ISSN 2949-2726

Hi-Hume Journal

ЖУРНАЛ ВЫСОКИХ ГУМАНИТАРНЫХ ТЕХНОЛОГИЙ

№3 (3) 2023

ISSN 2949-2726 Hi-Hume Journal — Журнал высоких гуманитарных технологий 2023 №3(3) Октябрь — декабрь

ISSN 2949-2726

Hi-Hume Journal **№3 (3)**

Журнал высоких гуманитарных технологий **2023**

Ежеквартальное научное издание **Октябрь—декабрь**

Свидетельство государственной регистрации: Эл № ФС 77-83536 от 13.07.2022

Выходит 4 раза в год (ежеквартально).

Возрастная категория: 16 +

В журнале публикуются статьи по научным специальностям:

2.3. Информационные технологии и телекоммуникации

5.9. Филология

5.10. Искусствоведение и культурология

Издание для научных работников, преподавателей высшей школы, аспирантов, студентов и всех, кто интересуется достижениями современной российской науки.

Вёрстка: Шухер П.Д.
Корректор: Бальтерманц Л. Ф.

Учредитель: Былевский П. Г.

Издатель: Институт информационных наук Московского государственного лингвистического университета

Адрес редакции:
119034 Россия, Москва, ул. Остоженка, 36

https://www.linguanet.ru

E-mail: hi-hume@yandex.ru

Номер подписан в печать 20.12.2023

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ

ФИЛОЛОГИЯ

ИСКУССТВОВЕДЕНИЕ И КУЛЬТУРОЛОГИЯ

CONTENT

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

PHILOLOGY

ART AND CULTURAL STUDIES

УДК 519.728

ЛОГАРИФМИЧЕСКИЕ ПОДСТАНОВКИ: ОПРЕДЕЛЕНИЕ, СВОЙСТВА И ВОЗМОЖНОЕ ПРИМЕНЕНИЕ. ЧАСТЬ 2

Масленников М. Е.
Московский государственный лингвистический университет
(Россия, Москва),
mikhailmaslennikov@yandex.ru

Аннотация

Подстановки, взаимно-однозначные преобразования множества в себя, часто применяются для обработки информации. Среди них взаимно-однозначные преобразования множества всевозможных значений байт, кольца вычетов по модулю 256. Для операций фиксированной подстановки оказывается достаточно 256 байт памяти. Вычисления значения подстановки для конкретных байтов представляют собой простейшие операции обращения к памяти по их адресам. Для использования подстановок разработчики информационных систем учитывают операции с байтами вместе с подстановками. Наиболее часто используются сложения и вычитания байт по модулю 256. Каковы критерии при выборе подстановки?

В первой статье рассматривался вопрос о выборе критерия оценки подстановок. Одним из возможных критериев является так называемая матрица частот подстановки. Матрицу частот можно построить для любой подстановки, более хорошей будем считать ту подстановку, у которой матрица частот более «равномерная». В первой статье дается определение наиболее «равномерной» матрицы частот. Такая матрица называется оптимальной. В настоящей статье приводится пример подстановок с оптимальной матрицей частот. Такие подстановки называются логарифмическими.

Ключевые слова: подстановка, симметрическая группа подстановок, матрица частот подстановки, логарифмическая подстановка

LOGARITHMIC SUBSTITUTIONS: DEFINITION, PROPERTIES AND POSSIBLE APPLICATION. PART 2

Mikhail E. Maslennikov
Moscow State Linguistic University
(Russia, Moscow),
mikhailmaslennikov@yandex.ru

Abstract

Substitutions, one-to-one transformations of a set into itself, are often used to process information. Among them are one-to-one transformations of a set of possible byte values, rings of deductions modulo 256. 256 bytes of memory are sufficient for fixed substitution operations. Calculations of the substitution value for specific bytes are the simplest operations of accessing memory at their addresses. To use substitutions, information system developers take into account byte operations along with substitutions. The most commonly used additions and subtractions of bytes modulo 256. What are the criteria for choosing a substitution?

In the first article, the question of choosing a criterion for evaluating substitutions was considered. One of the possible criteria is the so-called substitution frequency matrix. The frequency matrix can be constructed for any substitution, we will consider the substitution with a more "uniform" frequency matrix to be the better one. The first article defines the most "uniform" frequency matrix. Such a matrix is called optimal. This article provides an example of substitutions with an optimal frequency matrix. Such substitutions are called logarithmic.

Keywords: substitution, symmetrical group of substitutions, matrix of the substitution frequency, logarithmic substitution

Список используемых определений, терминов и обозначений

N — некоторое целое число, превосходящее 2;
Z/N — кольцо вычетов по модулю N;
GF(P) — поле Галуа для простого целого P;
⊕ — операция сложения в поле Галуа;
⊖ — операция вычитания в поле Галуа;
{} — границы множества, например: {0} – множество, состоящее только из 0;
ϵ — символ, обозначающий принадлежность элемента множеству;
S_N — симметрическая группа всех подстановок на множестве {0,1,...,N – 1};
E_N — тождественная (единичная) подстановка из S_N;
^ — обозначение операции возведения в степень, т.е. A^x = A^(x);
/ — обозначение операции деления, т.е. $\frac{a}{b}$ = a/b;
**** — обозначение операции исключения элементов из множества;
U — обозначение операции объединения множеств;
=> — обозначение словосочетания «из этого следует»;
■ — окончание доказательства некоторого утверждения (Теоремы, Следствия к ней).

Если знак ■ стоит сразу после формулировки некоторого утверждения, то это означает, что доказательство утверждения очевидно.

Под весом некоторого элемента из Z/N будем понимать количество единиц в его двоичном представлении. Под суммарным весом нескольких элементов будем понимать сумму весов всех этих элементов.

Под подстановкой π из симметрической группы S_N будем понимать взаимно-однозначное отображение Z/N в Z/N [1].

Матрицей частот встречаемости разностей ненулевых биграмм произвольной подстановки $\pi \in S_N$, или просто *матрицей частот подстановки*, в дальнейшем будем называть матрицу P(π) размера (N – 1) x (N – 1), у которой на пересечении i-ой строки и j-го столбца, $i,j \neq 0$, находится элемент p_{ij}, равный числу решений системы

$$x - y = i$$
$$\pi(x) - \pi(y) = j$$

в кольце Z/N относительно x и y.

Через L_r при некотором фиксированном $r \in Z/N$ будем обозначать линейное преобразование Z/N в Z/N вида

$$L_r(x) = x + r$$

Очевидно, что $L_r \in S_N$.

Под произведением некоторых отображений π_1 и π_2 будем понимать их последовательное применение слева направо: $\pi = \pi_1\pi_2$ будет обозначать итоговое отображение $\pi(x) = \pi_2(\pi_1(x))$. Эти отображения могут быть, а могут и не быть подстановками.

Множество подстановок из S_N образуют группу относительно приведенной выше операции умножения, однако эта группа не является коммутативной, т.е. для многих (но не всех) подстановок $\pi_1\pi_2 \neq \pi_2\pi_1$ [2], [4].

Под ***циклом*** длины k будем понимать подстановку $\tau \in S_N$ такую, что в ней ровно k различных элементов из Z/N циклически переходят друг в друга, а остальные остаются без изменений. Цикл будем обозначать как $(x_1,x_2,\ldots,x_k)$, где $x_i \in Z/N$, $\tau(x_i) = x_{i+1}$ при всех i от 1 до k – 1, $\tau(x_k) = x_1$ и $\tau(y) = y$ для любого значения $y \in Z/N\backslash\{x_1,x_2,\ldots,x_k\}$. Величину k будем называть ***длиной цикла***. Цикл длины 1 будем называть тождественным [3].

Под ***транспозицией*** будем понимать цикл длины 2, т.е. подстановку $\tau \in S_N$ такую, что в Z/N найдутся ровно две различные точки a и b, для которых $\tau(a) = b$ и $\tau(b) = a$. Для всех остальных точек $x \in Z/N\backslash\{a,b\}$ справедливо $\tau(x) = x$. Транспозиция обозначается как пара из a и b: $\tau = (a,b) \in S_N$. Транспозиция называется тождественной, если a = b.

Подстановку $\pi \in S_N$ будем называть ***полноцикловой***, если она состоит из одного цикла длины N.

Точку $x \in Z/N$ будем называть ***неподвижной точкой*** подстановки $\pi \in S_N$, если $\pi(x) = x$.

Подстановку из S_N будем называть ***единичной*** или ***тождественной***, если число ее неподвижных точек равно N.

При рассмотрении элементов матрицы символом p_{ij} будем обозначать элемент, находящийся на пересечении i-ой строки и j-го столбца. Иногда индекс строки или столбца или и строки, и столбца будем приводить в круглых скобках: $p_{ij} = p_{(i)(j)} = p_{i(j)} = p_{(i)j}$.

Для сокращения текста будем объединять однотипные утверждения. Например, утверждение «в строках (столбцах) выполняется условие 1 (условие 2) соответственно» будет означать объединение двух утверждений: «в строках выполняется условие 1» и «в столбцах выполняется условие 2», а утверждение «в строках (столбцах) выполняется условие» будет означать, что это условие выполняется как в строках, так и в столбцах.

Поскольку в поле Галуа GF(P) [5] все ненулевые элементы образуют группу относительно операции умножения, то для каждого элемента a ϵ GF(P)\{0} найдется обратный к нему относительно операции умножения элемент, который мы будем обозначать, как a^{-1} или 1/a. При этом a^{-1} ϵ GF(P)\{0}, т.е. a^{-1} – это целое число такое, что $aa^{-1} = 1 (\mathrm{mod}\ P)$.

Под примитивным элементом поля Галуа GF(P) будем понимать ненулевое значение θ, образующее в поле Галуа группу из ненулевых элементов относительно операции умножения. Значение нулевой степени для θ будем считать равным 1. Для любого примитивного элемента θ справедливы следующие утверждения:

1. множество $\{\theta^0, \theta^1, \ldots, \theta^{P-2}\}$ совпадает с GF(P)\{0}, т. е. все элементы в нем ненулевые и различны;
2. для любых x и y ϵ Z/(P – 1) справедливо $\theta^x \theta^y = \theta^{x+y}$, где сложение x и y осуществляется в кольце Z/(P – 1);
3. $\theta^{P-1} = \theta^0 = 1$.

Всюду далее полагаем N ≥ 3, иные значения N в настоящей работе не рассматриваются.

Во всех трех статьях (частях), посвященных логарифмическим подстановкам, применяется единая сквозная нумерация формул и теорем, при этом первая цифра обозначает часть – 1, 2 или 3.

Основные логарифмические тождества

Всюду далее в настоящей работе мы будем использовать следующие основные логарифмические тождества [6] и свойства логарифмов применительно к полям Галуа GF(N + 1), когда N + 1 – простое число, θ – примитивный элемент GF(N + 1).

1. для всех x ϵ GF(N + 1)\{0} справедливо $\log_\theta(x)$ ϵ Z/N;
2. $\theta\hat{}(\log_\theta(x)) = x$ для всех x ϵ GF(N + 1)\{0};
3. $\log_\theta(1) = 0$;
4. $\log_\theta(\theta) = 1$;
5. $\theta^N = 1$;
6. $\log_\theta(\theta^x) = x$ для всех x ϵ Z/N;
7. $\log_\theta(xy) = \log_\theta(x) + \log_\theta(y)$;

8. $\log_\theta(x/y) = \log_\theta(x) - \log_\theta(y)$;
9. $\log_\theta((\ominus x)(\ominus y)) = \log_\theta(xy)$;
10. $\log_\theta((\ominus x)/(\ominus y)) = \log_\theta(x/y)$.

Отметим, что поскольку функция $\log_\theta(x)$ отображает GF(N + 1)\{0} в Z/N, то в соотношениях 7 и 8 операции сложения и вычитания осуществляются в Z/N.

В соотношениях 9 и 10 обозначение $\ominus x$ – это элемент из GF(N + 1), обратный к x относительно операции сложения, т.е. $\ominus x = N + 1 – x$.

Логарифмические подстановки

Пусть N – четное число такое, что N > 2 и N + 1 является простым числом. Такие числа в дальнейшем будем называть предпростыми. Примерами практически интересных предпростых чисел являются N = 16 и N = 256.

θ – произвольный примитивный элемент поля GF(N + 1);
ρ – произвольный элемент поля GF(N + 1);
r – произвольный элемент кольца Z/N.

Определим преобразование $LS_{\{\theta,\ \rho,\ r\}}$ из Z/N в Z/N следующим образом:

$$LS_{\{\theta,\rho,r\}}(x) = \log_\theta(\theta^{x+r} \oplus \rho) \quad \text{если } \theta^{x+r} \oplus \rho \neq 0,$$
$$LS_{\{\theta,\rho,r\}}(x) = \log_\theta \rho \quad \text{если } \theta^{x+r} \oplus \rho = 0, \qquad (2.1),$$

где

$\oplus$ –операция сложения в поле GF(N + 1);
+ - операция сложения в кольце Z/N.

Замечания.

1. Символом $\ominus$ будем обозначать операцию вычитания в поле GF(N + 1).
2. Для простоты операцию возведения примитивного элемента θ в степень x будем обозначать либо θ^x, либо $\theta\hat{}(x)$. Последнее будет использоваться в случаях, когда показателем степени является громоздкое выражение.

В дальнейшем значение x, при котором $\theta^{x+r} \oplus \rho = 0$, будем называть эксклюзивной точкой преобразования $LS_{\{\theta,\ \rho,\ r\}}$.

Теорема 2.1.

Пусть в преобразовании (2.1) ρ = 0. Тогда $LS_{\{\theta,\ 0,\ r\}}(x) = x + r$, т. е. $LS_{\{\theta,\ 0,\ r\}}$ совпадает с линейным преобразованием L_r.

Доказательство.

Используем логарифмическое тождество $\log_\theta(\theta^x) = x$.■

Замечание 1.

Очевидно, что при ρ = 0 у преобразования (2.1) нет эксклюзивной точки.

Замечание 2.

$LS_{\{\theta,\ 0,\ 0\}}$ – тождественная (единичная) подстановка E_N на множестве Z/N.

Теорема 2.2.

При любом ненулевом значении ρ ϵ GF(N + 1) $LS_{\{\theta,\ \rho,\ r\}}$ – взаимно-однозначное отображение Z/N в Z/N.

Доказательство.

Обозначим $Q^r_\rho = \{\theta^{0+r}\oplus\rho,\ \theta^{1+r}\oplus\rho,\ldots,\ \theta^{(N-1)+r}\oplus\rho\}$ - множество из N элементов поля GF(N + 1). Поскольку θ – примитивный элемент поля GF(N + 1), то множество Q^r_ρ совпадает с GF(N + 1) \ {ρ} при любом значении ρ из GF(N + 1) и r из Z/N.

Определим преобразование $\phi_{\{\theta,\rho,r\}}$ следующим образом:

$$\phi_{\{\theta,\rho,r\}}(x) = \theta^{x+r}\oplus\rho \qquad (2.2)$$

для всех x ϵ Z/N.

Это однозначное отображение Z/N в Q^r_ρ, т.е. в GF(N + 1) \ {ρ}, так как при любых $x_1 \neq x_2$ справедливо $\phi_{\{\theta,\rho,r\}}(x_1) \neq \phi_{\{\theta,\rho,r\}}(x_2)$.

Обратным к (2.2) будет преобразование $\phi^{-1}_{\{\theta,\rho,r\}}$ вида $\phi^{-1}_{\{\theta,\rho,r\}}(x) = \log_\theta(x\ominus\rho) - r$. Обратное преобразование также однозначно отображает GF(N + 1) \ {ρ} в Z/N, т.е. преобразование (2.2) является взаимно-однозначным отображением Z/N в GF(N + 1) \ {ρ}.

Определим отображение $\tau_{\{\theta,\rho,r\}}$ множества GF(N + 1) \ {0} в Z/N следующим образом:

$$\tau_{\{\theta,\rho,r\}}(x) = \log_\theta(x) \qquad (2.3)$$

для всех x ϵ GF(N + 1)\{0}. Отображение $\tau_{\{\theta,\rho,r\}}$ является однозначным отображением множества GF(N + 1)\{0} в Z/N.

Обратным к (2.3) будет преобразование $\tau^{-1}_{\{\theta,\rho,r\}}(x) = \theta^x$. Оно однозначно отображает Z/N в GF(N + 1)\{0}, т.е. (2.3) является взаимно-однозначным отображением GF(N + 1)\{0} в Z/N.

Определим отображение $\alpha_{\{\theta,\rho,r\}}$ множества GF(N + 1) \ {ρ} в множество GF(N + 1) \ {0} следующим образом:

$$\alpha_{\{\theta,\rho,r\}}(x) = x, \text{ при всех } x \neq 0,\ x \neq \rho$$
$$\alpha_{\{\theta,\rho,r\}}(0) = \rho \qquad (2.4)$$

Обратным к (2.4) будет $\alpha^{-1}_{\{\theta,\rho,r\}}$, для которого

$$\alpha^{-1}_{\{\theta,\rho,r\}}(x) = x, \text{ при всех } x \neq \rho,\ x \neq 0$$
$$\alpha^{-1}_{\{\theta,\rho,r\}}(\rho) = 0$$

Очевидно, что (2.4) – взаимно-однозначное отображение GF(N + 1) \ {ρ} в GF(N + 1) \ {0}.

Рассмотрим последовательность преобразований (2.2), (2.4), (2.3), осуществляющих отображение Z/N в Z/N:

$\phi_{\{\theta,\rho,r\}}\ \alpha_{\{\theta,\rho,r\}}\ \tau_{\{\theta,\rho,r\}}(x) = \alpha_{\{\theta,\rho,r\}}\ \tau_{\{\theta,\rho,r\}}(\theta^{x+r}\oplus\rho) = \tau_{\{\theta,\rho,r\}}(\theta^{x+r}\oplus\rho) = \log_\theta(\theta^{x+r}\oplus\rho)$,
если $\theta^{x+r}\oplus\rho \neq 0$,

$\phi_{\{\theta,\rho,r\}}\ \alpha_{\{\theta,\rho,r\}}\ \tau_{\{\theta,\rho,r\}}(x) = \alpha_{\{\theta,\rho,r\}}\ \tau_{\{\theta,\rho,r\}}(\theta^{x+r}\oplus\rho) = \alpha_{\{\theta,\rho,r\}}\ \tau_{\{\theta,\rho,r\}}(0) = \tau_{\{\theta,\rho,r\}}(\rho) = \log_\theta\rho$,
если $\theta^{x+r}\oplus\rho = 0$.

Таким образом, последовательность преобразований (2.2), (2.4), (2.3), осуществляющих отображение Z/N в Z/N, является преобразованием (2.1). Поскольку все преобразования (2.2), (2.4), (2.3) являются взаимно-однозначными, то и (2.1) является взаимно-однозначным отображением Z/N в Z/N.■

Подстановки $LS_{\{\theta,\ \rho,\ r\}}$ вида (2.1) при $\rho \neq 0$ в дальнейшем будем называть ***логарифмическими***.

Логарифмические подстановки при r = 0 будем называть ***чистыми***.

Значение $\rho \neq 0$ логарифмической подстановки $LS_{\{\theta,\ \rho,\ r\}}$ будем называть ***образующим элементом*** логарифмической подстановки.

Теорема 2.3.

Пусть $LS_{\{\theta,\ \rho,\ r\}}$ – логарифмическая подстановка. Тогда

$$LS_{\{\theta,\ \rho,\ r\}} = L_r\, LS_{\{\theta,\ \rho,\ 0\}} \qquad (2.5)$$

и обратной к ней будет подстановка

$$LS^{-1}_{\{\theta,\ \rho,\ r\}} = LS_{\{\theta,\ \ominus\rho,\ 0\}} L_{-r} \qquad (2.6)$$

где L_r – линейное преобразование.

Доказательство.

Соотношение (2.5) очевидно вытекает из (2.1).

Подстановка $LS^{-1}_{\{\theta,\ \rho,\ r\}}$, обратная к $LS_{\{\theta,\ \rho,\ r\}}$, является последовательностью взаимно-однозначных преобразований (2.3), (2.4), (2.2):

$LS^{-1}_{\{\theta,\ \rho,\ r\}}(x) = \tau^{-1}_{\{\theta,\rho,r\}}\alpha^{-1}_{\{\theta,\rho,r\}}\phi^{-1}_{\{\theta,\rho,r\}}(x) = \alpha^{-1}_{\{\theta,\rho,r\}}\phi^{-1}_{\{\theta,\rho,r\}}(\theta^x) = \phi^{-1}_{\{\theta,\rho,r\}}(\theta^x) = \log_\theta(\theta^x \ominus \rho) - r,$ если $\theta^x \ominus \rho \neq 0$,

$LS^{-1}_{\{\theta,\ \rho,\ r\}}(x) = \tau^{-1}_{\{\theta,\rho,r\}}\alpha^{-1}_{\{\theta,\rho,r\}}\phi^{-1}_{\{\theta,\rho,r\}}(x) = \alpha^{-1}_{\{\theta,\rho,r\}}\phi^{-1}_{\{\theta,\rho,r\}}(\theta^x) = \phi^{-1}_{\{\theta,\rho,r\}}(0) = \log_\theta(\ominus\rho) - r,$ если $\theta^x \ominus \rho = 0$.

Таким образом, справедливо (2.6). ■

Следствие 1.

При любом r ϵ Z/N матрица частот логарифмической подстановки $LS_{\{\theta,\ \rho,\ r\}}$ совпадает с матрицей частот соответствующей ей чистой логарифмической подстановки $LS_{\{\theta,\ \rho,\ 0\}}$.

Доказательство.

Непосредственно следует из (2.5) и Теоремы 1.5.■

Следствие 2.

При любом r ϵ Z/N матрица частот логарифмической подстановки $LS^{-1}_{\{\theta,\ \rho,\ r\}}$, обратной к логарифмической подстановке $LS_{\{\theta,\ \rho,\ r\}}$, совпадает с матрицей частот чистой логарифмической подстановки $LS_{\{\theta,\ \ominus\rho,\ 0\}}$.

Доказательство.

Непосредственно следует из (2.6) и Теоремы 1.5.■

Следствие 3.

Пусть $LS_{\{\theta,\ \rho,\ 0\}}$ – чистая логарифмическая подстановка. Обратной к ней будет также чистая логарифмическая подстановка вида $LS_{\{\theta,\ \ominus\rho,\ 0\}}$.

Доказательство.

Непосредственно следует из (2.6) при r = 0.■

Аналогично (1.15), для любого фиксированного i ϵ Z/N, i ≠ 0, и произвольного x ϵ Z/N определим

$$\mu^{i}_{\{\theta,\rho,r\}}(x) = LS_{\{\theta,\rho,r\}}(x + i) - LS_{\{\theta,\rho,r\}}(x) \qquad (2.7)$$

Очевидно, что при любом ненулевом значении i и любом x ϵ Z/N справедливо $\mu^{i}_{\{\theta,\rho,r\}}(x) \neq 0$, т.е. $\mu^{i}_{\{\theta,\rho,r\}}$ отображает Z/N в Z/N\{0}.

Теорема 2.4.

