессов *В.Н. Пушкин* подчёркивал особую роль эмоций и потребностей в побуждении и регуляции поведения. «Эмоциональные процессы играют огромную роль в регуляции поведения животных и человека. Роль эта …связана с обслуживанием процесса удовлетворения важных для человека потребностей. …Эмоции создают на своём специфическом языке переживаний состояние напряжённости, которое толкает субъекта к действиям, ведущим к удовлетворению потребности. …Благодаря связи эмоционального переживания с потребностями субъекта эмоциональная сфера выступает в качестве побуждения к деятельности, в качестве важнейшего условия активности субъекта» (*Дубров А.П., Пушкин В.Н.,* 1990, с. 58).

Соглашаясь в целом с этими положениями о ведущей роли мотивационно-эмоциональной сферы в **управлении** поведением, т.е. в его побуждении, организации (программировании) и регуляции (контроле и коррекции текущих результатов и схем действий), нельзя в то же время не задать беспокоящие ум вопросы: «*И имеет ли смысл все психические процессы - мотивационные, эмоциональные, когнитивные, психомоторные, коммуникативные – называть обобщённо «информационными» процессами? Есть ли между ними существенная разница в их кодировании?»* Если разница есть, то, возможно, что **управляющие процессы,** их «когнитивные схемы», имеют особые «информационные» характеристики, особые метки, способы их обозначения в психике, связанные с мотивационными стремлениями и эмоциональными оценками, присущие только им, отличающие их существенно от процессов **исполнительных**. Такие информационные метки, видимо, дают им и особое, руководящее место в психической сфере (помимо, возможно, роли и самого их топологического расположения в организме).

Вениамина Ноевича очень интересовала «материальная основа психики». Он выдвинул тезисы о существовании во Вселенной особой психической материи, гипотезу о голографической природе психических образов. «…Материальное кодирование психики осуществляется не на клеточном и молекулярном, а на существенно

более глубоком, фундаментальном уровне. В связи с этим возникает идея весьма тонких биофизических процессов, которые происходят с использованием внутреннего пространства информационных молекул. …Раздражителем для растений в этих экспериментах может быть некая **биофизическая структура**, несущая в себе информацию о психическом состоянии человека. Экстериоризация этой структуры, происходящая в тот момент, когда человек осуществляет интенсивное эмоциональное переживание, вызывает в клетках растения электрическую реакцию» (там же, с. 90). И далее *В.Н. Пушкин* пишет: «…Материальный носитель идущего от человека сигнала должен содержать в себе самом некоторую *структуру образа* того живого объекта, к которому он был направлен. …Организм этот взаимодействует со своим образом, закодированном в сообщении, и в результате – кожно-гальваническая реакция именно данного растения, а не какого-либо другого. …Быть может, в данном случае …имеется взаимодействие образа как голографической волны с объектом как выражением устойчивой волновой структуры. Эта волновая гипотеза мира легко могла бы объяснить отмеченные в эксперименте взаимодействия» (там же, с. 93).

В другой статье *В.Н. Пушкин*, опираясь на голографическую гипотезу материального субстрата психики, делает попытку разъяснить, что происходит при порождении образа: «… Построение пространственных свойств объекта при восприятии может быть рассмотрено как процесс возникновения … стоячей волны, пространственные особенности распределения амплитуд которой соответствуют системе распределения амплитуд воспринимаемого объекта. …можно предположить, что волновая структура образов отражает реально существующую волновую структуру объектов нашего мира – Вселенной. …Язык человеческой психики с физической точки зрения представляет собой язык стоячих волн, язык голограмм» (*Пушкин В.Н. и др.*, 1976. с. 171). «…Мозг… располагает …возможностями фиксации, воспроизведения и оперирования с голографическими моделями-образами элементов окружающей среды. При этом волновым носителем… выступает квантово-механическая **Ψ-волна»** (там же, с. 174). «…информационные записи на соответствующих молекулах в нейронах целесообразно рассматривать как совокупность голограмм, каждая из которых, не будучи еще образом… представляет основу для создания этого образа. Образ или модель объекта возникает лишь в том случае, когда через записи такого

рода проходят пси-волны. …сами образы …локализуются не в коре, а в пространстве – подобно образу оптической голограммы» (там же, с. 176).

Вопрос о материальном носителе психической информации, конечно, важен. Уникальные исследования *В.Н. Пушкина* и других искателей истины существенно расширяют наши представления о материальном субстрате психики. Видимо, её материальным субстратом действительно могут быть как образования «грубой» материи (особые молекулы в ядре клетки и в её протоплазме - у одноклеточных и растений, нервная система, мозг у более сложных организмов), так и образования материи «тонкой» (системы стоячих волн как коды образа или потребности, или других «предметов» психики, специфические пси-волны, голографические психические образы). Эксперименты по изучению контакта между человеком и растением доказывают наличие психики и у растений, позволяют говорить о психике как существенной и обязательной характеристике любого живого существа. Однако, *внося большую ясность в наши фундаментальные представления о материальной основе психики и её наличии у простых организмов, эти исследования ещё не решают проблемы определения приоритетных, сущностных функций психики, соотношения специфических психических процессов друг с другом, проблемы её строения.*

Теперь попробуем глубже представить, что всё-таки происходит при взаимодействии человека с растением. Возможно, что КГР растения возникает не просто на транслируемый ему его же образ, как пишет *В.Н. Пушкин*, а в первую очередь на резкое, положительное или отрицательное, изменение эмоциональной окраски его образа. Когда образ испытуемого-растения насыщен мотивационно-эмоциональным зарядом, он предстаёт уже как особо отмеченный неосознаваемый образ-импульс. Видимо, эмоциональный заряд также кодируется каким-то способом в образе растения у испытуемого и в передающей его системе биофизических пси-волн. Этот особый *эмоциональный код* и придаёт высокую значимость образу, определяет его жизненность, его особая силу. Именно на этот острый эмоциональный компонент («специи») своего образа и реагирует в первую очередь растение. «Мне очень хорошо» - появляется реакция бегонии. «Мне очень плохо» - опять волновая реакция растения. Именно в этом видится не «мёртвое», а, как выражается *В.Н. Пушкин*, «живое кодирование живого существа» в передаваемом растению со стороны испытуемого образе. Ведь эмоции – одна из древнейших структур

психики наряду с первичными потребностями. Только такой, *эмоционально заряженный* образ, видимо, и воспринимает растение. *Элементарные механизмы потребностей и эмоций, видимо, есть и у растений?* Иначе они не могли бы реагировать на эмоционально окрашенные собственные образы, идущие от другого живого существа любого уровня биологической организации.

Кроме того, кажется правдоподобным, что образ растения, не осознаваемо транслируемый испытуемым этому растению, возможно, по гипотезе *В.Н. Пушкина*, с помощью биофизических пси-волн, уже имеется первоначально и у самого растения как некий образ или скорее как целостное чувство себя, своего «физического Я». При получении растением транслируемого ему испытуемым эмоционально окрашенного образа самого себя по *механизму резонанса* происходит мгновенное узнавание и активация образа себя. В случае ощущения резкой, например, негативной эмоциональной окраски этого образа себя в растении возникает состояние повышенной активации, связанное, вероятно, с оценкой этого ощущения как некоей опасности для себя, т.е. с активацией его потребности в безопасности. Растение выдаёт эту «эмоциональную» реакцию переживания опасности, которую и фиксирует прибор в виде волны КГР.

Т.е. можно сделать вывод, что живые управляющие психические процессы и живое «отражение» существенно отличаются от их неживых аналогов (процессов в холодильнике, компьютере, отражения в зеркале, и т.п.) в первую очередь наличием у них **мотивационно-эмоциональной** составляющей. Информация в психике – это в большей или меньшей степени целевая, значимая и эмоционально окрашенная информация. Психика изначально несёт в себе жизненные цели живого организма и возможности самоорганизации его жизнедеятельности в направлении их осуществления. Таких живых целей нет у любого предмета неодушевлённой природы.

К альтернативным по отношению к традиционным взглядам на сущность психики можно отнести и гораздо более ранние воззрения автора знаменитых «Мировых загадок» *Э. Геккеля*. Обобщив современные ему физиологические исследования одноклеточных, он пришёл к выводу о существовании психики у всех живых существ: «В своих «Психофизиологических исследованиях о протистах» (1889) он показал (ОМ – *Макс Ферворн*), …что предложенная мною (1866) «*теория клеточной души*» вполне подтверждается точным изучением одноклеточных простейших…»

(*Геккель Э.* Мировые загадки. М., 1920. С. 51-52). «Наибольшую же важность представляет тот факт, что и зародыш человека, подобно зародышам всех других животных, первоначально развивается из простой клетки...» (там же, с. 83). «Так как эта последняя с самого начала является «*одухотворённой*», то то же нужно допустить и относительно соответствующей *одноклеточной родоначальной формы*, которая в древнейшем ряду предков человека была представлена цепью различных *протозойных*» (там же, с. 145).

Мы видим, что *Геккель* считает «душу» (ОМ – т.е. то, что мы сегодня называем психикой) «безусловно общей принадлежностью всего живущего» (там же, с. 106). Фактически она является у него одним из сущностных признаков любого живого существа. Важно, что эта теория «биопсихизма» опиралась на эмпирические исследования простейших и растений, а также и на философское представление о единстве законов органического мира. Эти представления удивительно перекликаются с рассмотренными выше современными исследованиями «биоинформационного контакта человек-растение» *В.Н. Пушкина*, который тоже пришёл к выводу о наличии психики у любой живой особи, включая и растения. Другие современные учёные открыли наличие раздражимости и чувствительности у растений (*Д.Ч. Бос*), обнаружили электрические импульсы и другие процессы в растениях, имеющие «много общего с электрическими процессами, происходящими в организме животных и человека» (*И.И. Гунар, В.Г. Карманов*) (цит. по: *Пушкин В.Н.*, 1990, с.81). Таким образом, накапливается всё больше экспериментальных данных, подтверждающих правоту теории «биопсихизма». Если же мы возьмём во внимание представление академика *В.И. Вернадского* о том, что «живое вещество» не могло возникнуть из неорганической материи, и что жизнь, как и космос, вечны, то напрашивается вывод и о вечном существовании психики во Вселенной (*Вернадский В.И.*, 1960. Т. 5. С. 137).

Геккель связывал психику с определённой материальной субстанцией живого организма. «Все без исключения явления душевной жизни связаны с материальными процессами в живом веществе организма, в *плазме* или *протоплазме*. Мы назвали ту часть её, которая является непременным носителем души, **психоплазмой**…» (*Геккель Э.*, 1920, с. 107). «У человека и высших животных психоплазма …является дифференцированной составной частью нервной системы, *невроплазмой* ганглиозных клеток… у одноклеточных простейших психоплазма или тождественна со всей живою *протоплазмой* простой клетки, или

составляет некоторую часть её» (там же, 108). «Процессы низшей душевной жизни у одноклеточных простейших и растений …их раздражимость, их рефлекторные движения, их чувствительность и стремление к самосохранению прямо обусловлены психологическими процессами в *плазме* их клеток, физическими и химическими изменениями, которые могут быть объяснены отчасти *наследственностью*, отчасти *приспособлением*» (там же, с. 90).

У автора некая часть клеточного вещества «плазмы» или вся она является материальным носителем психики у живых существ, а физические и химические процессы в этой «психоплазме» обусловливают все их психические проявления.

Геккель солидарен с *Ромэнсом*, утверждавшим, что вся душевная жизнь человека отличается от таковой у животных любого уровня развития «лишь *степенью*, а не *родом*. Лишь количественно, а не качественно» (там же, с. 104). Такое представление опирается на более общий постулат о том, что «…органическая жизнь развивается на всех ступенях от одноклеточных простейших организмов до человека, под влиянием одних и тех же элементарных сил природы, складывается из физиологических функций ощущения и движения» (там же, с. 107). Т.е. общая первооснова, природный фундамент жизни и психики, в частности, является общим для всех живых организмов.

Здесь же автор выделяет и две основные элементарные «физиологические» функции психики, «ощущение и движение», которые он трактует очень широко: «К области ощущения в широком смысле относится чувство удовольствия и страдания …к области движения принадлежит соответственным образом *влечение* и *отвращени*е …стремление к достижению удовольствия и избежанию страдания» (там же, с. 123). *Геккель* подчёркивает, что «во всякой живой материи, во всякой протоплазме нужно уметь различать присутствие начальных элементов психической жизни, зачаточную форму чувствительности к *удовольствию* и *страданию*, зачаточную форму *влечения* и *отвращения*» (там же, с. 106). Т.е. **элементарными функциями, «начальными элементами» психики** у него фактически являются функции и механизмы мотивации и эмоций! Это удивительно, если сравнить такой подход с рассмотренным выше определением важнейшей функции психики в традиционной отечественной психологии (может быть, это и к вопросу о том, к чему приводят размышления и усилия независимого и зависимого от господствующей идеологии ума).

Какие же элементарные влечения определяются как основополагающие у нашего естествоиспытателя и философа, как составляющие каркас и, возможно, представляющие главную движущую силу психики и поведения организма?

В параграфе об инстинктах *Геккель* так отвечает на этот вопрос. «…Инстинкты существуют у *всех* организмов, у всех протистов и растений, так же, как и у всех животных и человека … *Первичные инстинкты* суть общие низшие влечения, присущие психоплазме с самого начала органической жизни (!) и бессознательные, прежде всего стремление к самосохранению (защита и питание) и сохранению вида (размножение и уход за потомством). Эти два **основных влечения** органической жизни, *голод* и *любовь*, первоначально у всех возникают бессознательно, без участия рассудка или разума…» (там же, 120). «Уже на самой низкой ступени органической жизни мы находим у всех протистов те элементарные ощущения удовольствия и страдания, которые проявляются в их так называемых *тропизмах*, в *стремлении* к свету или темноте, к теплу или холоду, в различном отношении к положительному или отрицательному электричеству. …Автоматические, так же как и рефлекторные движения, которые мы уже наблюдали у всех одноклеточных протистов, являются следствиями *стремлений*, неразрывно соединённых с самым понятием жизни» (там же, с. 123-124).

Пожалуй, *Геккель* – это первый автор, который ясно сказал о наличии у любого живого существа первичных влечений или, как мы сегодня их называем, потребностей. И причинно связал автоматические и рефлекторные движения, «реакции на биотические и абиотические раздражители», с действием первичных стремлений. Эти движения и реакции являются результатом функционирования первичных стремлений, подчинены их управляющему, направляющему и побуждающему действию. Более того, в одной фразе он подчеркнул и то, что наличие первичных стремлений является сущностной характеристикой любого живого организма! Смею предположить, что *потребности, обеспечивающие жизненную целенаправленность, активизацию процессов общей и оперативной организации (управления) поведения организма для осуществления содержащихся в них его жизненно важных требований, являются самой важной и главной отличительной чертой всякого живого существа*. Можно согласиться (с некоторой оговоркой) с нашим скромным профессором и с тем, что первичны именно влечения к самосохранению и сохранению жизни вида или рода. Однако я не нашёл у *Э. Геккеля* разъяснения,

исчерпывается ли список безусловно важных «первичных влечений» организма только теми, которые он осветил в своём замечательном тексте? Эти встроенные природой в «душу» живой особи первопричины её поведения следует, скорее всего, дополнить и некоторыми другими, также обеспечивающими её общее благополучие, о чём речь пойдёт несколько ниже.

В целом логика и смелые обобщения *Э. Геккеля* будят мысль и заставляют шире смотреть на фундаментальные вопросы сущности жизни и психики.

Авторское понимание функций психики и её строения

Настала пора изложить по возможности кратко собственные ответы на поставленные вопросы. Конечно, они носят, как и любые другие интерпретации имеющихся фактов, гипотетический характер. Я старался, по мере возможности, руководствоваться целостным, предметным, естественно-научным подходом к рассмотрению психики, её строения и развития, и опираться как на экспериментальные биологические и психологические данные, так и на мнения известных учёных. Методологический *принцип предметности* здесь означает, что в любой природной вещи можно и нужно находить одновременно как её особенный материальный субстрат, так и её специальные функции (*Мотков О.И.*, 2008).

У. Джемс при анализе психики особое внимание обращал на её назначение в живом организме (*Джемс У.*, 1991). Такой же вопрос в первую очередь волновал и меня при попытках понять сущность главных её функций. И вот предварительный вывод: **психика** – это специальные орган и система функций живого существа, отвечающие, прежде всего, за целостное построение его оптимального поведения по удовлетворению изначально встроенных в него жизненных целей (потребностей) и образующихся в течение жизни производных от них мотиваций, за его общее благополучие. Т.е. она предстаёт, прежде всего, как центральный организатор и регулятор целостного поведения всего организма.

Я солидарен с данными и мнением Эрнста Геккеля, В.Н. Пушкина и других авторов о том, что психика есть у *любого* живого организма, в том числе у одноклеточных простейших и у растений. Они также изначально обладают жизненными стремлениями, «общими тенденциями направления» (*Э. Кречмер*), которые руководят построением их пусть и примитивного, но целостного поведения (*Кречмер Э.*, 1927, с. 108). Таким образом, потребности

имеются у *всех* живых существ. Именно они несут в себе фундаментальные требования организма, включают, запускают процессы целостной самоорганизации его поведения и прекращают эти процессы при констатации наступления ожидаемого приспособительного эффекта. Помимо потребностей, у живых особей есть и раздражимость и чувствительность, и движения – реакции на биотические и абиотические раздражители. У низших живых существ обнаруживаются только побуждающая, направляющая и автоматически регулирующая *управляющие функции* их потребностей. У них ещё отсутствуют в целом подчиняющиеся потребностям специальные аппараты, выполняющие ситуативное и долговременное программирование поведения. Хотя на элементарном уровне уже наблюдаются и зачатки программирования, в виде учёта не только биотических, но и абиотических стимулов, которые увязываются с будущим появлением стимулов биотических. Мы приходим к выводу, что психические функции в целом являются важнейшим сущностным признаком *любого* живого организма.

Л.С. Выготский, на мой взгляд, ухватил самую суть вопроса, когда писал в 1925 году в Предисловии к книге А.Ф. Лазурского «Психология общая и экспериментальная»: «Новая психология исходит из инстинктов и влечений, как основного *ядра психики*…» (*Выготский Л.С.*, 1925, с. 23). Мысль о том, что потребности («влечения», «импульсы» инстинкта) запускают поведение и осуществляют общее управление поиском, восприятием и действиями, присутствует у многих физиологов, этологов и психологов. Об этом писали Э. Геккель, У. Джемс, Ч.Л. Морган, У. Мак-Дауголл, А.Ф. Лазурский, Л.С. Выготский, Г. Мюррей, П.К. Анохин, П.В. Симонов, К.Х. Уоддингтон, К. Левин, А. Маслоу, К. Обуховский, В.Р. Дольник и др. Об их главном месте в психике и культуре человека говорили антропологи Б. Малиновский, Х. Шельски, и пр. Б. Малиновский, например, так характеризовал назначение культуры человеческого общества: «*Культура*… предоставляет человеку лучшие возможности решения конкретных проблем, возникающих в ходе приспособления к окружающей среде *и удовлетворения потребностей*» (цит. по: *Обуховский К.*, 1972, с. 83-84).

Утверждать, после всех этих наработок, что потребности не относятся к психике и к личности, выносить потребности в своей теории за их пределы, как это делают некоторые российские авторы, представляется мне совершенно нелогичным действием,

противоречащим очевидным фактам, разрушающим целостное понимание сущности и функций психики.

На основе анализа множества жизненных наблюдений и подходов как биологов, так и психологов, я пришёл к убеждению, что *потребности* составляют ядро психики любого живого существа. Они и являются первым характерным признаком «высокоорганизованной материи», так как отвечают за оптимальную самоорганизацию поведения особи, за поддержание её общего оптимального функционирования. «Высокая» организация живого в первую очередь и состоит в способности к самоподдержанию своих жизненных параметров, включая и энергетические, чего нет в любом сложнейшем механизме – компьютере, роботе, космическом корабле. Очень вероятно, что именно наличие жизненных целей и самоорганизации поведения по их осуществлению и отличает в первую очередь всё живое от неживых предметов.

Мы рассмотрели различные подходы и к *материальному субстрату психики*. И признали, что психика является специальным органом и особыми функциями тела любого живого организма, содержит в себе его интегральные требования и чаяния, изначально присущие ему жизненные цели, а также инструменты познания, коммуникации, ясного видения и действования во внешнем и внутреннем мире. Данные исследований показали, что психические функции обнаруживаются и у живых существ, не имеющих нервной системы и мозга (Геккель Э., Ферворн М., Д.Ч. Бос, И.И. Гунар, Пушкин В.Н., Гиппенрейтер Ю.Б., и др.). Мой общий вывод заключается в следующем. Материальным субстратом психики могут быть, во-первых, образования «плотной» материи (особые молекулы и их компоненты в ядре клетки и в её протоплазме - у одноклеточных и растений, или нервная система, мозг - у более сложных организмов). Во-вторых, по всей видимости, и образования «тонких» биофизических структур, в виде системы стоячих волн как кодов образа или потребности, специфических пси-волн, «оживляющих» эти коды, объёмных голографических психических образов.

Проблема определения факторов и закономерностей функционирования психических волновых структур ещё далека от своего окончательного решения.

Для некоторых психологов остаётся не до конца ясным вопрос о *сферах функционирования, взаимодействия психики*. Здесь можно дать чёткий, недвусмысленный ответ. С помощью психики живое существо активно взаимодействует как с особенностями своего *тела*,

так и с различными факторами *природного* и *социального* окружения, в котором оно изначально находится. При рассмотрении сфер действия личности мы увидим, что к этим трем средам взаимодействия необходимо добавляются еще две внутренние области рефлексии – собственные характеристики *психики* и *личности*. Т.е. очевидно, что взаимодействие психики с внешним окружением не сводится лишь к взаимодействию с социумом. Не меньшую роль в её функционировании и развитии играет взаимодействие с параметрами собственного организма, с живой и неживой природной средой, а также с психологическими самохарактеристиками (рис. 1). Психика призвана Природой организовывать оптимальное взаимодействие со всеми возможными сферами бытия организма, как внутренними, так и внешними.

Во многих рассмотренных мною подходах к психике не определено *соотношение, соподчинение функций психики*. Такие её функции как «отражение» признаков внутренней и внешней среды, организация и регуляция поведения, обеспечение коммуникации и движения рядоположены у большинства авторов, хотя в действительности они достаточно чётко структурированы. Сама логика построения психики уже указывает на *приоритетное место* в ней определённых функций и органов.

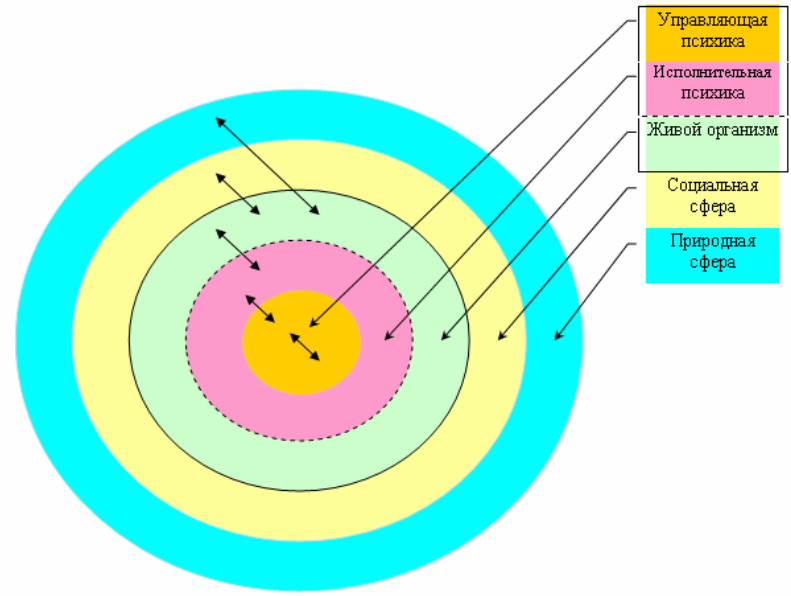


Рис. 1. Сферы взаимодействия психики и личности (Управляющей психики)

В самом общем плане психику можно представить как функционально, так и субстанционально в виде двухблоковой, частично саморегулируемой, структуры (рис. 2).

Это, во-первых, блок *управляющих,* мотивационно-эмоциональных функций - побуждающих, направляющих, интегрирующих, программирующих и регулирующих (контролирующих и корректирующих). И во-вторых, блок функций *исполнительных* - познавательных, коммуникативных, психомоторных и функции осознания. Управляющий и Исполнительный блоки психики постоянно взаимодействуют друг с другом. Древним ядром управляющих функций являются базовые, первичные потребности. Более подробное описание состава этих блоков можно найти в моей книге «Личность и психика. Сущность, структура и развитие». Самара: Бахрах-М, 2008.

Рис. 2. Общая структура психики

Ещё раз обратим внимание на то, что психика в первую очередь выполняет функцию центрального организатора и регулятора жизненных процессов, осуществляет саморегуляцию состояний всего организма. Поэтому логично предположить, что главными в психике являются функции её центрального управляющего блока, заключающиеся у сложноорганизованных организмов в побуждении, направлении, оперативном программировании и регуляции поведения по удовлетворению их актуальных потребностей. Все эти вместе взятые функции я для краткости обозначаю как управляющие функции. Они представлены у сложноорганизованных организмов специальной системой отделов нервной системы – гипоталамусом, лимбической системой, некоторыми подкорковыми ядрами, а также базальными, медиальными и префронтальными отделами лобных долей коры головного мозга (А.Р. Лурия, П. Лафренье - о триедином мозге МакЛина, Э. Голдберг, П.В. Симонов, Регуляторные системы…, и др).

