ISSN 2222-8772

Математические Структуры и Моделирование

№ 4(56)
2020

МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМ. Ф.М. ДОСТОЕВСКОГО»

МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ И МОДЕЛИРОВАНИЕ

№ 4(56)

Омск
2020

Математические структуры и моделирование. — Омск : Омский государственный университет, 2020. — № 4(56). – 164 с.
ISSN 2222-8772 (print) ISSN 2222-8799 (online)

Редакционная коллегия

А. К. Гуц	главный редактор, председатель редакционной коллегии, доктор физ.-мат. наук, профессор, зав. кафедрой кибернетики, Омский государственный университет им. Ф. М. Достоевского.
Д. Н. Лавров	зам. глав. редактора, канд. техн. наук, доцент, проректор по информационным технологиям, зав. каф. компьютерных технологий и сетей, Омский государственный университет им. Ф. М. Достоевского.
Н. Ф. Богаченко	технический редактор, зам. глав. редактора, канд. физ.-мат. наук, доцент, Омский государственный университет им. Ф. М. Достоевского.
В. П. Голубятников	доктор физ.-мат. наук, профессор Новосибирского государственного университета, главный научный сотрудник Института математики СО РАН, г. Новосибирск.
С. И. Горлов	доктор физ.-мат. наук, профессор, ректор Нижневартовского государственного университета.
А. Г. Гринь	доктор физ.-мат. наук, профессор, кафедра кибернетики, Омский государственный университет им. Ф. М. Достоевского.
В. А. Еровенко	доктор физ.-мат. наук, профессор, кафедра общей математики и информатики, Белорусский государственный университет, г. Минск, Республика Беларусь.
B. Zilber	Dr.Sc. (Phys.-Math.), Professor of Mathematical Logic, Mathematical Institute, University of Oxford, UK.
А. Н. Кабанов	канд. физ.-мат. наук, кафедра кибернетики, Омский государственный университет им. Ф. М. Достоевского.
А. В. Копыльцов	доктор техн. наук, профессор, кафедра информационных систем, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина).
А. Г. Коробейников	доктор техн. наук, профессор, зам. директора по науке Санкт--Петербургского филиала Института земного магнетизма, ионосферы и распространения радиоволн им. Н.В. Пушкова РАН.
П. А. Корчагин	доктор техн. наук, профессор, проректор по научной работе, Сибирская государственная автомобильно-дорожная академия (СибАДИ), г. Омск.
V. Kreinovich	Ph.D. (Phys.-Math.), Professor, Computer Science Department, University of Texas at El Paso, Texas, USA.
В. А. Плетюхов	доктор физ.-мат. наук, профессор кафедры общей и теоретической физики Брестского государственного университета им. А.С. Пушкина, г. Брест, Республика Беларусь.
Л. Б. Соколинский	доктор физ.-мат. наук, профессор, проректор по информатизации, зав. кафедрой системного программирования, Южно-Уральский государственный университет (национальный исследовательский университет), г. Челябинск.
A. A. Fedorenko	Ph.D. (Phys.-Math.), Researcher (CR1) at the French National Centre of Scientific Research (CNRS) Laboratoire de Physique de l'ENS-Lyon, France.
А. Н. Фирсов	доктор техн. наук, профессор, Высшая школа киберфизических систем и управления, Санкт-Петербургский политехнический университет Петра Великого.
A. Jadczyk	Ph.D., Professor, Researcher, Laboratoire de Physique, Universite de Toulouse III et CNRS, France.

Учредитель

Федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф. М. Достоевского».
Свидетельство о регистрации средства массовой информации ПИ № ФС77-72200 от 15 января 2018 г. выдано Роскомнадзором.

Адрес редакции, издателя и типографии

644077, Омская обл., г. Омск, пр-т Мира, д. 55а.

Дата выхода в свет: 18.12.2020.

Тираж 60 экз.

Свободная цена.

МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ и МОДЕЛИРОВАНИЕ

Журнал основан в 1998 году. В журнале публикуются статьи, в которых излагаются результаты исследований по фундаментальной и прикладной математике, теоретической физике, компьютерным наукам, философии и истории математики и информатики, а также размышления, касающиеся окружающей нас природы и общества. Объекты исследования должны быть представлены в форме некоторых математических структур и моделей.

Все статьи журнала проходят обязательное рецензирование. Рефераты статей журнала опубликованы в «Реферативном журнале» и «Mathematical Reviews» (США). Журнал индексируется в РИНЦ (elibrary.ru) и «Zentralblat für Mathematik» (Германия). Журнал входит в Перечень рецензируемых научных изданий ВАК РФ, в которых должны быть опубликованы основные результаты диссертаций на соискание учёных степеней (Приказ Минобрнауки России от 25 июля 2014 г. № 793).

Все статьи в журнале публикуются под лицензией Attribution 4.0 International (CC-BY).

Электронная версия журнала представлена в сети:

http://msm.univer.omsk.su
http://msm.omsu.ru

Подписной индекс по каталогу «Пресса России»: 94082

Электронная почта главного редактора:

guts@omsu.ru

Электронная почта выпускающего редактора:

lavrov@omsu.ru

СОДЕРЖАНИЕ

Фундаментальная математика и физика

А.Г. Гринь. *О строгом притяжении функций от зависимых величин к нормальному закону* . . . 5

А.К. Гуц. *Распад пространства-времени на «вечные» параллельные исторические эпохи, временная сцепленность и машина времени* . . . 20

А.В. Левичев, А.Ю. Пальянов. *О цветах и электрических зарядах кварков: моделирование в терминах групп U(n) и SU(n,n)* . . . 31

Прикладная математика и моделирование

Н.Ф. Богаченко, Д.Н. Лавров. *Об особенностях реализации интервального метода анализа иерархий в задаче оценки эффективности работы службы занятости* . . . 41

Л.А. Володченкова, А.К. Гуц. *Математическое моделирование мозаичности лесных экосистем* . . . 49

Компьютерные науки

Н.Ф. Богаченко, И.О. Горохов. *Построение генератора псевдослучайных последовательностей на основе клеточного автомата* . . . 64

Д.Э. Вильховский. *Обзор методов стеганографического анализа изображений в работах зарубежных авторов* . . . 75

А.К. Гуц, Д.Э. Вильховский. *Стегоанализ цветных изображений с низким заполнением стегоконтейнера с использованием программного комплекса* . . . 103

А.А. Магазев, А.С. Мельникова, В.Ф. Цырульник. *Оценка среднего времени до отказа безопасности на основе марковских цепей с непрерывным временем* . . . 112

С.В. Усов. *О представлении некоторых ролевых моделей разграничения доступа объектно-ориентированной моделью HRU: наследование таксономическим листовым методом* . . . 126

Продолжение на следующей странице

Наши публикации

О.А. Бондаренко, Е.А. Костюшина, Т.В. Олейникова, Д.Н. Лавров. *Проектирование модуля уведомлений о событиях в информационной системе управления учебным процессом ОмГУ* 136

Н.В. Коляда, Е.А. Костюшина, Д.Н. Лавров. *Аудиальное сопровождение сайта «Электронные сервисы ОмГУ»* 148

Математические структуры и моделирование
2020. № 4(56). С. 5–19

УДК 519.214
DOI 10.24147/2222-8772.2020.4.5-19

О СТРОГОМ ПРИТЯЖЕНИИ ФУНКЦИЙ ОТ ЗАВИСИМЫХ ВЕЛИЧИН К НОРМАЛЬНОМУ ЗАКОНУ

А.Г. Гринь
профессор, д.ф.-м.н., e-mail: griniran@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Для симметрических функций от случайных величин из стационарных последовательностей, удовлетворяющих условию равномерно сильного перемешивания, получены общие условия притяжения к нормальному закону в терминах распределений отдельных слагаемых. Основной результат работы обобщает все известные к настоящему времени результаты такого типа.

Ключевые слова: Симметрические функции, равномерно сильное перемешивание, строгое притяжение к нормальному закону, гипотеза Ибрагимова–Иосифеску.

Будем писать $\xi \stackrel{d}{=} \eta$ и $\xi_n \stackrel{d}{\to} \eta$ в случаях, когда, соответственно, распределения ξ и η совпадают и $\{\xi_n\}$ сходятся к η по распределению.

Пусть при каждом $n \in \mathbb{N}$ определена симметрическая вещественнозначная функция f, то есть $f(x_1, x_2, ..., x_n) = f(x_{i_1}, ..., x_{i_n})$, для любых $x_1, ..., x_n \in \mathbb{R}$ для любой перестановки $\{i_1, ..., i_n\}$ множества $\{1, ..., n\}$ (на самом деле определена последовательность функций, но чтобы не загромождать рассуждений, мы не будем подчёркивать зависимость f от n какими-либо индексами и называть f последовательностью).

Будем обозначать $\{\xi_n\} = \{\xi_n,\ n \in \mathbb{Z}\}$ стационарную в узком смысле последовательность, $X_n = f(\xi_1, ..., \xi_n)$, а $\mathcal{N}(0,1)$ — случайную величину, имеющую нормальное распределение с параметрами 0 и 1.

Если при некотором выборе нормирующих констант A_n и B_n

$$B_n^{-1}(X_n - A_n) \stackrel{d}{\to} \mathcal{N}(0,1), \quad n \to \infty,$$

то будем говорить, что последовательность $\{X_n\}$ притягивается к нормальному закону. Если $\mathbb{E}X_n^2 < \infty,\ n = 1, 2, ...,$ и

$$(\mathbb{D}X_n)^{-1/2}(X_n - \mathbb{E}X_n) \stackrel{d}{\to} \mathcal{N}(0,1),$$

то говорят, что к последовательности $\{X_n\}$ применима центральная предельная теорема.

В настоящей работе рассматриваются стационарные последовательности, удовлетворяющие условию равномерно сильного перемешивания (φ–перемешивания).

Пусть $\{\xi_n\} = \{\xi_n,\ n = 1, 2, ...\}$ — стационарная в узком смысле последовательность и пусть $\mathcal{F}_{\leqslant n}$ и $\mathcal{F}_{\geqslant n}$–$\sigma$-алгебры, порождённые семействами $\{\xi_i : i \leqslant n\}$ и $\{\xi_i : i \geqslant n\}$. Говорят, что последовательность $\{\xi_n\}$ удовлетворяет *условию равномерно сильного перемешивания (φ-перемешивания)* с коэффициентом перемешивания $\varphi(n)$, если

$$\varphi(n) = \sup\left\{\frac{|\mathbb{P}(AB) - \mathbb{P}(A)\mathbb{P}(B)|}{\mathbb{P}(A)} :\ A \in \mathcal{F}_{\leqslant 0},\ B \in \mathcal{F}_{\geqslant n}\right\} \to 0, \quad n \to \infty.$$

Если к тому же $\varphi(1) < 1$, то такое условие будем называть условием *φ_1-перемешивания*.

Если $\{\xi_n\} = \{\xi_n,\ n = 1, 2, ...\}$ — стационарная последовательность, удовлетворяющая условию φ-перемешивания, ξ измерима относительно $\mathcal{F}_{\leqslant 0}$, η — относительно $\mathcal{F}_{\geqslant n}$, $\|\xi\|_s = (\mathbb{E}|\xi|^s)^{1/s} < \infty$, $\|\eta\|_t < \infty$, $s, t \geqslant 1$, $1/s + 1/t = 1$, то

$$|\mathbb{E}\xi\eta - \mathbb{E}\xi\mathbb{E}\eta| \leqslant 2\varphi^{\frac{1}{s}}(n)\|\xi\|_s\|\eta\|_t \tag{1}$$

[1, с. 392].

В случае, когда $X_n = S_n = \sum\limits_{k=1}^{n} \xi_k$ притяжение (или нет) последовательностей $\{S_n\}$ к нормальному закону во многом обусловлено поведением дисперсий сумм S_n или дисперсий сумм «срезок» величин ξ_n (см., например [2]). Вместе с тем, существуют условия на распределение ξ_1, обеспечивающие притяжение к нормальному закону любой последовательности $\{S_n\}$, если только $\{\xi_n\}$ удовлетворяет условию φ_1-перемешивания (и, следовательно, при любом возможном поведении дисперсий сумм).

Пусть $\mathbb{E}\{\xi, A\} = \int\limits_A \xi\, \mathbb{P}(d\omega)$, а $L(\xi)$ обозначает распределение случайной величины ξ.

Обозначим через $\mathcal{N}$ классическую *область притяжения нормального закона*: $\mathcal{N} = \{L(\xi) : \mathbb{E}\{\xi^2, |\xi| \leqslant x\}$ – медленно меняющаяся функция$\}$, через $\mathcal{N}_0$ множество всех распределений таких, что если $\{\xi_n\}$ удовлетворяет условию φ_1-перемешивания и $L(\xi_1) \in \mathcal{N}_0$, то к $\{S_n\}$ применима центральная предельная теорема, а через *$\mathcal{N}_1$–область строгого притяжения нормального закона*, то есть если $\{\xi_n\}$ удовлетворяет условию φ_1-перемешивания и $L(\xi_1) \in \mathcal{N}_1$, то $\{S_n\}$ притягивается к нормальному закону.

Ясно, что $\mathcal{N}_0 \subseteq \mathcal{N}_1 \subseteq \mathcal{N}$.

Известны следующие результаты, касающиеся строгого притяжения стационарных последовательностей с φ_1-перемешиванием к нормальному закону.

1. Если $\mathbb{E}|\xi|^p < \infty$, $p > 2$, то $L(\xi) \in \mathcal{N}_0$ (И.А. Ибрагимов [1, Теорема 18.5.1]).

2. Если $\mathbb{P}\{|\xi| \geqslant x\}$ — правильно меняющаяся функция порядка -2, то $L(\xi) \in \mathcal{N}_1$ (М. Пелиград, [3]).

3. Если $\mathbb{P}\{|\xi| \geqslant x\} = x^{-2}h(x)$, где $h(x)$ такова, что при любом $\lambda \geqslant 1$

$$0 < C_1 \leqslant \liminf_{x\to\infty} \frac{h(\lambda x)}{h(x)} \leqslant \limsup_{x\to\infty} \frac{h(\lambda x)}{h(x)} \leqslant C_2 < \infty,$$

то $L(\xi) \in \mathcal{N}_1$ (С.А. Клоков, [4]).

Описанные выше функции $h(x)$ названы в [5] SO-меняющимися; класс SO-меняющихся функций существенно шире класса медленно меняющихся функций: в него входят, например, все функции, отделённые от нуля и бесконечности.

Здесь же следует упомянуть не доказанную и не опровергнутую до настоящего времени *гипотезу Ибрагимова–Иосифеску*, которая утверждает, что $\mathcal{N}_1 = \mathcal{N}$ (см. [1], [3]).

Обозначим

$$b_n(p) = \| \max(\xi_1', .., \xi_n')\|_p = \{\mathbb{E}| \max(\xi_1', .., \xi_n')|^p\}^{\frac{1}{p}}, \ p > 0,$$

где через $\xi_1', .., \xi_n'$ обозначены *независимые* случайные величины такие, что $\xi_k' \stackrel{d}{=} \xi_k, \ k = 1, 2, ..., n$. Так как $\xi_1, ..., \xi_n$ одинаково распределены, то $b_n(p)$ при каждых $p > 0$ и $n \in \mathbb{N}$ определяется только распределением ξ_1.

В [6] получено следующее обобщение приведённых выше результатов.

Теорема 1. *1. Если при некотором* $p > 0$

$$\lim_{N\to\infty} \limsup_{n\to\infty} n \int\limits_N^\infty \mathbb{P}\{\xi_1^2 \geqslant x b_n^2(p)\}\, dx = 0, \tag{2}$$

то $L(\xi_1) \in \mathcal{N}_0$.

2. Если при некотором $p > 0$

$$\lim_{\varepsilon\to 0} \liminf_{n\to\infty} n \int\limits_\varepsilon^1 \mathbb{P}\{\xi_1^2 \geqslant x b_n^2(p)\}\, dx = \infty, \tag{3}$$

то $L(\xi_1) \in \mathcal{N}_1$.

Если $\mathbb{E}|\xi_1|^p < \infty$, $p > 2$, то выполняется (2), и мы получаем результат И.А. Ибрагимова, а если $\mathbb{P}\{|\xi_1| \geqslant x\} = x^{-2}h(x)$, где $h(x)$ SO-меняющаяся функция (в частности, если $\mathbb{P}\{|\xi_1| \geqslant x\}$ — правильно меняющаяся функция порядка -2), то выполняется (3), откуда следуют результаты М. Пелиград и С.А. Клокова. В случае, когда $\mathbb{P}\{|\xi_1| \geqslant x\} = x^{-\rho}h(x)$, $\rho > 0$, где $h(x)$ — SO-меняющаяся функция, условия (1) и (2) являются необходимыми и достаточными для того, чтобы $L(\xi_1) \in \mathcal{N}_0$ и $L(\xi_1) \in \mathcal{N}_1$ соответственно, и сказанное можно сформулировать так: гипотеза Ибрагимова–Иосифеску выполняется в указанном классе распределений [6].

Пусть при каждом $n \in \mathbb{N}$ определена функция $f(\mathbf{x}) = f(x_1, x_2, ..., x_n)$, удовлетворяющая следующим условиям:

f1. $f(x_1, x_2, ..., x_n) = f(x_{i_1}, ..., x_{i_n})$, для любых $x_1, ..., x_n \in \mathbb{R}$ для любой перестановки $\{i_1, ..., i_n\}$ множества $\{1, ..., n\}$;

f2. $f(x_1, x_2, ..., x_{n-1}, 0) = f(x_1, x_2, ..., x_{n-1})$;

f3. $f(-\mathbf{x}) = -f(\mathbf{x})$;

f4. $f(\mathbf{x}+\mathbf{y}) \sim f(\mathbf{x}) + f(\mathbf{y})$, если $\tau(\mathbf{x},\mathbf{y}) = |f(\mathbf{x}+\mathbf{y})| + |f(\mathbf{x})| + |f(\mathbf{y})| \to \infty$, (то есть хотя бы одно из слагаемых в $\tau(\mathbf{x},\mathbf{y})$ стремится к бесконечности). Эквивалентность в f_3 понимается следующим образом: для любого $\varepsilon > 0$ найдётся $N = N(\varepsilon) > 0$ такое, что если $\tau(\mathbf{x},\mathbf{y}) > N$, то

$$|f(\mathbf{x}+\mathbf{y}) - f(\mathbf{x}) - f(\mathbf{y})| \leqslant \varepsilon |f(\mathbf{x}+\mathbf{y})|.$$

Отсюда нетрудно вывести (см. [7])

$$|f(\mathbf{x_1}+...+\mathbf{x_k}) - f(\mathbf{x_1}) - ... - f(\mathbf{x_k})| \leqslant \varepsilon(|f(\mathbf{x_1})| + ... + |f(\mathbf{x_{k-1}})| + (k-1)N. \quad (4)$$

Пусть, как и выше, $X_n = f(\xi_1, ..., \xi_n)$, $n = 1, 2, ...$, но функция f удовлетворяет условиям $f_1 - f_4$, $Y_n = f(\xi_n)$,

$$Z_n = \max(Y_1, ..., Y_n),\ Z'_n = \max(Y'_1, ..., Y'_n),\ c_n(p) = \|Z'_n\|_p.$$

При каждых $p > 0$ и $n \in \mathbb{N}$ $c_n(p)$ зависит только от распределения $Y_1 \stackrel{d}{=} X_1$, то есть от распределения ξ_1 и функции f, $\{c_n(p)\}$ не убывает по n.

Через $\mathcal{N}_0(f)$ будем обозначать множество всех распределений таких, что если $\{\xi_n\}$ удовлетворяет условию φ_1-перемешивания и $L(X_1) \in \mathcal{N}_0(f)$, то к $\{X_n\}$ применима центральная предельная теорема, а через $\mathcal{N}_1(f)$ — *область строгого притяжения к нормальному закону*, то есть если $\{\xi_n\}$ удовлетворяет условию φ_1-перемешивания и $L(X_1) \in \mathcal{N}_1(f)$, то $\{X_n\}$ притягивается к нормальному закону.

В настоящей работе выводится следующее обобщение теоремы 1.

Теорема 2. *1. Если при некотором* $p \geqslant 1$

$$\lim_{N\to\infty} \limsup_{n\to\infty} n \int_N^\infty \mathbb{P}\{X_1^2 \geqslant x c_n^2(p)\}\, dx = 0, \quad (5)$$

то $L(X_1) \in \mathcal{N}_0(f)$.

2. Если при некотором $p \geqslant 1$

$$\lim_{\varepsilon\to 0} \liminf_{n\to\infty} n \int_\varepsilon^1 \mathbb{P}\{X_1^2 \geqslant x c_n^2(p)\}\, dx = \infty, \quad (6)$$

то $L(X_1) \in \mathcal{N}_1(f)$.

Замечание 1. Теорема 2 справедлива и при $0 < p < 1$, но в этом случае не предполагается существование $\mathbb{E}|X_n|^p$, $p \geqslant 1$, и в доказательстве потребуются соответствующие корректировки (понадобится введение других центрирующих констант вместо $\mathbb{E}X_n$, $\|\xi\|_p$ не будет являться нормой и т. п.). Чтобы не приводить двух параллельных доказательств, мы ограничимся случаем $p \geqslant 1$.

Лемма 1. [3] *Для любых x и $n \geqslant 1$*

$$(1-\varphi(1))\mathbf{P}\{Z'_n \geqslant x\} \leqslant \mathbf{P}\{Z_n \geqslant x\} \leqslant (1+\varphi(1))\mathbf{P}\{Z'_n \geqslant x\}. \tag{7}$$

При любом $p > 0$

$$(1-\varphi(1))c_n^p(p) \leqslant \mathbf{E}|Z_n|^p \leqslant (1+\varphi(1))c_n^p(p). \tag{8}$$

Пусть $X_{k,n} = f(\Xi_{k,n}) = f(\xi_k, ..., \xi_n)$, $k \leqslant n$. Введём *симметризованные* величины $\widetilde{X}_{k,n} = f(\Xi_{k,n}) - f(\Xi'_{k,n})$, где векторы $\Xi_{k,n}$ и $\Xi'_{k,n}$ независимы и одинаково распределены, и пусть $\widetilde{Z}'_n = \max\limits_{1\leqslant k\leqslant n} \widetilde{Y}'_k$. Легко видеть, что для последовательности $\{\widetilde{X}_n\}$ выполняется соотношение (3), а последовательность $\{\widetilde{Y}_n\}$, $\widetilde{Y}_n = f(\xi_n) - f(\xi'_n)$ удовлетворяет условию φ-перемешивания с коэффициентом перемешивания $\widetilde{\varphi}(n) \leqslant 1-(1-\varphi(n))^2$ [8, Lemma 2.3].

Имеют место неравенства симметризации [9, с. 261]

$$\mathbb{P}\left\{\max_{1\leqslant k\leqslant n}(Y'_k - \mu) \geqslant x\right\} \leqslant 2\mathbb{P}\left\{\widetilde{Z}'_n \geqslant x\right\} \leqslant 4\mathbb{P}\left\{\max_{1\leqslant k\leqslant n}(Y'_k - a) \geqslant x/2\right\} \tag{9}$$

и слабые неравенства симметризации [9, с. 259]

$$\mathbb{P}\{|X_n - \mu_n| \geqslant x\} \leqslant 2\mathbb{P}\{|\widetilde{X}_n| \geqslant x\} \leqslant 4\mathbb{P}\{|X_n - a| \geqslant x/2\},\ x \geqslant 0. \tag{10}$$

Здесь μ — медиана Y_1, μ_n — медиана X_n, $a \in \mathbb{R}$. Из (10) и (9) соответственно при $p > 0$ следуют соотношения

$$\mathbb{E}\left|\max_{1\leqslant k\leqslant n}(Y'_k - \mu)\right|^p \leqslant 2\mathbb{E}\left|\widetilde{Z}'_n\right|^p \leqslant 2^{p+2}\mathbb{E}\left|\max_{1\leqslant k\leqslant n}(Y'_k - a)\right|^p, \tag{11}$$

$$\mathbb{E}\left\{|X_n - \mu_n|^p,\ |X_n - \mu_n| \geqslant x\right\} \leqslant$$
$$\leqslant 2\mathbb{E}\{|\widetilde{X}_n|^p,\ |\widetilde{X}_n| \geqslant x\} \leqslant 2^{p+2}\mathbb{E}\left\{|X_n - a|^p,\ |X_n - A_n| \geqslant x/2\right\}. \tag{12}$$

Обозначим

$$\overline{X}_n = \max_{1\leqslant k\leqslant n}|\widetilde{X}_k|,\ k, n \in \mathbb{N}.$$

Из (4) следует, что для любого $\varepsilon > 0$ найдётся $N = N(\varepsilon) > 0$ такое, что при $i + m \leqslant k$

$$|\widetilde{X}_n| \geqslant |\widetilde{X}_i| - (1+\varepsilon)|\widetilde{X}_{i+1,n}| - N. \tag{13}$$

Введём ещё некоторые обозначения. Будем писать $\alpha(n) \ll \beta(n)$ в случае, когда $\alpha(n) = O(\beta(n))$, $n \to \infty$, и $\alpha(n) \asymp \beta(n))$, если $\alpha(n) \ll \beta(n)$ и $\beta(n) \ll \alpha(n)$.

Лемма 2. *Пусть $\varepsilon > 0$, функция f удовлетворяет условиям $f_1 - f_4$, $\varphi(1) < 1$, а $c_n \to \infty$. Если n таково, что $N < c_n$, где N — константа из* (13) *и*

$$\gamma = \max_{1\leqslant k\leqslant n}\mathbb{P}\left\{|\widetilde{X}_k| \geqslant \frac{c_n}{1+\varepsilon}\right\} + \widetilde{\varphi}_1 < 1,\ \widetilde{\varphi}_1 = 1-(1-\varphi(1))^2,$$

то $\mathbb{E}\left(\overline{X}_n\right)^p \ll c_n^p + \mathbb{E}|\widetilde{X}_n|^p$.

Доказательство. Пусть $E_i = \{\overline{X}_{i-1} < (r+3)c_n \leqslant |\widetilde{X}_i|\}$, $i = 1, ..., n$. Тогда $E_iE_j = \varnothing$, $i \neq j$, $\bigcup\limits_{i=1}^{n} E_i = \{\overline{X}_n \geqslant (r+3)c_n\}$. В силу (13) при $i \leqslant n-1$

$$\left\{|\widetilde{X}_i| \geqslant (r+3)c_n,\ |\widetilde{X}_{i+1,n}| < \frac{2c_n}{1+\varepsilon}\right\} \subseteq \left\{|\widetilde{X}_n| \geqslant rc_n\right\},$$

то есть

$$\left\{|\widetilde{X}_n| < rc_n\right\} \subseteq \{|\widetilde{X}_i| < (r+3)c_n\} \cup \left\{|\widetilde{X}_{i+1,n}| \geqslant \frac{2c_n}{1+\varepsilon}\right\},$$

откуда

$$\left\{|\widetilde{X}_n| < rc_n, E_i\right\} \subseteq \left\{|\widetilde{X}_{i+1,n}| \geqslant \frac{2c_n}{1+\varepsilon}, E_i\right\}. \tag{14}$$

С помощью (14) и условия φ_1-перемешивания получаем

$$\mathbb{P}\{\overline{X}_n \geqslant (r+3)c_n\} \leqslant \mathbb{P}\left\{|\widetilde{X}_n| \geqslant rc_n\right\} + \sum_{i=1}^{n-1} \mathbb{P}\left\{|\widetilde{X}_n| < rc_n,\ E_i\right\} \leqslant$$

$$\leqslant \mathbb{P}\left\{|\widetilde{X}_n| \geqslant rc_n\right\} + \sum_{i=1}^{n-1} \mathbb{P}\left\{|\widetilde{X}_{i+1,k}| \geqslant \frac{c_n}{1+\varepsilon}, E_i\right\} \leqslant \mathbb{P}\left\{|\widetilde{X}_n| \geqslant rc_n\right\} +$$

$$+ \left(\max_{1\leqslant k\leqslant n} \mathbb{P}\left\{|\widetilde{X}_k| \geqslant \frac{c_n}{1+\varepsilon}\right\} + \widetilde{\varphi}_1\right) \sum_{i=1}^{n} \mathbb{P}\{E_i\} \leqslant \mathbb{P}\left\{|\widetilde{X}_n| \geqslant rc_n\right\} +$$

$+\gamma\mathbb{P}\{\overline{X}_n \geqslant (r+3)c_n\}$, откуда

$$\mathbb{P}\{\overline{X}_n \geqslant (r+3)c_n\} \leqslant \frac{1}{1-\gamma}\mathbb{P}\left\{|\widetilde{X}_n| \geqslant rc_n\right\}. \tag{15}$$

Далее

$$\mathbb{E}\{|\xi|^p, |\xi| \geqslant N\} = N^p\mathbb{P}\{|\xi| \geqslant N\} + p\int\limits_N^\infty x^{p-1}\mathbb{P}\{|\xi| \geqslant x\}\,dx.$$

Из (15) при $N \geqslant 1$ и достаточно больших n получаем

$$\mathbb{E}\overline{X}_n^p \leqslant (4Nc_n)^p + \mathbb{E}\left\{\overline{X}_n^p,\ |\overline{X}_n| \geqslant 4Nc_n\right\} \leqslant (4Nc_n)^p + (4Nc_n)^p\mathbb{P}\{\overline{X}_n \geqslant 4Nc_n\} +$$

$$+p(4c_n)^p \int\limits_N^\infty x^{p-1}\mathbb{P}\left\{\overline{X}_n \geqslant 4xc_n\right\}\,dx \leqslant (4Nc_n)^p + \frac{(4Nc_n)^p}{1-\gamma}\mathbb{P}\left\{|\widetilde{X}_n| \geqslant Nc_n\right\} +$$

$$+\frac{p(4c_n)^p}{1-\gamma}\int\limits_N^\infty x^{p-1}\mathbb{P}\{|\widetilde{X}_n| \geqslant xc_n\}\,dx \ll c_n^p + \mathbb{E}|\widetilde{X}_n|^p.$$

■

Будем обозначать

$$B_n(p) = \|\widetilde{X}_n\|_p,\ p \geqslant 1,\ \sigma_n = B_n(2),\ \widetilde{Z}_n = \max(\widetilde{Y}_1, ..., \widetilde{Y}_n),$$

$$\widetilde{Z}'_n = \max(\widetilde{Y}'_1, ..., \widetilde{Y}'_n),\ \widetilde{c}_n(p) = \|\widetilde{Z}'_n\|_p,\ a_n = \sup\left\{x : n\mathbb{P}\{|\widetilde{Y}_1| \geqslant x\} \geqslant 1\right\}.$$

Тогда

$$n\mathbb{P}\{|\widetilde{Y}_1| \geqslant a_n\} \geqslant 1,\ n\mathbb{P}\{|\widetilde{Y}_1| > a_n\} < 1,$$

$$\mathbb{P}\{|\widetilde{Y}_1| = a_n\} \leqslant \mathbb{P}\{|\widetilde{Y}_1| > a_{n-1}\} - \mathbb{P}\{|\widetilde{Y}_1| \geqslant a_{n+1}\} \leqslant \frac{1}{n-1} - \frac{1}{n+1} = \frac{2}{n^2-1} \quad (16)$$

$$\widetilde{c}^p_{n+m}(p) \leqslant \widetilde{c}^p_n(p) + \widetilde{c}^p_m(p). \quad (17)$$

Как и в [6], мы будем рассматривать последовательности $\{\xi_n\}$, у которых $\mathbb{P}\{|X_1| \geqslant x\} > 0$ при любом $x > 0$; в этом случае $a_n \to \infty$, $\widetilde{c}_n(p) \to \infty$ (см. лемму 3). В противном случае условие (4) выполняется очевидным образом, а вопрос о применимости центральной предельной теоремы к последовательности $\{X_n\}$ решается, например, в теореме 3 из [10].

Лемма 3. *Пусть $\{\xi_n\}$ — стационарная последовательность, удовлетворяющая условию φ_1-перемешивания, функция f удовлетворяет условиям $f_1 - f_4$, и пусть $\mathbf{E}|X_1|^p < \infty$, $p \geqslant 1$. Тогда*

a) $\|\overline{X}_n\|_p \ll B_n(p)$;

b) $a^p_n \leqslant 2\widetilde{c}^p_n(p)$, $a^p_n \leqslant n\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\}$;

c) $1/2 \leqslant \widetilde{c}_n^{-p}(p) n\mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_n\} \leqslant 4$, $n \geqslant 3$.;

d) $\widetilde{c}_n(p) \asymp c_n(p)$;

e) $B_n(p) \gg \widetilde{c}_n(p)$.

Д о к а з а т е л ь с т в о. a) Положим в лемме 1 $c_n = N \max\limits_{1\leqslant k\leqslant n} B_k(p)$. Тогда

$$\max_{1\leqslant k\leqslant n} \mathbb{P}\left\{|\widetilde{X}_k| \geqslant \frac{c_n}{1+\varepsilon}\right\} \leqslant \frac{(1+\varepsilon)^p}{N^p},$$

и, выбрав достаточно большое $N > 0$, мы обеспечим выполнение условий леммы 2, из которой следует $\|\overline{X}_n\|_p \ll \max\limits_{1\leqslant k\leqslant n} B_k(p)$. Далее $\max\limits_{1\leqslant k\leqslant n} B_k(p) \ll B_n(p)$ [7, лемма 1], и мы получаем утверждение a).

b) Нетрудно показать (см., например [3]), что

$$\frac{n\mathbb{P}\{|\widetilde{Y}_1| \geqslant x\}}{1 + n\mathbb{P}\{|\widetilde{Y}_1| \geqslant x\}} \leqslant \mathbb{P}\{|\widetilde{Z}'_n| \geqslant x\} \leqslant n\mathbb{P}\{|\widetilde{Y}_1| \geqslant x\},\ x > 0. \quad (18)$$

Отсюда

$$\widetilde{c}^p_n(p) = \int\limits_0^\infty \mathbb{P}\{|\widetilde{Z}'_n|^p \geqslant x\}\, dx \geqslant \int\limits_0^{a^p_n} \frac{n\mathbb{P}\{|\widetilde{Y}_1|^p \geqslant x\}}{1 + n\mathbb{P}\{|\widetilde{Y}_1|^p \geqslant x\}}\, dx \geqslant \frac{a^p_n}{2}.$$

Далее
$$1 \leqslant n\mathbb{P}\{|\widetilde{Y}_1| \geqslant a_n\} \leqslant na_n^{-p}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\},$$
то есть $a_n^p \leqslant n\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\}$.

c) Из (18) следует
$$\frac{n}{2}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| > a_n\} \leqslant \mathbb{E}\{|\widetilde{Z}_n'|^p, |\widetilde{Z}_n'| > a_n\} \leqslant n\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\}, \qquad (19)$$
откуда с помощью утверждения b) и (16) выводим
$$\widetilde{c}_n^p(p) \geqslant \frac{n}{2}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| > a_n\} = \frac{n}{2}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\} - \frac{n}{2}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| = a_n\} =$$
$$= \frac{n}{2}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\} - \frac{na_n^p}{2}\mathbb{P}\{|\widetilde{Y}_1| = a_n\} \geqslant \frac{n}{2}\mathbb{E}\{|\widetilde{Y}_1|^p, |\widetilde{Y}_1| \geqslant a_n\} - \frac{2n\widetilde{c}_n^p(p)}{n^2-1}.$$
Далее из (19) и утверждения b) получаем
$$\widetilde{c}_n^p(p) \leqslant a_n^p + \mathbb{E}\{|\widetilde{Z}_n'|^p, |\widetilde{Z}_n'| \geqslant a_n\} \leqslant 2n\mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_n\}.$$
Так как $2n(n^2-1)^{-1} \leqslant 3/4,\ n \geqslant 3$, то из двух последних соотношений следует утверждение c).

d) С помощью (11) получаем
$$c_n^p(p) = \mathbb{E}\max_{1\leqslant k\leqslant n}|Y_k'|^p \leqslant 2^{p-1}\mathbb{E}\left|\max_{1\leqslant k\leqslant n}(|Y_k'| - \nu)\right|^p + 2^{p-1}\nu^p \leqslant 2^p\mathbb{E}\left|\max_{1\leqslant k\leqslant n}(|Y_k'| - |Y_k''|)\right|^p +$$
$$+2^{p-1}\nu^p \leqslant 2^p\mathbb{E}\max_{1\leqslant k\leqslant n}|\widetilde{Y}_k'|^p + 2^p\mu^p = 2^p\widetilde{c}_n(p) + 2^{p-1}\nu^p.$$
Здесь $\nu > 0$ — медиана $|Y_1|$, а Y_k' и Y_k'' независимы и одинаково распределены. Поскольку в наших предположениях $c_n(p) \to \infty,\ n \to \infty$, то отсюда следует $\widetilde{c}_n(p) \gg c_n(p)$. С другой стороны, $\widetilde{c}_n(p) = \|\widetilde{Z}_n'\|_p \leqslant 2\|Z_n'\|_p = 2c_n(p)$. Утверждение d) доказано.

e) Воспользуемся (4): $|\widetilde{X}_k - \widetilde{X}_{k-1} - \widetilde{Y}_k| \leqslant \varepsilon|\widetilde{Y}_k| + N$, откуда
$$|\widetilde{Y}_k| \leqslant (1-\varepsilon)^{-1}(|\widetilde{X}_k| + |\widetilde{X}_{k-1}| + N), \text{ следовательно, } |\widetilde{Z}_n| \ll \overline{X}_n + N,$$
и, в силу леммы 1 и утверждения a),
$$\widetilde{c}_n(p) = \|\widetilde{Z}_n'\|_p \ll \|\widetilde{Z}_n\|_p \ll \|\overline{X}_n\|_p + N \ll B_n(p) + N.$$
Поскольку в наших предположениях $\widetilde{c}_n(p) \to \infty,\ n \to \infty$, то из последнего соотношения следует $\widetilde{c}_n(p) \ll B_n(p)$.

Лемма 4. [7] *Пусть $\varepsilon > 0$ и $r \geqslant 1$, функция f удовлетворяет условиям $f_1 - f_4$, а $c_n \to \infty$. Если n таково, что в* (3) $(m+1)N < c_n$ *и*
$$\max_{1\leqslant j\leqslant n}\mathbb{P}\left\{|X_j| \geqslant \frac{c_n}{1+\varepsilon}\right\} + \varphi(m) \leqslant \gamma < 1,$$
то
$$\mathbb{P}\{|X_n| \geqslant (r+6)c_n\} \leqslant \frac{\gamma}{1-\gamma}\mathbb{P}\{|X_n| \geqslant rc_n\} + \frac{1}{1-\gamma}\mathbb{P}\left\{\max_{1\leqslant j\leqslant n}|Y_j| \geqslant \frac{c_n}{m(1+\varepsilon)}\right\}.$$

Пусть $s \in \mathbb{N}$, $\mathbf{1}(A) = \begin{cases} 1, & \omega \in A \\ 0, & \omega \notin A \end{cases}$. Обозначим

$$\xi_j^{\triangledown}(s) = \xi_j \mathbf{1}(|f(\xi_j)| \leqslant 2\widetilde{c}_s(p)), \quad \xi_j^{\vartriangle}(s) = \xi_j \mathbf{1}(|f(\xi_j)| > 2\widetilde{c}_s(p)),$$

$$X_{j,n}^{\triangledown}(s) = f(\Xi_{j,n}^{\triangledown}) = f(\xi_j^{\triangledown}(s), ..., \xi_n^{\triangledown}(s)), \ X_{j,n}^{\vartriangle}(s) = f(\Xi_{j,n}^{\vartriangle}) = f(\xi_j^{\vartriangle}(s), ..., \xi_n^{\vartriangle}(s)),$$

$$X_{j,n}^{'\triangledown}(s) = f(\Xi_{j,n}^{'\triangledown}), \ X_{j,n}^{'\vartriangle}(s) = f(\Xi_{j,n}^{'\vartriangle}),$$

где векторы $(\Xi_{j,n}^{\triangledown})$ и $(\Xi_{j,n}^{'\triangledown})$ независимы и одинаково распределены, то же касается $(\Xi_{j,n}^{\vartriangle})$ и $(\Xi_{j,n}^{'\vartriangle})$. Далее, обозначим

$$X_{j,n}^{\blacktriangledown}(s) = X_{j,n}^{\triangledown}(s) - X_{j,n}^{'\triangledown}(s), \quad X_{j,n}^{\blacktriangle}(s) = X_{j,n}^{\vartriangle}(s) - X_{j,n}^{'\vartriangle}(s),$$

$$Y_j^{\triangledown}(s) = f(\xi_j^{\triangledown}(s)), \ Y_j^{\vartriangle}(s) = f(\xi_j^{\vartriangle}(s)), \ Y_j^{\blacktriangledown}(s) = Y_j^{\triangledown}(s) - Y_j^{'\triangledown}(s),$$

$$Y_j^{\blacktriangle}(s) = Y_j^{\vartriangle}(s) - Y_j^{'\vartriangle}(s), \ \sigma_n^{\blacktriangledown}(s) = \|X_n^{\blacktriangledown}(s)\|_2.$$

Нижний индекс n используется вместо $(1, n)$, например $X_n = X_{1,n}$.

Лемма 5. *В условиях леммы 3 Если $s \in \mathbb{N}$ достаточно велико, то*
a) $\max\limits_{1 \leqslant j \leqslant n} \|X_j^{\blacktriangle}(ns)\|_p \ll \widetilde{c}_n(p)$;
b) $B_{nk}(p) \gg \sqrt{k}\sigma_n^{\blacktriangledown}(nks)$, $B_m(p) \gg \sqrt{k}\sigma_n^{\blacktriangledown}(nks)$ *при* $nk \leqslant m \leqslant (k+1)n$.
c) Если $\mathbb{E}X_1^2 < \infty$, *то* $\sigma_{nk} \gg \sqrt{k}\sigma_n$ *и* $\sigma_m \asymp \sigma_{nk}$ *при* $nk \leqslant m \leqslant (k+1)n$.
d) Если $\mathbb{E}X_1^2 < \infty$, *то* $\sigma_n \gg \widetilde{c}_n(p)$.

Доказательство. a) В силу леммы 3b)

$$\max_{1 \leqslant i \leqslant j} \mathbb{P}\{|X_i^{\blacktriangle}(ns)| \geqslant x\} \leqslant n\mathbb{P}\{|\widetilde{X}_1| > 2\widetilde{c}_{ns}(p)\} \leqslant n\mathbb{P}\{|\widetilde{X}_1| > a_{ns}\} \leqslant \frac{1}{s}, \ x > 0,$$

так что s и m можно выбрать такими, чтобы

$$\max_{1 \leqslant i \leqslant j} \mathbb{P}\{|X_i^{\blacktriangle}(ns)| \geqslant x\} + \varphi(m) \leqslant \gamma, \quad \frac{7^p\gamma}{1-\gamma} < 1$$

и из леммы 4 получаем при $x > 0$

$$\mathbb{P}\{|X_j^{\blacktriangle}(ns)| \geqslant 7x\} \leqslant \frac{\gamma}{1-\gamma}\mathbb{P}\{|X_j^{\blacktriangle}(ns)| \geqslant x\} + \frac{1}{1-\gamma}\mathbb{P}\left\{\max_{1 \leqslant i \leqslant j} |Y_i^{\blacktriangle}(ns)| \geqslant \frac{x}{m(1+\varepsilon)}\right\}.$$

Откуда

$$\mathbb{E}|X_j^{\blacktriangle}(ns)|^p \leqslant \frac{7^p\gamma}{1-\gamma}\mathbb{E}|X_j^{\blacktriangle}(ns)|^p + \frac{(7m(1+\varepsilon))^p}{1-\gamma}\mathbb{E}\left\{\max_{1 \leqslant i \leqslant j} |Y_i^{\blacktriangle}(ns)|^p\right\}.$$

Отсюда с помощью (8) выводим

$$\max_{1 \leqslant j \leqslant n} \mathbb{E}|X_j^{\blacktriangle}(ns)|^p \ll \mathbb{E}\left\{\max_{1 \leqslant j \leqslant n} |Y_j^{\blacktriangle}(ns)|^p\right\} \leqslant \mathbb{E}\left\{\max_{1 \leqslant j \leqslant n} |\widetilde{Y}_j|^p\right\} \ll \widetilde{c}_n^p(p). \tag{20}$$

b) Положим в лемме 4 $c_n = MB_n(p)$. Из (4) следует $|X_j^{\blacktriangledown}(ns)| \leqslant |\widetilde{X}_j| + (1+\varepsilon)|X_j^{\blacktriangle}(ns)| + N$ откуда с помощью (20) и леммы 3a) и e) получаем

$$\max_{1\leqslant j\leqslant n} \mathbb{P}\left\{|X_j^{\blacktriangledown}(ns)| \geqslant \frac{MB_n(p)}{1+\varepsilon}\right\} \ll \max_{1\leqslant j\leqslant n} \frac{\mathbb{E}|\widetilde{X}_j|^p + \mathbb{E}|X_j^{\blacktriangle}(ns)|^p + N^p}{(MB_n(p))^p} \ll \frac{1}{M^p},$$

так что, выбрав M и m достаточно большими, мы обеспечим выполнение условий леммы 4. Далее, из леммы 3 e) и (17) следует, что $MB_n(p) \gg M\widetilde{c}_n(p) \geqslant \sqrt{M}\widetilde{c}_{nr}(p)$, где $r = \left[M^{p/2}\right]$, а $[x]$ — целая часть x, так что при достаточно больших $M > 0$ $MB_n(p) > 2m(1+\varepsilon)\widetilde{c}_{ns}(p)$, и

$$\mathbb{P}\left\{\max_{1\leqslant j\leqslant n} |Y_j^{\blacktriangledown}(ns)| \geqslant \frac{MB_n(p)}{m(1+\varepsilon)}\right\} = 0.$$

Из леммы 3 получаем

$$\mathbb{P}\{|X_n^{\blacktriangledown}(ns)| \geqslant 7x\} \leqslant \frac{\gamma}{1-\gamma}\mathbb{P}\{|X_n^{\blacktriangledown}(ns)| \geqslant x\},\ x \geqslant MB_n(p). \tag{21}$$

Если $M > 0$ и m таковы, что

$$\max_{1\leqslant j\leqslant n} \mathbb{P}\left\{|X_j^{\blacktriangledown}(ns)| \geqslant \frac{MB_n(p)}{1+\varepsilon}\right\} + \varphi(m) \leqslant \gamma, \quad \frac{7^2\gamma}{1-\gamma} < 1,$$

то из (21) выводим

$$(\sigma_n^{\blacktriangledown}(ns))^2 = \mathbb{E}|X_n^{\blacktriangledown}(ns)|^2 \leqslant (7MB_n(p))^2 + \frac{7^2\gamma}{1-\gamma}\mathbb{E}|X_n^{\blacktriangledown}(ns)|^2,$$

откуда следует

$$B_n(p) \gg \sigma_n^{\blacktriangledown}(ns). \tag{22}$$

Далее, из леммы 3 e) и (17) выводим

$$\mathbb{E}|Y_j^{\blacktriangledown}(nks)|^2 = o(\widetilde{c}_{nks}^2(p)) = o(\widetilde{c}_{nk}^2(p)) = o(B_{nk}^2(p))$$

Так как в силу (4) $|X_m^{\blacktriangledown}(nks)| \leqslant (1+\varepsilon)(|Y_1^{\blacktriangledown}(nks)| + ... + |Y_m^{\blacktriangledown}(nks)|) + mN$, то при любых $k, s \in \mathbb{N}$ найдётся $m = m(n) \to \infty$ такое, что

$$\sigma_m^{\blacktriangledown}(nks) = o(B_{nk}(p)),\ \sigma_{km}^{\blacktriangledown}(nks) = o(B_{nk}(p))\ n \to \infty.$$

Обозначим $U_j = X^{\blacktriangledown}_{(j-1)(n+m)+1,jn+(j-1)m}(nks),\ j = 1, ..., k,$
$V_j = X^{\blacktriangledown}_{jn+(j-1)m+1,j(n+m)}(nks),\ \ j = 1, ..., k-1,\ W = X^{\blacktriangledown}_{kn+1,kn+(k-1)m}(nks).$

В силу (4)

$$|X_{nk}^{\blacktriangledown}(nks) - \sum_{j=1}^{k} U_j - \sum_{j=1}^{k-1} V_j - W| \leqslant \varepsilon\left(\sum_{j=1}^{k}|U_j| + \sum_{j=1}^{k-1}|V_j| + |W|\right) + 2kN.$$

Отсюда

$$\left|\sigma_{nk}^{\blacktriangledown}(nks) - \left\|\sum_{j=1}^{k} U_j\right\|_2\right| \leqslant k\varepsilon\sigma_n^{\blacktriangledown}(nks) + k(1+\varepsilon))\sigma_m^{\blacktriangledown}(nks) + (1+\varepsilon)\sigma_{km}^{\blacktriangledown}(nks) + 2kN =$$

$$= k\varepsilon\sigma_n^{\blacktriangledown}(nks) + o(B_{nk}(p)). \tag{23}$$

Из (1) следует, что $|\mathbb{E}U_jU_l| \leqslant 4\varphi^{1/2}(m)(\sigma_n^{\blacktriangledown}(nks))^2,\ j \neq l$, откуда

$$\mathbb{E}\left(\sum_{j=1}^{k} U_j\right)^2 = k\mathbb{E}U_1^2 + \sum_{j\neq l=l}^{k} \mathbb{E}U_jU_l = k(\sigma_n^{\blacktriangledown}(nks))^2(1+o_n(1)). \tag{24}$$

Из (22), (23) и (24) при $\varepsilon < k^{-1}$ получаем

$$B_{nk}(p) \gg \sigma_{nk}^{\blacktriangledown}(nks) \geqslant (\sqrt{k}-1)\sigma_n^{\blacktriangledown}(nks) + o(B_{nk}(p)),$$

откуда следует первое утверждение в b), а из него получается второе утверждение, так как $B_m(p) \gg B_{n(k-1)}(p)$ [7, лемма 1].

c) Доказательство $\sigma_{nk} \gg \sqrt{k}\sigma_n$ по сути повторяет доказательство утверждения b), где вместо $X_n^{\blacktriangledown}$ нужно взять $\widetilde{X}_n$.

В силу (4)

$$|\widetilde{X}_m - \widetilde{X}_{nk} - \widetilde{X}_{nk+1,m}| \leqslant \varepsilon|\widetilde{X}_{nk+1,m}| + N$$

и так как $\sigma_{m-nk} \ll \sigma_n$ [7, лемма 1], то $|\sigma_m - \sigma_{nk}| \ll \sigma_n + N \ll \dfrac{\sigma_{nk}}{\sqrt{k}}$.

d) Если $p \leqslant 2$, то в силу леммы 3 e) $\sigma_n \geqslant B_n(p) \gg \widetilde{c}_n(p)$.

Пусть $p > 2$. Положим $\rho_n = \dfrac{\widetilde{c}_n^p(p)}{\sigma_n^p}$. Из (17) и утверждения c) следует, что найдутся $n_0 \in \mathbb{N}$ и $C > 0$ такие, что при $n \geqslant n_0$ $\rho_{kn} \leqslant Ck^{1-p/2}\rho_n \leqslant \tau\rho_n,\ \tau < 1$ если k достаточно велико. Отсюда $\rho_{k^m n_0} \leqslant \tau^m\rho_{n_0} \to 0,\ m \to \infty$ и из утверждения c) и неубывания $\{\widetilde{c}_n^p(p)\}$ по n следует $\rho_n \to 0,\ n \to \infty$. ■

Доказательство теоремы 2.

1) Пусть $\{\xi_n\}$ — стационарная последовательность, удовлетворяющая условию φ_1-перемешивания, функция f удовлетворяет условиям $f_1 - f_4$ и $L(X_1) \in \mathcal{N}_0(f)$.