Пусть $LS_{\{\theta,\rho,r\}}$ - произвольная логарифмическая подстановка, x_0 – ее эксклюзивная точка. Тогда для любого i ≠ 0 и для любой пары $x_1, x_2 \in Z/N\backslash\{x_0 - i, x_0\}$, $x_1 \neq x_2$, справедливо

$$\mu^{i}_{\{\theta,\rho,r\}}(x_1) \neq \mu^{i}_{\{\theta,\rho,r\}}(x_2). \qquad (2.8)$$

Доказательство.

Пусть $x_1, x_2 \in Z/N\backslash\{x_0 - i, x_0\}$ такие, что

$$\mu^{i}_{\{\theta,\rho,r\}}(x_1) = \mu^{i}_{\{\theta,\rho,r\}}(x_2)$$

Из этого вытекает, что

$$\theta\hat{}(\mu^{i}_{\{\theta,\rho,r\}}(x_1)) = \theta\hat{}(\mu^{i}_{\{\theta,\rho,r\}}(x_2)). \qquad (2.9)$$

Из (2.9) и (2.7) получаем

$$\theta\hat{}(LS_{\{\theta,\rho,r\}}(x_1 + i) - LS_{\{\theta,\rho,r\}}(x_1)) = \theta\hat{}(LS_{\{\theta,\rho,r\}}(x_2 + i) - LS_{\{\theta,\rho,r\}}(x_2)),$$

откуда следует

$$\theta\hat{}(LS_{\{\theta,\rho,r\}}(x_1 + i))/\theta\hat{}(LS_{\{\theta,\rho,r\}}(x_1)) = \theta\hat{}(LS_{\{\theta,\rho,r\}}(x_2 + i))/\theta\hat{}(LS_{\{\theta,\rho,r\}}(x_2)) \qquad (2.10)$$

Из условия $x_1, x_2 \in Z/N\backslash\{x_0 - i, x_0\}$ вытекает, что все точки $x_1, x_2, x_1+i, x_2+i, \in Z/N$ не являются эксклюзивными. Тогда из (2.10), основного логарифмического тождества $\theta\hat{}(\log_\theta(x)) = x$ и определения (2.1) следует, что

$$(\theta\hat{}(x_1+r+i) \oplus \rho)/(\theta\hat{}(x_1+r) \oplus \rho) = (\theta\hat{}(x_2+r+i) \oplus \rho)/(\theta\hat{}(x_2+r) \oplus \rho) \qquad (2.11)$$

Из (2.11) вытекает

$$(\theta\hat{}(x_1+r+i) \oplus \rho)(\theta\hat{}(x_2+r) \oplus \rho) = (\theta\hat{}(x_2+r+i) \oplus \rho)(\theta\hat{}(x_1+r) \oplus \rho).$$

Раскрывая скобки, получаем

$$\theta\hat{}(x_1+r+i+x_2+r) \oplus \theta\hat{}(x_1+r+i)\rho \oplus \rho\theta\hat{}(x_2+r) \oplus \rho^2 = \theta\hat{}(x_2+r+i+x_1+r) \oplus \theta\hat{}(x_2+r+i)\rho \oplus \rho\theta\hat{}(x_1+r) \oplus \rho^2.$$

После сокращения, получаем

$$\theta\hat{}(x_1+r+i) \oplus \theta\hat{}(x_2+r) = \theta\hat{}(x_2+r+i) \oplus \theta\hat{}(x_1+r),$$

откуда вытекает

$$\theta\hat{}(x_1+r+i) \ominus \theta\hat{}(x_1+r) = \theta\hat{}(x_2+r+i) \ominus \theta\hat{}(x_2+r).$$

Выносим общий член за скобки

$$\theta\hat{}(x_1+r)(\theta^{i} \ominus 1) = \theta\hat{}(x_2+r)(\theta^{i} \ominus 1)$$

Поскольку значение i – ненулевое, то $\theta^{i} \neq 1$, $(\theta^{i} \ominus 1) \neq 0$ и после сокращения получаем

$$\theta\hat{}(x_1+r) = \theta\hat{}(x_2+r),$$

откуда следует, что $x_1 = x_2$.

Таким образом, если $\mu^{i}_{\{\theta,\rho,r\}}(x_1) = \mu^{i}_{\{\theta,\rho,r\}}(x_2)$, то отсюда вытекает, что $x_1 = x_2$. Следовательно, если $x_1 \neq x_2$, то отсюда следует (2.8)■

Следствие 1.

Для произвольной логарифмической подстановки $LS_{\{\theta,\ \rho,\ r\}}$, любого ненулевого i є Z/N\{0} число нулей в i-ой строке (столбце) матрицы частот не превосходит 1.

Доказательство.

Размер строки матрицы частот равен N – 1, количество элементов в $Z/N\backslash\{x_0 - i,\ x_0\}$ не меньше N – 2, все значения (2.8), по частотам встречаемости которых строится i-я строка матрицы частот, различны в силу Теоремы 2.4. Следовательно, в i-ой строке матрицы частот количество ненулевых элементов не меньше, чем N – 2. Отсюда число нулей не превосходит (N – 1) – (N – 2) = 1.

Поскольку подстановкой, обратной к $LS_{\{\theta,\ \rho,\ r\}}$, в соответствии с (2.6) будет $LS_{\{\theta,\ \ominus\rho,\ 0\}}L_{-r}$, то матрица частот подстановки, обратной к $LS_{\{\theta,\ \rho,\ r\}}$, в соответствии с Теоремой 1.5, будет совпадать с матрицей частот $LS_{\{\theta,\ \ominus\rho,\ 0\}}$, обратной к $LS_{\{\theta,\ \rho,\ 0\}}$. Поскольку обратная подстановка $LS_{\{\theta,\ \ominus\rho,\ 0\}}$, в соответствии с Теоремой 1.4, имеет матрицу частот, транспонированную из матрицы частот $LS_{\{\theta,\ \rho,\ 0\}}$, то отсюда вытекает утверждение Следствия 1 к Теореме 2.4 для столбцов.■

Рассмотрим эксклюзивную точку x_0 произвольной логарифмической подстановки.

Теорема 2.5.

Пусть $LS_{\{\theta,\ \rho,\ r\}}$ - произвольная логарифмическая подстановка, x_0 – ее эксклюзивная точка.

Тогда

$$x_0 = \log_\theta(\ominus\rho) - r. \qquad (2.12)$$

Доказательство.

Непосредственно следует из (2.1).■

Следствие 1.

При $\rho = \ominus 1$ справедливо $x_0 = -r$. ■

Следствие 2.

При $\rho = 1$ справедливо $x_0 = N/2 - r$.

Доказательство.

В силу (2.12) достаточно доказать, что при $\rho = 1$ и r = 0 справедливо $x_0 = N/2$.

При $\rho = 1$ и r = 0 из (2.12) вытекает, что

$$\theta\hat{}(x_0) = \ominus 1 \qquad (2.13)$$

Возведя обе части (2.13) в квадрат, получаем

$$\theta\hat{}(2x_0) = 1$$

откуда следует, что $2x_0 = 0$ в кольце Z/N. Таким образом, x_0 может быть равен либо 0, либо N/2. При $x_0 = 0$, $\rho = 1$ и r = 0 не выполняется (2.1), таким образом, $x_0 = N/2$.■

Рассмотрим диагональ матрицы частот логарифмической подстановки.

Теорема 2.6.

Пусть $LS_{\{\theta, \rho, r\}}$ - произвольная логарифмическая подстановка, x_0 – ее эксклюзивная точка. Тогда для любого $i \neq 0$ и для любой точки $x \in Z/N\backslash\{x_0 - i, x_0\}$ справедливо

$$\mu^i_{\{\theta, \rho, r\}}(x) \neq i \qquad (2.14)$$

Доказательство.

Пусть $x \in Z/N\backslash\{x_0 - i, x_0\}$ такой, что

$$\mu^i_{\{\theta, \rho, r\}}(x) = i$$

Из этого вытекает, что

$$\theta\hat{}(\mu^i_{\{\theta, \rho, r\}}(x)) = \theta^i. \qquad (2.15)$$

Из (2.15) и (2.7) получаем

$$\theta\hat{}(LS_{\{\theta, \rho, r\}}(x + i) - LS_{\{\theta, \rho, r\}}(x)) = \theta^i,$$

откуда следует

$$\theta\hat{}(LS_{\{\theta, \rho, r\}}(x + i))/\theta\hat{}(LS_{\{\theta, \rho, r\}}(x)) = \theta^i$$

Поскольку ни x, ни x + i не являются эксклюзивными точками, то

$$\theta^{x+i+r} \oplus \rho = \theta^i(\theta^{x+r} \oplus \rho)$$

Раскрыв скобки, получаем $\rho = \theta^i\rho$, откуда следует, что $\rho = 0$. Противоречие с тем, что подстановка $LS_{\{\theta, \rho, r\}}$ является логарифмической.■

Теорема 2.7.

Пусть $LS_{\{\theta, \rho, 0\}}$ - произвольная чистая логарифмическая подстановка, x_0 – ее эксклюзивная точка. Тогда на диагонали матрицы частот подстановки $LS_{\{\theta, \rho, r\}}$ ненулевыми являются элементы с номерами i1 и i2, где $i1 = \log_\theta(2)$ и $i2 = \log_\theta(2^{-1})$ и только они.

Доказательство.

В силу Теоремы 2.6 для любого $i \in Z/N\backslash\{0\}$ и всех элементов из $x \in Z/N\backslash\{x_0 - i, x_0\}$ справедливо (2.14). Таким образом, создавать ненулевые элементы на диагонали матрицы частот могут только две точки: x_0 и $x_0 - i$, т.е. либо $\mu^i_{\{\theta, \rho, 0\}}(x_0) = i$, либо $\mu^i_{\{\theta, \rho, 0\}}(x_0 - i) = i$.

Пусть $\mu^i_{\{\theta, \rho, 0\}}(x_0) = i$.

$$\begin{aligned}
&\mu^i_{\{\theta, \rho, 0\}}(x_0) = i && \Rightarrow\\
&\theta\hat{}(LS_{\{\theta, \rho, 0\}}(x_0 + i) - LS_{\{\theta, \rho, 0\}}(x_0)) = \theta^i && \Rightarrow\\
&\theta\hat{}(LS_{\{\theta, \rho, 0\}}(x_0 + i))/\theta\hat{}(LS_{\{\theta, \rho, 0\}}(x_0)) = \theta^i && \Rightarrow\\
&(\theta\hat{}(x_0 + i) \oplus \rho)/\rho = \theta^i && \Rightarrow\\
&\theta\hat{}(x_0 + i) = \rho\,(\theta^i \ominus 1) && \Rightarrow\\
&\theta\hat{}(x_0)\,\theta^i = \rho\,(\theta^i \ominus 1)
\end{aligned}$$

В силу (2.1) при r = 0 для эксклюзивной точки x_0 справедливо $x_0 = \log_\theta(\ominus\rho)$, т.е. $\theta\hat{}(x_0) = \ominus\rho$.

Таким образом, $2\rho\theta^i = \rho$ и, поскольку $\rho \neq 0$, то $2\theta^i = 1 \Rightarrow \theta^i = 2^{-1} \Rightarrow i = \log_\theta(2^{-1})$.

Пусть $i = \log_\theta(2^{-1})$. Покажем, что в этом случае выполняется $\mu^i_{\{\theta, \rho, 0\}}(x_0) = i$.

$$\begin{aligned}
&\mu^i_{\{\theta, \rho, 0\}}(x_0) = LS_{\{\theta, \rho, 0\}}(x_0 + i) - LS_{\{\theta, \rho, 0\}}(x_0) && \Rightarrow\\
&\theta\hat{}(\mu^i_{\{\theta, \rho, 0\}}(x_0)) = \theta\hat{}(LS_{\{\theta, \rho, 0\}}(x_0 + i) - LS_{\{\theta, \rho, 0\}}(x_0)) && \Rightarrow\\
&\theta\hat{}(\mu^i_{\{\theta, \rho, 0\}}(x_0)) = \theta\hat{}(LS_{\{\theta, \rho, 0\}}(x_0 + i))/\theta\hat{}(LS_{\{\theta, \rho, 0\}}(x_0)) && \Rightarrow\\
&\theta\hat{}(\mu^i_{\{\theta, \rho, 0\}}(x_0)) = (\theta\hat{}(x_0 + i) \oplus \rho)/\rho && \Rightarrow
\end{aligned}$$

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0))\rho = \theta\hat{}(x_0 + i) \oplus \rho$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0))\rho = \theta\hat{}(x_0)\theta^{i} \oplus \rho$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0))\rho = \rho(1 \ominus 2^{-1})$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0)) = (1 \ominus 2^{-1}) = 2^{-1}$ =>

$\mu^{i}_{\{\theta,\rho,0\}}(x_0) = \log_{\theta}(2^{-1})$.

Пусть $\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i) = i$.

$\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i) = i$ =>

$\theta\hat{}(LS_{\{\theta,\rho,0\}}(x_0) - LS_{\{\theta,\rho,0\}}(x_0 - i)) = \theta^{i}$ =>

$\theta\hat{}(LS_{\{\theta,\rho,0\}}(x_0))/\theta\hat{}(LS_{\{\theta,\rho,0\}}(x_0 - i)) = \theta^{i}$ =>

$\rho/(\theta\hat{}(x_0 - i) \oplus \rho) = \theta^{i}$ =>

$(\theta\hat{}(x_0 - i) \oplus \rho)\theta^{i} = \rho$ =>

$\theta\hat{}(x_0) \oplus \rho\theta^{i} = \rho$ =>

$\rho\theta^{i} = 2\rho$

Поскольку $\rho \neq 0$, то $\theta^{i} = 2$ => $i = \log_{\theta}(2)$.

Пусть $i = \log_{\theta}(2)$. Покажем, что в этом случае выполняется $\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i) = i$.

$\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i) = LS_{\{\theta,\rho,0\}}(x_0) - LS_{\{\theta,\rho,0\}}(x_0 - i)$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i)) = \theta\hat{}(LS_{\{\theta,\rho,0\}}(x_0) - LS_{\{\theta,\rho,0\}}(x_0 - i))$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i)) = \theta\hat{}(LS_{\{\theta,\rho,0\}}(x_0))/\theta\hat{}(LS_{\{\theta,\rho,0\}}(x_0 - i))$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i)) = \rho/(\theta\hat{}(x_0 - i) \oplus \rho)$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i))(\theta\hat{}(x_0 - i) \oplus \rho) = \rho$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i))(\theta\hat{}(x_0)/\theta^{i} \oplus \rho) = \rho$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i)) (1 \ominus \theta^{-1}) \rho = \rho$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i))(1 \ominus 2^{-1}) = 1$ =>

$\theta\hat{}(\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i)) = 2$ =>

$\mu^{i}_{\{\theta,\rho,0\}}(x_0 - i) = \log_{\theta}(2)$. ■

Замечание.

Поскольку $\theta^{N} = 1$, то $\log_{\theta}(2^{-1}) = \log_{\theta}(1/2) = \log_{\theta}(1) - \log_{\theta}(2) = N - \log_{\theta}(2)$.

Следствие 1.

Пусть $LS_{\{\theta,\ \rho,\ 0\}}$ - произвольная чистая логарифмическая подстановка. Тогда ее матрица частот является симметричной оптимальной, в которой две оптимальных строки (столбца) с номерами $i1 = \log_{\theta}(2)$ и $i2 = N - \log_{\theta}(2)$.■

Суммируя результаты Теорем 2.2 – 2.7, получаем следующую Теорему 2.8.

Теорема 2.8.

Пусть:

$N + 1$ – простое число;

θ – произвольный примитивный элемент поля $GF(N + 1)$;

ρ – произвольный ненулевой элемент поля $GF(N + 1)$;

$r1, r2$ – произвольные элементы из Z/N.

Тогда для любой подстановки π вида

$$\pi = L_{r1}LS_{\{\theta,\ \rho,\ 0\}}L_{r2} \qquad (2.16),$$

где $LS_{\{\theta,\ \rho,\ 0\}}$ – чистая логарифмическая подстановка вида (2.1), L_{r1} и L_{r2} – подстановки вида (1.6), справедливо:

— матрица частот P(π) является симметричной оптимальной;

— $P(\pi) = P(\pi^{-1})$;

— матрица P(π) содержит две (два) оптимальных строки (столбца) с номерами $\log_\theta(2)$ и $N - \log_\theta(2)$.■

Таким образом, номера оптимальных строк и столбцов в P(π) зависят исключительно от выбора примитивного элемента θ поля Галуа GF(N + 1).

Теорема 2.9.

Пусть $LS_{\{\theta,\ \rho,\ 0\}}$ – произвольная чистая логарифмическая подстановка. Тогда при любом x ϵ Z/N справедливо

$$LS_{\{\theta,\ \rho,\ 0\}}(x) \neq x. \qquad (2.17)$$

Доказательство.

Покажем, что (2.17) справедливо для эксклюзивной точки x_0. Пусть $LS_{\{\theta,\ \rho,\ 0\}}(x_0) = x_0$. Тогда в соответствии с (2.1) и (2.12)

$\log_\theta(\rho) = \log_\theta(\ominus\rho)$ =>

$\log_\theta(\rho) - \log_\theta(\ominus\rho) = 0$ =>

$\log_\theta(\ominus 1) = 0$ =>

$\theta\text{^}\log_\theta(\ominus 1) = \theta^0$ =>

$\ominus 1 = 1$.

Последнее равенство неверно для полей Галуа.

Таким образом, $LS_{\{\theta,\ \rho,\ 0\}}(x_0) \neq x_0$.

Пусть $x \in Z/N\backslash\{x_0\}$. Пусть $LS_{\{\theta,\ \rho,\ 0\}}(x) = x$. В соответствии с (2.1) имеем

$\log_\theta(\theta^x \oplus \rho) = x$ =>

$\theta\text{^}(\log_\theta(\theta^x \oplus \rho)) = \theta^x$ =>

$\theta^x \oplus \rho = \theta^x$ =>

$\rho = 0$.

Последнее равенство противоречит определению логарифмической подстановки.■

Пусть $\pi = LS_{\{\theta,\ \rho,\ 0\}}$ – произвольная чистая логарифмическая подстановка. Рассмотрим подстановку $\pi^2 = \pi\,\pi$.

Ниже символом (a,b) обозначается транспозиция, т.е. подстановка из S_N, переставляющая значения a и b.

Теорема 2.10.

Пусть

$\pi 1 = LS_{\{\theta,\ \rho 1,\ 0\}}$ – произвольная чистая логарифмическая подстановка, $x1_0$ – ее эксклюзивная точка,

$\pi 2 = LS_{\{\theta,\ \rho 2,\ 0\}}$ – произвольная чистая логарифмическая подстановка, $x2_0$ – ее эксклюзивная точка,

$\rho 1 \oplus \rho 2 \neq 0$.

Тогда

$$(\log_\theta(\ominus\rho1), \log_\theta(\ominus(\rho1 \oplus \rho2)))LS_{\{\theta,\ \rho1,\ 0\}}\ LS_{\{\theta,\ \rho2,\ 0\}} = \ LS_{\{\theta,\ \rho1\oplus\rho2,\ 0\}}, \quad (2.18)$$

$$LS_{\{\theta,\ \rho1,\ 0\}}\ LS_{\{\theta,\ \rho2,\ 0\}}(\log_\theta(\rho2), \log_\theta((\rho1 \oplus \rho2))) = \ LS_{\{\theta,\ \rho1\oplus\rho2,\ 0\}}. \quad (2.19)$$

Перед доказательством Теоремы 2.10 сделаем два замечания.

Замечание 1.

В случае, когда $\rho1 \oplus \rho2 = 0$, то в соответствии с Теоремой 2.3, справедливо $\pi2 = \pi1^{-1}$.

Замечание 2.

Эксклюзивной точкой для логарифмической подстановки $LS_{\{\theta,\ \rho1\oplus\rho2,\ 0\}}$, как следует из (2.12), будет значение $\log_\theta(\ominus(\rho1 \oplus \rho2))$.

Замечание 3.

Для эксклюзивной точки x_0 чистой логарифмической подстановки π, в силу (2.12) справедливо $x_0 = \log_\theta(\ominus\rho)$. Величина $\log_\theta(\rho)$, согласно (2.6) и (2.12), является эксклюзивной точкой подстановки π^{-1}. В дальнейшем величину $\log_\theta(\rho)$ будем также называть ***обратной эксклюзивной точкой*** подстановки π.

Доказательство Теоремы 2.10.

Заметим, что в силу (2.12) для эксклюзивных точек $x1_0$ и $x2_0$ справедливо:

$$x1_0 = \log_\theta(\ominus\rho1)$$
$$x2_0 = \log_\theta(\ominus\rho2)$$

Таким образом,

$$x2_0 + x1_0 = \log_\theta(\ominus\rho2) + \log_\theta(\ominus\rho1) \quad =>$$
$$x2_0 + x1_0 = \log_\theta(\rho2\ \rho1) \quad =>$$
$$x2_0 = \log_\theta(\rho2\ \rho1) - x1_0 = \log_\theta((\ominus\rho2)\ (\ominus\rho1)) - x1_0.$$

Рассмотрим произвольную чистую логарифмическую подстановку $\pi = LS_{\{\theta,\ \rho,\ 0\}}$ при некотором ненулевом значении ρ. Пусть x_0 – ее эксклюзивная точка.

Пусть $x \in Z/N \setminus \{x_0\}$ – произвольная точка такая, что $x = x_0 + k$ при некотором ненулевом k. Тогда в силу (2.1)

$$\theta\hat{}(x_0) = \ominus\rho \quad =>$$
$$\pi(x) = \log_\theta(\theta\hat{}(x_0 + k) \ominus \theta\hat{}(x_0)) \quad =>$$
$$\pi(x) = \log_\theta(\theta\hat{}(x_0)(\theta^k \ominus 1)) \quad =>$$
$$\pi(x) = x_0 + \log_\theta(\theta^k \ominus 1). \quad (2.20)$$

Таким образом, если $x \in Z/N \setminus \{x1_0\}$, т.е. $x = x1_0 + k1$ при некотором ненулевом значении $k1$, то

$$\pi1(x) = x1_0 + k2, \quad (2.21)$$

где

$$k2 = \log_\theta(\theta^{k1} \ominus 1). \quad (2.22)$$

Предположим, что

$$\pi1(x) = x2_0 + k3 \quad =>$$
$$\pi1(x) = \log_\theta(\rho2\ \rho1) - x1_0 + k3$$

Таким образом, с учетом (2.20)

$x1_0 + \log_\theta(\theta^{k1} \ominus 1) = \log_\theta(\rho2\ \rho1) - x1_0 + k3$ =>

$k3 = 2x1_0 + \log_\theta(\theta^{k1} \ominus 1) - \log_\theta(\rho2\ \rho1)$ =>

$k3 = 2\log_\theta(\ominus\rho1) + \log_\theta(\theta^{k1} \ominus 1) - \log_\theta(\ominus\rho2) - \log_\theta(\ominus\rho1)$ =>

$k3 = \log_\theta(\ominus\rho1) - \log_\theta(\ominus\rho2) + \log_\theta(\theta^{k1} \ominus 1)$

Таким образом, k3 = 0 тогда и только тогда, когда

$\log_\theta(\rho2/\rho1) = \log_\theta(\theta^{k1} \ominus 1)$. =>

$\rho2/\rho1 = \theta^{k1} \ominus 1$ =>

$\theta^{k1} = 1 \oplus \rho2/\rho1$ =>

$k1 = \log_\theta(1 \oplus \rho2/\rho1)$ =>

$k1 = \log_\theta(\rho1 \oplus \rho2) - \log_\theta(\rho1)$. (2.23)

Следовательно, если $x = x1_0 + k1$ при некотором ненулевом значении k1, то точка $\pi1(x)$ будет эксклюзивной для логарифмической подстановки $\pi2$ тогда и только тогда, когда выполнено (2.23).