В связи со сказанным *Управляющую психику* имеет смысл рассматривать как **личность** индивида. У высокоорганизованных животных и человека она имеет иерархическое многоуровневое строение (см. подробнее: *Мотков О.И.*, 2008). Под субъектом же логично понимать лишь *оперативный, «диспетчерский» отдел личности* - аппарат оперативного программирования, регуляции и контроля поведения «здесь и теперь», представленный в нервной системе животных и человека подкорковыми ядрами стриарного тела, миндалины и корковыми префронтальными зонами лобных долей большого мозга (*Мотков О.И.,* 2008а). Возможно, что у одноклеточных и растений оперативные функции субъекта определяются имеющимися у них молекулярными управляющими регуляторными образованиями. Этот вопрос ещё ждёт своего дальнейшего изучения.

«Отражение», т.е. на психологическом языке познавательные процессы ощущения, восприятия и др., дают возможность индивиду проанализировать, понять как внешние особенности текущей ситуации, так и свои внутренние характеристики, и на основе результатов этого анализа организовать целесообразное поведение по осуществлению актуальной потребности (желания, мотива, цели и т.п.). Мы видим, что «отражательные», поисковые, мыслительные, коммуникативные, психомоторные функции, а также процессы осознания, являются лишь *психическими средствами*, подчиняющимися центральным управляющим психическим процессам животного или человека - постоянным мотивационно-эмоциональным и оперативным программирующим и регулирующим процессам и органам. Поэтому я называю их исполнительными функциями психики. Вместе с соответствующими, осуществляющими их, органами они составляют *Исполнительную психику* организма. Об этой обслуживающей функции исполнительных психических процессов говорили Э. Геккель, А.Ф. Лазурский, Л.С. Выготский, Э. Кречмер, Д.Э. Когхилл, Ч.Л. Морган, Н.А. Бернштейн, К.С. Лешли, У. Пенфилд, П. Лафренье, П.В. Симонов, А.В. Либин, А. Маслоу, В.Р. Дольник и др.

С учётом воззрений этих авторов можно определить следующие *генеральные закономерности строения и развития психики*:

- отдельные частные психические функции подчиняются целостной стержневой жизненной направленности психики и общей интегральной преструктуре поведения, т.е. психические функции изначально иерархизированы;

- мотивационные производные, в виде мотивов, целей, намерений и т.п., а также все исполнительные психические процессы, подчиняются в конечном итоге в ходе своего функционирования общему тренду – требованиям породившей их первичной потребности (*Г.А. Мюррей*: «Потребность – это конструкт…, обозначающий силу (неизвестной физико-химической природы), которая *организует* восприятие, апперцепцию, интеллект, волю (conation) и действие таким образом, чтобы изменить в определенном направлении имеющуюся неудовлетворительную ситуацию» - цит. По: *Хекхаузен Х.*, 2003, p. 123-124);

- ситуативные, переменчивые психические образования дополняют и конкретизируют более постоянные и устойчивые компоненты психики (*Э. Кречмер*: «…и самые изменчивые в отдельных своих выполнениях человеческие действия в своей основе имеют инстинктивный компонент; *общая тенденция направления* твёрдо вложена наследственно, специальное выполнение варьирует сообразно интеллекту» - *Кречмер Э.*, 1927, с. 108);

- каркасом прижизненно образующихся функциональных систем всегда являются природные первичные функциональные системы (*Ч.Л. Морган*: «Инстинкт очерчивает контуры поведения, а опыт добавляет к ним тени и краски» - цит. По: *Боровский В.М.*, 1935, с. 24);

- активизация исполнительных психических процессов обусловлена влиянием первичных влечений, потребностей (*Э. Геккель*: «Автоматические, так же как и рефлекторные движения, которые мы уже наблюдали у всех одноклеточных протистов, являются следствиями стремлений, неразрывно соединённых с самым понятием жизни» - *Геккель Э.*, 1920. с. 124).

- наследственно обусловленная интеграция психики диктует свои условия опыту, во многом подстраивая его под свои нужды (*Д.Э. Когхилл*: «С самого начала имеется известный порядок (ОМ – в психике и организме животного), доминирующий над опытом» - *Когхилл Д.Э.*, 1934, с. 68);

- более древние структуры мозга и соответствующие психические функции не исчезают в ходе эволюционного развития и не подавляются более молодыми и поздними образованиями, а продолжают свою простую, но важную организаторскую и исполнительную работу (т.е. сохраняется преемственность в общей направленности и в структуре поведения, общий природный

«гештальт» при образовании новых мозговых структур и психических функций);

- мотивационно-эмоциональные управляющие структуры созревают быстрее, чем механизмы исполнительных процессов – мотивация ведёт за собой как целостное психическое развитие, так и обучение.

Таким образом, познавательные, психомоторные, коммуникативные, «осознавательные» процессы, «культурные» образования опыта всегда работают на удовлетворение каких-то потребностей, желаний и интересов, выполняют приспособительную задачу. Их активность поддерживается или прекращается мотивацией и выражающими её состояния эмоциями. Косвенно об этом хорошо сказал *П.В. Симонов*: «…Решающую роль в реализации выбора реакции с более или менее ценным подкреплением играет *влияние мотивационных структур гипоталамуса на передние отделы новой коры*, но отнюдь не обратное влияние "интеллектуальных" структур коры на мотивационную сферу. …Б. Спиноза: страсти побеждаются не разумом, но более сильными страстями» (*Симонов П.В.*, 1998, с. 35).

Частные и прижизненно образующиеся психические функции присоединяются, встраиваются в природные первичные функциональные системы психики организма. Актуальная потребность является *динамическим системообразующим центром*, движителем любой функциональной системы поведения. Она интегрирует, объединяет и подключает на время своего осуществления в совместную работу различные частные, более конкретно и ситуативно ориентированные, мотивационные механизмы, организует создание новых ситуативных целей (осуществляет вместе с оперативным аппаратом субъекта целеполагающую функцию), а также активирует необходимые психические и телесные исполнительные органы и процессы.

Можно заключить, что важнейшая и главная функция психики заключается в организации и регуляции оптимального поведения по осуществлению актуальных потребностей индивида, с учетом своих физических и психологических возможностей и особенностей окружающей природной и социальной среды.

Последнее, что хотелось бы рассмотреть, это **состав первичных потребностей** *всех* живых существ. *Э. Геккель* в этой связи отмечал, что «…*первичные инстинкты* суть общие низшие влечения, присущие психоплазме с самого начала органической жизни и бессознательные, прежде всего стремление к

самосохранению (защита и питание) и сохранению вида (размножение и уход за потомством). Эти два *основных влечения* органической жизни, *голод* и *любовь*, первоначально у всех возникают бессознательно, без участия рассудка или разума…» (*Геккель Э.*, 1920, с. 120).

Э. Кречмер выделял три главных жизненных стремления: «…Как влечения, следует обозначить аффективные тенденции, которые группируются вокруг трёх …главных жизненных пунктов: принятия пищи, охраны от опасности и размножения. Первые два можно противопоставить …как влечения *к самосохранению*, влечениям *сохранения рода*» (*Кречмер Э.*, 1927, с. 161).

У *П.В. Симонова* мы находим развёрнутую картину потребностей (безусловных рефлексов). «…Центры наиболее сложных безусловных рефлексов обнаруживаются в гипоталамусе, являясь, по сути, центрами биологически значимых потребностей» (*Регуляторные системы организма человека*. 2003, с. 198). «Типы безусловных рефлексов (по П.В. Симонову). *Витальные*: пищевые, питьевые, пассивно- и активно-оборонительные, гомеостатические, груминг, рефлекс экономии сил. …Витальные рефлексы можно определить как направленные на сохранение самой жизни индивидуума. *Зоосоциальные*: половые, детское и родительское поведение, территориальные, стайные (иерархические). …Те варианты врождённого поведения, которые возникают при взаимодействии с другими особями своего вида. *Саморазвития*: исследовательские, рефлекс свободы, подражательные, игровые. …Реакции, не связанные с адаптацией к текущей ситуации, а как бы «обращённые в будущее» (*там же*, с. 202). «…Они (ОМ – безусловные рефлексы, потребности) являются той основой, на которой «растёт» всё многообразие поведения. Проследив даже самые сложные приобретённые реакции, мы можем обнаружить их врождённый фундамент, который в своё время явился как бы «источником энергии», позволившей реализовать процессы обучения» (*там же*, с. 212). Добавим, что «врождённый фундамент» является не только «источником энергии», но и задаёт с помощью своих безусловно значимых «когнитивных схем» общие метанаправления выстраиваемого поведения.

Итак, обобщая, можно констатировать, что *Э. Геккель, Э. Кречмер* и наш современник *П.В. Симонов* выделяют у живых существ витальные и зоосоциальные метапотребности *самосохранения своей жизни и жизни рода*, а также метапотребности *саморазвития*. Соглашаясь в принципе с таким определением основных жизненных целей всех

биологических особей, хотелось бы обратить внимание ещё на одну метапотребность, присутствующую, как мне представляется, также у всех живых существ. Это потребность в *оптимальном, гармоничном функционировании,* в хорошем процессе жизни. О её различных проявлениях писали нейрофизиологи и психологи К. Юнг, К.С. Лешли, А. Маслоу, К. Роджерс, К..М. Шоломий, Г.А. Голицын и В.М. Петров.

К.С. Лешли приводил примеры наличия саморегуляции в нервной системе: «…Даже деменция не является совершенно бессмысленной. Она заключает в себе снижение уровня понимания и сложности тех отношений, которые могут быть поняты, но то, что больной может выполнить, он выполняет в упорядоченной и осмысленной форме. …Очевидно, всегда наступает известная *спонтанная компенсация* или приспособительная реорганизация. …Такого рода явления показывают, что нервная система обладает способностью к саморегуляции, придающей *связный, логический характер её функционированию* независимо от того, каково нарушение составляющих её анатомических элементов» (*Лешли К.С.*, 1930, с. 310-311). Физиолог *В.А. Дубынин* и др. говорят об известном феномене угашения рефлексов: «При длительном неиспользовании условных рефлексов идёт их *самопроизвольное* угашение («забывание»). Угашение – биологически важное приспособление, благодаря которому организм перестаёт напрасно тратить энергию и реагировать на сигнал, потерявший своё значение» (*Регуляторные системы*…, 2003, с. 246). Это пример психофизиологической автоматической саморегуляции в психике, облегчающей и делающей более экономным её функционирование. Биологи *Г.А. Голицын и В.М. Петров* рассуждают о биологических принципах оптимальности строения и поведения живых существ: «…В основе гармонии живого лежит точный расчёт, равновесие сил, экономия ресурсов, максимальное использование благоприятных возможностей…» (*Голицын Г.А., Петров В.М.*, 1990, с. 6). «При прочих равных условиях оптимальной структурой …будет такая, которая обеспечивает наименьший расход метаболической энергии (достаточный в то же время для нужд организма)» - *Розен Р.*» (там же, с. 20).

В психологии давно известен факт автоматизации успешных действий, который также приводит к *более экономному функционированию* психики: «Все успешные программы поведения стремятся к автоматизации…» (*Ловелле Р.П.*, 2004, http://www.terpsy.ru). В своих «Психологических типах» *К. Юнг*

подчёркивал, что «…Каждому выраженному типу присуща особая тенденция к компенсации односторонности его типа, тенденция, которая биологически целесообразна, так как она стремится удержать душевное равновесие» (*Юнг К.*, 1927, с. 6). Т.е. оптимальное функционирование психики – это и *разнообразное* её действие. *А. Маслоу* утверждал, что «мускулистому человеку нравится использовать свои мускулы, более того, он должен их использовать во имя своей самоактуализации и обретения чувства гармоничного, свободного, приносящего удовлетворение функционирования, которое является важнейшим аспектом психического здоровья» (*Маслоу А.*, 1997, с. 189). Здесь оптимальное функционирование – это и *более полное самовыражение психических и телесных потенциалов*. Близкий подход к психическому функционированию у человека мы находим у К. Роджерса, которые определил пять признаков «полноценно функционирующих людей», признаков «хорошей жизни». Он подчёркивал, что «хорошая жизнь – это процесс, а не состояние бытия», что это «возрастающая открытость опыту», *более полное функционирование* в настоящем с доверием своему организму, своим ощущениям себя, *свободная и творческая организация жизни* и её протекание (*Роджерс К.*, 1994, гл. 9).

К. Обуховский, рассматривая «нормальное функционирование», приводит слова К. Гольдштейна о *тенденции особи к поддержанию оптимального уровня напряжения организма*: «Концепция *Гольдшейна* (1939)… Организм… имеет постоянное среднее состояние напряжения и к этому состоянию старается вернуться, как только наступает какое-либо отклонение. …Все созревание, накапливание жизненного опыта – это не что иное, как только *стремление к сбалансированию напряжения*, что практически означает стремление избежать фрустрации и внутренних конфликтов». (*Обуховский К.*, 1972, с. 76). Можно обозначить тенденцию к оптимальному напряжению как *стремление к умеренному функционированию* - по общим затратам сил, по силе желаний, притязаний и по другим проявлениям. По моим экспериментальным данным, это стремление и его ценность усиливаются с возрастом.

Российский психолог *К.М. Шоломий* в оригинальных экспериментах показал, что «существует *оптимизирующая саморегуляция* мышления …непроизвольный психический процесс, протекающий параллельно умственной деятельности …и направленный на её совершенствование» (*Шоломий К.М.*, 1979, с. 77). Это «автоматически действующий психологический механизм, который выполняет функцию слежения за текущей мыслительной деятельностью с

точки зрения её оптимальности» (*там же*, с. 82). «Переход к *более оптимальной*, *энергетически лёгкой и более рациональной модели работы* происходит спонтанно и непроизвольно – это всеобщее свойство мышления» (*там же*, с. 81). Оптимизирующая саморегуляция, видимо, является проявлением изначальной общей метапотребности в гармоничном функционировании. Её неосознанное протекание может указывать на то, что она присутствует не только у человека, но и у высших и низших животных, и даже, возможно, у одноклеточных и растений. У людей она может иметь не только спонтанный неосознаваемый характер, но и становиться осознанной целью гармонизирующего саморазвития, вполне произвольным процессом.

Таким образом, приведенные данные позволяют выделить три вида самых общих метапотребностей живых существ: жизненное стремление к самосохранению и сохранению рода, потребность в саморазвитии и жизненное стремление к оптимальному, гармоничному функционированию. Эта последняя потребность имеет как общие для всех живых организмов характеристики (экономичное расходование сил, поддержание оптимального напряжения, поддержание достаточного разнообразия видов поведения, необходимой полноты жизненных проявлений, и т.п.), так и, вероятно, видоспецифичные и индивидуальные особенности построения «хорошей жизни».

В заключение отмечу, что в данной работе я намеренно не касался сложных вопросов различия между психикой человека и животных. Такая тема требует специального рассмотрения и анализа. Здесь же уместно привести лишь связанную с этой проблемой основополагающую мысль философского антрополога *Макса Шелера*: «…всякий «подлинно человеческий акт» изначально «двойственен»: одновременно духовен и инстинктивен …Каждый феномен человеческой жизни …единство инстинктивно-витальных и культурно-духовных начал…» (*Шелер Макс.* В: «Современная западная социология». М., 1990, с. 397. *Ю.Н. Давыдов*).

Литература

1. БАЗЫМА Б.А. *К вопросу о природе психики* //Вестник Харьковского университета. Серия “Психология”, №432, 1999, с.9-18 http://www.colorpsy.boom.ru
2. БАРАБАНЩИКОВ В.А. *Принцип системности в психологии*/ Психология: Журнал Высшей школы экономики. 2004. Т.1, № 3, с.3-17.

3. БОРОВСКИЙ В.М. *Вопрос об инстинктах в трудах Ч.Л. Моргана* / Инстинкты, навыки: Психол. исследования. Т. 1. Отв. Ред. В. Боровский. М.-Л-д: Соцэкгиз, 1935. С. 13-32
4. ВЕРНАДСКИЙ В.И. *Собр. соч.* М.: Изд-во АН СССР, 1960. Т. 5. С. 120-142
5. ВЫГОТСКИЙ Л.С. *Предисловие* к кн. *Лазурского А.В.* Психология общая и экспериментальная. Лен-д: Госиздат, 1925 , с. 5 – 23.
6. ВЫГОТСКИЙ Л.С. *Игра и ее роль в психическом развитии ребенка*/Журнал Психол. общества им. Л.С. Выготского. 2000, № 1, с. 2-18.
7. ГЕККЕЛЬ Э. *Мировые загадки*. М.: Братья А. и И. ГРАНАТ и К°, 1920 – 410 с.
8. ГЕЛЬГОРН Э., ЛУФБОРРОУ Д. *Эмоции и эмоциональные расстройства*: Нейрофизиологическое исследование. М.: Мир, 1966 – 672 с. Пред. *П.К. Анохина*
9. ГИППЕНРЕЙТЕР Ю.Б. *Введение в общую психологию*. М., 1996. Гл. 11. Происхождение и развитие психики в филогенезе. Объективный критерий психики. С. 169-197 (Интернет)
10. ГОЛДБЕРГ Э. *Управляющий мозг: Лобные доли, лидерство и цивилизация*. М.: Смысл, 2003 – 335 с.
11. ГОЛИЦЫН Г.А., ПЕТРОВ В.М. *Гармония и алгебра живого*: *В поисках биологических принципов оптимальности*. М.: Знание, 1990
12. ДЖЕМС У. *Психология*. М.: Педагогика, 1991
13. ДОЛЬНИК В.Р. *Вышли мы все из природы*. М.: LINKA-PRESS, 1996
14. ДУБРОВ А.П., ПУШКИН В.Н. *Парапсихология и современное естествознание*. М.: Соваминко, 1989 – 280 с. (Части 1 и 2 написаны В.Н. Пушкиным)
15. КАШИРСКИЙ Д.В. (*электронное письмо* для ОМ от 16.12.03)
16. КОГХИЛЛ Д.Э. *Анатомия и проблема поведения*. Пер. с англ. и ред. В.М. Боровского. М.-Л-д: Биомедгиз, 1934 – 88 с.
17. КРЕЧМЕР Э. *Медицинская психология*. М.: Жизнь и Знание, 1927
18. ЛАЗУРСКИЙ А.Ф. *О составе личности.*//Психология личности в трудах отечественных психологов. Сост. Куликов Л.В. СПб: Питер, 2000; 480 с.
19. ЛАФРЕНЬЕ П. *Эмоциональное развитие детей и подростков*. СПб: прайм-ЕВРОЗНАК, 2004 – 256 с. (Emotional development. A biosocial perspective).
20. ЛЕОНТЬЕВ А.Н. *Проблемы развития психики*. М., 1972
21. ЛЕОНТЬЕВ А.Н. *Психика* / БСЭ. Т. 21. М.: Сов. энциклопедия, 1975. С. 187 . На сайтах www.tests.pp.ru/library/encyclopedia/psyche.phtml http://slovari.yandex.ru/dict/bse/article/00063/69900.htm
22. ЛЕШЛИ К.С. *Основные нервные механизмы поведения* / Ж. Психология. Т. III. Вып. 3. Отв. Ред. К.Н. Корнилов, 1930 – с. 293-315.

23. ЛИБИН А.В. *Дифференциальная психология*: На пересечении европейских, российских и американских традиций. М.: Смысл, 2000 - 549 с.
24. ЛОВЕЛЛЕ Р.П. *Ядро личности, невротические симптомы и эффект психотерапии*/ Статья в Интернете, ноябрь 2004 (http://www.terpsy.ru)
25. ЛУРИЯ А.Р. *Основы нейропсихологии*. Учеб. пос. М.: Академия,, 202 – 384 с.
26. ЛУРЬЕ С.В. *Психологическая антропология*: история, современное состояние, перспективы. Учеб. пос. М.: Академический Проект: Альма Матер, 2005 – 624 с. С. 79 – (*Б. Малиновский*). Культура как инструмент удовлетворения психобиологическиъх потребностей.
27. МАСЛОУ А. *Психология бытия*. М. Рефл-бук, Ваклер, 1997; 304 с.
28. МАСЛОУ А. *Мотивация и личность*. СПб: Евразия, 2001 – 478 с
29. МОТКОВ О.И. *О природе высших психических функций* /Перспективы развития культурно-ист. теории. Мат-лы VII Межд. чтений памяти Л.С. Выготского (14-17 ноября 2006). Ред. проф. В.Т. Кудрявцев. М., 2006. С. 62-68.
30. МОТКОВ О.И. *Природа личности: сущность, структура и развитие*. М.: ГУП Воскресенская типография, 2007 – 248 с.
31. МОТКОВ О.И. *Личность и психика*. Сущность, структура и развитие. Самара: Бахрах-М, 2008 – 160 с.
32. МОТКОВ О.И. *Субъект как оперативный блок личности* / Д.А. Ошанин и современная психология: к 100-летию со дня рожд. Д.А. Ошанина. Ред. И.В. Панов и Н.Л. Морина. М.; Обнинск: ИГ-СОЦИН, 2008а – 292 с. С. 210-236. Также на сайтах: http://psychology.rsuh.ru/archive/motarticle26.rtf и http://hpsy.ru/public/x3251.htm
33. МЮРРЕЙ Г.А. / *Хекхаузен Х. Классификация мотивов на основе отношений личности и окружения: Генри А. Мюррей*/ *Хекхаузен Х. Мотивация и деятельность*. СПб, 2003. С. 126-130. На сайте www.psychology-online.net (Научная и популярная психология)
34. ОБУХОВСКИЙ К. *Психология влечений человека*. М.: Прогресс, 1972
35. ПЕТРОВСКИЙ А.В., ЯРОШЕВСКИЙ М.А. (общая ред.) Психологический словарь. М., 1999 (См. Психика).
36. ПСИХОЛОГИЯ: ПОПУЛЯРНЫЙ СЛОВАРИК / ред. Дубровина И.В. М.: Академия. Кафедра, 1997 – 96 с. С. 52 – Психика.
37. ПУШКИН В.Н. *О материальной основе отражения действительности человеком* / Вопросы психогигиены, психофизиологии, социологии труда в угольной промышленности и психоэнергетики. М., 1980. С. 339
38. ПУШКИН В.Н., ЕРМОЛАЕВА-ТОМИНА Л.Б., ЕРМОЛАЕВ О.Ю., НИКИФОРОВ В.Г., ШАВЫРИНА Г.В. *Электропунктура и психофизиология.*/Сб. «Электропунктура и проблемы информационно-энергетической регуляции деятельности человека». Ред. В.Н. Пушкин и В.Г. Никифоров. М., 1976.

39. РАМЕНДИК Д.М., ОДИНЦОВА О.В. *Психология и психологический практикум*. М.: Химия, КолосС, 2004 – 240 с.
40. РЕГУЛЯТОРНЫЕ СИСТЕМЫ ОРГАНИЗМА ЧЕЛОВЕКА: Учеб. пос. для вузов / *Дубынин В.А., Каменский А.А., Сапин М.Р.* и др. М.: Дрофа, 2003 – 368 с. Гл. 4. С. 184-313.
41. РОДЖЕРС К. *Взгляд на психотерапию. Становление человека*. М.: Прогресс, 1994
42. СИМОНОВ П.В., ЕРШОВ П.М. *Темперамент. Характер. Личность*. М.: Наука, 1984; 161 с.
43. СИМОНОВ П.В. *Лекции о работе головного мозга. Потребностно-информационная теория высшей нервной деятельности*. М.: ИП РАН, 1998; 98 с.
44. УОДДИНГТОН К.Х. *Основные биологические концепции* / На пути к теоретической биологии. 1. Пролегомены. М.: Мир, 1970, с. 34. С. 11-38).
45. ЧУПРИКОВА Н.И. *Психика и предмет психологии в свете достижений современной нейронауки* //Вопр. психологии. 2004, № 2. С. 104-118.
46. ШАБЕЛЬНИКОВ В.К. *Функциональная психология (формирование психологических систем)*. М.: Академический проект, 2004 – 592 с.
47. ШЕЛЕР Макс. *В: «Соврем. западная социология»*. М.: Политиздат, 1990 (*Ю.Н. Давыдов*). С. 397
48. ШЕЛЬСКИ Хельмут. *В: «Соврем. западная социология»*. М.: Политиздат, 1990 (*А.Ф. Филиппов*).
49. ШОЛОМИЙ К.М. *Об одном виде саморегуляции мышления*/ Вопросы психологии, 1979, № 6.
50. ЮНГ К.Г. *Психологические типы*. Пред. И.Д. Ермакова. М.: ГИЗ, 1927

Серия: **ФИЗИКА И АСТРОНОМИЯ**

Иванов Г. П.

Преобразования Лоренца как тождественная форма преобразований Галилея и невозможность переноса импульса электромагнитной волной

Аннотация

Если применить преобразования Галилея к фазе бегущей волны, распространяющейся от движущегося точечного источника в любой однородной волнопроводящей недисперсионной среде, будь то жидкость, газ, твёрдое тело или физическое пространство, то в результате тождественных преобразований, как бы сами собой появятся преобразования Лоренца. Нет необходимости постулирования релятивистского принципа относительности, который, как оказалось, является прямым следствием принципа относительности Галилея, действующего в определённых условиях. Попутно выявляется, что бегущая волна любой природы не способна переносить импульс. В частности доказывается, что понятие определяемого через вектор Пойнтинга электромагнитного импульса лишено физического смысла и опровергается прямыми расчётами для системы антенных дипольных излучателей, раскрывается подлинный физический смысл этого понятия. Также попутно выявляется, что в системе антенных излучателей действуют постоянные по направлению эфироопорные силы, имеющие перспективы их практического использования в энергетике и на транспорте.