Если $\xi \geqslant 0,\ \mathbb{E}\xi < \infty$, то $x\mathbb{P}\{\xi \geqslant x\} \to 0, x \to \infty$, так что

$$\mathbb{E}\{(Z_n')^2, |Z_n'| \geqslant Nc_n(p)\} = N^2c_n^2(p)\mathbb{P}\{|Z_n'| \geqslant Nc_n(p)\} + \int\limits_{N^2c_n^2(p)}^{\infty} \mathbb{P}\{(Z_n')^2 \geqslant x\}\,dx =$$

$$= c_n^2(p)\int\limits_{N^2}^{\infty} \mathbb{P}\{(Z_n')^2 \geqslant xc_n^2(p)\}\,dx + o_n(1) \leqslant nc_n^2(p)\int\limits_{N^2}^{\infty} \mathbb{P}\{X_1^2 \geqslant xc_n^2(p)\}\,dx + o_n(1),$$

откуда в силу (5) следует, что последовательность $\{c_n^{-2}(p)(Z_n')^2\}$ равномерно интегрируема. Так как $\sigma_n^2 = 2\mathbb{D}X_n = 2(\sigma_n^*)^2$, то из лемм 3 d) и 5 d) получаем $\sigma_n^* \gg \sigma_n \gg \widetilde{c}_n(p) \gg c_n(p)$, так что равномерно интегрируемой является последовательность $\{(\sigma_n^*)^{-2}(Z_n')^2\}$. Отсюда, если $k = k(n) \to \infty$ достаточно медленно, с помощью (19) и лемм 3 b) и 5 c) при некотором $a > 0$ получаем

$$nk(\sigma_{nk}^*)^{-2}\mathbb{E}\{X_1^2, X_1^2 \geqslant \delta(\sigma_{nk}^*)^2\} \ll n(\sigma_n^*)^{-2}\mathbb{E}\left\{X_1^2, X_1^2 \geqslant a\delta k(\sigma_n^*)^2\right\} \ll$$

$$\ll (\sigma_n^*)^{-2}\mathbb{E}\left\{(Z_n')^2, (Z_n')^2 \geqslant a\delta k(\sigma_n^*)^2\right\} \to 0,\ n \to \infty.$$

Если $nk \leqslant m \leqslant n(k+1)$, то в силу леммы 5 c)

$$m(\sigma_m^*)^{-2}\mathbb{E}\{X_1^2, X_1^2 \geqslant \delta(\sigma_m^*)^2\} \ll n(\sigma_n^*)^{-2}\mathbb{E}\{X_1^2, X_1^2 \geqslant N(\sigma_n^*)^2\},\ N \gg k\delta,$$

откуда следует условие Линдеберга для последовательности $\{X_n\}$: при любом $\delta > 0$

$$m(\sigma_m^*)^{-2}\mathbb{E}\{X_1^2, X_1^2 \geqslant \delta(\sigma_m^*)^2\} \to 0,\ m \to \infty.$$

В силу теоремы 3 из [10] к последовательности $\{X_n\}$ применима центральная предельная теорема.

2) Из (10) и Леммы 3 d) при достаточно больших n получаем

$$\mathbb{P}\{X_1^2 \geqslant xc_n^2(p)\} \leqslant \mathbb{P}\{|X_1 - \mu| \geqslant \sqrt{x}c_n(p) - |\mu|\} \leqslant 2\mathbb{P}\{\widetilde{X}_1^2 \geqslant Cx\widetilde{c}_n^2(p)\}, \tag{25}$$

$C > 0,\ x > 0,\ \mu$ — медиана X_1, и из условия (6) следует теперь

$$\lim_{\varepsilon\to 0}\liminf_{n\to\infty} n\int\limits_{\varepsilon}^{1}\mathbb{P}\{|\widetilde{X}_1|^2 \geqslant x\widetilde{c}_{nk}^2(p)\}\,dx = \infty. \tag{26}$$

В силу (4): $|X_j^{\blacktriangledown}(nks) - X_{j-1}^{\blacktriangledown}(nks) - Y_j^{\blacktriangledown}(nks)| \leqslant \varepsilon|Y_j^{\blacktriangledown}(nks)| + N$, откуда

$$|Y_j^{\blacktriangledown}(nks)| \leqslant (1-\varepsilon)^{-1}(|X_j^{\blacktriangledown}(nks)| + |X_{j-1}^{\blacktriangledown}(nks)| + N),$$

и, следовательно,

$$\max_{1\leqslant j\leqslant n}|Y_j^{\blacktriangledown}(nks)| \ll \max_{1\leqslant j\leqslant n}|X_j^{\blacktriangledown}(nks)| + N.$$

С помощью леммы 3 a) выводим $\|\max\limits_{1\leqslant j\leqslant n} X_j^{\blacktriangledown}(nks)\|_2 \ll \|X_n^{\blacktriangledown}(nks)\|_2 = \sigma_n^{\blacktriangledown}(nks))$. Пусть $a_n^* = \sup\left\{x : n\mathbb{P}\left\{|Y_j^{\blacktriangledown}(nks)| \geqslant x\right\} \geqslant 1\right\} \leqslant a_n$.

Из (19), лемм 1 и 5 b) следует

$$B_{nk}^2(p) \gg k(\sigma_n^{\blacktriangledown}(nks))^2 \gg k\mathbb{E}(\max_{1\leqslant j\leqslant n}|Y_j^{\blacktriangledown}(nks)| - N)^2 \gg$$

$$\gg nk\mathbb{E}\{|Y_1^{\blacktriangledown}(nks)|^2, |Y_1^{\blacktriangledown}(nks)| > a_n^*\} \geqslant nk\int\limits_{a_n^2}^{4\widetilde{c}_{nks}^2(p)}\mathbb{P}\{|\widetilde{Y}_1|^2 \geqslant x\}\,dx \geqslant$$

$$\geqslant nk\widetilde{c}_{nk}^2(p)\int\limits_{\varepsilon_n^2}^{1}\mathbb{P}\{|\widetilde{X}_1|^2 \geqslant x\widetilde{c}_{nk}^2(p)\}\,dx, \tag{27}$$

где в силу леммы 3 b) и c)

$$\varepsilon_n^p = \frac{a_n^p}{\widetilde{c}_{nk}^p(p)} \leqslant \frac{8n\mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_n\}}{nk\mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_{nk}\}} \leqslant \frac{8(f_n + g_n)}{kf_n},\ n \geqslant 3,\ \text{где}$$

$$f_n = \mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_{nk}\},\ g_n = \mathbb{E}\{|\widetilde{X}_1|^p,\ a_n \leqslant |\widetilde{X}_1| < a_{nk}\}.$$

Если $g_n \leqslant \sqrt{k} f_n$, то $\varepsilon_n^p \leqslant \dfrac{8(\sqrt{k}+1)}{k} \to 0,\ k \to \infty$, и в силу (26)

$$B_{nk}^2(p) \gg \widetilde{c}_{nk}^2(p) h(k),\ h(k) \to \infty,\ k \to \infty.$$

Если же $g_n > \sqrt{k} f_n$, то с помощью (27), леммы 3 b) и c) получаем

$$B_{nk}^p(p) \gg nk\mathbb{E}\{|X_1^{\blacktriangledown}(nks)|^p, |X_1^{\blacktriangledown}(nks)| \geqslant a_n\} = nk\mathbb{E}\{|\widetilde{X}_1|^p, a_n \leqslant |\widetilde{X}_1| \leqslant 2\widetilde{c}_{nks}(p)\} \gg$$

$$\gg nkg_n > \sqrt{k} nk\mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_{nk}\} \gg \sqrt{k}\widetilde{c}_{nk}^p(p).$$

И в том и в другом случае $B_{nk}(p)/\widetilde{c}_{nk}(p) \to \infty$ при некотором $k = k(n) \to \infty$. Если $nk \leqslant m \leqslant n(k+1)$, то $B_m(p) \ll B_{n(k+1)}(p)$ [7, лемма 1], а в силу (17) $\widetilde{c}_m(p) \gg \widetilde{c}_{n(k+1)}(p)$, так что $B_m(p)/\widetilde{c}_m(p) \to \infty, m \to \infty$.

Далее при любом $\varepsilon > 0$

$$\widetilde{c}_m^{-p}(p))\mathbb{E}\left\{\left|\widetilde{Z}'_m\right|^p, |\widetilde{Z}'_m| \geqslant \varepsilon\widetilde{c}_m(p)\right\} \leqslant 1,$$

откуда

$$B_m^{-p}(p)\mathbb{E}\left\{|\widetilde{Z}'_m|^p, |\widetilde{Z}'_m| \geqslant \varepsilon B_m(p)\right\} \to 0,$$

и так как $\varepsilon B_m(p) > a_m$ при достаточно больших m, из (19) получаем условие Линдеберга порядка p:

$$mB_m^{-p}(p)\mathbb{E}\left\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant \varepsilon B_m(p)\right\} \to 0.$$

В силу Теоремы 3 из [7] $\{\widetilde{X}_n\}$, а вместе с ней и $\{X_n\}$ притягиваются к нормальному закону. Теорема доказана.

Замечание 2. 1. Пусть $\mathbb{E}|X_1|^p < \infty,\ p > 2$. Из (25) и леммы 3 b) получаем

$$n\mathbb{P}\{X_1^2 \geqslant xc_n^2(p)\} \leqslant 2n\mathbb{P}\{\widetilde{X}_1^2 \geqslant Cx\widetilde{c}_n^2(p)\} \leqslant 2n\mathbb{P}\{|\widetilde{X}_1| > a_{ny}\} \leqslant \frac{2}{y},$$

где $x > 0,\ y = \left[1/2(Cx)^{p/2}\right]$, $[x]$ — целая часть x. Отсюда

$$n\int\limits_N^\infty \mathbb{P}\{X_1^2 \geqslant xc_n^2(p)\}\,dx \ll \int\limits_N^\infty x^{-p/2}\,dx \to 0,\ N \to \infty,$$

так что выполняется (5), значит, к последовательности $\{X_n\}$ применима центральная предельная теорема и мы получаем обобщение теоремы И.А. Ибрагимова из [1].

2. Пусть $\mathbb{P}\{|X_1| \geqslant x\}$ — правильно меняющаяся функция порядка -2. Тогда $\mathbb{P}\{|\widetilde{X}_1| \geqslant x\}$ — правильно меняющаяся функция порядка -2 [11, с. 319] и при $p < 2$ получаем $\widetilde{c}_n^p \leqslant 2n\mathbb{E}\{|\widetilde{X}_1|^p, |\widetilde{X}_1| \geqslant a_n\} \ll a_n^p$ [11, с. 322].

С помощью леммы 3 с) и (10) при $x > 0$ и некотором $C_1 > 0$ выводим

$$2n\mathbb{P}\{X_1^2 \geqslant xc_n^2(p)\} \geqslant n\mathbb{P}\{\widetilde{X}_1^2 \geqslant 2C_1x\widetilde{c}_n^2(p)\} \geqslant n\mathbb{P}\{\widetilde{X}_1^2 \geqslant C_1xa_n^2\} \sim \frac{1}{x\sqrt{C_1}}.$$

Так как $\int\limits_{\varepsilon}^{1} x^{-1}\,dx \to \infty$, $\varepsilon \to 0$, то из последнего соотношения следует (6), последовательность $\{X_n\}$ притягивается к нормальному закону, и мы имеем обобщение результата М. Пелиград из [3].

Литература

1. Ибрагимов И.А., Линник Ю.В. Независимые и стационарно связанные величины. М. : Наука, 1965. 524 с.
2. Гринь А.Г. Нормирующие последовательности в предельных теоремах для слабо зависимых величин // Теория вероятностей и её применения. 1991. Т. 36, № 2. С. 285–300.
3. Peligrad M. On Ibragimov–Iosifescu conjecture for φ-mixing sequences // Stochastic Processes and their Applications. 1990. V .35. P. 293–308.
4. Клоков С.А. Строгое притяжение к нормальному закону для стационарных последовательностей с равномерно сильным перемешиванием // Вестник Омского университета. 1997. № 2. С. 11–13.
5. Сенета Е. Правильно меняющиеся функции. М. : Наука, 1983. 142 с.
6. Гринь А.Г. О строгом притяжении стационарных последовательностей к нормальному закону // Теория вероятностей и её применения. 1999. Т. 44, № 4. С. 1–10.
7. Гринь А.Г. О притяжении к нормальному закону функций от слабо зависимых величин // Математические структуры и моделирование. 2020. № 2(54). С. 24–39.
8. Bradley R. On the φ-mixind condition for stationary random sequences // Duke Math. J. 1980. V. 47. P. 421–433.
9. Лоэв М. Теория вероятностей. М. : ИЛ, 1962. 719 с.
10. Гринь А.Г. Об асимптотически нормальных функциях от зависимых величин // Математические структуры и моделирование. 2019. № 4(52). С. 5–16.
11. Феллер В. Введение в теорию вероятностей и её приложения. Т. 2. М. : Мир, 1984. 751 с.

ON THE STRONG ATTRACTION OF FUNCTIONS ON DEPENDENT VARIABLES TO THE NORMAL LAW

A.G. Grin

Professor, Dr.Sc.(Phys.-Math.), e-mail: griniran@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. For symmetric functions on random variables from stationary sequences satisfying the uniformly strong mixing condition, the general conditions of attraction

to the normal law in terms of distributions of individual items are obtained. The main result of the paper generalizes all known to present results of this type.

Keywords: Symmetric functions, uniformly strong mixing, strong attraction to the normal law, Ibragimov-Iosifesku hypothesis.

References

1. Ibragimov I.A. and Linnik Yu.V. Nezavisimye i statsionarno svyazannye velichiny. Moscow, Nauka Publ., 1965, 524 p. (in Russian)
2. Grin' A.G. Normiruyushchie posledovatel'nosti v predel'nykh teoremakh dlya slabo zavisimykh velichin. Teoriya veroyatnostei i ee primeneniya, 1991, vol. 36, no. 2, pp. 285–300. (in Russian)
3. Peligrad M. On Ibragimov–Iosifescu conjecture for φ-mixing sequences. Stochastic Processes and their Applications, 1990, vol .35, pp. 293–308.
4. Klokov S.A. Strogoe prityazhenie k normal'nomu zakonu dlya statsionarnykh posledovatel'nostei s ravnomerno sil'nym peremeshivaniem. Vestnik Omskogo universiteta, 1997, no. 2, pp. 11–13. (in Russian)
5. Seneta E. Pravil'no menyayushchiesya funktsii. Moscow, Nauka Publ., 1983, 142 p. (in Russian)
6. Grin' A.G. O strogom prityazhenii statsionarnykh posledovatel'nostei k normal'nomu zakonu. Teoriya veroyatnostei i ee primeneniya, 1999, vol. 44, no. 4, pp. 1–10. (in Russian)
7. Grin' A.G. O prityazhenii k normal'nomu zakonu funktsii ot slabo zavisimykh velichin. Matematicheskie struktury i modelirovanie, 2020, no. 2(54), pp. 24–39. (in Russian)
8. Bradley R. On the φ-mixind condition for stationary random sequences. Duke Math. J., 1980, vol. 47, pp. 421–433.
9. Loev M. Teoriya veroyatnostei. Moscow, IL Publ., 1962, 719 p. (in Russian)
10. Grin' A.G. Ob asimptoticheski normal'nykh funktsiyakh ot zavisimykh velichin. Matematicheskie struktury i modelirovanie, 2019, no. 4(52), pp. 5–16. (in Russian)
11. Feller V. Vvedenie v teoriyu veroyatnostei i ee prilozheniya. Vol. 2. Moscow, Mir Publ., 1984, 751 p. (in Russian)

Дата поступления в редакцию: 18.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 20–30

УДК 530.12: 530.145
DOI 10.24147/2222-8772.2020.4.20-30

РАСПАД ПРОСТРАНСТВА-ВРЕМЕНИ НА «ВЕЧНЫЕ» ПАРАЛЛЕЛЬНЫЕ ИСТОРИЧЕСКИЕ ЭПОХИ, ВРЕМЕННАЯ СЦЕПЛЕННОСТЬ И МАШИНА ВРЕМЕНИ

А.К. Гуц
д.ф.-м.н., профессор, e-mail: guts@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье показано, каким образом можно математически описать процесс распада пространства-времени на бесконечное число различных пространств-времён, которые с точки зрения некоторого наблюдателя существуют вечно. Рассматривается связь этого распада с временной сцепленностью (запутанностью) квантовых полей на бесконечно удалённой границе пространства-времени в рамках AdS/CFT-соответствия.

Ключевые слова: распад пространства-времени, исторические эпохи, машина времени, AdS/CFT-соответствие, временная запутанность.

В статьях [1, 2] мы предложили теорию машины времени, в которой предполагается существование Мира исторических эпох, переход между которыми совершает аппарат, называемый квантовой машиной времени. Этот аппарат использует квантовую сцепленность пространственных областей различных исторических эпох.

Существенным моментом, который даёт нашей теории квантовой машины времени право на существование, является предъявление доказательств того, что:

1) исторические эпохи столь же реальны, как Наша эпоха;

2) среди многообразия исторических эпох действительно присутствуют *прошлые* эпохи, например эпоха Христа (т. е. времена, когда жил Христос или его прообраз).

1. Прошлое реально

Специальная теория относительности (СТО) даёт нам доказательство того, что прошлое другого наблюдателя можно увидеть, и это говорит о его реальности[1]. Для этого необходимо быть от него достаточно далеко и нестись с огромной скоростью. Данную ситуацию хорошо описала американская студентка-физик Элла Олдерсон:

[1]Не надо путать это ви́дение с наблюдением далёких галактик.

> Движение даёт человеку другой темп времени и, следовательно, другое восприятие кадра и того, что в нем происходит. Хотя теория относительности действует на Земле всё время, различия настолько малы, что незаметны. Однако если два наблюдателя находятся на достаточном расстоянии (скажем, в десятках миллиардов световых лет) и один из них движется с огромной скоростью относительно другого, то движение может изменить их восприятие кадра и включить для движущегося наблюдателя события из прошлого и будущего. Но если это правда и наше будущее или/и прошлое могут быть частью восприятия другого наблюдателя, это должно привести нас к выводу о том, что обе эти вещи — и наше прошлое, и наше будущее — уже существуют: будущее не разворачивается, и прошлое не недоступно» [3].

Если добавить к этому Мир событий общей теории относительности (ОТО), в которой и прошлое, и настоящее, и будущее *всегда есть*, то доказательство реальности прошлого сводится к экспериментальной проверке ОТО. Но ОТО имеет множество экспериментальных подтверждений. Поэтому остаётся только уверенно констатировать, что прошлое столь же реально, сколь и настоящее. Различие иллюзорно:

> Now he has again preceded me a little in parting from this strange world. This has no importance. For people like us who believe in physics, the separation between past, present and future has only the importance of an admittedly tenacious illusion (Эйнштейн. На смерть М. Бессо. Письмо его семье, 1955).

2. Как «добраться» до эпохи Христа

Итак, прошлое, прошлые эпохи — реальность. Реальность — и эпоха Христа. Она отделена от нас слоями времени, составляющими иные, промежуточные эпохи (рис. 1).

С точностью до преобразования пространства-времени мы можем представить мировую трубу цивилизации Земли как 4-параллелепипед в $\mathbb{R}^4$, разбитый на конгруэнтные 4-подпараллелепипеды, соответствующие историческим эпохам (рис. 2, А).

Построим разбиение $\mathbb{R}^4$, состоящее из 4-параллелепипедов (4-кубов), конгруэнтных тем, что изображают исторические эпохи (рис. 2, Б).

Начнем менять топологию $\mathbb{R}^4$ так, что оно распадётся на изолированные 4-параллелепипеды, а история цивилизации Земли — на изолированные исторические эпохи. При этом позже введём лоренцеву метрику в $\mathbb{R}^4$ так, что каждая историческая эпоха будет отделена от другой (ближайшей), как во времени, так и в пространстве, бесконечным промежутком времени или расстояния.

Рис. 1. Мировая труба, состоящая из мировых линий объектов цивилизации Земли

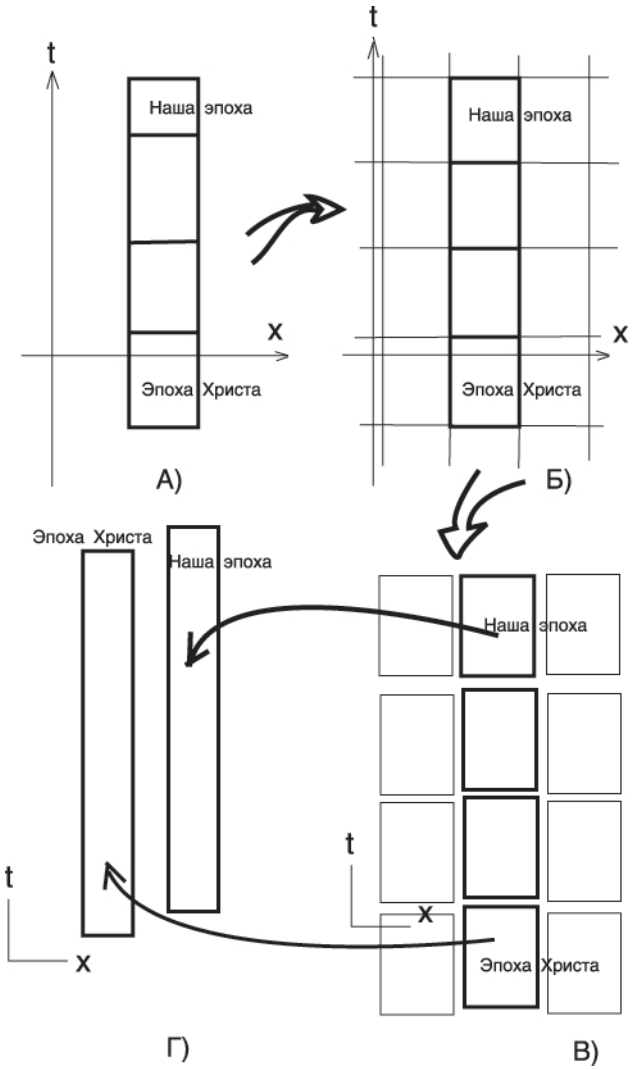

Рис. 2. А) Наша эпоха и эпоха Христа в пространстве-времени (t, x, y, z); Б) преобразование пространства-времени, разбивающего его на равные параллелепипеды; В) топологический разрыв пространства-времени на несвязные эпохи; Г) преобразование пространства-времени, в котором Наша эпоха и эпоха Христа «рядом и **параллельны** во времени»

Самым важным в наших построениях является то, что прошлая эпоха Христа оказывается самостоятельным пространством-временем, находящимся «рядом» с Нашей эпохой, и она столь же реальна, как и Наша эпоха, и в той же мере, в какой справедлива теория относительности.

Описанный процесс распада единого пространства-времени на изолированные эпохи представлен как искусственно организованный, как результат волевого акта людей. Но вполне можно допустить, что это естественный процесс, который происходит в силу ослабления или потери взаимодействия между историческими эпохами. Более того, естественен и обратный процесс, когда изолированные друг от друга исторические эпохи — компоненты некогда единого пространства-времени вновь «сливаются» и образуют, возможно, по-новому организованное единое связное пространство-время.

3. «Распад» плоскости $\mathbb{R}^2$

Чтобы представить, каким образом 4-мерное пространство-время, которое мы разбили на 4-параллелепипеды (4-кубы), распадётся на не связанные друг с другом 4-параллелепипеды за счёт введения динамически меняющейся со временем топологии, продемонстрируем это на примере распада плоскости $\mathbb{R}^2$ на квадраты.

Для описания изменения топологии плоскости $\mathbb{R}^2$, ведущей к потере связности и распаду плоскости на квадраты с целочисленными координатами вершин (k, m), $k, m \in Z$, квадратов, вводим семейство функций

$$z = f_t(x, y), \quad 0 \leqslant t \leqslant 1,$$

причём при $t < 1$

$$f_t(x, y) \in C^\infty,$$

$$f_0(x, y) \equiv 1,$$

$$0 < f_t(x, y) \leqslant 1, \quad f_t(k/2, m/2) = 1, \quad f_t(x, y) > f_{t'}(x, y) \ (t < t'), \quad f_1(x, y) < f_t(x, y)$$

$$\lim_{t \to 1-0} f_t(x, y) = f_1(x, y),$$

и функция $f_1(x, y)$ показана на рис. 3.

Мы видим, что функция $f_1(x, y)$ теряет гладкость на прямых $x = k$ и $y = m$, по которым будем разрывать плоскость.

Точки (a, b) и (c, d) считаем эквивалентными, если $a = c = k/2$ и $b = d = m/2$.

Если этот случай не имеет места, то $(a, b), (c, d) \in \mathbb{R}^2$ назовём t-эквивалентными при выполнении следующих условий:

1) $a = b$, $c = d$;

2) $f_t(a, b) = f_t(c, d)$;

3)

$$\lim_{\substack{x \to a-0 \\ y \to b-0}} \frac{\partial f_t}{\partial x}(x, y) = \lim_{\substack{x \to c+0 \\ y \to d+0}} \frac{\partial f_t}{\partial x}(x, y),$$

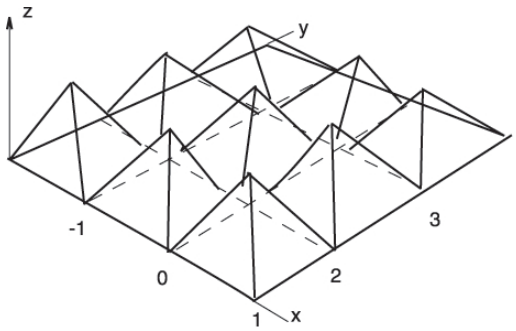

Рис. 3. Функция $f_1(x, y)$.

$$\lim_{\substack{x\to a-0\\ y\to b-0}} \frac{\partial f_t}{\partial y}(x,y) = \lim_{\substack{x\to c+0\\ y\to d+0}} \frac{\partial f_t}{\partial y}(x,y).$$

Профакторизуем пространство $\mathbb{R}^2$ по введённому отношению эквивалентности $\sim_t$. Получаем фактор-пространство $\Gamma_t = \mathbb{R}/_{\sim_t}$.

Нетрудно увидеть, что это фактор-пространство Γ_t при $t < 1$ гомеоморфно плоскости $\mathbb{R}^2$, а при $t = 1$ — несвязному пространству, состоящему из счётного числа компонент связности S_α, каждая из которых гомеоморфна квадрату $[0,1] \times [0,1]$.

Другими словами, плоскость распалась на счётное объединение непересекающихся квадратов, т. е. на «атомы» пространства $S_\alpha = [k_+, (k+1)_-]$, $k \in Z$:

$$\mathbb{R}^2 \to \Gamma_1 = \bigcup_{\alpha\in Z} S_\alpha.$$

В [4] аналогично описан распад пространства $\mathbb{R}^3$ и прямой $\mathbb{R}$.

4. Распад $\mathbb{R}^4$

В случае $\mathbb{R}^4$ мы введём функции $f_\tau(t,x,y,z)$ $(0 \leqslant \tau \leqslant 1)$, аналогичные функциям $f_t(x,y)$, где τ — время того, кто осуществляет распад пространства-времени на исторические эпохи (рис.2, В). Важно, что функция $f_1(t,x,y,z) = 0$ на границах 4-параллелепипедов (4-кубов) Q_α, на которые распадается пространство-время.

Таким образом, в нашем распоряжении появится «набор атомов пространства-времени» $\{Q_\alpha\}$, на которые распалось пространство-время

$$\mathbb{R}^4 \to \Gamma_1 = \bigcup_{\alpha\in Z} Q_\alpha,$$

состоящий, в частности, из исторических эпох.

Ничто теперь не мешает нам перетасовать эти «атомы» так, чтобы Наша эпоха и эпоха Христа были рядом и параллельны во времени (рис.2, Г). Для этого надо отобразить их в единое подходящее пространство-время (или объединить

нужным нам образом в единое пространство-время посредством введения подходящей топологии, которая склеит все распавшиеся куски-«атомы»).

Метрика, о которой говорили выше, может иметь следующий вид:

$$ds_\tau^2 = \frac{1}{[f_\tau(t, x^1, x^2, x^3)]^2} g_{ik}(t, x^1, x^2, x^3) dx^i dx^k \to_{\tau \to 1}$$

$$\to \frac{1}{[f_1(t, x^1, x^2, x^3)]^2} g_{ik}(t, x^1, x^2, x^3) dx^i dx^k = ds_1^2,$$

$$x^0 = t, \quad x^1 = x, x^2 = y, x^3 = z.$$

Очевидно, что в метрике ds_τ^2 расстояния и промежутки времени, соединяющие разные 4-кубы, стремятся к $+\infty$ при $\tau \to 1$.

5. Какие действия формируют распад $\mathbb{R}^4$

Напомним [5], что при AdS/CFT-соответствии ряд свойств пространства-времени анти-де Ситтера с $(d+2)$-метрикой

$$ds^2 = R \frac{dz^2 - dx^{0^2} + \sum_{i=1}^d dx^{i^2}}{z^2}$$

определяются свойствами квантовых полей CFT_{d+1} на границе $z = 0$. В частности, сцепленность полей S_A (entanglement entropy of a spatial region A in a holographic CFT) в пространственных непересекающихся областях A и B определяет потерю связности при $S_A \to 0$ пространства в мире анти-де Ситтера в соответствии с формулой Рю–Такаянаги (рис. 4).

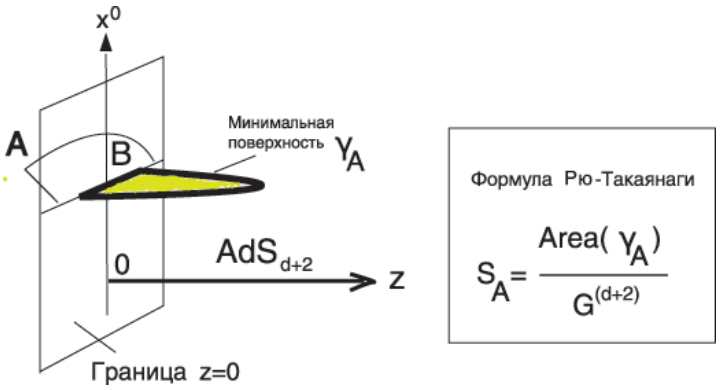

Рис. 4. Потеря связности в $(d+1)$-пространстве мира AdS_{d+2} по γ_A.

В свете AdS/CFT-соответствия, или голографической теории [5], а также с учётом формулы Рю-Такаянаги [6, 7], определённые действия над квантовыми полями на бесконечно удалённой конформной границе $Fr(\mathbb{R}^4)$ пространства-времени $\mathbb{R}^4$ обеспечивают распад $\mathbb{R}^4$ на исторические эпохи, поскольку геометрия балка AdS_{d+2}, его топология (форма), как известно, отражает граничную зацепленность.

О какой границе в нашем случае идёт речь? О множестве

$$Fr(\mathbb{R}^4) = \{(t, x^1, x^2, x^3) \in \mathbb{R}^4 : f_1(t, x^1, x^2, x^3) = 0\}.$$

А *определённые действия* над квантовыми полями — это процедура расцепления/сцепления (распутывания/запутывания) квантовых полей в непересекащихся областях границы. Расцеплению соответствует $S_A \to 0$; при сцеплении S_A увеличивается.

Граница $Fr(\mathbb{R}^4)$ имеет одну временную составляющую и две пространственные. И в отличие от пространственного сцепления, т. е. сцепления квантовых полей в непересекающихся областях A и B, принадлежащих одному пространственному сечению (рис. 4), нам, скорее всего, необходимо рассматривать временно́е сцепление, или временно́е запутывание (time entanglement), когда A и B временны́е области. Теория временно́го сцепления слабо разработана, и, тем более, соответствующие экспериментальные исследования фактически отсутствуют. Правда, зачатки нужной теории предложены в статьях польского физика Новаковского [8–12], а также иной вариант теории изложен в статье Ааронова и Вайдмана [13], но как будет выглядеть временно́й аналог формулы Рю–Такаянаги, можно только предполагать.

Новаковский определил сцепленность непротиворечивых историй, эволюционирующей во времени t системы с гамильтонианом H, записываемых в виде (тензорного) произведения

$$|H^i) = P_n^{i_n} \odot P_{n-1}^{i_{n-1}} \odot ... \odot P_1^{i_1}, \quad i = (i_n, i_{n-1}, ..., i_1),$$

$$\sum_i |H^i) = I,$$

где $P_x^{i_x}$ — оператор проектирования в момент времени t_x, $t_1 < t_2 < ... < t_n$, каждый из которых соответствует некоторой измеряемой в разные моменты времени физической величине (эрмитовому оператору). Трудно, однако, понять, как это увязывается со связностью пространства-времени, иначе говоря, как выглядит временно́й аналог формулы Рю–Такаянаги.

Обратим внимание на то, что в нашем временно́м сцеплении должны участвовать как моменты настоящего t_x, так и моменты прошлого t'_x, и моменты будущего t''_x, а сам акт сцепления/расцепления должен происходить (одновременно?) по часам τ.

Временное сцепление — это, по сути дела, синхронистичность по Юнгу, которую в какой-то мере пытался изучать нобелевский лауреат Вигнер. Путешествие в прошлое предполагает установление квантовой корреляции во времени, т. е. несиловой связи между прошлым и настоящим, или временной сцепленности, поскольку Прошлое не ждёт того, что будет сделано в Настоящем.

6. Как сцепить разные исторические эпохи

Чтобы заработала машина времени, соединяющая две исторические эпохи, нужно их пространственные области сцепить (запутать) [1, 2]. Как это сде-

лать? Обратим внимание, что это уже иное сцепление, чем сцепление квантовых полей на границе $Fr(\mathbb{R}^4)$, а именно это уже сцепление двух траекторий (пространств-времён) в суперпространстве Уилера–деВитта, или сцепление внутри балка, если иметь в виду теорию AdA/CFT.

Думается, здесь достаточно строить 4-мерную кротовую нору, соединяющую эти исторические эпохи. Почему? По заявлению Малдасены и Заскинда [14], ЭПР-пара, т. е. сцепленные частицы, соединяются 3-мерной кротовой норой. В нашем случае сцепленность временная, поэтому и нора будет 4-мерной [19].

7. Теория MIW

Есть ли в квантовой теории способы установить реальность прошлого, или параллельных миров, которые тождественны прошлым историческим эпохам?

Как теория Эверетта, которая декларирует существование параллельных миров, но не прорисовывает их явно, так и её аналог в духе де Бройля–Бома [15, 16], где эти миры уже прорисованы как геометрические траектории, не дают убедительного доказательства реальности параллельных вселенных.

Недавно появилась теория MIW (многих взаимодействующих миров) [17]. Число миров в ней конечно, и все они классические.

«Прелесть теории MIW в том, — как заявляют авторы, — что если существует только один мир, то наша теория сводится к ньютоновской механике, а если существует гигантское количество миров, она воспроизводит квантовую механику» [18]. Квантовая механика — реальность, следовательно, параллельные миры реальны.

Хотя это опять лишь декларация, но что более интересно, авторы говорят: теория «многих взаимодействующих миров» создаёт исключительную возможность проверки существования других миров: «Возможность аппроксимировать квантовую эволюцию с использованием конечного числа миров может иметь значительные разветвления в молекулярной динамике, что важно для понимания химических реакций и действия лекарств» [18].

Таким образом, о реальности прошлого теория MIW ничего не говорит. Но ценно то, что она говорит о возможности проверки реальности параллельных миров.

Поэтому нам остаётся надеяться на доказательства теории относительности, возможности AdS/CFT-соответствия и авторитет Эйнштейна.

Литература

1. Гуц А.К. Не-гёделевская машина времени // Математические структуры и моделирование. 2016. № 3(39). С. 48–58.
2. Гуц А.К. Временные эффекты коллапса волнового пакета в суперпространстве Уилера // Международный научный семинар «Нелинейные модели в механике, статистике, теории поля и космологии» GRACOS-16. Лекции школы и материалы семинара (5–7 ноября 2016 г. Казань). Казань: Казанский (Приволжский) федеральный университет, 2016. С. 273–280.

3. Ella A. Everything Exists at Once: Past, Present, and Future. On the relativity and illusion of time. URL: https://medium.com/futuresin/everything-exists-at-once-past-present-and-future-264b252e0748.
4. Гуц А.К. Моделирование распада пространства на «атомы пространства» // Математические структуры и моделирование. 2020. № 3(55). С. 12–21.
5. Nishioka T., Ryu S., Takayanagi T. Holographic Entanglement Entropy: An Overview. URL: https://arxiv.org/abs/0905.0932v2.
6. Гуц А.К. Теории пространства-времени // Пространство, время и фундаментальные взаимодействия. 2019. № 4. С. 23–47.
7. Ryu S., Takayanagi T. Aspects of Holographic Entanglement Entropy. URL: https://arxiv.org/abs/hep-th/0605073v3.
8. Nowakowski M. Quantum entanglement in time // AIP Conference Proceedings 1841, 020007. 2017. URL: https://doi.org/10.1063/1.4982771 Published Online: 31 May 2017.
9. Nowakowski M. Quantum Entanglement in Time. arXiv:1701.08116v1 [quant-ph]. 2017.
10. Nowakowski M. Monogamy of quantum entanglement in time. arXiv:1604.03976v1 [quant-ph]. 2016.
11. Nowakowski M., Cohen E. Entangled Histories vs. the Two-State-Vector Formalism — Towards a Better Understanding of Quantum Temporal Correlations. arXiv:1803.11267v2 [quant-ph]. 2018.
12. Nowakowski M. Are temporal quantum correlations generally non-monogamous? arXiv:2011.08437v1 [quant-ph]. 2020.
13. Aharonov Y., Vaidman L. The two-state vector formalism of quantum mechanics // Time in Quantum Mechanics. Springer, 2002. P. 369–447.
14. Maldacena J., Susskind L. Cool horizons for entangled black holes. arXiv:1306.0533.
15. Nelson Pinto-Netom Ward Struyvey. Bohmian quantum gravity and cosmology. arXiv:1801.03353v1 [gr-qc]. 10 Jan 2018.
16. Valentini A. De Broglie-Bohm Pilot-Wave Theory: Many Worlds in Denial? arXiv:0811.0810v2 [quant-ph]. 5 Nov 2008.
17. Hall M.J.W., Deckert D-A., Wiseman H.M. Quantum Phenomena Modeled by Interactions between Many Classical Worlds // Phys. Rev. X 4. 2014. P. 041013.
18. Many Interacting Worlds theory: Scientists propose existence and interaction of parallel worlds. URL: https://phys.org/news/2014-10-interacting-worlds-theory-scientists-interaction.html.
19. Guts A.K. Time machine as four-dimensional wormhole. arxiv: gr-qc/9612064. 1996.

THE DECAY OF SPACE-TIME TO THE ETERNAL PARALLEL HISTORICAL EPOCHS, TIME ENTANGLEMENT AND TIME MACHINE

A.K. Guts
Dr.Sc. (Phys.-Math.), Professor, e-mail: guts@omsu.ru

Dostoevsky Omsk State University

Abstract. The article shows how mathematics can describe the process of the decay of space-time to infinite number of different space-times, which from the point of view

of some observer are eternal. The relation of this decay to the time entanglement of quantum fields on an infinitely distant boundary of space-time within the AdS/CFT-correspondence is considered.

Keywords: decay of space-time, historical epochs, machine time, AdS/CFT-duality, time entanglement.

References

1. Guts A.K. Ne-gedelevskaya mashina vremeni. Matematicheskie struktury i modelirovanie, 2016, no. 3(39), pp. 48-58. (in Russian)
2. Guts A.K. Vremennye effekty kollapsa volnovogo paketa v superprostranstve Uilera. Mezhdunarodnyi nauchnyi seminar ¡¡Nelineinye modeli v mekhanike, statistike, teorii polya i kosmologii¿¿ GRACOS-16. Lektsii shkoly i materialy seminara (5–7 noyabrya 2016 g., Kazan'). Kazan': Kazanskii (Privolzhskii) federal'nyi universitet, 2016, pp. 273–280. (in Russian)
3. Ella A. Everything Exists at Once: Past, Present, and Future. On the relativity and illusion of time. URL: `https://medium.com/futuresin/everything-exists-at-once-past-present-and-future-264b252e0748`.
4. Guts A.K. Modelirovanie raspada prostranstva na ¡¡atomy prostranstva¿¿. Matematicheskie struktury i modelirovanie, 2020, no. 3(55), pp. 12–21. (in Russian)
5. Nishioka T., Ryu S., and Takayanagi T. Holographic Entanglement Entropy: An Overview. URL: `https://arxiv.org/abs/0905.0932v2`.
6. Guts A.K. Teorii prostranstva-vremeni. Prostranstvo, vremya i fundamental'nye vzaimodeistviya, 2019, no.4, pp. 23-47. (in Russian)
7. Ryu S. and Takayanagi T. Aspects of Holographic Entanglement Entropy. URL: `https://arxiv.org/abs/hep-th/0605073v3`.
8. Nowakowski M. Quantum entanglement in time, AIP Conference Proceedings 1841, 020007, 2017. URL: `https://doi.org/10.1063/1.4982771`. Published Online: 31 May 2017
9. Nowakowski M. Quantum Entanglement in Time. arXiv:1701.08116v1 [quant-ph], 2017.
10. Nowakowski M. Monogamy of quantum entanglement in time. arXiv:1604.03976v1 [quant-ph], 2016.
11. Nowakowski M. and Cohen E. Entangled Histories vs. the Two-State-Vector Formalism — Towards a Better Understanding of Quantum Temporal Correlations. arXiv:1803.11267v2 [quant-ph], 2018.
12. Nowakowski M. Are temporal quantum correlations generally non-monogamous? arXiv:2011.08437v1 [quant-ph], 2020.
13. Aharonov Y. and Vaidman L. The two-state vector formalism of quantum mechanics,in: Time in Quantum Mechanics. Springer, 2002, P. 369–447.
14. Maldacena J. and Susskind L. Cool horizons for entangled black holes, arXiv:1306.0533.
15. Nelson Pinto-Netom Ward Struyvey. Bohmian quantum gravity and cosmology. arXiv:1801.03353v1 [gr-qc], 10 Jan 2018.
16. Valentini A. De Broglie-Bohm Pilot-Wave Theory: Many Worlds in Denial? arXiv:0811.0810v2 [quant-ph], 5 Nov 2008.

17. Hall M.J.W., Deckert D-A., and Wiseman H.M. Quantum Phenomena Modeled by Interactions between Many Classical Worlds, Phys. Rev. X 4, 2014, P. 041013.
18. Many Interacting Worlds theory: Scientists propose existence and interaction of parallel worlds. URL: `https://phys.org/news/2014-10-interacting-worlds-theory-scientists-interaction.html`.
19. Guts A.K. Time machine as four-dimensional wormhole. arxiv: gr-qc/9612064, 1996.

Дата поступления в редакцию: 22.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 31–40

УДК 539.1
DOI 10.24147/2222-8772.2020.4.31-40

О ЦВЕТАХ И ЭЛЕКТРИЧЕСКИХ ЗАРЯДАХ КВАРКОВ: МОДЕЛИРОВАНИЕ В ТЕРМИНАХ ГРУПП U(n) И SU(n,n)

А.В. Левичев[1]
профессор, д.ф.-м.н., с.н.с., e-mail: alevichev@gmail.com
А.Ю. Пальянов[2]
д.ф.-м.н., в.н.с., e-mail: palyanov@iis.nsk.su

[1]Институт математики СО РАН им. С.Л. Соболева, Новосибирск, Россия
[2]Институт систем информатики СО РАН им. А.П. Ершова, Новосибирск, Россия

Аннотация. Приведено краткое описание многоуровневой модели кварк-глюонной среды. В рамках этой модели, используя подход Вигнера–Сигала к элементарным частицам и модифицируя схему Хана–Намбу, предложено рассматривать электрический заряд протона как частный случай целочисленных цветовых зарядов кварков. Дробные же электрические заряды кварков интерпретированы как получающиеся среднестатистически.

Ключевые слова: многоуровневая модель кварк-глюонной среды; метод Вигнера–Сигала и хронометрические фермионы; цветовые заряды; схема Хана–Намбу.

1. Введение: хронометрия Сигала и много-уровневая модель кварк-глюонной среды

В [1] была предложена многоуровневая модель (МУМ, для краткости) кварк-глюонной среды. Все используемые ниже обозначения введены в [1] и/или в [2]; в них же введена соответствующая терминология. МУМ основана на последовательности *канонических* (т. е., соответствующих главным минорам рассматриваемых матриц) вложений групп: $U(2)$ в $U(3)$, $U(2)$ в $U(4)$, $U(2)$ в $U(5)$ и т. д. Эти группы названы *уровнями* (материи): $U(2)$ — нулевым (это наш — «обычный»), $U(3)$ – первым, $U(4)$ – вторым и т. д. Такая договорённость соответствует стандартным *поколениям* кварков. В данной заметке нет необходимости рассматривать глюоны, поэтому ниже (в Секциях 2, 3) приводятся лишь те определения и обозначения, которые относятся к кваркам.

Согласно *хронометрии* Сигала (Irving E. Segal, 1918-1998), имеется всюду определённое дробно-линейное конформное действие группы $SU(2,2)$ на $\mathbf{D} = U(2)$. Исходя из него можно отыскать список всех элементарных (хронометрических) частиц спина $1/2$ в пространстве-времени $\mathbf{D}$. Сигал утверждал (см. [3], где предлагалось использование т. н. *кривой* параллелизации, но полного доказательства там нет), что их четыре: *эксон* — (гипотетическая) нейтральная массивная частица, мюонное нейтрино — ν_μ, электронное нейтрино

— ν_e и электрон — e. Соответствующие им пространства представлений поразному встроены в композиционный ряд. В [4] было предложено интерпретировать нижнее инвариантное подпространство как протонное p, нежели эксонное. Тогда цепочка факторов композиционного ряда такова: $p < \nu_\mu < \nu_e < e$. Использовалась т.н. *кривая* параллелизация.

Замечание 1.1. В [5] доказано, что «между» протоном и электроном имеется ЛИШЬ ОДНО нейтрино. Оно интерпретировано как электронное нейтрино. Использовалась т. н. *плоская* параллелизация.

Состояния протона принадлежат $SU(2,2)$-инвариантному подпространству, поэтому протон является стабильной частицей. Согласно МУМ, кварк может быть интерпретирован как (попавший на «более глубокий» уровень) протон. Такая интерпретация не противоречит детектированию трёх точечных составляющих в протоне при глубоко-неупругом электрон-протонном рассеянии (см. [6]) и упругому электрон-кварковому рассеянию. Число цветов зависит от рассматриваемого уровня [1]. Отметим в связи с этим, что есть работы, где число цветов больше трёх (и даже обсуждаются пределы, когда число цветов стремится к бесконечности). МУМ предсказывает ТРИ кварка четвёртого поколения (см. [7]), в то время как обычно ведётся поиск ДВУХ таковых.

2. Аромат и цвет кварков первого поколения

Исторически (чтобы не получилось противоречие с принципом Паули) составляющим протон фермионам (т. е. кваркам) был приписан *цвет*. В отличие от Стандартной Модели (СМ, для краткости) в МУМ не предполагается, что протон состоит из каких-либо частиц. Однако понятие цвета (хронометрических) кварков как бы «встроено» в саму МУМ (см. наши Секции 2 – 4).

Конкретизируем (упомянутые в Секции 1) вложения групп. Для уровня $U(3)$ задаём такие вложения, что при действии каждого из них матрица Z из $\mathbf{D} = U(2)$ переходит в некоторый главный минор соответствующей 3 на 3 матрицы из $U(3)$. Обозначим через D_{12} такой образ (при действии вложения A_{12}) исходного $\mathbf{D}$, что:

(2.1) каждая матрица Z из $\mathbf{D}$ теперь является 2 на 2 верхним главным минором в 3 на 3 матрице $A_{12}(Z)$ в $U(3)$,

(2.2) оставшийся диагональный элемент в $A_{12}(Z)$ равен 1,

(2.3) в $A_{12}(Z)$ все неупомянутые в (2.1) и (2.2) элементы равны нулю.

Оставшиеся два вложения, A_{13} и A_{23}, задаются аналогично. Очевидно, что D_{12}, D_{13} и D_{23} являются $U(2)$–подгруппами в $U(3)$. Отметим, что группа $U(2)$ замкнута по отношению к комплексному сопряжению и по отношению к (матричному) транспонированию. Результат Z^T транспонирования можно рассматривать как матрицу, симметричную этой Z относительно главной диагонали. Отсюда следует, что каждая из подгрупп D_{12}, D_{13}, D_{23} инвариантна по отношению к этим операциям в $U(3)$. Отметим также, что перечисляя все D_{ij}, достаточно считать, что всегда $i < j$.

На множестве всех m на m матриц введём P_m, симметрию относительно побочной диагонали. Очевидно, что если Z из $U(2)$, то и $P_2(Z)$ является эле-

ментом $U(2)$. Отсюда следует, что подгруппа D_{13} является P_3-инвариантной в $U(3)$, в то время как $P_3(D_{12}) = D_{23}, P_3(D_{23}) = D_{12}$. Назовём вложения A_{12} и A_{23} эквивалентными: одно переходит в другое при композиции с P_3. **Получилось соответствие с двумя u-кварками «в» протоне, в то время как A_{13} соответствует наличию d-кварка в этом протоне.** Таким образом введено понятие *аромата* кварка (для кварков первого уровня).

Цвет кварков был введён в [1] следующим образом. Известно, что каждая матрица g_n (в $G_n = SU(n,n)$) образована n на n блоками A_n, B_n, C_n, D_n; при этом G_n действует на $U(n)$ дробно-линейно; дополнительные детали приведены, например в [8, Секция 2.1]. Начнём с вложения A_{12}. Оно выделяет первую и вторую строки и первый и второй столбцы. Такое выделение (= выбор) строк и столбцов задаёт $SU(2,2)$-подгруппу G_{12} в G_3. Именно каждая g_3 в G_{12} составлена (из блоков A_2, B_2, C_2, D_2 исходной матрицы g_2 из $G_2 = SU(2,2)$) следующим образом: A_2 — это верхний главный минор в 6 на 6 матрице g_3; D_2 — главный минор, который стоит на пересечении строк и столбцов с номерами 4 и 5; ещё один (не являющийся главным) минор B_2 стоит на пересечении строк (1 и 2) со столбцами 4 и 5; C_2 стоит на пересечении строк (4 и 5) со столбцами 1 и 2. Остальные элементы матрицы g_3 таковы: 1 (если на главной диагонали) и 0 (если вне главной диагонали). Подгруппы G_{13} и G_{23} задаются аналогично. На каждой из $U(2)$-подгрупп D_{12}, D_{13}, D_{23} задаётся (естественным образом) действие любой (выбранной из G_{12}, G_{13} и G_{23}) $SU(2,2)$-подгруппы. **Цвет** (один из трёх возможных на первом уровне) **кварка** D_{ij} задаётся выбором одной подгруппы (из G_{12}, G_{13}, G_{23}).

3. Описание дальнейших уровней и общее число кварков

Сначала рассмотрим вложения $\mathbf{D} = U(2)$ в $U(4)$. Вот их список: A_{12}, A_{13}, A_{14}, A_{23}, A_{24}, A_{34}; смысл нижних индексов вполне ясен: см. предыдущую секцию. Чтобы ввести эквивалентности, привлечём (заданный выше) оператор P_4. Ясно, что A_{12} эквивалентно A_{34}, а A_{13} эквивалентно A_{24}. Каждая из подгрупп D_{14}, D_{23} является P_4–инвариантной. Соотнесём D_{14} с **s**-кварком, а D_{23} – с **c**-кварком. На этом (т. е. втором) уровне D_{12} (она эквивалентна D_{34}) ассоциируется с **u**-кварком, в то время как D_{13} (эквивалентная D_{24}) – с **d**-кварком. Следовательно (в модели), на втором уровне «живут» кварки обоих поколений (первого и второго). Понятие цвета вводится аналогично предыдущему уровню. Число цветов (на втором уровне) равно шести.

Теперь введём понятие цвета для любого уровня $U(n)$. Пусть выбрано вложение A_{ij} группы $\mathbf{D} = U(2)$ в $U(n)$. Под G_{ij} будем понимать некоторую (вполне определённую) $SU(2,2)$-подгруппу в $G_n = SU(n,n)$. Именно G_{ij} состоит из всевозможных матриц g_n, однозначно задаваемых четырьмя n на n блоками: A_n, B_n, C_n, D_n. Эти четыре блока однозначно воспроизводятся по матрице g_2 (произвольно выбранной) из $G_2 = SU(2,2)$; в частности, G_{ij} окажется изоморфной $SU(2,2)$ – см. Утверждение 1 ниже. Каждый g_2 задаётся своими 2 на 2 блоками A_2, B_2, C_2, D_2. Чтобы задать каждый n на n блок в g_n, действуем следующим образом. Выбор A_{ij} задаёт определённый 2 на 2 главный минор

(в произвольной n на n матрице). Блок A_n задаётся теми условиями, что A_2 «занимает» в нём в точности такой же 2 на 2 минор, а остальные элементы в A_n — это единицы (если этот элемент на главной диагонали) или нули (если элемент — вне главной диагонали) — ср. с тем, как была определена G_{12} в Секции 2. Блок D_n задаём аналогично: исходя из D_2. Оставшиеся блоки, B_n и C_n, задаются (с помощью B_2 и C_2) несколько иначе. Именно каждый элемент вне соответствующего 2 на 2 главного минора в блоке равен нулю. Следующее утверждение было доказано в [9].