В силу (2.12) для такой точки x имеем

$x = x1_0 + k1 = x1_0 + \log_\theta(\rho1 \oplus \rho2) - \log_\theta(\rho1) = \log_\theta(\ominus\rho1) - \log_\theta(\rho1) + \log_\theta(\rho1 \oplus \rho2)$ =>

$$x = \log_\theta(\ominus1) + \log_\theta(\rho1 \oplus \rho2) = \log_\theta(\ominus(\rho1 \oplus \rho2)),$$

т.е. значение $x = x1_0 + k1$, где k1 удовлетворяет (2.23), является эксклюзивной точкой логарифмической подстановки $LS_{\{\theta,\ \rho1 \oplus \rho2,\ 0\}}$. В дальнейшем будем обозначать эксклюзивную точку $LS_{\{\theta,\ \rho1 \oplus \rho2,\ 0\}}$ как $x1\_2_0$.

Предположим, что $x = x1_0 + k1$, где значение k1 – ненулевое и соотношение (2.23) не имеет места. Тогда точка x не является эксклюзивной для $\pi1$ и точка $\pi1(x)$ не является эксклюзивной для $\pi2$. В этом случае

$\pi1\pi2(x) = \pi2(\pi1(x)) = \pi2(\log_\theta(\theta^x \oplus \rho1)) = \log_\theta(\theta\text{^}(\log_\theta(\theta^x \oplus \rho1)) \oplus \rho2)$ =>

$$\pi1\pi2(x) = \log_\theta(\theta^x \oplus (\rho1 \oplus \rho2)). \quad (2.24)$$

Пусть $x = x1_0$. Тогда

$$\pi1\pi2(x) = \pi2(\pi1(x)) = \pi2(\log_\theta(\rho1)). \quad (2.25)$$

В силу (2.12) если $x2_0 = \log_\theta(\rho1)$, то $\log_\theta(\rho1) = \log_\theta(\ominus\rho2)$ => $\rho1 \oplus \rho2 = 0$, что противоречит условиям Теоремы 2.10.

Таким образом, из (2.25) вытекает, что при $x = x1_0$

$$\pi1\pi2(x) = \log_\theta(\theta\text{^}(\log_\theta(\rho1)) \oplus \rho2) = \log_\theta(\rho1 \oplus \rho2). \quad (2.26)$$

Если значение x удовлетворяет (2.23), то $\pi1(x) = x2_0$ и, следовательно,

$$\pi1\pi2(x) = \log_\theta(\rho2) \quad (2.27)$$

Из (2.25), (2.26) и (2.27) вытекает, что подстановка $\pi1\pi2$, являющаяся произведением логарифмических подстановок $LS_{\{\theta,\ \rho1,\ 0\}}$ и $LS_{\{\theta,\ \rho2,\ 0\}}$, отличается от подстановки $LS_{\{\theta,\ \rho1 \oplus \rho2,\ 0\}}$ только в двух эксклюзивных точках: $x1_0$ – эксклюзивная точка $LS_{\{\theta,\ \rho1,\ 0\}}$ и $x1\_2_0$ – эксклюзивная точка $LS_{\{\theta,\ \rho1 \oplus \rho2,\ 0\}}$. Для совпадения произведения $\pi1\pi2$ с $LS_{\{\theta,\ \rho1 \oplus \rho2,\ 0\}}$ нужно переставить эти значения до выполнения операции умножения подстановок $\pi1\pi2$, либо после умножения переставить результаты применения $\pi1\pi2$ к этим точкам.

Перестановка эксклюзивных точек до операции умножения равносильна умножению слева произведения подстановок на транспозицию $(x1_0, x1\_2_0) = ((\log_\theta(\ominus\rho1), \log_\theta(\ominus(\rho1 \oplus \rho2)))$, откуда следует (2.18).

Перестановка результатов применения произведения $\pi1\pi2$ к эксклюзивным точкам $x1_0$ и $x1\_2_0$ в силу (2.26) и (2.27) равносильна умножению справа произведения подстановок на транспозицию $(\log_\theta(\rho2), \log_\theta((\rho1 \oplus \rho2)))$, откуда следует (2.19).■

Перед следующей Теоремой 2.11 сделаем несколько очевидных Замечаний, касающихся циклов.

Замечание 1.

Пусть подстановка $\tau \in S_N$ – цикл длины k, $\tau = (x_1,x_2,\ldots,x_k)$. Тогда $\tau^{-1} = (x_k,x_{k-1},\ldots,x_1)$.■

Замечание 2.

Пусть подстановка $\tau \in S_N$ – цикл длины k, $\tau = (x_1,x_2,\ldots,x_k)$, $x_{k+1} \in Z/N\backslash\{x_1,x_2,\ldots,x_k\}$. Тогда в результате умножения слева этого цикла на транспозицию (x_k, x_{k+1}) получается цикл $(x_1,x_2,\ldots,x_k,x_{k+1})$ длины k + 1.

$$(x_k, x_{k+1})(x_1,x_2,\ldots,x_k) = (x_1,x_2,\ldots,x_k,x_{k+1}) \blacksquare \qquad (2.28)$$

Замечание 3.

Пусть подстановка $\tau \in S_N$ – цикл длины k, $\tau = (x_1,x_2,\ldots,x_k)$, $x_{k+1} \in Z/N\backslash\{x_1,x_2,\ldots,x_k\}$. Тогда в результате умножения справа этого цикла на транспозицию (x_1, x_{k+1}) получается цикл $(x_1,x_2,\ldots,x_k,x_{k+1})$ длины k + 1.

$$(x_1,x_2,\ldots,x_k)(x_1,x_{k+1}) = (x_1,x_2,\ldots,x_k,x_{k+1}) \blacksquare \qquad (2.29)$$

Теорема 2.11.

Пусть $\pi = LS_{\{\theta,\ \rho,\ 0\}}$ – произвольная чистая логарифмическая подстановка, k – произвольное число из $GF(N + 1)\backslash\{0\}$.

Пусть

$$C_{\ominus k} = (\log_\theta(\ominus\rho), \log_\theta(\ominus2\rho),\ldots,\log_\theta(\ominus k\rho)) \qquad (2.30)$$

и

$$C_k = (\log_\theta(\rho), \log_\theta(2\rho),\ldots,\log_\theta(k\rho))$$

циклы длины k.

Пусть

$$C^{-1}_k = (\log_\theta(k\rho), \log_\theta((k-1)\rho),\ldots,\log_\theta(\rho)) \qquad (2.31)$$

цикл, обратный к циклу C_k.

Тогда

$$C_{\ominus k}\pi^k = LS_{\{\theta,\ k\rho,\ 0\}}, \qquad (2.32)$$

$$\pi^k C^{-1}_k = LS_{\{\theta,\ k\rho,\ 0\}}. \qquad (2.33)$$

Доказательство.

Соотношения (2.32) и (2.33) будем доказывать методом математической индукции.

При k = 1 циклы в (2.32) и (2.33) тождественны.

При k = 2 соотношения (2.32) и (2.33) вытекают из (2.18) и (2.19) Теоремы 2.10.

Заметим, что в циклах (2.30) и (2.31) все элементы – различные.

Пусть (2.32) верно при любом n < k, рассмотрим случай n = k.

$$C_{\ominus k}\pi^k = C_{\ominus k}\pi^{k-1}\pi.$$

В силу (2.28)

$$C_{\ominus k} = (\log_\theta(\ominus(k-1)\rho), \log_\theta(\ominus k\rho))\, C_{\ominus(k-1)}.$$

Таким образом, с учетом (2.18) и предположения индукции $C_{\ominus k}\pi^k = (\log_\theta(\ominus(k-1)\rho), \log_\theta(\ominus k\rho))\, C_{\ominus(k-1)}\, \pi^{k-1}\pi = (\log_\theta(\ominus(k-1)\rho), \log_\theta(\ominus k\rho))LS_{\{\theta,\ (k-1)\rho,\ 0\}}\, LS_{\{\theta,\ \rho,\ 0\}} = LS_{\{\theta,\ k\rho,\ 0\}}$.

Пусть (2.33) верно при любом n < k, рассмотрим случай n = k.

$$\pi^k C^{-1}{}_k = \pi\pi^{k-1}C^{-1}{}_k.$$

В силу (2.29)

$$C^{-1}{}_k = C^{-1}{}_{k-1}\,(\log_\theta((k-1)\rho), \log_\theta(k\rho)).$$

Таким образом, с учетом (2.19) и предположения индукции $\pi^k C_k = \pi\,\pi^{k-1}C^{-1}{}_{k-1}(\log_\theta((k-1)\rho), \log_\theta(k\rho)) = LS_{\{\theta,\ \rho,\ 0\}}\, LS_{\{\theta,\ (k-1)\rho,\ 0\}}(\log_\theta((k-1)\rho), \log_\theta(k\rho)) = LS_{\{\theta,\ k\rho,\ 0\}}$. ■

Теорема 2.12.

Любая чистая логарифмическая подстановка $LS_{\{\theta,\ \rho,\ 0\}}$ является полноцикловой.

Доказательство.

Рассмотрим полный цикл

$$C_N = (\log_\theta(\rho), \log_\theta(2\rho),\ldots,\log_\theta(N\rho)) \qquad (2.34)$$

Заметим, что $N\rho = (N + 1 - 1)\rho = \ominus\rho$ и в соответствии с (2.12), значение $x_0 = \log_\theta(\ominus\rho)$ является эксклюзивной точкой $LS_{\{\theta,\ \rho,\ 0\}}$.

Имеем при всех $k \neq N$

$$LS_{\{\theta,\ \rho,\ 0\}}(\log_\theta(k\rho)) = \log_\theta(\theta\hat{}(\log_\theta(k\rho)) \oplus \rho) = (\log_\theta((k + 1)\rho)).$$

При k = N

$$LS_{\{\theta,\ \rho,\ 0\}}(\log_\theta(N\rho)) = LS_{\{\theta,\ \rho,\ 0\}}(x_0) = \log_\theta(\rho).$$

Таким образом, цикл (2.34) является логарифмической подстановкой $LS_{\{\theta,\ \rho,\ 0\}}$.■

Список источников

1. Винберг Э. Б. Курс алгебры. М.: Факториал-Пресс, 2001. 544 с.

2. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука, Физматлит, 1982. 288 с.

3. Кострикин А. И. Введение в алгебру. Часть III. Основные структуры. М.: Физматлит, 2004. 272 с.

4. Курош А. Г. Теория групп. М.: Наука, Физматлит, 1967. 648 с.

5. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х т. М.: Мир, 1988. 428 с., 818 с.6.

Нестеренко Ю. В. Дискретное логарифмирование (Глава 4, 8) / Введение в криптографию. Под общей ред. В. В. Ященко. С.-Пб.: Питер, 2001. 288 с.

Об авторе

Масленников Михаил Евгеньевич — кандидат физико-математических наук, эксперт кафедры международной информационной безопасности Института информационных наук; Московский государственный лингвистический университет (Россия, Москва).
E-mail: mikhailmaslennikov@yandex.ru.

About the author

Mikhail E. Maslennikov — Candidate of Physical and Mathematical Sciences, expert of the Department of International Information Security of the Institute of Information Sciences; Moscow State Linguistic University (Russia, Moscow).
E-mail: mikhailmaslennikov@yandex.ru.

УДК 004.094

ОСОБЕННОСТИ МОДЕЛИРОВАНИЯ ГРАВИТАЦИОННОГО ИЗЛУЧЕНИЯ

Фисенко С. И.
Московский государственный лингвистический университет (Россия, Москва)
StanislavFisenko@yandex.ru

Аннотация
Рассматривается методика моделирования образом, позволяющим вычислять квантовые состояния, генерируемые гравитационным взаимодействием. Моделирование не предполагает никаких дополнительных допущений или построений, кроме уравнений квантовой механики и уравнений релятивистской теории гравитации с Λ-членом. Демонстрация осуществляется существованием спектра стационарных состояний в соответствующем гравитационном поле.

Ключевые слова: гравитационное излучение, моделирование, квантовые состояния, релятивистская теории гравитации

FEATURES OF GRAVITATIONAL RADIATION MODELING

Stanislav I. Fisenko
Moscow State Linguistic University (Russia, Moscow)
StanislavFisenko@yandex.ru

Abstract
The modeling technique is considered in a way that allows calculating the quantum states generated by the gravitational interaction. Modeling does not involve any additional assumptions or constructions, except for the equations of quantum mechanics and the equations of the relativistic theory of gravity with a Λ-term.The demonstration is carried out by the existence of a spectrum of stationary states in the corresponding gravitational field.

Keywords: gravitational radiation, modeling, quantum states, relativistic theory of gravity

Введение

Считается, что согласно Общей теории относительности (ОТО), системы с переменными квадрупольными или более высокими мультипольными моментами могут генерировать гравитационное излучение. При этом предположении мощность соответствующего гравитационного излучения пропорциональна квадрупольному тензору распределения масс излучающей системы, а постоянная (гравитационная постоянная Ньютона), которая включена в эту зависимость, дает порядок величины мощности излучения. Не законность использования этой формулы заключается не в использовании квадрупольного приближения, а в схеме расчета. Система может излучать только в определенных квантовых состояниях, и это относится к любому излучению, независимо от его природы. Это аксиома квантовой механики, так же как и существование элементарного источника излучения, обладающего этими состояниями. Следовательно, теоретическое предсказание спектра гравитационного излучения требует оценки квантовых состояний, переходы между которыми вызывают излучение.

Методика моделирования гравитационного излучения

Понятие гравитационного излучения как излучения того же уровня, что и электромагнитное излучение, основано на теоретически обоснованном и экспериментально подтвержденном факте существования стационарных состояний электрона в его гравитационном поле, характеризующихся гравитационной постоянной K = 1042 G (G — ньютоновская гравитационная постоянная) и неустранимой кривизной пространства-времени Λ [1; 2]. К таким экспериментальным фактам относятся, в частности, данные об расширении характерных спектров излучения многоэлектронных атомов. Такое расширение спектров может быть вызвано только дополнительным механизмом расширения, в частности, наличием возбужденных состояний электронов в их собственном гравитационном поле. Другим подтверждающим фактом является новая линия в спектре рентгеновского излучения, полученная при наблюдении MOS-камеры обсерватории XMM-Newton [3]. Обнаружение неопознанной линии излучения в сложенном рентгеновском спектре скоплений галактик.

Эта линия, в отличие от других идентифицированных линий электромагнитного излучения, не может быть отнесена к какому-либо атомному переходу. Энергетический спектр электрона в его собственном гравитационном поле и энергетические спектры многоэлектронных атомов

таковы, что возникает резонанс этих спектров. Результатом этого резонансного взаимодействия является появление, в том числе новых линий, электромагнитных переходов, не связанных с атомными переходами. Гравитационное излучение (в результате переходов частицы через стационарные состояния в ее собственном гравитационном поле) может возбуждаться в плотной высокотемпературной плазме и усиливаться при определенных условиях, но его усиление приведет к сжатию излучающей системы.

Следовательно, в условиях усиления гравитационного излучения будет наблюдаться не само гравитационное излучение, а только результат его действия. Сам факт сжатия плазмы излучаемым гравитационным полем может быть использован для термоядерного синтеза. Количественные характеристики спектра гравитационного излучения (как излучения одного уровня с электромагнитным излучением) могут быть определены путем расширения спектра электромагнитного излучения[4; 5]. Соответствующие результаты были опубликованы в прилагаемой статье и представлены на XXII Международном совещании "Физические интерпретации теории относительности-2021", 05–09 июля, Москва, 2021. Система может излучать только в определенных квантовых состояниях.

Эта аксиома квантовой механики, безусловно, верна и для гравитационного излучения, а также для существования элементарного источника излучения, обладающего этими состояниями. Гравитационных волн с постоянной G, предположительно излучаемых системой тел с колеблющимся, но случайным квадрупольным моментом, нет и быть не может (именно это необоснованное предположение лежит в основе проектов LIGO и LISA [6; 7; 8]). Это полное игнорирование квантовых концепций. Без сомнения, исследования, связанные с попыткой зарегистрировать гравитационное излучение черных дыр, глубоко ошибочны.Именно высокотемпературная плазма (лабораторная или астрофизическая) должна быть подходящим объектом исследования.

Кстати, Нобелевская премия уже была присуждена в 1993 году за предполагаемое обнаружение макроскопического источника гравитационных волн (Рассел Алан Халс), однако сейчас об этом никто даже не упоминает.

Заключение

Следовательно, наибольший интерес (с точки зрения регистрации гравитационного излучения) в астрофизических исследованиях представляют исследования в рамках программы Advanced Telescope for High-Energy Astrophysics (Athena).Факт наличия гравитационного излучения

(как излучения того же уровня, что и электромагнитное излучение) будет вытекать из регистрации:

а) линии излучения горячего межгалактического газа, заполняющего скопление галактик, которые не соответствуют никаким атомным переходам,

б) регистрация участков спектра мягкого рентгеновского излучения, таких, что подгонка в соответствии с известными механизмами расширения не полностью воспроизводит точное расширение зарегистрированной части спектра излучения.

Это будет свидетельствовать о наличии дополнительного механизма расширения регистрируемой части спектра характеристического излучения за счет вклада возбужденных состояний электронов в их собственное гравитационное поле.

Более подробно этот вопрос описан в статье [9].

Список источников

1. Fisenko S. On the issue of gravitational radiation and thermonuclear fusion // Journal of Physics Conference Series. 2020. 1557(1):012019. DOI: 10.1088/1742–6596/1557/1/012019

2. Fisenko S. I., Beilinson M. M., Umanov B. G. Some notes on the concept of “strong” gravitation and possibilities of its experimental investigation // Physics Letters. 1990. Vol.148. Iss.8–9. Pp.405–407. DOI: 10.1016/0375–9601(90)90489-b

3. Boyarsky A., Ruchayskiy O., Iakubovskyi D. Franse J. An unidentified line in X-ray spectra of the Andromeda galaxy and Perseus galaxy cluster // Physical Review Letters. 2014. Vol. 113. Iss.25. Pp.1–5. DOI: 10.1103/PhysRevLett.113.251301

4. Politov V. Yu., Potapov A. V., Antonova L. V. Proceeding of International Conference V Zababakhin Scientific Proceedings”. 1998. Pp.28–34.

5. Burenkov O. M. et al. New Configuration of Experiments for MAGO Program / XIV International Conference on Megagauss Magnetic Field Generation and Related Topics (Maui, Havaii, USA, October 14–19, 2012). Pp. 95–99. DOI: 10.1109/MEGAGAUSS.2012.6781427.

6. Arun K. G. et al. New Horizons for Fundamental Physics with LISA // Living Reviews in Relativity. 03.05.2022. [Электронный ресурс] URL: https://arxiv.org/abs/2205.01597 (Дата обращения 18.12.2023)

7. Cañas Herrera G., Contigiani O., Vardanyan V. Cross-correlation of the astrophysical gravitational-wave background with galaxy clustering // Physical

Review D. 2020. Vol.102. Iss.4. [Электронный ресурс] URL: https://arxiv.org/abs/1910.08353 (Дата обращения 18.12.2023)

8. Tahura S., Nichols D. A., Yagi K. Gravitational-wave memory effects in Brans-Dicke theory: Waveforms and effects in the post-Newtonian approximation // Physical Review D. 2021. Vol.104. Iss.10. [Электронный ресурс] URL: https://arxiv.org/abs/2107.02208 (Дата обращения 18.12.2023) DOI: 10.1103/PhysRevD.104.104010

9. Fisenko S. Gravitational radiation and nuclear fusion // Oriental Journal of Physical Sciences. 2019. Vol.4. Iss.1. Pp.04–05. DOI: 10.13005/OJPS04.01.02

Об авторе

Фисенко Станислав Иванович —
кандидат технических наук, доцент, доцент кафедры международной информационной безопасности Московского государственного лингвистического университета
(Россия, Москва)
E-mail: StanislavFisenko@yandex.ru –

About the author

Stanislav I. Fisenko —
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of International Information Security, Moscow State Linguistic University
(Russia, Moscow)
E-mail: StanislavFisenko@yandex.ru

УДК 004.056

ВОЗРАСТАНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК РЕЗУЛЬТАТ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Помещиков С. Е.
Московский университет МВД России им. В.Я. Кикотя (Россия, Москва)
spomeshchikov@yandex.ru

Научный руководитель:
Полянская Е. П.
Московский университет МВД России им. В.Я. Кикотя (Россия, Москва)
azhara87@bk.ru

Аннотация
В эпоху цифровой трансформации, когда компьютерно-сетевые технологии проникли во все сферы жизни, уровень угроз информационной безопасности значительно возрос. От крупных корпораций до обычных пользователей — все стали более уязвимыми для кибератак и киберпреступлений. В свете этих изменений важность обеспечения информационной безопасности стала национальным и международным приоритетом. В данной статье рассмотрены факторы, которые привели к увеличению угроз информационной безопасности, а также поднят вопрос цифровой грамотности населения.

Ключевые слова: информационная безопасность, информационные технологии, киберугрозы, персональные данные, цифровая трансформация

INCREASING THREATS TO INFORMATION SECURITY AS A RESULT OF DIGITAL TRANSFORMATION

Stanislav E. Pomeshchikov
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
spomeshchikov@yandex.ru

Scientific supervisor:
Elena P. Polyanskaya
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
azhara87@bk.ru

Abstract
In the era of digital transformation, when computer and network technologies have penetrated into all spheres of life, the level of threats to information security has increased significantly. From large corporations to ordinary users, everyone has become more vulnerable to cyber attacks and cybercrimes. In light of these changes, the importance of information security has become a national and international priority. This article examines the factors that have led to an increase in threats to information security, and also raises the issue of digital literacy of the population.

Keywords: information security, information technology, cyber threats, personal data, digital transformation

В современном мире цифровая трансформация играет всё более значительную роль, занимая лидирующие позиции во всех областях нашей жизни. С развитием технологий и использованием цифровых платформ всё больше организаций и отраслей сталкиваются с необходимостью адаптироваться к новым реалиям. Однако, вместе с открывающимися возможностями, которые предоставляет цифровая трансформация, возникают и новые угрозы в области информационной безопасности.