Оглавление

1. Различные способы разложения бегущей волны на стоячие и бегущие (в противоположных направлениях) компоненты и проблема переноса импульса

Бегущую расходящуюся сферическую волну от точечного (в смысле малого по сравнению с длиной волны) источника, покоящегося в изотропной волнопроводящей конденсированной среде (без дисперсии) можно представить в виде функции

$$\Phi = \frac{A}{r}\cos(\omega_0 t - k_0 r) = a\cos\omega_0\left(t - \frac{r}{c}\right) = a\cos 2\pi\left(\frac{t}{T_0} - \frac{r}{\lambda_0}\right) \qquad (1)$$

где A – амплитуда колебаний в точках среды на расстоянии от источника, равном единице, r – расстояние от источника, ω_0 – циклическая частота, $k_0 = 2\pi/\lambda_0$ – волновой вектор, λ_0 – длина волны, t – текущее время, $a = A/r$ – амплитудная функция, c – скорость распространения волн в рассматриваемой среде, T_0 – период волны.

Напишем цепочку легкопроверяемых тригонометрических тождеств, справедливых для точек, расположенных на любом расстоянии от источника:

$$\cos(\omega_0 t - k_0 r) \equiv 0.5\{[\cos(\omega_0 t - k_0 r) + \cos(\omega_0 t + k_0 r)] + [\cos(\omega_0 t - k_0 r) - \cos(\omega_0 t + k_0 r)]\} \equiv$$

$$\equiv \cos k_0 r \cos \omega_0 t + \sin k_0 r \sin \omega_0 t \qquad (2)$$

или в другом представлении:

$$\cos 2\pi\left(\frac{t}{T_0} - \frac{r}{\lambda_0}\right) \equiv \cos 2\pi\frac{r}{\lambda_0}\cos 2\pi\frac{t}{T_0} + \sin 2\pi\frac{r}{\lambda_0}\sin 2\pi\frac{t}{T_0} \qquad (2a)$$

Согласно написанному, любая бегущая волна есть суперпозиция двух стоячих волн, сдвинутых по фазе на $\pi/2$. Оказывается, точечный источник бегущей сферической волны не «излучает» ничего, кроме пары стоячих волн. Но это ещё не всё, на что он способен! Ничто не мешает нам написать тождество

$$\cos 2\pi\left(\frac{t}{T_0} - \frac{r}{\lambda_0}\right) \equiv 2\cos 2\pi\frac{r}{\lambda_0}\cos 2\pi\frac{t}{T_0} - \cos 2\pi\left(\frac{t}{T_0} + \frac{r}{\lambda_0}\right) \qquad (2b)$$

Получается так, что наш источник вместо расходящихся волн, уносящих импульс в любом заданном направлении, «излучает» не имеющие импульса стоячие волны и приносящие импульс сходящиеся волны. Таким образом, понятие «импульс волны» лишено физического смысла. Теперь понятно, почему волны, например, в жидкой среде не способны переносить импульс без переноса вещества [1]. Но как быть с электромагнитными волнами, излучаемыми, к примеру, источником света? Ведь наше рассмотрение применимо к любой волнопроводящей среде (включая эфир, вакуум, пространство, или как там его ни называй).

С одной стороны, в любой точке пространства электромагнитную волну можно разложить на две поляризованные компоненты, по отношению к каждой из которых справедливы тождества (2), (2a), (2b), согласно которым импульс электромагнитных волн, в лучшем случае, не удовлетворяет принципу суперпозиции, в худшем - вовсе не существует. С другой стороны принято считать, что электромагнитная волна имеет плотность импульса, определяемую через вектор Пойнтинга, и переносит импульс. Этот принципиально важный вопрос имеет однозначное решение, которое представлено ниже, в приложении к настоящей статье.

Следует отметить, что разложение бегущей волны на стоячие компоненты не пустая формальность, а факт физической реальности. При желании для любой волнопроводящей среды

можно «изобрести» техническое устройство, «фазовый детектор», позволяющий выделять и исследовать любую стоячую компоненту бегущей волны.

2. Автоматическое «превращение» преобразований Галилея для волны движущегося излучателя в преобразования Лоренца для координат и времени

Мы говорили выше о покоящемся в среде источнике, теперь перейдём к движущемуся. Примем, что покоящийся источник размещён в начале декартовой системы координат (x, y, z), а движущийся (x', y', z'). В начальный момент времени координатные оси обеих систем (движущейся и неподвижной) совпадают. Скорость движения v направлена вдоль оси x.

Фазу бегущей волны покоящегося излучателя, распространяющейся вдоль оси y, можно представить в виде:

$$\phi_0 = \omega_0\left(t - \frac{y}{c}\right) \qquad (3)$$

При переходе к движущемуся излучателю для волны, распространяющейся по оси y' (поперёк скорости) параметры t и y примут вид в соответствии с преобразованиями Галилея для времени и координаты, c – в соответствии с галилеевским правилом нахождения относительной скорости при известных абсолютной и поступательной. Циклическая частота излучателя ω выбирается применительно к условию решаемой задачи.

Таким образом, фаза волны, распространяющейся поперёк направления скорости источника, (вдоль оси y'), запишется в виде:

$$\phi = \omega\left(t - \frac{y}{c\alpha}\right), \text{ где } \alpha = \sqrt{1 - \frac{v^2}{c^2}} \qquad (3a)$$

На основании тождества (2) разложение бегущей волны с фазой (3a) на две стоячие компоненты будет иметь вид:

$$\cos\omega\left(t - \frac{y}{c\alpha}\right) \equiv \cos\frac{\omega}{c\alpha} y \cos\omega t + \sin\frac{\omega}{c\alpha} y \sin\omega t \qquad (4)$$

Перейдём к волне, излучаемой по направлению скорости. Сравним фазы бегущих волн, от покоящегося и движущегося излучателей:

$$\phi_0 = \omega_0\left(t - \frac{x}{c}\right), \qquad \phi = \omega\left(t - \frac{x - vt}{c - v}\right). \qquad (5)$$

Так же, как и в предыдущем случае, переход от фазы покоящегося к фазе движущегося излучателя произведён путём замены

координаты, времени и скорости в соответствии с преобразованиями Галилея.

Подставляя выражение для фазы движущегося излучателя (5) в (2), путём прямых вычислений получаем бегущую волну как суперпозицию двух стоячих волн следующим образом:

$$\cos\omega\left(t-\frac{x-vt}{c-v}\right)\equiv\cos\frac{\omega}{c\alpha}x'\cos\frac{\omega}{\alpha}t'+\sin\frac{\omega}{c\alpha}x'\sin\frac{\omega}{\alpha}t' \qquad (6)$$

где x' и t' – есть преобразования по форме неотличимые от преобразований Лоренца для координаты и времени, а именно

$$x'=\frac{x-vt}{\sqrt{1-\frac{v^2}{c^2}}}, \qquad (6a)$$

$$t'=\frac{t-\frac{xv}{c^2}}{\sqrt{1-\frac{v^2}{c^2}}}. \qquad (6b)$$

2.1. Соотношение длин стоячей волны вдоль и поперёк направления скорости излучателя

Определим расстояния между соседними узлами стоячих компонент движущегося излучателя в направлении поперёк скорости (по оси y* = y) и вдоль скорости (по оси x* = x -vt) и сравним их между собой. Будем учитывать расстояние между узлами для одной из двух стоячих компонент, сдвинутых по отношению друг к другу на $\pi\backslash 2$ (между узлами разных компонент это расстояние было бы в два раза меньшим), в связи с чем, ограничимся членами, содержащими синусы, т. е. вторыми членами правых частей (4) и (6). Исходя из условия, что минимальное расстояние между соседними узлами равно половине длины волны ($y = \lambda_\perp/2$, $\Delta x^* = \Delta x = \lambda_{II}/2$) аргументы соответствующих амплитудных функций должны иметь вид:

$$\frac{\omega}{c\alpha}\frac{\lambda_\perp}{2}=n\pi, \qquad \frac{\omega}{c\alpha^2}\frac{\lambda_{II}}{2}=n\pi.$$

Отсюда получим:

$$\lambda_\perp=\lambda_{II}\alpha=\lambda_{II}\sqrt{1-\frac{v^2}{c^2}}. \qquad (7)$$

Пришли к выводу, что расстояние между соседними узлами стоячих волн в направлении скорости движения излучателя в α раз сокращается, по сравнению с расстоянием между узлами в поперечном направлении. Важно отметить, что полученная закономерность остаётся справедливой при любом характере зависимости частоты излучателя от скорости его движения (мы не задавались конкретным характером такой зависимости).

2.2. Картина стоячих волн при постоянной частоте излучателя

Одним из практически важных случаев является независимость частоты излучателя от скорости его движению по отношению к волнопроводящей среде. Такие излучатели удобны при экспериментальном исследовании стоячих волн в воздухе, воде и др. средах. Автор [2] Ю. Н. Иванов измерял параметры стоячих волн, устанавливая звуковые излучатели и приёмники звука (микрофоны) в поле на ветру или на крышах движущихся поездов. Результаты таких исследований подробно описаны в [2]. Расчётным и опытным путём он определил, что стоячие волны уменьшают свою длину в $\alpha = (1 - v^2/c^2)^{0.5}$ раз в поперечном по отношению к скорости направлении и в α^2 раз, в продольном, что непосредственно следует из формул (6), (7). Фигурально выражаясь, у него получились сплющенные (в α раз сжатые) преобразования Лоренца, которые, в отличие от настоящих преобразований Лоренца, не обладают свойством обратимости. Деление на α приводит его преобразования к виду, формально совпадающему с преобразованиями Лоренца.

2.3. Картина стоячих волн при постоянной длине волны, распространяющейся поперёк скорости излучателя

Очень важным как в теоретическом, так и в практическом отношениях, является случай, при котором, длина стоячей волны, ориентированной поперёк скорости излучателя, не зависит от величины его скорости. В качестве примера можно привести движение в свободном пространстве, при котором эталон длины (набранный из определённого количества стоячих волн), ориентированный поперёк направления скорости, сохраняет свою длину независимо от величины этой скорости (при ориентации вдоль скорости, как известно, имеет место лоренцево сокращение, что подробно будет рассмотрено ниже).

Другой замечательный пример – согласно модели Френкеля и Конторовой в твёрдом теле существуют солитоны (дислокации) [3],

которые при взаимодействии друг с другом могут образовывать бризеры. Процитируем из [3]: - « … образуется стоящее на месте пульсирующее состояние. Его называют *бризером* (от англ. breath – дышать, одно из значений слова breather – живое существо), или *бионом* … . Бризер внешне выглядит как стоячая волна. … Бризер может равномерно двигаться. Он ускоряется или замедляется вблизи неоднородностей. При столкновениях с солитонами или другими бризерами он … ведёт себя как частица. С другой стороны в бризере наглядно проявляется волновая природа солитонов. Бризер нельзя описать как две частицы, … связанные пружиной. «Внутри» него действительно пульсирует стоячая волна сжатий и разряжений «среды».» *Конец цитаты*. Важно отметить, что бризеры и солитоны при их поступательном движении не меняют своих размеров в поперечном по отношению к скорости направлении, а в продольном направлении испытывают сокращение по формуле $l = l_0(1 - v^2/c^2)^{0.5}$ где l, l_0 – текущая длина и длина солитона в состоянии покоя, v – скорость солитона, c скорость звука в волнопроводящей среде. Таким образом, солитоны ведут себя как релятивистские, привязанные к скорости звука, частицы, в обличие от обычных частиц, релятивизм которых «привязан» к скорости света. «Звуковой» релятивизм аналогичен «световому» релятивизму, по крайней мере, в некотором идеальном приближении и, в отличии от последнего, имеет некоторые вполне понятные границы применимости, к чему мы вернёмся ниже. Следует также отметить, что в физике имеет место и встречная тенденция рассмотрения элементарных частиц как солитонных состояний [3].

Итак, мы приняли условие, согласно которому длина волны, испускаемой в направлении, перпендикулярном скорости ($\lambda_\perp$), в системе отсчёта источника не зависит от скорости его движения по отношению к волнопроводящей среде:

$$\lambda_\perp = \lambda_0 . \qquad (8)$$

Принимая во внимание (3), (3а), запишем:

$$\lambda_0 = \frac{2\pi c}{\omega_0}; \qquad \lambda_\perp = \frac{2\pi c\alpha}{\omega}.$$

Так как $\lambda_\perp = \lambda_0$, то

$$\omega = \omega_0\alpha. \qquad (9)$$

Тогда, с учётом того, что волновое число $k_0 = \omega_0/c$, на основании (4) получим:

$$\cos(\omega t - k_0 y) \equiv \cos k_0 y \cos \omega t + \sin k_0 y \sin \omega t \qquad (10)$$

Согласно полученной формуле волна, излучаемая движущимся источником, в поперечном направлении, отличается от волны, излучаемой покоящимся источником (2), только частотой излучателя, которая с увеличением скорости уменьшается по закону $\omega = \omega_0\alpha$, что обусловлено принятым нами условием равенства длин волн и правилом сложения скоростей по Галилею.

Перейдём к волне, излучаемой по направлению скорости. Сравним фазы бегущих волн, от покоящегося и движущегося излучателей:

$$\phi_0 = \omega_0\left(t - \frac{x}{c}\right), \qquad \phi = \omega_0\alpha\left(t - \frac{x - vt}{c - v}\right). \tag{11}$$

Заметим, что переход от фазы покоящегося к фазе движущегося излучателя произведён путём замены всех определяющих фазу величин (частоты , времени, координаты, скорости) в соответствии с преобразованиями Галилея применительно к принятому условию для длин волн.

Подставляя выражение для фазы движущегося излучателя (11) в (2), путём прямых вычислений получаем бегущую волну как суперпозицию двух стоячих волн следующим образом:

$$\cos\ \omega_0\sqrt{1-\frac{v^2}{c^2}}\left(t - \frac{x-vt}{c-v}\right) \equiv \left\{\begin{array}{l} \cos k_0 \dfrac{x-vt}{\sqrt{1-\dfrac{v^2}{c^2}}}\ \cos\ \omega_0 \dfrac{t-\dfrac{xv}{c^2}}{\sqrt{1-\dfrac{v^2}{c^2}}} \\ + \sin k_0 \dfrac{x-vt}{\sqrt{1-\dfrac{v^2}{c^2}}}\ \sin \omega_0 \dfrac{t-\dfrac{xv}{c^2}}{\sqrt{1-\dfrac{v^2}{c^2}}} \end{array}\right\} \tag{12}$$

Тот же результат можно получить путём подстановки (9) в (6).

Сравним с формулой для неподвижного излучателя, которую в соответствии с (2) можно переписать в виде:

$$\cos\omega_0\left(t - \frac{x}{c}\right) \equiv \cos k_0 x\ \cos\ \omega_0 t + \sin\ k_0 x\ \sin\ \omega_0 t \tag{13}$$

Присмотримся к тому, что мы фактически сделали. В формулу для бегущей компоненты неподвижного излучателя [левая часть (13)] подставили преобразования Галилея для всех входящих туда величин (координата, время, скорость, частота) и получили формулу для бегущей компоненты движущегося излучателя [левая часть (12)]. Далее, в стоячих компонентах неподвижного излучателя

[правая часть (13)] оставили без изменения циклическую частоту ω_0 и волновое число k_0, все остальные параметры у нас автоматически сгруппировались в преобразования Лоренца для координаты и времени (12), (6a), (6b). Таким образом, формула (12) сама трансформирует преобразования Галилея в преобразования Лоренца! Или, фигурально выражаясь, она «разлагает» преобразования Галилея на преобразования Лоренца.

Покажем, что это правило справедливо и для волны, распространяющейся поперёк направления скорости. Учитывая, что на оси y' = y, x' = 0, из (6a) получаем x = vt (означающее, что точка x' движется относительно среды со скоростью v, что и так очевидно), подставляя в (6b), находим:

$$t'_{x'=0} = t\alpha \qquad (14)$$

Отсюда, принимая во внимание (10), получаем:

$$\cos\omega_0\alpha\left(t-\frac{y}{c\alpha}\right) \equiv \cos k_0 y' \cos\omega_0 t'_{x'=0} + \sin k_0 y' \sin\omega_0 t'_{x'=0} \qquad (15)$$

Сравнивая (12) и (15) заключаем, что переход от волн, излучаемых покоящимся источником, к волнам, излучаемым движущимся источником в продольном и поперечном по отношению к скорости направлениях, осуществляется по одним и тем же правилам. Таким образом, преобразования Лоренца всегда (со времён сотворения мира) были «зарыты» в преобразованиях Галилея, а мы просто извлекли их оттуда на всеобщее обозрение.

Путём прямых вычислений нетрудно убедиться, что обратное тоже верно, стоячая волна движущегося источника, разлагаясь на две бегущие компоненты, фигурально выражаясь, также «разлагает» преобразования Лоренца на преобразования Галилея , см. ниже формулу (22). Что первично, что вторично? Бегущие волны (от источника, движущегося с малой скоростью, v << c) «подчиняются» галилеевскому представлению, а стоячие – лоренцевскому.

Рассмотрим и сравним межузловые расстояния неподвижного и движущегося излучателей. Координаты узлов неподвижного излучателя (r_n) можно определить из условия:

$$k_0 r_n = 2\pi r_n/\lambda_0 = n\pi,$$

где r_n – n-ный по счёту узел, считая от начала координат.

Отсюда $r_n = n\lambda_0/2$. Расстояние между узлами с номерами n_1 и n_2 будет равным $(n_2 - n_1)\lambda_0/2 = \Delta n\lambda_0/2$. Минимальное расстояние равно половине длины волны:

$$L_0 = \lambda_0/2 . \qquad (16)$$

Подобным образом определяем расстояние между соседними узлами на оси y' движущегося излучателя : $k_0 y'_n = 2\pi y'_n/\lambda_0 = n\pi$. Отсюда минимальное межузловое расстояние равно

$$L_{y'} = \lambda_0/2, \qquad (17)$$

что соответствует принятому в начале условию (8), $\lambda_\perp = \lambda_0$.

Таким образом, межузловые расстояния поперёк скорости движущегося и покоящегося излучателей совпадают.

Аналогично, координаты узлов вдоль направления скорости в соответствии с правой частью (12), находим из условия $k_0 x'_n = 2\pi x'_n/\lambda_0 = n\pi$, откуда следует, что $x'_n = n\lambda_0/2$. Заменяя x'_n на x_n в соответствии с (6а), получим $x_n - vt = n\alpha\lambda_0/2$. Расстояние между узлами с номерами n_1 и n_2 в любой фиксированный момент времени будет равным $(n_2 - n_1)\ \alpha\lambda_0/2 = \Delta n\alpha\lambda_0/2$. Минимальное расстояние $L_{x'}$ получается при $\Delta n = 1$:

$$L_{x'} = \alpha\lambda_0/2. \qquad (18)$$

Таким образом, расстояние между узлами стоячих волн от движущегося излучателя вдоль скорости «сжимается» в α раз по сравнению с расстоянием поперёк скорости и по сравнению с межузловым расстоянием покоящегося излучателя, что и следовало ожидать. Это значит, что длина стоячей волны $\lambda_{x'}$, связанной с движущимся источником тоже таким же образом «сжимается» по направлению скорости в α раз:

$$\lambda_{x'} = \lambda_\perp\alpha = \lambda_0\alpha. \qquad (18а)$$

Покоящийся излучатель окружён множеством сферических волновых поверхностей, каждая из которых есть геометрическое место точек, удаленных от начала координат на одинаковое количество длин волн N в любом направлении. Для движущегося излучателя общая длина одного и того же количества волн вдоль направления движения, согласно (18а), будет в α раз короче, чем поперёк направления движения, вследствие чего, волновые поверхности станут эллипсоидальными, сплющенными по оси x. Таким образом, мы пришли к лоренцеву сокращению на базе преобразований Галилея (12).

Перейдём к рассмотрению временных фаз. Перенесёмся мысленно на минуту во вторую половину XIX века. Все, что нам нужно знать, о стоячих и бегущих волнах в те времена было известно и мы могли бы спокойно заниматься нашими вопросами.

Сопоставляя правые части (2), (12), (15), приходим к заключению, что параметр t' определяет фазы стоячих волн движущегося излучателя точно так же, как время определяет фазы стоячих волн

покоящегося излучателя. Для определённости будем называть его волновым временем. Выше (14) мы нашли соотношение волнового и обычного времени для точки x' = 0. Отсюда, на основании (15), для этой точки справедливо соотношение $t'_{x'=0}/T_0 = t\alpha/T_0 = t/T$, из которого следует, что периоды стоячих волн движущегося и покоящегося излучателей связаны следующим образом:

$$T = T_0/\alpha. \qquad (19)$$

Отсюда видно, что волны движущегося излучателя колеблются с периодом в $1/\alpha$ раз большим, чем покоящегося. Соотношение (14) определено для начала координат (x' = 0), а как ведёт себя волновое время в произвольной точке оси x', удалённой от нулевой точки на расстояние L? Подставляя в (6b) x = vt + L, получим:

$$t' = t\alpha - \frac{Lv}{c^2\alpha} = t\alpha - \frac{L'v}{c^2}, \qquad (20)$$

где $L' = L/\alpha$.

Отсюда следует, что волновое время в произвольной точке на оси x' отстаёт по фазе от волнового времени в нулевой точке, что можно видеть на графике, см. ниже Рис. 1. Стоячие волны от движущегося излучателя колеблются несинфазно, в отличие от стоячих волн от неподвижного излучателя.

Волновое время можно определять числом периодов N_T, от которого оно, в общем случае, может отличаться, каким-то градуировочным множителем, зависящем от выбранной системы измерения величин. Любое устройство, способное измерять число периодов стоячей волны, а, значит, и волновое время, по сути дела, есть волновые часы.

Известен способ синхронизации часов путём их медленного переноса из одной точки в другую. Как поведут себя волновые часы при их переносе на расстояние L (L') от нулевой точки оси x'? Итак, имеем волновые часы, показания которых зависят от скорости по закону $t' = t\alpha$ (при начале отсчёта t' = t = 0). Дифференцируя и учитывая, что tdv = dL, получим:

$$dt' = \alpha dt - \frac{vtdv}{c^2\alpha} = \alpha dt - \frac{vdL}{c^2\alpha}. \qquad (20a)$$

Непосредственно видно, что при интегрировании правой части, получится знакомая формула (20). Таким образом, при медленном переносе фаза волновых часов отстаёт так, что они показывают правильное волновое время в той точке, в которую их перенесли. Стало быть, медленный перенос работает как способ синхронизации волновых часов.

Выясним теперь физический смысл условия (8), $\lambda_{\perp} = \lambda_0$, благодаря которому однозначно определяются свойства межузловых расстояний и периодов колебаний стоячих компонент бегущей волны, (17), (18), (18a), (19). Оно получится, если частота излучателя будет согласована с волновым временем или с каким-либо генератором импульсов, повторяющихся с периодом, зависящем от скорости по закону, отображаемому формулой (19). Подойдёт, например, устройство (назовём его «акустические часы»), в котором акустический импульс попеременно отражается от двух плоскостей, расположенных на расстоянии L друг от друга, ориентированных параллельно вектору скорости излучателя.

Мы убедились, что образуемая движущимся излучателем картина стоячих волн, при условии $\lambda_{\perp} = \lambda_0$, ведёт себя в точности так же как любой релятивистский объект, в соответствии с преобразованиями Лоренца. Она сохраняет свой размер поперёк направлению скорости и «сжимается» вдоль скорости. Периоды стоячих волн движущегося излучателя удлиняются по сравнению с периодами стоячих волн покоящегося излучателя в соответствии с преобразованиями Лоренца. Различные части стоячей волны покоящегося излучателя, удалённые друг от друга на целое число длин волн колеблются строго синфазно (2), в связи с чем, их можно рассматривать как синхронно идущие часы (если снабдить счётчиками периодов). Для движущегося излучателя различные части стоячей волны колеблются несинфазно, разность хода связанных с ними часов определяется в соответствии с преобразованиями Лоренца (6a), (6b). Всё вышесказанное позволяет говорить о соотношениях (12), (15) как о преобразованиях Лоренца в тригонометрической форме или как о галилеевских преобразованиях Лоренца, область применимости которых охватывает все волнопроводящие среды от воды и воздуха до физического пространства. Эта форма явно указывает на тот факт, что преобразования Лоренца прямо «вырастают» из преобразований Галилея путём тождественных преобразований, следовательно, они представляют собой форму существования преобразований Галилея. Интересно отметить, что в рассматриваемом аспекте преобразования Галилея имеют более общий характер, чем преобразования Лоренца, потому что последние появляются как следствие применения преобразований Галилея к волнопроводящим средам. Иными словами, преобразования Галилея первичны – преобразования Лоренца

вторичны, стало быть, именно преобразования Галилея определяют настоящее физическое время.

Можно свернуть правую часть (12) по образцу (13), после чего, приравнивая к левой части (12), придти к следующему соотношению:

$$\phi = \omega_0\sqrt{1-\frac{v^2}{c^2}}\left(t-\frac{x-vt}{c-v}\right)\equiv\omega_0\frac{t-\frac{xv}{c^2}}{\sqrt{1-\frac{v^2}{c^2}}}-k_0\frac{x-vt}{\sqrt{1-\frac{v^2}{c^2}}}\quad,(21)$$

где ф – фаза гармонической функции.