Утверждение 1. G_{ij} является подгруппой в G_n; она изоморфна $SU(2,2)$.

Для каждого уровня $U(n), n > 2$ кварк (определённого аромата и цвета) задаётся как упорядоченная тройка (D_{pq}, G_{ij}, m). Здесь m равно 1 или минус 1 (в зависимости от того идёт ли речь о частице, или о её античастице). Подгруппа D_{pq} в $U(n)$ задаёт *аромат*, а подгруппа G_{ij} в $SU(n,n)$ задаёт *цвет*. Неявной частью такого определения является вполне определённое пространство представления (p-пространство, в нём «живёт» волновая функция протона), в котором задано действие группы G_{ij}. Нетрудно установить (доказательство опускаем) следующее:

Утверждение 2. Общее число цветов на уровне $U(n)$ равно $n(n-1)/2$.

Теперь перечислим все $U(2)$–вложения в $U(5)$: A_{12}, A_{13}, A_{14}, A_{15}, A_{23}, A_{24}, A_{25}, A_{34}, A_{35}, A_{45}. Ясно, что $P_5(D_{12}) = D_{45}$, u-кварк; $P_5(D_{13}) = D_{35}$, d-кварк; $P_5(D_{14}) = D_{25}$, s-кварк; $P_5(D_{23}) = D_{34}$, c-кварк. Каждая же из следующих двух подгрупп, D_{15} (t-кварк) и D_{24} (b-кварк), является P_5–инвариантной. Общее число цветов (для третьего уровня) равно 10.

Введём обозначение $q(n; i, j)$ для соответствующего кварка поколения n: речь идёт об уровне $U(n+2)$. Напомним, что здесь всегда $i < j$. Следствием такой договорённости являются следующие соотношения:

$$q(1;1,2) = q(1;2,3) = u, q(1;1,3) = d; q(2;1,2) = q(2;3,4) = u,$$
$$q(2;1,3) = q(2;2,4) = d, q(2;2,3) = c, q(2;1,4) = s;$$
$$q(3;1,2) = q(3;4,5) = u, q(3;1,3) = q(3;3,5) = d, q(3;2,3) = q(3;3,4) = c,$$
$$q(3;1,4) = q(3;2,5) = s, q(3;2,4) = b, q(3;1,5) = t,$$

где t – «топ-кварк».

В [1] было доказано, что у кварков четвёртого поколения имеются **три аромата** (эти новые ароматы появляются на уровне $U(6)$). В общем виде следующее утверждения было доказано в [1]:

Теорема 1. *На уровне $U(n)$ пусть $U(2)$-подгруппа D_{ij} не является P_n-инвариантной. Тогда D_{ij} соответствует кварку, «появившемуся» на более низком уровне. Имеют место следующие (рекуррентная (3.1) и явная (3.2)) формулы (для общего числа m_n кварков, «живущих» на уровне $U(n)$):*

$$m_2 = 1, m_n = m_{n-1} + [n/2], \tag{3.1}$$

$$m_n = \{n(n-1)/2 + [n/2]\}/2. \tag{3.2}$$

Под $[x]$ здесь понимается *наибольшая целая часть* (вещественного) числа x.

4. Дробные заряды кварков и схема Хана–Намбу

В СМ считается, что электрический заряд кварков u, c, t равен 2/3, а заряд кварков d, s, b равен минус 1/3. Известны и модели с целыми зарядами кварков: см., например, [10]. В этой статье даны и ссылки на (пионерские) работы Хана (Han) и Намбу (Nambu). Такой подход называется схемой Хана–Намбу. Данная секция посвящена её адаптации к МУМ. Сначала рассматриваем уровень $U(3)$. Воспроизведём (используя введённые нами обозначения) таблицу со с.1 статьи [10].

Таблица 1.

f \ c	12	23	13
u:12, 23	1	1	0
d: 13	0	0	-1

Здесь под f понимается аромат (flavor), т. е. u или d; под c — цвет (color). Последние три элемента первой строки этой таблицы правильнее было бы ввести как G_{12}, G_{23}, G_{13} (см. нашу Секцию 2), но и 12, 23, 13 не должны привести к недоразумению. Аналогично (в начале второй строки) используются 12, 23 вместо D_{12}, D_{23} и т. д. Возможная «механистическая» интерпретация такова: когда протон (в результате глубоко-неупругого взаимодействия) попал в ячейку D_{13} (и на какое-то, весьма незначительное, время там задержался), то там его цвет будет (с огромной частотой «перескоков» между цветами, по-видимому) одним из трёх: G_{12}, G_{23} или G_{13}. Так как эти цветовые подгруппы генерируют в D_{13} электрические заряды 0, 0, минус 1, то средний (average) заряд кварка d равен минус $1/3$. Аналогично: заряд кварка u равен $2/3$. Для уровня $U(4)$ вводится следующая

Таблица 2.

f \ c	12	13	14	23	24	34
u: 12, 34	1	0	1	1	0	1
d: 13, 24	0	-1	0	0	-1	0
s: 14	0	-1	0	0	-1	0
c: 23	1	0	1	1	0	1

В итоге применение схемы Хана–Намбу позволяет сделать вывод о «правильных» электрических зарядах кварков u, d, c, s на этом уровне. На уровне $U(5)$ имеются 10 цветов (см. таблицу 3). Получается, что кварки u, c, t заряжены на $7/10$, а кварки d, s, b заряжены на минус $3/10$. Таким образом, на этом уровне положения СМ и выводы МУМ (в предположении выполнения схемы Хана–Намбу) противоречат друг другу (по электрическим зарядам кварков).

Замечание 4.1. Представляется, что экспериментально данное расхождение можно исследовать в терминах следующей функции: $R =$ отношение числа случаев рождения адронов к числу случаев рождения мюон-мюон$^+$ пары при электрон-позитронной аннигиляции. Как известно (см., например, [11, с. 269]), это отношение является одним из основных объектов экспериментального изучения. В области резонансов $R(E)$ — это сложная функция. Вне резонансов: $R = 3\sum(f^2)$, где суммирование идёт по всем кваркам с массой меньше энергии E, а $f = f(q)$ - электрические заряды соответствующих кварков (вне резонансов R является кусочно-постоянной функцией). Однако сначала надо вывести аналог этой формулы для многоуровневой модели – ведь теперь число цветов равно трём лишь на уровне $U(3)$. Тем не менее (даже без знания этой формулы), можно предположить (если считать верной схему Хана–Намбу), что на уровне $U(5)$ функция R ведёт себя (качественно) иначе по сравнению с предыдущими уровнями — $U(3), U(4)$ и последующим — $U(6)$. Отметим, что в [9], в Секции 6 при рассмотрении уровня $U(5)$ были слишком поспешно предложены соответствующие численные поправки. Как мы только что отметили, сейчас этот вопрос представляется более сложным.

Таблица 3.

f \ c	12	13	14	15	23	24	25	34	35	45
u: 12, 45	1	0	1	1	1	0	1	1	0	1
d: 13, 35	0	-1	0	0	0	-1	0	0	-1	0
s: 14, 25	0	-1	0	0	0	-1	0	0	-1	0
c: 12, 45	1	0	1	1	1	0	1	1	0	1
b: 14, 25	0	-1	0	0	0	-1	0	0	-1	0
t: 12, 45	1	0	1	1	1	0	1	1	0	1

На уровне $U(6)$ число цветов равно 15, см. таблицу 4. Добавляются три новых аромата, заряды соответствующих «новых» кварков таковы: $f(4;1,6) = f(4;3,4) = 2/3; f(4;2,5) = -1/3$. На этом уровне заряды всех кварков предыдущих поколений те же, что в СМ.

Замечание 4.2. В [7] введено условие *неотрицательной минимальной целочисленности* всех канонических $U(3)$-вложений U_{ijk} (в $U(4)$, в $U(5)$ и т. д.). Также там постулируется условие *соответствия уровней*. Предполагается (чисто математически), что электрические заряды двух кварков (u и d) стандартны, а схема Хана–Намбу не используется. Доказано, что выполнение этих двух условий обеспечивает стандартность электрических зарядов остальных известных кварков (т. е. в поколениях 2 и 3). Кроме того, в [7] получены и (вышеупомянутые) значения: $f(4;1,6) = f(4;3,4) = 2/3; f(4;2,5) = -1/3$.

Таблица 4.

f \ c	12	13	14	15	16	23	24	25	26	34	35	36	45	46	56
u: 12, 56	1	0	1	1	0	1	0	1	1	1	0	1	1	0	1
d: 13, 46	0	-1	0	0	-1	0	-1	0	0	0	-1	0	0	-1	0
s: 14, 36	0	-1	0	0	-1	0	-1	0	0	0	-1	0	0	-1	0
c: 23, 45	1	0	1	1	0	1	0	1	1	1	0	1	1	0	1
b: 24, 35	0	-1	0	0	-1	0	-1	0	0	0	-1	0	0	-1	0
t: 15, 26	1	0	1	1	0	1	0	1	1	1	0	1	1	0	1
q(4;1;6)	1	0	1	1	0	1	0	1	1	1	0	1	1	0	1
q(4;2;5)	0	-1	0	0	-1	0	-1	0	0	0	-1	0	0	-1	0
q(4;3;4)	1	0	1	1	0	1	0	1	1	1	0	1	1	0	1

5. Заключение

Хронометрические фермионы (т. е. частицы спина $1/2$) вводятся исходя из т. н. спэннорного (см. [3]) представления. Мы предлагаем назвать этот способ моделирования элементарных частиц *методом Вигнера–Сигала*. В [5] было установлено, что композиционный ряд фермионов — трёхступенчатый. Крайние (т. е. нижний и верхний) факторы соответствуют заряженным частицам: протону и электрону. Этот вывод позволяет «математически» ответить на вопрос о происхождении электрического заряда следующим образом: **электрический заряд обусловлен действием конформной группы** (в виде $SU(2,2)$, например) в пространстве спэннорного представления. С точки зрения обычной кварковой модели (являющейся составной частью СМ), а также в рамках МУМ имеются и цветовые заряды. Согласно СМ, электрические заряды кварков дробны. Авторы данной заметки предлагают (в рамках МУМ) интерпретировать электрический заряд протона как частный случай цветовых зарядов ‘МУМ-кварков’ (и использовать подход Хана–Намбу). Согласно введённой (выше) конструкции, каждый МУМ-кварк — это (хронометрический) протон, попавший в определённую ячейку (на определённом уровне). В *слое* (это синоним термина уровень) $U(2)$ действует лишь одна $SU(2,2)$, т. е имеется лишь один цветовой заряд. Он интерпретируется (для протона) как электрический. В слое $U(3)$ действуют три подгруппы группы $SU(3,3)$: в нашей Секции 2 они обозначены G_{12}, G_{13}, G_{23}. Каждая из этих подгрупп изоморфна $SU(2,2)$. Отсюда — три цветовых заряда («величина» каждого из них — единица, см. таблицу 1). И т. д.: в любом слое $U(n)$ каждый цветовой заряд «генерируется» соответствующей подгруппой, изоморфной $SU(2,2)$. Электрический же заряд каждого МУМ-кварка — это статистическое среднее (average) его цветовых зарядов (более подробное описание было нами приведено выше: сразу после таблицы 1, в секции 4).

6. Финансовая поддержка

Работа А. Левичева была частично профинансирована в рамках Программы фундаментальных научных исследований СО РАН № I.1.2., проект № 0314-2019-0006.

Литература

1. Levichev A.V. Towards a matrix multi-level model of quark-gluon media // Journal of Progressive Research in Mathematics. 2016. V. 10, Issue 2. P. 1493–1496. URL: http://scitecresearch.com/journals/index.php/jprm/article/view/974/0 (дата обращения: 16.10.19).
2. Левичев А.В., Пальянов А.Ю. Анализ в космических расслоениях на основе групп U(1,1) и U(2): случаи SU(2,2)-действий в их 2- и 4-накрытиях // Математические структуры и моделирование. 2018. № 45(1). С. 12–22.
3. Segal I.E. Is the cygnet the quintessential baryon? // Proc. Natl. Acad. Sci. USA. 1991. V. 88. P. 994–998.
4. Левичев А.В. Хроногеометрия Сигала: становление теории, её применение к физике частиц и взаимодействий, перспективы развития // Поиск математических закономерностей Мироздания: физические идеи, подходы, концепции / ред. М.М. Лаврентьев, В.Н. Самойлов. Новосибирск, 2010. С. 69–99.
5. Jakobsen H.P., Levichev A.V. The representation of SU(2,2) which is interpreted as describing chronometric fermions (proton, neutrino, and electron) in terms of a single composition series // Physics of Elementary Particles and Atomic Nuclei, Letters. 2020. Submitted.
6. Breidenbach, M. et al. Observed Behavior of Highly Inelastic Electron-Proton Scattering // Phys. Rev. Lett. 1969. V. 23. P. 935–939.
7. Levichev A.V., Palyanov A.Yu. Standard charges of quarks determination in terms of the multi-level model // Proceedings of the All-Russia conference with the international participation "Knowledge-Ontology-Theories"(KONT-2019), 7-11 October 2019. Novosibirsk : Sobolev Institute of Mathematics of the Siberian Division, RAS. Novosibirsk, Russia, 2019. P. 222–226. URL: http://math.nsc.ru/conference/zont/19/ (дата обращения: 16.10.19).
8. Paneitz S.M., Segal I.E. Analysis in space-time bundles I: General considerations and the scalar bundle // Journal of Functional Analysis. 1982. V. 7. P. 78–142.
9. Levichev A.V. One Possible Application of the Chronometric Theory of I.E. Segal: A Toy Model of Quarks and Gluons. // Journal of Physics: Conference Series. 2019. V. 1194, 012071. P. 1–6.
10. Faessler M.A. Weinberg Angle and Integer Electric Charges of Quarks. URL: https://arxiv.org/abs/1308.5900 (дата обращения: 16.10.19).
11. Волошин М.Б., Тер-Мартиросян К.А. Теория калибровочных взаимодействий элементарных частиц. Москва : Энергоатомиздат, 1984.

ON COLORS AND ELECTRIC CHARGES OF QUARKS: MODELING IN TERMS OF GROUPS U(n) AND SU(n,n)

A.V. Levichev[1]
Dr.Sc.(Phys.-Math.), Professor, Senior Researcher, e-mail: alevichev@gmail.com
A.Yu. Palyanov[2]
Dr.Sc.(Phys.-Math.), Leading Researcher, e-mail: palyanov@iis.nsk.su

[1]Sobolev Institute of Mathematics SB RAS, Novosibirsk, Russia
[2]Ershov Institute of Informatics SB RAS, Novosibirsk, Russia

Abstract. A brief description of the multi-level model of the quark-gluon media is presented. In terms of this model, we use the Wigner–Segal approach to elementary particles and we modify the Han–Nambu scheme. By doing so, we suggest to view the proton's electric charge as a special case of color charges of quarks. While fractional electric charges of quarks are interpreted as statistical averages of integer color charges.

Keywords: the multi-level model of the quark-gluon media; the Wigner–Segal method and chronometric fermions; color charges; the Han–Nambu scheme.

References

1. Levichev A.V. Towards a matrix multi-level model of quark-gluon media. Journal of Progressive Research in Mathematics, 2016, vol. 10, issue 2, pp. 1493–1496. URL: `http://scitecresearch.com/journals/index.php/jprm/article/view/974/0` (16.10.19).
2. Levichev A.V. and Pal'yanov A.Yu. Analiz v kosmicheskikh rassloeniyakh na osnove grupp U(1,1) i U(2): sluchai SU(2,2)-deistvii v ikh 2- i 4-nakrytiyakh. Matematicheskie struktury i modelirovanie, 2018, no. 45(1), pp. 12–22. (in Russian)
3. Segal I.E. Is the cygnet the quintessential baryon? Proc. Natl. Acad. Sci., USA, 1991, vol. 88, pp. 994–998.
4. Levichev A.V. Khronogeometriya Sigala: stanovlenie teorii, ee primenenie k fizike chastits i vzaimodeistvii, perspektivy razvitiya. Poisk matematicheskikh zakonomernostei Mirozdaniya: fizicheskie idei, podkhody, kontseptsii, Red. M.M. Lavrent'ev, V.N. Samoilov, Novosibirsk, 2010, pp. 69–99. (in Russian)
5. Jakobsen H.P. and Levichev A.V. The representation of SU(2,2) which is interpreted as describing chronometric fermions (proton, neutrino, and electron) in terms of a single composition series. Physics of Elementary Particles and Atomic Nuclei, Letters, 2020, Submitted.
6. Breidenbach, M. et al. Observed Behavior of Highly Inelastic Electron-Proton Scattering. Phys. Rev. Lett., 1969, vol. 23, pp. 935–939.
7. Levichev A.V. and Palyanov A.Yu. Standard charges of quarks determination in terms of the multi-level model. Proceedings of the All-Russia conference with the international participation "Knowledge-Ontology-Theories" (KONvol. 2019), 7-11 October 2019,

Novosibirsk, Sobolev Institute of Mathematics of the Siberian Division, RAS, Novosibirsk, Russia, 2019, pp. 222–226. URL: `http://math.nsc.ru/conference/zont/19/` (16.10.19).

8. Paneitz S.M. and Segal I.E. Analysis in space-time bundles I: General considerations and the scalar bundle. Journal of Functional Analysis, 1982, vol. 7, pp. 78–142.
9. Levichev A.V. One Possible Application of the Chronometric Theory of I.E. Segal: A Toy Model of Quarks and Gluons. Journal of Physics: Conference Series, 2019, vol. 1194, 012071, pp. 1–6.
10. Faessler M.A. Weinberg Angle and Integer Electric Charges of Quarks. URL: `https://arxiv.org/abs/1308.5900` (16.10.19).
11. Voloshin M.B. and Ter-Martirosyan K.A. Teoriya kalibrovochnykh vzaimodeistvii elementarnykh chastits. Moscow, Energoatomizdat Publ., 1984. (in Russian)

Дата поступления в редакцию: 16.10.20

Математические структуры и моделирование
2020. № 4(56). С. 41–48

УДК 004.048:331.5
DOI 10.24147/2222-8772.2020.4.41-48

ОБ ОСОБЕННОСТЯХ РЕАЛИЗАЦИИ ИНТЕРВАЛЬНОГО МЕТОДА АНАЛИЗА ИЕРАРХИЙ В ЗАДАЧЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ РАБОТЫ СЛУЖБЫ ЗАНЯТОСТИ

Н.Ф. Богаченко
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru
Д.Н. Лавров
к.т.н., доцент, e-mail: dmitry.lavrov72@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Для определения весовых коэффициентов функции эффективности работы службы занятости использованы метод анализа иерархий и интервальная арифметика. Это позволило учесть мнения различных экспертов без потери согласованности матриц парных сравнений.

Ключевые слова: метод анализа иерархий, интервальная арифметика, функция эффективности.

Введение

В рамках выполнения научного проекта «Методология и инструменты оценки эффективности активной политики занятости на рынке труда» предложена функция эффективности работы службы занятости F, учитывающая причины снятия безработных граждан с учёта и услуги, оказанные им службой занятости:

$$F = \alpha G - \beta R, \quad G = \frac{\sum\limits_{i=1}^{N} w_i x_i}{\sum\limits_{i=1}^{N} x_i}, \quad R = \frac{\sum\limits_{k=1}^{M} \left[v_k \sum\limits_{i=1}^{X} u_{ik} \right]}{\sum\limits_{k=1}^{M} \sum\limits_{i=1}^{X} u_{ik}},$$

$$x_i \geqslant 0, \quad \sum_{i=1}^{N} x_i = X, \quad u_{ik} \geqslant 0, \quad \sum_{k=1}^{M} u_{ik} \geqslant 1, \quad u_k = \sum_{i=1}^{X} u_{ik},$$

где x_i — число безработных, завершивших период безработицы с i-ой причиной снятия с учёта; N — число статистически значимых причин снятия с учёта; w_i — условная результативность или вес i-ой причины снятия с учёта; X — число безработных; u_{ik} — число услуг вида k, оказанных i-ому безработному; v_k — условная трудоёмкость оказания услуги, или вес услуги вида k; M — число видов услуг; α, β — нормировочные коэффициенты [1]. Часть параметров модели вычисляется статистически на основе данных, предоставленных службой занятости. Для определения весовых коэффициентов w_i и v_k были привлечены эксперты и использован метод анализа иерархий (МАИ), хорошо

известный из теории поддержки принятия решений [2]. МАИ используется в случаях принятия решений на основе плохо структурированных данных, в ситуациях неопределённости, когда в зависимости от применяемых критериев мы получаем разные результаты. При работе с экспертами выяснилось, что их оценки обладают высокой вариативностью и часто сильно отличаются друг от друга. Особенно это касается экспертов, привлечённых от службы занятости. Связано это с субъективными факторами: эксперт считает более важными те критерии, которые характеризуют качество именно его работы. Решить данную проблему можно несколькими способами. Первый описан в [3] и предполагает корректировку и возможно расширение списка критериев МАИ. В данной статье предлагается применить другой подход: использование интервального МАИ для контроля получаемых в результате его работы весовых коэффициентов w_i и v_k вышеприведённой целевой функции. В этом случае и сама целевая функция F становится интервальной.

1. Реализация классического МАИ

Применение МАИ начинается со структурирования задачи в виде иерархии.

Для вычисления w_i построена трёхуровневая иерархия: цель, критерии и альтернативы. Уровень альтернатив — это $N = 9$ статистически значимых причин снятия с учёта. Вершина иерархии (цель) — ожидаемый результат работы метода — ранжирование причин снятия с учёта по степени влияния на результативность (G) работы службы занятости. После консультаций с экспертами и специалистами службы занятости были выбраны 4 критерия, влияющих на достижение поставленной цели [3].

Для оценки трудоёмкости оказания услуг (R) построена двухуровневая иерархия. Уровень альтернатив – это $M = 14$ видов услуг, оказываемых службой занятости. Вершина иерархии (цель) — ранжирование услуг по трудоёмкости их оказания службой занятости. Уровень критериев в данной иерархии отсутствует.

Следующий этап — построение матриц парных сравнений. Каждая пара критериев или альтернатив сравнивается по обратносимметричной девятибалльной шакале:

$$1/9, 1/8, \ldots, 1/2, 1, 2, 3, \ldots, 9.$$

Единица означает равное влияние, а 9 — подавляющее преимущество. Полную шкалу оценок и их смысловых эквивалентов можно найти в [2]. В трёхуровневой иерархии матрица парных сравнений уровня критериев имеет размерность 4×4, а четыре матрицы парных сравнений уровня альтернатив имеют размерность 9×9. В двухуровневой иерархии матрица парных сравнений имеет размерность 14×14.

Мера согласованности суждений экспертов в матрице парных сравнений определяется индексом согласованности

$$CI = \frac{|\lambda_{\max} - n|}{n - 1},$$

где $\lambda_{\max}$ — максимальное собственное число матрицы, n — размерность матрицы. На основе индекса согласованности рассчитывается относительная согласованность

$$CR = \frac{CI}{RI_n},$$

где RI_n — случайный индекс согласованности, зависящий от размерности матрицы [2].

Учёт мнений всех экспертов может быть сделан различными способами. Например, простым усреднением матриц парных сравнений. К сожалению, такой подход может привести к несогласованным матрицам, хотя каждая матрица конкретного эксперта по отдельности может быть идеально согласована.

В следующем разделе будет описан метод, основанный на интервальной арифметике.

2. Получение интервальных весов

Учёт расхождения мнений экспертов можно контролировать введением интервальных весовых коэффициентов (весов).

Для обозначения интервальных скалярных переменных будем использовать квадратные скобки:

$$[a] = [\underline{a}, \overline{a}],$$

где $\underline{a}$ — левая граница интервала, $\overline{a}$ — правая граница. Матрицы и векторы будем обозначать полужирным шрифтом, например так: $\mathbf{A}$, а интервальные матрицы и векторы — полужирным шрифтом в квадратных скобках: $[\mathbf{A}]$. Компоненты векторов и матриц нумеруются нижними индексами, так для матрицы $\mathbf{A}$ элемент, стоящий в i-ой строке и j-ом столбце, обозначается $A_{i,j}$.

Кратко нашу идею интервального расширения МАИ можно описать следующим образом:

1. Вычисляем для каждой матрицы парных сравнений собственный вектор и соответствующее ему максимальное собственное число с помощью степенного метода [4].
2. По вычисленным собственным векторам на минимаксной основе строим интервальные векторы весов и интервальные собственные числа матриц парных сравнений.
3. Интервальные векторы весов используем для оценки целевой функции эффективности работы службы занятости $[F]$, а интервальные собственные числа — для интервальной оценки согласованности $[CR]$.

Другие авторы часто строят интервальные матрицы парных сравнений [5–7]. Данные подходы обычно используют для оценки собственного вектора метод геометрического среднего или метод арифметического среднего [2, 8]. Степенной метод может быть применён, но как показано в [9], объём интервального «бруса» собственного вектора в итеративных алгоритмах неограниченно растёт. Наш подход основан на простой идее: необходимо отобразить матрицы парных сравнений с помощью степенного метода в множество соответствующих им собственных векторов, а затем аппроксимировать данное

множество интервальным «брусом», который будет представлен теперь уже интервальным собственным вектором.

Опишем данный подход более подробно. Даны матрицы парных сравнений, полученные от S экспертов:

$$\mathcal{A}_s = \{\mathbf{A}^{(i,j)}\},$$

где i — номер уровня в иерархии ($i = 0, \ldots, N-2$, N — число уровней в иерархии); j — номер критерия на i-ом уровне иерархии ($j = 0, \ldots, M_i - 1$, M_i — число критериев на i-ом уровне); s — номер эксперта ($s = 0, \ldots, S-1$); $\mathbf{A}^{(i,j)}$ — матрица парных сравнений s-ого эксперта (индекс s у матрицы будем опускать, чтобы не загромождать обозначения).

Для каждого эксперта структура иерархии неизменна, но набор матриц индивидуален. Пример структуры дан на рисунке 1.

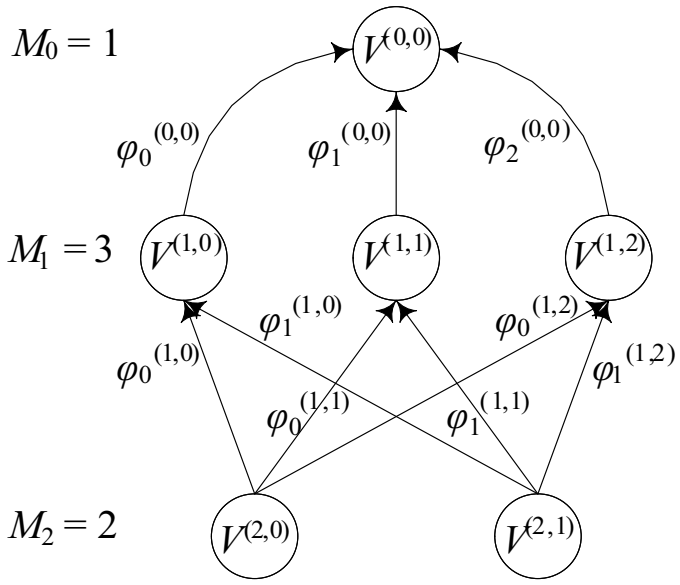

Рис. 1. Пример трёхуровневой иерархии

Для каждой матрицы парных сравнений каждого эксперта с помощью степенного метода находим собственный вектор, соответствующий максимальному собственному значению. Эти векторы образуют множество

$$\Phi_s = \{\Phi^{(i,j)}\}.$$

Экспериментально замечено, что в случае равных компонент вектора начального приближения сходимость степенного метода достигается за число шагов, равное размерности матрицы. Для ускорения сходимости начальное приближение вычисляем методом средних [8], в ситуации идеальной согласованности оно даёт точное решение. Для корректировки решения в случае рассогласованности суждений будет достаточно всего лишь нескольких итераций степенного метода.

```
function INITIAL_VECTOR(A)
    n ← SIZE(A)
    φ ← (0, ..., 0)  [n штук]
    s ← (0, ..., 0)  [n штук]
    for i ∈ {0, ..., n − 1} do
        for j ∈ {0, ..., n − 1} do
            s_i ← s_i + A_{j,i}
        end for
        for j ∈ {0, ..., n − 1} do
            A_{j,i} ← A_{j,i}/s_i
        end for
    end for
    for i ∈ {0, ..., n − 1} do
        for j ∈ {0, ..., n − 1} do
            φ_i ← φ_i + A_{i,j}
        end for
        φ_i ← φ_i/n
    end for
    return φ
end function

function POWER_METHOD(A, ε)
    φ ← INITIAL_VECTOR(A)
    n ← SIZE(A)
    repeat
        ψ ← φ
        φ ← A * ψ
        λ ← ||φ||_1
        φ ← φ/λ
    until ||φ − ψ||_1 < ε
    return λ, φ
end function
```

Интервальный вектор собственных чисел вычисляется по правилу:

$$[\boldsymbol{\varphi}] = \begin{pmatrix} [\min\limits_i \varphi_1^{(i)},\ \max\limits_i \varphi_1^{(i)}] \\ [\min\limits_i \varphi_2^{(i)},\ \max\limits_i \varphi_2^{(i)}] \\ \vdots \\ [\min\limits_i \varphi_n^{(i)},\ \max\limits_i \varphi_n^{(i)}] \end{pmatrix}$$

function INTERVAL_WEIGHT($\mathcal{A}_s$, ε)
  $N \leftarrow$ SIZE($\mathcal{A}_s$)
  $[\boldsymbol{\varphi}] \leftarrow (\underbrace{[\infty, -\infty], \ldots, [\infty, -\infty]}_{n \text{ штук}})$
  for $\mathbf{A} \in \mathcal{A}_s$ **do**
    $\mathbf{w} \leftarrow$ POWER_METHOD($\mathbf{A}$, ε)
    for $i \in \{0, \ldots, N-1\}$ **do**
      $[\underline{\varphi_i}, \overline{\varphi_i}] \leftarrow [\min(\underline{w_i}, \varphi_i),\ \max(\overline{w_i}, \varphi_i)]$
    end for
  end for
  return $[\boldsymbol{\varphi}]$
end function

Далее уже в интервальной арифметике производится суммирование весов по уровням иерархии и делается заключение о размере интервалов и точности оценки весов для выбора альтернатив. Расчёт итоговых весов производится от вершины иерархии к уровню альтернатив по формулам:

$$[V^{(i,j)}] = \sum_{k=0}^{M_{i-1}-1} [\varphi_j^{(i-1,k)}][V^{(i-1,k)}]$$

$$[V^{(0,0)}] = [1, 1],$$

где верхние индексы отвечают за номер уровня и номер критерия внутри этого уровня, а нижние индексы — за компоненты векторов.

Затем данные веса используются в вычислениях функции эффективности службы занятости $[F]$.

Заключение

В ходе проведённой работы были получены следующие результаты:

- предложена одна из возможных интервальных реализаций МАИ, адаптированная к задаче оценки эффективности работы службы занятости;
- предложен способ ускорения сходимости степенного метода для МАИ.

Благодарности

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20–010–00489.

Литература

1. Богаченко Н.Ф., Лавров Д.Н., Стукен Т.Ю. Математическая модель эффективности работы службы занятости // Математическое и компьютерное моделирование : сборник материалов VIII Международной научной конференции. Омск : Изд-во Ом. гос. ун-та, 2020. С. 151–153.

2. Saaty T.L. The Analytic Hierarchy Process. New York : McGraw Hill, 1980.
3. Богаченко Н.Ф., Лавров Д.Н., Стукен Т.Ю. Формирование экспертных оценок критериев эффективности работы службы занятости Омской области для метода анализа иерархий // Омские научные чтения — 2020 : материалы Четвёртой Всероссийской научной конференции. Омск : Изд-во Ом. гос. ун-та, 2020 (в печати).
4. Амосов А.А., Дубинский Ю.А., Копченова Н.В. Вычислительные методы для инженеров. М. : Высш. шк., 1994. 544 с.
5. Zadnik S.L., Groselj P. Estimating Priorities in Group AHP Using Interval Comparison Matrices // Multiple Criteria Decision Making. 2013. No. 8. P. 143–159.
6. Pamucar D., Stankovic M.S., Janackovic G.Lj. Modification of the AHP method based on interval valued rough numbers // International conference Transport and Logistics. 2017. V. 6. P. 295–301.
7. Entani T. Interval AHP for a group of decision makers // Proceedings of the Joint 2009 International Fuzzy Systems Association World Congress and 2009 European Society of Fuzzy Logic and Technology Conference. Lisbon, Portugal, July 20-24, 2009. P. 155–160.
8. Таха Х.А. Введение в исследование операций. М. : Издательский дом «Вильямс», 2001. 912 с.
9. Шарый С.П. Конечномерный интервальный анализ. Новосибирск : Издательство «XYZ», 2020. 643 с.

ON THE FEATURES OF THE IMPLEMENTATION OF THE INTERVAL METHOD FOR ANALYTIC HIERARCHY PROCESS IN THE PROBLEM OF ASSESSING THE EFFECTIVENESS OF THE EMPLOYMENT SERVICE

N.F. Bogachenko
Ph.D.(Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru
D.N. Lavrov
Ph.D.(Eng.), Associate Professor, e-mail: dmitry.lavrov72@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. To determine the weight coefficients of the efficiency function of the employment service, the analytic hierarchy process and interval arithmetic were used. This made it possible to take into account the opinions of various experts without losing the consistency of the matrices of pairwise comparisons.

Keywords: analytic hierarchy process, interval arithmetic, efficiency function.

References

1. Bogachenko N.F., Lavrov D.N., and Stuken T.Yu. Matematicheskaya model' effektivnosti raboty sluzhby zanyatosti. Matematicheskoe i komp'yuternoe modelirovanie, Sbornik materialov VIII Mezhdunarodnoi nauchnoi konferentsii, Omsk, Izd-vo Om. gos. un-ta, 2020, pp. 151–153. (in Russian)

2. Saaty T.L. The Analytic Hierarchy Process. New York, McGraw Hill, 1980.
3. Bogachenko N.F., Lavrov D.N., and Stuken T.Yu. Formirovanie ekspertnykh otsenok kriteriev effektivnosti raboty sluzhby zanyatosti Omskoi oblasti dlya metoda analiza ierarkhii. Omskie nauchnye chteniya — 2020, materialy Chetvertoi Vserossiiskoi nauchnoi konferentsii, Omsk, Izd-vo Om. gos. un-ta, 2020 (v pechati). (in Russian)
4. Amosov A.A., Dubinskii Yu.A., and Kopchenova N.V. Vychislitel'nye metody dlya inzhenerov. Moscow, Vyssh. shk. Publ., 1994, 544 p. (in Russian)
5. Zadnik S.L. and Groselj P. Estimating Priorities in Group AHP Using Interval Comparison Matrices. Multiple Criteria Decision Making, 2013, no. 8, pp. 143–159.
6. Pamucar D., Stankovic M.S., and Janackovic G.Lj. Modification of the AHP method based on interval valued rough numbers. International conference Transport and Logistics, 2017, vol. 6, pp. 295–301.
7. Entani T. Interval AHP for a group of decision makers. Proceedings of the Joint 2009 International Fuzzy Systems Association World Congress and 2009 European Society of Fuzzy Logic and Technology Conference, Lisbon, Portugal, July 20-24, 2009, pp. 155–160.
8. Takha Kh.A. Vvedenie v issledovanie operatsii. Moscow, Izdatel'skii dom ¡¡Vil'yams¿¿, 2001, 912 p. (in Russian)
9. Sharyi S.P. Konechnomernyi interval'nyi analiz. Novosibirsk, Izdatel'stvo «XYZ», 2020, 643 p. (in Russian)

Дата поступления в редакцию: 23.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 49–63

УДК 004.9:631.4
DOI 10.24147/2222-8772.2020.4.49-63

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ МОЗАИЧНОСТИ ЛЕСНЫХ ЭКОСИСТЕМ

Л.А. Володченкова
к.б.н., доцент, e-mail: volodchenkova2007@yandex.ru
А.К. Гуц
д.ф.-м.н., профессор, e-mail: guts@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье предложен небольшой обзор основных математических моделей, описывающих мозаичную динамику лесных сообществ: катастрофическая модель, модель Тузинкевича, модель Кахъямы и gap-модели.

Ключевые слова: мозаичность, лесные экосистемы, gap-модель.

Введение

Лесные биоценозы, как правило, обладают более или менее выраженной пространственной структурированностью и сильной неоднородностью. Другими словами, леса имеют мозаичную структуру[1]: в лесных массивах большинство видов растений заполняют свои места обитания весьма неравномерно, образуя скопления (пятна) и пустоты, «которые далеко не всегда удаётся убедительно объяснить неоднородностью условий внешней среды на соответствующих ареалах» [4]. Лесной биоценоз представляет собой пространственную мозаику, состоящую из разрозненных в пространстве групп растений. «Элементом леса», его фундаментальной единицей является не отдельное дерево, а ассоциация деревьев, находящихся на определённом участке. Развитие «элементов леса» идёт независимо и асинхронно [1]. Гибель этой единицы леса, отдельной группы деревьев образует прогалину (окно, gap).

Каким образом математически, а точнее, аналитически моделируется в современной экологии лесных сообществ мозаичная структура леса? Статья представляет небольшой обзор соответствующих математико-компьютерных моделей.

1. Сложность экосистем и простота их моделей

Прежде всего попытаемся понять, что можно ожидать от таких моделей лесных экосистем.

[1]Мозаика — нечто, состоящее из разнородных частей (пятен).

Лесные экосистемы (геобиоценозы) крайне сложны, если рассматривать их разносторонне с учётом всех факторов: географических, биологических, гидрологических, климатических и пр. Поэтому естественен вопрос: должны ли столь сложными быть сами модели?

Станислав Лем как-то написал, что лучшей моделью яблока является само яблоко. Иначе говоря, при построении модели следует быть рациональным — она должна давать предсказания по тем проблемам, которые в данный момент для исследователя представляются первоочередными.

Австралийский лесовед-эколог Ландсберг так описывал ситуацию с моделированием: «Это аксиома, что любая модель, задуманная как инструмент управления, должна быть максимально простой. Количество параметров должно быть сокращено до минимума, соизмеримого с существенными особенностями проблемы и реалистичными ответами на анализируемые переменные. Сложные, многопараметрические модели, как правило, остаются в качестве инструментов исследования в научном сообществе, и даже там они, чаще всего, используются только их создателями и, возможно, небольшим кругом коллег. Также важно, чтобы модели были сбалансированы; например, не представляется оправданным рассчитывать фотосинтез на уровне листа с точки зрения концентраций ферментов в моделях, предназначенных для применения в региональном или даже глобальном масштабе» [2], т. е. не следуют всё доводить до чрезмерной детализации.

Конечно, упрощения и допущения не способствуют уверенности в правильности модели. Но очень часто оказывается, что другой модели-то и нет. При этом следует бережно относиться к аналитическим моделям. Вся классическая наука построена на таких моделях.

По этому поводу Лансберг обнадёживающе заверяет нас: «Учёные, как правило, хорошо осведомлены о недостатках своих моделей, поэтому иногда не хотят выпускать их для практического использования. Очевидно, что важно знать о проблемных областях, которые могут привести к ошибкам, но многие несовершенные модели будут лучше, чем догадки или практические правила, поэтому позвольте нам их использовать. Улучшения последуют» [2],

2. Мозаично-ярусная модель лесного фитоценоза, основанная на дифференциальном уравнении

В работе [3] предложена *модель роста биомассы лесного биогеоценоза*, учитывающая пространственно неоднородную структуру состояния лесной экосистемы, но не описывающую её явно:

$$\frac{dx}{dt} = -\frac{\partial}{\partial x} V(x, k, m, a, w), \tag{1}$$

где

$$V(x, k, m, a, w) = \frac{\alpha}{p+2} x^{p+2} + kx^4 + mx^3 + ax^2 + wx \tag{2}$$

где $\alpha = \alpha_1 ... \alpha_p$ — фактор, учитывающий p ярусов, k — фактор, учитывающий конкуренцию, m — фактор мозаичности (оконная динамика, gap), a — антропогенный фактор, w — влажность почвы:

$$k = -c_k(CI - CI_{\text{гр}}), \quad m = c_m\left(\frac{s^2}{\mu} - 1\right),$$

$$a = -c_a(\text{УАН} - \text{УАН}_{\text{гр}}), \quad w = c_w(W - W_{\text{гр}}),$$

где $CI_{\text{гр}}$, $(s^2/\mu)_{\text{гр}} = 1$, $\text{УАН}_{\text{гр}}$, $W_{\text{гр}}$ — критические значения факторов, обозначающие границы экологической устойчивости фитоценоза.

Отметим, что доброкачественность характеризуется неравенством $x > 0$; наличие конкуренции — неравенством $k < 0$, действенность оконной динамики — неравенством $m > 0$; вырубка лесов, пожары — неравенством $a < 0$, недостаток влаги — неравенством $w < 0$.

Функция $V(x, k, m, a, w)$, заданная выражением (2), описывает при изменении параметров k, m, a, w самые различные бифуркации, называемые в математической теории катастроф катастрофами типа «бабочка» [3]. Данная модель не рассчитана на исследование образования мозаичности (окон), а создана для прогнозирования лесных экологических катастроф, которые по-разному могут протекать в зависимости от степени пространственного распределения деревьев в лесу.

Нас интересует, прежде всего, влияет ли учёт мозаичности на продукцию биомассы? Если да, то можно говорить об определённой действенности предлагаемой модели.

Степень мозаичности отражена на рис. 1. Для того чтобы понять, как может влиять фактор мозаичности m на продукцию биомассы, мы приводим графики (см. рис. 2) для решений модельного уравнения вида:

$$\frac{dx}{dt} = -6x^5 + x^3 + mx^2, \quad a = w = 0,$$

$$x(0) = 1, \quad t \in [0, 20],$$

учитывающего только наличие конкуренции и степень мозаичности.

Известно, что в образовавшемся окне (gap) происходит восстановление растительности, идёт сукцессия. Серийные (временно существующие) растительные сообщества, характеризующие этапы сукцессии, — это равновесные состояния, т. е. для них биомасса не меняется со временем, или

$$\frac{dx}{dt} = 0.$$

Это состояния, к которым последовательно скачкообразно (катастрофически) переходит лесная экосистема в ходе сукцессии.

Модель (1)–(2) позволяет проследить эти равновесные ситуации, уточнить вид соответствующего потенциала V. На рис. 3 изображён вид потенциала при

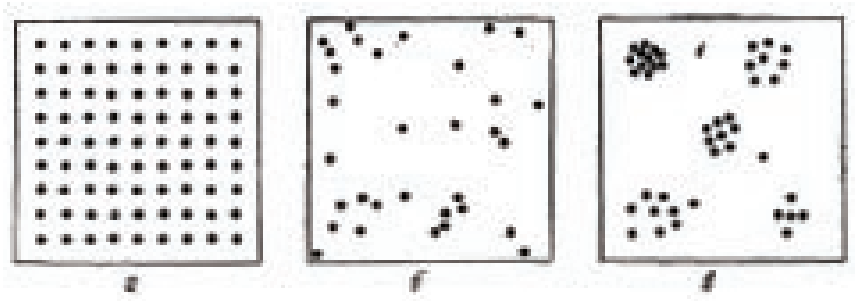

Рис. 1. Способы размещения деревьев в лесу: а) регулярное распределение ($m < 0$), б) случайное (равномерное) распределение ($m = 0$), в) контагиозное (пятнистое, мозаичное) распределение ($m > 0$)

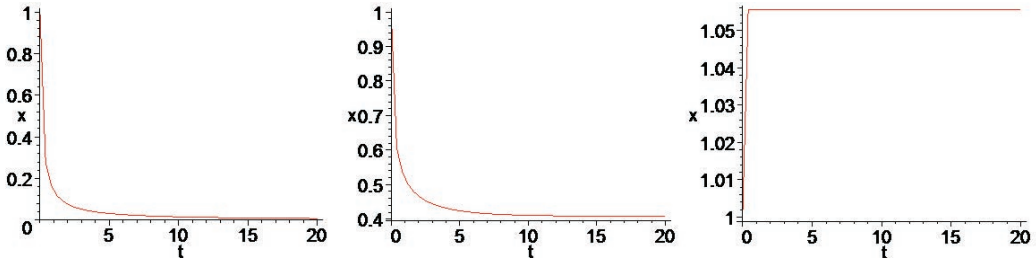

Рис. 2. Продукция биомассы в зависимости от типа пространственного распределения деревьев в лесу: а) регулярное распределение ($m = -6 < 0$), б) случайное (равномерное) распределение ($m = 0$), в) контагиозное (пятнистое, мозаичное) распределение ($m = 6 > 0$)

разных значениях фактора мозаичности m в паре с антропогенным воздействием (пожар, вырубка).

Мы видим из графиков рис. 2, 3, что модель (1)–(2) способна учитывать значения фактора мозаичности лесной экосистемы при определении биомассы.

Но хотелось бы иметь модель, которая, основываясь на ярусно-мозаичной парадигме, в своих предсказаниях не просто учитывает значения фактор мозаичности, но и показывала бы, как происходит возникновение пространственно неоднородного (пятнистого) распределения деревьев в лесном сообществе. Такую аналитическую модель предложили, например, А.В. Тузинкевич и другие [4].

3. Аналитические модели, использующие уравнения в частных производных

В этом параграфе рассмотрим модели А.В. Тузинкевич [4] и Кахъямы [6], описывающие динамику мозаичного леса, динамику образования окон (gap'ов) и восстановление растительности в них, т. е. сукцессию.

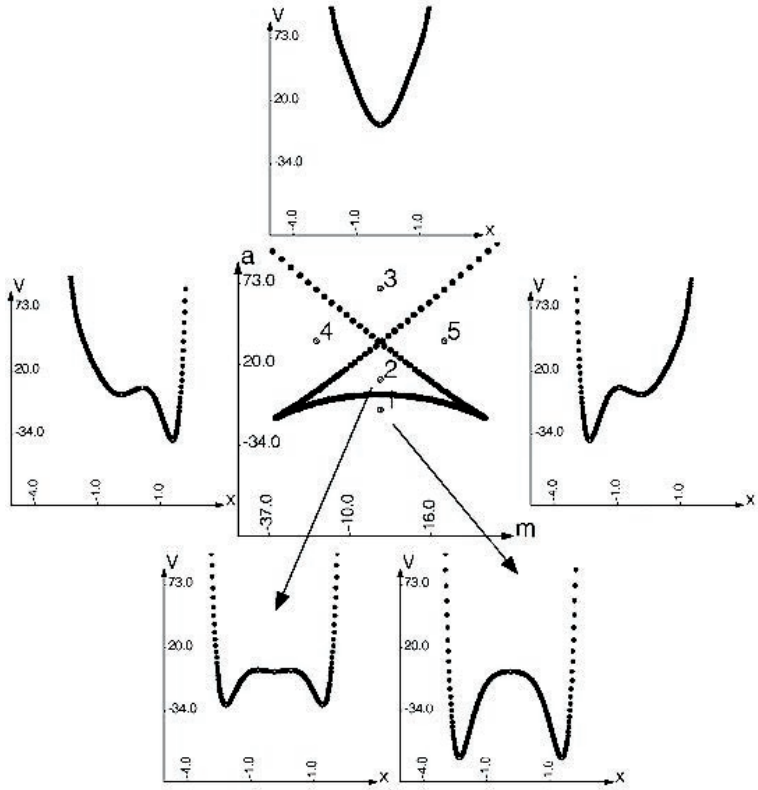

Рис. 3. Графики потенциала V и равновесные состояния при сукцессии (ямки на графике потенциала) для 6-ярусного леса в плоскости «мозаичность m – пожары (вырубка) a» в случае $w = 0$, $k = -20$ [3]

3.1. Модель возникновения мозаичных растительных сообществ, основанная на системе интегро-дифференциальных уравнений

При построении данной модели учитывалось взаимодействие растений, расположенных рядом и оказывающих влияние как на увеличение биомассы (например новая поросль), так и на ограничение её роста, вызванное конкуренцией за ресурсы, необходимые для жизнедеятельности (в первую очередь за свет) [4].

Предлагаемая модель имеет вид

$$\frac{\partial u_i}{\partial t}(x,t) = \int\limits_M \alpha_i(x,y)u_i(y,t)dy - [u_i(x,t)]^{\gamma_i} \sum_j \int\limits_M \gamma_{ij}(x,y)[u_j(y,t)]^{\rho_j} dy, \qquad (3)$$

где $u_i(x,t)$ — плотность биомассы i-го вида в точке x в момент времени t, M — физическое пространство, ареал обитания сообщества. Параметр γ_i характеризует чувствительность подавляемой биомассы к конкурентному воздействию, параметр ρ_j отражает нелинейность зависимости степени конкурентного лимитирования от плотности подавляющей биомассы. Ядра $\alpha_i(x,y)$ характеризуют «прорастание» биомассы i-го вида из точки y в точку x, ядра $\beta_{ij}(x,y)$ характеризуют интенсивность конкурентного подавления биомассы i-го вида в точке

x биомассой j-го вида, расположенного в точке y. Эти ядра (α_i, β_{ij}) зависят только от расстояния между точками x и y.

Для одновидового леса имеем уравнение

$$\frac{\partial u}{\partial t}(x,t) = \int\limits_M \alpha(x,y)u(y,t)dy - [u(x,t)]^\gamma \int\limits_M \gamma(x,y)[u(y,t)]^\rho dy. \qquad (4)$$

Для этого уравнения неоднородное пространственное распределение получаем из начального однородного $u(x,0) = 0,3$ для всех x. Для того чтобы получить неоднородное пространственное распределение, параметр γ был взят достаточно малым ($\gamma = 0,1$), а параметр ρ больше 1 ($\rho = 3,9$), радиус ядра конкурентного воздействия больше радиуса ядра прорастания, $r_\beta > r_\alpha$: $r_\alpha = 1, r_\beta = 5,9$.

Как результат получено неоднородное распределение (рис. 3 а).

Если увеличивать значение параметра r_α, то неоднородность распределения будет увеличиваться: сначала число пиков уменьшится, между ними появятся точки, в которых биомасса равна нулю, амплитуда пиков возрастёт (в этих точках биомасса $r_\alpha = 3,9$ будет почти в три раза больше начальной), при $r_\alpha = 3,9$ их число станет равным 4 по каждой координате (рис. 3 б). Затем, если взять $r_\alpha > r_\beta$, то распределение станет крайне неоднородным (рис. 3 в), с большим числом пиков и большой их амплитудой ($\max u(x,t)$ больше $u(x,0)$ в 10 раз). Между пиками останутся точки с нулевой плотностью, но их станет значительно меньше по сравнению с предыдущими результатами.

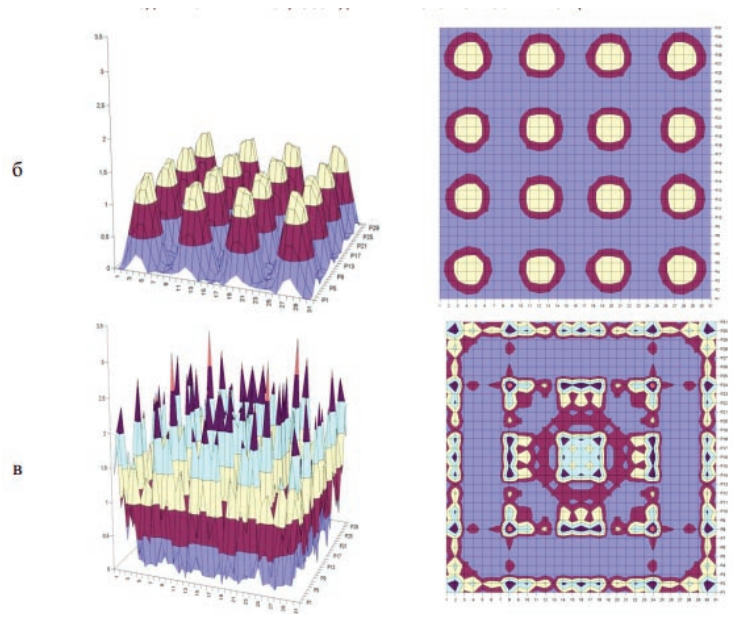

Рис. 4. Мозаика одновидового леса. Слева — вид сбоку, справа — сверху [4]

Таким образом, мы получаем возникновение мозаики.