В свете цифровой трансформации становится ясно, что безопасность информации стала одним из главных факторов, определяющих успешность и устойчивость организаций в современных реалиях. Основная проблема заключается в том, что с увеличением уровня цифровой трансформации, растет и уровень угроз информационной безопасности. Всё больше различных организаций расширяются в цифровое пространство, что означает и рост количества злоумышленников, желающих похитить ценную информацию. Однако, данные о природе и уровне угроз в этом новом контексте остаются недостаточными. В связи с этим, целью данного исследования является анализ и оценка важности информационной безопасности в эпоху цифровой трансформации и возросшего уровня угроз в этой области.

Для полного понимания изучаемой проблемы следует для начала обозначить основные понятия, используемые в сфере информационной безопасности. Информационная безопасность (ИБ) — это комплекс мер, направленных на защиту информации от несанкционированного доступа, использования или распространения. В условиях современных технологий и возросшей угрозы цифровых преступлений, ИБ играет огромную роль в защите как личных данных, так и данных организаций и государственных структур.

Информационные технологии (ИТ) — это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов посредством компьютерно-сетевых технологий и решений [1].

Современные киберугрозы включают в себя кибератаки, вирусы, хакерские атаки и многие другие способы и формы такого рода преступлений. Если обратиться к статистическим данным, можно заметить, что за последние несколько лет количество и сложность угроз многократно возросли. Причиной этого является стремительное развитие технологий и общая цифровая трансформация.

Нарушение информационной безопасности может иметь серьезные последствия. Прежде всего, это уязвимость персональных данных. Возможна утечка личной информации и финансовые мошенничества. Также нарушение информационной безопасности может нанести вред бизнесу, включая потерю данных, нарушение производственных процессов и репутационный ущерб. Кроме того, угрозы для национальной безопасности и государственных структур также являются серьезной проблемой.

В первую очередь именно нарушение информационной безопасности имеет серьезные последствия, прежде всего оставляя уязвимыми персональные данные. Нарушение информационной безопасности наносит огромный ущерб бизнесу и различным предприятиям, поскольку данные хранятся с нарушением основных правил и требований, что в свою очередь позволяет злоумышленникам получить к ним доступ. Это приводит к замедлению производственных процессов или же к полной их остановке. Также стоит учитывать и репутационный ущерб, который тоже имеет большое значение для организаций в современных реалиях. Кроме того, угрозы для государственных структур и национальной безопасности в целом также являются серьезной проблемой, требующей правильного подхода.

Наиболее распространёнными киберугрозами для компаний в настоящее время являются:

• Методы социальной инженерии, такие как фишинговые сайты (54%) и электронные письма (27%);

• Вредоносное программное обеспечение (ПО), в частности растёт доля инцидентов с использованием шпионского ПО в атаках на частных лиц (65%), в то же время доля использования шпионского ПО в успешных атаках на организации сохраняет свой уровень (20%) [3];

• Программы вымогатели (шифровальщики), которые по сей день атакуют в совершенно разных секторах нашей жизни: образования и науки, государственных и медицинских организациях (11%) [4].

Многие компании считают главной проблемой кибербезопасности в России низкий уровень цифровой грамотности сотрудников. На основании опроса, проведённого Лабораторией Касперского, более половины представителей бизнеса (57%) в России считают ключевой проблемой кибербезопасности низкий уровень цифровой грамотности сотрудников. На втором месте — потеря или утечка данных (40%), на третьем — нехватка бюджета, необходимого для обеспечения кибербезопасности корпоративной ИТ-инфраструктуры (31%) [2].

Исходя из вышеперечисленного, можно сделать вывод о необходимости развития эффективной защиты от угроз в информационной сфере. Важно обеспечить образование и информационную грамотность населения, ИБ должна быть включена в образовательные программы. Обучение сотрудников и пользователей основам безопасности должно быть важным аспектом работы любой организации. В частности, для повышения общей цифровой грамотности сотрудников рассматривается возможность внедрения новой политики безопасности корпоративных электронных почт предприятий, а также безопасного обращения с интернет-ресурсами. Важна профилактика и повышение осведомленности о роли каждого человека в защите от таких угроз.

Выводы

ИБ является актуальной и важной темой в эпоху цифровой трансформации. Ее роль необходима для защиты от постоянно растущего уровня угроз, связанных с развитием технологий и цифровизацией процессов и общества в целом. Реализация мер по защите цифровой информации, а также обучение сотрудником и общества в целом правильной работе с информацией в современных условиях стремительного развития информационных технологий и повышение общего уровня цифровой грамотности населения поможет снизить возможность киберугроз и предотвратить негативные последствия.

Список источников

1. «Об информации, информационных технологиях и о защите информации». Федеральный закон от 27.07.2006 № 149-ФЗ // КонсультантПлюс (Электронный ресурс) URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c (дата обращения: 01.11.2023).

2. Низкий уровень цифровой грамотности — главная проблема кибербезопасности для бизнеса в России // Лаборатория Касперского (Электронный ресурс) URL: https://www.kaspersky.ru/about/press-releases/2023_nizkij-uroven-cifrovoj-gramotnosti-glavnaya-problema-kiberbezopasnosti-dlya-biznesa-v-rossii (дата обращения: 09.11.2023).

3. Актуальные киберугрозы: III квартал 2023 года // Positive Technologies (Электронный ресурс) URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q3 (дата обращения: 10.11.2023).

4. Актуальные киберугрозы: II квартал 2023 года // Positive Technologies (Электронный ресурс) URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2023-q2 (дата обращения: 10.11.2023).

Об авторе

Помещиков Станислав Евгеньевич — курсант 2 курса Московского университета МВД России им. В. Я. Кикотя (Россия, Москва)
E-mail: spomeshchikov@yandex.ru

Научный руководитель

Полянская Елена Петровна — старший преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России им. В. Я. Кикотя (Россия, Москва)
E-mail: azhara87@bk.ru

About the author

Stanislav E. Pomeshchikov — 2nd year cadet of the Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
E-mail: spomeshchikov@yandex.ru

Scientific supervisor

Elena P. Polyanskaya — senior lecturer at the Department of Information Security of the educational and Scientific complex of Information Technologies Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
E-mail: azhara87@bk.ru

УДК 004+34

ПРОБЛЕМА «РЕГУЛЯТОРНОЙ ГИЛЬОТИНЫ» ДЛЯ БИЗНЕС-СРЕДЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Прохорова Д. А.
Московский университет МВД России им. В.Я. Кикотя (Россия, Москва)
dasha280803@mail.ru

Научный руководитель:
Полянская Е. П.
Московский университет МВД России им. В.Я. Кикотя (Россия, Москва)
azhara87@bk.ru

Аннотация

В данной статье предлагается рассмотреть относительно новый механизм деятельности государства «регуляторная гильотина», который позволяет пересмотреть нормативно-правовую базу преимущественно в экономической сфере, проработать рациональность требований, предъявляемых к предприятиям и снизить количество издержек. Данный механизм представлен на примере России и других стран, где был реализован такой метод, включая новые федеральные законы, подзаконные акты, которые появились для осуществления целей «регуляторной гильотины». Соответственно результаты применения такого метода, которые имеются к настоящему моменту.

Ключевые слова: регуляторная гильотина, государственный контроль, предпринимательская деятельность, развитие нормативно-правовых актов, контрольно-надзорная деятельность

THE PROBLEM OF THE “REGULATORY GUILLOTINE” FOR THE INFORMATION TECHNOLOGY BUSINESS ENVIRONMENT

Darya A. Prokhorova
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
dasha280803@mail.ru

Scientific supervisor:
Elena P. Polyanskaya
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
azhara87@bk.ru

Abstract
This article proposes to consider a relatively new mechanism of state activity «regulatory guillotine», which allows us to revise the regulatory framework mainly in the economic sphere, work out the rationality of the requirements for enterprises and reduce the number of costs. This mechanism is presented using the example of Russia and other countries where this method was implemented. New federal laws and regulations that have appeared to implement the goals of the «regulatory guillotine». Accordingly, the results of applying this method that are available to date.

Keywords: regulatory guillotine, state control, entrepreneurial activity, development of normative legal acts, control and supervisory activities

Современное общество динамично развивается в настоящее время, в связи с чем претерпевает множество изменений в различных сферах жизни. Отрасль права не стала исключением. На это влияет множество факторов, в том числе развитие цифровых технологий, увеличение угроз в сфере безопасности, расширение прав человека и многое другое. Одним из результатов развития и изменения общества стала «регуляторная гильотина».

Регуляторная гильотина обычно относится к некоторым мерам и положениям, направленным на контроль и регулирование определенных областей деятельности, как правило, в сфере бизнеса, включая информационные технологии. Это может включать в себя разработку новых нормативно-правовых актов, пересмотр и отмену старых, лицензирование и другие инструменты, направленные на обеспечение соблюдения действующего законодательства и стандартов. Подобные меры часто используются для обеспечения защиты интересов общества, поддержания порядка и стимулирования развития экономики.

Термин «регуляторная гильотина» не имеет нормативного законодательного определения, однако можно сказать, что он означает инструмент пересмотра и отмены нормативных правовых актов, негативно влияющих на общий бизнес-климат и регуляторную среду, включая

отрасль информационных технологий [1]. Этот инструмент позволяет государству и органам управления регулировать деятельность предприятий, ограничивать недобросовестные практики, создавать четкие требования к хозяйствующим субъектам, снизить риски причинения ущерба охраняемым ценностям. «Гильотина» также может использоваться для предотвращения монополий, защиты прав потребителей, поддержания конкуренции и обеспечивать экономическую стабильность в обществе.

В России началась реализация регуляторной гильотины в 2020 году совместно с появлением нового Федерального закона «Об обязательных требованиях в Российской Федерации» от 31.07.2020 №247-ФЗ. Согласно ч.1 ст.1 выше названного ФЗ, данный закон определяет правовые основы применения содержащихся в нормативных правовых актах требований, которые связаны с осуществлением предпринимательской и иной экономической деятельности [2]. То есть представленные обязательные требования должны базироваться на таких принципах, как законность, обоснованность, исполнимость.

К новшествам после вступления закона в силу можно отнести: введены правила вступления в силу нормативных правовых актов с обязательными требованиями; создание реестра обязательных требований; для обеспечения анализа обязательных требований периодический пересмотр подзаконных актов (до 6 лет); участие заинтересованных лиц на этапах установления и оценки применения обязательных требований [1]. Также исходя из ст. 15 настоящего ФЗ, обеспечение реализации положений обязательных требований закона должно быть реализовано посредством использования регуляторной гильотины. На основании данного закона можно сказать, что термин «регуляторная гильотина» используется в качестве системы регулирования и контроля, прежде всего, в экономической деятельности.

Целью гильотины можно определить сокращение производственных издержек предприятий на соблюдение избыточных требований, которые уже не являются актуальными и необходимыми в настоящее время. Избыточные требования к предпринимательской деятельности порождают риски, в результате которых предприятие может закрыться после проверки, так как у него не хватает ресурсов для обеспечения соответствия предъявленным требованиям. Также увеличивается вероятность проявления коррупционной составляющей, представителям включая информационных технологий иногда проще откупиться от контролирующих органов, чем реализовать требования, предъявляемые к их предприятию. Таким образом, возникает вопрос о целесообразности

предъявляемых требований к экономической деятельности. Устранение сомнительных требований в современных реалиях может поспособствовать развитию инвестиций и всех включая отрасль информационных технологий в целом, что благоприятно скажется на экономике страны.

Реализацию регуляторной гильотины можно назвать реформой в контрольно-надзорной деятельности со стороны государства в отношении информационных технологий. Как определил Президент России в 2019 году, суть данной реформы состоит в отмене с 1 января 2021 года всех нормативных правовых актов, устанавливающих требования, соблюдение которых подлежит проверке при осуществлении государственного контроля, и введение в действие новых норм, содержащих актуализированные требования, разработанные с учетом риск-ориентированного подхода и современного уровня технологического развития [3]. С появлением регуляторной гильотины появились так называемые «рабочие группы». Были сформированы 43 рабочие группы по реализации механизма регуляторной гильотины [4]. Их состав был определен подкомиссией по совершенствованию контрольных (надзорных) и разрешительных функций федеральных органов исполнительной власти.

Согласно данным Министерства экономического развития в РФ, в реализации «гильотины» принимали участие 39 министерств и ведомств, более 1300 экспертов, 43 рабочие группы [1]. Предложения, связанные с пересмотром и отменой нормативных правовых актов, должны были рассматриваться в рабочих группах, перечень которых был подписан Заместителем Председателя Правительства Российской Федерации-Руководитель Аппарата Правительства Российской Федерации, К. Чуйченко [5].

В данном перечне содержалось наименование рабочей группы, ее сфера деятельности, ответственные федеральные органы исполнительной власти, участвующие федеральные органы исполнительной власти. Рабочая группа могла влиять на решения, связанные с пересмотром нормативных правовых актов посредством голосования, однако при возникновении разногласий, данный вопрос рассматривался Подкомиссией по совершенствованию контрольных (надзорных) и разрешительных функций федеральных органов исполнительной власти Правительственной комиссии по проведению административной реформы.

Однако заметных результатов данного регулирующего фильтра особо не было. На это повлияли такие факторы, как различная степень вовлеченности участников рабочих групп в ту или иную тему, выносимую

на обсуждение. Также повлияло то, что новые акты должны были соответствовать требованиям федеральных законов, в отношении которых регуляторная гильотина не проводилась [6]. Кроме того, деятельность рабочих групп была закрытой. Возможно, если бы она имела публичный характер, эффективность данного метода была бы выше.

Можно выделить несколько ключевых методов, которые в себя включает гильотина в России:

1. Законодательный и правоприменительный: данный метод включает в себя пересмотр действующих нормативных правовых актов; соответствие их правил, которые устанавливают стандарты поведения для предприятий, организаций и граждан в различных сферах деятельности, настоящим реалиям; необходимость отмены нормативных правовых актов для достижения целей гильотины; разработка и внедрение новых законов и стандартов.

2. Диалог с бизнесом и обществом в области информационных технологий: данный метод был осуществлен посредством создания рабочих групп, которые участвовали в пересмотре действующих нормативных правовых актов; именно установление диалога с представителями рассматриваемой отрасли и другими заинтересованными лицами позволяет более объективно подойти к решению поставленной задачи и учесть мнения представителей экономической деятельности в данном вопросе.

3. Обновление законодательства: именно периодический просмотр действующих нормативных правовых актов на соответствие предъявляемых требований настоящим реалиям позволит более эффективно решать задачи гильотины.

4. Лицензирование и сертификация: установление порядка лицензирования и сертификации для контроля за профессиональной деятельностью, качеством продукции или услуг, обеспечивая соответствие установленным стандартам.

5. Контроль и надзор: создание государственных и негосударственных органов, ответственных за контроль и надзор за соблюдением законов; это включает в себя проверки, мониторинг и реагирование на нарушения; при этом осуществляемый контроль и надзор должен быть более лоялен к представителям информационных технологий и носить не карательный характер, а превентивный, чтобы не было рисков проявления коррупционной составляющей.

6. Наказания и санкции: введение административной и уголовной ответственности за нарушение установленных требований, в случае неоднократных нарушений, которые влекут снижение качества услуг, оказываемых потребителям.

Вышеперечисленные методы широко используются в России для решения задач, связанных с реализацией регуляторной гильотины. Однако Россия была не первой страной, открывшей для себя подобный метод регулирования экономической составляющей страны. Регуляторная гильотина широко используется в США, Евросоюзе, Китае. Современный метод использования «регуляторной гильотины» был основан на опыте Швеции и Южной Кореи [7].

Данный метод включает в себя некоторый алгоритм, действуя по которому, можно добиться весомых результатов в сфере развития бизнеса и экономики в отрасли информационных технологий. Для начала Правительство или иной орган определяют цель «регуляторной гильотины». Ведомства предоставляют список нормативных правовых актов, которые относятся к теме «гильотины». Документ, не прошедший трехступенчатую фильтрацию, упрощается либо отменяется.

В США также используется метод «регуляторной гильотины». Данный термин не представляет собой официальный термин в юридической терминологии. В США существует система различных регуляторных мер и органов, которые обеспечивают соблюдение законов в различных областях и реализацию гильотины. Примеры регуляторных агентств в США включают:

1. SEC (Комиссия по ценным бумагам и биржам): данный регулятор способствует финансовой стабильности и защите инвесторов через контроль за ценными бумагами и финансовыми компаниями.

2. FDA (Агентство по контрою за продуктами и лекарствами): ответственно за контроль качества и безопасности продуктов питания, лекарств и медицинских устройств.

3. EPA (Агентство по охране окружающей среды): занимается регулированием вопросов окружающей среды и обеспечением ее защиты; деятельность агентства направлена на соблюдение экологических стандартов, контроль за выбросами и обеспечению устойчивости окружающей среды.

4. FCC (Федеральная комиссия связи): отвечает за регулирование связи и массовых коммуникаций, обеспечивая их безопасность и равенства доступа.

5. FTC (Комиссия по торговле): защищает потребителей и обеспечивает соблюдение антимонопольных законов, предотвращает недобросовестную конкуренцию, что способствует честной торговле и защите конкуренции.

Помимо этого, с целью эффективного управления государственными расходами в США был введен принцип «2:1», который заключался в

том, что для принятия одной новой нормы, необходимо исключить две старые [7]. Благодаря такому принципу, расходы, необходимые для принятия новой нормы, компенсировались за счет отмены старой.

Результаты данных регуляторных мер, осуществляемых различными агентствами США, могут варьироваться, но в целом они направлены на обеспечение справедливости, безопасности и эффективности в различных секторах общества. Таким образом, в США отменены 244 действующие нормы, исключены из планов принятия 535 норм.

Если рассматривать систему регулирования и контроля в Китае, осуществляемую посредством «регуляторной гильотины», можно выделить несколько основных аспектов:

1. Государственный контроль: Китай характеризуется сильным государственным контролем в различных областях, включая экономику, общество и информационные технологии.

2. Централизованное управление: в Китае преобладает централизованная система управления, в которой государство принимает активное участие в экономической деятельности и регулировании.

3. Технологии и Интернет: Китай активно применяет регуляторные меры в сфере технологий и Интернета, включая цензуру контента и меры по обеспечению безопасности в сети.

4. Экономическая политика: государственное вмешательство в экономику, принятие стратегических решений и регулирование финансовых рынков направлены на обеспечение стабильности и устойчивого развития.

5. Экологические стандарты: с целью снижения воздействия на окружающую среду принимаются регуляторные меры в области охраны природы и экологических стандартов.

6. Соблюдение политических норм: в Китае применяются регуляторные меры для поддержания политической стабильности и соблюдения идеологических стандартов.

Общий характер китайской системы регулирования отличается от западных моделей, и он обусловлен особенностями политической системы и экономической политики Китая.

Таким образом, в общем смысле термин «регуляторная гильотина» используется для обозначения мер, направленных на регулирование и контроль в бизнес-среде в отрасли информационных технологий. Эти меры включают в себя пересмотр и отмену законов, принятие новых и другие инструменты, направленные на обеспечение соблюдения законов и развитие экономики. Исходя из вышесказанного, можно сделать вывод о том, что регуляторная гильотина широко используется в раз-

личных странах, основываясь на различных методах. Зарубежный опыт показывает, что применение гильотины принесло весомые результаты, что поспособствовало стимулированию бизнеса и развитию экономики страны. Несмотря на то, что благодаря реализации регуляторной гильотины, в России отменили более 12 000 актов, которые были признаны устаревшими, говорить о каких-то результатах применения гильотины еще рано. Однако общество меняется каждый день, соответственно правовая составляющая не должна отставать от таких изменений, именно поэтому «регуляторная гильотина» станет механизмом, который будет применяться во всех сферах жизни и общества.

Список источников

1. Механизм «регуляторной гильотины» / Министерство экономического развития Российской Федерации (Электронный ресурс) URL: https://economy.gov.ru/material/directions/gosudarstvennoe_upravlenie/mehanizm_regulyatornoy_gilotiny/ (дата обращения: 05.11.2023).

2. Федеральный закон «Об обязательных требованиях в Российской Федерации» от 31.07.2020 № 247-ФЗ / КонсультантПлюс (Электронный ресурс) URL: https://www.consultant.ru/document/cons_doc_LAW_358670 (дата обращения: 05.11.2023).

3. Перечень поручений по реализации Послания Президента Федеральному Собранию / Официальный сайт Президента России (Электронный ресурс) URL: http://kremlin.ru/acts/assignments/orders/59898 (дата обращения: 05.11.2023).

4. Утверждены составы и порядок работы рабочих групп «регуляторной гильотины» / Правительство России. Официальный сайт (Электронный ресурс) URL: http://government.ru/news/38212/ (дата обращения: 05.11.2023).

5. Перечень рабочих групп по реализации механизма «регуляторной гильотины» по сферам деятельности федеральных органов исполнительной власти / Правительство России. Официальный сайт (Электронный ресурс) URL: http://static.government.ru/media/files/tAnyU4YBGkuo4Fa4TgQJiHFvhfKN6WD4.pdf (дата обращения: 05.11.2023).

6. Кнутов А.В., Плаксин С.М., Синятуллин Р.Х., Чаплинский А.В. «Регуляторная гильотина» в России и ее количественные результаты // Право. Журнал Высшей школы экономики. 2022. Т.15. № 2. С.4-27.

7. Александров О.В. Регуляторные гильотины: международный опыт устранения препятствий для бизнеса и инвестирования // Торговая политика. Trade policy. 2019. №1(17). С. 109-117.

Об авторе

Прохорова Дарья Александровна —
курсант 3 курса
Московского университета
МВД России им. В. Я. Кикотя
(Россия, Москва)
E-mail: dasha280803@mail.ru

Научный руководитель

Полянская Елена Петровна —
старший преподаватель кафедры
информационной безопасности
учебно-научного комплекса
информационных технологий
Московского университета
МВД России им. В. Я. Кикотя
(Россия, Москва)
E-mail: azhara87@bk.ru

About the author

Darya A. Prokhorova —3rd year cadet of
the Vladimir Kikot Moscow University of
the Ministry of Internal Affairs of Russia
(Russia, Moscow)
E-mail: dasha280803@mail.ru

Scientific supervisor

Elena P. Polyanskaya —
senior lecturer at the Department of
Information Security
of the educational and Scientific complex
of Information Technologies
Vladimir Kikot Moscow University of
the Ministry of Internal Affairs of Russia
(Russia, Moscow)
E-mail: azhara87@bk.ru

УДК 004.056, 51–7

ПРЕИМУЩЕСТВА ЦЕНТРАЛИЗАЦИИ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В КРЕДИТНО-БАНКОВСКОЙ СФЕРЕ

Павлов Е. О.
Финансовый университет при Правительстве Российской Федерации (Россия, Москва)
epavlov466@gmail.com
Научный руководитель:

Резниченко С. А.
Финансовый университет при Правительстве Российской Федерации (Россия, Москва);
Национальный исследовательский ядерный университет «МИФИ» (Россия, Москва);
Российский государственный гуманитарный университет (Россия, Москва)
rsa_5@bk.ru

Аннотация

Проведены исследования в области управления информационной безопасностью на уровне регуляторов в кредитно-банковской сфере. Результаты анализа показали отсутствие централизованного руководства вопросами информационной безопасностью значимых объектов критической информационной инфраструктуры (КИИ), а также единой нормативно-правовой базы. В работе предлагается создание единого органа управления в сфере информационной безопасности (ИБ), которому бы делегировались основные полномочия, необходимые при решении ключевых проблем в области информационной безопасности, в частности, связанных с КИИ.