В левой части тождества фаза бегущей волны движущегося излучателя выражена в соответствии с преобразованиями Галилея, в правой части та же фаза выражена в соответствии с преобразованиями Лоренца. Эти выражения фазы могут использоваться как аргументы гармонических функций в тригонометрическом или экспоненциальном представлении.

Отсюда вытекает следующее лаконичное соотношение между преобразованиями Галилея и преобразованиями Лоренца:

$$c_{\perp\text{Галилея}}\left(t-\frac{x'_{\text{Галилея}}}{c_{\parallel\text{Галилея}}}\right)\equiv c\left(t'_{\text{Лоренца}}-\frac{x'_{\text{Лоренца}}}{c}\right),\qquad(22)$$

где $c_{\perp\ \text{Галилея}} = c\ (1 - v^2/c^2)^{0.5}$ и $c_{||\ \text{Галилея}} = c - v$ - относительные скорости света, распространяющего от движущегося источника в поперечном и продольном направлениях, $x'_{\text{Галилея}} = x - vt$ - преобразование Галилея для координаты, $t'_{\text{Лоренца}} = t'$, $x'_{\text{Лоренца}} = x'$- преобразования Лоренца для времени и координаты, см. (6a), (6b).

Все величины в левой части соответствуют преобразованиям Галилея, а все величины в правой части соответствуют преобразованиям Лоренца (учитывая, что $t = t'_{\text{Галилея}}$, $c = c'_{\text{Лоренца}}$). Группы величин в левой и правой частях (22) отличается от фазы гармонической функции постоянным множителем $2\pi/\lambda_\perp$.

Переходя к обычным обозначениям, получим:

$$\sqrt{1-\frac{v^2}{c^2}}\left(t-\frac{x-vt}{c-v}\right)\equiv t'-\frac{x'}{c}.\qquad(22a)$$

Отсюда приходим к фазовому инварианту:

$$\sqrt{\frac{c-v}{c+v}}\left(t'-\frac{x'}{c}\right)=t-\frac{x}{c}\quad.\qquad(23)$$

2.4. Визуализация тождественности преобразований Галилея и преобразований Лоренца

На основании (2) для излучателя, покоящегося в волнопроводящей среде, справедливо следующее тригонометрическое тождество:

$$\cos \omega_0(t - x/c) + \cos \omega_0(t + x/c) \equiv 2\cos k_0 x \cos \omega_0 t \qquad (24)$$

В левой части сумма двух встречных волн, бегущих вдоль оси x, в правой части образуемая ими стоячая волна. Пусть излучатель движется при выполнении условия (8), согласно которому длина волны, излучаемой поперёк скорости, есть константа, $\lambda_\perp = \lambda_0$, что эквивалентно условию $\omega = \omega_0(1 - v^2/c^2)^{0.5}$, где ω - циклическая частота движущегося излучателя. Остальные параметры (кроме частоты), определяющие фазы бегущих встречных волн, должны быть замены, согласно преобразованиям Галилея: $t \to t$, $x \to x - vt$, $c \to c + v$ или $c \to c - v$, после чего тождество (24) примет вид:

$$\cos \omega_0 \sqrt{1-\frac{v^2}{c^2}}\left(t-\frac{x-vt}{c-v}\right) + \cos \omega_0 \sqrt{1-\frac{v^2}{c^2}}\left(t+\frac{x-vt}{c+v}\right)$$

$$\equiv 2\cos k_0 \frac{x-vt}{\sqrt{1-\frac{v^2}{c^2}}} \cos \omega_0 \frac{t-\frac{xv}{c^2}}{\sqrt{1-\frac{v^2}{c^2}}}. \qquad (25)$$

Несмотря на то, что выражения (24), (25) получены из компонент волнового поля точечного излучателя (2), они вполне могут быть применены к волновой картине между двумя излучателями плоских волн, наглядно демонстрирующей «синтез» преобразований Лоренца из преобразований Галилея, см. Рис. 1.

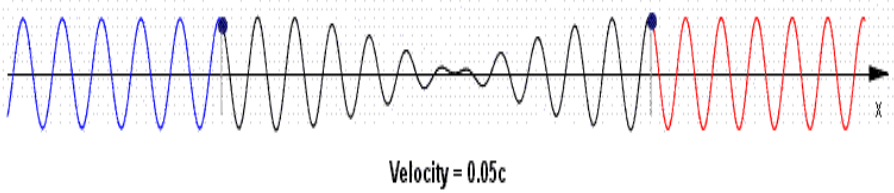


Рис. 1. «Синтез» преобразований Лоренца из преобразований Галилея.

Вследствие галилеевского правила сложения скоростей, волна, распространяющаяся влево от первого (который слева) излучателя, имеет большую относительную скорость, а, значит, и большую длину, чем волна, распространяющаяся вправо от второго излучателя, что на рисунке можно заметить даже невооружённым

глазом. Эти подчиняющиеся преобразованиям Галилея бегущие волны, в пространстве между излучателями «синтезируются» в подчиняющуюся преобразованиям Лоренца стоячую волну, длина которой мало отличается от длины волны покоящихся излучателей (v^2/c^2 = 0.25 %). Видно, что амплитуды разных участков стоячей волны неодинаковы, нет синфазности, присущей стоячей волне, образуемой покоящимися излучателями, что согласуется с правыми частями формул (24), (25). Эта несинфазность в теории Эйнштейна трактуется как «относительность одновременности».

Анимацию приведённого рисунка можно посмотреть здесь http://tts.lt/~nara/stechwelle/volna1.gif или здесь http://ivanov-georgij2010.narod.ru/imag/volna1.gif

3. Как «устроена» относительность

Примем теперь **кардинальное соглашение** – все длины будем измерять длинами определённой (опорной) стоячей волны (что эквивалентно измерению межузловыми расстояниями), а все времена – периодами стоячей волны в той системе отсчёта, в которой покоится наблюдатель. Получается так, что каждая волнопроводящая среда, имеет индивидуальные, присущие ей волновые меры длин и времён. Примером может служить волнопроводящее пространство Вселенной, где роль опорной волны в свое время была прописана для излучения изотопа криптона 86 (эталон длины) и цезия 133 (эталон времени). Опорная волна (одна или несколько) для той или иной волнопроводящей среды может быть выбрана из множества волн, отличающихся частотами (длинами волн). В частности, аналогичным образом, для звукопроводящей среды можно выбрать опорную звуковую длину волны и опорную частоту, и создать устройства, поддерживающие заданное число длин волн (волновой эталон длины) и заданный период колебаний или частоту (волновой эталон времени).

Так как длины стоячих волн от движущегося источника «сжимаются» по направлению скорости, а периоды удлиняются (12), (15) и точно так же ведут себя волновые эталоны длины и времени, то результаты измерений, полученные наблюдателем, покоящимся по отношению к движущемуся излучателю, не будут зависеть от скорости последнего. Так как эталонные волновые часы при медленном переносе вдоль направления скорости «самосинхронизуются», см. (20а), то движущийся наблюдатель, будет считать, что в его системе отсчёта различные участки стоячей волны колеблются в одинаковых фазах, так же как это происходит в

системе отсчёта, покоящейся по отношению к волнопроводящей среде. Иными словами, на основании своих измерений наблюдатель не сможет определить состояние своего движения или покоя по отношению к среде.

Пусть наблюдатель, пользующийся исключительно волновыми мерами длины и времени, покоится в движущейся со скоростью v (вправо по оси x) системе координат (x', y', t') и ставит своей задачей написать формулу бегущей волны покоящегося в среде (x, y, t) излучателя, включая её разложение на стоячие волны. Согласно вышеизложенному, такой наблюдатель будет считать себя покоящимся, а излучатель движущимся влево по оси x' (т. е. со скоростью -v).

Фаза бегущей волны относительно наблюдателя будет иметь вид:

$$\phi' = \omega_0 \alpha \left(t' - \frac{x' + vt'}{c + v} \right) /$$

А разложение бегущей волны на стоячие компоненты запишется в виде:

$$\cos \omega_0 \alpha \left(t' - \frac{x' + vt'}{c + v} \right) = \cos k_0 x \cos \omega_0 t + \sin k_0 x \sin \omega_0 t , \qquad (26)$$

где

$$x = \frac{x' + vt'}{\sqrt{1 - \frac{v^2}{c^2}}}, \qquad (26a)$$

$$t = \frac{t' + \frac{x'v}{c^2}}{\sqrt{1 - \frac{v^2}{c^2}}}. \qquad (26b)$$

Решая тригонометрические тождества, мы получили обратные преобразования Лоренца и установили их обратимость. Тот же результат, обычно получают решением уравнений (6a), (6b) относительно неизвестных x, y. Мы пришли к выводу, что любая недисперсионная волнопроводящая среда обладает врождённым (природным) свойством относительности, основываясь на посылке, согласно которой длина волны, испускаемая движущимся излучателем в поперечном по отношению к скорости направлении, не зависит от величины этой скорости, что согласуется с опытом для физического пространства и для солитонообразующих твёрдых тел. В жидких и газообразных волнопроводящих средах это

свойство моделируется техническими приёмами реализации присущих данной среде волновых мер длины и времени. Говоря точнее, выражаемый преобразованиями Лоренца релятивистский характер относительности есть врождённое свойство преобразований Галилея, выявляющееся при их применении к волнопроводящим средам.

3.1. Сравнение различных концепций относительности

Различные концепции относительности отличаются друг от друга разными способами получения одной и той же сущности – преобразований Лоренца - и различной трактовкой их физического смысла.

3.1.1. Волновая концепция относительности

По существу, выше мы сформулировали своеобразную «волновую» концепцию относительности, представленную как свойство волнопроводящих сред, которая отвечает современным тенденциям, к рассмотрению элементарных частиц (а значит и всего мироздания) как солитонов или солитоноподобных объектов [3]. Чтобы получить представление о важности этого направления, достаточно перечислить некоторые причастные к его разработке имена: - Густав Ми, Макс Борн, Альберт Эйнштейн, Вернер Гейзенберг, Поль Дирак и др. Английский физик-теоретик Тони Скирм в 70 – 80 годах прошлого века даже создал свою теорию «скирмионов», согласно которой протон и нейтрон следует рассматривать как солитоны, образующиеся при нелинейном взаимодействии мезонных полей. Так что мысль о волновой природе всего сущего материального мира вполне реальна, о чём еще не могли подозревать современники автора своего знаменитого опыта – Майкельсона. Основываясь на изложенной концепции, мы можем сказать, что опыт Майкельсона имеет отрицательный результат, потому что вся установка Майкельсона (включая его интерферометр и столешницу), будучи волнообразуемой (либо солитоноподобной) материей, сокращается по направлению движения в эфире в той же мере, в которой сокращается стоячая световая волна в плечах интерферометра. Согласно нашей волновой концепции относительности, вообще не существует таких опытов, которые позволят обнаружить движение относительно эфира (если только со временем не откроют взаимодействия принципиально иной природы, волновая скорость которых намного превышает световую).

3.1.2. Эфирная концепция относительности Лоренца – Пуанкаре - Фицджеральда

Исторически первая концепция относительности, полностью согласующая с электродинамикой Максвелла – Лоренца (по существу, современной классической электродинамики), принадлежит Лоренцу, Фитцджеральду и Пуанкаре [4]. Лоренц пришел к ней и получил преобразования, носящие его имя, задавшись вопросом об инвариантности уравнений Максвелла в различных инерциальных системах отсчёта (ИСО) [5].

Согласно этой концепции существует неподвижный эфир, который по Лоренцу можно мыслить себе как материю настолько большой плотности, что никакие силы не в состоянии привести в движение одних его (эфира) частей, по отношению к другим его частям (в идеале эфир получается как материя бесконечно большой эффективной плотности). Все тела природы сокращают свои размеры одинаковым образом в зависимости от скорости их движения по отношению к эфиру, поэтому результаты измерений размеров одинаковы во всех ИСО. В БСЭ [4] говорится: - «Ситуация наталкивала на мысль о необнаружимости движения относительно эфира. Такой вывод сделал А. Пуанкаре, который начиная с 1895 выражал убеждение, что движение относительно эфира необнаружимо принципиально. В 1900-е гг. при обсуждении электромагнитных явлений он начал пользоваться термином "принцип относительности", формулируя его как невозможность обнаружения движения относительно эфира.» *Конец цитаты.* Согласно Лоренцу настоящее физическое время имеет место только в системе отсчёта, в которой эфир покоится. Показания часов в движущейся ИСО нельзя отождествлять с физическим временем, они показывают пространственно временной параметр, который Лоренц называл «местным временем». Заметим, что «местное время» Лоренца имеет такой же физический смысл, как рассмотренное нами выше «волновое время». С одной стороны, формально, оно ведёт себя как настоящее, с другой стороны оно не настоящее, потому не имеет никакого отношения к принципу причинности. Это отличие сразу бросается в глаза при рассмотрении акустических волнопродящих сред (твёрдых, жидких, газообразных и пр.) потому что мы видим сразу два времени, волновое, определяемое скоростью звука, и определяемое скоростью света физическое время, которое мы замеряем обычными механическими или электронными часами (сверенное с эталонным

– волновым – временем нашего физического пространства, эфира). Акустическое волновое время мы воспринимаем как время низшего типа, оно своё для каждой волнопроводящей среды, а физическое «световое» время, высшего типа, оно одно для всех акустических сред.

Гораздо труднее и запутаннее ситуация с лоренцевским настоящим эфирным временем и его «местным» временем. Лоренц в [5] пишет, что если все силы природы, ведут себя как электромагнитные силы, то мы никогда не сможем определить скорость по отношению к эфиру, а, значит, и не сможем узнать в какой именно ИСО «местное», а в какой «эфирное» время. Остаётся надеяться, что когда-нибудь будет открыто сверхсветовое взаимодействие, тогда у нас появится время «высшего типа» по отношению к «местному» времени, которое позволит определить систему покоя эфира и расставить все точки над i. Но нет насущной необходимости ждать свершения этого замечательного события, потому что в середине XX века был открыт так называемый «новый эфир» вполне пригодный для практического использования вместо настоящего эфира. А именно, было обнаружено, охватывающее всю нашу Вселенную микроволновое фоновое реликтовое излучение [6], которое, согласно теории «большого взрыва», родилось в сингулярной точке вместе со Вселенной [7]. Существует единственная инерциальная система отсчёта, в которой реликтовое излучение изотропно по отношению к любому объекту, покоящемуся в ней. При движении объекта возникает анизотропия, характер которой определяется величиной и направлением его скорости. К примеру, солнечная системы движется относительно «реликтовой» ИСО со скоростью ≈ 400 км/с в направлении созвездия Льва.

В соответствии с основными законами сохранения, реликтовая ИСО либо покоится в эфире, либо движется по отношению к нему с постоянной скоростью, что позволяет использовать её вместо абсолютной системы отсчёта (в которой эфир покоится), потому что фактически используется разность энергий вещественно-полевых объектов, которая будет в обоих случаях одинаковой. Главное, что реликтовая ИСО обеспечивает возможность использования одинаковых мер длины и времени, в любых сколь угодно удалённых друг от друга областях Вселенной без непосредственного обмена сигнальной информацией. Концепция Лоренца – Пуанкаре – Фицджеральда становится актуальной.

3.1.3. Постулатная концепция относительности Эйнштейна

Постулатная концепция относительности в её полном и законченном виде представлена Эйнштейном в 1905 г. в его работе «К электродинамике движущихся тел» [8]. Принцип относительности постулируется, все инерциальные системы отсчёта (ИСО) принимаются равноправными, скорость света в каждой из них одна и та же, время относительно, одновременность относительна. Время это то, что показывают часы в той ИСО, в которой они покоятся. Согласно Эйнштейну, цитирую: - «Введение «светоносного эфира» окажется … излишним, поскольку в предполагаемой теории не вводится «абсолютно покоящееся пространство», наделённое особыми свойствами … ». В своей концепции Эйнштейн отождествляет физическое время с тем пространственно-временным параметром, который в волновой концепции представляет собой «волновое время», а в концепции Лоренца – Пуанкаре – Фицджеральда «местное время», что на первых порах сыграло положительную роль, потому что послужило субъективным фактором понимания важности относительности и активизировало её практическое использование при решении различных вопросов и задач электродинамики. В «Теории электронов» [5] Лоренц пишет: - «… мне не удалось получить уравнения, отнесённые к подвижным осям, в точно такой же форме, что и уравнения для неподвижной системы, Эйнштейн же выполнил это при помощи системы новых переменных, весьма, впрочем, мало отличающихся от тех, которые были выведены мной. Я не пользовался этими подстановками только по той причине, что формулы представляются довольно сложными и имеют несколько искусственный вид, если только не выводить их из самого принципа относительности». *Конец цитаты.* Переменные, о которых говорит Лоренц, это то, что мы сейчас называем «преобразованиями Лоренца». Дело в том, что Лоренц не сразу осознал, что в его теории эфира имеет место относительность и в этом осознании ему помог Эйнштейн (не в прямом смысле, а через свои работы). Невозможность обнаружения никакими экспериментами движение одной ИСО по отношению к другой ИСО в одинаковой мере вытекает как из эфирной относительности Лоренца, так и из специальной теории относительности Эйнштейна, потому что обе теории опираются на одни и те же преобразования Лоренца. В свою очередь, Эйнштейн не сразу осознал необходимость существования эфира. В 1920 г. он говорит [9]: - «…пространство немыслимо без эфира; действительно, в таком пространстве не

только было бы невозможно распространение света, но не могли бы существовать масштабы и часы и не было бы никаких пространственно-временных расстояний в физическом смысле слова. Однако этот эфир нельзя представить себе состоящим из прослеживаемых во времени частей; таким свойством обладает только весомая материя; точно так же к нему нельзя применять понятие движения.». *Конец цитаты*. Однако, процитированное мнение Эйнштейна не приняли к сведению его последователи. Они до настоящего времени остаются на тех позициях отрицания эфира, которые были присущи Эйнштейну в 1905 [8]. Таким образом, в наше время в научном мире бытуют две концепции относительности постулатная Эйнштейна и, в меньшей степени, эфирная Лоренца – Пуанкаре – Фицджеральда [10].

Все вышеперечисленные концепции относительности в зоне пересечения их областей применимости дают одинаковые результаты решения различных задач. Самую узкую область применимости имеет концепция Эйнштейна. Её недостатком, в отличие от других концепций, является нарушение принципа причинности при переходе к сверхсветовым скоростям как для гипотетически существующих сверхсветовых взаимодействий, так и для тоже гипотетически существующих тахионов, согласующихся с лоренц-инвариантностью сверхсветовых частиц, см. [4]. Более существенный недостаток (отсутствующий в других концепциях) связан с нарушением закона сохранения энергии при обнаруженных в недавнее время эфироопорных взаимодействиях [11], [16], см. также «Приложение» к настоящей статье. Перечисленные недостатки устраняются отменой отождествления введенного Эйнштейном понятия времени с реальным физическим временем, что никак не отразится на физико-математическом аппарате его теории. Тогда концепция Эйнштейна становится эквивалентной концепции Лоренца – Пуанкаре – Фицджеральда.

3.2. Естественные ограничения закона относительности

Ограничения на относительность, понимаемые как ограничения на применимость преобразований Лоренца, легче всего проследить в некоторых волнообразующих средах. К примеру, в газовой среде, длина волны ограничена снизу расстоянием между молекулами, по этой причине относительность применима только к достаточно длинным волнам.

Более общий характер применимости относительности выявляется при сравнении плотности энергии волны и плотности энергии

среды, последняя должна быть больше первой. В идеальном случае плотность волновой энергии должна физически бесконечно малой по отношению к плотности энергии среды. При приближении плотности волновой энергии к плотности энергии среды движение волновых объектов перестанет строго подчиняться преобразованиям Лоренца. Если говорить о солитонах, то, например, в металлах энергия образования точечных дефектов составляет десятые доли – единицы эВ, что одного порядка с энергией парообразования (сублимации), составляющей несколько эВ в пересчёте на один атом. Следовательно, движение таких солитонов будет не строго, а приблизительно подчиняться преобразованиям Лоренца (в части зависимости размеров и энергии от времени), что отмечается в [3].

Оценим границу применимости закона относительности для физического вакуума (эфира). Определим плотность энергии самых высокоэнергетичных космических частиц и сравним её с планковской плотностью энергии флуктуаций физического вакуума, которая, по оценке Уиллера [12] составляет 10^{114} Дж/м^3. Самые высокоэнергетичные протоны и ядра атомов первичного космического излучения могут достигать энергии 10^{21} эВ и выше. Т. е. один протон может иметь вполне макроскопическую энергию более 100 Дж, достаточную, чтобы часами поддерживать свечение светодиода, что соответствует плотности энергии 10^{58} Дж/м^3 – исчезающее малая величина, по сравнению с вышеприведённой плотностью энергии вакуума (на 56 порядков меньшая). Чтобы приблизиться к критической плотности энергии (10^{114} Дж/м^3), при которой преобразования Лоренца, а, значит, и закон относительности начнут давать сбои, протон следует «разогнать» до энергии порядка 10^{48} эВ, чего хватит, чтобы около часа поддерживать энерговыделение Солнца. Таким образом, реально достижимые плотности энергии вещественной материи исчезающее малы по сравнению с критической величиной, что обеспечивает практически идеальное выполнение закона относительности для нашего физического пространства (эфира).

Благодарности

Хочу выразить благодарности Валерию Борисовичу Морозову за представленные интересные материалы, касающиеся переноса импульса в акустике и активное участие в обсуждении сопутствующих вопросов, участнику форума SciTecLibrary под ником **txAlien** за активное обсуждение материалов по

тригонометрическим преобразованиям Лоренца и предоставление анимированного графика.

Приложение

Невозможность переноса импульса электромагнитной волной – решающий фактор существования эфира Лоренца

Вот что писал Анри Пуанкаре в 1900 г для Международного конгресса физиков в Париже: - «… можно вообразить опыты, которые ввели бы нас в еще более тесное соприкосновение с ним (*с эфиром)*. Предположим, что закон Ньютона, утверждающий равенство действия и противодействия, будучи приложен только к материи, оказался неверным, и нам удалось это установить. Геометрическая сумма всех сил, приложенных ко всем материальным частицам, не равнялась бы нулю. Тогда пришлось бы либо изменить всю механику, либо ввести эфир так, чтобы действие, испытываемое материей, компенсировалось противодействием, оказываемым материей на что-то другое» [13].

Это пророческое высказывание получило свой первый импульс на пути его превращения в реальность в 1929 году, когда И. Е. Тамм в своей известной книге «Основы теории электричества» описал мысленный эксперимент с цилиндрическим конденсатором в магнитном поле [14], в сущности, явившийся прототипом опыта Грехема и Лахоза, поставленного ими в 1980 г. [15]. В последние годы на основе классической электродинамики создана «Теория электродинамического эфироопорного движения», согласно которой равенство действия и противодействия и закон сохранения энергии нарушаются, если не учитывать прямое силовое и энергетическое взаимодействие с новым фактором, который автор отождествил с эфиром Лоренца, являющимся, по его мнению, качественно своеобразным видом материи, отличной от вещества и поля и, что важно, от различных долоренцевых механических и прочих моделей эфира [11]. Надо заметить, что даже Эйнштейн говорил об эфире Лоренца, не отождествляя его с другими, в том числе и со своей собственной, моделями эфира [9]. Эффект действия эфироопорной силы был зарегистрирован в серии экспериментов автора [11], повторённых ливанским профессором Ассадом Хури. Разработаны рекомендации по постановке дальнейших экспериментов, которых следует ожидать по мере

проникновения разработок по эфироопорности в сознание научных кругов [16].

Имеющиеся у автора обоснования эфироопорности главным образом относятся к квазистатическим и сводящимся к ним системам, размеры которых не превосходят длину волны, соответствующую рабочим частотам [11]. В настоящем приложении установлено нарушение третьего закона Ньютона при взаимодействии дипольных антенных излучателей, расположенных в волновых зонах друг друга, что на качественном уровне отмечено в популярной статье [17].

Задача 1

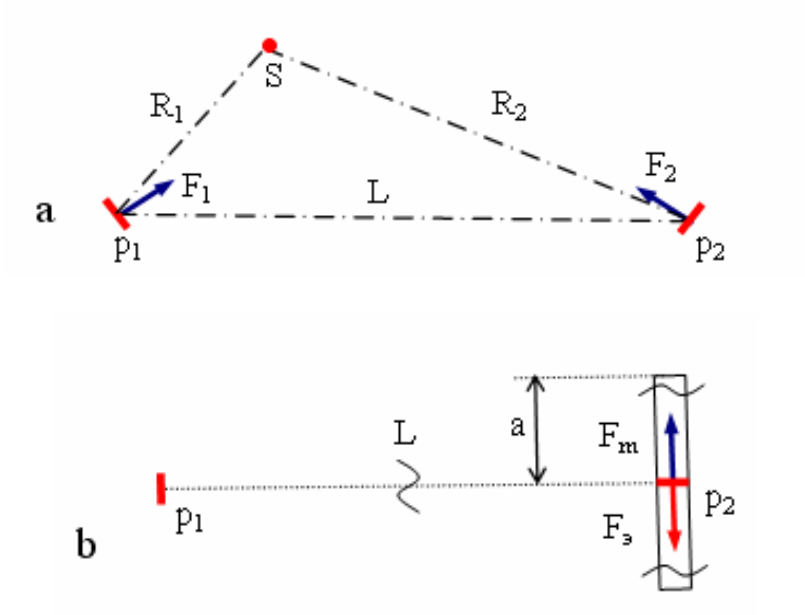


Рис. 2. Взаимодействие антенных излучателей. a, b – произвольная и взаимно перпендикулярная ориентации антенных дипольных моментов $\mathbf{p}_1$ и $\mathbf{p}_2$. F_1, F_2 – действующие на антенны силы Ампера, F_m – равнодействующая системы антенных излучателей, L – расстояние между антеннами, R_1, R_2 – расстояния от антенн до точки S, расположенной на удалённой сферической поверхности.