3.2. Модель Кахъямы

Пусть $f(t, a, x)$ — плотность деревьев на единицу площади леса размером x (диаметр D ствола на уровне груди, рост H или любой другой размер) с возрастом a древостоя участка в момент времени t.

Плотность деревьев $f(t, a, x)$ определяется для каждого участка леса.

Зависящее от времени изменение $f(t, a, x)$ описывается демографическими процессами, а именно ростом размера дерева, гибелью и воспроизводством деревьев, старением участков леса и образованием окон (gap), а также перемещением по различным географическим местоположениям посредством разноса семян.

Определим $G(t, a, x)$ как скорость роста деревьев размера x; $\gamma(a)$ — как скорость образования окна (gap) (или уровень смертности участка возраста a, который возрождается на участке с исходным возрастом 0), $\mu(t, a, x)$ — как смертность деревьев размера x в древостое возраста a вне зависимости от событий образования прогалин (окон, gap), а $R(t, l)$ — скорость производства зрелых семян материнскими деревьями в меняющемся ландшафте участков леса в момент t.

Динамика популяций деревьев со структурой мозаики моделируется уравнением [5]:

$$\frac{\partial f(t,a,x)}{\partial t} = -\frac{\partial G(t,a,x) f(t,a,x)}{\partial x} -$$

$$-\frac{\partial f(t,a,x)}{\partial a} - \gamma(a) f(t,a,x) - \mu(t,a,x) f(t,a,x). \qquad (5)$$

Зависимость распределения f от времени t позволяет описывать перемещение окон (shifting-gap mosaic) в лесной экосистеме.

При определённых уточнениях модели касательно входящих в неё функций и краевых условий получается стационарное распределение, изображённое на рис. 5.

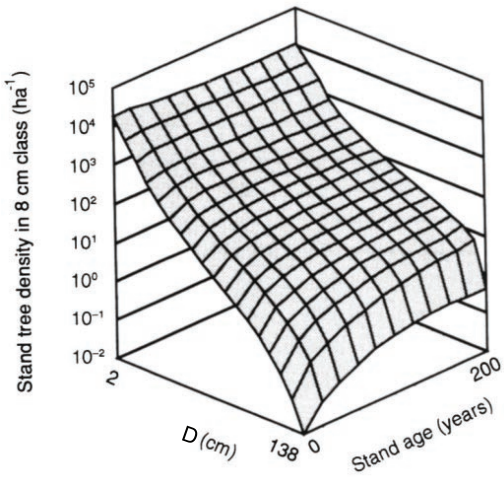

Рис. 5. Стационарное распределение деревьев (в log масштабе) [5]

На рис. 6 сравниваются наблюдаемое распределение деревьев в окнах и закрытых насаждениях с таковым же в модели (5). Соответствие наблюдаемых и смоделированных распределений на рис. 6 замечательно, поскольку в модели не использовались данные о наблюдаемом распределении.

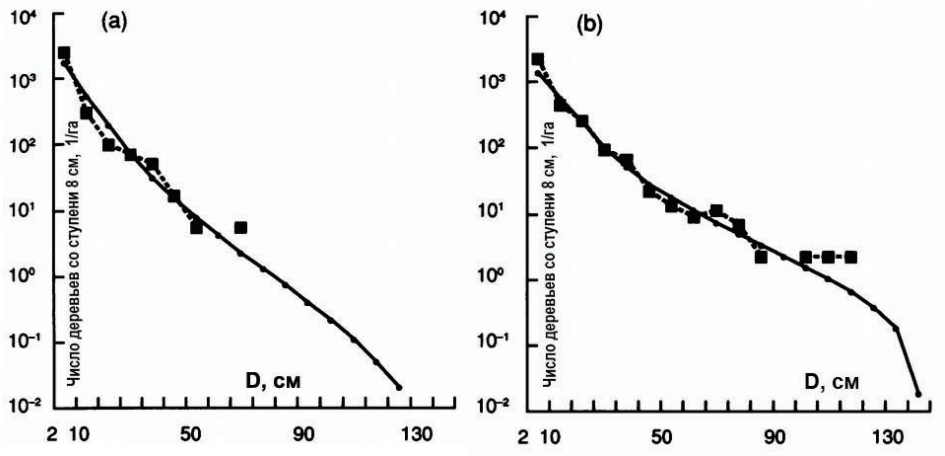

Рис. 6. Сравнение наблюдаемого и смоделированного распределения размеров деревьев в окнах и закрытых насаждениях. Наблюдаемые распределения в лесу Сегире на острове Якусима обозначены квадратами с пунктирными линиями; смоделированные — сплошными линиями с точками: (a) наблюдаемое распределение в окнах, смоделированное для древостоев от 0 до 20 лет; (b) наблюдаемое распределение в закрытых насаждениях, смоделированное для древостоев старше 20 лет (в log масштабе) [5]

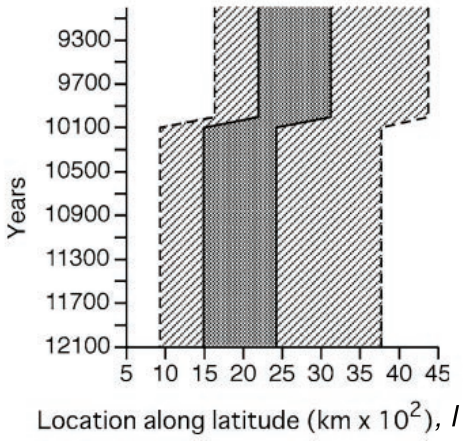

Рис. 7. Фундаментальная (потенциальная ниша) и реализованная ниша для видов, представляющих умеренно-тёплый тропический лес при сценарии глобального потепления между $t = 10000$ и $t = 10100$. Потенциальная ниша — полосатая зона внутри пунктирных линий; реализованная ниша — это заштрихованная зона внутри сплошных линий (темнее) [6]

Полученные результаты говорят в пользу предложенной аналитической модели. В статье [6] эта модель используется для предсказания перемещения экологических ниш трёх видов лесов по географическим широтам (latitude) l при глобальном потеплении (рис. 7).

4. Gap-модели

Альтернативой описанию лесных экосистем с помощью моделей в форме дифференциальных уравнений в частных производных являются gap-модели. Эти модели успешно описывают долгосрочную динамику биомассы, включающую процессы физиологии и демографии деревьев в лесных экосистемах [6].

Эти модели представляют мозаику перемещающихся участков лесных ландшафтов в соответствии с возрастным распределением участков с разной структурой размеров деревьев, при этом создание прогалин (окон) при падении деревьев соответствует «смерти» участка определённого возраста и одновременное «рождение» gap'a, обнуляющего возраст участка-окна [6], на котором запускается процесс сукцессии.

Gap-модели изучают динамику восстановления леса в окне (gap), которое образовалось в результате гибели леса на данном участке. Размер окна 10 м $\times$ 10 м (до 20 м $\times$ 20 м). Рассматриваются отдельные деревья с такими параметрами, как диаметр, высота и т. д.

Иначе говоря, gap-модели исходят из парадигмы ярусно-мозачной структуры леса (оконной динамики) и созданы для исследования динамики лесной биомассы в окне.

4.1. JABOWA и другие

Первой такой моделью была компьютерная модель JABOWA, предложенная Боткиным и др. [7]–[9], с уравнением для диаметра D деревьев

$$\frac{\Delta D}{\Delta t} = gD\phi(D)\frac{1}{b(D)}f(e), \tag{6}$$

где D — диаметр на высоте груди деревьев, параметр H — высота дерева, g — скорость роста, функция $b(D)$ — это величина, заключающая в себе данную аллометрическую взаимосвязь, $f(e)$ — величина, влияющая на абиотическую и биотическую среду при росте дерева.

$$\phi(D) = \left(1 - \frac{DH}{D_{max}H_{max}}\right).$$

Рассматривается также иное соотношение высота-диаметр, дифференциальная форма уравнения роста в модели JABOWA которого имеет вид

$$\frac{dD}{dt} = gD\phi(D), \tag{7}$$

$$\phi(D) = \frac{1 - H/H_{max}}{2H_{max} - b(-sD/b + 2)e^{-Ds/b}},$$

где s — параметр, обозначающий начальный рост высоты по отношению к росту диаметра, то есть «тонкость» дерева [10].

Используя эти уравнения, имитируют на компьютере в различных случайных условиях возобновление (рождение и рост) и гибель деревьев на участке

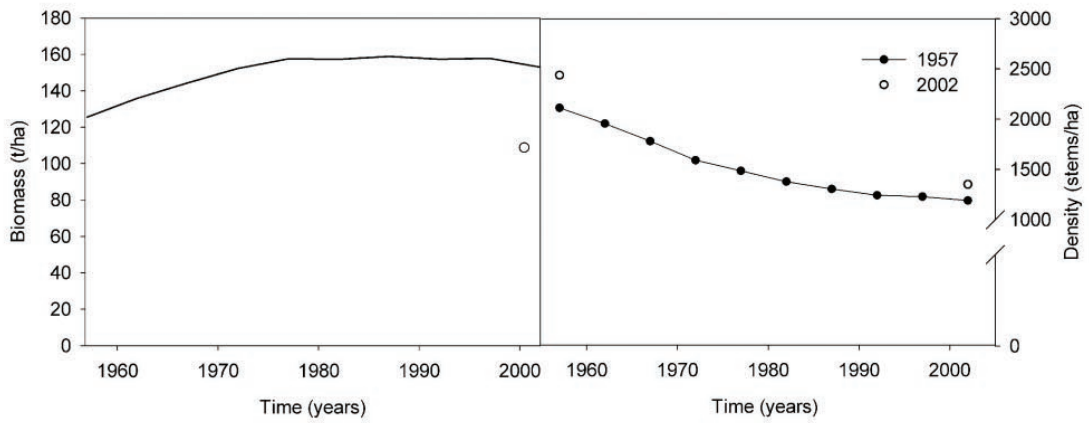

Рис. 8. Смоделировано развитие древостоя типа «горная сосна» в период с 1957 по 2001/2002‘гг. С использованием gap-модели ForClim V2.9.3. Слева: смоделированная совокупная биомасса (деревья/га). Белый кружок указывает на эмпирические значения, оценённые для этого типа насаждений в 2001/2002 г. (биомасса 106 деревьев/га). Справа: смоделированное общее количество стеблей на гектар (закрашенные кружки). Два открытых круга указывают на эмпирическое количество стеблей/га [10]

окна. Начальное распределение также берётся случайным. Состояние gap (окна) берётся усреднением по достаточно большому числу реализаций (имитаций).

Таким образом, gap-модель изучает динамику отдельного пятна мозаики леса, в котором каждое такое пятно развивается несинхронно и достаточно независимо.

Сегодня существуют различные gap-модели JABOVA, FORSKA, ForClim и другие.

Имеются различные формулы для связи диаметра дерева и его высоты. Для gap-модели FORSKA используется формула [11]

$$H = 1,3 + (H_{maz} - 1,3)(1 - \exp[-sD/(H_{max} - 1,3)]).$$

Формула для объёма [12]

$$\frac{dV}{dt} = RL_a\left(1 - \frac{DH}{D_{max}H_{max}}\right),$$

где V и L_a представляют объём и площадь листьев дерева, а R — константа, которую можно интерпретировать как регулирующую скорость ассимиляции дерева.

Таким образом, мы можем вычислять биомассу gap и число стеблей (см. рис. 8).

На рис. 9 приводятся различные симуляции (прогоны) в gap-модели ForClim V2.9.3.

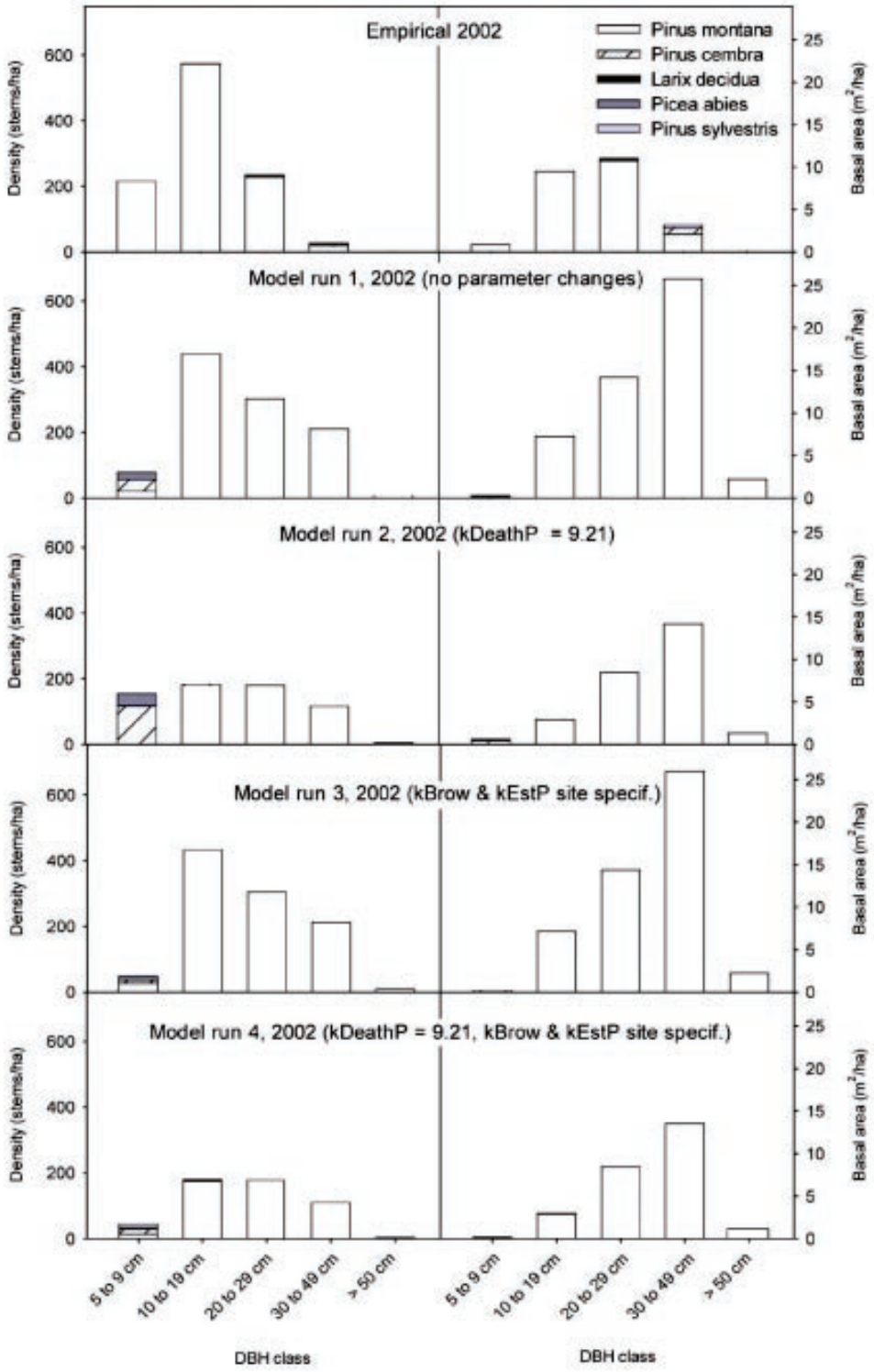

Рис. 9. Эмпирическое и смоделированное количество стеблей/га в древостое типа «сосна горная» в 2001/2002 гг. Моделирование было проведено с четырьмя различными моделями (model run 1,2,3,4) настройки gap-модели ForClim V2.9.3 [10]

4.2. Российская gap-модель

В статье [4] представлена имитационная российская gap-модель появления пространственнонеоднородной (мозаичной) структуры леса. Эта модель представляет сукцессию леса в окне.

Модель основана на уравнениях

$$\begin{cases} \dfrac{dV}{dt} = EbV - cVH, \\ \dfrac{dH}{dt} = aH(H_{max} - H), \\ D = \sqrt{\dfrac{4V}{\pi H f}}. \end{cases} \tag{8}$$

Источником роста деревьев является фотосинтез. Гибель рассматривается в ходе конкуренции и старения. Естественная смертность наступает в результате старения дерева.

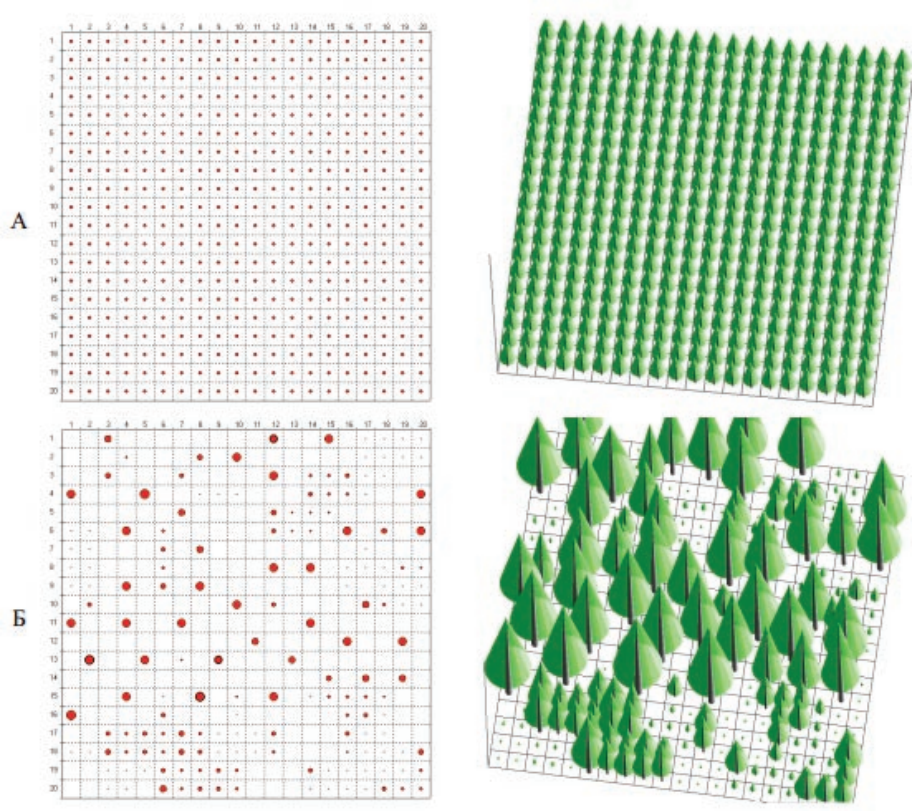

Рис. 10. Образования мозаичного распределения деревьев в результате внутренних взаимодействий (слева — двумерный вид, справа — трёхмерный): А) начало моделирования; Б) конец моделирования [4]

Прирост биомассы B дерева записываем как разность между доходами, за

счёт фотосинтетической продукции, и расходами на дыхание, транспорт:

$$\frac{dB}{dt} = P(B) - R(B).$$

Интенсивность фотосинтеза зависит от количества падающего света. В результате затенения интенсивность фотосинтеза снижается. Возможно наступление такого момента, когда затраты энергии на дыхание превысят доходы, тогда начнётся процесс отмирания биомассы, в итоге дерево погибает. Таким образом в модели учитывается затенённость деревьев в силу их ярусности.

Один из результатов компьютерных экспериментов представлен на рис. 10.

5. Заключение

Наш обзор демонстрирует заметные успехи аналитических моделей. Они способны описывать рождение мозаики и перемещение окон леса.

С другой стороны, gap-модели могут, в силу того, что они являются компьютерными и основываются на огромных данных самого различного содержания, детально прослеживать динамику возрождения леса в окне (и его гибель).

Внимательный анализ gap-моделей лесных экосистем показывает, что часто исследователи изучают изолированные «элементы леса» (по 100-200 деревьев) в силу ограниченных возможностей вычислительной техники, учитывая при этом взаимодействие деревьев. Скорее всего, основной целью является получение пространственной неоднородности деревьев (или «элементов леса»). Но и то, и другое либо основывается на ярусно-мозаичной парадигме, либо подтверждает её.

Литература

1. Карев Г.П. Структурные модели лесных экосистем // Экологический журнал. 1999. № 4. С. 381–396.
2. Landsberg J. Modelling forest ecosystems: state of the art, challenges, and future directions // Can. J. Forest Research. 2003. V. 33, Iss. 3. P. 385–397.
3. Володченкова Л.А., Гуц А.К. Кибернетика катастроф лесных экосистем. Омск : Изд-во КАН, 2012. 220 с.
4. Колобов А.Н., Фрисман Е.Я. Моделирование процессов динамической самоорганизации в пространственно распределённых растительных сообществах // Математическая биология и биоинформатика. 2008. Т. 3, № 2. С. 85–102. URL: `http://www.matbio.org/downloads/Kolobov2008(3_85).pdf` (дата обращения: 07.10.2020).
5. Kohyama T. Size-Structured Tree Populations in Gap-Dynamic Forest–The Forest Architecture Hypothesis for the Stable Coexistence of Species // Journal of Ecology. 1993. V. 81, No. 1. P. 131–143.
6. Kohyama T. Scaling up from shifting-gap mosaic to geographic distribution in the modeling of forest dynamics // Ecol. Research. 2005. V. 20. P. 305–312.
7. Botkin D.B., Janak J.F., Wallis J.R. Rationale, limitations, and assumptions of a northeastern forest growth simulator // IBM Journal of Research and Development. 1972. V. 16, No. 2. P. 101–116.

8. Botkin D.B., Janak J.F., Wallis J.R. Some ecological consequences of a computer model of forest growth // Th Journal of Ecology. 1972. V. 60, No. 3. P. 849–872.
9. Botkin D.B. Forest Dynamics: An Ecological Model. Oxford University Press, 1993.
10. Risch A.C., Heiri C., Bugmann H. Simulating structural forest patterns with a forest gap model: a model evaluation // Ecological Modelling. 2005. V. 181, No. 2–3. P. 161–172.
11. Lindner M., Siev'ken R., Pretzsch H. Improving the simulation of stand structure in a forest gap model // Forest Ecology and Management. 1997. V. 95. P. 183–195.
12. Moore A.D. On the maximum growth equation used in forest gap simulation models // Ecological Modelling. 1989. V. 45. P. 63–67.

MATHEMATICAL MODELING OF THE MOSAIC OF FOREST SYSTEMS

L.A. Volodchenkova
Ph.D.(Biology), Associate Professor, e-mail: volodchenkova2007@yandex.ru
A.K. Guts
Dr.Sc.(Phys.-Math.), Professor, e-mail: guts@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. In the article a small review of the main mathematical models describing the mosaic dynamics of forest communities is given: catastrophic model, the Tuzinkevich model, the Hahyama model and gap-models.

Keywords: mosaic structure, forest ecosystems, gap-model.

References

1. Karev G.P. Strukturnye modeli lesnykh ekosistem. Ekologicheskii zhurnal, 1999, no. 4, pp. 381–396. (in Russian)
2. Landsberg J. Modelling forest ecosystems: state of the art, challenges, and future directions. Can. J. Forest Research, 2003, vol. 33, iss. 3, pp. 385–397.
3. Volodchenkova L.A. and Guts A.K. Kibernetika katastrof lesnykh ekosistem. Omsk, Izd-vo KAN, 2012, 220 p. (in Russian)
4. Kolobov A.N. and Frisman E.Ya. Modelirovanie protsessov dinamicheskoi samoorganizatsii v prostranstvenno raspredelennykh rastitel'nykh soobshchestvakh. Matematicheskaya biologiya i bioinformatika, 2008, vol. 3, no. 2, pp. 85–102. URL: `http://www.matbio.org/downloads/Kolobov2008(3_85).pdf` (07.10.2020). (in Russian)
5. Kohyama T. Size-Structured Tree Populations in Gap-Dynamic Forest–The Forest Architecture Hypothesis for the Stable Coexistence of Species. Journal of Ecology, 1993, vol. 81, no. 1, pp. 131–143.
6. Kohyama T. Scaling up from shifting-gap mosaic to geographic distribution in the modeling of forest dynamics. Ecol. Research, 2005, vol. 20, pp. 305–312.
7. Botkin D.B., Janak J.F., and Wallis J.R. Rationale, limitations, and assumptions of a northeastern forest growth simulator. IBM Journal of Research and Development, 1972, vol. 16, no. 2, pp. 101–116.

8. Botkin D.B., Janak J.F., and Wallis J.R. Some ecological consequences of a computer model of forest growth. Th Journal of Ecology, 1972, vol. 60, nNo. 3, pp. 849–872.
9. Botkin D.B. Forest Dynamics: An Ecological Model. Oxford University Press, 1993.
10. Risch A.C., Heiri C., and Bugmann H. Simulating structural forest patterns with a forest gap model: a model evaluation. Ecological Modelling, 2005, vol. 181, no. 2–3, pp. 161–172.
11. Lindner M., Siev'ken R., and Pretzsch H. Improving the simulation of stand structure in a forest gap model. Forest Ecology and Management, 1997, vol. 95, pp. 183–195.
12. Moore A.D. On the maximum growth equation used in forest gap simulation models. Ecological Modelling, 1989, vol. 45, pp. 63–67.

Дата поступления в редакцию: 08.10.2020

Математические структуры и моделирование
2020. № 4(56). С. 64–74

УДК 004.056
DOI 10.24147/2222-8772.2020.4.64-74

ПОСТРОЕНИЕ ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ КЛЕТОЧНОГО АВТОМАТА

Н.Ф. Богаченко
к.ф.-м.н., доцент, e-mail: nfbogachenko@mail.ru
И.О. Горохов
студент, e-mail: vixxman@ya.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Работа посвящена реализации и тестированию генератора псевдослучайных последовательностей, построенного на основе модели клеточного автомата.

Ключевые слова: псевдослучайная последовательность, клеточный автомат.

Введение

Клеточные автоматы — самостоятельные объекты теоретического изучения. Изначально клеточные автоматы были разработаны для исследования самовоспроизводящихся машин. В то же время клеточные автоматы представляют собой мощный инструмент для моделирования многих физических процессов. Главное преимущество клеточных автоматов — это относительная простота в сочетании с большими возможностями для моделирования. И, конечно, такая потенциально мощная дискретная модель неоднократно находила применение в криптографии [1–7]. В данной работе модель клеточного автомата использована для построения генератора псевдослучайных последовательностей (ПСП).

Клеточный автомат является дискретной моделью, состоящей из решётки ячеек (клеток), каждая из которых может находиться в одном из нескольких состояний. В простейшем случае таких состояний 2: состояние 0 – клетка «мертва», состояние 1 – клетка «жива». Решётка автомата может быть любой размерности. Возможно создание не только плоского автомата, но и двумерного, и многомерного. Также для каждой ячейки определяется окрестность — множество клеток, которые будут влиять на дальнейшее состояние ячейки. Для работы автомата требуется первоначальное заполнение всех его ячеек, а также задание правил перехода из одного состояния в другое. Правила перехода являются общими для всех ячеек. В каждый дискретный момент времени к каждой клетке применяется правило перехода и исходя из состояний ячеек в окрестности текущая клетка меняет своё состояние. Поколением автомата называется множество ячеек в каждый дискретный момент времени. А эволю-

ция клеточного автомата — это изменение конфигурации автомата с течением времени.

Клеточные автоматы классифицируются по скорости стабилизации состояний и наличию устойчивых структур.

1. Класс 1 — в ходе эволюции быстрая стабилизация состояний автомата. Случайные структуры быстро исчезают.

2. Класс 2 — в ходе эволюции быстрая стабилизация состояний автомата. Большинство случайных структур исчезает, но некоторые остаются.

3. Класс 3 — в ходе эволюции любые стабильные структуры почти сразу уничтожаются шумом. Автомат заполнен псевдослучайными, хаотическими последовательностями.

4. Класс 4 — в ходе эволюции образуются устойчивые структуры, взаимодействующие друг с другом сложным образом. Данные структуры способны выживать долгое время.

В рамках криптографических задач несомненную ценность представляет 3-й класс клеточных автоматов.

1. Реализация клеточного автомата

Проект был реализован в среде Visual Studio Community Edition 2017 на языке C# с использованием технологии Windows Forms. Интерфейс программы представлен на рисунках 1–3.

1. Форма PRNG (рис. 1) отвечает за инициализацию Visualiser, извлечение состояний ячеек клеточного автомата и запись в файл сгенерированных чисел.

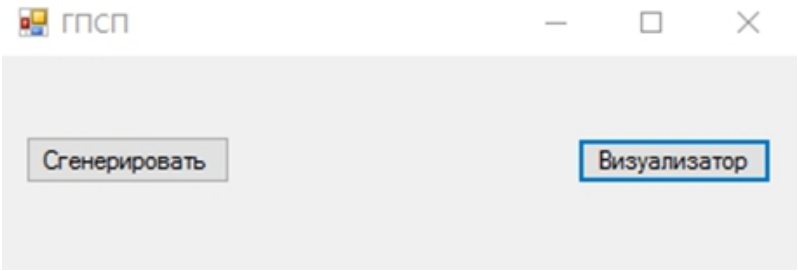

Рис. 1. Главная форма PRNG

2. Форма Visualiser (рис. 2) отвечает за инициализацию клеточного автомата, установку «по умолчанию» правил перехода и количества состояний клетки, отрисовку клеточного автомата. Имеет набор горячих клавиш, таких как пересоздание клеточного автомата, пауза, пошаговая эволюция и запуск формы Setting.

3. Форма Setting (рис. 3) отвечает за формирование правил перехода и смену количества состояний клетки.

Цикл работы клеточного автомата.

1. Точка входа main инициализирует форму PRNG.

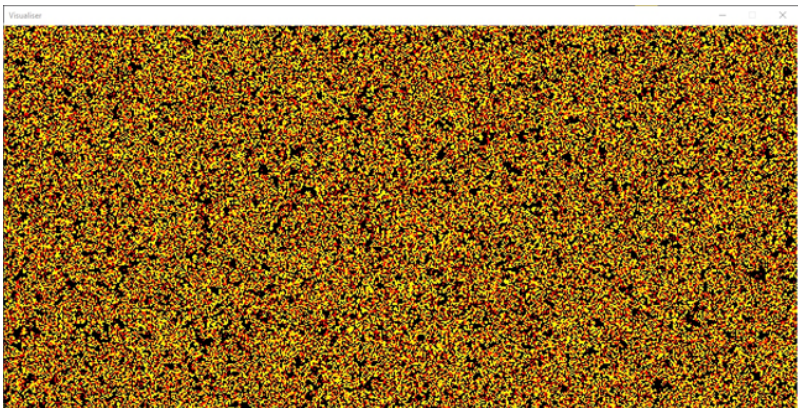

Рис. 2. Форма Visualiser

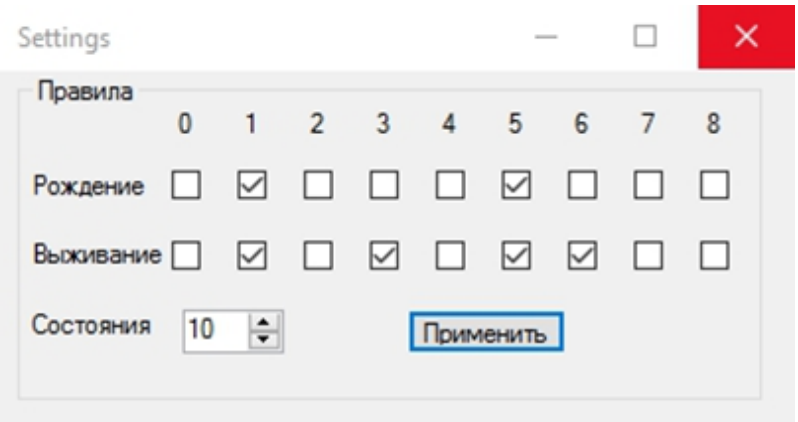

Рис. 3. Форма Setting

2. Класс PRNG инициализирует класс Visualiser.

3. Класс Visualiser создаёт Bitmap, задаёт «по умолчанию» правила перехода и количество состояний ячейки клеточного автомата и вызывает конструктор класса Automat. Создаёт класс Palette, представляющий из себя кортеж из 3-х байт (RGB). Количество элементов в списке цветов соответствует текущему количеству состояний.

4. Начальные состояния всех клеток заполняются случайным образом системной функцией System.Random.

5. Каждые 16 мс срабатывает таймер, который вызывает функцию расчёта следующего поколения автомата и перерисовку Bitmap.

Плоскость автомата представляет собой двумерное поле размерности 600×400. Клеточный автомат в текущей конфигурации использует полную окрестность Мура — окрестность 3×3, включая состояние текущей клетки. Данная окрестность была выбрана не случайно. Исследователями доказано, что именно она из всех стандартных окрестностей обладает оптимальным лавинным эффектом [8]. Этот лавинный эффект характеризуется равномерным распространением изменений состояний клеточного автомата с максимально возможной

скоростью. Каждая ячейка автомата может принимать целочисленное значение в диапазоне [0, 256]. В ходе вычислительных экспериментов выяснилось, что чем большее число состояний используется, тем более плавные и периодичные изменения происходят по всей плоскости автомата. Поэтому максимальным на данный момент выбран предел в 11 состояний: состояния клеток — это целые числа от 0 до 10. Каждому состоянию ставится в соответствие цвет в процессе отрисовки автомата.

Важно пояснить принцип работы правил. На рисунке 3 можно увидеть 18 checkbox'ов, по 9 в каждой строке. Первая строка «рождение» отвечает за условия, при которых клетка может «ожить», т. е. сменить состояние «0» на «1». В представленном примере для «рождения» клетки необходимо, чтобы количество ячеек не в состоянии «0» в окрестности 3×3 было равно 1 или 5. По похожему принципу работает механизм «выживание». Вторая строка checkbox'ов устанавливает условия, при которых текущая клетка сменит своё i-ое состояние на $i+1$-е состояние, в противном случае клетка примет состояние «0». Для правил на рисунке 3 предположим, что текущая клетка находится в состоянии «4». Тогда клетка перейдёт в состояние «5», если в её окрестности 1, 3, 5 или 6 клеток находятся не в состоянии «0». В противном случае, если количество не 0-х клеток будет, например 2, то текущая клетка перейдёт в состояние «0». Если клетка находится в максимально возможном состоянии (в текущей конфигурации это «10»), то клетка принимает состояние «0» в любом случае.

2. Реализация генератора ПСП

В текущей реализации происходит генерация 40 000 1-байтовых чисел с последующей конвертацией в строку двоичного представления и записью в файл. Каждое псевдослучайное число является продуктом разных поколений автомата.

На первом этапе вычислительных экспериментов алгоритм генерации псевдослучайного числа (ПСЧ) состоял из следующих шагов (рис. 4)

1. На вход поступает массив 600×400 клеток, из которого случайным образом выбираются 18 клеток, и извлекаются их состояния.

2. На основе полученных целых чисел формируются 2 матрицы размерностью 3×3 и перемножаются между собой.

3. Элементы полученной результирующей матрицы подвергаются операции XOR. Каждый текущий элемент «ксорится» с последующим, результат операции пишется в последующий, т. е. $[i,j] = [i,j] \oplus [i,j-1]$. Кроме редактирования самой матрицы каждое полученное число переводится в двоичный вид и записывается в строку.

4. Двоичная строка, полученная на 3 этапе, переводится в целое число и «ксорится» с целочисленным числом, полученном на 3 этапе предыдущей итерации алгоритма.

5. Полученное число переводится опять в двоичную строку, и от неё берётся хеш-функция SHA256.

6. Из полученной хэш-строки случайным образом извлекаются 8 символов,

из которых тоже случайным образом извлекается по 1 биту в случайной позиции. Полученная последовательность бит является сгенерированным целым псевдослучайным числом.

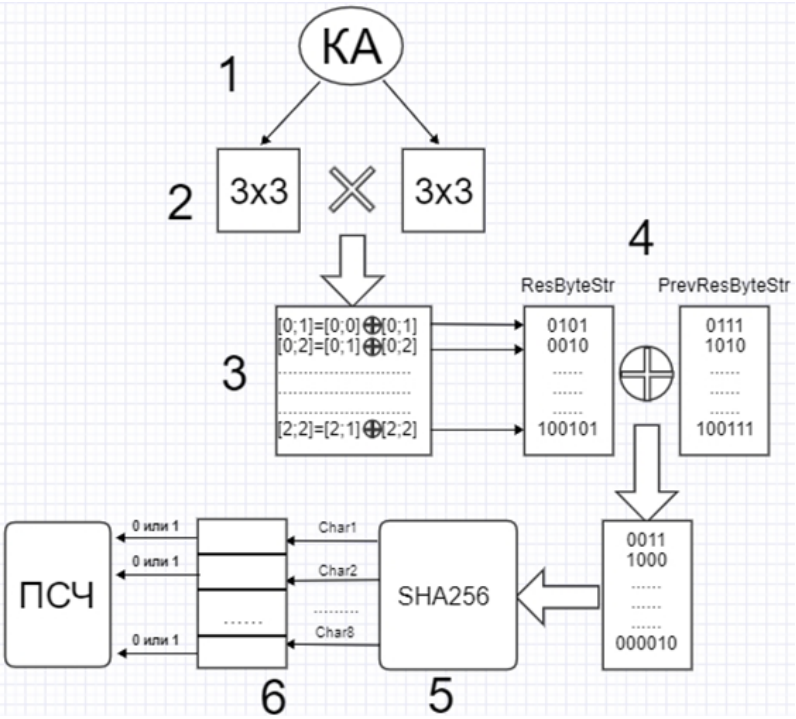

Рис. 4. Поэтапная схема генерации ПСЧ

3. Тестирование генератора ПСП

В качестве инструмента тестирования был выбран пакет статистических тестов NIST STS. На данный момент это одно из самых популярных средств тестирования генераторов ПСП [9–11]. Данный пакет содержит набор тестов, направленных на выявление каких-либо дефектов в последовательности. В таблице 1 приведены список тестов и выявляемые ими дефекты случайности [9].

Для проведения тестирования было сгенерировано 40 000 однобайтовых целых чисел, разбитых на 100 подпоследовательностей длиною в 400 чисел. Показателем качества последовательности является значение P-Value, находящееся в диапазоне от 0 до 1 включительно. Если P-Value принимает значение 0 — последовательность является абсолютно предсказуемой. Если P-Value принимает значение 1 — последовательность случайная. Тест считается пройденным, если P-Value > 0,01. Усреднённые результаты тестирования 100 подпоследовательностей приведены в таблице 2.

В рамках исследования несомненный интерес представляет наглядное сравнение статистических показателей с существующими алгоритмами генерации ПСП. Для сравнения были выбраны 5 генераторов, имеющихся в пакете NIST

Таблица 1. Статистические тесты пакета NIST STS

№	*Название теста*	*Определяемый дефект*
1	Частотный (монобитный тест)	Слишком много нулей либо единиц во всей последовательности. Их количество должно быть примерно одинаковым.
2	Блочный тест на частоту	Слишком много нулей либо единиц внутри m-битных блоков. Их количество должно быть примерно одинаковым.
3	Тест на серийность	Отклонение числа серий из единиц (из нулей) различной длины, в частности, частоты чередования 1 и 0.
4	Тест кумулятивных сумм	Слишком много нулей или единиц в начале последовательности.
5	Спектральный тест на основе дискретного преобразования Фурье	Выявление периодических слагаемых (шаблонов) в двоичной последовательности.
6	Тест на линейную сложность	Сниженная линейная сложность последовательности.
7	Тест на длиннейшую серию единиц в блоке	Отклонение от теоретического закона распределения максимальных длин серий единиц
8	Тест не пересекающихся шаблонов	Непериодические шаблоны встречаются слишком часто.
9	Тест пересекающихся шаблонов	Слишком часто встречаются m-битные последовательности единиц.
10	Тест рангов бинарных матриц	Отклонение значений рангов матрицы, анализ линейной зависимости элементов последовательности.
11	Тест приблизительной энтропии	Неравномерность распределения m-грамм (регулярность свойств генератора последовательностей).
12	Тест на периодичность	Неравномерность распределения m-битных слов.

Таблица 2. Статистические тесты пакета NIST STS

№	*Название теста*	*P-Value*	*Результат*
1	Частотный (монобитный тест)	0,47918666	Тест пройден
2	Блочный тест на частоту	0,47789048	Тест пройден
3	Тест на серийность	0,53582583	Тест пройден
4	Тест кумулятивных сумм	0,48842218	Тест пройден
5	Спектральный тест на основе дискретного преобразования Фурье	0,52557954	Тест пройден
6	Тест на линейную сложность	0,58009578	Тест пройден
7	Тест на длиннейшую серию единиц в блоке	0,53939177	Тест пройден
8	Тест непересекающихся шаблонов	0,53161099	Тест пройден
9	Тест пересекающихся шаблонов	0,49977973	Тест пройден
10	Тест рангов бинарных матриц	0,46442867	Тест пройден
11	Тест приблизительной энтропии	0,50172644	Тест пройден
12	Тест на периодичность	0,53398629	Тест пройден

STS. Тестирование генераторов проводилось с теми же параметрами, что и тестирование генератора ПСП на основе клеточного автомата. Результаты тестирования приведены в таблице 3, где 12 строк — это 12 тестов, порядок и название которых соответствует таблице 1. Численные значения в таблице отражают усреднённые значения P-Value по каждому из тестов.

Как видно из таблицы 3, реализованный эвристическим путём алгоритм генерации ПСП на основе КА полностью оправдывается статистическими показателями и в рамках отдельных тестов демонстрирует лучшие значения среди сравниваемых генераторов. Важно понимать, что сложно реализовать алгоритм, который показывал бы отличные статистические результаты по всем тестам. Поэтому не лишним будет перейти к сравнению средних значений по всем тестам каждого генератора. Средние значения P-Value по 12 тестам каждого из генераторов приведены далее.

1. Линейный конгруэнтный генератор: 0,49059889.
2. Квадратичный конгруэнтный генератор: 0,4927076.
3. Micali-Shcnorr: 0,51080925.
4. Blum-Blum-Shub: 0,48831351.
5. Модулярно-экспоненциальный генератор: 0,50401959
6. Генератор на основе КА: 0,51316036.

Следующим этапом являлось исследование зависимости характеристик ПСП от параметров клеточного автомата и от алгоритма генерации ПСЧ.

Непосредственное влияние на эволюцию клеточного автомата и выходную последовательность оказывают количество состояний и правила перехода. Для краткости изложения введём условное обозначение текущих параметров авто-

Таблица 3. Статистические тесты пакета NIST STS (Г1 — линейный конгруэнтный генератор, Г2 – квадратичный конгруэнтный генератор, Г3 — Micali-Shcnorr, Г4 — Blum-Blum-Shub, Г5 — модулярно экспоненциальный генератор) и Г6 – генератор на основе КА

№	Г1	Г2	Г3	Г4	Г5	**Г6**
1	0,4808706	0,4865253	0,54483113	0,43734769	0,50222298	0,47918666
2	0,48264618	0,42435623	0,48836388	0,41852682	0,48641801	0,47789048
3	0,48647511	0,51587904	0,51144753	0,50576546	0,51370477	0,53582583
4	0,47519589	0,49126063	0,54919581	0,45471316	0,50266348	0,48842218
5	0,47599264	0,49951031	0,47713432	0,46424687	0,49055585	0,52557954
6	0,53060168	0,5259644	0,52680149	0,50991242	0,52988905	0,58009578
7	0,48308109	0,45039169	0,52299557	0,51815044	0,45264045	0,53939177
8	0,53227178	0,53203322	0,53045616	0,53667222	0,53409214	0,53161099
9	0,46629077	0,51013325	0,49721174	0,5094293	0,52428777	0,49977973
10	0,47734816	0,47754565	0,47875372	0,50464686	0,50132254	0,46442867
11	0,46561875	0,50866382	0,50724831	0,50300328	0,46291012	0,50172644
12	0,53079404	0,49022771	0,49527144	0,49734770	0,54752802	0,53398629

мата на примере параметров на рисунке 3. Текущие настройки можно записать следующим образом 1-5/1-3-5-6/10, где 1-5 – количество живых клеток, необходимых для рождения клетки, 1-3-5-6 — количество живых клеток, необходимых для смены i-го состояния на $i+1$-е, 10 — количество состояний. Были проведены следующие изменения параметров.

1. Увеличение количества состояний без смены правила (1-5/1-3-5-6/30).

2. Уменьшение количества состояний без смены правила (1-5/1-3-5-6/5).

3. Смена правила, при котором в автомате появляются неустойчивые, но цикличные структуры (1-2-4-6/0-3-5/10).

4. Уменьшение количества состояний в правиле с неустойчивыми структурами (1-2-4-6/0-3-5/5).

5. Смена правила, при котором в автомате появляются устойчивые и цикличные структуры (2-7/2-3-5-6/20).

Средние значения P-Value по 12-ти тестам по каждой из 5 конфигураций, а также среднее значение P-Value для исходной конфигурации представлены далее.

1. 1-5/1-3-5-6/30: 0,50580696.
2. 1-5/1-3-5-6/5: 0,49698226.
3. 1-2-4-6/0-3-5/10: 0,50058212.
4. 1-2-4-6/0-3-5/5: 0,5039827.
5. 2-7/2-3-5-6/20: 0,50384019.
6. 1-5/1-3-5-6/10: 0,513160363 (исходная конфигурация).

По данным вычислительного эксперимента можно сделать вывод, что никакие из изменений не привели к ощутимым отклонениям ни в лучшую, ни в худшую сторону. А это, в свою очередь, говорит о том, что при текущем алгоритме

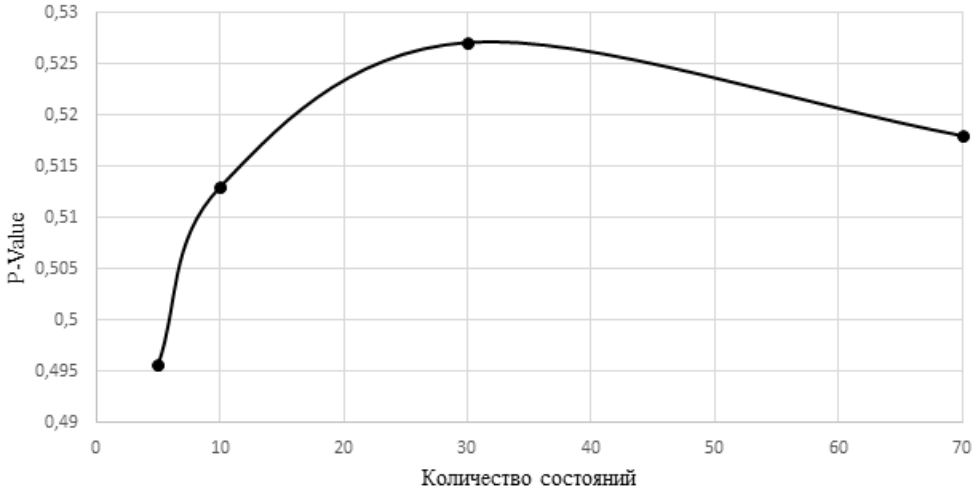

Рис. 5. Зависимость P-Value от количества состояний КА

параметры клеточного автомата не играют существенной роли в формировании выходной последовательности.

Перейдём к исследованию и модификации алгоритма генерации ПСЧ. Первым шагом по упрощению алгоритма стало удаление 5-го и 6-го этапов (рис. 4). Также было реализовано «вбрасывание» 40 случайных состояний в случайные клетки каждые 20 поколений автомата. После вышеупомянутых модификаций было проведено тестирование и сравнение изменённого алгоритма на разных параметрах клеточного автомата.

Средние значения P-Value по 12-ти тестам для каждой конфигурации представлены далее.

1. Без SHA256: 0,51309172.
2. Без SHA256 на 5 состояниях: 0,49571853.
3. Без SHA256 на 30 состояниях: 0,5271106.
4. С SHA256 на 10 состояниях (исходная конфигурация): 0,513160363.
5. Без SHA256 на 70 состояниях: 0,518555851.
6. Без SHA256 2-4-7/1-3-6/70: 0,51142996.
7. Без SHA256 1-2-4-6/0-3-5/30: 0,507571585.

На данном этапе исследования нам удалось убедиться в том, что уменьшение количества состояний клеток негативно сказывается на последовательности, как и увеличение после определённого порога (см. рис. 5).

Заключение

Итогом данной работы является программная реализация генератора ПСП на основе клеточного автомата, а также исследовательский вклад в изучение клеточного автомата как источника программных шумов для генератора ПСП. Текущая версия генератора обладает хорошими статистическими показателями, сравнимыми с известными генераторами ПСП.

Литература

1. Ефремова А.А., Гамова А.Н. Генератор псевдослучайных чисел на основе клеточных автоматов // Компьютерные науки и информационные технологии. Материалы Международной научной конференции, 2016. С. 131–134.
2. Жуков А.Е. Клеточные автоматы в криптографии. Часть 1 // Вопросы кибербезопасности. 2017. № 3(21). С. 70–76.
3. Жуков А.Е. Клеточные автоматы в криптографии. Часть 2 // Вопросы кибербезопасности. 2017. № 4(22). С. 47–66.
4. Ключарёв П.Г. Метод построения криптографических хэш-функций на основе итераций обобщённого клеточного автомата // Вопросы кибербезопасности. 2017. № 1(19). С. 45–50.
5. Мухамеджанов Д.Д, Левина А.Б. Генератор псевдослучайных чисел на основе клеточных автоматов // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, № 5. С. 894–900.
6. Сухинин Б.М. Высокоскоростные генераторы псевдослучайных последовательностей на основе клеточных автоматов // Прикладная дискретная математика. 2010. № 2. С. 34–41.
7. Selvavinayagam G., Umamaheswari K. Performance Enhancement in Image Encryption using Parallel Non Uniform Cellular Automata based PRN Generation // Asian Journal of Research in Social Sciences and Humanities. 2017. Vol. 7, No. 2. P. 1079–1093.
8. Сухинин Б.М. О лавинном эффекте в клеточных автоматах // Объединённый научный журнал. 2010. № 8. С. 41–46.
9. Будько М.Б., Будько М.Ю., Гирик А.В., Грозов В.А. Методы генерации и тестирования случайных последовательностей. СПб : Университет ИТМО, 2019. С. 44.
10. Григорьев А.Ю. Методы тестирования генераторов случайных и псевдослучайных последовательностей // Учёные записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017. № 1. С. 22–28.
11. Миненко А.И. Экспериментальное исследование эффективности тестов для проверки генераторов случайных чисел // Вестник СибГУТИ. 2010. № 4. С. 36–46.

CONSTRUCTION OF A PSEUDO-RANDOM SEQUENCE GENERATOR BASED ON A CELLULAR AUTOMATON

N.F. Bogachenko
Ph.D.(Phys.-Math.), Associate Professor, e-mail: nfbogachenko@mail.ru
I.O. Gorohov
Student, e-mail: vixxman@ya.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The work is devoted to the implementation and testing of a pseudo-random sequence generator based on a cellular automaton model.

Keywords: pseudo-random sequence, cellular automaton.