Ключевые слова: информационная безопасность, управление информационной безопасностью, регулятор, критическая информационная инфраструктура

ADVANTAGES OF CENTRALIZING INFORMATION SECURITY MANAGEMENT IN THE CREDIT AND BANKING SECTOR

Egor O. Pavlov
Financial University under the Government of the Russian Federation (Russia, Moscow)
epavlov466@gmail.com

Scientific supervisor:
Sergey A. Reznichenko
Financial University under the Government of the Russian Federation (Russia, Moscow);
National Research Nuclear University "MEPhI" (Russia, Moscow);
Russian State University for the Humanities (Russia, Moscow)
rsa_5@bk.ru

Abstract

Research has been conducted in the field of information security management at the level of regulators in the credit and banking sector. The results of the analysis showed the lack of centralized management of information security issues of significant critical information infrastructure (CII) facilities, as well as a unified regulatory framework. The paper proposes the creation of a single management body in the field of information security (IS), which would be delegated the main powers necessary to solve key problems in the field of information security, in particular, related to CII.

Keywords: information security, information security management, regulator, critical information infrastructure

Введение

В современном мире информация стала объектом для изменения многих процессов из разных областей человеческой жизнедеятельности, в связи с чем информационные ресурсы стали более уязвимы к атакам со стороны злоумышленников. Вследствие этого факта возникает необходимость в управлении информационной безопасностью. Управление информационной безопасностью представляет собой комплекс процессов защиты данных и активов организации от потенциальных угроз [1]. Основными целями этих процессов является обеспечение безопасности конфиденциальности, целостности и доступности информации. Управ-

ление информационной безопасностью может определяться как внутренними политиками корпоративной безопасности, так и внешними нормативными актами, федеральными законами, постановления Правительства РФ, а также приказами и распоряжениями регуляторов.

Важность системы управления информационной безопасностью

Уровень развития информации, информационных систем и технологий привел к тому, что организации различных видов в своей повседневной деятельности используют электронный документооборот, электронную подпись, документы в цифровом формате разного вида важности, дистанционные порталы для удаленного режима работы и обмена информацией, а также облачные хранилища с персональными данными. Все это является жизненно важными элементами для конкурентного преимущества организации и ее способности работать [2]. Именно поэтому эффективная архитектура управления безопасностью имеет значительное влияние, так как организациям необходимо предпринимать шаги по защите этих данных, чтобы защитить внутреннего и внешнего потребителя.

Основные стандарты управления информационной безопасностью

Цель системы управления информационной безопасности может быть достигнута выполнением большим множеством задач. Данные задачи могут основываться на внутренней политике и документах федерального, регионального уровня, а также на международных стандартах. В сфере управления информационной безопасности существует ряд основополагающих документов, требования которых необходимо строго соблюдать и выполнять.

Линейка международных стандартов дополняет конкретными рекомендациями и требованиями по защите информации, а также по вопросам управления информационной безопасности, описывая передовые методы обеспечения безопасности и предписывая внедрение системы управления информационной безопасностью. Основными стандартами являются стандарты серии, выпущенной организациями ISO и IEC:

- **ISO/IEC 17799 «Информационные технологии — Технологии безопасности — Практические правила менеджмента информационной безопасности»**; документ предлагает лучшие практические рекомендации для специалистов, занимающихся созданием и обслуживанием систем управления информационной безопасности.
- **ISO/IEC 27000** — стандарт содержит лучшие практики и советы в области информационной безопасности для создания, развития и под-

держания системы менеджмента информационной безопасности, а также фундаментальные определения в данной области.

- **ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования».** Документ содержит описания лучших мировых практик в области УИБ, а также предписывает требования к системе менеджмента информационной безопасности для демонстрации способности организации защищать свои информационные ресурсы.
- **ISO/IEC 27005** — настоящий стандарт предназначен для персонала, занимающегося вопросами менеджмента риска информационной безопасности.
- Также существует британский международный стандарт, части которого были выпущены британским институтом стандартов:
- **BS 7799–1** — первая часть стандарта описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью организации, определённых на основе лучших примеров мирового опыта в данной области.
- **BS 7799–2** — вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации, а также определяет спецификацию СУИБ.

Что касается проведения сертификации на соответствие требованиям международных стандартов — такой опции на данный момент в России нет, так как ввиду санкций на нашу страну наложены ограничения по проведению сертификации со стороны зарубежных специалистов, что в свою очередь не позволяет нам обновлять свою нормативно-правовую базу в соответствии с мировой нормативно-правовой практикой и сертифицировать объекты на соответствие требованиям новых документов.

Более того, не менее важную роль занимают основные государственные стандарты РФ в области управления информационной безопасности. Такими являются:

- **ГОСТ Р ИСО/МЭК 27006–2008** — требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности.
- **ГОСТ Р ИСО/МЭК 27007–2014** — руководства по аудиту систем менеджмента информационной безопасности.
- **ГОСТ Р 50992–2006** — защита информации. Основные термины и определения.
- **Р 50.1.053–2005** — Информационные технологии. Основные термины и определения в области технической защиты информации.

- **ГОСТ Р 51188–98** — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
- **ГОСТ Р 51275–2006** — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

В настоящий момент также приняты и введены в действие распоряжением Банка России следующие основные отраслевые стандарты в области УИБ:

- **СТО БР ИББС-1.1–2007** — аудит информационной безопасности.
- **РС БР ИББС-2.5–2014** — менеджмент инцидентов информационной безопасности.
- **СТО БР ИББС-1.4–2018** — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском информационной безопасности при аутсорсинге.
- **СТО БР ИББС-1.2–2014** — Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0–2014.

Таким образом, были рассмотрены фундаментальные документы в области управления информационной безопасности. Современные предприятия должны соблюдать положения данных документов, основываясь на принципах и механизмах, описанных в содержании вышеперечисленных стандартов.

Взаимодействие регуляторов в сфере ИБ, их роль и сущность

Более примечательно то, что Указом Президента РФ от 01.05. 2022 N250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» создание структурного подразделения, осуществляющего функции по обеспечению безопасности, на объектах критической информационной инфраструктуры становится обязательным. Теперь информационная безопасность начинает принимать более четкую иерархичность и структурированность [3]. Вопросы, связанные с киберпреступлениями и защитой от компьютерных атак, поднимаются на государственном уровне. Руководящие документы в области ИБ подчеркивают ответственность руководителя организации за обеспечение информационной безопасности предприятия [4]. В настоящее время Уголовный кодекс РФ предусматривает наказания сроком до 10 лет лишения свободы за нарушение требований в области информационной безопасности объектов КИИ.

Стоит отметить тот факт, что в текущий период развития сферы информационных технологий в России существует немалое количество органов, регулирующих работу компаний в кредитно-банковской обла-

сти. ФСТЭК, ФСБ, Минцифры, Роскомнадзор, Центральный Банк — все данные структурные подразделения контролируют работу компаний по различным вопросам. Также важно упомянуть, что информация о зафиксированных компьютерных инцидентах должна рассылаться компаниями самостоятельно в такие государственные системы как: ГосСОПКА, ФинЦЕРТ и НКЦКИ. Это свидетельствует о том, что на данный момент отсутствует общая межведомственная система взаимодействия по обмену информацией между данными структурами [5]. Также отсутствует одно ведомство, которое централизованно взяло бы на себя полномочия по управлению вопросами в области информационной безопасности.

Мероприятия, связанные с переходом на российские программное обеспечение (ПО) и средства защиты информации (СЗИ), а также по внедрению отделов ИБ согласно Постановление Правительства РФ от 15.07.2022 № 1272 «Об утверждении Типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и Типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)», показывают необходимость государственного регулирования вопросами информационной безопасности объектов КИИ.

Указ Указ Президента Российской Федерации от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», связанный с переходом на российское ПО и средства защиты информации, также Постановление Правительства № 1272 о создании структур, отделов, групп информационной безопасности. Необходимо уделять внимание объектам КИИ на государственном уровне.

Заключение

Таким образом, в заключении статьи можно выдвинуть ряд предложений, которые позволили развивать сферу информационной безопасности в нашей стране и на международной арене.

Во-первых, необходимо создать один орган, которому бы делегировались основные полномочия, необходимые при решении ключевых проблем в области информационной безопасности, в частности, связанных с КИИ. Именно благодаря четкому, выверенному и централизованному управлению можно добиться успешного развития.

Во-вторых, необходимо внедрить систему межведомственного взаимодействия между всеми регуляторами, которые имеют отношение к организации деятельности компании в сфере. Это значительно повы-

сило бы эффективность управления всеми процессами ответственными органами, а также компаний в конкретных подотраслях сферы информационных технологий, а также поспособствовало быстродействию электронного документооборота.

В-третьих, по возможности постараться создать ситуацию, при которой сертификация по международным стандартам стала бы возможной и доступной.

Мировой опыт многих стран мира всегда расширяется и дополняется полезными ресурсами и информацией, именно поэтому нам стоит добиться отношений, при которых мы смогли актуализировать международные инновации и в нашей стране.

Список источников

1. Крючков А. В., Прус Ю. В., Резниченко С. А. Технологические основы национальной информационной безопасности // Сборник статей, Международной научно-практической конференции Российского государственного гуманитарного университета. 2018. С. 58–63.

2. Резниченко С. А., Дмитриева Т. В., Подкосов С. В., Евдокимов О. Г., Семухин С. Д. Проблемы управления информационной безопасностью в кредитно-банковской системе передачи данных // Московский экономический журнал. 2022. № 2. С. 617–625.

3. Резниченко С. А., Сиротский А. А. Формализованная модель аудита информационной безопасности организации на предмет соответствия требованиям стандартов // Безопасность информационных технологий. 2021. Том.28, № 3. С. 103–117.

4. Резниченко С. А., Гавришев А. А. Государственная система поддержки деятельности российских СМИ по продвижению их продукции на зарубежные информационные рынки в условиях информационных войн // Государственное управление. Электронный вестник. 2023. № 96. С. 148–162.

5. Репенко В. А., Резниченко С. А. Защита от атак с применением средств и методов социальной инженерии// Вестник Дагестанского государственного технического университета. Технические науки. 2022. Т. 49. № 4. С. 85–96.

Об авторе

Павлов Егор Олегович —
студент 2-го курса (бакалавриат)
Финансового университета при
Правительстве Российской Федерации
(Россия, Москва)
E-mail: epavlov466.gmail.com

Научный руководитель

Резниченко Сергей Анатольевич —
кандидат технических наук, доцент,
доцент департамента информационной
безопасности Финансового университета
при Правительстве Российской
Федерации (Россия, Москва);
доцент кафедры стратегических
информационных исследований
Национального исследовательского
ядерного университета «МИФИ»
(Россия, Москва);
доцент кафедры информационной
безопасности Российского
государственного гуманитарного
университета (Россия, Москва)
E-mail: rsa_5@bk.ru

About the author

Egor O. Pavlov —2nd year student
(Bachelor's degree)
Financial University at The
Government of the Russian Federation
(Russia, Moscow)
E-mail: epavlov466.gmail.com

Scientific supervisor

Sergey A. Reznichenko —
Candidate of Technical Sciences,
Associate Professor, Associate Professor
of the Information Security Department
of the Financial University under the
Government of the Russian Federation
(Russia, Moscow);
Associate Professor of the Department
of Strategic Information Studies National
Research Nuclear University "MEPhI"
(Russia, Moscow);
Associate Professor of the Department of
Information Security at the Russian State
University for the Humanities (Russia,
Moscow)
E-mail: rsa_5@bk.ru

УДК 004.008+34

ЗАРУБЕЖНЫЙ ОПЫТ РЕГУЛИРОВАНИЯ БЕЗОПАСНОСТИ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Кошелевич Ю. Д.
Московский университет МВД России им. В. Я. Кикотя (Россия, Москва)
(Russia, Moscow)
koshelevich03@bk.ru

Научный руководитель:
Поликарпов Е. С.
Московский государственный лингвистический университет (Россия, Москва)
binox@mail.ru

Аннотация

В статье проанализированы современные проблемы регулирования искусственного интеллекта, глобальные тренды и национальные подходы. Данная работа исследует современные вызовы, стоящие перед искусственным интеллектом, и представляет собой анализ правовых и регуляторных подходов в США, Китае и России. Результаты помогают лучше понимать мировую динамику ИИ и его будущего регулирования.

Ключевые слова: искусственный интеллект, регулирование, нормативно-правовые акты, алгоритмы, угрозы

FOREIGN EXPERIENCE IN REGULATING THE SECURITY OF ARTIFICIAL INTELLIGENCE SYSTEMS

Yulia D. Koshelevich
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
koshelevich03@bk.ru

Scientific supervisor:
Evgeny S. Polikarpov
Moscow State Linguistic University (Moscow, Russia)
binox@mail.ru Alexkhasin@mail.ru

Abstract

The article analyzes the current problems of artificial intelligence regulation, global trends and national approaches. This work explores the current challenges facing artificial intelligence and provides an analysis of legal and regulatory approaches in the United States, China and Russia. The results help to better understand the global dynamics of AI and its future regulation.

Keywords: artificial intelligence, regulation, regulations, algorithms, threats

Введение

По мере того, как системы искусственного интеллекта оказываются все более полезными в реальных приложениях, расширяется сфера их применения, что приводит к росту рисков неправильного, чрезмерного и явного использования. По мере роста возможностей систем ИИ и их более полной интеграции в инфраструктуру общества последствия потери реального контроля над ними становятся все более тревожными. Новые исследования направлены на переосмысление основ этой области, чтобы сделать системы ИИ менее зависимыми от явных и легко ошибочных целей. Особенно заметная опасность заключается в том, что ИИ может упростить создание машин, способных шпионить и даже убивать в больших масштабах. Однако в настоящее время существует множество других важных и более тонких опасностей.

Возможности и угрозы технологий и систем ИИ

Одной из наиболее острых опасностей ИИ является «технорешительство» — мнение, что ИИ может рассматриваться как панацея, в то время как он является всего лишь инструментом [1]. По мере того как мы видим все новые достижения в области ИИ, растет соблазн применить ИИ для принятия решений по всем общественным проблемам. Однако в процессе решения мелких проблем технологии часто создают более крупные. В 2018 г. компания Amazon сочла необходимым отказаться от собственного инструмента рекрутинга, поскольку исторические данные, на которых он был обучен, привели к тому, что система оказалась систематически предвзятой по отношению к женщинам.

Автоматизированное принятие решений часто может воспроизводить, усугублять и даже усиливать те самые предрассудки, которые мы хотели бы устранить. Поскольку предвзятые пользователи сообщают алгоритму предвзятую информацию, он отвечает на нее еще более несправедливо,

что усугубляет понимание пользователей и их предвзятость, и так далее. Поскольку любая технология — это продукт предвзятой системы, недостатки «технорешения» очень глубоки: творение ограничено ограничениями его создателя.

Автоматизированное принятие решений может приводить к искаженным результатам, которые воспроизводят и усиливают существующие предубеждения. Потенциальная опасность заключается в том, что общество принимает выводы, сделанные с помощью ИИ, как несомненные. Такой детерминистский подход к принятию решений с помощью ИИ может иметь тяжелые последствия как в криминальной сфере, так и в здравоохранении. Такие подходы, как PredPol, программное обеспечение, изначально разработанное полицейским департаментом Лос-Анджелеса и Калифорнийским университетом, призванное помочь защитить каждого жителя США, предсказывают, когда, где и как произойдет преступление.

Данный подход непропорционально прогнозирует преступления в районах с более высокой численностью небелых и малообеспеченных жителей. Эта опасная реальность означает, что алгоритмическая оценка степени риска человека для общества может быть истолкована другими людьми как почти уверенность — результат, вводящий в заблуждение, от которого предостерегали даже разработчики первоначального инструмента. Принятие вероятности за уверенность означает, что прошлое всегда будет диктовать будущее. Все данные в той или иной степени интерпретируются [4].

Нежелательные предубеждения могут быть скрыты как за непрозрачностью используемой технологии, так и за использованием прокси, номинально невинных атрибутов, которые позволяют принять решение, в основе которого лежит предубеждение. Без прозрачности данных и алгоритмов ИИ, которые их интерпретируют, общество может остаться в неведении относительно того, как принимаются решения, существенно влияющие на его жизнь. Не имея достаточной информации для предъявления судебного иска, люди могут доверие к процессуальным нормам и средствам правовой защиты, если считают, что системы искусственного интеллекта вынесли им неправомерное или ошибочное решение. Утрата самостоятельности может стать следствием создания ИИ «информационных пузырей», сужающих круг общения человека в интернете так, что он уже и не подозревает о других точках зрения.

Системы искусственного интеллекта используются для дезинформации в интернете, что может стать угрозой для демократии и инструментом фашизма. От видеороликов «deepfake» до онлайн-ботов,

манипулирующих общественным дискурсом, симулируя консенсус и распространяя фальшивые новости, существует опасность того, что системы искусственного интеллекта могут подорвать доверие в обществе. Эти технологии могут быть использованы преступниками, государствами-изгоями, идеологическими экстремистами или просто группами с особыми интересами для манипулирования людьми с целью получения экономической выгоды или политических преимуществ [3]. Дезинформация представляет собой серьезную угрозу для общества, эффективно подменяя и манипулируя фактами, создавая социальные петли обратной связи, подрывая представление об объективной истине.

Современные бизнес-модели применения ИИ в здравоохранении, как правило, ориентированы на создание единой системы, которая может быть продана многим покупателям. Однако такие системы зачастую не способны обобщать данные, полученные в ходе обучения. Даже различия в порядке проведения клинических анализов могут исказить предсказания, а со временем точность системы часто снижается по мере изменения практики. Алгоритмы искусственного интеллекта играют роль в принятии решений о распределении органов, вакцин и других элементов здравоохранения. Ошибки в этих подходах могут иметь буквальное значение для жизни и смерти.

Неправильно обученный алгоритм может принести больше вреда, чем пользы пациентам из группы риска, полностью пропуская раковые заболевания или выдавая ложноположительные результаты. По мере того, как новые алгоритмы насыщают рынок обещаниями медицинских чудес, упущение из виду заложенных в их результатах предубеждений может привести к потере человеческого биоразнообразия, поскольку людям, не попавшим в первоначальные наборы данных, будет отказано в адекватной медицинской помощи. Хотя точные долгосрочные последствия применения алгоритмов в здравоохранении неизвестны, их потенциал к воспроизведению предвзятости означает, что любые улучшения, которые они дают населению в совокупности — от диагностики до распределения ресурсов, — могут происходить за счет наиболее уязвимых слоев населения.

В связи с широким развитием ИИ в последние годы примерами отраслей, в которых ИИ в значительной степени зависит от повседневной деятельности, являются финансовые услуги, финтех и платежию. Потребители могут оформить кредитную карту, подать заявку на кредит, открыть брокерский счет, получить консультацию по финансовым вопросам или инвестициям — и все это без непосредственного общения с живым человеком. Решения по кредитам могут приниматься алгорит-

мами искусственного интеллекта, а консультирование может осуществляться «робоконсультантами». Платежи теперь защищены системой обнаружения и защиты от мошенничества на базе ИИ. FinTech разрабатывает новые технологии искусственного интеллекта, которые через приобретения попадают в экосистему финансовых услуг.

Первоначальный опыт регулирования систем ИИ в США

В США в 2022 году появился первый подход к регулированию ИИ, ориентированный на конкретные случаи использования ИИ. Чаще всего регулированию подвергались случаи использования ИИ при подборе персонала или трудоустройстве. Например, Нью-Йорк присоединился к ряду штатов, включая Иллинойс и Мэриленд, и начал регулировать автоматизированные инструменты принятия решений о найме (AEDT), которые используют ИИ для принятия или существенной помощи при отборе кандидатов или принятии решений о найме.

Законы штатов о конфиденциальности — общие требования к ИИ, ориентированному на потребителя, в 2023 году. В 2023 году, вероятно, появятся первые общие обязательства, применимые ко всем случаям использования ИИ, которые будут содержаться в законах о конфиденциальности, принятых в некоторых штатах. Новые правила США в области ИИ вдохновлены аналогичными положениями Общего регламента Европейского союза по защите данных (GDPR). GDPR требует соблюдения повышенных требований, когда компании используют технологии, подобные ИИ, исключительно для принятия автоматизированных решений, которые оказывают «правовое … или аналогичное значительное» воздействие на потребителя.

Федеральное регулирование ИИ может исходить от ФТК. На федеральном уровне законопроекты, посвященные ИИ, уже вносились в Конгресс, но не получили значительной поддержки и интереса. Однако, как представляется, регулирование ИИ может появиться со стороны Федеральной торговой комиссии (ФТК). В последние годы ФТК выпустила две публикации, предвещающие усиление внимания к регулированию ИИ. ФТК заявила, что она накопила опыт в области ИИ при исполнении различных законодательных актов, таких как Закон о справедливом кредитном информировании, Закон о равных кредитных возможностях и Закон о ФТК. В этих публикациях стали излагаться основные правила разработки и использования ИИ, в том числе:

- убедиться в том, что ИИ обучается на репрезентативных наборах данных, которые не «пропускают» информацию из конкретных групп населения;

- тестировать ИИ перед внедрением и периодически после этого, чтобы убедиться, что он работает так, как задумано, и не приводит к дискриминационным или предвзятым результатам;
- обеспечить объяснимость результатов ИИ на случай, если решения ИИ придется объяснять потребителям или регулирующим органам;
- создать механизмы подотчетности и управления для документирования честной и ответственной разработки, внедрения и использования ИИ.

Для США одним из преимуществ сравнительно медленного прогресса в области управления ИИ является возможность перенять опыт зарубежных экспериментов в области регулирования — если политики готовы серьезно относиться к зарубежным нормативным актам [5].

Детальное и подробное регулирования систем ИИ в Китае

В настоящее время в Китае разрабатывается один из самых ранних и наиболее подробных нормативных документов, регулирующих деятельность искусственного интеллекта (ИИ). Они включают меры по регулированию рекомендательных алгоритмов — наиболее распространенной формы ИИ, используемой в Интернете, — а также новые правила для синтетически созданных изображений и чат-ботов по образцу ChatGPT. Создаваемая Китаем система управления ИИ изменит порядок создания и внедрения технологий внутри Китая и за его пределами, окажет влияние как на экспорт китайских технологий, так и на глобальные исследовательские сети в области ИИ. Китай формирует политику управления ИИ, которая может быть использована для прогнозирования будущей траектории развития китайского управления ИИ. Три наиболее конкретных и влиятельных нормативных акта Китая в области алгоритмов и ИИ — это нормативный акт 2021 года о рекомендательных алгоритмах, правила глубокого синтеза (синтетически созданного контента) 2022 года и проект правил генеративного ИИ 2023 года. Все три положения требуют от разработчиков подачи заявки в китайский реестр алгоритмов — недавно созданное государственное хранилище, в котором собирается информация о том, как происходит обучение алгоритмов, а также прохождения самооценки безопасности.