На Рис. 2. a изображены две дипольно излучающие произвольно ориентированные в пространстве синхронно работающие антенны $\mathbf{p}_1$ и $\mathbf{p}_2$. Длина излучаемой волны мала по сравнению с расстоянием L между антеннами (**L** – радиус-вектор, отсчитываемый от первой

антенны), размеры которых, в свою очередь, малы по сравнению с длиной волны, что позволяет окружающие их поля в определённом приближении считать однородными. Полагаем, что антенны работают независимо друг от друга и рассеянное или поглощённое излучение от соседней антенны пренебрежимо мало по сравнению с собственным излучением.

На основании закона сохранения импульса системы зарядов и поля [19], [14], справедливо следующее соотношение:

$$\mathbf{F}_m + \mathbf{F}_e + \frac{d\mathbf{G}}{dt} = \oint_S T_{\alpha\beta} n_\alpha \mathbf{m}_\beta dS \qquad (1^*)$$

где $\mathbf{F}_m$ – суммарная магнитная сила Ампера, $\mathbf{F}_e$ – суммарная электрическая сила, действующая на заряды системы, $\mathbf{G}$ – импульс электромагнитного поля, S – охватывающая систему поверхность интегрирования, компоненты нормали к которой равны n_α, $T_{\alpha\beta}$ - тензор натяжений Максвелла, $\mathbf{m}_\beta$ - единичные векторы декартовой системы координат.

Приведённое в правой части тензорное выражение может быть представлено в векторной форме следующим образом, см. [20], [21] (в гауссовой системе единиц измерения):

$$\oint_S T_{\alpha\beta} n_\alpha \mathbf{m}_\beta dS = \frac{1}{4\pi} \oint_S \left\{ \left[\mathbf{E}(\mathbf{nE}) - \frac{1}{2} E^2 \mathbf{n} \right] + \left[\mathbf{H}(\mathbf{nH}) - \frac{1}{2} H^2 \mathbf{n} \right] \right\} dS, \quad (2^*)$$

где $\mathbf{E}$, $\mathbf{H}$ – электрическое и магнитное поля излучения на поверхности интегрирования, $\mathbf{n}$ – вектор нормали поверхности интегрирования.

Определим все силы в обеих частях (1*), с учётом (2*), применительно к рассматриваемой антенной системе.

Магнитное поле излучения в волновой зоне можно представить в виде [18]:

$$\mathbf{H} = -\frac{k^2}{R^2} \mathbf{p}_0 \times \mathbf{R} \cos(\omega t - kR), \qquad (3^*)$$

где k – волновое число, R – расстояние от антенны до точки наблюдения, $\mathbf{p}_0$ – амплитуда дипольного момента антенны, ω - циклическая частота.

Магнитные поля каждой из антенн $\mathbf{H}_1$, $\mathbf{H}_2$ вызывают силы (Ампера) $\mathbf{F}_{m2}$, $\mathbf{F}_{m1}$, действующие на токи антенн $\dot{\mathbf{p}}_2, \dot{\mathbf{p}}_1$. Суммарная сила Ампера $\mathbf{F}_m$ будет равна:

$$\mathbf{F}_m = \frac{1}{c} (\dot{\mathbf{p}}_1 \times \mathbf{H}_2 + \dot{\mathbf{p}}_2 \times \mathbf{H}_1). \qquad (4^*)$$

На основании (3*), учитывая, что $\mathbf{p}_1 = \mathbf{p}_{01}\cos\omega t$, $\mathbf{p}_2 = \mathbf{p}_{02}\cos\omega t$ где $\mathbf{p}_{01}$, $\mathbf{p}_{02}$ – амплитудные значения дипольных моментов $\mathbf{p}_1$, $\mathbf{p}_2$, получим:

$$\mathbf{F}_{m2} = \frac{k^3}{L^2}\mathbf{p}_{02}\times(\mathbf{p}_{01}\times\mathbf{L})\sin\omega t\cos(\omega t - kL). \qquad (5^*)$$

Аналогичным образом найдём силу, действующую на первую антенну, со стороны поля, излучаемого второй антенной:

$$\mathbf{F}_{m1} = -\frac{k^3}{L^2}\mathbf{p}_{01}\times(\mathbf{p}_{02}\times\mathbf{L})\sin\omega t\cos(\omega t - kL). \qquad (6^*)$$

Складывая (5*) и (6*), найдём магнитную силу Ампера системы, соответствующую первому члену левой части формулы (1*):

$$\mathbf{F}_m = \frac{k^3}{L^2}\mathbf{L}\times(\mathbf{p}_{01}\times\mathbf{p}_{02})\sin\omega t\cos(\omega t - kL). \qquad (7^*)$$

В частности, если расстояние между антеннами L удовлетворяет соотношению $L = \lambda(n + 1/8)$, $\mathbf{p}_1$ и $\mathbf{p}_2$ взаимно перпендикулярны, $\mathbf{R}$ и $\mathbf{p}_2$ параллельны, как на Рис. 2b, то суммарная магнитная сила Ампера будет постоянной по направлению со средним значением, равным

$$\langle F_m\rangle = \frac{k^3 p_{01}p_{02}}{2L}\ . \qquad (8^*)$$

Перейдём ко второму члену левой части (1*), электрическим силам. Электрическое поле в волновой зоне определяется по формуле, см. [18]:

$$\mathbf{E} = \frac{1}{c^2R^3}\mathbf{R}\times(\mathbf{R}\times\ddot{\mathbf{p}}) = \frac{k^2}{R^3}\mathbf{R}\times(\mathbf{p}_0\times\mathbf{R})\cos(\omega t - kR) = \mathbf{E}(\mathbf{R})\cos\varphi, \qquad (9^*)$$

где $\mathbf{E}(\mathbf{R})$ и φ - обозначения, соответствующие приведённому выражению.

Силу $\mathbf{F}_e$ можно найти по формуле, см. [7]:

$$\mathbf{F}_e = \left\{\begin{matrix}[(\mathbf{p}_2\nabla)\mathbf{E}_1(\mathbf{R}) + (\mathbf{p}_1\nabla)\mathbf{E}_2(\mathbf{R})]\cos\varphi + \\ \mathbf{E}_1(\mathbf{R})(\mathbf{p}_2\nabla)\cos\varphi + \mathbf{E}_2(\mathbf{R})(\mathbf{p}_1\nabla)\cos\varphi\end{matrix}\right\} \qquad (10^*)$$

Определяем члены, заключённые в квадратные скобки:

$$\mathbf{F}_{e2} = (\mathbf{p}_2\nabla)\mathbf{E}_1(\mathbf{R}) =$$

$$= \frac{k^2}{L^3}\cos\omega t\cos(\omega t - kL)\begin{Bmatrix}(\mathbf{p}_{01}\mathbf{L})\left[\dfrac{3(\mathbf{p}_{02}\mathbf{L})\mathbf{L}}{R^2} - \mathbf{p}_{02}\right] - \\ \mathbf{L}(\mathbf{p}_{01}\mathbf{p}_{02}) - \mathbf{p}_{01}(\mathbf{p}_{02}\mathbf{L})\end{Bmatrix},$$

$$\mathbf{F}_{e1} = \frac{k^2}{L^3}\cos\omega t\cos(\omega t - kL)\begin{Bmatrix}-(\mathbf{p}_{02}\mathbf{L})\left[\dfrac{3(\mathbf{p}_{01}\mathbf{L})\mathbf{L}}{R^2} - \mathbf{p}_{01}\right] + \\ \mathbf{L}(\mathbf{p}_{01}\mathbf{p}_{02}) + \mathbf{p}_{02}(\mathbf{p}_{01}\mathbf{L})\end{Bmatrix}.$$

Складывая $\mathbf{F}_{e1}$ и $\mathbf{F}_{e2}$, получим нуль.

Остальные члены правой части (10*), учитывая, что $(\mathbf{p}\nabla)\cos(\omega t - kR) = k(\mathbf{pR}/R)\sin(\omega t - kR)$, дадут результат:

$$\mathbf{F}_e = \frac{k^3}{L^2}\mathbf{L}\times(\mathbf{p}_{01}\times\mathbf{p}_{02})\cos\omega t\sin(\omega t - kL), \qquad (11^*)$$

который только тригонометрическими множителями отличается от суммарной магнитной силы Ампера (7*). Аналогично, если расстояние между антеннами L удовлетворяет соотношению $L = \lambda(n + 1/8)$, $\mathbf{p}_1$ и $\mathbf{p}_2$ взаимно перпендикулярны, $\mathbf{R}$ и $\mathbf{p}_2$ параллельны, как на Рис. 2b, то суммарная электрическая сила будет постоянной по направлению со средним значением, равным:

$$\langle F_e\rangle = -\frac{k^3 p_{01}p_{02}}{2L} \quad (11a^*)$$

В соответствии с (7*), (11*), в произвольно выбранный момент времени электрические и магнитные силы не компенсируют друг друга, как и в квазистатическом случае. Можно было бы подумать, что, согласно (8*), (11a*) компенсируются средние значения, но это такая же иллюзия, как и в квазистатике [11], потому что мы ещё не рассмотрели зарядовые магнитодинамические силы, действие которых можно продемонстрировать следующим образом.

Электрическое поле, как в ближней, так и в дальней зонах имеет вид:

$$\mathbf{E} = \mathrm{rot}\,\mathrm{rot}\frac{\mathbf{p}}{R}\ . \qquad (12^*)$$

Согласно этой формуле, любые два колеблющихся в системе дипольных излучателей заряда Q и q действуют друг на друга с силой:

$$\mathbf{F}_{eq} = -\frac{Qq}{k^2}\,\mathrm{rot}\,\mathrm{rot}\,\frac{\mathbf{w}_Q}{R}\,, \qquad (13a^*)$$

$$\mathbf{F}_{eQ} = -\frac{Qq}{k^2}\,\mathrm{rot}\,\mathrm{rot}\,\frac{\mathbf{w}_q}{R}, \qquad (13b^*)$$

где $\mathbf{w}_Q, \mathbf{w}_q$ - ускорения зарядов Q и q в процессе их колебательного движения.

В сопутствующей заряду Q неинерциальной системе отсчёта [24] заряд q движется с

ускорением $\mathbf{w}_q - \mathbf{w}_Q$ и, в свою очередь, в сопутствующей заряду q неинерциальной системе отсчёта заряд Q движется с ускорением $\mathbf{w}_Q - \mathbf{w}_q$, вследствие чего, заряды будут действовать друг на друга с силами:

$$\mathbf{F}'_{eq} = -\frac{Qq}{k^2}\,rot\,rot\,\frac{\mathbf{w}_Q - \mathbf{w}_q}{R} = -\frac{Qq}{k^2}\,rot\,rot\,\frac{\mathbf{w}_Q}{R} + \frac{Qq}{k^2}\,rot\,rot\,\frac{\mathbf{w}_q}{R} = \qquad (14a^*)$$

$$= \mathbf{F}_{eq} - \mathbf{F}_{eQ} = \mathbf{F}_{eq} + \mathbf{F}_{mQ}$$

$$\mathbf{F}'_{eQ} = -\frac{Qq}{k^2}\,\mathrm{rot}\,\mathrm{rot}\,\frac{\mathbf{w}_q - \mathbf{w}_Q}{R} = \mathbf{F}_{eQ} - \mathbf{F}_{eq} = \mathbf{F}_{eQ} + \mathbf{F}_{mq} \qquad (14b^*)$$

Чтобы прояснить смысл написанных формул, предположим, что один из зарядов, например q, покоится, $\mathbf{w}_q = 0$. Тогда из (14a*) следует, что сила, действующая на этот покоящийся заряд со стороны колеблющегося, одинакова как в исходной инерциальной, так и в сопутствующей заряду Q неинерциальной системах отсчёта, $\mathbf{F}'_{eq} = \mathbf{F}_{eq}$. Что касается колеблющегося заряда Q, то в инерциальной системе, согласно (13b*), на него не действует никакая сила. В сопутствующей системе на него будет действовать сила, равная по величине противоположная по знаку той силе, с которой он действует на покоящийся в инерциальной системе заряд q, и которая остаётся при возвращении в инерциальную систему (14*). Это и есть зарядовая магнитодинамическая сила $\mathbf{F}_{mq}$. Делаем вывод, что с какой силой колеблющийся заряд действует на покоящийся, с такой же, равной по величине, противоположной по направлению ответной силой на него действует посредством своего поля покоящийся заряд. Иначе в простейшей системе покоящегося и колеблющегося зарядов не выполнялся бы третий закон Ньютона. Складывая (14a*) и (14b*), получим:

$$\mathbf{F}_{eq} + \mathbf{F}_{eQ} = -(\mathbf{F}_{mq} + \mathbf{F}_{mQ})\,. \qquad (15^*)$$

Сумма электрических сил взаимодействующих в волновой зоне зарядов равна по величине, противоположна по направлению сумме зарядовых магнитодинамических сил. Зарядовая магнитодинамическая сила существует независимо от того, в какой системе отсчёта мы её рассматриваем, в инерциальной или в сопутствующей. Переход к неинерциальной системе это просто один из способов её выявления.

Сравнивая волновую и квазистатическую системы [11], мы видим что, несмотря на разный характер полей, структура силового взаимодействия у них одна и та же. В обоих случаях суммарные электрическая и зарядовая магнитодинамическая силы взаимно уравновешиваются. Остаётся неуравновешенной лишь суммарная магнитная сила Ампера.

Перейдём к третьему члену левой части (1*) который связывают с силовым фактором импульса электромагнитного поля. Считается, что плотность импульса волнового излучения $\mathbf{g}$ и вектор Пойнтинга $\mathbf{S} = c\mathbf{E} \times \mathbf{H}/4\pi$ связаны соотношением $\mathbf{g} = \mathbf{S}/c^2$.

$$\frac{d\mathbf{G}}{dt} = \frac{d}{dt}\int \mathbf{g}dV = \frac{1}{4\pi c}\frac{d}{dt}\int \mathbf{E}\times\mathbf{H}dV \qquad (16^*)$$

В соответствии с (3*), (9*) интеграл в правой части (16*) всюду сходится, стало быть, функция $\mathbf{G}$ меняется в конечном интервале и по этой причине имеет нулевое среднее значение [18]. Действительно,

$$\left\langle \frac{d\mathbf{G}}{dt} \right\rangle = \frac{1}{T}\int_0^T \frac{d\mathbf{G}}{dt}dt = \frac{\mathbf{G}(T)-\mathbf{G}(0)}{T}$$

Поскольку $\mathbf{G}(t)$ меняется в конечных пределах, то при неограниченном увеличении T это среднее значение стремится к нулю, в отличие от магнитной силы Ампера, которая, согласно (8*), явно отлична от нуля. Ещё проще, если мы, учитывая периодичность подынтегральной функции, сразу приходим к нулю для среднего по периоду значения.

Осталось вычислить правую часть (1*), равную правой части (2*). Может быть, магнитная сила Ампера уравновесится реакцией излучения? Нет. Правая часть (2*), как сила четвёртого порядка по v/c (она зависит от E^2, H^2, значит от k^4, пренебрежимо мала по сравнению с силой Ампера системы $\mathbf{F}_m$ третьего порядка, зависящую, согласно (7*), (8*), от k^3, поэтому мы спокойно можем приравнять поверхностный интеграл (2*) к нулю. Однако, посмотрим, что получится, если мы его всё-таки вычислим.

Выпишем из (2*) электрическую компоненту $\mathbf{F}_{te}$ силы натяжения:

$$\mathbf{F}_{te} = \frac{1}{4\pi}\oint_S \left\{\left[(\mathbf{E}_1 + \mathbf{E}_2)(\mathbf{n}(\mathbf{E}_1 + \mathbf{E}_2)) - \frac{1}{2}(\mathbf{E}_1 + \mathbf{E}_2)^2 \mathbf{n} \right]\right\} dS \qquad (17^*)$$

Выберем сферическую поверхность так, чтобы первая антенна находилась в центре, а вторая располагалась на расстоянии L от неё в соответствии с Рис. 2а. Тогда, в соответствии с (9*), на поверхности сферы электрические поля, излучаемые первым и вторым диполями (учитывая, что $\mathbf{R}_2 = \mathbf{R}_1 - \mathbf{L}$), будут иметь вид:

$$\mathbf{E}_1 = \frac{k^2}{R_1}\mathbf{n}_1 \times (\mathbf{p}_1 \times \mathbf{n}_1) ; \qquad (18^*)$$

$$\mathbf{E}_2 = \frac{k^2}{|\mathbf{R}_1 - \mathbf{L}|}\mathbf{n}_2 \times (\mathbf{p}_2 \times \mathbf{n}_2) , \qquad (19^*)$$

где $\mathbf{n}_1 = \mathbf{R}_1/R_1$ и $\mathbf{n}_2 = (\mathbf{R}_1 - \mathbf{L})/|\mathbf{R}_1 - \mathbf{L}|$ - единичные векторы, отсчитываемые от первой и второй антенны.

Нормаль в любой точке поверхности лежит на прямой, соединяющей эту точку с центром сферы, в котором находится первая антенна, значит, $\mathbf{n}_1 = \mathbf{n}$. Следовательно, $(\mathbf{n}\mathbf{E}_1) = (k^2/R)\mathbf{n}[\mathbf{n} \times (\mathbf{p}_1 \times \mathbf{n})] = 0$, так как содержит смешенное (скалярно-векторное) произведение двух одинаковых векторов $\mathbf{n}$. Перейдём к рассмотрению $\mathbf{E}_2$. При достаточно больших размерах поверхности интегрирования расстояние между антеннами станет пренебрежимо малым по сравнению с радиусом сферы, $L << R$. При удалении этой поверхности в бесконечность $L/R \to 0$. Отсюда следует, что на этой поверхности:

$$R_2 = |\mathbf{R}_1 - \mathbf{L}| = |\mathbf{R} - \mathbf{L}| = R\sqrt{1 + \frac{L^2}{R^2} - 2\frac{L}{R}\cos\varphi} = R$$

где φ - угол между векторами $\mathbf{L}$ и $\mathbf{R}$.

Применяя теорему косинусов к треугольнику со сторонами L, R_1, R_2, Рис. 2а, получим соотношение:

$$R_1^2 + R_2^2 - 2R_1R_2 \cos\theta = L^2,$$

где θ - угол между векторами $\mathbf{R}_1$, $\mathbf{R}_2$.

Учитывая, что при удалении поверхности сферы на бесконечность $R_1 = R_2 = R$, и пренебрегая L^2, найдём $\cos\theta = 1$, $\theta = 0$. Это значит, что при удалении на бесконечность вектора $\mathbf{R}_1$, $\mathbf{R}_2$ «сливаются» в один вектор $\mathbf{R}$ (как имеющие общую точку при нулевом угле схождения), являющийся нормалью к поверхности сферы. Тогда из (9*) следует, что $(\mathbf{n}\mathbf{E}_2)$ равно нулю по той же причине, что и $(\mathbf{n}\mathbf{E}_1)$.

В соответствии с вышесказанным поставленная задача решается вычислением входящего в (17*) интеграла, $\int(\mathbf{E}_1 + \mathbf{E}_2)^2\mathbf{n}dS$. Применим к нему неравенство Минковского [22]:

$$\left[\oint_S(\mathbf{E}_1+\mathbf{E}_2)^2\mathbf{n}dS\right]^{0.5} \le \left[\oint_S\mathbf{E}_1^2\mathbf{n}dS\right]^{0.5} + \left[\oint_S\mathbf{E}_2^2\mathbf{n}dS\right]^{0.5}. \qquad (20^*)$$

Вычислим первый интеграл правой части:

$$\mathbf{I}_1 = \oint_S\mathbf{E}_1^2\mathbf{n}dS = k^4\oint_S\frac{\mathbf{p}_{01}^2-(\mathbf{p}_{01}\mathbf{n})^2}{R^2}\cos^2(\omega t-kR)\mathbf{n}dS. \qquad (21^*)$$

Выберем систему декартовых координат (x, y, z) так, чтобы вектор $\mathbf{p}_{01}$ лежал на оси z. Тогда его координаты будут $\{0, 0, p_{01}\}$. Учитывая, что $\mathbf{R} = \{x, y, z\}$, получим соотношение $(\mathbf{p}_{01}\mathbf{n}) = p_{01}z/R$ и формула (21*) примет вид:

$$\mathbf{I}_1 = k^4\oint_S\frac{p_{01}^2(R^2-z^2)}{R^5}\cos^2(\omega t-kR)\mathbf{R}dS. \qquad (22^*)$$

Найдём компоненты $\mathbf{I}_1$ при удалении поверхности интегрирования на бесконечность ($R \to \infty$). Представляя элемент поверхности в виде $dS = 2\pi R dz$ и переходя к интегрированию по координате, получим:

$$I_{1z} = 2\pi k^4\int_{-\infty}^{\infty}\frac{p_{01}^2(R^2-z^2)}{R^4}\cos^2(\omega t-kR)zdz = 0. \qquad (23^*)$$

Равенство нулю обеспечивается нечётностью подынтегральной функцией при симметричных относительно нуля пределах интегрирования.

Представляя элемент поверхности в виде

$$dS = \sqrt{\left(\frac{\partial z}{\partial x}\right)^2+\left(\frac{\partial z}{\partial y}\right)^2+1}\,dxdy = \frac{R}{|z|}dxdy, \quad z = \sqrt{R^2-x^2-y^2}$$

[22] также найдём, что $I_{1x} = 0$; $I_{1y} = 0$.

Перейдём ко второму интегралу правой части (20*). Отметим, что он содержит тригонометрический множитель, который нарушает нечётность подынтегральной функции, в отличие от тригонометрического множителя, содержащегося в (21*). Этот множитель удовлетворяет неравенству $\cos^2(\omega t - kR_2) \le 1$, что даёт возможность избавиться от него следующим образом:

$$\mathbf{I}_2 = \oint_S \mathbf{E}_2^2 \mathbf{n} dS = k^4 \oint_S \frac{\mathbf{p}_{02}^2 - (\mathbf{p}_{02}\mathbf{n})^2}{R^2} \cos^2(\omega t - kR_2)\,\mathbf{n} dS$$
$$\leq k^4 \oint_S \frac{\mathbf{p}_{02}^2 - (\mathbf{p}_{02}\mathbf{n})^2}{R^2} \mathbf{n} dS \qquad (24^*)$$

Выберем теперь другую систему декартовых координат (x_1, y_1, z_1) так, чтобы вектор $\mathbf{p}_{02}$ лежал на оси z_1. Тогда его координаты будут {0, 0, p_{02}}. Правая часть (24*) примет вид:

$$\mathbf{I}_2 \leq k^4 \oint_S \frac{p_{02}^2 (R^2 - z_1^2)}{R^5} \mathbf{R} dS = 0 \qquad (25^*)$$

Равенство $\mathbf{I}_2$ нулю обеспечивается нечётностью подынтегральной функции по всем координатам вектора $\mathbf{R}$ = {x_1, y_1, z_1}, что легко проверятся аналогичными для $\mathbf{I}_1$ вычислениями.

Подставляя $\mathbf{I}_1 = \mathbf{I}_2 = 0$ в (20*), получаем $\oint_S \left|\mathbf{E}_1 + \mathbf{E}_2\right|^2 \mathbf{n} dS = 0$, откуда следует, что компонента интеграла тензора натяжений, обусловленная электрическими полями излучения обеих антенн (17*), равна нулю. Аналогичные вычисления для магнитных полей тоже дадут нулевой результат.

Таким образом, интеграл тензора натяжений по удалённой замкнутой поверхности равен нулю даже в четвёртом порядке. Отличная от нуля постоянная по направлению антенная равнодействующая (8*) не уравновешивается ни реакцией антенного излучения, ни временной производной величины, именуемой импульсом электромагнитного поля (16*), принципиально не имеющей постоянной по направлению компоненты. Равенство нулю тензорной силы (2*) и объёмной силы (16*) при наличии постоянной по величине и направлению равнодействующей (8*) есть факт, утверждающий отсутствие переноса импульса электромагнитной волной, и отсутствия физического смысла у понятия «импульс электромагнитного поля», что согласуется с описанным выше, в основном тексте, разложением бегущей волны на стоячие компоненты.

Выражение (1*), применительно к нашему случаю, представляет собой общую форму закона сохранения импульса. Получается такой вывод, что современная классическая электродинамика, опирающаяся на постулатную концепцию относительности, не согласуется с основными физическими законами. Ведь нарушение

закона сохранения импульса, в соответствии с [11], влечёт за собой и нарушение закона сохранения энергии.

Дело не в электродинамике, а именно в концепции, потому что то же самое антенное взаимодействие прекрасно согласуется с представленной в основном тексте эфирной концепцией относительности Лоренца – Пуанкаре – Фицджеральда.

Положение спасает обоснованная в [11] не вещественная, но материальная эфироопорная сила, уравновешивающая магнитную силу Ампера $\mathbf{F}_m$, учёт которой, чисто внешне, лишь слегка изменяет форму написания закона сохранения импульса (1*):

$$\mathbf{F}_m + \mathbf{F}_e + \left(\frac{d\mathbf{G}}{dt}\right)_H = \oint_S T_{\alpha\beta} n_\alpha \mathbf{m}_\beta dS \ , \qquad (26^*)$$

где индекс «Н» означает, что при взятии производной магнитное поле считается постоянным, хотя, на самом деле, оно может меняться.