References

1. Efremova A.A. and Gamova A.N. Generator psevdosluchainykh chisel na osnove kletochnykh avtomatov. Komp'yuternye nauki i informatsionnye tekhnologii, Materialy Mezhdunarodnoi nauchnoi konferentsii, 2016, pp. 131–134. (in Russian)
2. Zhukov A.E. Kletochnye avtomaty v kriptografii. Chast' 1. Voprosy kiberbezopasnosti, 2017, no. 3(21), pp. 70–76. (in Russian)
3. Zhukov A.E. Kletochnye avtomaty v kriptografii. Chast' 2. Voprosy kiberbezopasnosti, 2017, no. 4(22), pp. 47–66.
(in Russian)
4. Klyucharev P.G. Metod postroeniya kriptograficheskikh khesh-funktsii na osnove iteratsii obobshchennogo kletochnogo avtomata. Voprosy kiberbezopasnosti, 2017, no. 1(19), pp. 45–50.
(in Russian)
5. Mukhamedzhanov D.D and Levina A.B. Generator psevdosluchainykh chisel na osnove kletochnykh avtomatov. Nauchno-tekhnicheskii vestnik informatsionnykh tekhnologii, mekhaniki i optiki, 2018, vol. 18, no. 5. pp. 894–900. (in Russian)
6. Sukhinin B.M. Vysokoskorostnye generatory psevdosluchainykh posledovatel'nostei na osnove kletochnykh avtomatov. Prikladnaya diskretnaya matematika, 2010, no. 2, pp. 34–41. (in Russian)
7. Selvavinayagam G. and Umamaheswari K. Performance Enhancement in Image Encryption using Parallel Non Uniform Cellular Automata based PRN Generation. Asian Journal of Research in Social Sciences and Humanities, 2017, vol. 7, no. 2, pp. 1079–1093.
8. Sukhinin B.M. O lavinnom effekte v kletochnykh avtomatakh. Ob"edinennyi nauchnyi zhurnal, 2010, no. 8, pp. 41–46. (in Russian)
9. Bud'ko M.B., Bud'ko M.Yu., Girik A.V., and Grozov V.A. Metody generatsii i testirovaniya sluchainykh posledovatel'nostei. SPb., Universitet ITMO, 2019, pp. 44. (in Russian)
10. Grigor'ev A.Yu. Metody testirovaniya generatorov sluchainykh i psevdosluchainykh posledovatel'nostei. Uchenye zapiski UlGU. Ser. Matematika i informatsionnye tekhnologii, UlGU, Elektron. zhurn., 2017, no. 1, pp. 22–28. (in Russian)
11. Minenko A.I. Eksperimental'noe issledovanie effektivnosti testov dlya proverki generatorov sluchainykh chisel. Vestnik SibGUTI, 2010, no. 4, pp. 36–46. (in Russian)

Дата поступления в редакцию: 01.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 75–102

УДК 004.932.2
DOI 10.24147/2222-8772.2020.4.75-102

ОБЗОР МЕТОДОВ СТЕГАНОГРАФИЧЕСКОГО АНАЛИЗА ИЗОБРАЖЕНИЙ В РАБОТАХ ЗАРУБЕЖНЫХ АВТОРОВ

Д.Э. Вильховский
ассистент кафедры информационной безопасности, e-mail: vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье представлен обзор зарубежных исследований в области стеганографического анализа изображений, направленного на обнаружение стеговставок, выполненных на основе алгоритмов замены наименее значащих битов и дискретного косинусного преобразования. Отмечается, что дальнейшее развитие методологии стегоанализа идёт в двух направлениях: уменьшение трудоёмкости и стоимости вычислений при сохранении высокого уровня чувствительности, что вполне оправдывает себя в случае наличия стеговставок с достаточно большой полезной нагрузкой, т. е. при полном заполнении стегоконтейнера, или повышение эффективности методов распознавания изображений со стеговставками при условии низкого уровня заполнения стегоконтейнера. При этом в последние пять лет доминирующую роль в стеганографическом анализе стали занимать методы, основанные на машинном и глубоком обучении.

Ключевые слова: стегоанализ, стеганографический анализ, LSB-вставка, метод замены наименее значащих битов.

Введение

Если стеганография имеет целью незаметную передачу данных, встроенных в какое-либо мультимедиа так, чтобы сам факт встраивания оставался незамеченным, то стеганографический анализ (стегоанализ) направлен на обнаружение встроенных данных, т. е. факта встраивания. Соответственно, являясь антагонистическими по своей сущности, оба направления находятся в непрерывном развитии. В первом случае речь идёт о разработке новых методов, алгоритмов и схем встраивания, а во втором — о разработке методов, моделей и алгоритмов обнаружения встраивания.

В большинстве случаев разрабатываются универсальные (слепые) методы стегоанализа, призванные эффективно работать при любых алгоритмах и схемах встраивания в условиях слепого применения, т. е. когда алгоритмы и схемы встраивания неизвестны стегоаналитику. Единственным допущением, закладывающимся при разработке универсальных методов, является допущение о методе встраивания, что важно для определения того, в какой области (пространственной или преобразования) осуществляется встраивание.

В данной статье исследуются методы стегоанализа, работающие на обнаружение встраиваний в пространственную область, выполненных путём замены наименее значащих битов.

Статья содержит ряд специфических терминов, пришедших из англоязычных исследований. Для удобства прочтения и понимания представленного материала в таблице 1 приводится перечень основных терминов с расшифровкой их аббревиатуры на английском языке и значения на русском.

Таблица 1. Перечень терминов, используемых в настоящей статье

Термин	Расшифровка на английском языке	Значение на русском языке
ALE	Amplitude of local extrema	Амплитуда локальных экстремумов
ANOVA	ANalysis Of VAriance	Дисперсионный анализ
CNN	Convolutional neural network	Свёрточная нейронная сеть
CSW	Channel similarity weight	Вес подобий цветовых каналов
DCT	Discrete Cosine Transform	Дискретное косинусное преобразование
FAR	False Alarm Rate	Частота ложных тревог
FDR	False Detection Rate	Частота ложных обнаружений
FLD	Fisher Linear Discriminant	Линейный дискриминант Фишера
GLCM	Gray Level Co-occurrence Matrix	Матрица совпадений уровней серого
HCF	Histogram characteristic function	Характеристическая функция гистограммы
HCF-COM	Histogram characteristic function — center of mass	Характеристическая функция гистограммы с использованием центра масс
LSB	Least Significant Bit	Наименьший значимый бит
PDF	Probability Density Function	Функциия плотности вероятности
PoV	Pairs of Values	Пары значений
PSO	Particle Swarm Optimization	Оптимизация роя частиц
PSW	Pixel Similarity Weight	Вес подобий пикселей
QMF	Quadrature Mirror Filter	Квадратурный зеркальный фильтр
RBF	Radial Basis Function	Радиальная базисная функция
RHB	Right Half-Byte	Правый полубайт
RS	Regular or Singular	Регулярный или сингулярный
SC	Simplicial Complex	Симплициальный комплекс
SC Rips	Vietoris-Rips complex	Симплициальный комплекс Виеториса–Рипса
SRM	Spatial Rich Model	Пространственнобогатая модель
SVM	Support Vector Machine	Метод опорных векторов
SW	Similarity Weight	Вес подобий
T	Threshold	Порог (пороговые значения)

Продолжение таблицы 1

Термин	Расшифровка на английском языке	Значение на русском языке
TDA	Topological Data Analysis	Анализ топологических данных
ULBP	Uniform Local Binary Pattern	Однородный локальный двоичный шаблон
WAM	Wavelet Absolute Moments	Абсолютные вейвлет-моменты

1. Обзор ранних исследований в области обнаружения LSB-вставок

В последние годы прошлого столетия как ответ на развитие методов стеганографии появились первые работы в области стеганографического анализа. В течение последующих лет отмечено возрастание интереса к проблемам обнаружения стеганографических вставок, что находит отражение в ежегодном увеличении количества работ данной проблематики.

В таблице 2 представлен перечень наиболее значимых работ, посвящённых стеганографическому анализу и опубликованных в ранний период. Представленные работы можно охарактеризовать как основополагающие, поскольку именно в них были впервые предложены различные методы слепого (универсального) стегоанализа, определившие вектор дальнейших изучений в этой области.

Таблица 2. Методы стеганографического анализа в ранних работах

Авторы	Год издания	Краткое описание предложенного метода
Метод Хи-квадрата		
Westfeld A. et al, [35–37]	1999 – 2002	Использует статистический анализе пар значений (PoV), которыми обмениваются во время встраивания секретных данных. Основан на том, что любые стеганографические методы изменяют частоту пары значений в процессе встраивания сообщения
RS-стегоанализ		
Fridrich J. et al. [12–14]	2000 – 2003	Впервые предложен метод регулярного и сингулярного анализа (RS-стегоанализа). В качестве отличительного признака используются близкие цветовые пары в 24-битных цветных изображениях и классификации пикселей на обычные и особые группы. Частота этих групп определяет длину секретного сообщения в стего-изображениях
Gul G. et al [17]	2010	Основан на линейных зависимостях строк / столбцов изображений в локальных окрестностях с использованием разложения по сингулярным значениям

Продолжение таблицы 2

Авторы	Год издания	Краткое описание предложенного метода
Анализ на основе вейвлет-разложения и статистики		
Farid H. et al [26]	2002	Впервые для построения статистических моделей высокого порядка естественных изображений используются вейвлет-разложения. Для различения нетронутых и искаженных изображений используется линейный дискриминантный анализ Фишера
Lyu S. et al [27]	2004	Учитывает зависимости между цветовыми каналами. Использует моменты остаточного шума более высокого порядка, полученные с использованием предикторов коэффициентов в QMF-разложении изображения из всех трёх цветовых каналов
Анализ на основе гистограмм		
Harmsen J., Pearlman W [18]	2003	Модель, известная как HCF-COM. Построена с использованием модели аддитивного шума. Основана на использовании центра тяжести характеристической функции гистограммы (HCF) с калибровкой путём повторной выборки и суммирования цветовых компонентов
Ker et al. [20–22]	2004 – 2005	Улучшены характеристики обнаружения метода стегоанализа HCF-COM, в модель HCF-COM добавлен механизм калибровки и гистограммы смежности
Zhang J. et al. [44], Cancelli G. et al. [2]	2007 – 2008	Модель, известная как ALE-модель. Основана на вычислении из гистограммы изображений амплитуды локальных экстремумов (ALE). В качестве стегоаналитического признака вычисляется сумма абсолютной разницы в значениях между локальными экстремумами и соседями гистограммы
Методы на основе машинного обучения		
Dumitrescu S. et al [9]	2005	Разработан как для цветных изображений, так и для изображений в градациях серого. Использует статистику более высокого порядка для вывода уравнений обнаружения и определения длины сообщения
Goljan M et al [15]	2006	Использует в качестве признаков 27 абсолютных вейвлет моментов (WAM) остаточного шума, полученного из трёх поддиапазонов более высоких частот в области вейвлета. В качестве классификатора используется линейный дискриминант Фишера (FLD)
Dumitrescu S. et al. [8]	2007	Основан на парах отсчётов из сигналов, возникающих в результате LSB-вставок. Как сообщают авторы, является точным, даже при условии малой длины сообщения

Продолжение таблицы 2

Авторы	Год издания	Краткое описание предложенного метода
Pevny T. et al [29]	2010	Для моделирования взаимосвязи между различиями соседних пикселей в восьми направлениях используются марковские процессы первого и второго порядка (с 686 элементами). В качестве классификатора используется метод опорных векторов (SVM)
Пространственнобогатая модель (SRM-модель)		
Fridrich J. et al [19]	2012	Многомодельная комбинированная функция, которая использует линейные и нелинейные вычисления зависимостей между соседними пикселями для количественной оценки шума изображений и матрицу совместной встречаемости высокого порядка в качестве основных характеристик

2. Обзор некоторых методов стеганографического анализа, предложенных в период 2014–2020 гг.

2.1. Ансамблевый SW-стегоанализ с применением машинного обучения

В работах [3, 4] описан низкоразмерный метод ансамблевого стегоанализа LSB-замены изображения с диапазоном встраивания до 0,25 бит на пиксель путём вычисления весов подобий (далее – ансамблевый SW-стегоанализ).

Общая характеристика метода

Метод основан на цветовой корреляции между пикселями и цветовыми каналами трёх различных классах в соседних зонах и гипотезе, что пиксели или каналы одинаковой интенсивности в каждой соседней зоне по-разному влияют на окончательное значение весов их подобий.

Сущность, характеристики и примеры классов пикселей представлены в таблице 3.

Таблица 3. Сущность, характеристики и область расположения классов пикселей

Класс пикселей	Характеристика	Область расположения
Плоский	Имеют самый высокий уровень цветовой корреляции	Область со сплошным цветом

Класс пикселей	Характеристика	Область расположения
Гладкий	Средний уровень цветовой корреляции	Цвет пикселей изменяется постепенно в более широком пространстве
Резкий	Самая низкая цветовая корреляция	Цвет пикселей меняется постоянно и резко

SW-анализ

В качестве аналитических параметров вычисляются веса подобий пикселей (PSW) и цветовых каналов (CSW), создаются наборы данных PSW и CSW, содержащих результаты анализа для каждого пикселя в трёх соседних зонах. Таким образом, для последующего обучения и классификации создаются шесть эталонных профилей со статистическими характеристиками изображений, включающие обнаруженные классы пикселей и степени принадлежности всех пикселей изображения.

В качестве эффективной границы анализа для PSW и CSW экспериментальным и оценочным способами определена третья соседняя зона.

Классификатор

В качестве классификатора используется метод опорных векторов с применением трапециевидной нечёткой функции принадлежности.

Разработанное ядро (SVM-ядро) поддерживает множественное членство и определяет степень членства для каждой согласованной группы данных. Структура разработанного SVM-ядра основывается на таких статистических функциях, как гауссовое (нормальное) распределение, правило трёх сигм и стандартное отклонение от среднего, что позволяет устранять естественный шум данных.

Принятие окончательного решения осуществляется в соответствии с иерархическими решениями, принятыми в подкомпонентах PSW и CSW, а также ансамблевой интерпретации.

Оценка эффективности метода

Для оценки эффективности методов стегоанализа использовались такие метрики, как процент истинно положительных сигналов тревоги от общего количества проанализированных экземпляров (основной критерий) и процент правильно обнаруженных чистых (без стего-вставок) изображений. Данные об эффективности метода представлены в таблице 4.

Таблица 4. Чувствительность PSW, CSW и ансамблевого SW методов, %

	PSW	CSW	Ансамблевый SW
Чистое изображение			
Зона 1	0	0	0
Зона 2	81,315	8,968	8,641

	PSW	CSW	Ансамблевый SW
Зона 3	67,115	91,928	66,8161
Изображение со стеговставкой, коэффициент встраивания 0,125			
Зона 1	100	68,983	100
Зона 2	56,325	68,983	100
Зона 3	74,887	64,573	86,7713
Изображение со стеговставкой, коэффициент встраивания 0,25			
Зона 1	68,983	68,983	100
Зона 2	100	56,875	100
Зона 3	98,056	74,1405	99,626

PSW более эффективен при более высоком уровне заполнения стегоконтейнера, в то время как CSW более эффективен при более низких соотношениях. Таким образом, делается вывод, что для достижения наилучших общих результатов необходимо использовать комбинацию методов интерпретации PSW и CSW.

Согласно значениям PSW (67,115 %) и SW ансамбля (66,8161 %) недостаточно хороши для надежного обнаружения изображения обложки. Следовательно, авторы отмечают, что метод рассчитан на CSW из-за обеспечения надёжной работы с 91,928 % достигнутого успеха.

Данный метод стегоанализа обеспечивает чувствительность 86,77 % при коэффициенте внедрения 0,125 бит на пиксель. При 0,25 бит на пиксель эта чувствительность выросла до 99,626 %, что является логичным следствием большего уровня заполнения стегоконтейнера.

2.2. Стегоанализ на основе статистики текстур изображения

В работе [1] представлен метод слепого стегоанализа с новым набор функций, включающим матрицу совпадений уровней серого (GLCM) и другую статистику текстур изображения. Для экспериментальной работы был выбран формат одноканального изображения в градациях серого для исходных изображений.

Общая характеристика метода

Фокусное внимание предлагаемого метода сосредоточено на свойствах текстуры правого полубайта (RHB) 8-битного канала изображения в градациях серого, представляющего собой область наибольшего встраивания при любом алгоритме встраивания.

Встраивание осуществлялось с использованием схем 2LSB (замена двух бит LSB в байтах изображения) и 4LSB (замена четырёх бит LSB в байтах изображения). При 4LSB-схеме уровень заполнения стегоконтейнера составил около 50 %. При 2LSB-схеме заполнение стегоконтейнера составило 25 %.

Исследуемые признаки

Для анализа используются 22 элемента признаков, для каждого из которых определяется соответствующий вектор признаков как для чистого изображения, так и для стего.

Основными компонентами набора функций являются матрица совпадений уровней серого (GLCM), энтропия правых полубайтов, корреляция между левым и правым полубайтами, коэффициент вариации правых полубайтов и абсолютная разница между последовательными правыми полубайтами, а также дополнительные статистические показатели, которые призваны способствовать различению стего и чистых изображений. В таблице 5 приведён список предлагаемых элементов набора функций.

Таблица 5. Элементы набора характеристик

Характеристика	Описание	Примечание
CC-LR	Коэффициент корреляции между LHB и RHB	Является показателем изменения взимомосвязи между двумя половинами после вложения в правый полубайт
CVR	Коэффициент вариации правых полубайтов	Рассчитывается как отношение стандартного отклонения к среднему, вычисляется для правой половины вертикального среза изображения
GLCM-B	Контраст, корреляция, однородность и энергия полных байтов	Рассчитываются для всего изображения, т. е. для столбца полных байтов
GLCM-R	Контрастность, корреляция, однородность и энергия, RHB	Рассчитываются для правой половины вертикального среза изображения, который состоит из столбца правых полубайтов
GLCM-3	Контрастность, корреляция, однородность и энергия 4LSB	Рассчитываются для вертикальных срезов 3LSB изображения
GLCM-2	Контрастность, корреляция, однородность и энергия, 2LSB	Рассчитываются для вертикальных срезов 2LSB изображения
Энтропия-R	Энтропия RHB	Вычисляется для правой половины вертикального среза изображения

Продолжение таблицы 5

Характеристика	Описание	Примечание
Diff-R	Среднее значение абсолютной разницы между последовательными RHB	Фокусируется на влиянии изменений в правой половине изображения в результате встраивания

Классификатор

В качестве классификатора используется метод опорных векторов (SVM).

Оценка эффективности метода

Результаты классификации чистых изображений и изображений с применением 2LSB и 4LSB стеганографических схем представлены в таблице 6.

Таблица 6. Результаты классификации изображений с 2LSB и 4LSB, %

Оценочные показатели	2LSB	4LSB
Истинно положительный (TP)	99,22	100
Ложно-негативный (FN)	0,78	0
Истинно негативный (TN)	98,82	98,82
Ложно-позитивный (FP)	1,18	1,18
Точность обнаружения	99,02	99,41

Данные свидетельствуют о высокой точности обнаружения чистого и стегоизображения при применении метода. В обеих схемах встраивания коэффициент обнаружения истинно положительных значений немного выше, чем истинно негативный, это указывает на то, что модель лучше обнаруживает стегоизображения, чем чистые изображения.

4LSB-стегоконтейнер имеет немного более высокую точность обнаружения по сравнению с точностью обнаружения 2LSB-стегоконтейнера: 99,41 % при 4LSB-вставке против 99,02 % при 4LSB-вставке. Этот факт объясняется тем, что стегосхема 4LSB содержит вдвое больше встроенных данных. При этом чувствительность метода к обнаружению истинно негативных значений одинакова для обеих схем встраивания.

2.3. Стегоанализ изображений JPEG на основе машинного обучения

В работах [24, 31] представлена методология стегоанализа для изображений формата JPEG при 10 % заполнении стегоконтейнера с 10-кратной перекрёстной проверкой.

Общая характеристика метода

Метод применим для четырёх различных типа стеганографии, включая метод замены наименее значащих бит и использование дискретного косинусного преобразования (DCT). Рассматриваются четыре различных вида выборки: линейная, случайная, стратифицированная и автоматическая.

В работе также используется концепция калибровки, которая помогает получить оценку изображения обложки из изображения стего.

Исследуемые признаки

Анализ проводится с использованием признаков первого, второго порядков, признаков расширенного DCT и признаков Маркова. Общее количество признаков составляет 274, включая 165 признаков первого порядка, 28 признаков второго порядка и 81 признак расширенного DCT и признаков Маркова. Подробная информация об извлечённых признаках приведена в таблице 7.

Для всех исследованных ядер и образцов вычисляются векторы производительности с использованием таких метрик производительности, как надёжность, ошибка классификации и каппа.

Таблица 7. Таблица извлечённых признаков

Тип признака	Метод извлечения	Количество признаков
Признаки первого порядка	Двойная гистограмма	99
	Глобальная гистограмма	11
	Индивидуальная гистограмма	55
Признаки второго порядка	Совместная встречаемость	25
	Вариация	1
	Блочность	2
Признаки Маркова		81
	Общее количество	**274**

Классификатор

В качестве классификатора изначально применяется метод опорных векторов (SVM). В дальнейшем используется классификатор, в котором для оптимизации мощности отдельных методов и преодоления их недостатков объединены метод опорных векторов (SVM) и алгоритм оптимизации роя частиц (PSO) — SVM-PSO-классификатор.

В качестве ядер при классификации используются ядро Епанечникова, точечное / линейное ядро DOT, мультиквадратичное, радиальное, ядро ANOVA и полиномиальное ядро.

Оценка эффективности метода

Результаты классификации с использованием SVM- и SVM-PSO-классификаторов представлены в таблицах 8 и 9.

Таблица 8. Результаты классификации с использованием SVM-классификатора

Ядро	Линейная выборка	Случайная выборка	Стратифицированная выборка	Автоматическая выборка
Dot	8,49	43,27	44,52	44,52
Радиальное	6,12	13,37	11,5	11,5
Полиномиальное	9,11	42,64	43,21	43,21
Мультиквадратичное	10	48,12	49,94	49,94
Епанечникова	6,88	21,32	19,54	19,54
ANOVA	6,58	29,96	30,53	30,53

Таблица 9. Результаты классификации с использованием SVM-PSO-классификатора

Ядро	Линейная выборка	Случайная выборка	Стратифицированная выборка	Автоматическая выборка
Dot	25,54	48,96	49,94	49,94
Радиальное	20,64	26,68	25,22	25,22
Полиномиальное	48,87	49,55	50,36	50,36
Мультиквадратичное	71,5	50,92	51,07	51,07
Епанечникова	11,25	19,18	20,13	20,13
ANOVA	11,4	44,73	42,76	42,76

На основании представленных данных можно сделать вывод, что более низкие результаты сопоставления LSB были получены для линейной выборки с существенным повышением эффективности для остальных типах выборки.

При этом стратифицированная выборка даёт лучшие показатели по сравнению со случайной выборкой практически по всех ядрам, хотя различие не слишком существенное. Однако для ядер Епанечникова и радиального ядра наблюдается снижение результативности. Кроме того, показатели для стратифицированной и автоматической выборок являются идентичными для всех ядер.

Также отмечается, что радиальное ядро показало низкую результативность при всех типах выборок и, таким образом, не подходит для замены LSB. Мультиквадратичное ядро обеспечивает лучшую производительность, хорошие результаты были достигнуты также с полиномиальным и точечным ядрами.

Эффективность метода значительно повышается при использовании SVM-PSO-классификатора для всех ядер и выборок. При этом, если верить представленным данным в линейной выборке, наблюдается увеличение результативности в 5 и 7 раз при использовании полиномиального и мультиквадратичного ядер соответственно.

2.4. Компактный метод с применением машинного обучения

В работе [19] предложен компактный метод стегоанализа изображений с применением машинного обучения для обнаружения изображений с LSB-вставками методом сопоставления для изображений в оттенках серого.

Общая характеристика метода

Метод является низкоразмерным (компактным) и использует малое количество характеристик, позволяющих, тем не менее, эффективно различать чистые изображения и изображения с встроенным сообщением.

Исследуются четыре различных уровня заполнения стегоконтейнера — 100 %, 75 %, 50 % и 25 %.

Компактность схемы обеспечивает низкую компьютерную сложность как на этапе обучения, так и на этапе тестирования.

Исследуемые признаки

Анализ статистического артефакта, возникающего в результате встраивания, осуществляется с использованием 12 характеристик на основе функции плотности вероятности (PDF) разницы соседних пикселей и матрицы совпадения изображений, которые могут отличать стегоизображения от естественных изображений. Извлекаемые характеристики представлены в таблице 10.

Оценка эффективности метода

Таблица 10. Извлекаемые характеристики

Тип	Количество	Состав
Характеристики, связанные с параметром формы PDF и разницы значений соседних пикселей при 4 и 8 смежности	2	1. Соотношение параметра формы PDF разности соседних пикселей при 4-связной смежности между входным изображением и стегоизображением 2. Отношение параметра формы PDF к разности соседних пикселей при 8-связной смежности между входным изображением и стегоизображением

Продолжение таблицы 10

Тип	Количество	Состав
Характеристики, полученные из матрицы совместной встречаемости	4	3. Отношение суммы главной диагонали D 0 матрицы совместной встречаемости между входным изображением и стегоизображением. 4. Отношение суммы диагонали D 1 матрицы совместной встречаемости между входным изображением и стегоизображением 5. Отношение суммы диагонали D 2 матрицы совместной встречаемости между входным изображением и стегоизображением 6. Отношение суммы диагонали D 3 матрицы совместной встречаемости между входным изображением и стегоизображением
Характеристики, связанные с HCF-COM разностной матрицы смежности (4 и 8 смежностей)	2	7. Соотношение COM-HCF значений разности соседних пикселей (DCOM-HCF) при 4-связной смежности между входным изображением и стегоизображением 8. Соотношение COM-HCF значений разности соседних пикселей (DCOM-HCF) при 8-связной смежности между входным изображением и стегоизображением
Характеристики, относящиеся к центральной части PDF	4	9. Соотношение наклона центральной части PDF при 4-х связной смежности между входным изображением и стегоизображением 10. Соотношение наклона центральной части PDF при 8-связной смежности между входным изображением и стегоизображением 11. Соотношение наклона центральной части PDF при 4-х связной смежности между входным изображением и стегоизображением, созданым по схеме 2LSB 12. Соотношение наклона центральной части PDF при 8-связной смежности между входным изображением и стегоизображением, созданым по схеме 2LSB

Классификатор

В качестве классификатора используется метод опорных векторов с ядром радиальной базисной функции (RBF). Коэффициент регуляризации скорректирован методом перекрёстной проверки.

Эффективность метода

Эффективность на предмет обнаружения вставок была протестирована на двух различных базах данных изображений. Результаты тестирования представлены в таблице 11.

Таблица 11. Эффективность обнаружения для двух наборов данных

Уровень встраивания, %	База данных изображений BOWS-2	База данных изображений UCID
100	96,26	90,96
75	92,50	86,39
50	85,51	78,36
25	74,53	63,62

Метод показывает высокую результативность. Ожидаемо, что эффективность обнаружения снижается по мере снижения уровня встраивания — до 96,26 % для максимального заполнения стегоконтейнера и до 74,53 % для 25 % уровня заполнения стегоконтейнера.

При этом предложенный метод показывает различия в результативности в зависимости от используемой базы данных – разница в эффективности обнаружения составляет от 6 почти до 11 % с возрастанием по мере снижения объёма заполняемости стегоконтейнера.

Также в работе произведено сравнение с другими методами стегоанализа. Результаты эксперимента приведены в таблице 12.

Таблица 12. Эффективность обнаружения для двух наборов данных

Уровень встраивания, %	Метод Хи-квадрата			Метод Хи-квадрата		
	WAM	DHCF-COMs # 1	DHCF-COMs # 2	WAM	DHCF-COMs # 1	DHCF-COMs # 2
100	91,50	94,51	88,73	81,72	85,48	76,31
75	88,27	92,75	77,25	4,63	83,28	66,42
50	83,24	84,47	63,78	61,57	74,63	63,44
25	72,21	70,23	56,61	43,44	56,56	56,52

Сравнивая показатели эффективности предложенного метода с другими методами, авторы делают вывод, что предложенная схема стегоанализа показывает лучшие результаты, особенно для набора изображений UCID.

2.5. Стегоанализ с использованием сигнатуры близкой цветовой пары

В работе [28] предложен метод стегоанализа для несжатого формата цветного изображения высокой плотности с использованием сигнатуры близкой цветовой пары.

Общая характеристика метода

В качестве сигнатуры используется соотношение близких цветовых пар и уникальных цветов. Метод основан на следующих подтверждённых гипотезах.

1. Для чистого несжатого изображения значение соотношения близких цветовых пар и уникальных цветов больше по сравнению с изображением, в которое встроено сообщение.
2. Если изображение не имеет встроенного сообщения, то после встраивания соотношение близких цветовых пар и уникальных цветов значительно уменьшается.
3. Если изображение уже является изображением со встроенным сообщением, то последующее встраивание не приведёт к значительному изменению этого соотношения. Данные утверждения протестированы с использованием 20 % стеговставки.

Эффективность метода

Эффективность измеряется через частоту ложных тревог (FAR) и частоту ложных обнаружений (FDR). Показано, что при выборе порога с фиксированным значением классификация будет вполне удовлетворительной по некоторым типам изображений (зелень, люди, объекты, водные объекты, земля и здания), но имеет высокую вероятность ошибочного обнаружения для классов других типов изображений (лица, небо и облака, животные).

Использование переменного порога, основанного на статистике изображений, повышает эффективность метода. Эффективность метода при использовании переменного порога представлена в таблице 13.

Таблица 13. Экспериментальные результаты, показывающие улучшение FAR и FDR в случае переменного порогового значения, %

Класс изображений	Частота ложных обнаружений (FDR)		Частота ложных тревог (FAR)	
	Постоянный порог	Переменный порог	Постоянный порог	Переменный порог
Лицо	88,88	0	5,56	5,56
Небо и облака	38,46	0	0	0
Животные	0	4,65	48,83	16,27

Так, согласно представленным результатам, применение переменного порога позволяет добиться отсутствия ложных обнаружений по таким классам, как «лицо» и «небо и облака» (что, по сути, даёт отсыл к такой цветовой гамме, как оттенки бежевого и синего), а также снижает частоту ложных тревог в классе «животные» в три раза, что также является существенным повышением точности предложенной модели. В тоже время следует отметить, что постоянный порог даёт несколько лучшие результаты по частоте ложных обнаружений

по сравнению с переменным порогом значений.

Отмечается, что алгоритм будет намного более надёжным, если порог автоматически выбран на основе статистики 1-го и 2-го порядка, включая плотность цвета и корреляцию пар пикселей.

2.6. Расширенная SRM-модель для стегоанализа цветных изображений

В работе [16] предлагается расширение SRM-модели для стегоанализа цветных изображений.

Общая характеристика метода

Модель имеет размерность 18157 и состоит из двух компонентов

1. Классическая SRM-модель с шагом квантования q = 1 (SRMQ1) с размерностью 12753 (4D-совпадения с порогом T = 2).
2. Дополнительные характеристики общей размерностью 4704 (совместные 3D-совпадения с порогом T = 3 и квантованием q = 1).

Встраиваемая полезная нагрузка – от 0,05 до 0,5 бит на пиксель канала.

Входные изображения подвергаются предварительной обработке, в результате чего авторы исследования получили три базы данных изображений для последующего обучения и тестирования:

1) изображения с изменением размера – BOSSbaseRes,
2) изображения с применением алгоритма демозаинга Patterned Pixel Grouping (PPG) — BOSSbasePPG,
3) изображения с применением алгоритма демозаинга Adaptive Homogenity-Directed (AHD) – BOSSbaseAHD.

Исследуемые характеристики (дополнительные)

В качестве характеристик, при помощи которых предлагается расширить классическую пространственнобогатую модель, используется набор трёхмерных сочетаний остатков, вычисленных по всем трём цветовым каналам.

Эти характеристики формируются из остаточных значений шума и вычисляются с использованием двух типов локальных предикторов пикселей:

1) линейных, вычисляемых путём свёртки изображения с помощью высокочастотного фильтра с инвариантным к сдвигу ядром (остатки «спама», размерность 700);
2) нелинейных, получаемых из остатков максимума / минимума выходов от нескольких линейных фильтров, разделённых на пять классов в зависимости от структуры фильтра: фильтры, использующие разности первого, второго и третьего порядка, граничные ядра и квадратичные ядра.

Классификатор

Используются бинарные классификаторы, реализованные с использованием ансамбля FLD с настройками по умолчанию, минимизирующего общую вероятность ошибки классификации.

Эффективность метода

Эффективность оценивается через среднюю ошибку обнаружения как функцию полезной нагрузки. Результаты проведенных экспериментов графически представлены на рисунках 1-3.

Общей закономерностью является снижение ошибок обнаружения по мере увеличения встраиваемой нагрузки. Также отмечается, что исходная модель SRMQ1 выдаёт наибольшую погрешность в базах данных с применением демозаинга, тогда как модель SCRMQ1, адаптированная для анализа цветных изображений с целью обнаружения встраиваемых сообщений, показывает существенно лучшие результаты для всех трёх баз изображений. Так, ошибки обнаружения моделей SRMQ1, CRMQ1 и SCRMQ1 составляют 0,0225, 0,0117 и 0,0080 соответственно.

Также отмечается, что подмодели с меньшими ядрами обычно обнаруживают лучше, чем большие ядра. Сделан вывод, что способ предварительной обработки изображения не оказывает большого влияния на эффективность модели.

2.7. Стегоанализ на основе сочетания пространственной и вейвлет-фильтрации

В работе [40] предлагается метод стегоатаки, основанный на совместном использовании пространственного и вейвлет-фильтров.

Общая характеристика метода

Метод использует дискриминантные функции на основе остатков, полученных с помощью пространственной (пространственный остаток) и вейвлет-фильтрации (вейвлет-остаток), а затем объединяет результаты двух дискриминантных функций для определения местоположения изменённых пикселей.

Модель позволяет определить местоположение модифицированных пикселей при 10 % уровне заполнения стегоконтейнера.

Алгоритм слияния остатков

Пространственный и вейвлет-остатки объединяются методом голосования.

На вход подаётся стегоизображение и вычисляется коэффициент модификации α , обозначающий соотношение изменённых пикселей и порог дискриминации.

Промежуточные действия включают высокочастотную фильтрацию изображения с использованием среднего значения по 4-м соседям для получения пространственного остатка, нахождение пространственных остаточных квадратов, вычисление одноуровневого вейвлет-разложения изображения с помощью 8-ступенчатого фильтра Добеши, обратное вейвлет-преобразование для получения окончательного остаточного изображения.

На выходе получается оценочная матрица модификации. Когда пиксель распознаётся как модифицированный пиксель, элементу присваивается значение 1; в противном случае ему присваивается значение 0.

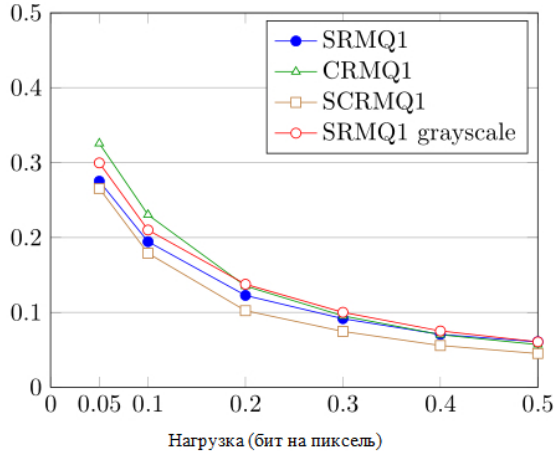

Рис. 1. Ошибка обнаружения как функция полезной нагрузки для трёх баз данных с использованием базы изображений BOSSbaseRes

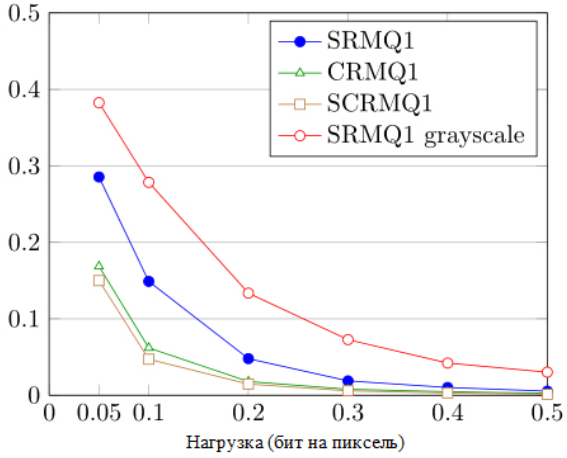

Рис. 2. Ошибка обнаружения как функция полезной нагрузки для трёх баз данных с использованием базы изображений BOSSbasePPG

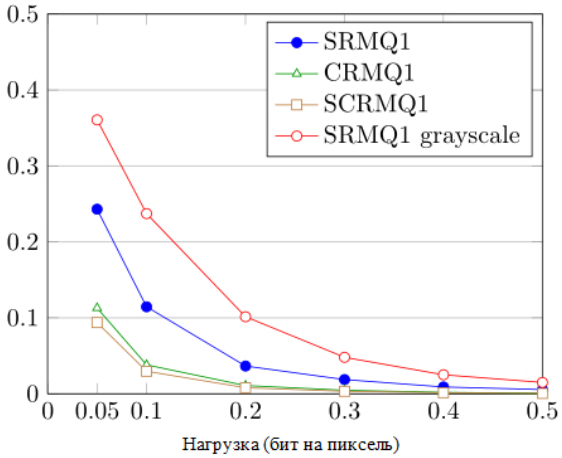

Рис. 3. Ошибка обнаружения как функция полезной нагрузки для трёх баз данных с использованием базы изображений BOSSbaseAHD

Эффективность метода

Эффективность алгоритма определяется через разницу между показателем истинно положительных и ложноположительных результатов. На основе тестирования 1000 изображений показывается значительно большая эффективность предложенного алгоритма по сравнению с использованием только пространственных или вейвлет-остатков.

2.8. Стегоанализ с применением топологических данных

В работе [30] описан метод стеганографческого анализа, основанного на концепции анализа топологических данных (TDA), связанных с определёнными характеристиками изображения.

Общая характеристика метода

Доказано, что разделение битов в соответствии с их образцами двоичного кода позволяет выявить присутствие определённых текстур путём построения симплициальных комплексов и сравнения количества связанных компонентов в последовательности возрастающих пороговых значений расстояния.

Метод разработан и апробирован для изображений в градациях серого. Входное изображение предварительно подвергается обработке с использованием mod16 для уменьшения диапазона значений пикселей от (0, ..., 255) до (0, ..., 15).

Исследуемая полезная нагрузка составляет 100 %.

Исследуемые характеристики

В качестве характеристик используются группы однородных локальных двоичных шаблонов (ULBP) (кодов ULBP) с дальнейшим построением возрастающей последовательности SC Rips, нулевые симплексы которой являются пикселями ориентиров ULBP из конечной возрастающей последовательности пороговых значений расстояний.

Отмечается, что для изображения в градациях серого существует 58 однородных LBP (ULBP) кодов. Исключив только нулевые или единичные шаблоны (00000000) и (11111111), оставшиеся 56 ULBP-кодов авторы разделяют на 7 групп, извлекая их в качестве симплексов, являющихся строительными блоками Rips SC.

Модель использует фиксированный набор пороговых значений расстояния $T\ i = 0, 4, 5, 7, 10, 15$, т. е. для каждого входного изображения будет вычислено 6 восьмимерных векторов признаков. Векторы извлекаются как для случая, когда коды ULBP содержат 6 единиц значений пикселей, так и для случая, когда коды ULBP содержат 3 единицы значений пикселей.

Эффективность метода

В таблицах 14 и 15 показаны средняя точность обнаружения стегоизображения для кодов ULBP с шестью и тремя единицами значений пикселей.

Таблица 14. Результаты классификации для кодов ULBP с шестью единицами значений пикселя, %

	T = 4	T = 5	T = 7	T = 10	T = 15
30 % Обучение	86,699	84,836	78,321	74,186	67,157
50 % Обучение	90,048	87,026	78,734	75,152	68,014
70 % Обучение	90,98	87,853	78,777	75,763	68,443
Обучение с исключением только одного изображения	92,7	88,7	79,1	75,8	68,132

Таблица 15. Результаты классификации для кодов ULBP с тремя единицами значений пикселя, %

	T = 4	T = 5	T = 7	T = 10	T = 15
30 % Обучение	86,449	84,46	87,234	78,306	66,573
50 % Обучение	89,382	84,882	88,738	79,578	68,338
70 % Обучение	90,43	85,213	89,54	80,133	69,24
Обучение с исключением только одного изображения	91,4	85,5	90,6	79,6	69,7

Представленные данные позволяют сделать вывод, что последовательность постоянных гомологических инвариантов может определять различия для целей стегоанализа с точностью более 90 %.

Метод позволяет обнаруживать стегоизображения с высокой точностью от первых пороговых значений, а затем постепенно уменьшать полученные результаты точности по мере его возрастания, что связано с увеличением размеров симплициальных комплексов.

Использование ULBP кода с 3-мя единицами значений пикселя приведёт к несколько более высокой точности классификации, по сравнению с ULBP кодом с 6-ю единицами значений пикселя.

3. Новейшие тенденции в стеганографическом анализе

Новейшей методологической основой стеганографического анализа стало использование технологии глубокого изучения. Так, в последние пять лет появилось большое количество работ, посвящённых возможностям использования сверточных нейронных сетей для обнаружения стеганографических вставок. Наиболее интересные работы в этой области приведены в таблице 16.

Таблица 16. Работы по изучению вопросов применения глубокого обучения и сверточных нейронных сетей в стегоанализе

Авторы	Год издания	Название работы
Xu G. et al [39]	2016	Ансамблевые CNN для целей стегоанализа: эмпирическое исследование
Xu G. et al [38]	2016	Структурный дизайн свёрточных нейронных сетей для стегоанализа
Ye J. et al [41]	2017	Иерархические представления глубокого обучения для стегоанализа изображений
Sharifzadeh M. et al [32]	2017	Применение свёрточного нейросетевого стегоанализа в стеганографии
Chen M. et al [6]	2018	Регрессоры глубокого обучения для количественного стегоанализа
Li B. et al [25]	2018	ReST-net: разнообразные модули активации и CNN на основе параллельных подсетей для стегоанализа пространственных изображений
Yedroudj M. et al [42]	2018	Yedroudj-net: эффективная CNN для пространственного стегоанализа
Zhang R. et al [45]	2018	Эффективное изучение функций и стегоанализ многоразмерных изображений на основе CNN

Продолжение таблицы 16

Авторы	Год издания	Название работы
Zhang T. et al [46]	2019	Новый метод стегоанализа изображений JPEG, сочетающий в себе особенности SRM-модели и свёрточных нейронных сетей
Cogranne R. et al [7]	2019	ALASKA-вызов в стегоанализе: первый шаг к стегоанализу
Kim J. et al [26]	2020	Стегоанализ изображений на основе CNN с использованием дополнительных данных
Wang Z. et al [34]	2020	Совместное многодоменное изучение функций для стегоанализа изображений на основе CNN
Eslam M. et al [10]	2020	Улучшение стегоанализа изображений на основе CNN на графических процессорах
Chaumont M. [5]	2020	Глубокое обучение в стеганографии и стегоанализе
You W. et al [43]	2020	Сиамские свёрточные нейронные сети для стегоанализа изображений
Soto R.T. et al [33]	2020	Стеганографический анализ цифровых медиа

Заключение

Следует отметить, что несмотря на многообразие имеющихся моделей стеганографического анализа, каждая имеет ряд ограничений, что вызывает необходимость разработки других, более совершенных (а значит, более эффективных) моделей.

Кроме того, появление новых методов и алгоритмов стеганографии является стимулом для дальнейшего развития. При этом наблюдается тенденция увеличения количества исследований, посвящённых вопросам стегоанализа, и существенный сдвиг методов стегоанализа на методы, связанные с применением свёрточных нейронных сетей. Предположительно, подобный сдвиг области исследований обусловлен развитием алгоритмов глубокого обучения и усовершенствования методов стеганографии и возрастанием их устойчивости к стегоатакам. В то же время предполагается сохранение актуальности любых других методов, направленных на обнаружение стеганографических вставок,

выполненных при помощи замены наименее значащих бит, что обусловлено простотой и, в связи с этим, широкой популярностью LSB-метода.

Литература

1. Al-Jarrah M., Al-Taei Z., Aboarqoub A. Steganalysis using LSB-focused statistical features // Proceedings of ICFNDS'17, Cambridge, United Kingdom, 2017, July 19-20, 5 pages. DOI: 10.1145/3102304.3109814.
2. Cancelli G., Doerr G., Cox I.J., Barni M. Detection of 1 LSB Steganography based on the Amplitude of Histogram Local Extrema // Int. Conf. Image Processing. 2008. P. 1288–1291.
3. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun. 2019. V. 70. P. 233–245.
4. Chaeikar. S.S., Ahmadi A. SW: A blind LSBR image steganalysis technique // Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018. P. 14–18.
5. Chaumont M. Deep learning in steganography and steganalysis // Digital Media Steganography, Academic Press. 2020. P. 321–349.
6. Chen M, Boroumand M, Fridrich J. Deep learning regressors for quantitative steganalysis // Electron Imaging 2018. V. 7. P. 160—161.
7. Cogranne R., Giboulot Q., Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis // Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019. P. 125–137.
8. Dumitrescu S., et al. Detection of lsb steganography via sample pair analysis // IEEE Trans. Signal Process. 2003. V. 51, No. 7. P. 1995-–2007.
9. Dumitrescu S., Wu X. A new framework of lsb steganalysis of digital media // IEEE Trans. Signal Process. 2005. V. 53. P. 3936-–3947.
10. Eslam M., Elshafey M.A., Mohamed M. Fouad. Enhancing CNN-based Image Steganalysis on GPUs // Journal of Information Hiding and Multimedia Signal Processing. 2020. V. 11, No. 3. P. 138–150.
11. Fridrich J, Kodovsky J. Rich models for steganalysis of digital images // IEEE Transactions on Information Forensics and Security. 2012. V. 7. P. 868–882.
12. Fridrich J., et al., Steganalysis of LSB encoding in colour image // Proc. 2000 IEEE International Conference on Multimedia and Expo, New York, USA. 2000 V. 3, P. 1279–1282.
13. Fridrich J., Goljan M., Du R. Reliable detection of LSB steganography in color and grayscale images // Proceedings of the 2001 workshop on Multimedia and security: new challenges, ACM. 2001. P. 27–30.
14. Fridrich J., Goljan M., Soukal D. Higher-order statistical steganalysis of palette images // Proc. SPIE, EI. 2003. V. 5020. P. 178–190.
15. Goljan M., Fridrich J., Holotyak T. New Blind Steganalysis and its Implications // SPIE Security, Steganography and watermarking of Multimedia Contents. 2006. V. 6072. P. 1–13.
16. Goljan, M., Fridrich, J., Cogranne, R. Rich model for steganalysis of color images // Information Forensics and Security (WIFS), 2014 IEEE International Workshop. 2014. P. 185–190.

17. Gul G., Kurugollu F., SVD-based universal spatial domain image steganalysis // IEEE Transactions on Information Forensics and Security. 2010. V. 5. P. 349–353.
18. Harmsen J., Pearlman W. Steganalysis of additive noise modelable information hiding // Proc. of SPIE. 2003. V. 5020. P. 131–142.
19. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography // 5th International Workshop on Biometrics and Forensics (IWBF). 2017. P. 1–6.
20. Ker A.D. Improved Detection of LSB Steganography in Grayscale Images // International Workshop on Information Hiding, IH. 2004. P. 97–115.
21. Ker A.D. Resampling and the detection of LSB matching in color bitmaps // Proc. SPIE, EI. 2005. V. 5681. P. 1–15.
22. Ker A.D. Steganalysis of LSB matching in grayscale images // IEEE signal processing letters. 2005. V. 12. P. 441–444.
23. Kim J, Park H, Park J.-I. CNN-based image steganalysis using additional data embedding // Multimed Tools Appl. 2020. V. 79. P. 1355—1372.
24. Kumar U.P., Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2019. V. 8. P. 1239–1246.
25. Li B., Wei W., Ferreira A, Tan S. ReST-net: diverse activation modules and parallel subnets-based CNN for spatial image steganalysis // IEEE Signal Process Lett. 2018. V. 25, No. 5. P. 650—654.
26. Lyu S., Farid H. Detecting hidden messages using higher order statistics and support vector machines // Proceedins of Lecture Notes in Computer Science: 5th International Workshop on Information Hiding. 2002. V. 2578. P. 340–354.
27. Lyu S., Farid H. Steganalysis using color wavelet statistics and one-class support vector machines // In Proc. SPIE, EI, 2004. V. 5306. P. 35—45.
28. Mitra S., Roy T., Mazumdar D., Saha A.B. Steganalysis of LSB encoding in uncompressed images by close colour pair analysis // IIT Kanpur Hackers' Workshop 2004(IITK-HACK04). 23–24 Feb. 2004.
29. Pevny T., Patrick B., Fridrich J. Steganalysis by subtractive pixel adjacency matrix // IEEE Transactions on information Forensics and Security. 2010, February. V. 5, P. 215–224.
30. Rashid R.D., Asaad A., Jassim S. Topological Data Analysis as Image Steganalysis Technique // Mobile Multimedia/Image Processing, Security, and Applications. 2018. V. 10668. P. 17–26.
31. Shankar D.D., Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO // Multimedia Tools and Applications. 2020. DOI: 10.1007/s11042-020-09820-7.
32. Sharifzadeh M., Agarwal C., Aloraini M., Schonfeld D. Convolutional neural network steganalysis's application to steganography // IEEE Visual Communications and Image Processing. Dec 2017. P. 1–4.
33. Soto R.T., Ramos-Pollan R., Isazad G., et al. Digital media steganalysis. Digital Media Steganography: Principles, Algorithms, and Advances // ElsevierISBN: 9780128194386. DOI: 10.1016/C2018-0-04865-3. 2020. P. 259-293.
34. Wang Z., Chen M., Yang Y. Joint multi-domain feature learning for image steganalysis based on CNN // EURASIP Journal on Image and Video Processing. 2020(1). DOI:

10.1186/s13640-020-00513-7.
35. Westfeld A. Detecting low embedding rates // Proc. IHW. 2002. V. 2578 of LNCS. P. 324—339.
36. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems // Proceedings of Lecture Notes in Computer Science. 2000. V. 1768. P. 61–75.
37. Westfeld A., Pfitzmann A. Attacks on steganographic systems // International workshop on information hiding, Springer. 1999. P. 61–76.
38. Xu G., Wu H.Z., Shi Y.Q. Structural design of convolutional neural networks for steganalysis // IEEE Signal Process. Lett. 2016. V. 23, No. 5. P. 708–712.
39. Xu G., Wu H-Z., Shi YQ. Ensemble of CNNs for steganalysis: An empirical study // Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. 2016. P. 103—107.
40. Yang C., Wang J. Lin C. Chen H., Wang W. Locating Steganalysis of LSB Matching Based on Spatial and Wavelet Filter Fusion // CMC-Comput. Mat. Contin. 2019. V. 60, No. 2. P. 633-–644.
41. Ye J., Ni J., Yi Y. Deep learning hierarchical representations for image steganalysis // IEEE Trans Inf Forensics Secur. 2017. V. 12, No. 11. P. 2545-–255.
42. Yedroudj M., Comby F., Chaumont M. Yedroudj-net: An efficient CNN for spatial steganalysis // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). 2018. P. 2092–2096.
43. You W, Zhang H., ZhaoX. A Siamese CNN for Image Steganalysis // IEEE Transactions on Information Forensics and Security. 2020. V. 16. P. 291–306.
44. Zhang J., et al., Steganalysis for LSB matching in images with high-frequency noise // Proc. MMSP 2007, Crete, Greece. 2007. P. 385-–388.
45. Zhang R., Zhu F., Liu J., Liu G. Efficient feature learning and multi-size image steganalysis based on CNN // arXiv Prepr. arXiv1807.11428. 2018.
46. Zhang T, Zhang H, Wang R, Wu Y. A new JPEG image steganalysis technique combining rich model features and convolutional neural networks // Math Biosci Eng. 2019. V. 16, No. 5. P. 4069-–4081.

A SURVEY OF STEGANALYSIS METHODS IN THE PAPERS OF FOREIGN AUTHORS

D.E. Vilkhovskiy
Assistant of the Department of Information Security, e-mail: vilkhovskiy@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The paper provides a survey of foreign studies regarding steganalysis, aimed to detect hidden message insertion made by applying least significant bit replacement and discrete cosine transform algorithms. It is noted the further steganalysis methodology development splits in two directions: a decrease of the complexity and cost of processing and detection while maintaining a high level of classification rate, which is quite justified in the case of the presence of insertions with a large payload, i.e. up to 100%; or an increase of the insert recognition efficiency when dealing with images of a low payload. Besides, during the last five years, steganalisys

methods based on machine learning and deep learning began to play a dominant role in steganalysis

Keywords: steganalysis, steganographic analysis, LSB insertion, least significant bit replacement method.