В ближайшие годы Китай продолжит разработку целевых нормативных актов в области ИИ и заложит основу для принятия основного национального закона об ИИ. Любая страна, компания или организация, которая надеется конкурировать, сотрудничать или просто понять китайскую экосистему ИИ, должна внимательно изучить эти шаги. За последние два года в Китае были приняты первые в мире обязательные национальные нормативные акты в области искусственного интеллекта

(ИИ). Эти правила касаются рекомендательных алгоритмов распространения контента, синтетически сгенерированных изображений и видео, а также генеративных систем ИИ.

В начале 2023 года лидер сенатского большинства Чак Шумер объявил о своих планах начать регулирование ИИ, он назвал усилия Китая «тревожным звонком для нации» и предупредил, что США не могут позволить своему геополитическому противнику «писать правила дорожного движения» для ИИ. Эти позиции имеют под собой реальную основу, но при этом создают «слепое пятно»: сами нормативные документы. Конкретные требования и ограничения, которые они накладывают на китайские продукты ИИ, имеют значение. Они изменят способы создания и внедрения технологий в стране, и их влияние не ограничится ее границами. Они будут распространяться по всему миру, становясь стандартными для экспорта китайских технологий. Они будут влиять на все — от контроля содержания языковых моделей в Индонезии до функций безопасности автономных транспортных средств в Европе.

Для Китая быть мировым лидером или моделью управления ИИ — это «приятное событие», небольшой бонус для его бизнеса и национальной «мягкой силы», но не существенная движущая сила этих нормативных актов в области ИИ. Выбор Китаем первых объектов регулирования — рекомендательных алгоритмов и глубокого синтеза — свидетельствует о том, что глобальное лидерство не является основным мотивом для управления ИИ. Рекомендательные алгоритмы — это повсеместное применение ИИ, но они не являются основным направлением глобального дискурса об управлении ИИ. Если бы страна хотела заявить о своей претензии на мировое лидерство в области управления ИИ, рекомендательные алгоритмы не были бы ее первой целью.

Регулирования систем ИИ в Российской Федерации

В Москве, а затем и по всей России формируется новый экспериментальный правовой режим развития проектов в области искусственного интеллекта (ИИ). Первая инициатива была представлена в начале 2020 года в виде законопроекта, который после первой публикации претерпел очень мало изменений. В результате 1 июля 2020 года в России вступил в силу Федеральный закон № 123-ФЗ, вводящий специальную правовую базу для «цифровых площадок» в Москве. Цифровые площадки — это территории, на которых можно разрабатывать и тестировать технологии, даже если они выходят за рамки действующего законодательства. Положения 123-ФЗ, касающиеся обработки персональных данных, уже вызвали серьезную обеспокоенность граждан. Например, закон

гласит, что никакие персональные данные, участвующие в проекте, не могут быть переданы лицам, не имеющим отношения к эксперименту, а также не могут храниться за пределами Москвы. Это кажется непонятным, учитывая безграничность интернета и то, что для хранения и доступа к данным широко используются облачные сервисы [2].

В новой редакции ст. 10 Федеральный закон от 27.07.2006 N 152-ФЗ «Закона о персональных данных» указано, что «обработка персональных данных о состоянии здоровья, полученных в результате обезличивания, допускается в целях повышения эффективности государственного или муниципального управления». В то же время закон не затрагивает такие принципиальные вопросы, как: где будут храниться данные о наших цифровых личностях и как они будут стираться; как именно будет обеспечиваться неприкосновенность частной жизни граждан; кто будет нести ответственность в случае невыполнения обезличивания данных. Такая регламентация персональных данных ставит под сомнение основную цель нового закона, а также вызывает опасения, что участники экспериментального режима будут иметь доступ к персональным данным граждан Москвы и смогут их обрабатывать.

Чтобы минимизировать негативный эффект от принятия закона, в Государственную Думу был внесен законопроект, предлагающий отложить введение закона до июля 2025 года, чтобы внести большую ясность в вопрос обработки обезличенных персональных данных. В целом Россия располагает ресурсами для внедрения инновационных технологий в свою деятельность, но законодательство пока существенно отстает. Это может привести к злоупотреблению полномочиями как со стороны властей, так и со стороны аккредитованных операторов, имеющих доступ к данным. Новый закон позволяет создавать цифровые площадки на всей территории страны. В отличие от 123-ФЗ, 258-ФЗ устанавливает максимальный срок действия режима — три года с возможностью продления. В число сфер, которым разрешено участвовать в новом режиме, входят медицина, транспорт и логистика, архитектура и строительство, финансы, дистанционная продажа товаров и услуг, коммунальное хозяйство, промышленное производство, сельское хозяйство. В дальнейшем могут быть добавлены и другие отрасли.

Согласно новому закону № 258-ФЗ “Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации”, государство получит право устанавливать исключения из некоторых законодательных требований, препятствующих внедрению цифровых инноваций. Однако для того, чтобы «цифровые площадки» начали работать сразу после введения 258-ФЗ, необходимо также внести соответ-

ствующие изменения в отраслевые федеральные законы, регулирующие соответствующие сферы деятельности. Кроме того, в связи с иерархией дублирующих положений 123-ФЗ, действующего в Москве, и 258-ФЗ, распространяющегося на всю страну, возникают вопросы, которые необходимо решить в процессе реализации новых законов.

Заключение

Исследование и анализ области регулирования искусственного интеллекта свидетельствует о том, что Китай, Россия и Соединенные Штаты Америки играют ключевую роль в формировании международного ландшафта ИИ. Китай активно разрабатывает и внедряет стратегии и нормативные акты, способствующие развитию ИИ и его применению в различных областях. Стремительное развитие китайской научно-технической инфраструктуры и значительные инвестиции делают его глобальным лидером в этой области.

Россия, занимая второе место, также активно работает над регулированием ИИ и развитием национальных проектов в этой сфере. Здесь отмечается важная роль государства, академического сообщества и частного сектора в поддержке исследований и разработок в области ИИ. США, хотя остаются одним из ключевых игроков в мировой индустрии ИИ, находятся на третьем месте. Однако они остаются лидерами в области привлечения талантливых специалистов и инноваций в эту сферу.

Однако следует подчеркнуть, что регулирование ИИ — это сложная задача, и обсуждение ее на международном уровне будет иметь решающее значение для обеспечения безопасного и этичного развития этой технологии. По мере того, как различные страны и регионы углубляют свое понимание и регулирование ИИ, они могут совместно разрабатывать стандарты и принципы, чтобы обеспечить гармоничное сосуществование ИИ и человечества. Таким образом, Китай, Россия и США представляют собой важных игроков в развитии и регулировании ИИ, и сотрудничество между этими странами может способствовать созданию более безопасного и этичного мира, где ИИ играет ключевую роль в решении сложных глобальных задач.

Список источников

1. Былевский П. Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56. DOI 10.7256/2454–0757.2023.8.43909. EDN UZDRFW.

2. Ларина Е., Овчинский В. Как развивается искусственный интеллект? // Завтра. 6 апреля 2021. (Электронный ресурс) URL: https://zavtra.ru/blogs/kak_razvivaetsya_iskusstvennij_intellekt (дата обращения: 05.11.2023).

3. Мельников С. Ю., Пересыпкин В. А. Об эволюции классических вероятностных моделей языка в естественно-языковых приложениях // Вестник современных цифровых технологий. 2023. № 16. С. 4–14. EDN: YDIGDT

4. Diakopoulos N. Algorithmic Accountability. Journalistic investigation of computational power structures // Digital Journalism. 2015. Vol.3. Iss.3 (Journalism in an Era of Big Data: Cases, Concepts, and Critiques). Pp.398–415. https://doi.org/10.1080/21670811.2014.976411

5. Mittelstadt B., Allo P., Taddeo M., Wachter S., Floridi L. The ethics of algorithms: Mapping the debate // Big Data & Society. 2016. № 1(21). Pp.1–21. DOI: 10.1177/2053951716679679

Об авторах

Кошелевич Юлия Данииловна —
курсант 3 курса Московского университета МВД России им. В. Я. Кикотя
(Россия, Москва)
E-mail: koshelevich03@bk.ru

Научный руководитель

Поликарпов Евгений Сергеевич —
кандидат технических наук, доцент, доцент кафедры международной информационной безопасности ИИН Московского государственного лингвистического университета
(Россия, Москва)
E-mail: binox@mail.ru

About the authors

Yulia D. Koshelevich —
3rd year cadet of the Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
E-mail: koshelevich03@bk.ru

Scientific supervisor

Evgeny S. Polikarpov —
Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of International Information Security of the Moscow State Linguistic University
(Russia, Moscow)
E-mail: binox@mail.ru

УДК 004.008+34

ПОТЕНЦИАЛ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

Кузнецова Т. Ю.
Московский университет МВД России им. В.Я. Кикотя (Россия, Москва)
(Russia, Moscow)
Not200104@mail.ru

Хасин А. Е.
Центр специального назначения инновационных технологий МВД России
(Москва, Россия)
Alexkhasin@mail.ru

Научный руководитель:
Полянская Е. П.
Московский университет МВД России им. В.Я. Кикотя (Россия, Москва)
azhara87@bk.ru

Аннотация

В современном мире все большую популярность набирает искусственный интеллект (ИИ), что вызывает широкие обсуждения и открывает новые перспективы для общества. Продвижение инсайтов ИИ основано на использовании нейронных сетей, которые эмулируют функционирование человеческого мозга и способны взаимодействовать между собой. Это позволяет создавать интеллектуальные системы, способные выполнять сложные задачи и анализировать большие объемы информации. Однако, опасения о возможной угрозе для рабочих мест и потере рабочей роли для людей остаются актуальными. Несмотря на это, дальнейшее развитие ИИ открывает новые перспективы для сферы обслуживания и создания инновационных продуктов.

Ключевые слова: искусственный интеллект, возможности, угрозы, технологии, данные, информация, правоохранительные органы

THE POTENTIAL OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN LAW ENFORCEMENT

Tatyana Yu. Kuznetsova
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
Not200104@mail.ru

Alexander E. Khasin
The Center for Special Purpose Innovative Technologies of the Ministry
of Internal Affairs of Russia (Moscow, Russia)
Alexkhasin@mail.ru

Scientific supervisor:
Elena P. Polyanskaya
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
azhara87@bk.ru

Abstract
Artificial intelligence (AI) is gaining more and more popularity in the modern world, which causes widespread discussion and opens up new prospects for society. Website promotion is based on the use of neural networks that emulate the functioning of the human brain and are able to interact with each other. This allows you to create intelligent systems capable of performing complex tasks and analyzing large amounts of information. However, concerns about a possible threat to jobs and the loss of a working role for people remain relevant. Despite this, further development opens up new prospects for the service sector and the creation of innovative products.

Keywords: artificial intelligence, opportunities, threats, technologies, data, information, law enforcement agencies

В современном мире на различных уровнях распространения информации все чаще обсуждаются темы, напрямую связанные с появлением искусственного интеллекта (в дальнейшем ИИ). Появление искусственного интеллекта является одним из ключевых факторов в современном мире, который вызывает много дискуссий и открывает новые возмож-

ности для общества в целом. Однако, разработка ИИ сопровождается опасениями. Так же надо понимать, что одно из их огромного множества, это безработица. Уже на данном этапе развития идет замещение ряда профессий, а какие-то уже выполняются ботами. Среди них консультанты, таксисты и токари, список не полный и с каждым годом будет пополняться [5].

Одно из технологических решений искусственного интеллекта представляет собой совокупность нейронных сетей, которые способны взаимодействовать. состоит из отдельных элементов, называемых нейронами, которые способны обмениваться информацией. Эти «нейроны» являются математическими моделями, которые имитируют работу человеческого мозга. Некоторые нейроны получают информацию извне с помощью органов чувств, другие обрабатывают эту информацию, а третьи генерируют окончательный результат, схематично показано на Рисунке 1:

Главная функция ИИ — это способность к «обучению» и совершенствованию в автоматическом режиме. Развитие искусственного интеллекта на данный момент занимает место одной из важнейших проблем. С помощью новых технологий и алгоритмов, исследователи и разработчики создают все более сложные системы, способные обрабатывать и анализировать огромные объемы данных, распознавать образы и речь, принимать решения и обучаться на основе опыта. Машинное обучение, где компьютерная программа сама на основе данных выявляет закономерности и обучается, стало одной из основных областей развития искусственного интеллекта [4]. Алгоритмы глубокого обучения, такие как сверточные нейронные сети и рекуррентные нейронные сети, позволяют моделировать сложные процессы, имитируя работу нейронов в человеческом мозге.

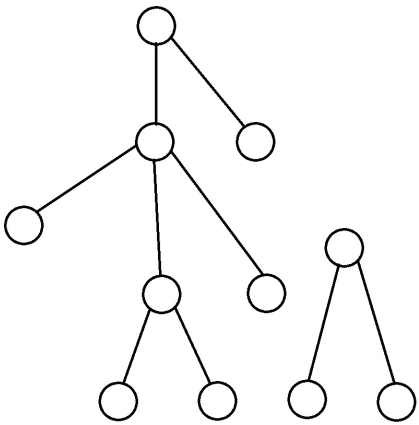

Рисунок 1. Схема простейшего ИИ

ИИ может использоваться для исключения человеческих ошибок. Это особо актуально в медицинской области, а именно при проведении сложных операций на сердце или при иных процедурах,

где человек может умереть от малейшей ошибки. Здесь идет речь о внедрении ИИ непосредственно в робототехнику. ИИ так же может быть полезен в качестве разработчика программ и алгоритмов, в том числе для вышеуказанной робототехники, исключая вероятность ошибки. Иными словами, способен адаптировать одну и туже робототехнику под различные задачи.

Также поможет улучшить процесс обучения и образования, помогая создавать адаптивные и персонализированные образовательные программы, предоставлять студентам индивидуальные рекомендации и помощь. ИИ позволит проанализировать потребности клиентов, и дать обратную связь, в виде сосредоточения большего внимания студента на «проседающих» темах.

Помимо вышеперечисленных возможностей, ИИ так же может найти применение в системе правоохранительных органов. В системе МВД России огромное количество времени уходит на работу с документацией. Внедрив ИИ в систему, у сотрудников появится намного больше времени для выполнения своих обязанностей и увеличения показателей. Сотрудники подразделений уголовного розыска смогут сосредоточиться на разработке и поимке преступников, а в подразделениях специальных технических мероприятий (далее ПСТМ) на выполнении порученных заданий. Кроме очевидных вещей, ИИ способен анализировать статистику совершенных преступлений и правонарушений, соответственно спрогнозировать их.

Это позволит пересмотреть общую концепцию предупреждения преступности в системе МВД России, поскольку будет известно вероятное место совершения преступлений [1]. Что касается ПСТМ, то в них ИИ можно внедрить в модули, которые подключены к видеокамерам по всей России. Сначала это будет простейшая нейронная сеть, но со временем её место займет полноценный интеллект. Поисковые модули смогут распознавать лица, в соответствии с запросами, с удивительной скоростью и точностью. Появится возможность создания автономных роботизированных точек в подразделениях государственной инспекции безопасности дорожного движения и внедрения ИИ для управления.

Также ИИ можно внедрить в точки приема экзаменов для получения водительского удостоверения и прочих государственных услуг. Это позволит ускорить и оптимизировать рабочий процесс. В экспертно-криминалистических подразделениях ИИ способен помочь с идентификацией и распознаванием и форматированием аудио- и видеоинформации. Файлы различного формата, смогут редактироваться без стороннего программного обеспечения или редакторов, при помощи

одной команды с четко поставленной задачей. В подразделениях, информационных технологий и защиты информации ИИ тоже найдется применение, а именно в составлении планов защиты помещений и их реализации. Кроме того, настройка сети и всё что выполняется человеком на компьютере вручную, будет происходить в автоматическом режиме.

Помимо системы МВД России, ИИ можно внедрить в Министерство Обороны Российской Федерации для автоматического управления ракетными установками и прочими сложными комплексами, как например системой противоракетной воздушной обороны, а также ещё в огромное количество областей.

Таким образом, достоинства ИИ перерастают в ряды проблем, которые он может доставить человечеству. Системы могут столкнуться с проблемой при анализе данных и принятии решений, что может привести к нежелательным результатам и некорректным выводам. Если ИИ имеет доступ к неправильным или неверно отфильтрованным данным, то возможно появление ошибок в решении. Кроме того, системы ИИ могут быть уязвимы к атакам, таким как неправильный ввод данных или их изменение с целью преобразования результатов для получения контроля над системой. Недостаточный контроль и прозрачность систем ИИ создают проблему доверия и этические вопросы. Если система бесконтрольна, возможно использование системы злоумышленниками. Перечисленные уязвимости требуют серьёзного внимания и предусмотрительности со стороны разработчиков, чтобы минимизировать появление негативных последствий. ИИ включает в себя набор алгоритмов и компьютерных систем, которые способны имитировать и выполнять задачи, которые ранее требовали участия человека [2].

Хотя ИИ стал изумительным достижением в технологической сфере, существуют определенные угрозы, которые он может представлять для человечества. Безработица: Развитие ИИ и автоматизации может привести к массовой потере рабочих мест. Многие профессии, требующие повторяемых задач, могут быть заменены ИИ и роботами, что может привести к социальным и экономическим последствиям, включая безработицу и неравенство. Зависимость от ИИ: Человечество может стать слишком зависимым от ИИ и технологии. Если ИИ не работает должным образом или сталкивается с проблемами, на которые нет решений, это может оказать серьезное отрицательное влияние на общество и его способность функционировать без него.

Потеря контроля: при достижении высокого уровня развития ИИ с возможностью самообучения и самосовершенствования могут воз-

никнуть проблемы с изолированием ИИ от потенциально вредоносных действий. Если ИИ развивается, не контролируется или выходит из-под контроля людей, он может представлять серьезную угрозу для человечества. Этические вопросы: ИИ может столкнуть нас с этическими дилеммами и сложными вопросами, такими как принятие решений о сохранении жизни в ситуации аварии, разделение ответственности между человеком и машиной в автономных системах. Решение таких этических проблем может быть сложным и спорным. Угроза приватности и безопасности: С ростом использования ИИ и собирания огромных объемов данных возникает риск нарушения приватности и безопасности людей [3].

Персональная информация может быть использована нелегально или неправомерно, а также быть уязвимой для хакерских атак. В заключение следует отметить, что появление искусственного интеллекта сопровождается как возможностями, так и опасностями. Он предоставляет широкий спектр преимуществ и применений, которые могут повысить эффективность и точность работы в различных областях. ИИ имеет потенциал изменить жизнь человечества как в лучшую, так и в худшую стороны. Необходимо внимательно относиться к его развитию и использованию, чтобы минимизировать потенциальные угрозы и проблемы.

Важно разработать соответствующие рамки и нормативы для гарантии надежности и безопасности систем ИИ. обеспечить соответствующую подготовку и обучение людей для работы с ним, адаптироваться к новым требованиям и вызовам, которые он представляет.

Необходимо продолжать исследования и разработку в области искусственного интеллекта, чтобы раскрыть его полный потенциал и найти новые способы применения. Искусственный интеллект должен служить интересам и благополучию человека, а не замещать его или создавать новые проблемы. Таким образом, развитие и использование искусственного интеллекта требуют баланса между новыми возможностями и социальными и этическими аспектами.

Список источников

1. Абдурагимова Т. И. Применение инновационных технологий (искусственного интеллекта) сотрудниками правоохранительных органов в раскрытии и расследований преступлений: перспективы и трудности // Вестник Московского университета МВД России. 2023. № 5. С. 21-23. DOI 10.24412/2073-0454-2023-5-21-23. EDN CVFFAR.

2. Былевский П.Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. №8. С.46-56. DOI 10.7256/2454-0757.2023.8.43909. EDN UZDRFW.

3. Искусственный интеллект — угроза человечеству? NTA. 27 марта 2020 // Vc.ru. Стартапы, бизнес, технологии (Электронный ресурс) URL: https://vc.ru/newtechaudit/115631-iskusstvennyy-intellekt-ugroza-chelovechestvu (дата обращения: 05.11.2023).

4. Мельников С.Ю., Пересыпкин В.А. Об эволюции классических вероятностных моделей языка в естественно-языковых приложениях // Вестник современных цифровых технологий. 2023. № 16. С. 4-14. EDN YDIGDT.

5. Морхат П.М. Риски и угрозы, связанные с применением искусственного интеллекта // Аграрное и земельное право. 2017. №12(156). С. 60-65.

Об авторах

Кузнецова Татьяна Юрьевна — курсант 3-го курса Московского университета МВД России им. В. Я. Кикотя (Россия, Москва)
E-mail: Not200104@mail.ru

Хасин Александр Евгеньевич — инспектор Центра специального назначения инновационных технологий МВД России (Россия, Москва)
E-mail: Alexkhasin@mail.ru

Научный руководитель

Полянская Елена Петровна — старший преподаватель кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России им. В. Я. Кикотя (Россия, Москва)
E-mail: azhara87@bk.ru

About the authors

Tatyana Yu. Kuznetsova —3nd year cadet of the Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
E-mail: Not200104@mail.ru

Alexander E. Khasin — Inspector of the Center for Special Purpose Innovative Technologies of the Ministry of Internal Affairs of Russia (Russia, Moscow)
E-mail: Alexkhasin@mail.ru

Scientific supervisor

Elena P. Polyanskaya — senior lecturer at the Department of Information Security of the educational and Scientific complex of Information Technologies Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
E-mail: azhara87@bk.ru

УДК 004.008: 004.056

ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ВОЗМОЖНОСТИ ИЛИ УГРОЗЫ

Самойлов А. В.
Московский университет МВД России им. В. Я. Кикотя (Россия, Москва)
(Russia, Moscow)
samojva05@gmail.com

Научный руководитель:
Полянская Е. П.
Московский университет МВД России им. В. Я. Кикотя (Россия, Москва)
azhara87@bk.ru

Аннотация

Статья предлагает читателям исследование возможностей и угроз технологий искусственного интеллекта. Рассматриваются меры безопасности, формулируются и рекомендации, которые могут помочь защитить пользователей, их компьютерно-сетевые ресурсы, сведения и данные. Анализ примеров использования искусственного интеллекта делают статью полезной для специалистов, занимающихся цифровой трансформацией разных отраслей.

Ключевые слова: искусственный интеллект, превентивные меры, информационная безопасность, угрозы, меры безопасности

ARTIFICIAL INTELLIGENCE TECHNOLOGIES: OPPORTUNITIES OR THREATS

Andrey V. Samoilov
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
samojva05@gmail.com

Scientific supervisor:
Elena P. Polyanskaya
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia
(Russia, Moscow)
azhara87@bk.ru

Abstract
The article offers readers a study of the possibilities and threats of artificial intelligence technologies. Security measures are considered, and recommendations are formulated that can help protect users, their computer and network resources, information and data. The analysis of examples of the use of artificial intelligence makes the article useful for specialists involved in the digital transformation of various industries.