Убирая равные нулю члены, получим:

$$\mathbf{F}_m = -\left(\frac{d\mathbf{G}}{dt}\right)_H = -\frac{1}{4\pi c}\int \dot{\mathbf{E}} \times \mathbf{H} dV = -\int \mathbf{j}_{см} \times \mathbf{H} dV \, , \qquad (27^*)$$

где точка над $\mathbf{E}$ означает производную по времени, $\mathbf{j}_{см}$ – текущий через вакуум максвелловкий ток смещения.

Интеграл в правой части (27*) по физическому смыслу представляет собой силу Ампера, действующую со стороны магнитного поля на совокупность максвелловских токов смещения, распределенных по всему пространству. Формула (27*) утверждает, что суммарная магнитная сила Ампера в системе частиц равна по величине, противоположна по знаку, действующей на *эфир Лоренца* силе Ампера, тем самым обеспечивая выполнение третьего закона Ньютона. Это и есть эфироопорная сила.

Вектор **G**, входящий в третий член левой части (26*), отличается от известного понятия «импульс электромагнитного поля» тем, что его изменение, вызванное изменением магнитного поля, не влечёт за собой изменение механического импульса системы, причина чего для квазистационарных систем излагается в работах [23], [11], а для нашей задачи будет рассмотрена ниже. Этот вектор, получивший название *«импульсный потенциал»*, является показателем импульсного обмена между вещественной системой и эфиром Лоренца.

Посмотрим, как «работает» эфироопорная сила в рассматриваемой нами антенной системе. Так как по условию задачи размеры антенных диполей малы, по сравнению с длиной волны, то магнитное поле налетающей волны в точке нахождения диполя

можно приближённо считать однородным. В этой области над полем излучения диполя очень сильно (на два порядка по v/c) преобладает его собственное электростатическое поле [18].

Представляет интерес рассчитать вектор $\mathbf{G}_2$, образуемый электростатическим полем диполя $\mathbf{p}_2$ ($\mathbf{E}_{2s}$) и излучаемым диполем $\mathbf{p}_1$ налетающим магнитным полем $\mathbf{H}_1$ (см. Рис. 2b), что даст следующую величину:

$$\mathbf{G}_2 = \frac{1}{4\pi c}\int \mathbf{E}_{2s} \times \mathbf{H}_1 dV = -\frac{1}{c}\mathbf{p}_2 \times \mathbf{H}_1 . \qquad (28^*)$$

Вклад в интеграл (28*) даёт область пространства, сосредоточенная между двумя плоскостями, проходящими через образующие диполь положительный и отрицательный заряды, перпендикулярно направлению дипольного момента, см. Рис. 2b. Для величины $\mathbf{G}$ имеет место соотношение

$$\mathbf{G_2 = (1/c)H_1d_2(1 - b/2a),}$$

где b – эффективное расстояние между образующими диполь зарядами, a – радиус цилиндрической поверхности, заключённой между оговоренными выше плоскостями (Рис 2b). Таким образом, для диполя малых размеров вектор $\mathbf{G}_2$ практически сосредоточен в пределах магнитного поля одной набегающей полуволны.

Аналогичным образом, вычисляя вектор $\mathbf{G}_1$, образуемый электростатическим полем диполя $\mathbf{p}_1$ и излучаемым диполем $\mathbf{p}_2$ налетающим магнитным полем $\mathbf{H}_2$ см. Рис. 2a, найдём $\mathbf{G}_1 = -\mathbf{p}_1 \times \mathbf{H}_2/c$. Сумма $\mathbf{G}_1$ и $\mathbf{G}_2$ это импульсный потенциал системы.

$$\mathbf{G_э = G_1 + G_2} = -(\mathbf{p}_1 \times \mathbf{H}_2 + \mathbf{p}_2 \times \mathbf{H}_1)/c$$

дифференцируя который, получим эфироопорную силу:

$$\mathbf{F}_э = \left(\frac{d\mathbf{G}_э}{dt}\right)_H = -\frac{1}{c}(\dot{\mathbf{p}}_1 \times \mathbf{H}_2 + \dot{\mathbf{p}}_2 \times \mathbf{H}_1), \qquad (29^*)$$

Сравнивая с (4*) видим, что

$$\mathbf{F}_m = -\mathbf{F}_э, \qquad \mathbf{F}_m + \mathbf{F}_э = 0. \qquad (30^*)$$

Результирующая сила Ампера системы взаимодействующих дипольных излучателей равна по величине противоположна по направлению эфироопорной силе, возбуждаемой этой системой в эфире Лоренца.

Таким образом, электромагнитная волна (как и акустическая) не переносит импульс. Вектор $\mathbf{G} = \mathbf{S}/c^2$ ($\mathbf{S}$ - вектор Пойнтинга), в законе сохранения импульса (1*) следует отождествлять не с плотностью импульса электромагнитного поля, а с численно равным ему импульсным потенциалом (26*), который «несёт с собой» одновременно и «действие» на вещество и равное по

величине, противоположное по направлению «противодействие» на эфир Лоренца.

Задача 2

Излучаемое антенными диполями свободное электромагнитное поле представляет собой самостоятельную сущность и открывает неизвестные свойства электромагнитных взаимодействий, выходящие за пределы постулатной концепции относительности. Например, из рассмотренной нами системы можно исключить одну из антенн.

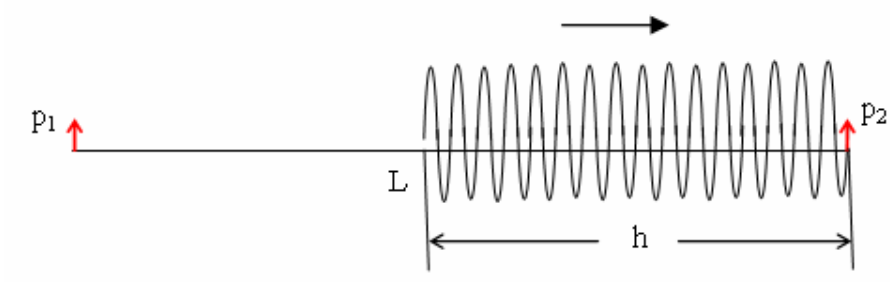


Рис. 3. Взаимодействие свободного электромагнитного поля с дипольным вибратором d_2 при исключённом из системы дипольном излучателе d_1.

На Рис. 3 изображёна дипольная антенна p_1 (излучатель), излучающая в направлении, указанном стрелкой, волновой пакет шириной h, не превышающей расстояние между антеннами L, после чего выключается. Антенна p_2 (вибратор) включается в момент времени, когда её достигает передний фронт волнового пакета и выключается при её прохождении задним фронтом. Пока вибратор p_2 работает, он успевает излучить в обратном направлении волновой пакет, от заднего фронта которого излучатель p_1 включается и цикл повторяется снова. Таким образом, обе антенны включаются и выключается поочерёдно. Вибратор p_2 при своём включении взаимодействует с полем, ранее испущенным излучателем p_1. Излучатель p_1 ни с каким сторонним полем не взаимодействует, вследствие чего, при рассмотрении баланса сил исключается из системы, в которой остаются только свободное поле и вибратор p_2. Дипольные моменты излучателя и вибратора ориентированы взаимно параллельно, перпендикулярно прямой L и изменяются синфазно $p_1 = p_{01} \cos \omega t$, $p_2 = p_{02} \cos \omega t$. Расстояние между антеннами, как и в ранее рассмотренной задаче, принимается равным $L = \lambda(n + 1/8)$. Задача решается по тем же формулам, что и предыдущая задача.

Равнодействующая системы равна силе, действующей на вибратор $\mathbf{p}_2$. Вычисляя магнитную силу Ампера в соответствии с формулой (5*) и усредняя по времени (без учёта скважности), получим:

$$\langle F_m \rangle = -\frac{k^3 p_{01} p_{02}}{2L} \ . \qquad (31^*)$$

Электрическую силу находим по формулам (9*), (10*):

$$F_e = -\frac{k^2 p_{01} p_{02}}{2L^2} \cos\omega t \sin\omega t \ . \qquad (32^*)$$

Её определяемое тригонометрическими множителями среднее значение равно нулю.

Таким образом, равнодействующая системы равна приложенной к вибратору $\mathbf{p}_2$ силе Ампера. Она компенсируется эфироопорной силой таким же образом как в предыдущей задаче, см. (29*), (30*). Отличительной особенностью рассматриваемой системы является отсутствие постоянной по направлению электрической силы, что позволяет не обращаться к зарядовой магнитодинамической силе, хотя и прямо вытекающей из электродинамики, но пока ещё мало кому известной. Подробное решение аналогичной задачи можно посмотреть по адресу - http://tts.lt/~nara/stechwelle/stechwelle.htm .

Задача 3

В предыдущих задачах 1 и 2 использовалась бегущая волна, разложив которую в соответствии с формулой (2) основного текста на стоячие компоненты, мы увидим, что магнитная равнодействующая системы определяется одной из них, а электрическая другой.

В этой связи представляет интерес рассмотреть взаимодействие антенного вибратора с отдельной стоячей волной, см. Рис. 4.

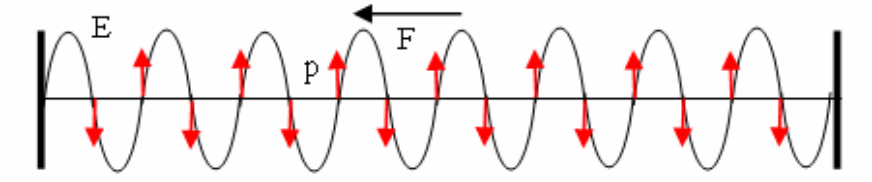


Рис. 4. Взаимодействие антенных вибраторов со стоячей волной. E - электрическое поле стоячей волны,
p - антенный вибратор, F – равнодействующая сила.

Антенные вибраторы расположены в узлах электрического поля стоячей волны, электрическое поле $\mathbf{E} = \mathbf{E}_0 \sin kx \sin \omega t$, магнитное поле $\mathbf{H} = \mathbf{H}_0 \cos kx \cos \omega t$ (x – координата вдоль распространения

бегущих компонент стоячей волны). Вибраторы, обозначенные стрелочками вверх (в чётных узлах), колеблются по закону $\mathbf{p} = \mathbf{p}_0 \sin \omega t$, а стрелочками вниз (в нечётных узлах) по закону $\mathbf{p} = -\mathbf{p}_0 \sin \omega t$. В чётных узлах электрического поля магнитное поле равно $\mathbf{H} = \mathbf{H}_0 \cos \omega t$, в нечётных $\mathbf{H} = -\mathbf{H}_0 \cos \omega t$. Определим силу $\mathbf{F}_m$, обусловленную действием магнитного поля на ток дипольной антенны (меняющийся электрический диполь), которую мы называем силой Ампера, за её формальную аналогию с обычной силой Ампера:

$$\mathbf{F}_m = \frac{1}{c}\dot{\mathbf{p}} \times \mathbf{H} = k\mathbf{p}_0 \times \mathbf{H}_0 \cos^2 \omega t . \qquad (33^*)$$

Усредняя по времени, получим постоянную на направлению составляющую:

$$\langle F_m \rangle = -kp_0 H_0 / 2 . \qquad (34^*)$$

Формула справедлива не только для четных, но и для нечётных узлов, в которых дипольный момент и магнитное поле одновременно меняют знаки на противоположные.

Электрическую силу определим по формуле:

$$\mathbf{F}_e = (\mathbf{p}\nabla)\mathbf{E} = -k\mathbf{E}_0(\mathbf{p}_0\mathbf{i}) \cos \omega t \sin \omega t = 0 , \qquad (35^*)$$

где $\mathbf{i}$ – единичный вектор вдоль направления оси x.

Равенство электрической силы $\mathbf{F}_e$ нулю обеспечивается перпендикулярностью вектора $\mathbf{p}_0$ по отношению к оси x.

Таким образом, на дипольную антенну (вибратор) в поле стоячей волны действует только постоянная по направлению сила Ампера. Электрическая сила равно нулю постоянно, а не только в среднем, как в предыдущей задаче, что, тем более, позволяет не обращаться к рассмотрению зарядовой магнитодинамической силы.

Импульсный потенциал равен $\mathbf{G} = -(\mathbf{p} \times \mathbf{H})/c$, значит, компенсирующая эфироопорная сила $\mathbf{F}_э = -\dot{\mathbf{p}} \times \mathbf{H}/c$, как водится, равна по величине, противоположна по направлению силе Ампера (33*).

***

Система взаимодействующих антенных излучателей, как оказалось, уникальна по своей самодостаточности, в том смысле, что, в отличие от других систем, позволяет придти к обоснованию эфироопорного движения, наиболее чистым и несомненным путём, опираясь только на знание широко известных всеми признаваемых магнитных и электрических сил, сводимых к силам Лоренца, $q\mathbf{E} + q\mathbf{v} \times \mathbf{H}/c$ (q – заряд) [18]. Отпадает необходимость в привлечении таких, прямо вытекающих из электродинамики, но, тем не менее,

неоднозначно воспринимаемых величин как магнитодинамическая сила и потенциалы Дарвина, которых нельзя избежать при анализе квазистатических систем [11]. Человек, ничего не знающий о явлении эфироопорности, но достаточно хорошо знакомый с классической электродинамикой может поставить задачу о взаимодействии дипольных излучателей и, решая её, открыть для себя и других эфироопорную силу и её основные свойства.

В соответствии с теоремой об энергии [17], [23], [11], антенная система под действием постоянной по направлению эфироопорной силы (8*), (31), (34*) может совершать ускоренное движение, увеличивая свою кинетическую энергию за счёт убыли внутренней энергии эфира Лоренца [11].

Возможность практического применения антенной эфироопорной силы для использования на транспорте и в энергетике определяется её величиной при технически достижимых параметрах. В качестве прототипа можно, к примеру, представить себе структуру, изображенную на Рис. 4, в которой стоячую волну создают в волноводе, начинённом блоками, изготовленными из материалов, молекулы которых обладают дипольными моментами, способными меняться с заданной частотой (может быть под действием каких-то внешних принуждающих факторов). Если, положим, молекула массой до 1000 атомных единиц имеет дипольный момент величиной в один Дебай, меняющийся с частотой, соответствующей длинам волн от сантиметрового до субмиллиметрового диапазона, то при индукции магнитного поля стоячей волны в один Тесла эфироопорная сила будет от трёх до шести порядков выше веса этой молекулы. Для третьего порядка по v/c очень даже не слабый коэффициент подъёмной силы.

Литература

1. Л Д. Ландау, Е. М. Лифшиц. Гидродинамика. Изд-во “Наука”, М., 1988, с. 359
2. Ю. Н. Иванов. Ритмодинамика, М., Новый центр, 1997
3. Филиппов А.Т. Многоликий солитон. М., Наука, 1990, с. 160-168, 263-267
4. Большая советская энциклопедия. Третье изд., 1969-1978, «Относительности теория»
5. Г. А. Лоренц. Теория электронов, М., 1953
6. Физическая энциклопедия. Главный редактор А. М. Прохоров, М., 1998, **3**, «Микроволновое фоновое излучение»

7. Физическая энциклопедия. Главный редактор А. М. Прохоров, М., 1998, «Сингулярность космологическая», «Электродинамика, магнитный заряд», «Диполь электрический»
8. А. Эйнштейн. К электродинамике движущихся тел. Собр. науч. трудов в 4-х томах. – М.: Наука, 1965. Т.1, с. 7 - 35
9. Эйнштейн А. Эфир и теория относительности. Собр. науч. трудов в 4-х томах. – М.: Наука, 1965. Т.1, с. 682-689
10. Tom Van Flandern. Что глобальная система GPS говорит нам об относительности. Open Questions in Relativistic Physics, edited by Franco Selleri, published by Apeiron, Montreal (1998), pp. 81-90, http://www.vixri.ru/d/Flandern Tom Van Chto global%27naja navigacionnaja sistema GPS govorit nam ob otnositel%27nosti.pdf
11. Иванов Г. П. Обоснование существования эфироопорных сил в классической электродинамике, «Доклады независимых авторов», изд. «DNA», Россия-Израиль, 2010, вып. 15, с. 120 - 135, printed in USA, Lulu Inc., ID 8976094, ISBN 978-0-557-52134-0, http://tts.lt/~nara/obosn/obosnovanie.htm
12. Уиллер Дж. Предвидение Эйнштейна. М., Мир, 1970, с. 59
13. Пуанкаре А. Наука и гипотеза, Глава X, Теории современной физики, М., 1904
14. И. Е.Тамм. Основы теории электричества. , М.,"НАУКА", 1989, § 18, 103 – 105, http://tts.lt/~nara/history/tamm.html
15. G. M. Graham, D. G. Lahoz. Nature, 285, 154, 1980. http://tts.lt/~nara/history/nature.html
16. Г. П. Иванов. Пособие для проектирования эфироопорных двигателей. Новая энергетика, № 2 (17), 2004, с. 57-60. http://tts.lt/~nara/help/ozenki.htm , http://tts.lt/~nara/opyt/opyt.htm
17. Иванов Г. П. Безреактивное движение за счет энергии, извлекаемой из пространства, как следствие фундаментальных законов классической электродинамики. Сознание и физическая реальность, № 1, 2002 г., с. 21. http://tts.lt/~nara/ruspopul.htm
18. Л. Д. Ландау, Е. М. Лифшиц. Теория поля. Изд-во “Наука”, М., 1973, § 17, 34, 72, 78
19. В. А. Угаров. Специальная теория относительности, «Наука», М., § 41, 1969
20. Физическая энциклопедия (под ред. А. М. Прохорова), 1998, **4**, с. 86

21. Дж. А. Стреттон. Теория электромагнетизма, ОГИЗ, 1948, с. 540
22. Г. Корн, Т. Корн. Справочник по математике, М., «Наука», 1984, с. 128, 169
23. Иванов Г. П. Классическая электродинамика и современность. Висагинас (Литва), с. 40, 47, 2002 г. http://tts.lt/~nara/aspecty.html
24. И. В. Савельев. Курс общей физики, т. 1, М., «Наука» 1970, с. 108 – 110

Петров В.В.

Альтернативная космология

Аннотация

В статье содержится критика современной космологической модели Вселенной, основанной на известной теории Большого взрыва. Предлагается концепция принципиально другой модели Вселенной, основанной на предположении о ее бесконечности в пространстве и во времени.

Введение

В космологии вопрос о конечности или бесконечности Вселенной имеет большое значение:

если Вселенная конечна, то, как показал Фридман, она не может находиться в стационарном состоянии и должна либо расширяться, либо сжиматься;

если же Вселенная бесконечна, то всякие предположения о ее сжатии или расширении теряют какой бы то ни было смысл.

Известно, что так называемые космологические парадоксы были выдвинуты как возражения против возможности существования бесконечной Вселенной, бесконечной в том смысле, что ни ее размеры, ни время существования, ни масса заключенного в ней вещества не могут быть выражены никакими, сколь угодно большими числами. Посмотрим же, насколько обоснованными оказываются эти возражения.

Космологические парадоксы – суть и исследование

Известно, что основные возражения против возможности существования бесконечной во времени и пространстве Вселенной заключаются в следующем.

1. «В 1744 г. швейцарский астроном Ж.Ф. Шезо первым усомнился в правильности представления о бесконечной Вселенной: если количество звезд во Вселенной бесконечно, то почему все небо не сверкает, как поверхность единой звезды? Почему небо темное? Почему звезды разделены темными промежутками?» [1]. Как полагают, такое же возражение против модели бесконечной Вселенной выдвинул немецкий философ Г. Олберс в 1823 г. «Контраргумент Олберса состоял в том, что свет,

идущий к нам от далеких звезд, должен ослабляться из-за поглощения в находящемся на его пути веществе. Но в таком случае само это вещество должно нагреться и ярко светиться, как звезды». [2]. Однако так оно и есть в действительности! Согласно современным представлениям, вакуум не есть «ничто», но представляет собой «нечто», обладающее вполне реальными физическими свойствами. Тогда почему не предположить, что свет взаимодействует с этим «нечто» таким образом, что каждый фотон света при движении в этом «нечто» теряет энергию пропорционально пройденному им расстоянию, вследствие чего излучение фотона смещается в красную часть спектра. Естественно, что поглощение вакуумом энергии фотонов сопровождается повышением температуры вакуума, вследствие чего вакуум становится источником вторичного излучения, которое можно назвать фоновым. Когда расстояние от Земли до излучающего объекта – звезды, галактики – достигает некоторого предельного значения, излучение от этого объекта получает настолько большое красное смещение, что сливается с фоновым излучением вакуума. Поэтому, хотя количество звезд в бесконечной Вселенной бесконечно, количество звезд, наблюдаемых с Земли, и вообще из любой точки Вселенной, конечно – в любой точке пространства наблюдатель видит себя как бы в центре Вселенной, из которого наблюдается некоторое ограниченное количество звезд (галактик). Вместе с тем, на частоте фонового излучения все небо сверкает как поверхность единой звезды, что и наблюдается в действительности.

Известно, что первым «красное смещение» обнаружил Хаббл в 1929 г. Как описывает Т.А. Агекян в [5], «Хаббл установил, что отношение изменения длины волны $\Delta\lambda$ к самой длине волны λ одинаково для всех линий спектра данной галактики. «Исследовав вопрос подробно, Хаббл установил, что отношение $\Delta\lambda / \lambda$, определяемое по спектру галактики, пропорционально расстоянию до галактики, т.е. красное смещение в спектрах галактик пропорционально расстоянию до галактик (подчеркнуто мной – В.П.). Этот закон, названный законом красного смещения спектров галактик, (устанавливающий зависимость величины красного смещения от расстояния до галактик – В.П.) … является одним из фундаментальнейших законов Вселенной, одним из основных законов природы (тогда как зависимость величины красного смещения от скорости «разбегания» галактик является произвольной интерпретацией этого закона – В.П.)».

Закон красного смещения, т.е. зависимость величины смещения от расстояния до излучающего объекта, может быть записан в виде:

$$c \cdot z = H \cdot r, \qquad (1)$$

откуда следует:

$$r = c \cdot z / H,$$

где $z = \Delta\lambda / \lambda$ – величина красного смещения; H = 75 (км/с)/Мпс; r – расстояние до излучающего объекта.

Так как отношение c к H равно 4000, получаем простое соотношение между расстоянием до источника излучения и его красным смещением:

$$R = 4000\, z \quad \text{Мпс} \qquad (2)$$

Исследовав в 1956 г. излучение 806 галактик, Хьюмасон, Мейалл и Сендидж подтвердили истинность закона Хаббла, выраженного в виде формулы (1). Это дает возможность определения расстояний до наиболее удаленных из известных в настоящее время объектов – квазаров. Так, для квазара OQ 172 величина z = 3,53. Подставляя величину этого смещения в формулу (2), получим: r = 4000 · 3,53 = 14120 мегапарсек или около 46 миллиардов световых лет.

Это означает, что в настоящее время мы наблюдаем свет, излученный квазаром 46 миллиардов лет тому назад из той самой точки, или области пространства, где мы его видим в настоящее время. Таким образом, возраст Вселенной никак не может быть меньше 46 миллиардов лет, что абсолютно не соответствует выводам теории Большого Взрыва.

Для источника, зарегистрированного в каталоге BATSE под номером 6665, красное смещение z равно 5,0. В соответствии с формулой (2) расстояние r до этого источника оказывается равным 4000 · 5,0 = 20000 Мпс = 20000 · 3,26 = 65,2 миллиарда световых лет, что в 4 раза превышает возраст Вселенной, определяемый на основе теории Большого взрыва. Таким образом, теория Большого взрыва не соответствует достаточно точным наблюдательным данным.

2. В 1850 г. немецкий физик Р. Клаузиус «... пришел к выводу, что в природе теплота переходит от теплого тела к холодному... состояние Вселенной должно все больше изменяться в определенном направлении... Эти представления развил английский физик Уильям Томсон, согласно которому все физические процессы во Вселенной сопровождаются превращением световой энергии в теплоту» [1]. Следовательно, Вселенную ожидает

«тепловая смерть», поэтому бесконечное существование Вселенной во времени невозможно. В действительности, это не так. Согласно современным представлениям, в «световую энергию» и «теплоту» вещество превращается в результате термоядерных процессов, идущих в звездах. «Тепловая смерть» наступит, как только все вещество Вселенной «сгорит» в термоядерных реакциях. Очевидно, что в бесконечной Вселенной и запасы вещества также являются бесконечными, следовательно, все вещество Вселенной «сгорит» за бесконечно большое время. «Тепловая смерть» угрожает скорее конечной Вселенной, поскольку запасы вещества в ней ограничены. Впрочем, и в случае конечной Вселенной ее «тепловая смерть» не является обязательной. Еще Ньютон сказал примерно следующее: «Природа любит превращения. Почему бы в ряду различных превращений не может быть таких, в которых вещество превращается в свет, а свет – в вещество». В настоящее время такие превращения хорошо известны: с одной стороны, вещество превращается в свет в результате термоядерных реакций, с другой – фотоны, т.е. свет, при определенных условиях превращаются в две вполне материальных частицы – электрон и позитрон. При «сгорании» вещества массой m выделяется энергия E, равная mc^2, соответственно, при образовании вещества (электрона и позитрона) массой m поглощается такое же количество энергии. В результате поддерживается тепловое равновесие, при котором температура вакуума (эфира) оказывается равной 2,7К. Таким образом, в природе осуществляется кругооборот вещества и энергии, что исключает «тепловую смерть» Вселенной.