References

1. Al-Jarrah M., Al-Taei Z. and Aboarqoub A. Steganalysis using LSB-focused statistical features. Proceedings of ICFNDS'17, Cambridge, United Kingdom, 2017, July 19-20, 5 pages. DOI: 10.1145/3102304.3109814.
2. Cancelli G., Doerr G., Cox I.J., and Barni M. Detection of 1 LSB Steganography based on the Amplitude of Histogram Local Extrema. Int. Conf. Image Processing, 2008, pp. 1288–1291.
3. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. Signal Process Image Commun., 2019, vol. 70, pp. 233–245.
4. Chaeikar. S.S. and Ahmadi A. SW: A blind LSBR image steganalysis technique. Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018, pp. 14–18.
5. Chaumont M. Deep learning in steganography and steganalysis. Digital Media Steganography, Academic Press, 2020, pp. 321–349.
6. Chen M, Boroumand M, and Fridrich J. Deep learning regressors for quantitative steganalysis. Electron Imaging, 2018, vol. 7, pp. 160—161.
7. Cogranne R., Giboulot Q., and Bas P. The ALASKA steganalysis challenge: A first step towards steganalysis. Proceedings of the ACM Workshop on Information Hiding and Multimedia Security, 2019, pp. 125–137.
8. Dumitrescu S., et al. Detection of lsb steganography via sample pair analysis. IEEE Trans. Signal Process, 2003, vol. 51, no. 7, pp. 1995-–2007.
9. Dumitrescu S. and Wu X. A new framework of lsb steganalysis of digital media. IEEE Trans. Signal Process, 2005, vol. 53, pp. 3936-–3947.
10. Eslam M., Elshafey M.A., and Mohamed M. Fouad. Enhancing CNN-based Image Steganalysis on GPUs. Journal of Information Hiding and Multimedia Signal Processing, 2020, vol. 11, no. 3, pp. 138–150.
11. Fridrich J and Kodovsky J. Rich models for steganalysis of digital images. IEEE Transactions on Information Forensics and Security, 2012, vol. 7, pp. 868–882.
12. Fridrich J., et al., Steganalysis of LSB encoding in colour image. Proc. 2000 IEEE International Conference on Multimedia and Expo, New York, USA, 2000, vol. 3, pp. 1279–1282.
13. Fridrich J., Goljan M., and Du R. Reliable detection of LSB steganography in color and grayscale images. Proceedings of the 2001 workshop on Multimedia and security: new challenges, ACM, 2001, pp. 27–30.
14. Fridrich J., Goljan M., and Soukal D. Higher-order statistical steganalysis of palette images. Proc. SPIE, EI., 2003, vol. 5020, pp. 178–190.
15. Goljan M., Fridrich J., and Holotyak T. New Blind Steganalysis and its Implications, SPIE Security, Steganography and watermarking of Multimedia Contents, 2006, vol. 6072, pp. 1–13.

16. Goljan, M., Fridrich, J., and Cogranne, R. Rich model for steganalysis of color images. Information Forensics and Security (WIFS), 2014 IEEE International Workshop, 2014, pp. 185–190.
17. Gul G. and Kurugollu F., SVD-based universal spatial domain image steganalysis. IEEE Transactions on Information Forensics and Security, 2010, vol. 5, pp. 349–353.
18. Harmsen J. and Pearlman W. Steganalysis of additive noise modelable information hiding. Proc. of SPIE, 2003, vol. 5020, pp. 131–142.
19. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography. 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1–6.
20. Ker A.D. Improved Detection of LSB Steganography in Grayscale Images. International Workshop on Information Hiding, IH, 2004, pp. 97–115.
21. Ker A.D. Resampling and the detection of LSB matching in color bitmaps. Proc. SPIE, EI, 2005, vol. 5681, pp. 1–15.
22. Ker A.D. Steganalysis of LSB matching in grayscale images. IEEE signal processing letters, 2005, vol. 12, pp. 441–444.
23. Kim J, Park H, and Park J.I. CNN-based image steganalysis using additional data embedding. Multimed Tools Appl., 2020, vol. 79, pp. 1355—1372.
24. Kumar U.P. and Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, vol. 8, pp. 1239–1246.
25. Li B., Wei W., Ferreira A, and Tan S. ReST-net: diverse activation modules and parallel subnets-based CNN for spatial image steganalysis. IEEE Signal Process Lett., 2018, vol. 25, no. 5, pp. 650—654.
26. Lyu S. and Farid H. Detecting hidden messages using higher order statistics and support vector machines. Proceedins of Lecture Notes in Computer Science: 5th International Workshop on Information Hiding, 2002, vol. 2578, pp. 340–354.
27. Lyu S. and Farid H. Steganalysis using color wavelet statistics and one-class support vector machines. In Proc. SPIE, EI, 2004, vol. 5306, pp. 35—45.
28. Mitra S., Roy T., Mazumdar D., and Saha A.B. Steganalysis of LSB encoding in uncompressed images by close colour pair analysis. IIT Kanpur Hackers' Workshop 2004(IITK-HApp. 04), 23–24 Feb. 2004.
29. Pevny T., Patrick B., and Fridrich J. Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on information Forensics and Security, 2010, February, vol. 5, pp. 215–224.
30. Rashid R.D., Asaad A., and Jassim S. Topological Data Analysis as Image Steganalysis Technique. Mobile Multimedia/Image Processing, Security, and Applications, 2018, vol. 10668, pp. 17–26.
31. Shankar D.D. and Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. Multimedia Tools and Applications, 2020. DOI: 10.1007/s11042-020-09820-7.
32. Sharifzadeh M., Agarwal C., Aloraini M., and Schonfeld D. Convolutional neural network steganalysis's application to steganography. IEEE Visual Communications and Image Processing, Dec 2017, pp. 1–4.
33. Soto R.T., Ramos-Pollan R., Isazad G., et al. Digital media steganalysis. Digital Media Steganography: Principles, Algorithms, and Advances, ElsevierISBN: 9780128194386.

DOI: 10.1016/pp. 018-0-04865-3. 2020. P. 259-293.

34. Wang Z., Chen M., and Yang Y. Joint multi-domain feature learning for image steganalysis based on CNN. EURASIP Journal on Image and Video Processing, 2020 (1). DOI: 10.1186/s13640-020-00513-7.
35. Westfeld A. Detecting low embedding rates. Proc. IHW, 2002, vol. 2578 of LNCS, pp. 324—339.
36. Westfeld A. and Pfitzmann A. Attacks on Steganographic Systems. Proceedings of Lecture Notes in Computer Science, 2000, vol. 1768, pp. 61–75.
37. Westfeld A. and Pfitzmann A. Attacks on steganographic systems. International workshop on information hiding, Springer, 1999, pp. 61–76.
38. Xu G., Wu H.Z., Shi Y.Q. Structural design of convolutional neural networks for steganalysis, IEEE Signal Process. Lett. 2016. V. 23, No. 5. P. 708–712.
39. Xu G., Wu H-Z. and Shi YQ. Ensemble of CNNs for steganalysis: An empirical study. Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, 2016, pp. 103—107.
40. Yang C., Wang J. Lin C. Chen H., and Wang W. Locating Steganalysis of LSB Matching Based on Spatial and Wavelet Filter Fusion. CMC-Comput. Mat. Contin., 2019, vol. 60, no. 2, pp. 633-–644.
41. Ye J., Ni J., and Yi Y. Deep learning hierarchical representations for image steganalysis. IEEE Trans Inf Forensics Secur., 2017, vol. 12, no. 11, pp. 2545-–255.
42. Yedroudj M., Comby F., and Chaumont M. Yedroudj-net: An efficient CNN for spatial steganalysis. IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2018, pp. 2092-–2096.
43. You W, Zhang H., and ZhaoX. A Siamese CNN for Image Steganalysis. IEEE Transactions on Information Forensics and Security, 2020, vol. 16, pp. 291–306.
44. Zhang J., et al., Steganalysis for LSB matching in images with high-frequency noise. Proc. MMSP 2007, Crete, Greece, 2007, pp. 385-–388.
45. Zhang R., Zhu F., Liu J., and Liu G. Efficient feature learning and multi-size image steganalysis based on CNN. arXiv Prepr. arXiv1807.11428, 2018.
46. Zhang T, Zhang H, Wang R, and Wu Y. A new JPEG image steganalysis technique combining rich model features and convolutional neural networks. Math Biosci Eng., 2019, vol. 16, no. 5, pp. 4069-–4081.

Дата поступления в редакцию: 23.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 103–111

УДК 004.932.2
DOI 10.24147/2222-8772.2020.4.103-111

СТЕГОАНАЛИЗ ЦВЕТНЫХ ИЗОБРАЖЕНИЙ С НИЗКИМ ЗАПОЛНЕНИЕМ СТЕГОКОНТЕЙНЕРА С ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО КОМПЛЕКСА

А.К. Гуц
д.ф.-м.н., профессор, e-mail: aguts@mail.ru
Д.Э. Вильховский
ассистент кафедры информационной безопасности, e-mail: vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В статье представлен программный комплекс, использование которого позволяет проводить стегоанализ цветных изображений на предмет выявления и извлечения скрытых сообщений в виде LSB-вставок, а также вставок, выполненных методом Коха–Жао. Комплекс объединяет ранее разработанные авторами алгоритмы и эффективен даже при малом заполнении стегоконтейнера (10–30 %). Приводятся результаты компьютерного эксперимента и сравнение эффективности предложенного комплекса с эффективностью других моделей

Ключевые слова: стегоанализ, стеганографический анализ, анализ стегоконтейнера, обнаружение LSB-вставки, обнаружение DCT-вставки, обнаружение вставки Коха–Жао.

Введение

Несмотря на развитие стеганографии и появление новых методов и алгоритмов методы замены наименее значащих бит (LSB), работающие с пространственной областью изображений, и метод Коха–Жао с использованием дискретного косинусного преобразования (DCT), работающий с частотной областью, до сих пор активно применяются для сокрытия данных. Следовательно, применение методов стегоанализа, направленных на обнаружение этих видов вставок, является по-прежнему актуальным.

Более того, злоумышленники, стремясь обойти существующие алгоритмы стегоатак, уменьшают объём встраиваемого сообщения, т. е. используют меньшее заполнение стегоконтейнера, что повышает уровень незаметности вставок. Следовательно, актуальной является разработка таких методов стегоанализа, которые могли бы обнаруживать изображения со встроенными сообщениями даже при низкоуровневой нагрузке.

Для решения данной задачи стеганографического анализа авторами разработан специальный программный комплекс на основе алгоритмов, обладающих высокой чувствительностью к стеговставкам при работе с цветными изображениями с малым заполнением стегоконтейнера. Объединение данных алгоритмов

в комплекс позволяет эффективно решать проблему обнаружения LSB-вставок и вставок, выполненных методом Коха-Жао.

С целью унификации трактовок в таблице 1 приведён ряд используемых в статье сокращений, заимствованных из англоязычных исследований и укоренившихся в отечественной терминологии.

Таблица 1. Перечень терминов, используемых в статье

Термин	Расшифровка на английском языке	Значение на русском языке
DCT	Discrete Cosine Transform	Дискретное косинусное преобразование
LSB	Least Significant Bit	Наименее значащий бит
TP	True positive	Истинно положительный
TN	True negative	Истинно отрицательный
FP	False positive	Ложно-положительный
FN	False negative	Ложно-отрицательный

1. Общая характеристика разработанного программного комплекса

Представляемый программный комплекс – это программное обеспечение, разработанное в виде веб-приложения с микросервисной архитектурой. Взаимодействие между клиентом и сервером осуществляется через GET/POST-запросы. Общая схема работы программного комплекса представлена на рисунке 1.

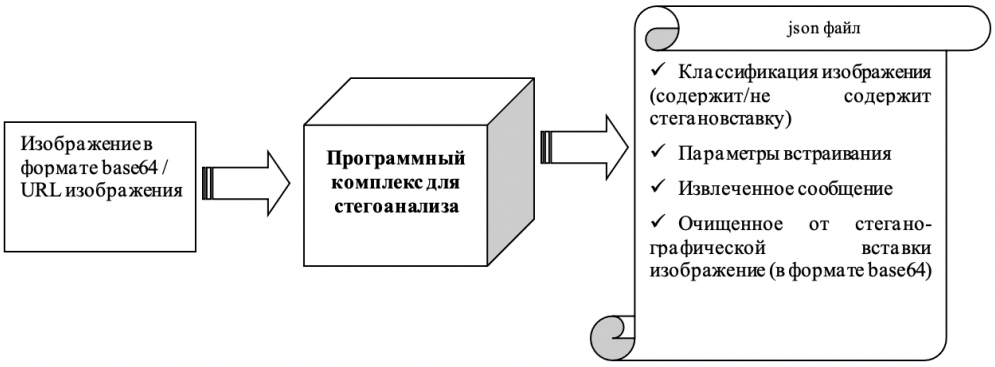

Рис. 1. Общая схема работы программного комплекса

Таким образом, для проведения стегоатаки можно либо загрузить анализируемое изображение непосредственно в программу, либо указать адрес его

размещения в сети. В результате программа возвращает не только констатацию факта наличия или отсутствия встроенного сообщения, но и параметры встраивания, а также извлечённое сообщение и изображение, очищенное от вставки.

Программный комплекс легко интегрируется с системой документооборота организации. Интеграция реализуется через хуки приложения, вызов которых осуществляется при загрузке файла на сервер или при добавлении или обновлении таблиц базы данных.

2. Основные компоненты программного комплекса

2.1. Первая компонента – алгоритм обнаружения стеговставок, выполненных методом LSB-замены

Алгоритм позволяет выявить скрытые сообщения, встраивание которых выполнено методом замены наименее значащих битов (LSB), при низком уровне заполнения стегоконтейнера минимальная величина встраиваемой нагрузки, при которой данный алгоритм всё ещё показывает высокую эффективность составляет 10 %. Основан на анализе младших слоев цветного цифрового изображения с применением алгоритма таксономии и метода анализа иерархий.

Использование метода анализа иерархий, описанного в работе [3], позволило существенно усовершенствовать модели, предложенные в работах [9, 10], и представить алгоритм в новой, более эффективной модификации.

Для анализа изображения на предмет наличия LSB-вставок и определения области встраивания проводится иерархический анализ трёх младших слоев — нулевого и двух вышележащих слоев. Пиксели каждого из трёх слоев анализируются на основе предложенных критериев и весовых коэффициентов, представленных в таблице 2. Иерархическая взаимосвязь младших битов, а также младших битов и битов более высокого порядка и её особенности позволяют классифицировать изображение как чистое или имеющее вставки.

Таблица 2. Критерии принятия решения и их весовые коэффициенты

Критерии	Весовые коэффициенты
Сравнение значения бита и значений соседних по сторонам битов	$r_1 = \dfrac{nk}{nk+k+1}$
Сравнение значения бита и значений соседних по углам битов	$r_2 = \dfrac{k}{nk+k+1}$
Сравнение значения бита и значений окружающих битов	$r_3 = \dfrac{1}{nk+k+1}$

Более того, на основе анализа поведения битов всех трёх слоев алгоритм способен не только сделать вывод о наличии или отсутствии замены младших битов, но и сформировать список пикселей со встроенным сообщением, что позволяет не только классифицировать изображение как стегоконтейнер, но и

определить область встраивания с высокой степенью точности.

Далее предложенный алгоритм был усовершенствован для возможности его применения в областях градиентной заливки, что достигается в том числе предварительной обработкой изображения.

Более детальное описание алгоритма представлено в работе [1].

2.2. Вторая компонента — алгоритм обнаружения стеговставок, выполненных методом Коха–Жао

Алгоритм позволяет выявлять стеганографические вставки, встраивание которых выполнено методом Коха–Жао, описанным в работе [7]. Для выявления блоков встраивания алгоритм использует анализ среднечастотных коэффициентов дискретного косинусного преобразования (далее DCT-коэффициентов) в трёх видах последовательности их величин. Необходимым условием успешного анализ является определение правильного порогового значения.

Анализ последовательности величин DCT-коэффициентов основан на том факте, что встраивание изменяет как минимум одну из последовательностей, что на гистограмме изображения будет иметь вид некой ступени, имеющей определённую высоту, равную величине порога.

В данную компоненту программного комплекса встроен модуль поиска ступенчатых изменений, что позволяет последовательно проходить по всем блокам изображения в поисках блоков встраивания.

В результате анализа последовательности и численного дифференцирования с использованием разностных схем для определения границ ступеней гистограммы формируются матрицы данных коэффициентов дискретного косинусного преобразования.

Таким образом, выявление факта изменения одной из последовательностей означает, что исследуемое изображение содержит встроенное сообщение. Более того, высокие пики на гистограмме зависимостей позволяют достоверно определить границы этого сообщения, а также осуществить его извлечение с минимальными потерями.

Более детальное описание алгоритма представлено в работе [2].

3. Эффективность программного комплекса

Эффективность предложенного программного комплекса тестировалась при помощи компьютерного эксперимента с использованием базы изображений BossBase и базы изображений праздников INRIA. Выбор данных баз изображений обусловлен, в первую очередь, популярностью их использования в других отечественных и зарубежных исследованиях, что позволило в дальнейшем получить сопоставимые данные по чувствительности предложенного программного комплекса и некоторых других моделей стегоанализа.

Тестирование проводилось с различными уровнями нагрузки (уровнями заполнения стегоконтейнера): 30 %, 25 %, 20 %, 15 %, и 10 %. Встраивание производилось методом LSB-замены и методом Коха–Жао (далее — DCT-вставки).

Встраивание методом LSB-замены осуществлялось в синюю компоненту. Результаты проведённого эксперимента представлены в таблицах 3 и 4.

Таблица 3. Результаты стегоатак, проведённых при помощи программного комплекса с использованием базы изображений BossBase, %

Тестируемая нагрузка	Обнаружение LSB-вставок				Обнаружение DCT-вставок			
	TP	FN	TN	FP	TP	FN	TN	FP
30 %	91,15	8,85	79,12	20,88	84,73	15,27	76,53	23,47
25 %	87,91	12,09			79,11	20,89		
20 %	79,87	20,13			74,64	25,36		
15 %	72,31	27,69			68,12	31,88		
10 %	63,12	36,88			63,88	36,12		

В самом общем виде можно сделать вывод, что оба алгоритма показывают лучшую чувствительность при работе с изображениями, содержащими скрытые сообщения, чем с чистыми изображениями. Однако полученные величины погрешностей при классификации чистых изображений находятся в пределах допустимых значений.

Таблица 4. Результаты стегоатак, проведённых при помощи программного комплекса с использованием базы изображений INRIA, %

Тестируемая нагрузка	Обнаружение LSB-вставок				Обнаружение DCT-вставок			
	TP	FN	TN	FP	TP	FN	TN	FP
30 %	90,36	9,64	78,31	21,69	86,3	13,7	79,15	20,85
25 %	86,89	13,11			80,26	19,74		
20 %	79,6	20,4			76,01	23,99		
15 %	72,03	27,97			69,94	30,06		
10 %	62,56	37,44			65,04	34,96		

Сводные данные по эффективности каждого из алгоритмов программного комплекса представлены в таблице 5.

Таблица 5. Эффективность программного комплекса, %

Тестируемая нагрузка	BossBase		INRIA	
	Обнаружение LSB-вставок	Обнаружение DCT-вставок	Обнаружение LSB-вставок	Обнаружение DCT-вставок
30 %	91,15	84,73	90,36	86,3
25 %	87,91	79,11	86,89	80,26
20 %	79,87	74,64	79,6	76,01
15 %	72,31	68,12	72,03	69,94

10 %	63,12	63,88	62,56	65,04

Данные, полученные в результате проведённого компьютерного эксперимента, свидетельствуют о высокой результативности предложенного программного комплекса. Ожидаемо, максимальная эффективность достигается при более высоких уровнях заполнения стегоконтейнера и снижается по мере уменьшения размера встраиваемого сообщения: 91,15 % и 86,3 % против 63,12 % и 65,04 % для LSB-вставок и DCT-вставок соответственно.

Также отмечается, что алгоритмы, используемые в программном комплексе, показывают некоторую чувствительность к базам изображений. Так, программный комплекс показывает лучшую результативность в обнаружении вставок, выполненных методом LSB-замены, при работе с изображениями из BossBase, по сравнению с изображениями из базы INRIA, тогда как алгоритм выявления сообщений, скрытых методом Коха–Жао, лучше работает с базой изображений праздников INRIA, чем с BossBase. Возможно, последний факт связан с тем, что база изображений праздников INRIA содержит изображения в формате JPEG, что соответствует принципам DCT, на основе которых работает алгоритм обнаружения вставок Коха–Жао, в результате чего наблюдается снижение ошибок классификации.

Для получения более полной картины о преимуществах и целесообразности использования предлагаемого нами программного комплекса для обнаружения LSB-вставок, сравним его результативность с результативностью некоторых методов, предложенных в исследованиях других авторов. В качестве базы сравнения нами рассмотрены ансамблевый SW-стегоанализ [4, 5], SVM-PSO-стегоанализ JPEG изображений [8, 11] и компактный метод стегоанализа [6]. Выбор данных исследований продиктован наличием чётких количественных выводов об эффективности обнаружения стеганографических вставок при низком уровне заполнения стегоконтейнера (10 или 25 %), что в полной мере соответствует объёму встраиваемой нагрузки, таргетируемой представленным программным комплексом. Сравнительная эффективность обнаружения представлена в таблице 6, сравнение происходит по наилучшим значениям работы программного комплекса.

Таблица 6. Сравнительная эффективность обнаружения

Встраиваемая нагрузка	Предлагаемый программный комплекс	Ансамблевый SW-стегоанализ	SVM-PSO стегоанализ JPEG изображений	Компактный метод стегоанализа
25%	87,91	86,77	–	74,53
10%	65,04	–	51,07	–

На основании данных, представленных в таблице 6, можно сделать вывод, что алгоритмы, реализованные в разработанном программном комплексе, по

своей эффективности обладают существенным превосходством по сравнению с другими рассматриваемыми алгоритмами. При этом, если при 25 % заполнении стегоконтейнера преимущество представленных нами алгоритмов по сравнению с моделями, использующими машинное обучения невелико и составляет чуть более 1 % (хотя и показывает лучшие значения по сравнению с компактным методом), то при 10 % заполнении стегоконтейнера алгоритмы предложенного программного комплекса выдают значительную разницу в результативности (65,04 % против 51,07 %)

Заключение

На основе разработанных алгоритмов обнаружения LSB-вставок с использованием метода анализа иерархий и таксономии, а также алгоритма обнаружения вставок, выполненных методом Коха–Жао, использующего дискретное косинусное преобразование, был создан программный комплекс. Тестирование его на двух базах показало, что данный комплекс позволяет обнаруживать (в наилучших значениях) до 91,15 % изображений, содержащих LSB-вставки и до 86,3 % изображений, содержащих вставки Коха–Жао. Ошибки классификации стего-изображений составляют, соответственно, 8,85 % и 13,7 %, в то время как ошибки классификации чистых изображений составляют, соответственно, 20,88 % и 20,85 % (в наименьших значениях), что в целом является допустимым уровнем.

Таким образом, делается вывод о высокой эффективности и целесообразности применения данного программного комплекса при проведении стеганографического анализа цветных изображений с малым заполнением стегоконтейнера (малой нагрузкой).

Литература

1. Белим С.В., Вильховский Д.Э. Алгоритм выявления стеганографических вставок типа LSB-замещения на основе анализа слоя младших битов // Информатика и системы управления. 2017. № 4 (54). С. 3—11.
2. Белим С.В., Вильховский Д.Э. Стеганоанализ алгоритма Коха–Жао // Математические структуры и моделирование. 2018. № 4(48). С. 113—119.
3. Amritha P.P., Sreedivya-Muraleedharan M., Rajeev K., Sethumadhavan M. Steganalysis of LSB Using Energy Function // Advances in Intelligent Systems and Computing. 2016. No. 384. P. 549–558.
4. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection // Signal Process Image Commun. 2019. No. 70. P. 233–245.
5. Chaeikar S.S., Ahmadi A. SW: A blind LSBR image steganalysis technique // In Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018. P. 14-–18.
6. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography // 5th International Workshop on Biometrics and Forensics (IWBF). 2017. P. 1–6.

7. Koch E. Towards robust and hidden image copyright labeling // IEEE Workshop on Nonlinear Signal and Image Processing. 1995; P. 452—455.
8. Kumar U.P., Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers // International Journal of Innovative Technology and Exploring Engineering (IJITEE). 2019, V. 8; P. 1239—1246.
9. Ojala T., Pietikainen M., Harwood D. A Comparative Study of Texture Measures with Classification Based on Feature Distributions // Pattern Recognition, 1996. No. 29. P. 51—59.
10. Saaty T.L. Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors // The Analytic Hierarchy/Network Process. Review of the Royal Spanish Academy of Sciences. Series A, Mathematics. 2008. No. 102(2). P. 251-–318.
11. Shankar D.D., Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO // Multimedia Tools and Applications. 2020. DOI: 10.1007/s11042-020-09820-7.

STEGANALYSIS OF LOW STEGO-PAYLOAD COLOR IMAGES USING SOFTWARE COMPLEX

A.K. Guts
Dr.Sc. (Phys.-Math.), Professor, e-mail: aguts@mail.ru
D.E. Vilkhovskiy
Assistant of the Department of Information Security, e-mail: vilkhovskiy@gmail.com

Dostoevsky Omsk State University, Omsk, Russia

Abstract. In the paper, a new software package is presented as a tool that allows to conduct steganalysis of color images and reveal embedded messages such as LSB inserts or Koha-Zhao inserts. The complex combines two algorithms previously developed by the authors and is highly effective even for small stegocontainer payload (10–30 %). The computer experiment results and a comparison of the software package and some other models performance are presented and discussed.”.

Keywords: steganalysis, steganographic analysis, stegocontainer analysis, LSB-insert detection, DCT-insert detection, Koch-Zhao insert detection..

References

1. Belim S.V. and Vil’khovskii D.E. Algoritm vyyavleniya steganograficheskikh vstavok tipa LSB-zameshcheniya na osnove analiza sloya mladshikh bitov. Informatika i sistemy upravleniya, 2017, no. 4(54), pp. 3—11. (in Russian)
2. Belim S.V., and Vil’khovskii D.E. Steganoanaliz algoritma Kokha–Zhao. Matematicheskie struktury i modelirovanie, 2018, no. 4(48), pp. 113—119. (in Russian)
3. Amritha P.P., Sreedivya-Muraleedharan M., Rajeev K., and Sethumadhavan M. Steganalysis of LSB Using Energy Function. Advances in Intelligent Systems and Computing, 2016, no. 384, pp. 549–558.

4. Chaeikar A. Ensemble SW image steganalysis: A low dimension method for LSBR detection. Signal Process Image Commun., 2019, no. 70, pp. 233–245.
5. Chaeikar S.S. and Ahmadi A. SW: A blind LSBR image steganalysis technique. In Proceedings of the 10th International Conference on Computer Modeling and Simulation, Sydney Australia, 8 January 2018, pp. 14-–18.
6. Juarez-Sandoval O., Cedillo-Hernandez M., Sanchez-Perez G. et all. Compact Image Steganalysis for LSB-Matching Steganography. 5th International Workshop on Biometrics and Forensics (IWBF), 2017, pp. 1–6.
7. Koch E. Towards robust and hidden image copyright labeling. IEEE Workshop on Nonlinear Signal and Image Processing, 1995, pp. 452—455.
8. Kumar U.P. and Shankar D.D. Blind Steganalysis for JPEG Image susing SVM and SVM-PSO Classifiers. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 2019, vol. 8, pp. 1239—1246.
9. Ojala T., Pietikainen M., and Harwood D. A Comparative Study of Texture Measures with Classification Based on Feature Distributions, Pattern Recognition, 1996, no. 29, pp. 51—59.
10. Saaty T.L. Relative Measurement and its Generalization in Decision Making: Why Pairwise Comparisons are Central in Mathematics for the Measurement of Intangible Factors. The Analytic Hierarchy/Network Process, Review of the Royal Spanish Academy of Sciences, Series A, Mathematics, 2008, no. 102(2), pp. 251-–318.
11. Shankar D.D. and Azhakath A.S. Minor blind feature based Steganalysis for calibrated JPEG images with cross validation and classification using SVM and SVM-PSO. Multimedia Tools and Applications, 2020. DOI: 10.1007/s11042-020-09820-7.

Дата поступления в редакцию: 23.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 112–125

УДК 004.056
DOI 10.24147/2222-8772.2020.4.112-125

ОЦЕНКА СРЕДНЕГО ВРЕМЕНИ ДО ОТКАЗА БЕЗОПАСНОСТИ НА ОСНОВЕ МАРКОВСКИХ ЦЕПЕЙ С НЕПРЕРЫВНЫМ ВРЕМЕНЕМ

А. А. Магазев
д.ф.-м.н., профессор, кафедра «Комплексная защита информации»,
e-mail: magazev@omgtu.ru
А. С. Мельникова
магистрант, кафедра «Комплексная защита информации»,
e-mail: anastasiya_m.96@mail.ru
В. Ф. Цырульник
аспирант, кафедра «Комплексная защита информации», e-mail: lera.tsyrulnik@mail.ru

Омский государственный технический университет, Омск, Россия

Аннотация. В статье рассматривается марковская модель компьютерных атак, в рамках которой атаки и ответные действия со стороны системы моделируются простейшими пуассоновскими потоками событий. Описан метод решения соответствующей системы уравнений Колмогорова с помощью вычисления собственных векторов и собственных чисел некоторой матрицы. Детально исследована важная случайная величина, ассоциированная с соответствующим марковским случайным процессом и называемая временем до отказа безопасности. Представлены результаты сравнения полученных результатов с результатами имитационного моделирования.

Ключевые слова: марковская цепь с непрерывным временем, уравнения Колмогорова, среднее время до отказа безопасности.

Введение

Оценка эффективности систем защиты информации представляет собой важную задачу информационной безопасности. Стоит, однако, отметить, что данная проблема всё ещё плохо поддаётся формализации, во многом из-за большого разнообразия актуальных угроз кибербезопасности и структурной сложности информационных систем, на которые эти угрозы направлены. Существующие нормативно-правовые механизмы подобной оценки (например, требования регуляторов сферы ИБ) носят, в основном, качественный характер и не учитывают множество тонких аспектов развития современных информационных технологий. В то же время подобные аспекты являются довольно актуальными, например, в коммерческом секторе, где владельцы защищаемой информации заинтересованы в более гибких и своевременных способах управления инвестициями в кибербезопасность.

Одним из современных направлений решения проблемы оценки защищённости информации является стохастическое моделирование и основанное на нём использование так называемых *метрик безопасности* (см. [1–3]). Последние представляют собой наборы количественных характеристик, правильная агрегация которых может служить оценкой уровня защищённости моделируемой компьютерной системы. Одной из наиболее часто применяемых метрик безопасности является *время до отказа безопасности*, то есть время, прошедшее до момента совершения события, ассоциируемого с нарушением режима безопасности. В качестве примера приведём работу [3], в которой авторы вычисляют эту метрику, основываясь на результатах моделирования компьютерных систем с помощью полумарковских цепей.

В статье [4] была предложена марковская модель с непрерывным временем, в которой кибератаки (или киберугрозы) моделируются простейшими пуассоновскими потоками событий. В настоящей статье мы более подробно исследуем эту марковскую модель; в частности, описываем алгебраический метод решения соответствующей системы уравнений Колмогорова, основанный на вычислении собственных чисел и собственных векторов некоторой матрицы. Далее мы определяем время до отказа безопасности как время, прошедшее с момента $t = 0$ до момента попадания системы в так называемое состояние *отказа безопасности*. После этого мы детально описываем эту случайную величину, вычислив её функцию плотности вероятности и получив формулы для её моментов произвольного порядка. В конце нашей статьи мы приводим результаты сравнения полученных нами теоретических результатов с результатами имитационного моделирования.

1. Моделирование кибератак с помощью марковских цепей с непрерывным временем

Рассмотрим некоторую компьютерную систему (далее просто *систему*), потенциально уязвимую для n различных кибератак. Под *кибератакой* мы понимаем любую попытку воздействия на систему, целью которой является несанкционированный доступ, уничтожение, модификация или кража информационных активов.

Опишем математическую модель, в рамках которой возможно количественное описание как самих кибератак, так и ответных действий со стороны системы [4]. Во-первых, мы будем предполагать, что последовательность появлений любой i-ой кибератаки представляет собой простейший пуассоновский поток событий с интенсивностью λ_i. Наше второе предположение состоит в том, что последовательность встречных действий (защитных реакций) со стороны системы также распределена в соответствии с пуассоновским распределением; интенсивность соответствующего потока мы обозначим μ_i, а вероятность успешного отражения i-ой кибератаки — r_i. Таким образом, наша модель описывается с помощью $3n$ входных параметров:

- $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$ — интенсивности потоков кибератак;
- $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ — интенсивности потоков отражений кибератак;

• $r = (r_1, r_2, \ldots, r_n)$ — вероятности отражения кибератак.

По своему смыслу эти параметры подчиняются следующим требованиям:

$$\lambda_i \geqslant 0, \quad \mu_i \geqslant 0, \quad 0 \leqslant r_i \leqslant 1, \quad i = 1, 2, \ldots, n.$$

В соответствии со сделанными предположениями, наша система может быть описана в терминах некоторой модели конечных состояний. Состояние s_0, в котором система не подвергается никаким кибератакам, мы будем называть *безопасным состоянием*. Состояние, ассоциированное с появлением i-ой кибератаки, мы обозначаем s_i и называем *состоянием i-ой кибератаки*. В этом состоянии система находится некоторое время, имеющее пуассоновское распределение с параметром μ_i. По истечении этого времени данная кибератака будет либо отражена с вероятностью r_i, либо не отражена с вероятностью $\bar{r}_i \equiv 1 - r_i$. В первом случае система возвращается в безопасное состояние s_0, во втором — переходит в состояние *отказа безопасности* s_{n+1}.

Состояние отказа безопасности s_{n+1} мы будем считать финальным, то есть система, однажды оказавшись в этом состоянии, останется в нём навсегда. Это состояние означает успешную реализацию атаки, что влечёт за собой определённые негативные последствия для системы (кража информации, финансовые потери и т. д.). Очевидно, на практике это состояние не является конечным; после осуществления различных восстановительных мероприятий система может быть возвращена в безопасное состояние s_0. Подобные действия, однако, выходят за рамки рассматриваемой модели, и мы их учитывать не будем.

На основе изложенных выше положений мы можем сделать вывод о том, что вероятность состояний системы в будущем зависит только от того, в каком состоянии система находится в настоящем, и не зависит от её поведения в прошлом. Это позволяет нам трактовать последовательность состояний системы как *марковский процесс* с непрерывным временем и конечным числом состояний. Общее представление о данном случайном процессе даёт размеченный граф состояний системы, показанный на рис. 1.

Обозначим $p_i(t)$ вероятность того, что система в момент времени t находится в состоянии s_i, $i = 0, 1, \ldots, n+1$. Как известно, эти вероятности могут быть найдены путём решения системы обыкновенных дифференциальных уравнений первого порядка, называемых *уравнениями Колмогорова*. В нашем случае эти уравнения легко могут быть выписаны с использованием размеченного графа состояний, изображённого на рис. 1:

$$\frac{dp_0(t)}{dt} = -\lambda_0 p_0(t) + \sum_{k=1}^{n} \mu_k r_k p_k(t); \tag{1}$$

$$\frac{dp_i(t)}{dt} = \lambda_i p_0(t) - \mu_i p_i(t), \quad i = 1, \ldots, n; \tag{2}$$

$$\frac{dp_{n+1}(t)}{dt} = \sum_{k=1}^{n} \mu_k \bar{r}_k p_k(t). \tag{3}$$

Здесь мы ввели дополнительное обозначение $\lambda_0 \equiv \sum_{i=1}^{n} \lambda_i$. Для однозначного определения вероятностей $p_i(t)$ требуется задать их значения в начальный

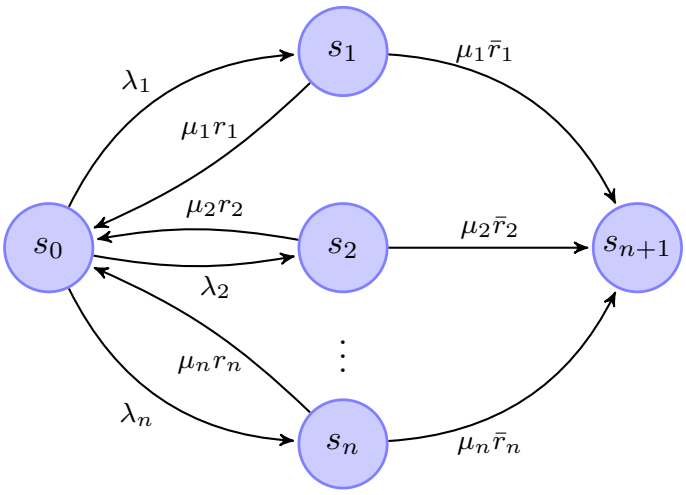

Рис. 1. Размеченный граф состояний системы

момент времени $t = 0$; мы сделаем это, наложив условие

$$p_0(0) = 1, \quad p_1(0) = p_2(0) = \cdots = p_{n+1}(0) = 0, \tag{4}$$

означающее, что в момент времени $t = 0$ система находится в безопасном состоянии s_0. Решение задачи Коши (1)–(4) полностью определяет динамику системы.

В практических вычислениях удобнее всего представлять систему уравнений (1)–(3) в матричной форме

$$\frac{d\mathbf{p}(t)}{dt} = \mathbf{p}(t) \cdot \Pi. \tag{5}$$

Здесь $\mathbf{p}(t) = (p_0(t), p_1(t), \ldots, p_{n+1}(t))$ — вектор вероятностей состояний системы в момент t, а квадратная матрица Π порядка $n + 2$ имеет вид

$$\Pi = \begin{pmatrix} -\lambda_0 & \lambda_1 & \lambda_2 & \ldots & \lambda_n & 0 \\ \mu_1 r_1 & -\mu_1 & 0 & \ldots & 0 & \mu_1\bar{r}_1 \\ \mu_2 r_2 & 0 & -\mu_2 & \ldots & 0 & \mu_2\bar{r}_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \mu_n r_n & 0 & 0 & \ldots & -\mu_n & \mu_n\bar{r}_n \\ 0 & 0 & 0 & \ldots & \ldots & 0 \end{pmatrix}. \tag{6}$$

Матрица Π обладает следующим важным свойством: сумма элементов каждой её строки равна нулю.

2. Алгебраический метод решения уравнений Колмогорова

Перед тем как заняться решением задачи (1)–(4) в общем случае, рассмотрим две частные ситуации, в которых эту задачу можно сравнительно легко

решить в аналитическом виде.

ПРИМЕР 1 (случай отсутствия кибератак). Пусть $\lambda_i = 0$ для всех i. В этой ситуации решение задачи Коши (1)–(4) имеет простой вид:

$$p_0(t) = 1, \quad p_1(t) = p_2(t) = \cdots = p_{n+1}(t) = 0.$$

Данное решение иллюстрирует тривиальный факт: в отсутствие кибератак система всегда будет находиться в безопасном состоянии.

ПРИМЕР 2 (случай отсутствия защиты). Предположим, что $r_i = 0$ для всех i. Если ни один параметр μ_i не совпадает с λ_0, решение задачи (1)–(4) также находится элементарно

$$p_0(t) = e^{-\lambda_0 t};$$

$$p_i(t) = \frac{\lambda_i}{\lambda_0 - \mu_i}\left(e^{-\mu_i t} - e^{-\lambda_0 t}\right), \quad i = 1, \ldots, n;$$

$$p_{n+1}(t) = 1 - e^{-\lambda_0 t} - \sum_{j=1}^{n} \frac{\lambda_j}{\lambda_0 - \mu_j}\left(e^{-\mu_j t} - e^{-\lambda_0 t}\right).$$

Отсюда видно, что с ростом t вероятность обнаружения системы в безопасном состоянии s_0 экспоненциально уменьшается, а в состоянии s_{n+1}, напротив, увеличивается и стремится к единице. Отметим, что хотя случаи, когда некоторые из μ_i совпадают с λ_0, необходимо рассматривать отдельно, получить аналитическое решение не составляет труда и в таких ситуациях.

Вернёмся к общему случаю. Обычно для построения общего решения системы уравнений Колмогорова с постоянными коэффициентами широко применяется преобразование Лапласа. В нашем случае, однако, более удобным будет метод, использующий собственные числа и собственные векторы матрицы (6). Предварительно отметим некоторую полезную информацию о собственных числах матрицы П.

Предложение 1. *Все собственные числа матрицы* (6) *вещественны и принадлежат отрезку* $[-2\gamma, 0]$, *где* $\gamma = \max\{\lambda_0, \mu_1, \ldots, \mu_n\}$.

Доказательство. Вещественность собственных чисел матрицы (6) следует из результата Дрейзина и Хейнсворса, приведённого в работе [5]. Доказательство второй части утверждения базируется на теореме Гершгорина (см., например, монографию [6]), согласно которой все собственные значения матрицы (6) заключены в объединении $n+1$ отрезков

$$[-2\lambda_0, 0] \cup [-2\mu_1, 0] \cup [-2\mu_2, 0] \cup \cdots \cup [-2\mu_n, 0].$$

Отсюда следует, что всякое собственное число будет принадлежать отрезку $[-2\gamma, 0]$, где γ — максимум из чисел $\lambda_0, \mu_1, \ldots, \mu_n$. ■

Отметим, что в силу наличия в матрице (6) нулевой строки, матрица П всегда имеет одно нулевое собственное число $\sigma_0 = 0$. Таким образом, спектр матрицы (6) имеет следующую структуру

$$\mathrm{Spec}(\Pi) = \{\sigma_0 = 0, -|\sigma_1|, -|\sigma_2|, \ldots, -|\sigma_{n+1}|\},$$

где $\sigma_1, \ldots, \sigma_{n+1}$ — отрицательные вещественные числа (для упрощения дальнейших рассуждений мы будем считать, что спектр матрицы (6) является простым).

Из общей теории систем линейных однородных дифференциальных уравнений с постоянными коэффициентами известно, что система (5) имеет $n+2$ линейно независимых решения вида

$$\mathbf{p}_0(t) = \mathbf{c}_0, \quad \mathbf{p}_1(t) = \mathbf{c}_1 e^{\sigma_1 t}, \quad \mathbf{p}_2(t) = \mathbf{c}_2 e^{\sigma_2 t}, \quad \ldots, \quad \mathbf{p}_{n+1}(t) = \mathbf{c}_{n+1} e^{\sigma_{n+1} t},$$

где $\mathbf{c}_\nu$ — левый собственный вектор матрицы Π, отвечающий собственному значению σ_ν, $\nu = 0, 1, \ldots, n+1$.

Выберем собственные векторы $\mathbf{c}_\nu$ так, чтобы выполнялось условие $\sum_{\nu=0}^{n+1} \mathbf{c}_\nu = \mathbf{e}_0$, где $\mathbf{e}_0 = (1, 0, \ldots, 0)$ — вектор с единицей в первой позиции и с нулями в остальных. Тогда решение системы уравнений Колмогорова (1)–(3), удовлетворяющее начальному условию (4), будет иметь вид

$$\mathbf{p}(t) = \sum_{\nu=0}^{n+1} \mathbf{c}_\nu e^{\sigma_\nu t} = \mathbf{c}_0 + \mathbf{c}_1 e^{\sigma_1 t} + \cdots + \mathbf{c}_{n+1} e^{\sigma_{n+1} t}. \tag{7}$$

Последняя формула в покомпонентной записи может быть переписана как

$$p_i(t) = \delta_{i,n+1} + \sum_{\nu=1}^{n+1} c_{\nu,i} e^{\sigma_\nu t}, \quad i = 0, \ldots, n+1, \tag{8}$$

где через $c_{\nu,i}$ обозначена i-ая компонента собственного вектора $\mathbf{c}_\nu$, δ_{ij} — символ Кронеккера и, кроме того, мы учли тот факт, что собственный вектор, отвечающий собственному числу $\sigma_0 = 0$, имеет вид $\mathbf{c}_0 = (0, \ldots, 0, 1)$. Начальное условие (4) также может быть выражено в терминах собственных векторов $\mathbf{c}_\nu = (c_{\nu,i})$:

$$\sum_{\nu=1}^{n+1} c_{\nu,i} = \delta_{0,i} - \delta_{n+1,i}, \quad i = 0, 1, \ldots, n+1. \tag{9}$$

Резюмируя полученные результаты, приведем пошаговый алгоритм решения задачи Коши (1)–(4), который может быть легко реализован в помощью современных математических пакетов.

`Шаг 1`. По заданным входным параметрам модели λ, μ и r формируем матрицу Π в соответствии с формулой (6).

`Шаг 2`. Находим собственные числа σ_ν и собственные векторы $\mathbf{c}_\nu = (c_{\nu,i})$ матрицы Π.

`Шаг 3`. Решаем систему линейных однородных уравнений $\sum_{\nu=0}^{n+1} a_\nu c_{\nu,i} = \delta_{0,i}$ относительно неизвестных a_ν и делаем замену $\mathbf{c}_\nu \to a_\nu \mathbf{c}_\nu$ для всех $\nu = 0, 1, \ldots, n+1$.

`Шаг 4`. Выписываем решение задачи Коши (1)–(4) в соответствии с формулой (7).

ПРИМЕР 3. Приведём численный пример. Рассмотрим модель со следующими значениями входных параметров:

$$n = 3, \quad \lambda = (4.28, 3.97, 1.13), \quad \mu = (0.92, 0.42, 0.95), \quad r = (0.10, 0.40, 0.38). \tag{10}$$

В этом случае матрица (6) записывается как

$$\Pi = \begin{pmatrix} -9.38 & 4.28 & 3.97 & 1.13 & 0. \\ 0.092 & -0.92 & 0. & 0. & 0.828 \\ 0.168 & 0. & -0.42 & 0. & 0.252 \\ 0.361 & 0. & 0. & -0.95 & 0.589 \\ 0. & 0. & 0. & 0. & 0. \end{pmatrix}.$$

Спектр этой матрицы имеет вид

$$\mathrm{Spec}(\Pi) = \{0., -9.5462, -0.9374, -0.8529, -0.3335\}.$$

Соответствующие собственные векторы $\mathbf{c}_\nu$, нормированные условием $\sum_{\nu=0}^{4} \mathbf{c}_\nu = (1, 0, 0, 0, 0)$, равны

$$\begin{aligned} \mathbf{c}_0 &= (0, 0, 0, 0, 1); \\ \mathbf{c}_1 &= (0.9815, -0.4870, -0.4270, -0.1290, 0.0615); \\ \mathbf{c}_2 &= (0.0003, -0.0635, -0.0020, 0.0232, 0.0421); \\ \mathbf{c}_3 &= (0.0074, 0.4716, -0.0678, 0.0860, -0.4972); \\ \mathbf{c}_4 &= (0.0108, 0.07896, 0.4968, 0.0198, -0.6064). \end{aligned}$$

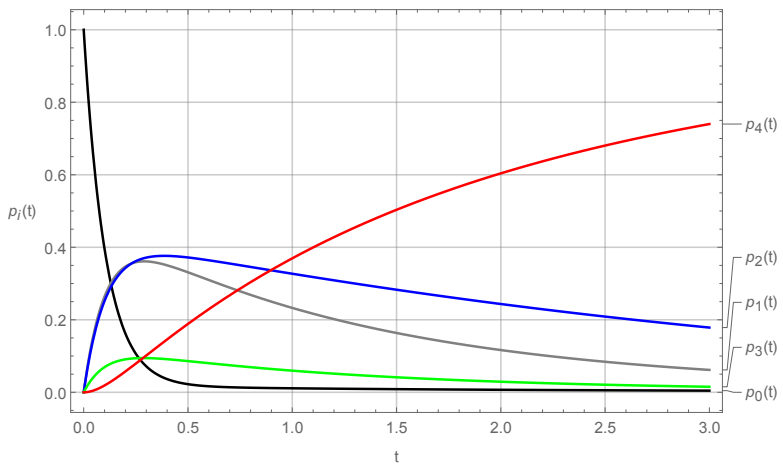

Рис. 2. Графики функций $p_i(t)$ при $\lambda = (4.28, 3.97, 1.13)$, $\mu = (0.92, 0.42, 0.95)$ и $r = (0.10, 0.40, 0.38)$.

Отсюда в соответствии с формулой (7) получаем следующее решение задачи Коши (1)–(4):

$$
\begin{aligned}
p_0(t) &= +0.9815e^{-9.5462t} + 0.0003e^{-0.9374t} + 0.0074e^{-0.8529t} + 0.0108e^{-0.3335t},\\
p_1(t) &= -0.4870e^{-9.5462t} - 0.0635e^{-0.9374t} + 0.4716e^{-0.8529t} + 0.0790e^{-0.3335t},\\
p_2(t) &= -0.4270e^{-9.5462t} - 0.0020e^{-0.9374t} - 0.0678e^{-0.8529t} + 0.4968e^{-0.3335t},\\
p_3(t) &= -0.1290e^{-9.5462t} + 0.0232e^{-0.9374t} + 0.0860e^{-0.8529t} + 0.0198e^{-0.3335t},\\
p_4(t) &= 1 + 0.0615e^{-9.5462t} + 0.0421e^{-0.9374t} - 0.4972e^{-0.8529t} - 0.6064e^{-0.3335t}.
\end{aligned}
$$

На рис. 2 приведены зависимости полученных вероятностей $p_i(t)$ от времени на отрезке $[0, 3]$.

3. Время до отказа безопасности

Стохастическое моделирование кибератак часто используется как вспомогательный инструмент для строгой теоретической оценки различных количественных характеристик систем защиты информации, отражающих их эффективность. Одной из таких характеристик является время до отказа безопасности, определяемое как время, прошедшее с момента $t = 0$ до момента попадания системы в конечное состояние, ассоциированное с успешной реализацией какой-либо из кибератак [3, 7, 8]. Приведём определение этой величины в рамках рассматриваемой марковской модели.

Определение 1. Время $T \in [0, +\infty)$, прошедшее с момента $t = 0$, когда система находилась в состоянии безопасности s_0, до момента $t = T$ попадания системы в финальное состояние s_{n+1}, называется *временем до отказа безопасности*.

Ясно, что T — непрерывная случайная величина. Исследуем подробнее её вероятностное распределение.

Пусть $F_T(t)$ — функция распределения непрерывной случайной величины T, а $f_T(t)$ — её плотность распределения. Считая, что $F_T(t)$ — дифференцируемая функция, имеем $f_T(t) = F'_T(t)$. По своему смыслу значение функции распределения в момент t даёт вероятность того, что величина T будет меньше либо равна t, то есть $F_T(t) = P\{T \leqslant t\}$. Указанная вероятность, в свою очередь, совпадает с вероятностью того, что в момент t система находится в состоянии s_{n+1}: $F_T(t) = p_{n+1}(t)$. Отсюда мы имеем $f_T(t) = p'_{n+1}(t)$ или в силу равенства (8):

$$
f_T(t) = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu e^{\sigma_\nu t}. \tag{11}
$$

Нетрудно убедиться, что полученная функция действительно удовлетворяет условию нормировки, так как

$$
\int\limits_0^{+\infty} f_T(t)dt = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu \int\limits_0^{+\infty} e^{\sigma_\nu t}dt = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu \cdot \frac{1}{\sigma_\nu} = \sum_{\nu=1}^{n+1} c_{\nu,n+1} = 1,
$$

где мы учли условие (9).

Получим теперь формулы, в соответствии с которыми мы сможем вычислять числовые характеристики времени до отказа безопасности в терминах собственных значений и собственных векторов матрицы П.

Предложение 2. *k-ые начальные моменты случайной величины T даются формулой*

$$\mu_k[T] = -\sum_{\nu=1}^{n+1} \frac{c_{\nu,n+1}}{|\sigma_\nu|^k}, \tag{12}$$

где $c_{\nu,n+1}$ — $(n+1)$-ая компонента собственного вектора $\mathbf{c}_\nu$ матрицы (6)*, отвечающего собственному числу σ_ν. В частности, математическое ожидание $\tau \equiv \mu_1[T]$ случайной величины T вычисляется как*

$$\tau = \sum_{\nu=1}^{n+1} \frac{c_{\nu,n+1}}{\sigma_\nu}. \tag{13}$$

Доказательство. Используя формулы (8) и (11), в соответствии с определением k-го начального момента, имеем

$$\mu_k[T] = \int_0^{+\infty} t^k f_T(t)dt = \sum_{\nu=1}^{n+1} c_{\nu,n+1}\sigma_\nu \int_0^{+\infty} t^k e^{\sigma_\nu t}dt. \tag{14}$$

Так как $\sigma_\nu < 0$ для всех $\nu = 1, \ldots, n+1$, интегралы в правой части полученного равенства сходятся и равны:

$$\int_0^{+\infty} t^k e^{\sigma_\nu t}dt = \frac{k!}{|\sigma_\nu|^{k+1}}. \tag{15}$$

Подставляя (15) в (14), получаем формулу (12). В частности, при $k = 1$ мы приходим к формуле (13). ■

Определение 2. Математическое ожидание τ случайной величины T будем называть *средним временем до отказа безопасности*.

Очевидно, что среднее время до отказа безопасности является одним из показателей эффективности имеющихся средств защиты от кибератак. В частности, на основе данной числовой характеристики мы можем сделать вывод о достаточности применяемых механизмов защиты или, напротив, о необходимости добавочных инвестиций в кибербезопасность.

Приведём несколько примеров вычисления среднего времени до отказа безопасности.