Keywords: artificial intelligence, preventive measures, information security, threats, security measures

Введение

В последние годы искусственный интеллект (ИИ) стал одной из самых обсуждаемых тем в мире технологий. ИИ — это область компьютерных наук, которая стремится создать интеллектуальные машины, способные анализировать, учиться и принимать решения, как это делают люди [3]. Благодаря своим возможностям ИИ находит все большее применение в различных отраслях и областях жизни.

Применение ИИ в медицине

Одно из наиболее важных и перспективных применений искусственного интеллекта — медицина. Использование ИИ в этой сфере может существенно повысить эффективность диагностики, лечения и прогнозирования заболеваний. Алгоритмы машинного обучения и ИИ уже помогают врачам определять ранние симптомы опасных заболеваний, таких как рак, болезни сердца и глаза. Более того, ИИ может помочь врачам в принятии решений по назначению лечения и определению наилучшего подхода к каждому пациенту. Интеллектуальные системы, основанные на ИИ, также могут помочь врачам в управлении медицинскими данными, улучшая качество медицинских услуг и позволяя врачам быстро находить нужную информацию [1].

Применение ИИ на транспорте

Другой сферой, где ИИ уже нашел широкое применение, является транспорт. Автоматизация транспортных средств и улучшение безопасности дорожного движения — главные задачи, решаемые при помощи искусственного интеллекта. Автомобильная промышленность уже использует технологии ИИ для создания автопилотов и улучшения систем безопасности. Искусственный интеллект позволяет свести к минимуму риск водителя и сделать дорогу безопаснее. Кроме того, ИИ применяется в системах управления транспортным потоком, позволяя оптимизировать движение транспорта и предотвращать пробки на дорогах.

Применение ИИ в финансовой сфере

Неотъемлемой частью банковской и финансовой сферы является применение искусственного интеллекта. Банки используют ИИ для анализа данных о клиентах, идентификации мошеннических операций и предоставления персонализированных услуг. ИИ может анализировать миллионы транзакций в режиме реального времени и обнаруживать любые аномалии, а также предоставлять рекомендации клиентам по инвестициям и управлению финансами [2].

Применение ИИ в полиции

Искусственный интеллект (ИИ) располагает колоссальной возможностью с целью использования его в правоохранительной деятельности, а также полиция уже стремительно вводит эту технологию с целью решения разных проблем, а также увеличения производительности собственной деятельность.

Один с более красочных образцов считается применение ИИ в концепциях видеонаблюдения, а также рассмотрения видеоданных. Системы, базирующиеся в ИИ, готовы автоматически выявлять подозрительные действия либо поведение в видеозаписях, что может помочь правоохранительным органам в расследовании преступлений. К примеру, ИИ способен выявлять нарушения общественного порядка, такие как драки либо небезопасное управление автотранспортным средством, кроме того, искать пропавших людей либо распознать подозреваемых по их внешним показателям [4].

Иным образцом использования ИИ в полиции считается применение алгоритмов машинного обучения с целью прогнозирования, а также предотвращения правонарушений. ИИ способен исследовать большие объёмы информации о преступности, в том числе о многих внешних

факторах, таких как погода либо даты происшествий, и в основе данных анализов прогнозировать вероятные места, а также периоды и в время совершения преступлений. Это дает возможность правоохранительным органам принять меры предварительно, а также избежать преступления либо наложить дополнительные меры безопасности [5].

Кроме того, ИИ стремительно используется в борьбе с киберпреступностью. Угрозы в области кибербезопасности регулярно эволюционируют, а также классические способы защиты имеют все шансы быть недостающими. Применение ИИ в данной сфере дает возможность автоматически выявлять, а также исследовать аномалии в Сети, моментально реагировать на кибератаки, а также прогнозировать возможные хакерские опасности. ИИ, кроме того, способен быть использован с целью исследования интеллектуальных систем прогноза, а также избежания, устранения, предупреждения киберпреступлений.

Заключение

Искусственный интеллект играет все более важную роль в нашей жизни и будет представлять большой интерес в ближайшие годы. Применение искусственного интеллекта в различных сферах уже принесло значительные преимущества, позволяющие снизить стоимость услуг, повысить эффективность и улучшить безопасность. Однако, несмотря на все достижения, следует помнить о потенциальных негативных последствиях, таких как угрозы приватности и потеря рабочих мест. Поэтому, развитие и применение искусственного интеллекта должны быть осуществлены с учетом этических и социальных аспектов.

Список источников

1. Арсеньев А. С., Ильенков Э. В., Давыдов В. В. Машина и человек, кибернетика и философия / Ильенков Э. В. Идеал. Собр. соч. Т. 3. М.: Канон+, РООИ «Реабилитация». С. 143–161.

2. Бруссард М. Искусственный интеллект. Пределы возможного. — М.: Альпина нон-фикшн, 2020. 361 с.

3. Былевский П. Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56. DOI 10.7256/2454–0757.2023.8.43909. EDN UZDRFW.

4. Грациано М. Наука сознания. Современная теория субъективного опыта. М.: Альпина нон-фикшн, 2021. 256 с.5. Девятков В. В. Системы искусственного интеллекта. М.: МГТУ им. Н. Э. Баумана, 2001. 352 с.

Об авторе

Самойлов Андрей Владимирович —
курсант 3 курса
Московского университета
МВД России им. В. Я. Кикотя
(Россия, Москва)
E-mail: samojva05@gmail.com

Научный руководитель

Полянская Елена Петровна —
старший преподаватель кафедры
информационной безопасности
учебно-научного комплекса
информационных технологий
Московского университета
МВД России им. В. Я. Кикотя
(Россия, Москва)
E-mail: azhara87@bk.ru

About the author

Andrey V. Samoilov —3rd year cadet of
the Vladimir Kikot Moscow University of
the Ministry of Internal Affairs of Russia
(Russia, Moscow)
E-mail: samojva05@gmail.com

Scientific supervisor

Elena P. Polyanskaya —
senior lecturer at the Department of
Information Security
of the educational and Scientific complex
of Information Technologies
Vladimir Kikot Moscow University of
the Ministry of Internal Affairs of Russia
(Russia, Moscow)
E-mail: azhara87@bk.ru

УДК 004.008: 004.056

ПРЕИМУЩЕСТВА И НЕДОСТАТКИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хуранова К. М.
Финансовый университет при Правительстве Российской Федерации
(Россия, Москва)
kama7trick@gmail.com

Научный руководитель:
Егоров Е. В.
Финансовый университет при Правительстве Российской Федерации
(Россия, Москва)
EVEgorov@fa.ru

Аннотация
В статье выделены основные применения искусственного интеллекта в задачах информационной безопасности, преимущества и недостатки, проанализированы риски и угрозы, связанные с искусственным интеллектом, даны рекомендации по минимизации рисков и оптимизации использования искусственного интеллекта.

Ключевые слова: искусственный интеллект, информационная безопасность, кибератаки, инциденты информационной безопасности

ADVANTAGES AND DISADVANTAGES OF ARTIFICIAL INTELLIGENCE IN ENSURING INFORMATION SECURITY

Kamilla M. Khuranova
Financial University under the Government of the Russian Federation (Russia, Moscow)
kama7trick@gmail.com

Scientific supervisor:
Evgeniy V. Egorov
Financial University under the Government of the Russian Federation (Russia, Moscow)
EVEgorov@fa.ru

Abstract
The article highlights the main applications of artificial intelligence in information security tasks, advantages and disadvantages, analyzes the risks and threats associated with artificial intelligence, and provides recommendations on minimizing risks and optimizing the use of artificial intelligence.

Keywords: artificial intelligence, information security, cyber attacks, information security incidents

Введение

В последнее время в связи с повышением значимости информационной безопасности различных объектов информатизации отмечается активное применение методов искусственного интеллекта в процессе решения задач по обеспечению защиты информации [2]. В современных условиях информационная составляющая оказалась на первом плане. Эксперты считают, что информационные войны с развитием искусственного интеллекта выходят на совершенно новый уровень. Использование новых технологий способствует роботизации процессов при ведении информационного и дезинформационного противоборства. Это, в свою очередь, может привести к возникновению кризисных явлений невероятных масштабов.

Главными целями являются рассмотрение основных преимуществ и недостатков использования искусственного интеллекта в сфере информационной безопасности; выявление возможных рисков и угроз, связанных с его применением; предложение рекомендаций по минимизации подобных рисков и оптимизации использования искусственного интеллекта для обеспечения информационной безопасности.

Объектом исследования является использование искусственного интеллекта в обеспечении информационной безопасности. Предметом исследования является анализ возможностей и рисков применения искусственного интеллекта в сфере информационной безопасности.

Значимость исследования заключается в выявлении рисков и угроз, связанных с использованием искусственного интеллекта. На основе этого

разработаны рекомендации и методики по минимизации рисков и оптимизации использования искусственного интеллекта для обеспечения информационной безопасности.

1. Применение искусственного интеллекта в задачах информационной безопасности

Искусственный интеллект (далее — ИИ) в области информационной безопасности представляет собой программное обеспечение, которое анализирует окружающую среду, распознаёт события и принимает соответствующие меры. Он особо эффективен в выявлении закономерностей и аномалий, что делает его полезным инструментом для обнаружения угроз.

Основными принципами информационной безопасности является триада: конфиденциальность, целостность, доступность. ИИ может обеспечить конфиденциальность данных путём использования алгоритмов шифрования, которые позволяют защитить данные от несанкционированного доступа. Для обеспечения целостности данных ИИ может использоваться либо для мониторинга и анализа данных, чтобы обнаружить любые несоответствия или ошибки в данных, либо для автоматического исправления ошибок и восстановления повреждённых данных [4]. Для того чтобы обеспечить доступность данных, ИИ может создавать автоматические резервные копии, а также управлять хранилищем, где как раз и находится какая-либо информация, требующая защиты.

Помимо выполнения всех принципов информационной безопасности ИИ активно используется в прогнозировании какой-либо атаки. К примеру, если была выявлена новая уязвимость, то для того, чтобы узнать использовалась ли она в прошлом, ИИ проанализирует данные журнала и даст оценку того, насколько критична данная уязвимость. При ситуации, если атака не встречалась ранее, ИИ проведёт анализ и даст оценку того, достаточно ли прямых доказательств для прогнозирования дальнейших действий злоумышленников.

Использование ИИ в области информационной безопасности обосновано двумя основными факторами: необходимостью быстрого реагирования на кибератаки и дефицитом опытных специалистов в этой области. Отвлекаясь на факт быстрого реагирования на кибератаки, приведём статистику сокращения времени обнаружения угроз при использовании технологий ИИ (см. статистику сокращения времени обнаружения угроз при использовании технологий ИИ на Рисунке 1). Таким образом, наглядно видно, что скорость обнаружения кибератак с использованием ИИ намного выше, чем в «ручном» режиме.

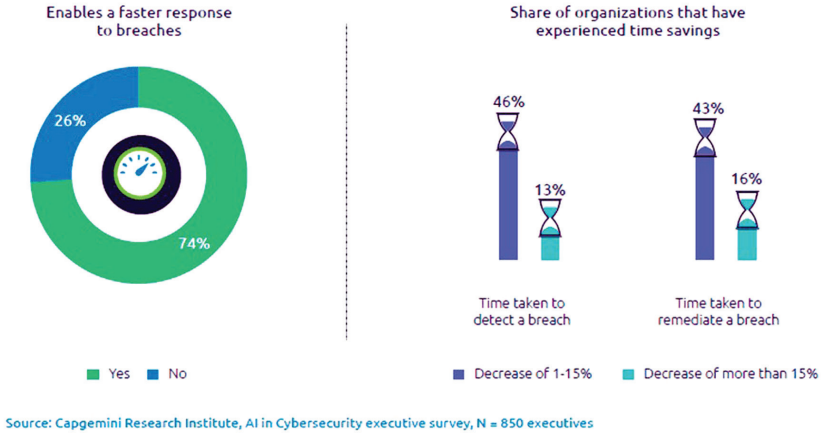

Рисунок 1. Статистика сокращения времени обнаружения угроз при использовании технологий ИИ

Крупные кибератаки могут происходить в любое время и развиваться очень быстро. Если компания не имеет круглосуточной службы безопасности, то защита в нерабочее время может быть затруднительной. Кроме того, злоумышленники могут проводить отвлекающие маневры, чтобы отвлечь киберспециалистов и это может привести к уязвимостям в системе. В таких случаях система реагирования на кибератаки на основе искусственного интеллекта может помочь, автоматизируя рутинные задачи аналитиков и обеспечивая быстрое реагирование на инциденты без участия человека.

К примеру, ИИ, обученный на ранее решённых инцидентах, самостоятельно даст рекомендацию по реагированию в зависимости от типа атаки и её свойств, но если атака не встречалась ранее, то ИИ, заподозрив нетипичное событие, оповестит сотрудников из департамента информационной безопасности [1]. ИИ находится на высоком уровне развития достаточным для решения задач информационной безопасности. К таким задачам относятся: анализ типов данных, выявление фишинга, спама, прогноз угроз и т.д.

2. Сильные и слабые стороны искусственного интеллекта в информационной безопасности

Использование искусственного интеллекта в информационной безопасности обусловлено несколькими факторами. Во-первых, ИИ обла-

дает высокой эффективностью и точностью. Во-вторых, он способен обрабатывать огромные объемы данных, что позволяет обнаруживать угрозы в режиме реального времени и быстро реагировать на кибератаки. Однако следует учитывать, что ИИ не является идеальной моделью и может допускать ошибки, особенно при обучении на недостаточном количестве данных [5].

Это может привести к ложным результатам детектирования аномалий. Помимо этого, использование ИИ требует больших вычислительных мощностей. Но несмотря на это, система реагирования на кибератаки на основе ИИ может помочь автоматизировать рутинные задачи аналитиков и обеспечить быстрое реагирование на инциденты без участия человека.

В дополнении к вышесказанному, к сильным сторонам относится тот факт, что системы ИИ постоянно учатся и адаптируются к развивающимся угрозам, улучшая свою способность обнаруживать новые векторы атак и реагировать на них.

К слабым сторонам нельзя не отнести возможность атак, специально предназначенных для обмана ИИ или манипулирования ими. Также ИИ с трудом интерпретирует сложную контекстуальную информацию или принимает интуитивные решения на основе неизмеримых факторов, что ограничивает его способность к пониманию намерений человека или выявление тонких угроз [3]. Важно отметить, что хоть ИИ и предлагает значительные преимущества в информационной безопасности, его следует использовать в сочетании с человеческим опытом и контролем, чтобы смягчить эти недостатки и обеспечить надёжную защиту.

3. Риски и угрозы искусственного интеллекта в сфере информационной безопасности

В своем исследовании о кибератаках на системы искусственного интеллекта, проведенном 2023 году, аналитическое агентство Gartner опросило разработчиков о случаях нарушения конфиденциальности ИИ и ИБ-инцидентах [7]. Ответы 41% опрошенных компаний подтвердили наличие таких нарушений. И на основе этих данных был составлен перечень атак, направленных на ИИ:

— шпионаж;
— саботаж;
— мошенничество.

Шпионаж предполагает получение знаний о системе и использование полученной информации в личных целях или для планирования сложных атак. **Саботаж** — противоправные манипуляции внутреннего

нарушителя, направленные на поломку системы ИИ. Данное деяние возможно провести несколькими способами:

— отправление такого количества запросов на сторону ИИ, обработка которых требует больше времени, чем обычно;

— увеличение количества неправильно классифицированных объектов, чтобы увеличить объем ручного труда для ложных срабатываний или подорвать доверие к системе;

— изменение модели путём её переобучения.

Мошенничество — своеобразный обман ИИ при использовании неправильной классификации. Мошенник может провести это деяние, например, взаимодействуя с системой на этапе её обучения, такой подход имеет название «Отравление». «Отравление» данных — тип кибератаки, при которой злоумышленник манипулирует или изменяет данные, используемые в системах машинного обучения или искусственного интеллекта. Цель атаки — обмануть систему путем введения вредоносных или вводящих в заблуждение данных, что приведет к неточным результатам или поставит под угрозу целостность системы.

4. Рекомендации по минимизации рисков и оптимизации использования искусственного интеллекта для обеспечения информационной безопасности

Нужно тщательно проводить анализ данных, которые будут использоваться для обучения ИИ. Необходимо убедиться в том, что данные не содержат конфиденциальной информации, которая может быть использована для взлома системы. Также необходимо убедиться в том, что данные не содержат ошибок или искажений, которые могут привести к неправильным выводам ИИ [6]. Также следует ввести использование методов шифрования каналов связи и многофакторную аутентификацию. Необходимо проводить различные тестирования над системой ИИ, например, тестирование на проникновение, чтобы проверять уровень защиты системы ИИ. Ещё следует установить контроль доступа, то есть ограничить доступ к системе ИИ только авторизированным пользователям.

Для оптимизации работы искусственного интеллекта в области информационной безопасности можно использовать автоматический сбор, структурирование и анализ информации из различных источников, включая открытые источники, новостные статьи, сообщества по информационной безопасности и социальные сети. Это позволяет получить более полное представление о текущей киберобстановке, новых угрозах и трендах. Кроме того, применение ИИ в анализе и прогнозировании

рисков позволяет создавать модели и сценарии для оценки вероятности возникновения определенных угроз и их потенциального воздействия на систему. Именно это поможет организациям принимать информированные решения и принимать меры по снижению рисков.

Заключение

Применение искусственного интеллекта в области кибербезопасности позволяет автоматически собирать и анализировать информацию из различных источников, что помогает организациям более эффективно оценивать риски и принимать информированные решения. Однако существуют риски, связанные с возможными атаками на системы ИИ. Для минимизации этих угроз необходимо принимать меры по улучшению безопасности систем ИИ, такие как шифрование данных и анализ аномальной активности.

Использование искусственного интеллекта в сфере кибербезопасности требует значительных вычислительных ресурсов и большого объема данных, однако, это является необходимым для эффективной борьбы с киберугрозами и повышения уровня безопасности в цифровом мире. Несмотря на это, следует учитывать возможные угрозы, связанные с атаками на системы ИИ, и принимать меры по улучшению безопасности, включая шифрование данных и анализ аномальной активности.

Таким образом, в ходе исследования были рассмотрены основные преимущества и недостатки использования искусственного интеллекта в сфере информационной безопасности. Были выявлены возможные риски и угрозы, связанные с применением ИИ в области ИБ. А также были предложены рекомендации по минимизации некоторых рисков и оптимизации использования ИИ для обеспечения информационной безопасности.

Список источников

1. Асатрян А. Применение ИИ и машинного обучения в кибербезопасности: взгляд эксперта на возможности, ограничения и риски использования новых технологий / CISOCLUB. 31.05.2023 (Электронный ресурс) URL: https://cisoclub.ru/primenenie-ii-i-mashinnogo-obuchenija-v-kiberbezopasnosti-vzgljad-jeksperta-na-vozmozhnosti-ogranichenija-i-riski-ispolzovanija-novyh-tehnologij (дата обращения: 05.11.2023).

2. Бекматов А. К., Кутдусова Э. Р., Мукимов Ш. И., Давлатова Н. Н. Прогрессивные тенденции применения искусственного интеллекта в области

информационной безопасности // Экономика и социум. 2023. № 6 (109). С. 1264–1270.

3. Былевский П. Г. Культурологическая деконструкция социально-культурных угроз ChatGPT информационной безопасности российских граждан // Философия и культура. 2023. № 8. С. 46–56. DOI 10.7256/2454–0757.2023.8.43909. EDN UZDRFW.

4. Куренная В. О. Искусственный интеллект в информационной безопасности // Научно-образовательный журнал для студентов и преподавателей «StudNet».2022. № 6. С. 7202–7208.

5. Литвинов Р. Искусственный интеллект в информационной безопасности / Инфобезопасность. 14 августа 2023 г. (Электронный ресурс) URL: https://infobezopasnost.ru/blog/articles/iskusstvennyj-intellekt-v-informatsionnoj-bezopasnosti (дата обращения: 05.11.2023).

6. Шабанов А. Применение технологий искусственного интеллекта в информационной безопасности / Anti-Malware.ru. 17 июня 2020 г. (Электронный ресурс) URL: https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security (дата обращения: 05.11.2023).

7. Top Strategic Cybersecurity Trends for 2023 / Gartner.com. 2023. April 19 (Электронный ресурс) URL: https://www.gartner.com/en/articles/top-strategic-cybersecurity-trends-for-2023 (дата обращения: 05.11.2023).

Об авторе

Хуранова Камилла Мухамедовна — студентка 2-го курса (бакалавриат) Финансового университета при Правительстве Российской Федерации (Россия, Москва)
E-mail: kama7trick@gmail.com

Научный руководитель

Егоров Евгений Владимирович — кандидат физико-математических наук, старший преподаватель департамента информационной безопасности Финансового университета при Правительстве Российской Федерации (Россия, Москва)
E-mail: EVEgorov@fa.ru

About the author

Kamilla M. Khuranova —2nd year student (Bachelor's degree) Financial University under The Government of the Russian Federation (Russia, Moscow)
E-mail: kama7trick@gmail.com

Scientific supervisor

Evgeniy V. Egorov — Candidate of Physical and Mathematical Sciences, Senior Lecturer at the Department of Information Security of the Financial University under the Government of the Russian Federation (Russia, Moscow)
E-mail: EVEgorov@fa.ru

УДК 004.008: 004.056

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ПРОГНОЗИРОВАНИЯ КИБЕРАТАК

Мишин А. Е.
Финансовый университет при Правительстве Российской Федерации
(Россия, Москва)222347@edu.fa.ru

Научный руководитель:
Былевский П. Г.
Московский государственный лингвистический университет (Россия, Москва);
Финансовый университет при Правительстве Российской Федерации
(Россия, Москва)
pr-911@yandex.ru

Аннотация

Данная статья представляет собой обзор применения машинного обучения в области кибербезопасности. Она начинается с общего представления о кибербезопасности и машинном обучении, а затем переходит к обсуждению различных типов кибератак и угроз, которые они представляют. Статья также рассматривает различные типы алгоритмов машинного обучения и их применение для применения из в области информационной безопасности, а именно в предсказании кибератак. В статье приводятся реальные примеры и тенденции применения этих механизмов и результаты, а также обсуждаются проблемы и вызовы, связанные с использованием машинного обучения в кибербезопасности. В заключении обобщаются основные идеи статьи и предлагаются возможные направления для будущих исследований.

Ключевые слова: машинное обучение, кибербезопасность, кибератаки, прогнозирование, алгоритмы машинного обучения

USING MACHINE LEARNING TO PREDICT CYBER ATTACKS

Alexey E. Mishin
Financial University under the Government of the Russian Federation (Russia, Moscow)222347@edu.fa.ru

Scientific supervisor:
Pavel G. Bylevskiy
Moscow State Linguistic University (Russia, Moscow);
Financial University under the Government of the Russian Federation (Russia, Moscow)
pr-911@yandex.ru

Abstract
This article provides an overview of the application of machine learning in the field of cybersecurity. It starts with a general understanding of cybersecurity and machine learning, and then proceeds to discuss the various types of cyber attacks and the threats they pose. The article also examines various types of machine learning algorithms and their application for information security applications, namely in the prediction of cyber attacks. The article provides real-world examples and trends in the use of these mechanisms and results, as well as discusses the problems and challenges associated with the use of machine learning in cybersecurity. In conclusion, the main ideas of the article are summarized and possible directions for future research are proposed.