3. В 1895 г. немецкий астроном Х. Зелигер «... пришел к выводу, что представление о бесконечном пространстве, заполненном веществом при конечной его плотности, несовместимо с законом тяготения Ньютона... Если в бесконечном пространстве плотность вещества не бесконечно мала, а каждые две частицы по закону Ньютона взаимно притягиваются, то сила тяготения, действующая на любое тело, была бы бесконечно большой, и под ее воздействием тела получили бы бесконечно большое ускорение» [1].

Как объясняет, например, И.Д. Новиков в [3], суть гравитационного парадокса заключается в следующем. «Пусть Вселенная в среднем равномерно заполнена небесными телами, так что средняя плотность вещества в очень больших объемах пространства одинакова. Попытаемся рассчитать в соответствии с законом Ньютона, какая гравитационная сила, вызванная всем

бесконечным веществом Вселенной, действует на тело (например, галактику), помещенную в произвольную точку пространства. Предположим сначала, что Вселенная пуста. Поместим в произвольную точку пространства пробное тело *A*. Окружим это тело веществом плотности, заполняющим шар радиуса *R*, чтобы тело *A* было в центре шара. Ясно без всяких расчетов, что в силу симметрии тяготение всех частичек вещества шара в его центре уравновешивает друг друга, и результирующая сила равна нулю, т.е. на тело *A* не действует никакая сила. Будем теперь добавлять к шару новые и новые сферические слои вещества той же плотности... сферические слои вещества не создают сил тяготения во внутренней полости и добавление этих слоев ничего не меняет, т.е. по-прежнему равнодействующая сила тяготения для *A* равна нулю. Продолжая процесс дополнения слоев, мы приходим в пределе к бесконечной Вселенной, равномерно заполненной материей, в которой результирующая гравитационная сила, действующая на *A*, равна нулю.

Однако рассуждения можно проводить и иначе. Возьмем снова однородный шар радиуса *R* в пустой Вселенной. Поместим наше тело не в центр этого шара с той же плотностью вещества, что и раньше, а на краю его. Теперь сила тяготения, которая действует на тело *A*, будет равна согласно закону Ньютона

$$F = GMm/R^2, \qquad (2)$$

где *M* – масса шара; *m* – масса пробного тела *A*.

Будем теперь добавлять сферические слои вещества к шару. После того, как к этому шару добавлена сферическая оболочка, она не добавит гравитационных сил внутри себя. Следовательно, сила тяготения, действующая на тело *A*, не изменится и по-прежнему равна *F*.

Продолжим процесс добавления сферических оболочек вещества одинаковой плотности. Сила *F* остается неизменной. В пределе мы снова получаем Вселенную, заполненную однородным веществом с той же плотностью. Однако теперь на тело *A* действует сила *F*. Очевидно, в зависимости от выбора первоначального шара, можно получить силу *F* после перехода к однородно заполненной веществом Вселенной. Вот эта неоднозначность и получила название гравитационного парадокса... теория Ньютона не дает возможности без добавочных предположений однозначно рассчитать гравитационные силы в бесконечной Вселенной. Только теория Эйнштейна позволяет рассчитать эти силы без всяких противоречий».

Противоречия, однако, сразу же исчезают, если мы вспомним, что бесконечная Вселенная – это не то же самое, что очень большая:

в бесконечной Вселенной сколько слоев вещества мы бы не прибавляли к шару, за его пределами остается еще бесконечно большое количество вещества;

в бесконечной Вселенной шар любого, сколь угодно большого радиуса с пробным телом на его поверхности, всегда можно окружить сферой еще большего радиуса таким образом, что и шар, и пробное тело на его поверхности окажутся внутри этой новой сферы, заполненной веществом той же плотности, что и внутри шара; в этом случае величина сил тяготения, действующих на пробное тело со стороны шара, окажется равной нулю.

Таким образом, сколько бы мы не увеличивали радиус шара и сколько бы слоев вещества не прибавляли, в бесконечной Вселенной, равномерно заполненной веществом, величина сил тяготения, действующих на пробное тело, всегда будет равна нулю. Другими словами, величина сил тяготения, создаваемых всем веществом Вселенной, в любой ее точке равна нулю. Однако если за пределами шара, на поверхности которого лежит пробное тело, нет вещества, т.е. если все вещество Вселенной сосредоточено внутри этого шара, тогда на пробное тело, лежащее на поверхности этого тела, действует сила тяготения, пропорциональная массе заключенного в шаре вещества. Под действием этой силы пробное тело, и вообще все внешние слои вещества шара, будет притягиваться к его центру – шар конечных размеров, однородно заполненный веществом, неизбежно будет сжиматься под действие сил тяготения. Этот вывод следует как из закона всемирного тяготения Ньютона, так и из общей теории относительности Эйнштейна: Вселенная конечных размеров не может существовать, так как под действием сил тяготения ее вещество должно непрерывно сжиматься к центру Вселенной.

«Ньютон понимал, что по его теории тяготения звезды должны притягиваться друг к другу и поэтому, казалось бы... должны упасть друг на друга, сблизившись в какой-то точке... Ньютон говорил, что *так* (здесь и далее выделено мной – *В.П.*) действительно *должно было бы быть*, если бы у нас было лишь *конечное* число звезд в *конечной* области пространства. Но... если число звезд *бесконечно* и они более или менее *равномерно* распределены по *бесконечному* пространству, то этого *никогда* не произойдет, так как нет центральной точки, куда им нужно было бы падать. Эти рассуждения – пример того, как легко попасть впросак, ведя разговоры о бесконечности. В бесконечной

Вселенной любую точку можно считать центром, так как по обе стороны от нее число звезд бесконечно. (Тогда можно – В.П.) ... взять конечную систему, в которой все звезды падают друг на друга, стремясь к центру, и посмотреть, какие будут изменения, если добавлять еще и еще звезд, распределенных приблизительно равномерно вне рассматриваемой области. Сколько бы звезд мы ни добавили, они всегда будут стремиться к центру» [2]. Таким образом, чтобы не «попасть впросак», мы должны выделить из бесконечной Вселенной некоторую *конечную* область, убедиться в том, что в такой *конечной* области звезды будут падать по направлению к центру этой области, после чего распространить этот вывод на бесконечную Вселенную и заявить, что существование такой Вселенной невозможно. Вот пример того, как «... на вселенную в целом...» переносится «... как нечто абсолютное такое состояние, ...которому ... может быть подвержена ... только часть материи» (Ф. Энгельс. Анти-Дюринг), например, отдельно взятая звезда или скопление звезд. В действительности, так как «в бесконечной Вселенной любую точку можно считать центром», количество таких точек-центров бесконечно. По направлению к какой же из этого бесконечного множества точек будут двигаться звезды? И еще: если даже вдруг обнаружится такая точка, то бесконечное количество звезд будет двигаться в направлении этой точки бесконечное время и сжатие в этой точке всей бесконечной Вселенной произойдет также за бесконечное время, т.е. никогда. Иное дело, если Вселенная конечна. В такой Вселенной существует единственная точка, которая и есть центр Вселенной – это точка, из которой началось расширение Вселенной и в которой опять сосредоточится все вещество, когда расширение Вселенной сменится ее сжатием. Таким образом, именно конечная Вселенная, т.е. Вселенная, размеры которой в каждый момент времени и величина сосредоточенного в ней вещества могут быть выражена какими-то конечными числами, обречена на сжатие. Находясь в состоянии сжатия, Вселенная никогда не сможет выйти из этого состояния без какого-то внешнего воздействия. Поскольку, однако, вне Вселенной нет ни вещества, ни пространства, ни времени, единственной причиной расширения Вселенной может быть действие, выраженное словами «Да будет свет!». Как написал однажды Ф. Энгельс, «Мы можем вертеться и изворачиваться как нам угодно, но... мы каждый раз опять возвращаемся... к персту Божию» (Ф. Энгельс. Анти-Дюринг). Однако перст Божий не может быть предметом изучения науки.

Заключение

Анализ так называемых космологических парадоксов позволяет заключить следующее.

1. Мировое пространство не является пустым, но заполнено некоторой средой, неважно, назовем ли мы эту среду эфиром или физическим вакуумом. При движении в этой среде фотоны теряют энергию пропорционально пройденному ими расстоянию, вследствие чего излучение фотонов смещается в красную часть спектра. В результате взаимодействия с фотонами температура вакуума или эфира повышается на несколько градусов выше абсолютного нуля, вследствие чего вакуум становится источником вторичного излучения, соответствующего его абсолютной температуре, что и наблюдается в действительности. На частоте этого излучения, которое действительно является фоновым излучением вакуума, все небо оказывается одинаково ярким, как это и предполагал Ж.Ф. Шезо.

2. Вопреки предположению Р. Клаузиуса, «тепловая смерть» не угрожает бесконечной Вселенной, включающей бесконечное количество вещества, которое может превратиться в теплоту за бесконечно большое время, т.е. никогда. «Тепловая смерть» угрожает конечной Вселенной, включающей конечное количество вещества, превращение которого в тепло может произойти за конечное время. Именно поэтому существование конечной Вселенной оказывается невозможным.

3. В бесконечной Вселенной, размеры которой не могут быть выражены никаким, сколь угодно большим числом, равномерно заполненной веществом при ненулевой его плотности, величина сил тяготения, действующих в любой точке Вселенной, равна нулю – это и есть истинный гравитационный парадокс бесконечной Вселенной. Равенство нулю сил тяготения в любой точке бесконечной Вселенной, равномерно заполненной веществом, означает, что пространство в такой Вселенной всюду является Евклидовым.

В конечной Вселенной, т.е. во Вселенной, размеры которой могут быть выражены какими-то, пусть и очень большими числами, на пробное тело, находящееся «на краю» Вселенной, действует сила притяжения, пропорциональная массе заключенного в ней вещества, вследствие чего это тело будет стремиться к центру Вселенной – конечная Вселенная, вещество которой равномерно распределено во всем ее ограниченном объеме, обречена на сжатие,

которое никогда не сменится расширением без какого-то внешнего воздействия.

Таким образом, все возражения, или парадоксы направленные, как считают, против возможности существования бесконечной во времени и пространстве Вселенной, в действительности направлены против возможности существования именно конечной Вселенной. В действительности, Вселенная бесконечна и в пространстве, и во времени; бесконечна в том смысле, что ни размеры Вселенной, ни количество заключенного в ней вещества, ни время ее жизни не могут быть выражены никакими, сколь угодно большими числами – бесконечность, она и есть бесконечность. Бесконечная Вселенная никогда не возникала ни как результат внезапного и необъяснимого расширения и дальнейшего развития некоторого «доматериального» объекта, ни как результат Божественного творения.

Надо полагать, тем не менее, что приведенные выше доводы покажутся сторонникам теории Большого взрыва абсолютно неубедительными. Как считает известный ученый Х. Альвен «Чем меньше существует научных доказательств, тем более фанатичной делается вера в этот миф. Похоже на то, что в теперешней интеллектуальной атмосфере огромным преимуществом космологии «Большого взрыва» служит то, что она является оскорблением здравого смысла: credo, quia absurdum (верю, ибо абсурдно)» (цитируется по [4]). К сожалению, с некоторых пор «фанатичная вера» в ту или иную теорию является традицией: чем больше появляется доказательств научной несостоятельности таких теорий, тем более фанатичной становится вера в их абсолютную непогрешимость.

Этими словами мы и закончим наше краткое исследование.

Литература

1. Климишин И.А. Релятивистская астрономия. М.: Наука, 1983.
2. Хокинг С. От большого взрыва до черных дыр. М.: Мир, 1990.
3. Новиков И.Д. Эволюция Вселенной. М.: Наука, 1983.
4. Гинзбург В.Л. О физике и астрофизике. Статьи и выступления. М.: Наука, 1985.
5. Агекян Т.А. Звезды, галактики, Метагалактика. Главная редакция физико-математической литературы. М.: Наука, 1981.

Кайнов А.Б.

О механизме расширения вселенной

Аннотация

Объекты, распространяющиеся по пространству в результате их случайных перемещений, и галактики во Вселенной движутся подобным образом. Это сходство требует уточнения законов тяготения и позволяет отказаться от гипотезы антитяготения.

Из закона Всемирного тяготения следует, что галактики должны притягиваться друг к другу, сближаясь в результате взаимодействия. Однако такого сближения, как всеобщей тенденции, не наблюдается. Напротив, как установлено, галактики удаляются друг от друга. Возможно, силам тяготения, в глобальном масштабе, противодействуют силы отталкивания, например порожденные действием таинственной «темной энергии». Также возможно и то, что закон Всемирного тяготения неприменим в отношении галактик, а их разбегание обусловлено действием иного механизма. В настоящее время популярна модель с «темной энергией». Но нет ли иных причин для разбегания галактик? Исследованию этого вопроса посвящена данная статья.

Открытие в начале 20 века красного смещения в спектрах излучения галактик выявило, что Вселенная является нестационарной системой, галактики в которой удаляются друг от друга (разбегаются) согласно закону Хаббла [1] со скоростью $\mathbf{v \approx H_0 R}$, где $\mathbf{H_0}$ – постоянная Хаббла, $\mathbf{R}$ – расстояние до галактики. Последующее изучение движения галактик обнаружило его некоторые особенности [2]:

- в ближних окрестностях нашей галактики, ряд галактик, находящихся на расстоянии более 1...2 Мпк от нее, удаляется по закону Хаббла, образуя местный хаббловский поток, а другие, находящиеся ближе (Местная группа), движутся иначе, аналогичное поведение – разделение галактик на движущиеся согласно закону Хаббла и не подчиняющиеся этому закону, характерно и для других скоплений галактик;

- значение постоянной Хаббла, определенное для сравнительно небольших объемов пространства с неравномерным распределением галактик, близко к ее значению для значительных

по размеру областей Вселенной, в которых галактики распределяются равномерно, местная постоянная Хаббла составляет 72±8 км/с/Мпк, в масштабах от 4 до 200 Мпк значение постоянной Хаббла составляет 62±7 км/с/Мпк;

- наблюдение сверхновых звезд выявило положительное ускорение движения (разбегания) наиболее удаленных галактик.

Основной причиной разбегания галактик называют, подтверждаемое теоретически, явление антитяготения, порождаемое действием «темной энергии», причем считается, что граница в 1,3...1,5 Мпк обусловлена началом преобладания антитяготения над тяготением [2]. Однако природа и механизм действия «темной энергии» остаются до настоящего времени невыясненными и поэтому гипотеза о действии «темной энергии» представляется спорной.

В качестве альтернативы предлагается другая гипотеза, объясняющая причины разбегания галактик, в соответствии с которой удаление галактик друг от друга связано с уменьшением плотности распределения галактик в результате их свободного перемещения по пространству (блуждания), описываемого законом нормального распределения. Такое движение галактик возможно, если гравитационное взаимодействие между ними осуществляется иначе, чем это следует из закона Всемирного тяготения, и не является определяющим для их поведения. Возможность отклонения величины гравитационного притяжения галактик от закона Всемирного тяготения отмечена в [3]. Суть альтернативной модели изложена ниже.

Пусть имеется трехмерное пространство, разбитое на одинаковые ячейки с размерами $\mathbf{1 \times 1 \times 1}$, пронумерованные от центра пространства так, что номера ячеек вдоль каждой оси принимают значения: 0; ±1; ±2; ±3 … . Пусть некоторый объект, первоначально находившийся в ячейке с номером «0, 0, 0» - центр пространства, осуществляет переходы по трем осям одновременно, изменяя за один шаг номер ячейки, в которой находится, на единицу вдоль каждой оси, при этом вероятности увеличения или уменьшения номеров ячеек равны. Тогда, по теореме Лапласа [4], после совершения $\mathbf{n}$ переходов, вероятность попадания объекта в ячейку с номером $(\mathbf{m_x}; \mathbf{m_y}; \mathbf{m_z})$ составит

$$\mathbf{P_{n,m} \approx (2 / \pi n)^{3/2} \cdot \exp[- (m_x^2 + m_y^2 + m_z^2) / 2n]} \; .$$

Если переходы по трехмерному пространству из ячейки «0, 0, 0» совершают одновременно N объектов, а время совершения одного шага $\tau = t / n$, где t - время, прошедшее с начала блуждания, то величина

$$v_r \approx r \cdot [1 - (m_x^2 + m_y^2 + m_z^2) / 3n] / 2t ,$$

где r - минимальное расстояние между объектами в ячейке, является скоростью относительного движения соседних объектов в ячейке $(m_x; m_y; m_z)$, при условии, что объекты распределены в этой ячейке равномерно. Такая скорость может быть, как больше нуля – взаимное удаление объектов при $(m_x^2 + m_y^2 + m_z^2) < 3n$ – область уменьшения плотности распределения объектов, так и меньше нуля – взаимное сближение объектов при $(m_x^2 + m_y^2 + m_z^2) > 3n$ – область увеличения плотности распределения объектов. Величина

$$H = [1 - (m_x^2 + m_y^2 + m_z^2) / 3n] / 2t$$

подобна постоянной Хаббла H_0.
Если $r = l$ – размер ячейки, то

$$v_l \approx l \cdot [1 - (m_x^2 + m_y^2 + m_z^2) / 3n] / 2t$$

представляет собой, условно, скорость линейного расширения указанной ячейки. Если объекты, для которых определяется скорость их взаимного удаления, расположены в разных ячейках пространства, то искомая величина скорости определяется суммой скоростей расширения ячеек, расположенных между данными объектами.

Рассмотрим движение объекта относительно центра пространства. Пусть объект находится в ячейке такой, что $m_x = m_y = m_z = m$. Тогда, при $m >> 1$, расстояние от центра пространства до объекта

$$R \approx 3^{1/2} \cdot ml ,$$

а скорость его удаления от центра пространства

$$v_r \approx R \cdot (1 - m^2 / 3n) / 2t ,$$

где m – пропорционально расстоянию до удаляющегося объекта, а n – пропорционально времени, прошедшему с начала блуждания, причем величины m и n – безразмерные.
Ускорение удаления от центра пространства объекта, находящегося в ячейке $m_x = m_y = m_z = m$, определяется выражением

$$a \approx R \cdot (2m^2 / 3n - 1) / 2t^2 .$$

При $m > (3n / 2)^{1/2}$, ускорение удаления положительно $a > 0$, а величина H уменьшается более чем в два раза по сравнению с ее значением в центре пространства при $m = 0$ $(H < 0{,}5 / 2t)$.
В ячейке $m_x = m_y = m_z = m$, при $m > (3n / 2)^{1/2}$, вероятность появления объекта $P_{n,m} < 0{,}1 \cdot (2 / \pi n)^{3/2}$. То есть, изменение плотности распределения объектов по пространству, в области отрицательных значений ускорений удаления, достаточно мало изменяется (в пределах одного порядка) от расстояния до центра пространства, и в большей степени зависит от прошедшего с момента начала блуждания времени (количества совершенных шагов).

Как видно из вышеизложенного, если большую часть наблюдаемой Вселенной отождествить с областью отрицательных значений ускорения удаления объектов, а место наблюдения (галактику Млечный путь) считать расположенным достаточно глубоко внутри этой области, то поведение объектов, участвующих в процессе случайного блуждания, аналогично поведению галактик:

- скорость взаимного удаления объектов, также как и в законе Хаббла, приблизительно пропорциональна расстоянию между ними и обратно пропорциональна времени, прошедшего с начала блуждания;

- при увеличении расстояния между объектами, скорость взаимного удаления объектов отклоняется от линейной зависимости в сторону уменьшения, что находит подтверждение в некотором уменьшении величины постоянной Хаббла с увеличением расстояний, для которых эта постоянная определялась;

- на значительных расстояниях от центра пространства, ускорение движения (удаления) объектов положительно так же, как ускорение разбегания наиболее удаленных галактик.

Тот факт, что величина постоянной Хаббла, определенная для небольших объемов пространства с неравномерным распределением галактик, близка к ее значению для значительных по размеру областей, в которых галактики распределяются равномерно, подтверждает независимость этой постоянной от плотности распределения вещества в пространстве.

В области снижения плотности объектов, вплоть до границ возникновения положительных значений ускорения их удаления от центра пространства, различия в плотности распределения объектов по величине не превышают одного порядка, что близко к ситуации с приблизительно равной плотностью распределения галактик в наблюдаемой части Вселенной [2].

Разделение галактик на «Местную группу» и хаббловский поток может быть объяснено следующим образом. Скорость движения галактики содержит случайную и систематическую составляющие. Случайная составляющая – это собственная скорость галактики, как предполагается независящая от расстояния до этой галактики. Систематическая составляющая – это скорость, связанная с уменьшением плотности распределения галактик вследствие их свободного блуждания, приблизительно линейно увеличивающаяся с расстоянием. Если галактики расположены сравнительно недалеко друг от друга, систематическая составляющая меньше случайной – галактики движутся в произвольных направлениях. При увеличении расстояния между галактиками, величина систематической составляющей возрастает – галактики разбегаются.

Если предлагаемая альтернативная гипотеза верна, то в закономерностях движения галактик должно наблюдаться следующее:

- отношение скорости удаления галактики к расстоянию до нее должно уменьшаться при увеличении этого расстояния;

- ускорения удаления галактик должны иметь преимущественно отрицательные значения, положительные значения должны наблюдаться на больших расстояниях от места наблюдения, при низких, относительно величины местной постоянной Хаббла, значениях этой постоянной;

- в области наблюдаемой Вселенной (до границ возникновения положительных значений ускорения удаления) должна проявляться пространственная анизотропия плотности

распределения галактик (в пределах одного порядка) и величины постоянной Хаббла (до двукратного уменьшения относительно местной постоянной Хаббла).

Литература

1. Физика: Энциклопедия./Под ред. Ю.В. Прохорова. – М.: Большая Российская энциклопедия, 2003. – 944 с.: ил.
2. И.Д. Караченцев, А.Д. Чернин. Темная энергия в ближней Вселенной. http://inauka.ru/.
3. Физика темноты или умножение сущностей. http://ankajnov.narod.ru/
4. Математика: Энциклопедия./Под ред. Ю.В. Прохорова. – М.: Большая Российская энциклопедия, 2003. – 845 с.: ил.

Каравдин П.А.

Размышления дилетанта о физике

В победном 1945 году я заканчивал деревенскую семилетку. Из физики у меня осталось впечатление, что наука еще не разобралась с проблемой света, который иногда вел себя как волны эфира, а иногда как поток корпускул. Но эта проблема меня не касается, это дело учёных. Я же стремился в технику. В вузе я неожиданно узнал, что свет обладает двойственной природой, он и волны эфира и поток корпускул. Мне было около 30 и я, подвергнув сомнению это тезис, стал изучать историю науки, чтобы понять, как наука дошла до такого абсурда. И скоро я понял, что двойственность света является следствием логической ошибки, заключающейся в совмещении двух несовместимых физик – Аристотеля и Ньютона. Собственно я ничего нового не нашел, всё это было известно задолго до меня, я только слегка подкорректировал их выводы.

Древние философы пришли к мысли, что если Мир один, то он должен состоять из бесконечного пустого пространства, в котором должны находиться все тела, состоящие из дискретной материи (из атомов). Если предположить, что Мир имеет границу, то неизбежно встанет вопрос, а что там за границей? Может быть другой Мир или Миры? Аристотель опроверг атомистов. Он считал, что вокруг неподвижного Земного шара, находящегося в центре Мира, вращается граница Мира в виде небесной сферы с небесными светилами. А что внутри между Землей и небом? Сейчас пишут о Галилее и Ньютоне, понявших закон инерции. Но первым был Аристотель, который писал, что если бы была пустота, то тело могло бы двигаться вечно: «...почему тело, приведенное в движение, где-нибудь остановится, ибо почему оно скорее остановится здесь, а не там? Следовательно, ему необходимо или покоится, или двигаться до бесконечности...» [1] .

Но так как наша Вселенная была конечной, то она должна быть заполнена материальной средой (эфиром), которая, тормозя движение, делала бы невозможным бесконечное движение в конечной Вселенной. Можно сказать, что Аристотель писал о законе инерции методом от противного. Если была бы пустота, то был бы и движение по инерции. От Ньютона прошло более 300 лет, а наука всё еще не знает что такое инерция. Вот что пишет известнейший физик-теоретик Роберт Фейнман: «... Свободное

движение не имеет никакой видимой причины. Почему предметы способны вечно лететь по прямой линии, мы не знаем. Происхождение закона инерции до сих пор остается загадкой» [2]. Ему вторит Н. Гулиа, который пишет, что понятие инерции — непростое [3].

Ньютон окончил университет, где изучал «эфирную» физику Аристотеля и был оставлен в университете преподавателем. В своих первых сочинениях он, как и принято в ученом мире, ссылался на своих предшественников, в том числе и на Аристотеля. Но вдруг, в какой-то момент он сообразил, что если планеты и кометы очень долго вращаются по своим орбитам, то это означает, что пространство не мешает их движению, что в пространстве нет эфира, что пространство пусто. Поняв это, Ньютон стал творцом классической физики, противоположной физике Аристотеля. Но нужно понимать, что законы Ньютона действуют в идеальной обстановке, когда нет никаких посторонних воздействий. Если бы не было тяготения, то все планеты и другие тела двигались бы по прямой, относительно друг друга. Никакой предельной скорости здесь быть не может. Тяготение делает невозможным прямое движение больших тел. Корпускулы света не испытывают гравитационного притяжения и потому летят по прямой.