ПРИМЕР 4 (случай отсутствия защиты). Если $r_i = 0$ для всех i, тогда собственные числа матрицы П равны $\sigma_0 = 0$, $\sigma_1 = -\mu_1$, $\ldots$, $\sigma_n = -\mu_n$, $\sigma_{n+1} =$

$-\lambda_0$. Соответствующие собственные векторы $\mathbf{c}_\nu$, удовлетворяющие требованию $\sum_{\nu=0}^{n+1} \mathbf{c}_\nu = \mathbf{e}_0$, имеют вид

$$\begin{aligned}
&\mathbf{c}_0 = (0, 0, 0, \ldots, 0, 1)\,,\\
&\mathbf{c}_1 = \left(0, \frac{\lambda_1}{\lambda_0 - \mu_1}, 0, \ldots, 0, -\frac{\lambda_1}{\lambda_0 - \mu_1}\right),\\
&\mathbf{c}_2 = \left(0, 0, \frac{\lambda_2}{\lambda_0 - \mu_2}, \ldots, 0, -\frac{\lambda_2}{\lambda_0 - \mu_2}\right),\\
&\ldots\\
&\mathbf{c}_n = \left(0, 0, 0, \ldots, \frac{\lambda_n}{\lambda_0 - \mu_n}, -\frac{\lambda_n}{\lambda_0 - \mu_n}\right),\\
&\mathbf{c}_{n+1} = \left(1, -\frac{\lambda_1}{\lambda_0 - \mu_1}, -\frac{\lambda_2}{\lambda_0 - \mu_2}, \ldots, -\frac{\lambda_n}{\lambda_0 - \mu_n}, \sum_{j=1}^{n} \frac{\lambda_j}{\lambda_0 - \mu_j} - 1\right).
\end{aligned}$$

Отсюда согласно формуле (13) для величины τ получаем следующее выражение

$$\tau = \frac{1}{\lambda_0}\left(1 + \sum_{i=1}^{n} \frac{\lambda_i}{\mu_i}\right). \tag{16}$$

В частности, при $n = 1$ имеем $\tau = 1/\lambda_1 + 1/\mu_1$. Данный результат имеет простое толкование: время τ есть сумма среднего времени до кибератаки $1/\lambda_1$ и среднего времени продолжительности атаки $1/\mu_1$.

Таким образом, при отсутствии защиты среднее время до отказа безопасности может быть найдено в аналитическом виде.

ПРИМЕР 5. В общем случае получение аналитических выражений для τ громоздко, поэтому предпочтительнее вычислять эту метрику безопасности численно. Рассмотрим, например, систему с входными параметрами, указанными в примере 3 из предыдущего раздела. Так как собственные значения и собственные векторы матрицы П для этого примера выше уже найдены, сразу же воспользуемся формулой (13):

$$\tau = \frac{0.0615}{-9.5462} + \frac{0.0421}{-0.9374} + \frac{-0.4972}{-0.8529} + \frac{-0.6064}{-0.3335} = 2.34967.$$

Отметим, что если допустить, что в этом примере все $r_i = 0$, а λ_i и μ_i остаются неизменными, по формуле (16) мы бы получили оценку

$$\tau_{\min} \equiv \tau|_{r=0} = 1.7371,$$

то есть, как и ожидается, $\tau_{\min} < \tau$ в силу того, что присутствие защитных механизмов увеличивает среднее время до отказа безопасности.

В заключение этого раздела сформулируем алгоритм нахождения среднего времени до отказа безопасности.

`Шаг 1.` По заданным входным параметрам модели λ, μ и r, формируем матрицу П в соответствии с формулой (6).

Шаг 2. Находим собственные числа σ_ν и собственные векторы $\mathbf{c}_\nu = (c_{\nu,i})$ матрицы Π.

Шаг 3. Решаем систему линейных однородных уравнений $\sum_{\nu=0}^{n+1} a_\nu c_{\nu,i} = \delta_{0,i}$ на неизвестные a_ν и делаем замену $\mathbf{c}_\nu \to a_\nu \mathbf{c}_\nu$ для всех $\nu = 0, 1, \ldots, n+1$.

Шаг 4. В соответствии с формулой (13) вычисляем среднее время до отказа безопасности τ.

4. Сравнение с результатами имитационного моделирования

Для оценки адекватности приведённых выше аналитических результатов проведём их сравнение с результатами, полученными в ходе имитационного моделирования.

Имитационное моделирование марковской цепи с непрерывным временем, описанной в разделе 1, осуществлялось нами с помощью пакета прикладных программ MatLAB. Для этих целей мы реализовали следующий набор функций:

- `GetErlang`(λ, k) — моделирование случайной величины, имеющей распределение Эрланга k-го порядка с параметром $\lambda > 0$;
- `GetState`(X, λ, μ, r, k) — разыгрывание нового случайного состояния марковской цепи при условии, что в настоящий момент система находится в состоянии X; λ, μ и r — векторные параметры модели, k — порядок потока Эрланга;
- `LifeTime`(λ, μ, r, k) — разыгрывание частной реализации марковской цепи и вычисление соответствующего этой реализации времени до отказа безопасности.

В частности, опишем подробнее алгоритм работы функции `GetState`.

Состояние X марковской цепи представляется парой (t, m), где t — момент времени, в который система перешла в это состояние, m — номер состояния, $m = 0, 1, \ldots, n+1$. Функция `GetState` осуществляет переход $X \to X'$, где $X = (t, m)$ — текущее состояние цепи, $X' = (t', m')$ — новое состояние, в которое переходит марковская цепь. При этом в зависимости от значения m мы имеем следующие варианты данного перехода.

1. Пусть $m = 0$ (система находится в безопасном состоянии). Тогда с помощью функции `GetState` мы генерируем n случайных чисел $\tau_1, \ldots, \tau_n$, распределённых по пуассоновскому закону с параметрами $\lambda_1, \ldots, \lambda_n$ соответственно. Пусть $\tau_i = \min\{\tau_1, \ldots, \tau_n\}$ для некоторого $i \in \{1, \ldots, n\}$. Полагаем $t' = t + \tau_i$ и $m' = m + i$, то есть $X' = (t + \tau_i, i)$.

2. Пусть $1 \leqslant m \leqslant n$ (осуществляется m-ая кибератака). С помощью функции `GetState` генерируем случайное число τ, распределённое по пуассоновскому закону с параметром μ_m, после чего полагаем $t' = t + \tau$. Далее с помощью штатной функции `rand`, входящей в состав ядра MATLab, разыгрываем случайное число x, равномерно распределённое на отрезке $[0, 1]$. Если $x < r_m$, полагаем $m' = 0$; в обратном случае имеем $m' = n + 1$.

3. Пусть $m = n + 1$ (состояние «отказ безопасности»). Тогда полагаем $t' = t$ и $m' = m$, то есть $X' = X$.

Используя функцию `GetState`, мы можем разыгрывать различные реализации марковской цепи, то есть последовательности состояний вида

$$X_0 = (t_0, m_0) \to X_1 = (t_1, m_1) \to \cdots \to X_N = (t_N, m_N) \to \ldots.$$

Реализации, начинающиеся с состояния $X_0 = (0, 0)$, генерируются функцией `LifeTime`. При этом переходы $X \to X'$ осуществляются до тех пор, пока мы не получим $X' = (t_M, n + 1)$ для некоторого $M \in \mathbb{N}$. Выходное значение функции `LifeTime` — это число t_M, которое и представляет собой время до отказа безопасности, отвечающее данной реализации.

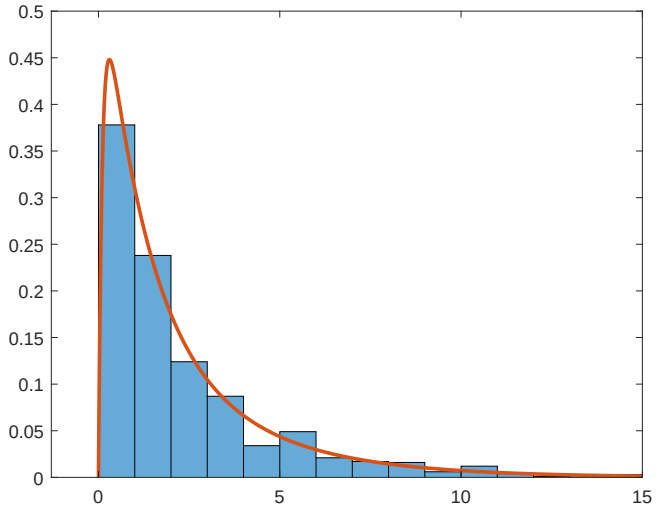

Рис. 3. Сравнение теоретической плотности распределения времени до отказа безопасности (сплошная кривая) с гистограммой, полученной по результатам имитационного моделирования

ПРИМЕР 6. В качестве конкретного примера проведём сравнение результатов, полученных в примерах 3 и 5, с результатами имитационного моделирования. Для этого $N = 1000$ раз мы запустим функцию `LifeTime`, выбрав в качестве значений параметров n, λ, μ и r величины (10). В результате получим 1000 возможных значений времени до отказа безопасности. На рис. 3 приведена гистограмма, построенная по полученным данным, а также теоретическая кривая плотности вероятности $f_T(t)$, полученная в результате дифферецирования функции $p_4(t)$, найденной в примере 3:

$$f_T(t) = -0.5869e^{-9.5462t} - 0.0395e^{-0.9374t} + 0.4240e^{-0.8529t} + 0.2022e^{-0.3335t}.$$

Из рисунка видно, что теоретическая и эмпирическая зависимости хорошо соответствуют друг другу.

Приведём также оценки для среднего времени до отказа безопасности, полученные в результате усреднения статистических испытаний, сводящихся к N запускам функции `LifeTime`. В таблице 1 указаны подобные оценки для $N = 10^3$, 10^4, 10^5 и 10^6. В последнем столбце приведена точная оценка, полученная в теоретических расчётах.

Таблица 1. Оценки среднего времени до отказа безопасности в имитационной модели при различном числе испытаний N

Число испытаний N	10^3	10^4	10^5	10^6	∞
Среднее время до отказа безопасности τ	2.3755	2.3576	2.3550	2.3471	**2.3497**

Литература

1. Wang A.J.A. Information security models and metrics // Proceedings of the 43rd annual Southeast regional conference. 2005. V. 2. P. 178–184.
2. Purboyo T.W., Rahardjo B., Kuspriyanto. Security metrics: a brief survey // 2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering. IEEE. 2011. P. 79–82.
3. Almasizadeh J., Azgomi M.A. A stochastic model of attack process for the evaluation of security metrics // Computer Networks. 2013. V. 57, No. 10. P. 2159–2180.
4. Росенко А.П., Бордак И.В. Математическая модель определения вероятности последствий от реализации злоумышленником угроз безопасности информации ограниченного распространения // Известия Южного федерального университета. Технические науки. 2015. № 7(168). С. 6–19.
5. Drazin M.P., Haynsworth E.V. Criteria for the reality of matrix eigenvalues // Mathematische Zeitschrift. 1962. V. 78, No. 1. P. 449–452.
6. Хорн Р., Джонсон Ч. Матричный анализ. М. : Мир, 1989.
7. Le N.T. et al. A threat computation model using a Markov Chain and common vulnerability scoring system and its application to cloud security // Australian Journal of Telecommunications and the Digital Economy. 2019. V. 7, No. 1. P. 37.
8. Jouini M., Rabai L.B.A. Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study // Journal of Computers. 2015. V. 10, No. 3. P. 184–194.

EVALUATING MEAN TIME TO SECURITY FAILURE BASED ON CONTINUOUS-TIME MARKOV CHAINS

A. A. Magazev
Dr.Sc.(Phys.-Math.), Professor, Department of Complex Information Security,
e-mail: magazev@omgtu.ru
A. S. Melnikova
Undergraduate, Department of Complex Information Security,
e-mail: anastasiya_m.96@mail.ru
V. F. Tsyrulnik
Postgraduate, Department of Complex Information Security,
e-mail: lera.tsyrulnik@mail.ru

Omsk State Technical University, Omsk, Russia

Abstract. In the article, we consider a Markov model of computer attacks, in the framework of which attacks and the system responses are modelled by homogeneous Poisson point processes. We describe a method of solving the corresponding Kolmogorov system of equations by calculating eigenvalues and eigenvectors of some matrix. An important random variable associated with the corresponding Markov chain and called the time to security failure is explored in detail. The comparison of the results obtained and the results of simulation modelling are presented.

Keywords: continuous-time Markov chain, Kolmogorov's equations, mean time to security failure.

References

1. Wang A.J.A. Information security models and metrics. Proceedings of the 43rd annual Southeast regional conference, 2005, vol. 2, pp. 178–184.
2. Purboyo T.W. and Rahardjo B., Kuspriyanto. Security metrics: a brief survey. 2011 2nd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering, IEEE, 2011, pp. 79–82.
3. Almasizadeh J. and Azgomi M.A. A stochastic model of attack process for the evaluation of security metrics. Computer Networks, 2013, vol. 57, no. 10, pp. 2159–2180.
4. Rosenko A.P. and Bordak I.V. Matematicheskaya model' opredeleniya veroyatnosti posledstvii ot realizatsii zloumyshlennikom ugroz bezopasnosti informatsii ogranichennogo rasprostraneniya. Izvestiya Yuzhnogo federal'nogo universiteta, Tekhnicheskie nauki, 2015, no. 7(168), pp. 6–19. (in Russian)
5. Drazin M.P. and Haynsworth E.V. Criteria for the reality of matrix eigenvalues. Mathematische Zeitschrift, 1962, vol. 78, no. 1, pp. 449–452.
6. Khorn R., Dzhonson Ch. Matrichnyi analiz. Moscow, Mir Publ., 1989. (in Russian)
7. Le N.T. et al. A threat computation model using a Markov Chain and common vulnerability scoring system and its application to cloud security. Australian Journal of Telecommunications and the Digital Economy, 2019, vol. 7, no. 1, pp. 37.
8. Jouini M. and Rabai L.B.A. Mean Failure Cost Extension Model towards Security Threats Assessment: A Cloud Computing Case Study. Journal of Computers, 2015, vol. 10, no. 3, pp. 184–194.

Дата поступления в редакцию: 26.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 126–135

УДК 004.056
DOI 10.24147/2222-8772.2020.4.126-135

О ПРЕДСТАВЛЕНИИ НЕКОТОРЫХ РОЛЕВЫХ МОДЕЛЕЙ РАЗГРАНИЧЕНИЯ ДОСТУПА ОБЪЕКТНО-ОРИЕНТИРОВАННОЙ МОДЕЛЬЮ HRU: НАСЛЕДОВАНИЕ ТАКСОНОМИЧЕСКИМ ЛИСТОВЫМ МЕТОДОМ

С.В. Усов
к.т.н., доцент, e-mail: raintower@mail.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Рассматривается возможность представления ролевых политик безопасности с помощью объектно-ориентированных дискреционных моделей разделения доступа. Рассмотрена ролевая модель с иерархией, в которой эксплуатируется таксономический листовой метод наследования. Полномочия ролевой модели представлены в виде наборов пар «объект-право доступа». Построена иерархия классов модели OOHRU, отражающая ролевую политику разграничения доступа. Описаны команды модели OOHRU, соответствующие переназначению ролей в исходной модели.

Ключевые слова: ролевые модели разграничения доступа, OOHRU, иерархия ролей.

Введение

Данная работа является прямым продолжением работы «О представлении некоторых ролевых моделей разграничения доступа объектно-ориентированной моделью HRU» [1], опубликованной двумя годами ранее. По этой причине позволим себе сократить как историческую справку, так и описание рассматриваемых моделей до минимума.

Рассматривается объектно-ориентированное развитие [4] дискреционной модели разграничения доступа, предложенной Харриссоном, Руззо и Ульманом [2]. Объектно-ориентированный подход позволил как расширить охват компьютерных систем, которые можно описать с помощью модели HRU, так и сделал исходную модель совместимой с рядом актуальных задач.

Напомним, что компьютерная система в OOHRU рассматривается в виде множества объектов $\mathbf{O}$, разбитых по множеству классов $\mathbf{K}$ (все объекты одного класса имеют одинаковый набор полей и методов), обладающих открытыми полями $f \in \mathbf{F}$ и скрытыми полями $p \in \mathbf{P}$, а также методами обработки полей $s \in \mathbf{S}$. Здесь $F = \bigcup_{k \in \mathbf{K}} k.\mathbf{F}$ — множество всевозможных открытых полей всех объектов и классов, $k.\mathbf{F}$ — множество открытых полей класса k (каждый объект класса k обладает тем же набором $k.\mathbf{F}$ открытых полей), аналогично

определяются $\mathbf{P}$ и $\mathbf{S}$. Причём если поле $k.f$ наследуется классом k у класса k', то соответствующее поле класса k' мы будем для удобства обозначать именно $k'.f$, подчёркивая тем самым их взаимосвязь (таким образом, $f \in k.\mathbf{F}$ и $f \in k'.\mathbf{F}$). Пусть $\mathbf{O}^k \in \mathbf{O}$ — множество объектов класса $k \in \mathbf{K}$. В случае, если требуется уточнить класс объекта, поле f объекта $o^k \in \mathbf{O}^k$ будем обозначать $o^k.f$, поле f класса k — $k.f$. Для скрытых полей класса будем использовать аналогичные обозначения.

1. Построения модели дискреционного разделения доступов

Для построения модели дискреционного разделения доступов для каждого объекта и для каждого класса вводится дополнительное скрытое поле M, содержащее локальную матрицу доступов, и методы работы с матрицей доступов. Строки матрицы доступов объекта o соответствуют объектам и классам системы, столбцы – полям и методам объекта o, а в ячейке, находящейся на пересечении строки, соответствующей объекту o', и столбца, соответствующего полю либо методу $x \in \mathbf{X} = \mathbf{F} \cup \mathbf{S}$, находится подмножество множества R прав доступа, определённых в системе, которое обозначается $o.M[o', x]$. Модификация матриц доступа производится посредством выполнения команд системы безопасности, о которых будет сказано ниже.

Модель безопасности OOHRU называется иерархической (или моделью с иерархией), если на множестве объектов $\mathbf{O}$ задан частичный порядок-иерархия и в любой момент работы системы для любых двух объектов $o, o' \in \mathbf{O}$ таких, что $o' \leqslant o$ для любого поля или метода $x \in \mathbf{X}$, общего для объектов o и o', и для любого поля или метода $x' \in \mathbf{X}$ объекта $o'' \in \mathbf{O}$ верно следующее: $o''.M[o, x'] \subset o''.M[o', x']$ и $o'.M[o'', x] \subset o.M[o'', x]$. Здесь и далее «$\leqslant$» – отношение частичного порядка, задающее иерархию.

Состояние системы в модели HRU изменяется под действием команд, которые состоят из условной части и последовательности элементарных операторов [2], которая выполняется, только если истинна условная часть. Список элементарных операторов в OOHRU включает [4]:

1. $Create(o^k, k)$ — создаёт объект o^k класса $k \in \mathbf{K}$, если $o^k \in \mathbf{O}$.
2. $Destroy(o^k)$ — уничтожает объект $o^k \in \mathbf{O}$.
3. $Enter(r, o^k, o'^{k'}.f)$ — вносит право доступа r в $o'^{k'}.M[o^k, o'^{k'}.f]$, где o^k — объект класса k, $o'^{k'}$ — объект класса k'.
4. $Delete(r, o^k, o'^{k'}.f)$ — удаляет право доступа r из $o'^{k'}.M[o^k, o'^{k'}.f]$.
5. $Grant(r, o^k, o'^{k'}.s)$ — разрешает вызов объектом o^k метода $o'^{k'}.s$.
6. $Deprive(r, o^k, o'^{k'}.s)$ — запрещает вызов объектом o^k метода $o'^{k'}.s$.

Изменения, производимые операторами, отражаются в матрицах доступа объектов системы. Подробное описание модели OOHRU можно найти в [4].

Также рассматриваются ролевые политики разграничения доступа [3].

Компьютерная система в рамках ролевой политики представляется совокупностью следующих множеств: множества пользователей U, множества ролей

Z, множества полномочий **Y** и множества сеансов работы пользователей с системой [3]. Обратим внимание, что использование нестандартных обозначений здесь вызвано необходимостью избежать конфликта с описанием модели HRU, где те же символы несут иную смысловую нагрузку по сравнению с классическими обозначениями сущностей, принятыми в ролевой модели.

Множество объектов системы не задаётся в явном виде, а представляется через множество полномочий **Y**: каждое полномочие заключает в себе отношение на декартовом произведении множества прав доступа и множества объектов системы, однако фактически каждое «элементарное» полномочие можно представить в виде пары $y = (x, r)$, где x отвечает объекту системы (или группе сходных объектов) в рамках субъектно-объектной парадигмы, а r – праву доступа к этому объекту (или группе объектов). В качестве r может также выступать право вызова, если x представляет собой активную сущность системы. Сформированное таким образом множество всех объектов системы обозначим через X, а множество всех прав доступа — через R.

Далее, пусть $z.y$ — обозначение элементарного полномочия y, относящегося к роли z (поскольку каждая роль задаётся именно набором полномочий), соответственно, $z.Y$ — полный набор полномочий роли z, $z.Y \subset Y$.

Управление доступом осуществляется на основе изменения множества активных сеансов системы. Каждому сеансу $c \in C$ сопоставляется пользователь $u_c \in U$, подмножество доступных пользователю в рамках данного сеанса ролей $Z_c \subset \mathbf{Z}$ и подмножество допустимых полномочий $Y_c \subset \mathbf{Y}$. Считается, что система функционирует безопасно, если пользователь u_c может осуществлять действия только в рамках полномочий из множества $Y_c = \bigcup_{z \in Z_c} z.Y$ во время сеанса $c \in C$.

На множестве ролей в реальных системах обычно возникает иерархия, индуцированная организационно-управленческими схемами организаций, в которых эксплуатируется система. Как правило, подчинённость ролей в иерархии включает наследование прав и полномочий, которое может быть направлено как «снизу», так и «сверху». При наследовании «сверху» подчинённый субъект наследует права родительских субъектов. Однако базовые ролевые модели эксплуатируют наследование «снизу». Здесь можно выделить три ключевых подхода к построению иерархии.

1. Строгий таксономический листовой подход. Всё множество полномочий разбивается на непересекающиеся подмножества, каждое из подмножеств приписывается листу дерева иерархии ролей. Роль в нелистовой вершине наделяется множеством полномочий, являющимся объединением множеств полномочий непосредственно подчинённых ролей (соответствие между ролями и полномочиями, таким образом, индуцируется полномочиями листовых вершин и устанавливается при движении по дереву ролей снизу вверх).

2. Нестрогий таксономический листовой подход. Единственное отличие от предыдущего подхода — отсутствие требования на запрет пересечения подмножеств полномочий, сопоставленных листовым вершинам.

3. Иерархически охватный подход. Граф такой иерархии ролей не обязан быть деревом (но, конечно, не может содержать сильных циклов). При таком

подходе считается, что если пользователю сопоставлена некоторая роль $r \in \mathbf{R}$, то ему также должны быть сопоставлены и все роли, подчинённые r. Что позволяет исключить из роли r полномочия, уже содержащиеся в подчинённых ей ролях.

В работе [4] была предложена иерархическая модель OOHRU, устройство которой подразумевает, что объект o, находящийся на более низком уровне иерархии, чем объект o', обладает меньшим набором прав (как в отношении доступа к другим объектам, так и в отношении ограничения доступа других объектов по отношению к себе) по сравнению с объектом o'. Такая структура напоминает решётку иерархии ролей, что позволяет предположить структурную близость данных моделей.

Целью данной работы является именно моделирование ряда ролевых политик безопасности средствами OOHRU. Связь между субъектно-объектной ролевой моделью без иерархии на множестве ролей и OOHRU, равно как и связь между субъектно-объектной ролевой моделью с иерархией с наследованием «сверху» на множестве ролей и OOHRU, были изучены в работе [1]. Здесь будет разобран случай ролевой модели с таксономическим листовым подходом к организации иерархии ролей.

2. Связь между субъектно-объектной ролевой моделью с иерархией на множестве ролей и OOHRU: случай таксономического листового подхода к наследованию

В этом разделе нас будет интересовать ролевая политика безопасности с таксономическим листовым подходом к наследованию.

Базовая ролевая политика разграничения доступа подразумевает статичность подсистемы безопасности в рамках одного сеанса, то есть полномочия неизменны, к каждой роли относится фиксированный набор полномочий, и каждому пользователю назначен неизменный в течение сеанса набор ролей. Таким образом, перераспределения прав доступа в смысле дискреционной политики безопасности не происходит. Построим иерархическую объектно-ориентированную модель HRU $\Sigma' = (O(t), M(t), K, R)$, соответствующую данной субъектно-объектной ролевой модели $\Sigma = (U, Z, Y, C)$.

Во-первых, сформируем множество R прав доступа модели Σ', вычленив права доступа r из элементарных полномочий, а также множество X объектов системы.

Во-вторых, зададим классы объектов, а также вспомогательные класс пользователей и класс сеансов: в реализующей ролевую политику с иерархией модели OOHRU они задаются так же, как и в случае реализации ролевой политики без иерархии на множестве ролей [1].

В частности, пассивной сущности $x \in X$ субъектно-объектной модели будет соответствовать объект o, имеющий поле f, содержащее информацию объекта x, и приватное поле M — матрицу доступов. Активной сущности x' субъектно-объектной модели будет соответствовать объект o', содержащий метод s, вы-

полняющий активные функции субъекта x', и приватное поле M — матрицу доступов. Объекты будут в дальнейшем разбиты по классам исходя из их структуры и возможностей доступа к ним. Каждой роли $z \in Z$ также будет сопоставлен класс $k_z \in K$ в модели OOHRU.

Заполнение матриц доступов объектов происходит следующим образом: если роль $z \in Z$ обладает элементарным полномочием $y = (x, r) = (o.f, r)$, где x — объект субъектно-объектной модели, объектно-ориентированной интерпретацией которого является объект o, то в матрицу доступов объекта o в ячейку на пересечении строки поля f и столбца класса k_z заносится право доступа r: $o.M[k_z, f] := o.M[k_z, f] \cup r$. Если же роль $z \in Z$ обладает элементарным полномочием $y = (x', r) = (o'.s, r)$, где x' — субъект субъектно-объектной модели, объектно-ориентированной интерпретацией которого является объект o', а r — право вызова процедуры, то в матрицу доступов объекта o в ячейку на пересечении строки метода f и столбца класса k_z заносится 1: $o.M[k_z, f] := 1$.

Осталось построить лишь иерархию классов ролей.

Иерархия классов ролей в OOHRU будет повторять иерархию ролей в исходной ролевой модели, только в отражённом виде. Каждой роли z будет сопоставлен класс k_z, кроме того, введём класс k_0, отвечающий пустому множеству ролей. Его наследниками будут классы, соответствующие листовым вершинам в дереве ролей. Далее, если роль z является непосредственным потомком роли z' в таксономической модели (при этом набор полномочий $z.Y$ роли z будет содержаться в наборе полномочий $z'.Y$ роли z'), то класс $k_{z'}$ будет непосредственным потомком класса k_z в OOHRU.

В дальнейшем мы будем называть такую иерархию в OOHRU таксономической иерархией ролей.

Если пользователь $u \in U$ при авторизации на сеанс $c \in C$ получает роль z, то в модели Σ' в классе k_z создаётся новый объект o_u. Каждый такой объект содержит в качестве private-поля собственную матрицу доступов (заполняется при создании объекта на основе совокупности всех элементарных полномочий, которыми обладает пользователь u во время сеанса c), поле идентификатора и методы, необходимые для работы с объектами системы. Так, например, каждому полномочию может соответствовать свой метод.

Дополним OOHRU командой старта сеанса с пользователем u с авторизацией его на роль z и командой завершения сеанса:

$CommandStartSession_z(o_u : k_z)$
$\quad Create(o_u, k_z).$

Команда завершения сеанса этим же пользователем:

$CommandEndSession_z(o_u : k_z)$
$\quad Destroy(o_u).$

Тот факт, что перед стартом сеанса выполняется проверка возможности пользователю u назначить роль z, может быть также отражён исключительно средствами модели OOHRU. Для этого вне иерархии введём два дополнительных класса: класс сеансов k_C и класс пользователей k_U. Для каждого сеанса c в класс k_C помещается объект o_c, содержащий поле-идентификатор сеанса,

метод $user$ инициализации пользователя и матрицу доступов. Для каждого пользователя u в класс k_U помещается объект o_u^*, содержащий метод $user$ и матрицу доступов. Аналогичный метод $user$ будут содержать все классы и объекты естественной иерархии подмножеств ролей. Роль этого метода формальна, нам потребуется лишь соответствующая ему ячейка в матрице доступов содержащего его объекта (класса).

Положим, что сеанс c подразумевает назначение пользователю u роли z. В этом случае при создании объекта o_c происходит модификация матриц доступа объекта o_u^* и класса k_z следующей командой:

$CommandCreateSession_z(o_c : k_C; o_u^* : k_U; k_z)$
$Create(o_c, k_C)$,
$Grant(o_c, o_u^*.user)$,
$Grant(o_c, k_z.user)$.

При выполнении этой команды матрицы доступов модифицируются следующим образом: $o_u^*.M[o_c, user] = 1$, $k_z.M[o_c, user] = 1$ (объект o_c получает право запускать метод $user$ объекта o_u^*, относящегося к пользователю u, и аналогичный метод класса k_z). Команда может быть выполнена, только если пользователь u зарегистрирован в системе, при регистрации был создан соответствующий ему объект o_u^*.

Теперь в команду сеанса мы можем включить проверку возможности пользователю u назначить роль z:

$CommandStartSession_z(o_c : k_C; o_u^* : k_U; o_u : k_z)$
If
$o_u^*.M[o_c, p_u] = 1$ and $kz.M[o_c, p_u] = 1$
then
$Create(o_u, k_z)$.

Существенное отличие от случая ролевой модели без иерархии заключается в том, что каждый пользовательский объект в индуцированной иерархии ролей соответствует одной роли из числа назначенных субъекту. В информационных системах, эксплуатирующих таксономический листовой подход к построению иерархии ролей, можно выделить два ключевых случая сочетания назначенных пользователю ролей.

Первый случай подразумевает назначение пользователю некоторого множества ролей из числа листовых (на прочие роли пользователь авторизован быть не может). В такой ситуации достаточно построить естественную иерархию подмножеств листовых ролей, игнорируя таксономическую листовую иерархию либо дополняя её. Фактически работа со множеством листовых ролей сводит данный случай к случаю ролевой модели, свободной от иерархии. Работа с созданием и удалением пользовательских объектов, переназначение ролей и полномочий происходит точно так же, как и в случае модели, свободной от иерархии [1].

Второй случай подразумевает назначение пользователю одной роли (не обязательно листовой), реже нескольких, из иерархии. В такой ситуации работа с созданием и удалением пользовательских объектов, переназначение ролей и

полномочий происходит аналогично случаю иерархии с наследованием «сверху».

Например, если необходимо назначить пользователю u роли z и z' в рамках уже построенной системы безопасности, достаточно создать при назначении пользователя на эти роли два отвечающих пользователю u объекта как в классе k_z, так и в классе $k_{z'}$:

$CommandStartSession_\{z, z'\}(o_u : k_z, o'_u : k_{z'})$
$\quad Create(o_u, k_z),$
$\quad Create(o'_u, k_{z'}).$
$CommandEndSession_\{z, z'\}(o_u : k_z, o'_u : k_{z'})$
$\quad Destroy(o_u),$
$\quad Destroy(o'_u).$

Аналогичные команды можно использовать для произвольного набора ролей α.

Как и в случае ролевой модели, свободной от иерархии, для смены набора назначенных ролей α на набор β пользователю необходимо завершить текущий сеанс и начать новый, в котором ему будет назначен требуемый набор ролей.

Рассмотрим, как может осуществляться модификация множества полномочий, назначенных роли z.

1) Только листовые роли могут быть назначены пользователю. Ролевая модель реализована с помощью естественной иерархии модели OOHRU. В этом случае наблюдается полное соответствие случаю ролевой модели без иерархии, случай которой был изучен в работе [1].

2) Только листовые роли могут быть назначены пользователю. При этом естественная иерархия в модели OOHRU не построена. В этом случае под каждую роль z, назначенную пользователю u, был создан отдельный объект o_z класса k_z. Модификация каждой отдельной роли осуществляется независимо с помощью команд вида:

$CommandAddPermission_z_r_f(k_z, o : k_o)$
$\quad Enter(r, k_z, o.f).$

Данная команда не нарушает наследование прав доступа в иерархии, поскольку в OOHRU оператор $Enter$ может быть выполнен, только если соблюдены так называемые условия целостности:

$$(r \in o.M[k_{z_1}, f])\& \ldots \&(r \in o.M[k_{z_s}, f])[4].$$

При необходимости добавить более широкий набор полномочий, расширяем список элементарных операторов $Enter$ в команде, добавляющих требуемые права доступа. Если элементарное полномочие содержит право вызова метода s объекта o некоторого класса k_o, используем команду несколько иного вида:

$CommandAddPermission_z_s(k_z, o : k_o)$
$\quad Grant(k_z, o.s).$

Удаление элементарного полномочия осуществляется аналогичным способом, только условия целостности будут наложены уже на родительские классы:

$CommandDeletePermission_z_r_f(k_z, o : k_o)$
$\quad Delete(r, k_z, o.f)$.

Отметим, что данный подход применим и в том случае, когда возможно назначение пользователю не только листовых ролей. Важно лишь, чтобы для каждой роли пользователя создавался отдельный пользовательский объект. В не подпадающих под это правило ситуациях необходимо воспользоваться рецептом, предложенным в одном из трёх оставшихся случаев.

3) Случай таксономически строгого подхода. Добавим в систему дополнительно роли z_y для каждого элементарного полномочия $y = (x, r)$, где $x \in X$ — объект, $r \in R$ – допустимое право доступа к этому объекту. Если $y \in z.Y$, то соответствующий этой роли класс k_y будет являться непосредственным наследником класса k_0 и непосредственным родителем класса k_z. При этом $r \in o.M[k_y, o.f]$ либо $o.M[k_y, o.p] = 1$, в зависимости от того, представляет ли элементарное полномочие y возможность доступа r к полю f объектно-ориентированной интерпретации o объекта x или же возможность вызова метода p объектно-ориентированной интерпретации o субъекта x. Далее рассмотрим случай с полем объекта (случай с методом субъекта аналогичен).

Во-первых, согласно условиям целостности все потомки класса k_y (то есть классы, соответствующие ролям, содержащим полномочие y) будут обладать правом r в соответствующей ячейке права доступа. При необходимости отозвать полномочие y у роли z (а значит и у всех ролей, ранее его содержавших, поскольку мы работаем в рамках таксономического листового подхода), необходимо применить команды вида:

$CommandDeletePermission_\alpha_r_f(k_\alpha, o : k_o)$
$\quad Delete(r, k_\alpha, o.f)$

ко всем классам таксономической иерархии, начиная с классов, содержащих (по включению) наимощнейшие наборы полномочий (классы, соответствующие самым верхним ролям или наборам ролей α в иерархии ролей), и заканчивая классами листовых ролей и далее классами листовых полномочий (на самом деле, среди последних удаление права пройдёт успешно только для класса k_y, поскольку остальные классы полномочий изначально не содержали этого права в соответствующей ячейке матрицы доступов). При таком просмотре графа ролей, «сверху вниз», условия целостности будут выполнены на всех этапах.

Для возвращения отозванного полномочия применяем команды вида

$CommandAddPermission_\alpha_r_f(k_\alpha, o : k_o)$
$\quad Enter(r, k_\alpha, o.f)$,

на этот раз начиная с класса полномочия y и классов листовых ролей, при этом двигаясь в обратном направлении, «снизу вверх» по таксономическому графу иерархии ролей.

4) Случай нестрогого таксономического подхода. В этом случае мы не можем воспользоваться конструкцией из предыдущего случая, поскольку одно и то же полномочие может принадлежать сразу нескольким листовым ролям, а удалить его нам может понадобиться только из одной листовой роли. Будем использовать команды того же вида, что и в строгом случае (разве что не станем

создавать классы полномочий), но несколько изменим порядок их применения.

Алгоритм отзыва полномочия y у роли z (все описанные ниже операции осуществляются инструментами модели OOHRU, описанными в случае 3 и ранее).

Шаг 1. Двигаясь (здесь и далее по графу дерева ролей при обходе «в ширину») сверху вниз, удаляем полномочие y у всех ролей.

Шаг 2. Добавляем полномочие y во все листовые роли, кроме роли z из числа тех, которым оно принадлежало ранее.

Шаг 3. Двигаясь снизу вверх, пытаемся добавить полномочие y во все обойдённые вершины. Благодаря условиям целостности мы сможем добавить его лишь тем ролям, которые «наследовали» бы его согласно устройству таксономической листовой иерархии ролей.

Алгоритм добавления полномочия y роли z гораздо проще: добавляем y листовой роли z средствами OOHRU и применяем Шаг 3 предыдущего алгоритма. Полномочие будет добавлено, куда положено, благодаря условиям целостности.

Тем самым доказана

Теорема 1. *Для любой субъектно-объектной иерархической ролевой модели с таксономическим листовым подходом к наследованию существует реализующая ее иерархическая модель OOHRU.*

Литература

1. Усов С.В. О представлении некоторых ролевых моделей разграничения доступа объектно-ориентированной моделью HRU // Математические структуры и моделирование. Омск : Ом. гос. ун-т, 2018. № 48. С. 127–137.
2. Harrison M.A., Ruzzo W.L., Ulman J.D. Protection in Operating Systems // Communications of the ACM. 1975. P. 14–25.
3. Ferraiolo D.F., Kuhn D.R. Role-Based Access Control // 15th National Computer Security Conference. 1992. P. 554–563.
4. Усов С.В. Об отношении между дискреционными моделями объектно-ориентированных и субъектно-объектных компьютерных систем // Проблемы информационной безопасности. Компьютерные системы. 2013. Т. 3. С. 18–26.

ON THE REPRESENTATION OF ROLE-BASED ACCESS CONTROL MODELS BY OBJECT-ORIENTED HRU MODEL: TAXONOMIC LEAF-BASED HIERARCHY CASE

S.V. Usov
Ph.D.(Eng.), Associate Professor, e-mail: raintower@mail.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. In this paper the possibility of representing of some types of role-based access control models by object-oriented discretionary access control model is considered. The role-based security models with taxonomic hierarchy are considered. The permissions of the role-based access control model are represented as a set of pairs of object and access right. A hierarchy of classes of the object-oriented HRU model, based on the role-based access control policy, is constructed. Commands of the object-oriented HRU model, corresponding to the reassignment of roles in the original role-based model, are described.

Keywords: role-based access control model, object-oriented discretionary access control model, role hierarchy.

References

1. Usov S.V. O predstavlenii nekotorykh rolevykh modelei razgranicheniya dostupa ob"ektno-orientirovannoi model'yu HRU. Matematicheskie struktury i modelirovanie, Omsk, Om. gos. un-t, 2018, no. 48, pp. 127–137. (in Russian)
2. Harrison M.A., Ruzzo W.L., and Ulman J.D. Protection in Operating Systems. Communications of the ACM, 1975, pp. 14–25.
3. Ferraiolo D.F. and Kuhn D.R. Role-Based Access Control. 15th National Computer Security Conference, 1992, pp. 554–563.
4. Usov S.V. Ob otnoshenii mezhdu diskretsionnymi modelyami ob"ektno-orientirovannykh i sub"ektno-ob"ektnykh komp'yuternykh sistem. Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy, 2013, vol. 3, pp. 18–26. (in Russian)

Дата поступления в редакцию: 30.10.20

Математические структуры и моделирование
2020. № 4(56). С. 136–147

УДК 004.05
DOI 10.24147/2222-8772.2020.4.136-147

ПРОЕКТИРОВАНИЕ МОДУЛЯ УВЕДОМЛЕНИЙ О СОБЫТИЯХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ УПРАВЛЕНИЯ УЧЕБНЫМ ПРОЦЕССОМ ОМГУ

О.А. Бондаренко
студент, e-mail: bondarenkoolga360@gmail.com
Е.А. Костюшина
к.т.н., доцент, e-mail: kea.omsu@gmail.com
Т.В. Олейникова
студент, e-mail: oleynikova.tan@gmail.com
Д.Н. Лавров
к.т.н., доцент, e-mail: lavrov@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. Статья посвящена особенностям проектирования модуля уведомлений в информационно-аналитической системе «Учебный процесс». В связи со сложностью и нелинейностью задачи решено было применить для исследования предметной области метод системного анализа. Кроме того, были рассмотрены существующие аналоги систем оповещения, что позволило определить максимально-возможный функционал модуля.

Ключевые слова: информационно-аналитическая система, события, учебный процесс.

Введение

Система уведомления о событиях ИИАС «Учебный процесс» — проект веб-модуля в рамках веб-приложения «Электронные сервисы ОмГУ» [5, 9], позволяющий пользователю получать уведомления с помощью электронном почты об изменениях в базе данных по событиям, на которые пользователь подписался и настроил в своём личном кабинете. Проект должен формировать уведомления по событиям информационной системы управления учебным процессом ОмГУ, учитывая группы пользователей, определённых во всех подсистемах системы, работать как для корпоративных ресурсов, так и для внешних ресурсов системы с точки зрения сети вуза. В настоящий момент в вузе для управления учебным процессом используется интегрированная информационно-аналитическая система «Учебный процесс» (ИИАС «Учебный процесс») [8].

В настоящий момент в ИИАС «Учебный процесс» пользователь не имеет возможности оперативно получать информацию об изменениях в базе данных (например, на кафедру переданы ресурсы, и их необходимо назначить преподавателю; студент через «Электронные сервисы ОмГУ» отправил заявку, и её нужно вовремя обработать).

Поэтому была поставлена задача спроектировать модуль формирования уведомлений в процессе фиксирования важных событий в виде данных в базе данных. Доступность настройки оповещения о событии должна быть привязана к привилегиям пользователя, предоставленным ему в информационной системе.

Для проектирования модуля в связи со сложностью и нелинейностью задачи решено было применить для исследования предметной области метод системного анализа. Кроме того, были рассмотрены существующие аналоги систем оповещения, что позволило определить в проекте максимально возможный функционал модуля.

1. Системный анализ предметной области

Целью применения системного анализа к проблеме является повышение степени обоснованности принимаемого решения, расширение множества вариантов, среди которых производится выбор, с указанием способов отбрасывания тех из них, которые заведомо уступают другим [6].

Рассматриваемую систему можно назвать сложной системой управления, так как в литературе определяется, что сложные системы «нельзя корректно описать математически либо потому, что в системе имеется очень большое число различных элементов, неизвестным образом связанных друг с другом, либо потому, что мы не знаем природы явлений, протекающих в системе, и потому не можем количественно их описать» [7].

Кроме того, если рассматривать модуль уведомления о событиях как явление, то оно обладает многомерностью (большие объёмы циркулирующих потоков информации, из которых отбираются данные для формирования списка событий), многообразием форм связи между элементами (многомерные, сетевые, линейные и др.), многообразием природы элементов (события о студентах, учебных ресурсах, учебных планах, преподавателях и т. п.), многократным изменением состояния структуры и состава системы [7].

Начнём с проектирования базы данных предметной области. При проектировании базы данных, необходимой для рассылки, будем учитывать тот факт, что она будет являться расширением уже существующей базы данных ИИАС «Учебный процесс» [8], поэтому в структуру были включены как новые таблицы, так и уже существующие таблицы (они выделены серым). ER-диаграмма представлена на рисунке 1.

При проектировании системы были учтены некоторые особенности.

1) Пользователь может самостоятельно настраивать уведомления, выбирая события из доступного ему списка. Администратор системы может управлять уведомлениями.
2) Для более легкого администрирования события были объединены в группы для разных типов пользователей. Это позволит уменьшить число уведомлений, получаемых пользователем.
3) При проектировании была учтена возможность редактировать или дополнять списки событий для каждой группы пользователей, чтобы не множить группы, а изменять текущую, добавляя или удаляя определённое

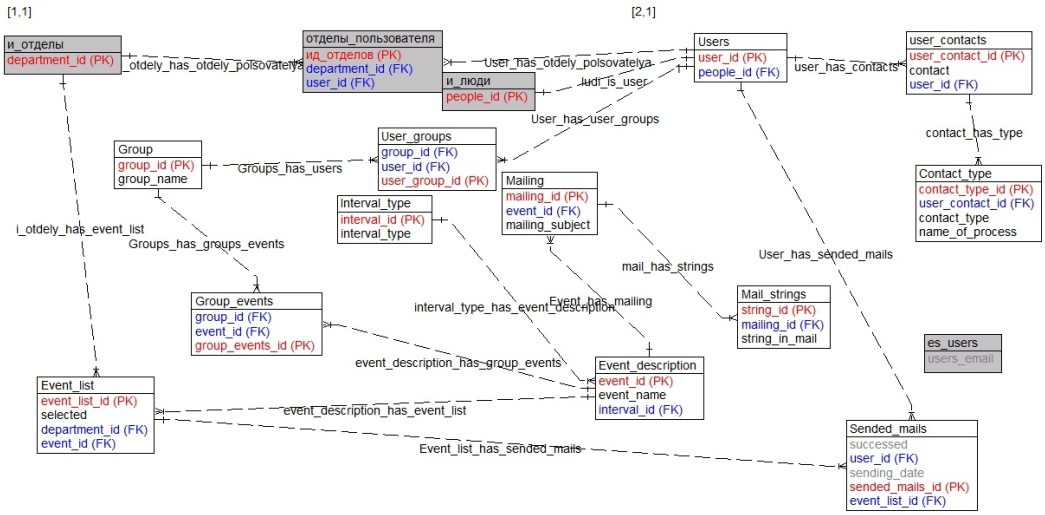

Рис. 1. ER-модель базы данных системы оповещений

событие для группы. Рассмотрим существующие аналоги систем уведомлений о событиях. Они предназначены для разного рода рассылок и, соответственно, имеют разную функциональность, но для проектирования нашего модуля важно выделить необходимый нам функционал (таблица 1).

Комментарии к таблице 1: «+» означает наличие данной функции, «-» — отсутствие, «?» — нет информации на этот счёт.

Ни одна из изученных систем не включает всего необходимого функцио-

Таблица 1. Сравнительный анализ сервисов массовых рассылок

Сфера применения	**Сервисы**	**Изменения статуса письма**			**Формирование шаблона**	**Возможность подписаться /отписаться от рассылки**	**Изменение данных пользователя**	**Возможность инициировать рассылку**	**Повторная отправка**	**Реакция на наступление события**
		отправлено	**доставлено**	**отклонено**						
Коммерция	Unisender [2]	+	+	+	-	+	+	+	+	+
	EmailChef [4]	+	+	+	+	+	+	+	+	+
Построение систем безопасности	Sigur [1]	?	?	?	?	+	?	+	?	+
Сфера оказания государственных услуг	Личный кабинет налогоплательщика	?	?	?	?	+	+	?	?	+
	Госуслуги [3]	?	?	?	?	+	+	?	?	+
Социальные сети	VK	?	?	?	?	+	+	?	-	+

нала, к тому же большинство аналогов сервисов массовой рассылки платные, поэтому было принято решение самостоятельно разработать систему уведомлений о событиях системы сопровождения учебного процесса ОмГУ. Отметим ещё, что основная причина отказа от существующих систем оповещения состояла в том, что задача требует привязки оповещения к событиям, отражающимся изменениями данных в базе данных, это логичнее всего сделать с применением механизма триггеров базы данных, что однозначно требует своей собственной разработки системы оповещения.

После анализа сервисов массовых рассылок была определена функциональность, которую необходимо спроектировать в системе уведомлений ИИАС «Учебный процесс». Список укрупнённых функций:

- изменение статуса письма,
- формирование шаблона письма,
- возможность подписывать пользователя на рассылку и отписывать от неё,
- возможность изменять данные пользователя,
- возможность инициировать рассылку и повторять её в случае необходимости,
- возможность системы реагировать на наступление какого-либо события.

2. Проектирование системы уведомлений

Напомним, что проектируемый модуль должен быть веб-модулем веб-приложения «Электронные сервисы ОмГУ». «Электронные сервисы ОмГУ» — это набор микросервисов, связанных DAS — системой хранения данных с прямым подключением DAS (Direct Attached Storage). Авторизация происходит на стороне «Электронных сервисов ОмГУ» с использованием DAS [9].

Для того чтобы пользователь переходил из одного раздела упомянутого портала в другой используется технология единого входа (Single Sign-On). Сама авторизация происходит с использованием протокола OAuth 2.0, позволяющего одному сервису выдать права на доступ к ресурсам пользователя на другом сервисе.

Здесь же отметим, что в «Электронных сервисах ОмГУ» платформой является Java, языком программирования — Scala. Существующая база данных реализована в среде СУБД Oracle. Для реализация фронтенда используется CSS.

Рассмотрим бизнес-логику системы (рис. 2).

В системе определены две роли пользователей: обычные пользователи и администраторы. В процессе авторизации пользователя приложение проверяет, какая роль ему назначена.

Далее рассмотрим действия, возможные для пользователя, и приведём макет интерфейса, позволяющий понять переходы между страницами интерфейса. Пользователь может выбирать, на какую почту он хочет получать рассылку, может выбирать события из списка, на которые он хочет подписаться. После этого происходит проверка, достаточно ли у него для этого прав (рис. 3).

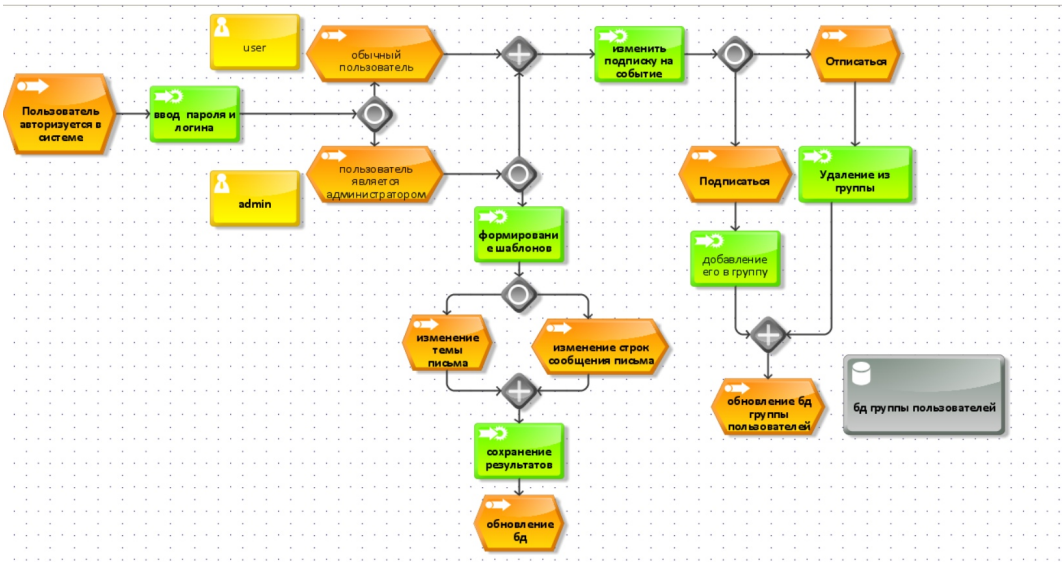

Рис. 2. Событийная модель системы уведомлений

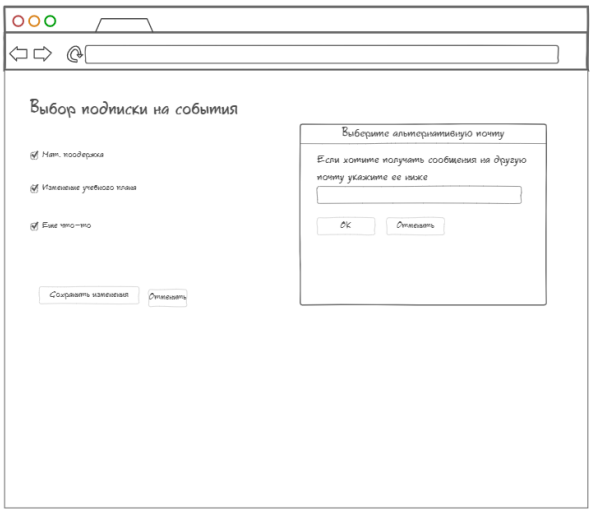

Рис. 3. Макет страницы подписки на события и выбора почты со стороны пользователя

Далее рассмотрим пользователя с правами администратора (рис. 4), он может выполнять те же действия, что и обычный пользователь, но уже для всех пользователей, то есть он может изменить почту выбранного пользователя, подписать или отписать его от информирования о группе событий (рис. 5) путём добавления или удаления его из группы. Например, могут быть выделены такие группы, как студенты с событиями «заявление на материальную поддержку», «группа для выдачи справки с места учёбы», преподаватели факультетов с событиями, такими как «изменение учебного плана».

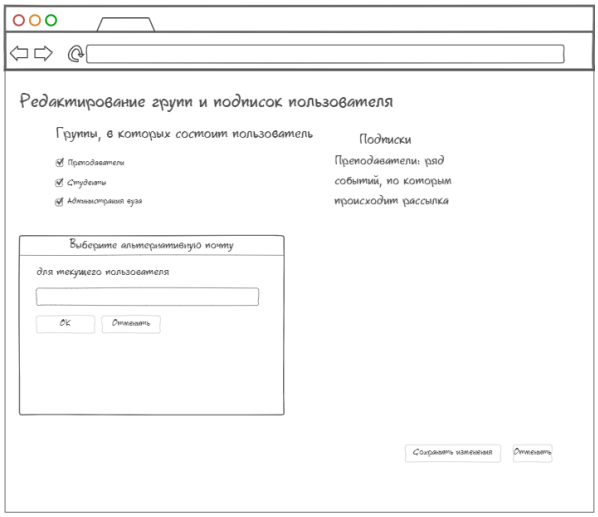

Рис. 4. Макет страницы выбора пользователя и группы со стороны администратора

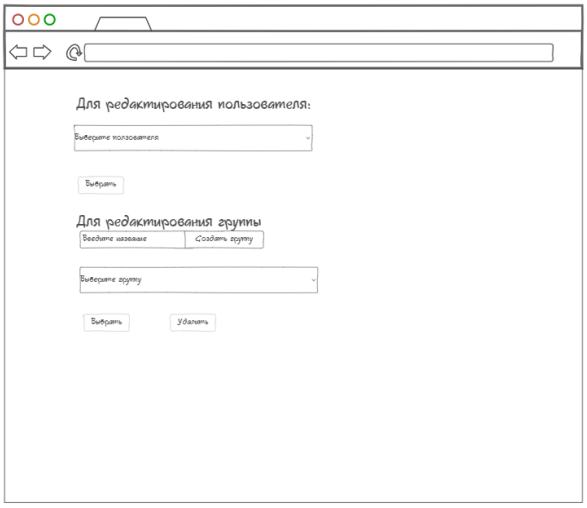

Рис. 5. Макет страницы редактирования пользователя

Администратор имеет дополнительную функциональность:

1) редактирование групп (рис. 6);

2) формирование шаблона сообщения с использованием реализованных выражений (рис. 7);
3) принудительное отправление сообщения пользователю;
4) формирование групп событий.

Рис. 6. Макет страницы редактирования групп

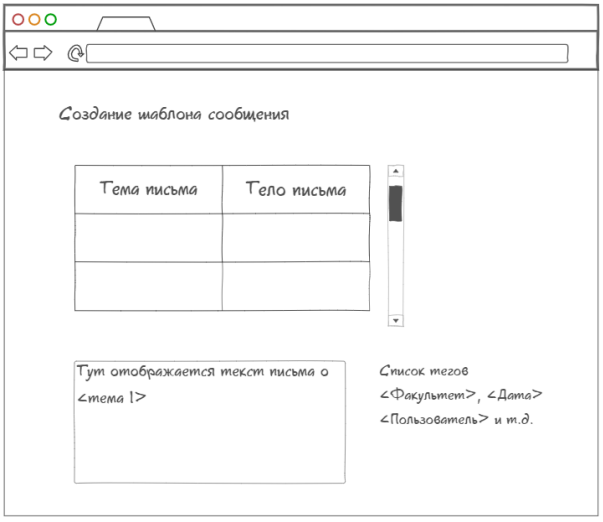

Рис. 7. Макет страницы создания шаблона сообщения

Таким образом, можно обобщить роли и их привилегии (табл. 2).

Более внимательно рассмотрим процесс рассылки сообщений. Пусть произошло событие из списка event_description, тогда в таблицу event_list добавляется идентификатор этого события (рис. 8).

События есть в некоторых группах, по группам находятся пользователи в группе, во внешней таблице отделы_пользователя по внешнему ключу user_id

Таблица 2. Роли и их привилегии

	Обычный пользователь	Администратор
Подписка/отписка от события	+	+
Изменение личной информации	+	+
Редактирование групп пользователей	-	+
Формирование групп событий	-	+
Формирование шаблона сообщения с использованием реализованных выражений	-	+
Принудительное отправление сообщения пользователю	-	+

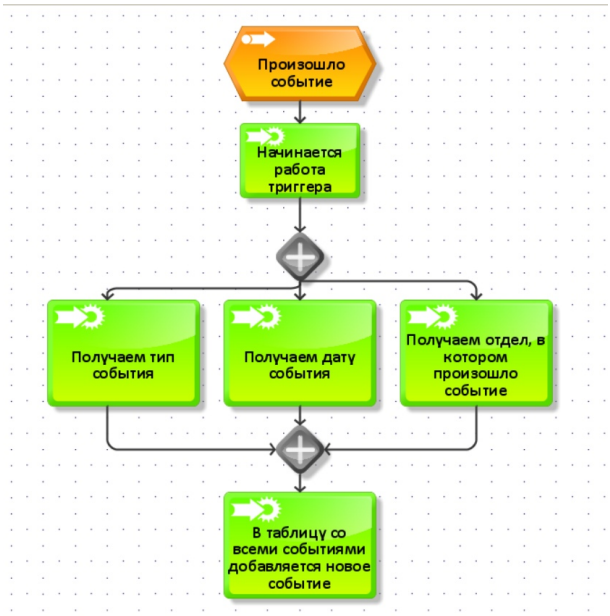

Рис. 8. Событийная модель функционирования триггера на заполнение таблицы Event_list

находится поле department_id, и этот идентификатор добавляется в таблицу event_list как внешний ключ. Атрибут selected показывает, обработано событие или нет, по умолчанию устанавливается 0, что означает: событие не обработано. Далее происходит работа триггера, и по событиям из таблицы Event_list формируются шаблоны сообщений, которые непосредственно и отправляются пользователям с определённой регулярностью или в случае, когда администратор инициирует рассылку (рис. 9).

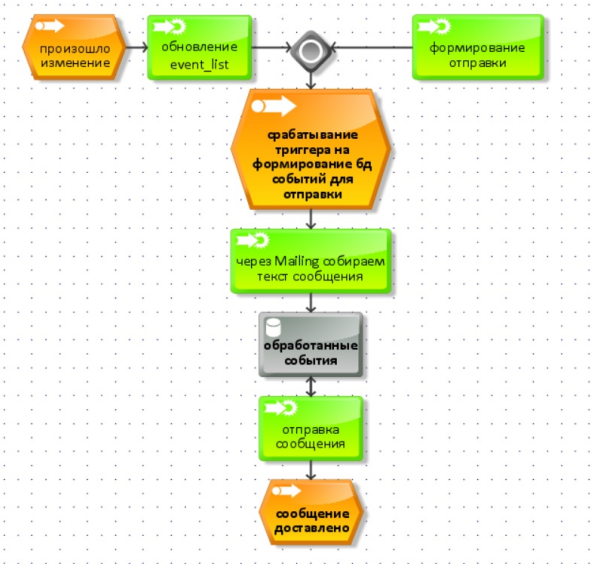

Рис. 9. Событийная модель процесса формирования отправки уведомления

Как можно увидеть на рисунке 9, после срабатывания триггера происходит формирование сообщений для отправки. Текст сообщений формируется с помощью таблиц Mailing и Mail_strings, где содержатся шаблоны тела письма и тема. Адресаты — это люди, находящиеся в определённой группе пользователей. На рисунке 10 показан процесс формирования сообщения для отправки. По полю event_id текущего события выполняется поиск строки в таблице Mailing. Заголовком будет являться атрибут mailing_subject, а по полю (первичному ключу) mailing_id происходит сборка тела письма по данным из таблицы Mail_strings. Во время формирования текста письма вместо тегов вставляется нужная информация, например отдел пользователя. Администратор заранее может самостоятельно изменять тему и текст сообщения для различных событий, используя различные теги.

После сборки текста уведомления готовое сообщение отправляется пользователям из группы, для которой произошло событие. После отправки отслеживается, было ли доставлено сообщение.

Все обработанные и отправленные события помещаются в таблицу Sended_mails; значение атрибута successed позволяет проверить, было ли доставлено сообщение пользователю (1 — сообщение доставлено, 0 — не доставлено (произошла ошибка при отправке)). В случае ошибки сообщение можно отправить заново за некоторое фиксированное число попыток.

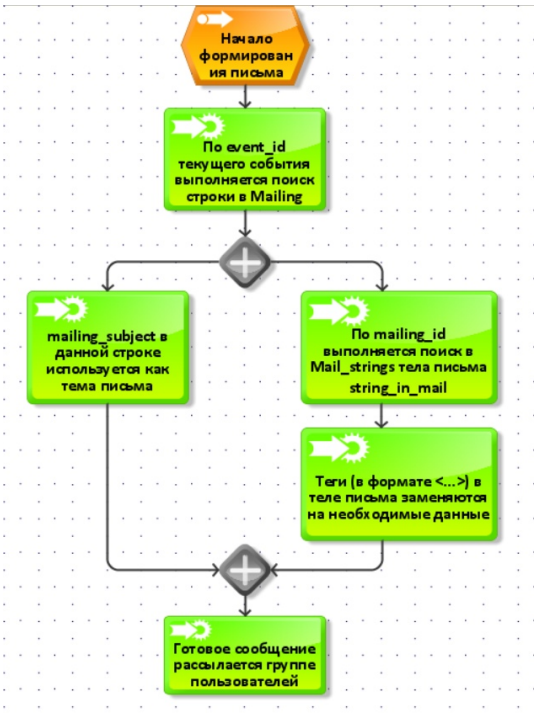

Рис. 10. Событийная модель процесса формирования текста письма

Во время формирования рассылки будет учитываться тип контакта пользователя (по умолчанию это электронная почта из таблицы es_users, но пользователь может менять как сам контакт, так и его тип в дальнейшем). В зависимости от типа контакта будет происходить рассылка.

В результате проведённого анализа спроектированы база данных и система уведомлений, описан процесс формирования динамического списка событий, оповещение о которых было бы полезно получать пользователю, разработан макет интерфейса, позволяющий проследить взаимодействие элементов интерфейса.

3. План развития

Следующая стадия развития проекта — его реализация. Непосредственно для отправки сообщения будет использоваться JavaMail — это Java API, предназначенное для получения и отправки электронной почты с использованием протоколов SMTP, POP3 и IMAP. Кроме того, с помощью JavaMail будет отслеживаться, доставлено ли сообщение, и в случае неудачи отправляться повторно определённое количество раз.

Как упоминалось выше, изначально отправка сообщений планируется по электронной почте. В последствии планируется осуществлять её через социальную сеть ВК с помощью чат-бота, потому что большинство студентов проверяют сообщения в этой социальной сети регулярнее, чем заходят на почту. То есть при использовании отправки сообщений не на почту, а в социальные

сети, повысится охват аудитории и актуальность модуля.

Литература

1. Система уведомлений о событиях (Webhooks) [Электронный ресурс]. Электрон. текстовые дан. URL: https://www.unisender.com/ru/support/api/common/sistema-uvedomlenij-o-sobytiyah-webhooks/(дата обращения 04.04.2020).
2. Features [Электронный ресурс]. Электрон. текстовые дан. URL: https://emailchef.com/features (дата обращения 27.03.2020).
3. Рассылка уведомлений о событиях системы [Электронный ресурс]. Электрон. текстовые дан. URL: https://sigursys.com/func_notifications.php (дата обращения 02.04.2020).
4. Уведомления о событиях в «Личном кабинете» можно получать на адрес электронной почты [Электронный ресурс]. Электрон. текстовые дан. URL: http://holmogori.ru/govinfo/govinfofns/media/2020/3/18/uvedomleniya-o-sobyitiyah-v-lichnom-kabinete-mozhno-poluchat-na-adres-elektronnoj-pochtyi (дата обращения 29.03.2020).
5. Электронные сервисы [Электронный ресурс]. Электрон. текстовые дан. URL: https://eservice.omsu.ru/ (дата обращения 17.10.2020).
6. Губанов В.А., Захаров В.В., Коваленко А.Н. Введение в системный анализ. Л : Издательство Ленинградского университета, 1988. 232 с.
7. Гуревич И.М. Законы информатики — основы исследований и проектирования сложных систем // Информационные технологии. 2003. № 11. Приложение. 24 с.
8. А.с. 2011612300 РФ, Роспатент. Интегрированная информационно-аналитическая система «Учебный процесс» (ИИАС «Учебный процесс») / Епанчинцева О.Л., Ворошилов В.В., Костюшина Е.А., Погромская Т.А. (RU). № 2010617657; заявл. 06.12.2010; опубл. 18.03.2011. Бюл. № 2(75). С. 329.
9. Костюшина Е.А., Илюшечкин Е.А., Ворошилов В.В., Городецкий А.Д. Многокомпонентное веб-приложение «Электронные сервисы вуза». Свидетельство об официальной регистрации программы для ЭВМ № 017612596, 01.03.17.

DESIGNING A MODULE FOR NOTIFICATIONS ABOUT EVENTS IN THE EDUCATIONAL PROCESS MANAGEMENT INFORMATION SYSTEM OF OMSU

O.A. Bondarenko
Student, e-mail: bondarenkoolga360@gmail.com
E.A. Kostushina
Ph.D.(Eng.), Associate Professor, e-mail: kea.omsu@gmail.com
T.V. Oleynikova
Student, e-mail: oleynikova.tan@gmail.com
D.N. Lavrov
Ph.D.(Eng.), Associate Professor, e-mail: lavrov@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. The article is devoted to the design features of the notification module in the information-analytical system "Educational process". Due to the complexity and nonlinearity of the problem, it was decided to apply the system analysis method to research the subject area. In addition, the existing analogues of warning systems were considered, which made it possible to determine the maximum possible functionality of the module.

Keywords: information and analytical system, events, educational process.

References

1. Sistema uvedomlenii o sobytiyakh (Webhooks) [Elektronnyi resurs]. Elektron. tekstovye dan. URL: `https://www.unisender.com/ru/support/api/common/sistema-uvedomlenij-o-sobytiyah-webhooks/`(data obrashcheniya 04.04.2020). (in Russian)
2. Features [Elektronnyi resurs]. Elektron. tekstovye dan. URL: `https://emailchef.com/features` (data obrashcheniya 27.03.2020). (in Russian)
3. Rassylka uvedomlenii o sobytiyakh sistemy [Elektronnyi resurs]. Elektron. tekstovye dan. URL: `https://sigursys.com/func_notifications.php` (data obrashcheniya 02.04.2020). (in Russian)
4. Uvedomleniya o sobytiyakh v "Lichnom kabinete" mozhno poluchat' na adres elektronnoi pochty [Elektronnyi resurs]. Elektron. tekstovye dan. URL: `http://holmogori.ru/govinfo/govinfofns/media/2020/3/18/uvedomleniya-o-sobyitiyah-v-lichnom-kabinete-mozhno-poluchat-na-adres-elektronnoj-pochtyi` (data obrashcheniya 29.03.2020). (in Russian)
5. Elektronnye servisy [Elektronnyi resurs]. Elektron. tekstovye dan. URL: `https://eservice.omsu.ru/` (data obrashcheniya 17.10.2020). (in Russian)
6. Gubanov V.A., Zakharov V.V., and Kovalenko A.N. Vvedenie v sistemnyi analiz. L., Izdatel'stvo Leningradskogo universiteta, 1988, 232 p. (in Russian)
7. Gurevich I.M. Zakony informatiki — osnovy issledovanii i proektirovaniya slozhnykh sistem. Informatsionnye tekhnologii, 2003, no. 11, Prilozhenie, 24 p. (in Russian)
8. A.s. 2011612300 RF, Rospatent. Integrirovannaya informatsionno-analiticheskaya sistema "Uchebnyi protsess" (IIAS "Uchebnyi protsess"), Epanchintseva O.L., Voroshilov V.V., Kostyushina E.A., Pogromskaya T.A. (RU). no. 2010617657; zayavl. 06.12.2010; opubl. 18.03.2011. Byul., no. 2(75), pp. 329. (in Russian)
9. Kostyushina E.A., Ilyushechkin E.A., Voroshilov V.V., and Gorodetskii A.D. Mnogokomponentnoe veb-prilozhenie "Elektronnye servisy vuza". Svidetel'stvo ob ofitsial'noi registratsii programmy dlya EVM no. 017612596, 01.03.17. (in Russian)

Дата поступления в редакцию: 15.11.2020

Математические структуры и моделирование
2020. № 4(56). С. 148–160

УДК 004.05
DOI 10.24147/2222-8772.2020.4.148-160

АУДИАЛЬНОЕ СОПРОВОЖДЕНИЕ САЙТА «ЭЛЕКТРОННЫЕ СЕРВИСЫ ОМГУ»

Н.В. Коляда
аспирант, инженер-программист, e-mail: nikita.nk16@yandex.ru
Е.А. Костюшина
к.т.н., доцент, e-mail: kea.omsu@gmail.com
Д.Н. Лавров
к.т.н., доцент, e-mail: lavrov@omsu.ru

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация. В данной статье представлена информация о функционале, правилах вёрстки, удобстве визуальной среды и специальных аспектах, требования к которым отражены в стандартах для обучающихся с нарушениями зрения.

Ключевые слова: сайт, слабовидящие, стандарты.

Введение

На сегодня в ФГБОУ ВО «Омский государственный университет им. Ф.М. Достоевского» остро стоит проблема предоставления доступа к электронным ресурсам для пользователей с ограниченными возможностями. В соответствии с Федеральным Законом «Об обеспечении доступа к информации...» и национальным стандартом РФ ГОСТ Р 52872-2012 «Интернет ресурсы. Требования доступности для инвалидов по зрению» все ресурсы государственных и муниципальных структур обязаны предоставить версии сайтов для людей с ограниченными возможностями. В связи с указанной выше проблемой в отделе разработки информационных систем (ОРИС) ОмГУ им Ф.М. Достоевского была поставлена задача по адаптированию веб-приложения «Электронные сервисы» для пользователей с ограниченными возможностями.

1. Обзор мировых практик

За стандарты разработки сайтов для людей с ограниченными возможностями отвечает руководство Web Content Accessibility Guidelines (WCAG), содержащее рекомендации по доступности содержимого веб-ресурсов. Последняя версия появилась в декабре 2008 года в рамках «Инициативы по обеспечению доступности» консорциума W3C [3]. Эта версия включила в себя требования не только к сайтам, но и ко всем веб-платформам в целом.

Руководство даёт рекомендации, как сделать контент интернет-ресурса доступным для пользователей с инвалидностью различных типов: ограничения

по зрению, слуху, опорно-двигательной системе, ограничения речи, ментальной сферы и пр.

Примером наиболее последовательного и бескомпромиссного подхода к законодательному обеспечению доступности веб-ресурсов могут служить Германия, Италия, США и Республика Корея. Германия — одна из немногих стран, подписавших и ратифицировавших не только саму Конвенцию [1] о правах инвалидов, но и факультативный протокол к ней [2].

Во всех рассмотренных выше странах основу режима обеспечения доступности веб-ресурсов составили уже существовавшие в них законы о предупреждении дискриминации в отношении инвалидов. WCAG — целиком или частично — был принят в качестве основы национальных рекомендаций в области доступности веб-ресурсов. Другие же страны выбрали иной путь (см. табл. 1).

Таблица 1. Страны и принятые положения

Положение	**Страна**	**Описание**
ГОСТ Р 52872-2012	Россия	«Интернет-ресурсы. Требования доступности для инвалидов по зрению»
WCAG	Германия Италия США Республика Корея Австралия Канада Великобритания Европейский Союз Израиль	«Руководства по обеспечению доступности веб-контента (WCAG) 2.0»
PWAG	Филиппины	Филиппинская Группа по вопросам доступности веб-ресурсов
Национальное руководство по обеспечению доступности веб-ресурсов	Таиланд	За основу была взята вторая версия WCAG
JIS X 8341	Япония	«Новая стратегия реформы информационных технологий»

Для понимания перспектив создания доступности интересен следующий факт: адаптация сайта Госуслуги в соответствии с Рекомендациями WCAG 2.0, проведённая в октябре-декабре 2012 года, привела к тому, что количество зарегистрировавшихся пользователей в возрасте от 45 лет и старше увеличилось только за январь-март 2013 года в 4 раза по отношению к ежегодному приросту этой категории пользователей в предыдущие годы. Интересно, что

такой результат стал возможным несмотря на то, что в рамках существующего ТЗ было возможно реализовать только 30 % рекомендаций.

Интересен в этой связи и такой факт, касающийся интернет-сайта Министерства здравоохранения и социального развития РФ (www.minzdravsoc.ru): в результате внутреннего анализа использования сайта оказалось, что 80 % сотрудников министерства использовали адаптированную версию для слабовидящих по причине того, что это «удобно, крупно, не утомляешься при работе с информацией».

Результаты мониторинга государственных сайтов АИС «Мониторинг госсайтов» на апрель 2013 года доступны в статье «Исследование обеспечения доступности интернет-ресурсов Рунета для людей с ограниченными возможностями здоровья (ОВЗ)» [6].

Согласно WCAG, доступность веб-ресурса определяется следующими четырьмя принципами: воспринимаемость, управляемость, понятность и надёжность. Каждый из них подразумевает свою цепочку правил. В зависимости от качества выполнения этих условий сайты подразделяются на несколько уровней доступности:

- минимальный (A),
- средний (AA),
- высокий (AAA).

Стоит сказать, что совместить все требования стандартов с крутым дизайном, отлаженным функционалом и кроссбраузерностью практически невозможно. Соблюдение всей строгости правил может в значительной мере повлиять на фирменный стиль компании, на удобство интерфейса для среднестатистического пользователя, на способ подачи информации и многое другое.

Стандарт следует воспринимать не как строгий гайдлайн, но как рекомендацию, которая значительно расширяет аудиторию ресурса.

2. Краткие рекомендации из положения WCAG

В таблице 2 ниже отражены основные правила и рекомендации при вёрстке страниц, выделенные из положения WCAG.

Таблица 2. Краткие рекомендации из положения WCAG [7]

Тип	**Описание правила**
Цвет	Не рекомендуется использовать цвет в качестве единственного визуального средства передачи информации или обозначения действия
	Цвет текста и фона могут быть выбраны пользователем

Продолжение таблицы на след. странице

Продолжение таблицы 2

Тип	**Описание правила**
Текст	Обычный текст и текст на картинках должны иметь контрастность не менее 7:1
	Должна предоставляться возможность изменения размера шрифта (кроме титров и изображений текста) в пределах до 200 % без потери контента и функциональности
	Цвет текста и фона должны иметь гибкие настройки, которые пользователь может менять сам
	Строка не должна быть длиннее 80 символов
	Запрещено выравнивание по ширине
	Минимальный межстрочный интервал — не менее 1,5 интервалов, а интервал между абзацами — минимум в 1,5 раза больше
	Текст на изображениях должен использоваться только для оформления
	Текст кнопок и ключевых элементов должен быть информативным
	Все поля ввода должны иметь осмысленные текстовые метки
	Шрифт должен быть разборчивым
Нетекстовый контент	Элементы управления должны иметь описание назначения
	Медиаконтент, а также контент для создания специфического восприятия должен иметь краткое описание содержания. Медиаконтент должен сопровождаться синхронизированными титрами.
	Контент, созданный в целях оформления, должен игнорироваться скринридерами. Для капчи должна описываться ее цель. Кроме того, должны быть предоставлены альтернативные формы капчи, доступные для других типов восприятия, помимо визуального.
	Картинки и ссылки должны иметь альтернативное описание (alt=)
Управление	Отсутствие ограничений по времени нажатия на клавишу
	Возможность ввода информации другими способами
	в случае использования нестандартного перевода курсора и фокуса предлагается описание метода его перемещения
Аудиосопровождение	Нельзя использовать опасные для психики элементы дизайна и аудиосопровождения. Ни один элемент не должен менять своё состояние более 3 раз в секунду (особенно вспышки).
	Стоит исключить появление неожиданных, излишне резких и чересчур громких звуков
	Фоновый звук должен либо полностью отсутствовать, либо должна быть возможность его отключения. В случае наличия фоновых звуков они должны быть тише, чем звук голосового контента переднего плана минимум на 20 дБ (примерно в 4 раза), за исключением отдельных звуков продолжительностью не более 1-2 с.

Продолжение таблицы на след. странице

Продолжение таблицы 2

Тип	**Описание правила**
Семантика разметки	При вёрстке элементов, имеющих особое назначение, таких как списки, таблицы, заголовки и т. п. следует использовать соответствующие теги. В таблице 2 приведены основные их них.
	role=main — блок основного контента role=navigation — блок служит для навигации по сайту role=banner — блок является баннером и т. п.
Инструменты валидации	Для проверки html-страниц на валидность, применяют различные сайты-валидаторы (по ссылке) и расширения для браузера

Таблица 3. Теги и атрибуты, которые следует использовать

Тэги и атрибуты	**Назначение**
       role	Ненумерованные списки Нумерованные списки Элемент списка Атрибут назначения Нельзя разбивать список на несколько только для красивого отображения. Это затруднит прочтение страницы с помощью скринридера
<table> <caption> <tr> <th> <td> role	Таблица Заголовок таблицы Строка таблицы Заголовок столбца Столбец таблицы Атрибут назначения Стоит помнить, что заголовки с colspan применяются для каждой нижестоящей ячейки. Нельзя разбивать для отображения (аналогично спискам)
<details> <summary>	Детализированная информация Заголовок детализированной информации
 <button> <a href="..."role="button» <input type="button» <role=button>	Рекомендуется оформлять кнопки кликабельными элементами Кнопка Ссылка с назначением кнопки Инпут кнопочного типа Менее желательно использование некликабельных элементов с использованием: <tabindex> Атрибут назначения

Продолжение таблицы на след. странице

Продолжение таблицы 3

Тэги и атрибуты	**Назначение**
	<onkeydown> Последовательность перехода между элементами по нажатию на TAB. Обработка события с клавиатуры при нажатии на enter

Для семантических областей и наименования информационных блоков используются следующие теги и атрибуты (Таблица 4).

Таблица 4. Теги и атрибуты, которые следует использовать для семантических областей

Тэги и атрибуты	**Назначение**
<h1> <h2> — <h4>	Заголовок первого уровня Чаще всего встречается на странице один раз и поясняет суть странички. В случае структуры Landing Page его используют для наименования каждой из секций (<section>). Заголовки 2-4 уровней Отделяют информационные блоки друг от друга
role=main role=navigation role=complementary role=banner	Разметка семантических областей

3. Валидаторы

Проверить сайт на общую валидность HTML можно с помощью классического валидатора [8]. А с помощью расширения WAVE Evaluation Tool для Chrome [9] можно проанализировать любой ресурс на наличие основных ошибок. Ресурс предоставит перечень выявленных ошибок и даст справку по их исправлению, подсветит синтаксис и атрибуты aria. Найти ошибки в логике применения атрибутов aria поможет и AInspector Sidebar for Firefox [10]. Он также выдаст список проверок, которые рекомендуется сделать вручную.

Разумеется, сообщения об ошибках, выдаваемые различными валидаторами, не представляют собой жёсткий критерий несоответствия WCAG, а носят рекомендательный характер. Решения по ним должны приниматься исходя из требований и конечных целей проекта.

Стоит упомянуть и о том, что далеко не все проблемы выявляются с помощью валидаторов. Для 100 % уверенности в удовлетворении вёрстки стандартам понадобится ручное тестирование в т. ч. с применением экранных чтецов. Эти программы довольно специфичны, но к их использованию удаётся быстро привыкнуть.

Самой легкой в настройке является бесплатная программа чтения экрана — NVDA [11]. Программы экранного доступа довольно специфичны для тех, кто

с ними сталкивается впервые, однако к пользованию ими можно относительно быстро привыкнуть.

Анализ электронных сервисов с помощью валидаторов

Для анализа на предмет ошибок валидации были выбраны «Главная страница» и сервис «Учебная карточка» в веб-приложении «Электронные сервисы ОмГУ» [5, 6] (см. таблицы 5, 6).

Таблица 5. Результаты проверки валидатором WAVE

Тип замечания	**Главная страница**	**Учебная карточка**
Ошибки	У 14 изображений отсутствует альтернативный текст	2 формы не имеют меток label
	Отсутствует заголовок страницы	Отсутствует заголовок страницы
	Отсутствует язык страницы	Отсутствует язык страницы
	17 элементов с низким контрастом между цветами переднего плана и фона	6 ссылок не содержит текста
		5 элементов с низким контрастом между цветами переднего плана и фона
Предупреждения	Отсутствует заголовок первого уровня	Отсутствуют заголовки 1-6 уровня
	6 ссылок на другое место внутри страницы присутствует, но не имеет соответствующего целевого объекта	10 ссылок на PDF-документы
	13 ссылок, указывающих на один и тот же ресурс	7 таблиц компоновки
Структурные элементы	10 маркировочных или неупорядоченных списков	2 маркировочных или неупорядоченных списка
	14 зон без указания роли	1 зона без указания роли
	14 элементов в роли кнопки	

Таблица 6. Результаты проверки валидатором validator.w3.org

Тип замечания	**Главная страница**	**Учебная карточка**
Ошибки	Элемент title не должен быть пустым	Элемент title не должен быть пустым
	img элемент должен иметь alt атрибут	
Предупреждения	Отсутствует язык страницы	Отсутствует язык страницы

Аудиальное сопровождение сайта. Для реализации встроенного скринридера можно воспользоваться либо платными сервисами, либо бесплатными биб-

Таблица 7. Технологии распознавания и синтеза речи

Сервис/Библиотека	**Платный**	**Функция**	**Описание**
Yandex SpeechKit	Да	Распознавание и синтез речи	Сервис Yandex SpeechKit позволяет разработчикам приложений использовать речевые технологии Яндекса: распознавание речи (Speech-to-Text) и синтез речи (Text-to-Speech).
SpeechRecognition	Нет	Распознавание речи	Экспериментальная технология. Интерфейс распознавания голоса Web Speech API является интерфейсом контроллера для сервиса распознавания
SpeechSynthesisUtterance	Нет	Синтез речи	Интерфейс синтезирования текста в речь
Google Cloud Speech	Да	Распознавание речи	Синтезатор в Google Cloud
pocketsphinx.js	Нет		Не поддерживают русский язык
watson-speech	Нет		

лиотеками (см. табл. 7).

В результате анализа были выбраны технологии SpeechRecognition и SpeechSynthesisUtterance, для реализации распознавания и синтеза речи соответственно.

На данный момент только в некоторых браузерах существует поддержка функции SpeechRecognition для распознавания речи. С синтезом речи SpeechSynthesisUtterance ситуация получше, данный модуль поддерживает большинство браузеров (табл. 8).

Таблица 8. Поддержка браузерами распознавания и синтеза речи

Технология / Браузер	**Chrome**	**Edge**	**Firefox**	**Internet Explorer**	**Opera**	**Safari**
SpeechRecognition	+	+	-	-	-	-
SpeechSynthesisUtterance	+	+	+	-	+	+

4. Внедрение технологий аудиальной поддержки

В качестве проекта для тестирования был выбран сервис «Заявления», позволяющий студентам оставлять заявки на материальную поддержку, подготовку справки об обучении, на повышенную академическую стипендию и др. Для использования библиотек SpeechRecognition и SpeechSynthesisUtterance были написаны модули «voiceListener» и «textReader». Код модуля «textReader» представлен ниже. На данном участке кода реализовано подключение библиотеки и функция синтеза речи из текста.

```
var utterance = new SpeechSynthesisUtterance();
utterance.lang = 'ru-RU';
utterance.voice =  window.speechSynthesis.getVoices()[17];
utterance.volume = 1;

function resumeReader() {
    speechSynthesis.resume();
}

function pauseReader() {
    speechSynthesis.pause();
}

function stopReader() {
    speechSynthesis.stop();
}

function read(text) {
    interval(function () {
        utterance.text = text;
        console.log(utterance);
        speechSynthesis.speak(utterance);
    }, function () {
        return !speechSynthesis.speaking;
    });

}

function readList(list) {
    console.log(list);
    list.map(function (index, item) {
        read(item);
    });
}
```

На следующем участке кода модуля «voiceListener» реализовано подключение библиотеки и функция получения результата после распознавания текста из речи пользователя.

```
var recognizer = new webkitSpeechRecognition();

recognizer.interimResults = true;
recognizer.continuous = true;
recognizer.lang = 'ru-Ru';

var commandIsRun = false;
var isListen = false;
var isStop = false;

recognizer.onresult = function (event) {
    var result = event.results[event.resultIndex];

    if (result.isFinal) {
        read('Вы сказали: ' + result[0].transcript);
        commandIsRun = true;
        parseCommand(result[0].transcript);

        interval(function () {
            listenCommand();
        }, function () {
            return !speechSynthesis.speaking && !commandIsRun;
        });
    }
};
```

Результаты можно увидеть на скриншотах ниже (рис. 1, 2).

Заключение

В результате исследования современных стандартов по адаптации электронных ресурсов для пользователей с ограниченными возможностями были проанализированы электронные сервисы на соответствие стандартам, в ходе чего выявлены ошибки, а также сформирован ряд правок по модернизации сервисов для таких пользователей.

Протестировано внедрение технологий SpeechRecognition и SpeechSynthesisUtterance для аудиальной поддержки электронного сервиса, команды которого выполняются последовательно (без ветвлений).

Литература

1. Конвенция о правах инвалидов. Принята резолюцией 61/106 Генеральной Ассамблеи от 13 декабря 2006 года. URL: `https://www.un.org/ru/documents/decl_conv/conventions/disability.shtml` (дата обращения: 16.11.2020).
2. Факультативный протокол к Конвенции о правах инвалидов // Объединённые нации. Права человека. Управление верховного комиссара. URL: `https://www.ohchr.org/ru/hrbodies/crpd/pages/optionalprotocolrightspersonswithdisabilities.aspx` (дата обращения: 16.11.2020).

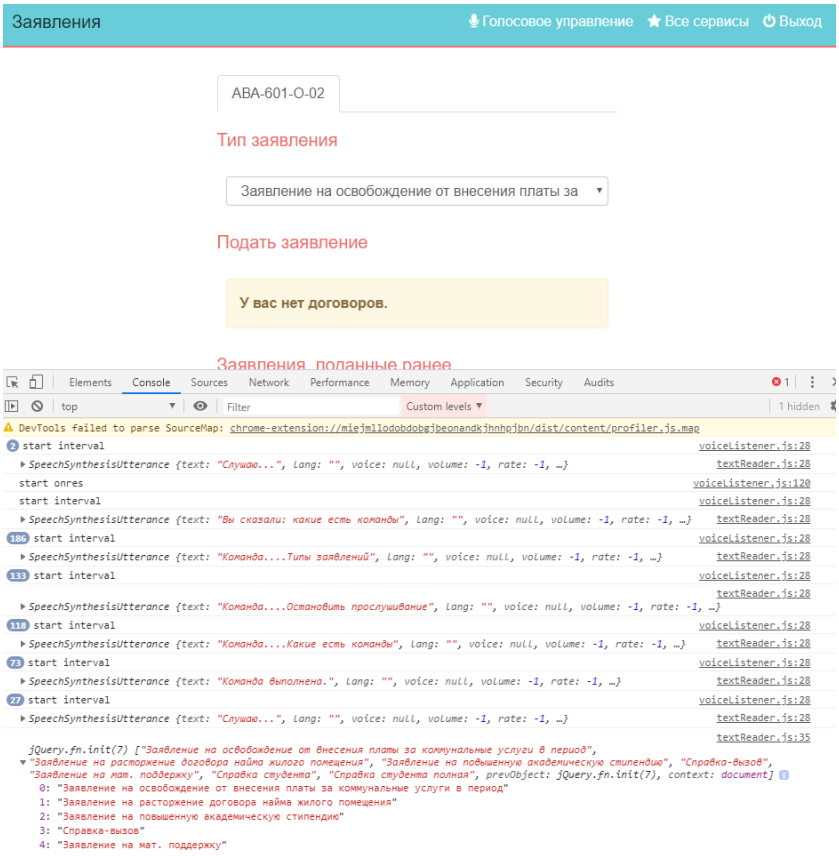

Рис. 1. Форма и результат разбора для голосового воспроизведения

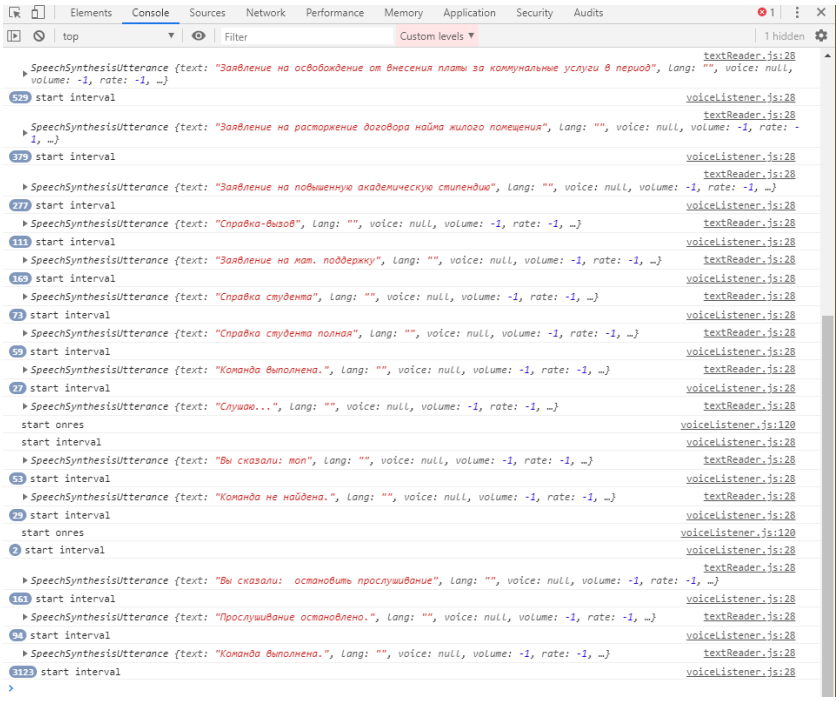

Рис. 2. Форма и результат разбора для голосового воспроизведения (продолжение)

3. Обзор стандартов W3C по обеспечению доступности веб-контента // Web Accessibility Initiative WAI: Стратегии, стандарты, ресурсы по веб-доступности для инвалидов. URL: https://www.w3.org/WAI/standards-guidelines/ru (дата обращения: 16.11.2020).
4. Костюшина Е.А., Илюшечкин Е.А., Ворошилов В.В., Городецкий А.Д. Многокомпонентное веб-приложение «Электронные сервисы вуза». Свидетельство об официальной регистрации программы для ЭВМ № 017612596, 01.03.17.
5. Электронные сервисы [Электронный ресурс]. Электрон. текстовые дан. URL: https://eservice.omsu.ru/ (дата обращения 17.10.2020).
6. Обеспечение доступности интернет-ресурсов Рунета для людей с ограниченными возможностями здоровья // Информационнйцентр ООН в Москве. НП Культурный центр «Без границ». Москва, 2013. URL: http://www.unic.ru/sites/default/files/Accessibility_of_Runet_2013.pdf (дата обращения 17.10.2020).
7. Web Content Accessibility Guidelines (WCAG) 2.0. URL: https://www.w3.org/TR/WCAG20/ (дата обращения 17.10.2020).
8. Markup Validation Service. URL: https://validator.w3.org/ (дата обращения 17.10.2020).
9. WAVE Evaluation Tool. URL: https://chrome.google.com/webstore/detail/wave-evaluation-tool/jbbplnpkjmmeebjpijfedlgcdilocofh (дата обращения 17.10.2020)
10. AInspector WCAG от Jon Gunderson, Nicholas Hoyt. URL: https://addons.mozilla.org/ru/firefox/addon/ainspector-wcag (дата обращения 17.10.2020)
11. NVDA.RU — Социально-информационный проект для людей с физическими ограничениями по зрению, использующих бесплатную программу экранного доступа NVDA. URL: https://nvda.ru/ (дата обращения 17.10.2020).

AUDITORY SUPPORT OF THE SITE "ELECTRONIC SERVICES OF OMSU"

N.V. Kolyada
Postgraduate Student, Software Engineer, e-mail: nikita.nk16@yandex.ru
E.A. Kostushina
Ph.D.(Eng.), Associate Professor, e-mail: kea.omsu@gmail.com
D.N. Lavrov
Ph.D.(Eng.), Associate Professor, e-mail: lavrov@omsu.ru

Dostoevsky Omsk State University, Omsk, Russia

Abstract. This article describes information about functionality, layout rules, usability of the visual environment and special aspects, the requirements for which are reflected in the standards for students with visual impairments.

Keywords: website, visually impaired, standards.

References

1. Konventsiya o pravakh invalidov. Prinyata rezolyutsiei 61/106 General'noi Assamblei ot 13 dekabrya 2006 goda. URL: https://www.un.org/ru/documents/decl_conv/conventions/disability.shtml (16.11.2020). (in Russian)
2. Fakul'tativnyi protokol k Konventsii o pravakh invalidov, Ob"edinennye natsii. Prava cheloveka. Upravlenie verkhovnogo komissara. URL: https://www.ohchr.org/ru/hrbodies/crpd/pages/optionalprotocolrightspersonswithdisabilities.aspx (16.11.2020). (in Russian)
3. Obzor standartov W3C po obespecheniyu dostupnosti veb-kontenta, Web Accessibility Initiative WAI: Strategii, standarty, resursy po veb-dostupnosti dlya invalidov. URL: https://www.w3.org/WAI/standards-guidelines/ru (16.11.2020). (in Russian)
4. Kostyushina E.A., Ilyushechkin E.A., Voroshilov V.V., and Gorodetskii A.D. Mnogokomponentnoe veb-prilozhenie ¡¡Elektronnye servisy vuza¿¿. Svidetel'stvo ob ofitsial'noi registratsii programmy dlya EVM no. 017612596, 01.03.17. (in Russian)
5. Elektronnye servisy [Elektronnyi resurs]. Elektron. tekstovye dan. URL: https://eservice.omsu.ru/ (data obrashcheniya 17.10.2020). (in Russian)
6. Obespechenie dostupnosti internet-resursov Runeta dlya lyudei s ogranichennymi vozmozhnostyami zdorov'ya, Informatsionnitsentr OON v Moskve. NP Kul'turnyi tsentr ¡¡Bez granits¿¿. Moskva, 2013. URL: http://www.unic.ru/sites/default/files/Accessibility_of_Runet_2013.pdf (data obrashcheniya 17.10.2020). (in Russian)
7. Web Content Accessibility Guidelines (WCAG) 2.0. URL: https://www.w3.org/TR/WCAG20/ (data obrashcheniya 17.10.2020). (in Russian)
8. Markup Validation Service. URL: https://validator.w3.org/ (data obrashcheniya 17.10.2020). (in Russian)
9. WAVE Evaluation Tool. URL: https://chrome.google.com/webstore/detail/wave-evaluation-tool/jbbplnpkjmmeebjpijfedlgcdilocofh (data obrashcheniya 17.10.2020) (in Russian)
10. AInspector WCAG ot Jon Gunderson, Nicholas Hoyt. URL: https://addons.mozilla.org/ru/firefox/addon/ainspector-wcag (data obrashcheniya 17.10.2020) (in Russian)
11. NVDA.RU — Sotsial'no-informatsionnyi proekt dlya lyudei s fizicheskimi ogranicheniyami po zreniyu, ispol'zuyushchikh besplatnuyu programmu ekrannogo dostupa NVDA. URL: https://nvda.ru/ (data obrashcheniya 17.10.2020). (in Russian)

Дата поступления в редакцию: 15.11.2020

Авторам

Предоставляемые данные и документы

Автор предоставляет в редакцию:
- рукопись статьи в формате LaTeX (см. требования к оформлению);
- список из трёх экспертов по тематике статьи, давших согласие написать рецензию на представленную работу[1];
- экспертное заключение о возможности открытого опубликования.

Лицензирование

Согласно ГК РФ ст. 1286 лицензионный договор с автором для публикации в периодических изданиях может быть заключён в устной форме. Сам факт получения рукописи статьи редколлегией журнала «Математические структуры и моделирование» является акцептом (принятием) лицензионного договора.

Все статьи в журнале «Математические структуры и моделирование» публикуются под лицензией Creative Commons Attribution 4.0 International (CC-BY). Текст лицензии находится по адресу `https://creativecommons.org/licenses/by/4.0/legalcode`.

Требования к оформлению рукописи

К публикации принимаются рукописи объёмом не более 16 страниц.

Авторам необходимо предоставить следующую информацию на русском и английском языках:
- название статьи;
- список авторов с указанием
  - фамилии, имени и отчества,
  - учёного звания,
  - учёной степени,
  - должности,
  - места работы или учёбы,
  - действующего адреса электронной почты;
- аннотация (абстракт) объёмом от 100 до 250 слов;
- список ключевых слов.

Автор также указывает УДК (универсальный десятичный код) статьи. Его можно подобрать по тематике статьи в справочнике `http://msm.univer.omsk.su/udc/`.

Библиографические ссылки оформляются согласно ГОСТ 7.0.5–2008.

Рукопись статьи представляется в редакцию по электронной почте в двух форматах pdf и tex. Статья должна быть набрана с использованием макропакета LaTeXи стиля msmb.cls, предоставляемого редакцией `http://msm.univer.omsk.su/files/msmb.zip`. Рекомендуется установить компилятор MiKTeX, так как именно им пользуются в редакции.

Отклонения в оформлении рукописи от приведённых правил позволяют редколлегии принять решение о снятии статьи с публикации. Статья может быть отклонена по причинам несоответствия тематике журнала или в связи с низким уровнем качества научного исследования.

В статье запрещается переопределять стандартные команды и окружения.

Нумеруемые формулы необходимо выделять в отдельную строку.

Нумерация только арабскими цифрами в порядке возрастания с единицы. Нумеровать следует только те формулы, на которые в тексте имеются ссылки.

---

[1]Необходимы полные данные экспертов (место работы, учёная степень, должность), с указанием способа связи с ними (e-mail, телефон). Редколлегия может обратиться к одному из экспертов из предложенного списка с просьбой написать рецензию или может назначить рецензента из собственного списка.

Запрещается использовать в формулах буквы русского алфавита. Если без них никак не обойтись, то следует использовать команду `\mbox{...}`.

Все рисунки и таблицы должны иметь подпись, оформленную с помощью команды `\caption{...}`.

Файлы с рисунками необходимо представить в формате PDF или EPS (использовать редакторы векторной графики типа InkScape, Adobe Illustrator или Corel Draw).

Используйте стандартные команды переключения на готический, каллиграфический и ажурный шрифты: `\mathfrak`, `\mathcal` и `\mathbb`.

Не допускается заканчивать статью рисунком или таблицей.

В списке литературы обязательно указание следующих данных: для книг — фамилии и инициалы авторов, название книги, место издания, издательство, год издания, количество страниц; для статей — фамилии и инициалы авторов, название статьи, название журнала, год издания, том, номер (выпуск), страницы начала и конца статьи (для депонированных статей обязательно указать номер регистрации).

Кавычки в русском тексте («абвгд») должны быть угловыми, в английском — прямыми верхними кавычками ("abcdefg" или “abcdefg”).

Обязательна расшифровка сокращений при первом вхождении термина. Например: ... искусственный интеллект (ИИ)...

Порядок рецензирования

Первичная экспертиза проводится главным редактором (заместителем главного редактора). При первичной экспертизе оценивается соответствие статьи тематике журнала, правилам оформления и требованиям, установленным редакцией журнала к научным публикациям.

Все статьи, поступившие в редакцию научного журнала «Математические структуры и моделирование», проходят через институт рецензирования.

Рецензент выбирается главным редактором журнала из числа членов редколлегии или ведущих специалистов по профилю данной работы.

Рецензенты уведомляются о том, что присланные им рукописи являются частной собственностью авторов и относятся к сведениям, не подлежащим разглашению. Рецензентам не разрешается делать копии статей для своих нужд.

Срок для написания рецензии устанавливается по согласованию с рецензентом.

Рецензия должна раскрывать актуальность представленного материала, степень научной новизны исследования, определять соответствие предлагаемого к публикации текста общему профилю издания и стиль изложения.

Рецензент выносит заключение о возможности опубликования статьи: «рекомендуется», «рекомендуется с учётом исправления замечаний, отмеченных рецензентом» или «не рекомендуется». В случае отрицательной рецензии редакция направляет автору мотивированный отказ, заверенный главным редактором или его заместителем.

В случае несогласия с мнением рецензента автор статьи имеет право предоставить аргументированный ответ в редакцию журнала. Статья может быть направлена на повторное рецензирование, либо на согласование в редакционную коллегию.

При наличии в рецензии рекомендаций по исправлению и доработке статьи автору направляется текст рецензии с предложением учесть их при подготовке нового варианта статьи или аргументированно (частично или полностью) их опровергнуть. Доработанная (переработанная) автором статья повторно направляются на рецензирование и рассматривается в общем порядке. В этом случае датой поступления в редакцию считается дата возвращения доработанной статьи.

После принятия редколлегией решения о допуске статьи к публикации автор информируется об этом и указываются сроки публикации.

Оригиналы рецензий хранятся в редакции в течение пяти лет.

Авторская этика

Авторы публикаций должны гарантировать, что в список авторов включены только лица, соответствующие критериям авторства (лица, внёсшие значительный вклад в работу), и что заслуживающие авторства исследователи не исключены из списка авторов.

Должны работать вместе с редакторами или издателями для скорейшего исправления своих работ в случае обнаружения в них ошибок или упущений после публикации.

Обязаны незамедлительно уведомлять редакцию в случае обнаружения ошибки в любой поданной ими на публикацию, принятой для публикации или уже опубликованной работе.

Не вправе копировать из других публикаций ссылки на работы, с которыми они сами не ознакомились; цитаты и ссылки на другие работы должны быть точными и оформленными в соответствии с предъявляемыми требованиями.

Должны ссылаться максимально правильно и точно на имеющие отношение к публикации предыдущие работы как других исследователей, так и самих авторов, обращаясь, прежде всего к первоисточнику; дословное воспроизведение собственных работ и их перефразирование неприемлемы, они могут быть использованы лишь в качестве основы для новых выводов.

Необходимо указывать авторство данных, текста, рисунков и идей, которые автор получил из других источников — они не должны представляться, как принадлежащие автору публикации; прямые цитаты из работ других исследователей должны выделяться кавычками и соответствующей ссылкой.

Должны соблюдать нормы законодательства о защите авторских прав; материалы, защищённые авторским правом (например, таблицы, цифры или крупные цитаты), могут воспроизводиться только с разрешения их владельцев.

Памятка для перевода должностей, учёных степеней и званий на английский язык

Профессор = Professor
Доцент = Associate Professor
Старший преподаватель = Assistant Professor
Преподаватель = Instructor
Ассистент = Instructor
Аспирант = Postgraduate Student или Ph.D. Student
Соискатель = Ph.D. Doctoral Candidate
Магистрант = Master's Degree Student
Студент = Student
д.ф.-м.н. = Dr.Sc. (Phys.-Math.)
к.ф.-м.н. = Ph.D. (Phys.-Math.)
д.т.н. = Dr.Sc. (Eng.)
к.т.н. = Ph.D. (Eng.)
Инженер-программист = Software Engineer
Старший/младший научный сотрудник = Senior/Junior Scientist Researcher

Электронная почта для отправки статей

`lavrov@omsu.ru` — зам. главного редактора (ответственный за выпуск) Д.Н. Лавров.

Научный журнал

Математические структуры и моделирование

№4(56)

Главный редактор
А.К. Гуц

Зам. глав. ред., выпускающий редактор
Д.Н. Лавров

Зам. глав. ред., технический редактор
Н.Ф. Богаченко

Корректор:
И.Н. Баловнева
Проверка корректности перевода:
А.Н. Кабанов

Адрес научной редакции
644077, Омская обл., г. Омск, пр-т Мира, д. 55а,
Омский государственный университет

E-mail: guts@omsu.ru, lavrov@omsu.ru
Электронная версия журнала:
http://msm.omsu.ru
http://msm.univer.omsk.su

Подписано в печать 14.12.2020. Формат 60 × 84 1/8.
Усл. печ. л. 17,9. Тираж 60 экз. Заказ № 178.

Отпечатано на полиграфической базе издательства ОмГУ им. Ф.М. Достоевского
644077, Омская обл., г. Омск, пр-т Мира, д. 55а

ISSN 2222-8772

20056>

9 772222 877005