В физике Аристотеля не было никакой теории света. Но старший современник Ньютона Христиан Гюйгенс предположил, что колебания (волны) эфира создают свет. Ньютон возразил, если нет эфира, то какие волны, какая волновая теория света? Свет может быть только потоком каких-то особых частиц (корпускул), состоящих их частиц (атомов) материи. Так появилась корпускулярная теория света. Классическая физика Ньютона, изложенная в книге «Математические начала натуральной философии», вся основана на идее пустого бесконечного пространства и дискретности материи, отсутствии эфира. «Если эфир – это такая среда, которая не тормозит движение, то она ничем не отличается от пустоты, и спор, следовательно, идет о словах, а не о деле».

Ньютон, в рамках корпускулярной теории света не объяснил явлений дифракции и интерференции света. И вскоре после его смерти началось движение назад к Аристотелю. В 1818 году Парижская АН с подачи Френеля вставила в физику Ньютона волновую теорию света из физики Аристотеля. Так началась двойственность света, лежащая в основе кризиса физики. Учёные понимали, недопустимость соединения двух физик, но уж так

убедительно объяснял Френель интерференцию и дифракцию света якобы с помощью волновой теории, что академики согласились с ним. В своё время И. Кант писал, что науке нужен философский надзор, иначе учёные каждый из-за своего «дерева» не увидят «леса». Так и случилось. Известный философ того времени Гегель пошел на поводу физиков и, чтобы как-то объяснить, совмещение вопреки логике недопустимых физик сочинил новую логику, назвав её диалектической. Если естественную формальную логику можно описать триадой «тезис-антитезис-анализ», то новую логику Гегель описал триадой «тезис-антитезис-синтез».

Преодолению кризиса мешает весьма популярная среди физиков точка зрения: "Вопрос о том, что же существует на самом деле, волна или корпускула, в глазах физика лишен содержания; это пустой вопрос" [4].

Или еще лучше: "Наше воображение бессильно представить нечто такое, что может быть одновременно и волной, и частицей, но само по себе существование дуализма волна-частица не вызывает сомнения" [5].

Физики утверждают: "Измерения Фуко показали, что скорость света в воде меньше, чем в воздухе, в соответствии с представлениями волновой теории света" [6].

И Гюйгенс, и Френель строили свои «волновые фронты» в представлении, что скорость света в более плотной среде уменьшается. Но это свойство корпускул. Волны же имеют тем больше скорость, чем плотнее среда. Можно простить Гюйгенсу и Френелю ошибку. Они не знали о скорости света в воде. Но измерения Фуко доказывают не волновую, а корпускулярную теорию света. Следовательно, все оптические явления нужно объяснять корпускулярностью света. Покажем как все свойства света (кроме интерференции) объясняются корпускулярностью.

Через вершину трехгранной стеклянной призмы «А» пустим луч света (рис. 1). Его направление не изменится. Добавим к призме «А» призму «В» так, чтобы они образовали единое целое (рис. 2). Луч света преломится. Этот рисунок позволяет понять разную роль двух призм. Призма «А» только уменьшает скорость света. Призма «В» притягивает корпускулы и изменяет направление движения света. Уберем призму «А» (рис. 3). Этот рисунок объясняет дифракцию света. На рис. 4 показано явление, известное под названием полного внутреннего отражения света. Теперь мы можем понять, что это явление не является отражением, а только притяжением. Корпускулы света при выходе из призмы .«А»

испытывают притяжение от призмы «В» и резко поворачивают влево.

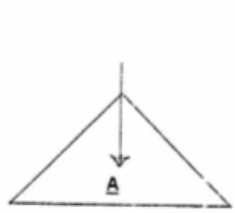


Рис. 1

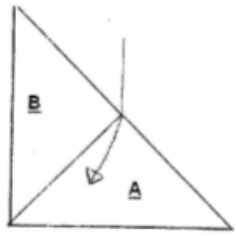


Рис.2

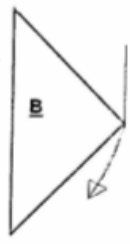


Рис. 3

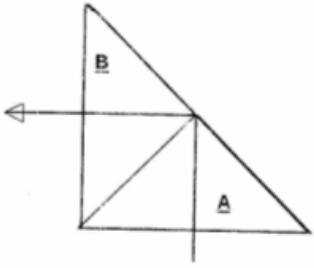


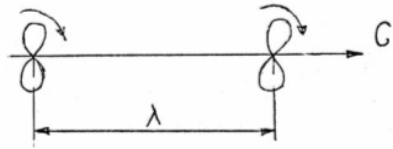
Рис. 4

Таким образом, и преломление, и дифракция, и полное внутреннее отражение имеют единую причину.

Остается объяснить интерференцию света, чтобы полностью избавиться от волновой гипотезы света.

Представим себе корпускулу света, имеющую форму восьмерки. Эта восьмерка летит по инерции через пространство и вращается в плоскости движения. Тогда количество оборотов в секунду будет частотой корпускулы. А путь, который проходит корпускула за время одного оборота - λ, будет длиной волны. Плоскость, в которой движется и вращается корпускула, будет плоскостью поляризации. Тогда наша корпускула, проходя через малое отверстие экрана, отклоняется от прямого пути (дифракция) и попадает на экран. Если в этот же момент в это же место попадет корпускула из другого отверстия, то произойдет их взаимодействие. Если они встретятся в одной фазе, то свет усилится (сложение). Если же корпускулы встретятся в противофазе, то свет погаснет(вычитание) Эта корпускула позволяет также понять, почему всегда часть света проходит через прозрачное тело, а другая часть отражается. Также легко объясняется и знаменитое красное смещение, принимаемое за расширение Вселенной. Чем больший путь прошла корпускула, тем медленней она вращается от

многочисленных контактов с различными материальными частицами.



Л.А.Друянов пишет: *«Направим пучок электронов из электронной пушки на непроницаемое препятствие, в котором имеются два отверстия. Поместим в отдалении за препятствием счетчик Гейгера и закроем одно отверстие. Пусть в этом случае счетчик регистрирует ежесекундно 2 электрона. Если откроем это отверстие и закроем другое, то снова получим 2 отсчета в секунду. II, наконец, откроем оба отверстия. На опыте при этом иногда наблюдается, что счетчик вообще перестает регистрировать электроны (2+2=0)!... Если немного подвигать счетчик в вертикальном направлении, можно найти точку, в которой он будет давать 8 отсчетов в секунду (2+2=8), т.е. вдвое больше простой суммы слагаемых. На первый взгляд всему этому трудно поверить, однако это так, и столь необычные явления обусловлены волновой природой электронов».*

Это и есть описание интерференции электронов. Фейнман утверждает, что электроны и фотоны ведут себя, хотя и необычно, но одинаково. Точно так же происходит интерференция фотонов. В одних случаях свет гасит свет, в других - свет усиливает свет. Явление интерференции впервые наблюдалось на морских волнах и никакой другой интерференции физики знать не желают. Но интерферировать могут не только волны, но и колебания. Вспомните, колебания моста, вызванные ротой солдат идущих в ногу, могут мост обрушить. Если же шаги будут вразнобой, колебаний моста можно не заметить. Колебания и волны математически неразличимы.

Корпускулу в виде восьмерки я «сконструировал» в 1965-66 годах еще не зная о странной арифметике интерференции. Но разве теперь не понятна эта арифметика? Восьмерка разрывается на колечки. Две корпускулы состоят из 4-х колечек. И тогда при усилении 4+4=8, а при ослаблении света 4 - 4=0.

Почему электроны и фотоны интерферируют одинаково? Ниже я излагаю свое понимание гравитации, которое отрицает планетарную модель Резерфорда. Электроны не точки, вращающиеся вокруг ядра, а колечки в виде тончайших нитей. Их переплетение и создаёт прочность тел. Фотоны те же колечки, свернувшиеся в восьмерку.

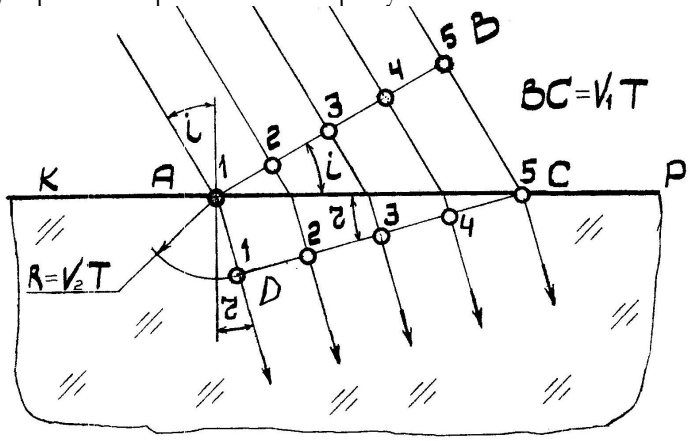
Разобравшись, хоть немного, с проблемой света перейдем к проблеме всемирного тяготения. В бесконечном пустом пространстве Вселенной находится чудовищно большое, но постоянное число одинаковых элементарных частиц – гравитонов, из которых построены все тела Вселенной. Опять ничего нового я не придумал. Многие мыслители с древних времен искали «первокирпичики». Последним, насколько я знаю, был Праут, который в XIX принял за них водород. Итак, множество объектов Вселенной состоят из одинаковых гравитонов. Как устроены они и как соединяются друг с другом нам неизвестно. Но все тела Вселенной существуют не изолированно друг от друга, а связаны между собой всемирным тяготением. И никакой причины тяготения, кроме круговорота гравитонов, придумать невозможно. Сразу возразят, что при этом возникнет не притяжение, а отталкивание. Неправда. Есть широко известный аналог тяготения – свет. Корпускулы света, состоящие из нескольких гравитонов, проходят через некоторые (прозрачные) тела не отталкивая их, а создавая слабое притяжение. П.Лебедев, доказавший что свет производит давление, доказал только, что свет оказывает давление на непрозрачные тела. В прозрачных же телах корпускулы, переходят от атома к атому, как поезд от станции к станции, имеют среднюю скорость меньше, чем в пустоте, но вылетают из атома в пустоту с первоначальной скоростью. При этом по законам физики должна происходить отдача (мини-тяготение).

Для гравитонов же нет непрозрачных тел. По аналогии со светом мы понимаем создание силы тяготения. В моих многочисленных статьях, рассеянных по газетам и Интернету есть более конкретное описание механизма тяготения, но здесь я предпочитаю философское объяснение.

Взаимодействуя с гравитонами, атомы тел непрерывно пульсируют, т. е. перемагничиваются. Перемагничивание же соответствует нагреванию тела. Это означает, что гравитоны планет разогревают Солнце, а его гравитоны греют планеты. Но так как объем планеты большей частью много меньше объема Солнца, то и нагрев ее соответственно меньше. Но не может быть полного равенства между излучением и приемом гравитонов. В итоге этого неравенства одни планеты постепенно увеличивают свою массу, другие - уменьшают.

Самым серьезным аргументом в защиту волновой гипотезы света несомненно является вывод Гюйгенсом закона преломления света якобы с помощью волновой гипотезы. Этот вывод приводится

Г.Ландсбергом в «Оптике» (М. 1978) на стр. 19. Я позволю себе подкорректировать рисунок Ландсберга, чтобы показать, что преломление света прекрасно интерпретируется и с помощью корпускулярной теории. Вот мой рисунок.



На рисунке показан луч света из корпускул. В луче выделены два положения корпускул 1,2,3,4,5. Пока корпускула 5 проходит путь BC в воздухе со скоростью V_1 , корпускула 1 в стекле проходит меньший путь AD с меньшей скоростью V_2. Чтобы найти положение корпускулы 1 в стекле нужно из точки A радиусом R= V_2T провести дугу, а из точки C провести касательную к этой дуге. В общей точке дуги и касательной и будет находиться корпускула 1. Таким образом фронт корпускул AB изменит свое положение в DC (произойдет преломление). Я описываю столь подробно суть преломления, потому что этот мой рисунок уже был опубликован, но люди «в упор» не понимали причину преломления, а обвиняли меня во всех грехах. Суть преломления в том, что в более плотной среде корпускулы уменьшают скорость. Если бы свет был волнами, то преломление происходило бы в другую сторону. Я не привожу здесь вывод закона преломления, он есть в упомянутой «Оптике», и доказывает не волновую гипотезу, а корпускулярную теорию.

Литература

1. Аристотель. Соч. т.3, М. 1981 г. с.139
2. Р. Фейнман. Характер физических законов. М. 1987. с. 14.
3. Н. Гулиа. «Инерция» М. 1982. с.11
4. Р.В. Поль. «Оптика и атомная физика» М.1966. с 480.
5. Поль Девис. "Суперсила" М.1981.с.30.
6. Ландсберг. "Оптика" М.1976. с. 425.
7. Л. Друянов. «Законы природы и их познание» М.1982 г. с.8-9.

Серия: **ЭВОЛЮЦИЯ**

Миркин В.И.

Далась обезьянам эта палка

Вряд ли кто оспорит ту истину, что становление разума человека происходило одновременно и взаимозависимо с развитием его рук. Но чтобы это стало возможным, чтобы руки приобрели такую чувствительность, такой диапазон усилий от ничтожно малых до достигающих десятков килограмм, необходимо было освободить их от функций опоры при хотьбе. То есть, прачеловек должен был выпрямиться. Что удивительно: по-прежнему остается непонятно, зачем обезьяна встала на задние лапы?

Всем известно утверждение (якобы Энгельса), что обезьяне потребовалось взять в «руки» палку, чтобы сбить банан. Утверждение выглядит наивно.

Во-первых, бананы не растут на такой высоте, чтобы обезьяна с палкой могла бы все их достать (ей все равно придется залезть на дерево, чтобы сорвать верхние). Во-вторых, обезьяна так хорошо умеет лазить по деревьм, что ей и в «голову» не придет идти и искать палку (которая явно не лежит под пальмой). Она за пару секунд заберется и по гладкому стволу, и по ветвистому дереву в любую точку его кроны. И при этом нужно учитывать «психологию» обезьяны: то, что может быть сорвано лапой отнюдь не очевидно может быть сбито палкой (по крайней мере, вам эту технологию кто-то показал в детстве).

В-третьих, процесс сбивания плода палкой занимает несколько секунд. Все остальное время обезьяна стоит на четырех конечностях, и все, что она умеет и любит гораздо удобнее делать на них. Почему какое-то действие, занимающее не более 1% времени, вдруг, начнет

превалировать над гораздо более длительными процессами? Разве кошки, которые встают на задние лапы, чтобы передними стучать в дверь, тоже скоро примут вертикальную стойку?

Иное предположения о роли палки в переходе обезьяны к прямохождению высказано в книге «Логика антропогенеза. Происхождение человека еще не завершено», выпущенной в Санкт-Петербургском издательстве «Алетейя» в 2008 году Виктором Мерцаловым. Он доказывает, что обезьяны взяли в «руки» палку, защищаясь от диких зверей, и при этом им пришлось постоянно носить палку с собой в передних лапах.

Есть все основание сомневаться в очевидности такого предположения. Во-первых, любому четвероногому гораздо удобнее переносить предметы в зубах. Во-вторых, при переходе на прямохождение у любой особи неизбежен длительный период, когда ходить и держать равновесие неудобно, скорости перемещения бы практически не было. Да и откуда у обезьян взялась бы техника удара палкой? У спортивных специалистов существует термин «мышечная память». Наверное, он не совсем верен, поскольку в запоминании движения обязательно должен участвовать мозг. Но, тем не менее, для запоминания движения требуется 500 повторений, да и то при наличии тренера, который мог видеть все фазы движения. Скорее всего, у обезьяны была только одна попытка. И еще представьте себе обезьяну, стоящую в позе бейсболиста (откуда она вообще может знать, какую ногу выставить вперед и как держать палку, чтобы нанести сильный и своевременный удар), сцепив зубы, мужественно готовясь отразить атаку дикого зверя.

Кроме того, средняя и крупная обезьяны – очень сильные животные с лапами, когтями и зубами, которые и без палки смогут разорвать любое среднее животное.

Палка нужна бы для крупных животных, таких как леопарды, гепарды, тигры и львы. Для таких зверей нужна была длинная и тяжелая палка, взмах которой требует большого размаха и, самое главное, длительного времени. Не уверен, что современный человек, который с детства умеет обращаться с палкой, сумел бы нанести такой удар.

Слышал мнение, что обезьяны выпрямились, поскольку оказались в местности, которую быстро затопило водой (те, кто не встал на задние лапы, утонули). Есть все основания сомневаться в этой версии: четвероногие в воде не встанут на задние лапы (ходить по дну неудобно, физически трудно из-за сопротивления воды, опасно из-за ям, которых не видно), они просто поплывут.

Можно придумать версию, что спустившись с дерева обезьяна попала в высокую траву, и чтобы видеть дальше ей пришлось подняться на задние лапы. И здесь возникает сомнение: из соображений безопасности лучше бы не высовываться. Но есть еще одно обстоятельство, о котором я скажу ниже.

Таким образом вопрос о том, почему же обезьяна выпрямилась, остается открытым.

Конечно, описанные выше предположения всего лишь плод фантазии их авторов. Да другого и быть не может. Разве только нашли большое количество черепов животных, проломленных ударами тупыми предметами. А поскольку не нашли, то выскажу свое предпожение. Причем, именно предположение, поскольку доказать это невозможно: оно основано лишь на логических рассуждениях.

Вот весьма вероятный сценарий событий. На равнинной местности деревья начали редеть, и их спасительные для обезьян кроны уже не соприкасались. Вынужденные периодически перебегать от одной группы деревьев к другой, теряя при этом сородичей, достающихся в пищу хищникам, те были вытеснены дикими животными с

равнины на крутые склоны гор, где четырехлапые перемещались с трудом.

Здесь необходимо пояснение. Любой процесс в эволюции является вероятностным. При пересечении местности между деревьями, обезьяны «решали» задачу: либо всем умереть от голода, либо потерять одну-две особи при перебежке. Собственно, мы и сейчас решаем подобные задачи, когда летаем на самолетах. При невысокой плотности хищников малые потери были еще терпимы, но при ее увеличении возникал вопрос о выживании обезьян как вида. Они неизбежно искали такую местность, где хищников было бы меньше.

Я сталкивался с возражением против моей гипотезы, что вот горные козлы прекрасно перемещаются в горах и не стали двуногими. Во-первых, то, что горные козлы не стали двуногими, не является доказательством того, что этого не могли сделать обезьяны (наверное, козлы никак не могли приспособить копыта к каким-то функциям). Во-вторых, горные козлы не конкуренты обезьянам, здесь можно было бы назвать снежных барсов. Но не известно, существовали ли тогда снежные барсы, а если существовали, то каково было их количество. Наверное, их было меньше, чем равнинных животных, да и нападать на крутых склонах труднее, ведь каждый возможный промах в атаке не так-то легко компенсировать.

Итак, нет причин не принимать такую версию. Как могли развиваться события дальше. На таких склонах по деревьям не попрыгаешь: нужно ходить по земле. Если идти вверх, то работают, в основном, только задние конечности, а передние нужны лишь для сохранения равновесия. Ну, а если идти вбок, и, особенно, вниз, то передвигаться можно только боком приставными шагами (шаг вбок одной ногой и подтягивание другой), поддерживая себя одной рукой.

И тут мы сталкиваемся с еще одним парадоксом (и это как раз то обстоятельство, к которому я обещел вернуться). Многие виды животных делятся на правшей и левшей. Однако, их соотношение с небольшими отклонениями приблизительно такое: процентов 40 правшей, 20% левшей, а остальные являются «двурукими». У людей левшей всего лишь 15%, а двуруких практически нет.

Асимметрия рук достаточно жестко связана с асимметрией ног: подавляющее большинство праворуких людей имеют левую толчковую ногу (это необходимо для равновесия при выполнении движений). Шаг у людей в местности без ориентиров правой ногой длиннее, чем левой, лестницы в домах закручены против часовой стрелки. По виражам стадионов спортсмены бегут против часовой стрелки (шаг правой длиннее на микроскопическую величину, однако, даже представить, что нужно бежать по часовой стрелке, трудно, значит, все не только в ногах, но и в голове).

Однако, несколько сотен лет назад левшей могло быть намного меньше, чем сейчас (кстати, на всю Библию лишь один левша, и о нем говорится, как об уникальном явлении). Лестницы в старинных башнях закручены по часовой стрелке. Сделано это для того, чтобы нападающим снизу было неудобно работать мечом правой рукой. Но, если бы левшей, как сейчас, было бы 15%, то в каждой сотне воинов нашлось бы 15 левшей, которые, меняясь через несколько ступенек (на узкой лестнице впереди может быть только один человек), атаковали бы защищающихся. То есть, строить лестницы, неудобные для каждодневного подъема, было бы бессмысленно.

Вернемся к обезьянам. При высовывании головы из травы, асимметрия не должна бы возникнуть, зато она может возникнуть, если каждый раз спускаться с горы одним боком вперед. Но почему обезьяны не могли

спускаться разными боками вперед? Животные весьма ревниво относятся к своей безопасности: они постоянно настороже, использую при этом зрение, слух и обоняние. Как лучше всего распорядиться этими системами защиты?

Зрение защищает спереди, но из-за его неширокой диаграммы направленности приходится либо поворачивать голову, либо все туловище, что крайне неудобно на крутом спуске. А вот слух и обоняние лучше всего работают, когда источник расположен с наветренной строны. Тогда оптимальное расположение тела будет следующим: глаза смотрят в ту же сторону, куда дует ветер, а все, что сзади, контролируется слухом и обонянием.

Если же теперь преимущественное направление ветра вдоль склона заставляет спускаться правым боком вперед (вполне допустимое предположение), то так обезьяна и будет делать всегда. Для закрепления навыка, причем не только в голове, но и в генах (разные руки и ноги работают по-разному) нужно всего несколько поколений. Это доказывается успехами дрессировки и искусственного отбора.

Скажем же спасибо тем диким зверям, которые загнали наших предков на крутые склоны гор.

Серия: **ОБЪЯВЛЕНИЯ**

Гершман Я.Х.

Новая технология производства инкубационных цыплят

Наша компания разработала и испытала новый промышленный инкубатор птицы с автоматической системой фотобиостимуляции, который может увеличить выход куриных цыплят класса "А" на 2-5%. Объем камеры- без ограничений.

EYA – high tech agricultural systems Ltd., Israel
eya_israel@hotmail.com
Dr. Yakov Gershman

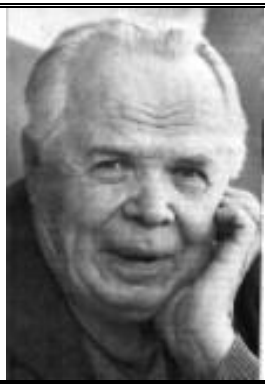
Авторы

Гершман Яков Хаимович; *Израиль.*
eya_israel@hotmail.com
К.т.н.
Директор компании " EYA –high tech agricultural systems Ltd", Израиль.
Работы в области прикладной агрофизики

Голубенко Наталья Борисовна, *Россия.*
natalia.gnb@mail.ru
Высшее библиотечное образование, работает библиотекарем в Кузбасском государственном техническом университете с 2004 года.

Иванов Георгий Петрович, *Литва.*
nara@tts.lt
Сайт http://tts.lt/~nara
1943 г.р. Закончил московский инженерно-физический институт (МИФИ). С 1969 по 1984 г.г. работал научным сотрудником в научно-исследовательском физико-химическом институте (НИФХИ) им. Л. Я. Карпова (г. Обнинск), с 1984 по 1999 работал на Игналинской атомной электростанции (Висагинас, Литва).

Кайнов Анатолий Борисович
ankajnov@yandex.ru
Кандидат технических наук с 1986 года, специализировался в области динамики и прочности, преподавал физику в высшем учебном заведении.



Каравдин Павел Александрович
pkaravdin@yandex.ru
1930 г.р. инженер-механик, любитель (дилетант) науки. Имеет много статей на научные темы в разных газетах и Интернете.

Миркин Владислав Иосифович, *США*
mirkinvlad@mail.ru
Мне 63 года, проживаю в Америке под Чикаго. Физик, кандидат технических наук.

Мотков Олег Иванович
oleg1748@mail.ru
61 год. Левша. Окончил в 1971 году факультет психологии МГУ им. М.В. Ломоносова. Женат, 4 детей. Работаю преподавателем психологии в Институте психологии им. Л.С. Выготского РГГУ (Российского государственного гуманитарного университета). Доцент кафедры психологии личности. Опубликовано 2 моих монографии "Психология самопознания личности" и "Природа личности". Самиздатом выпустил на ризографе сборник стихотворений "Жизнь – это поэзия". Интересы: психология гармоничной личности, устройство психики, горные путешествия, пейзажная фотография, искусство, поэзия и литература, музыка. Более 30 лет хожу по горам Кавказа и Средней Азии.

Недосекин Юрий Андреевич, *Россия.*
meson@inetcomm.ru
Окончил в 1969 году физфак Томского государственного университета по специальности “Теоретическая физика”.

Петров Валерий Владимирович, *Украина.*
vvpetrov@mksat.net
Родился 14.12.1940, г. Николаев. Окончил Николаевский кораблестроительный институт (сейчас - университет) в 1969 г. Специальность - технология машиностроительного производства.

Хмельник Соломон Ицкович, *Израиль.*
solik@netvision.net.il

К. т. н., научные интересы – электротехника, электроэнергетика, вычислительная техника, математика. Имеет около 200 изобретений СССР, патентов, статей, книг. Среди них – работы по теории и моделированию математических процессоров для операций с различными математическими объектами; работы по новым методам расчета электромеханических и электродинамических систем; работы по управлению в энергетике.