Keywords: machine learning, cybersecurity, cyber attacks, forecasting, machine learning algorithms

Введение

В современном мире кибербезопасность стала одним из ключевых аспектов, которые определяют надежность и эффективность информационных систем. С учетом растущего числа кибератак и угроз безопасности данных (порядка 40% только за последний год [3] и соответственно драматически растущих бюджетов организация на обеспечение информационной безопасности в целом и кибербезопасности в частности[1], о котором свидетельствуют исследования аналитических агентств [2] важность прогнозирования и предотвращения таких атак не может быть недооценена.

Одним из подходов, которые показали значительный потенциал в этой области, является использование машинного обучения. Машинное обучение в самом общем определении — это подраздел искусственного интеллекта, который использует статистические методы для улучшения производительности системы с течением времени, основываясь на данных из прошлого опыта.

В статье исследуется, как машинное обучение может быть использовано для прогнозирования. Мы рассмотрим различные типы кибератак, которые могут быть предсказаны с помощью машинного обучения, а также обсудим некоторые из основных алгоритмов машинного обуче-

ния, которые могут быть использованы в этом контексте. Наконец, мы обсудим некоторые из вызовов и проблем, связанных с использованием машинного обучения в кибербезопасности, и предложим возможные направления для будущих исследований.

Кибератаки: обзор и типы

Кибератаки представляют собой попытки несанкционированного доступа к, использования или уничтожения данных в цифровой форме. Они могут быть направлены против индивидуальных пользователей, корпораций и даже государств. Именно поэтому вопросы прогнозирования таких атак на различных уровнях является актуально проблемой и вызовом [4]. Вот некоторые из наиболее распространенных типов кибератак:

1**. Фишинг (Phishing).** Попытка обмануть пользователей, чтобы они предоставили свои личные данные, такие как пароли или номера кредитных карт, обычно через поддельные электронные сообщения или веб-сайты [5].

2**. Атака «отказ в обслуживании» (Denial of Service, DoS).** Целью является в самом общем случае перегрузка системы или сети, чтобы сделать ее недоступной для пользователей [6].

3**. Вредоносное ПО (Malware).** Любое программное обеспечение, которое было разработано для нанесения вреда данным, устройствам или людям [7].

4**. Атака «человек посередине» (Man-in-the-Middle, MitM).** Злоумышленник перехватывает и возможно изменяет коммуникацию между двумя сторонами [8].

Нетрудно заметить, что каждый из этих типов атак представляет собой уникальные угрозы для безопасности данных и требует различных стратегий для их предотвращения и обнаружения. Некоторые из таких подходов или же стратегий будут рассмотрены нами далее по ходу повествования.

Машинное обучение: обзор и типы

Попытаемся дать наиболее общее определение машинному обучению. Так, машинное обучение — это подраздел искусственного интеллекта, который использует статистические методы для улучшения производительности системы с течением времени, основываясь на данных о прошлом опыте. Приведём некоторые из основных типов алгоритмов машинного обучения, которые могут быть использованы в контексте кибербезопасности.

1. Логистическая регрессия

Согласно источнику [9], это статистический метод, который используется для прогнозирования вероятности возникновения определенного события путем подгонки данных к логистической функции. В общем случае, то, что из себя представляет данный метод, можно проиллюстрировать Рис. 1.

Рисунок 1. Логистическая регрессия [1]

2. Случайный лес (Random Forest)

Это алгоритм машинного обучения, который использует множество деревьев решений для классификации объектов на основе их признаков [10] (Рис. 2).

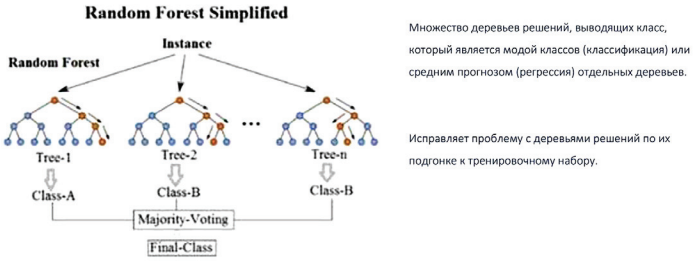

Рисунок 2. Случайный лес [2]

[1] Логистическая регрессия. Презентация. 98 фото / Фотобанк от TripTonkosti [Электронный ресурс] URL: https://triptonkosti.ru/2-foto/logisticheskaya-regressiya-prezentaciya-98-foto.html (дата обращения: 12.12.2023)

[2] Случайный лес / Ppt-online.org [Электронный ресурс] URL: https://cf2.ppt-online.org/files2/slide/x/X4UIwteRrs2ZG6f0O5liHKBdVkuN31DqJhCvTQ/slide-26.jpg (дата обращения: 12.12.2023)

3**. Метод ближайших соседей (K-Nearest Neighbor, KNN)**

Это алгоритм, который классифицирует объекты на основе близости их признаков к признакам объектов в обучающем наборе [11] (Рис. 3).

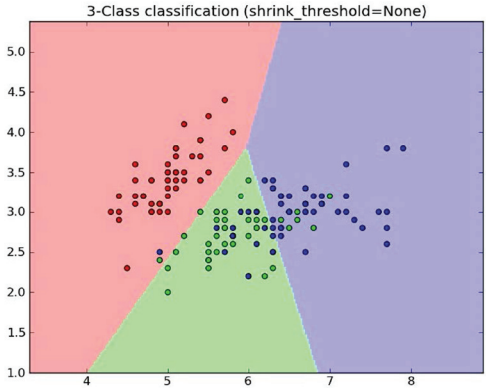

Рисунок 3. Метод ближайших соседей [3]

Применение машинного обучения для предсказания кибератак

Машинное обучение может быть использовано для предсказания кибератак различными способами. Вот некоторые из них:

1**. Обнаружение аномалий.** Алгоритмы машинного обучения могут быть обучены на нормальном поведении системы, и затем использованы для обнаружения отклонений от этого нормального поведения, которые могут указывать на кибератаку [12]. Это может включать в себя методы, такие как автоэнкодеры для обнаружения аномалий в данных временных рядов или методы кластеризации для группировки похожих типов поведения и выявления отклонений.

2**. Классификация атак.** Алгоритмы машинного обучения могут быть обучены на примерах различных типов атак, и затем использованы для классификации новых атак по типам [13]. Это может включать в себя методы, такие как глубокое обучение для автоматического извлечения признаков из сырых данных и последующей классификации на основе этих признаков.

[3] Метод ближайших соседей. Scikit-learn: Machine Learning in Python / Jaquesgrobler. github.io [Электронный ресурс] URL: https://jaquesgrobler.github.io/online-sklearn-build/_images/plot_nearest_centroid_11.png (дата обращения: 12.12.2023)

3**. Прогнозирование атак.** Алгоритмы машинного обучения могут быть обучены на исторических данных о кибератаках, и затем использованы для прогнозирования вероятности будущих атак [14]. Это может включать в себя методы, такие как рекуррентные нейронные сети для моделирования временных рядов атак и прогнозирования будущих атак на основе прошлых данных.

4**. Генерация графов атак.** Машинное обучение может быть использовано для генерации графов атак, которые представляют собой визуализацию возможных путей атаки в сети [15]. Это может включать в себя методы, такие как генеративно-состязательные сети для генерации реалистичных графов атак.

5**. Анализ угроз**. Машинное обучение может быть использовано для анализа и прогнозирования киберугроз [16]. Это может включать в себя методы, такие как нейронные сети для анализа больших объемов данных и выявления скрытых угроз.

Проблемы и вызовы

Несмотря на обещающие возможности машинного обучения в области кибербезопасности, существуют определенные проблемы и вызовы, которые необходимо преодолеть.

1**. Качество данных.** Отмечается важность качества данных в контексте машинного обучения для кибербезопасности [17], именно качество входных данных имеет решающее значение для эффективности моделей машинного обучения. Ввиду этого, недостаточное качество данных может привести к низкой точности прогнозирования.

2**. Адаптация к новым угрозам.** Киберугрозы постоянно эволюционируют [18], и модели машинного обучения должны быть способны адаптироваться к новым видам атак.

3**. Проблема интерпретируемости.** Многие алгоритмы машинного обучения, особенно глубокие нейронные сети, являются, образно говоря, «черными ящиками», что затрудняет понимание того, как они делают свои прогнозы [19].

4**. Вопросы приватности.** Неоднократно отмечалось, в том числе на конференциях [20], что использование машинного обучения для анализа сетевого трафика может вызвать проблемы с приватностью, если не будут соблюдены соответствующие меры предосторожности.

Реальные примеры использования

Уже сегодня на рынке можно найти примеры использования алгоритмов машинного обучения для предсказания кибератак.

Обратимся к примерам.

Microsoft Azure использует множество алгоритмов машинного обучения для обеспечения кибербезопасности. [Одним из примеров является использование алгоритмов обучения с учителем для классификации вредоносного ПО на основе его поведения [21]. Это означает, что модель обучается на основе предварительно размеченных данных, где каждому примеру (в данном случае, вредоносному ПО) сопоставляется метка (например, «вредоносное» или «безвредное»). Затем модель использует эти данные для обучения, чтобы в дальнейшем классифицировать новые, ранее неизвестные примеры.

Кроме того, Azure использует алгоритмы обучения без учителя для обнаружения аномалий в сетевом трафике. Эти алгоритмы обучаются на данных, которые не имеют предварительных меток, и пытаются найти структуру или шаблоны в данных. В контексте обнаружения аномалий это может означать обнаружение активности, которая существенно отличается от «нормального» поведения.

Yandex Cloud также использует машинное обучение для обеспечения кибербезопасности. Они используют алгоритмы глубокого обучения, такие как нейронные сети, для анализа больших объемов данных и выявления скрытых угроз [22]. Глубокое обучение — это подмножество машинного обучения, которое использует нейронные сети с большим количеством слоев. Эти «глубокие» нейронные сети способны моделировать очень сложные отношения и находить скрытые шаблоны в данных, что может быть особенно полезно при работе с большими объемами данных.

Заключение

В этой статье мы рассмотрели, как машинное обучение может быть использовано для предсказания кибератак. Мы обсудили различные типы кибератак и алгоритмы машинного обучения, которые могут быть использованы для их предсказания. Мы также рассмотрели некоторые из вызовов и проблем, связанных с использованием машинного обучения в области кибербезопасности.

Однако, несмотря на эти проблемы, потенциал машинного обучения в области кибербезопасности огромен. С развитием технологий и увеличением объема данных, доступных для анализа, возможности машинного обучения будут только расти [23].

В будущем исследования могут сосредоточиться на разработке новых алгоритмов машинного обучения, специально разработанных для обработки кибербезопасности. Кроме того, может быть проведено больше ра-

боты по созданию систем, которые могут автоматически адаптироваться к меняющимся угрозам без необходимости в ручном вмешательстве [24].

Согласно последним тенденциям [25], использование предобученных нейронных сетей является актуальным направлением развития технологии машинного обучения. Это позволяет системам масштабироваться для них, генерировать новые модели на ходу и предоставлять более быстрые и точные результаты.

В заключение, машинное обучение представляет собой мощный инструмент, который может значительно улучшить нашу способность предсказывать и предотвращать кибератаки. Однако, как и любой мощный инструмент, он должен использоваться с осторожностью и с учётом потенциальных рисков и проблем, некоторые из которых мы описали и рассмотрели пути к их нейтрализации.

Список источников

1. Cybersecurity Statistics. 2022 Cybersecurity Challenges / Fortinet.com [Электронный ресурс] URL: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics (дата обращения: 12.12.2023)

2. Kizzee K. Cyber Attack Statistics to Know / Parachute.cloud. 2023. September 13 [Электронный ресурс] URL: https://parachute.cloud/cyber-attack-statistics-data-and-trends/ (дата обращения: 12.12.2023)

3. Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks / Checkpoint.com. 2023, January 5. / [Электронный ресурс] URL: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks (дата обращения: 12.12.2023)

4. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice12. Syngress, 2014. 240 c.

5. Dodge R. C., Carver C., Ferguson A. J. Phishing for User Security Awareness // Computers & Security. 2007. № 1(26). Pp. 73–80.

6. Mirkovic J., Reiher P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms // ACM SIGCOMM Computer Communication Review. 2004. № 2(34). Pp.39–53. DOI: 10.1145/997150.997156

7. Aycock J. Computer Viruses and Malware. New York: Springer Science & Business Media, 2006. 228 p.

8. Conti M., Dragoni N., Lesyk V. A Survey of Man in the Middle Attacks // IEEE Communications Surveys & Tutorials. 2016. № 3. C. 2027–2051.

9. Hosmer D. W. Jr., Lemeshow S., Sturdivant R. X. Applied logistic regression. Hoboken: John Wiley & Sons, 2013. 528 p.

10. Breiman, L. Random forests // Machine learning. 2001. № 1(45). Pp. 5–32.

11. Altman N. S. An introduction to kernel and nearest-neighbor nonparametric regression // The American Statistician. 1992. № 3. Pp.175–185.

12. Chandola V., Banerjee A., Kumar V. Anomaly detection: A survey // ACM computing surveys (CSUR). 2009. № 3. Pp.1–58.

13. Buczak A. L., Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection // IEEE Communications Surveys & Tutorials. 2016. № 2. Pp.1153–1176.

14. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection // 31st IEEE Symposium on Security and Privacy, SP 2010, 16–19 May 2010, Berleley/Oakland, California, USA. IEEE Computer Society 2010. Pp. 305–316. DOI: 10.1109/SP.2010.25

15. Singh K., Jha S. Cyber Threat Analysis And Prediction Using Machine Learning // 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N). 2021, December 17–18. Pp.1–5. DOI: 10.1109/ICAC3N53548.2021.9725445

16. Sarker I. H., Kayes A. S.M., Badsha S., Alqahtani H., Watters P., Ng A. Cybersecurity data science: an overview from machine learning perspective // Journal of Big Data. 2020. № 7(41). Pp.1–29. DOI: 10.1186/s40537–020–00318–5

17. Buczak A. L., Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection // IEEE Communications Surveys & Tutorials. 2016. Vol.18. Iss.2. Pp.1153–1176. DOI: 10.1109/COMST.2015.2494502

18. Sommer R., Paxson V. Outside the closed world: On using machine learning for network intrusion detection / 31st IEEE Symposium on Security and Privacy, S&P 2010, 16–19 May 2010, Berleley/Oakland, California, USA. Pp. 305–316. DOI: 10.1109/SP.2010.25

19. Guidotti R. Monreale A., Monreale A., Turini F., Turini F., Giannotti F., Giannotti F. A survey of methods for explaining black box models // ACM computing surveys. 2018. № 5(51). Pp. 1–45. DOI: 10.1145/3236009

20. Fredrikson M., Jha S. K., Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures // CCS '15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. October 2015. Pp.1322–1333. DOI: 10.1145/2810103.2813677

21. Azure Machine Learning best practices for enterprise security. 18.10.2023 / Cloud Skills Challenge. Nov 15, 2023 — Jan 15, 2024 [Электронный ресурс] URL: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-best-practices/ai-machine-learning-enterprise-security(дата обращения: 12.12.2023)

22. Microsoft Threat Intelligence. Gamifying machine learning for stronger security and AI models. 8.12.2021 / www.microsoft.com [Электронный ресурс] URL: https://www.microsoft.com/en-us/security/blog/2021/04/08/gamifying-machine-learning-for-stronger-security-and-ai-models (дата обращения: 12.12.2023)

23. Prospects and the future of machine learning / Merehead ю Fintech & Blockchain solutions Official website [Электронный ресурс] // URL: https://merehead.com/ru/blog/machine-learning-trends-in-2022(дата обращения: 12.12.2023)

24. Vodogrey2012. Машинное обучение в кибербезопасности. 23 декабря 2020 г. / habr.com[Электронный ресурс] URL: https://habr.com/ru/articles/534674 (дата обращения: 12.12.2023)

25. Коротеев М. В. Обзор некоторых современных тенденций в технологии машинного обучения // E-Management. Т. 1. № 1. С. 26–35. DOI: 10.26425/2658–3445–2018–1–26–35

Об авторе

Мишин Алексей Евгеньевич —
студент 2-го курса (бакалавриат)
Финансового университета при
Правительстве Российской Федерации
(Россия, Москва)
E-mail: 222347@edu.fa.ru

Научный руководитель

Былевский Павел Геннадиевич —
кандидат философских наук, доцент
департамента информационной
безопасности Финансового университета
при Правительстве Российской Федерации
(Россия, Москва); доцент кафедры
международной информационной
безопасности Московского
государственного лингвистического
университета (Россия, Москва)
E-mail: pr-911@yandex.ru.

About the author

Alexey E. Mishin —2nd year student
(Bachelor's degree)
Financial University
under The Government of the Russian
Federation (Russia, Moscow)
E-mail: 222347@edu.fa.ru

Scientific supervisor

Pavel G. Bylevskiy —
Candidate of Philosophical Sciences,
Associate Professor of the Information
Security Department of the Financial
University at Government of the
Russian Federation (Moscow, Russia);
Associate Professor of the Department
of International Information Security at
the Moscow State Linguistic University
(Russia, Moscow)
E-mail: pr-911@yandex.ru.

УДК 004.008+376

ФОРМАЛИЗАЦИЯ ПРОЦЕССА ТИФЛОКОММЕНТИРОВАНИЯ ДЛЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Гроховский М. И.
Московский государственный лингвистический университет
(Россия, Москва)
markgrokhovskii@gmail.com

Научный руководитель:
Демина Д. А.
Московский государственный лингвистический университет
(Россия, Москва)
d.a.demina@linguanet.ru

Аннотация
В статье обосновывается и предлагается формализация процесса тифлокомментирования, описываются важнейшие этапы деятельности тифлокомментатора, предлагается рассматривать тифлокомментарий с точки зрения движения и обработки информации с целью постепенного движения в направлении применения технологи искусственного интеллекта (ИИ) в тифлокомментировании.

Ключевые слова: тифлокомментарий, алгоритм, формализация, тифлореальность, когнитивные фильтры, инклюзивные процессы

FORMALIZATION OF THE TYPHLOCOMMENTATION PROCESS FOR ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Mark I. Grokhovskii
Moscow State Linguistic University (Russia, Moscow)
markgrokhovskii@gmail.com

Scientific supervisor:
Darya A. Demina
Moscow State Linguistic University (Russia, Moscow)
d.a.demina@linguanet.ru

Abstract

The article substantiates and proposes the formalization of the process of audiodescription, describes the most important stages of the activity of the audiodescriber, it is proposed to consider audiodescription from the perspective of movement and information processing in order to gradually move towards the use of AI in typhlokommentation.

Keywords: audiodescription, algorithm, formalization, typhloreality, cognitive filters, inclusive processes

Введение

Тифлокомментирование (ТК), как значимый элемент инклюзии, активно развивается в Российской Федерации при поддержке государства и научного сообщества. В практической части развитием и широким распространением ТК занимается институт РЕАКОМП под руководством С. Н. Ваньшина, по материалам его работ утвержден ГОСТ 57891–2022, задающий основные параметры системы ТК в РФ. Компьютеризация инклюзивных процессов является логической необходимостью развития гуманитарного общества, и сообщество специалистов ТК готовится к следующему этапу — применению в процессах создания и развития доступной среды, в том числе в ТК, элементов искусственного интеллекта (ИИ), способного трансформировать инклюзию в полноценную социальную технологию.

Важнейшим этапом подготовки процесса ТК к применению ИИ является его формализация, как допустимо точное выделение и описание этапов процесса ТК, что позволит в дальнейшем специалистам в области широкого применения ИИ определить области его применения и обеспечить эффективность ТК как важной социальной технологии инклюзивного общества будущего. Полная формализация процесса тифлокомментирования требует упорного исследовательского труда сегодняшних студентов-лингвистов, специалистов-тифлокомментаторов, когнитивных психологов и специалистов по применению ИИ.

На рис. 1 предложена модель процесса ТК — результат попытки формализации процесса ТК при взгляде на процесс, как на систему движения и обработки информации. Формализация, как научный метод, «позволяет систематизировать, уточнить и методологически прояснить содержание теории» [1], что относится и к процессам, имеющий сложный ин-

формационный характер. Изначальная сложность процесса ТК состоит в двух аспектах — выявление и перевод визуальной, часто имплицитной, информации в другую семиотическую систему, а также в напряженной когнитивной работе, необходимой для переноса образа в другую, отличную от начальной систему понятий, образов и когнитивных схем.

Рис. 1. Формализация процесса ТК

Описание модели: Блок 1 — объект наблюдения, источник визуальной информации. Количество наблюдаемой информации зависит от характеристик наблюдателя, от его способности «извлечь» из объекта нарратив, контекст, аллюзии, метафоры, знаки и символы, т.е. все то, что позволяет наблюдателю в дальнейшем через когнитивную деятельность создать образ наблюдаемого (блок 2).

Личность наблюдателя решающим образом влияет на конечный образ — именно качество «видения», способность выявлять имплицитное, интуиция и воображение позволяют наблюдателю собрать наиболее полную, значимую информацию об объекте, что позволит, в результате прохождения информации через когнитивный фильтр (блок 3), создать полноценный портрет объекта, который в процессе ТК еще предстоит транслировать аудитории.

Остановимся подробней на функциях и описании когнитивного фильтра. Укрупненно его можно разнести на отдельные элементы, отвечающие за переработку информации собственным образом. Библиотека, содержащая систему понятий, позволяет правильно интерпретировать нарратив, подсказывая наблюдателю суть происходящего или увиденного.

Галерея образов обеспечивает правильную реакцию на аллюзии и метафоры, и играет важную роль в выявлении имплицитного. Библиотека

когнитивных схем не дает наблюдателю отклониться от определенных шаблонов, тем самым служит гарантией устойчивого восприятия, т.е. ограничивает произвольную интерпретацию и неуместную фантазию.

Рис. 2. Когнитивный фильтр

Интуиция, как важнейший элемент, позволяет наблюдателю чувствовать замысел, зачастую скрытый глубоко под формой, и обеспечивает более качественное выявление имплицитного, которое часто в визуальных формах имеет проявление в виде тончайших намеков, а не прямых аллюзий и метафор. Возможно, именно интуиция является главным инструментом профессионального наблюдателя — ведь, по утверждению Б. Паскаля, «выразить словами сущность этой работы разума не может никто, да и понимание того, что она вообще происходит, доступно лишь немногим» [2].

Прохождение информации через когнитивный фильтр и является когнитивной работой наблюдателя, в результате которой возникает устойчивый портрет объекта ТК (блок 4), подготовленный для передачи аудитории.

Непосредственно перевод в вербальную форму осуществляется в блоке 6, здесь наблюдатель формирует проект будущего аудиотекста, учитывая формальные ограничения, накладываемые ГОСТ 57891–2022 (блок 5), где есть прямые указания на профессиональные особенности процесса ТК. Наблюдатель также учитывает лексические ограничения, т.е. он использует специальный лексический корпус, называемый в настоящей статье тезаурусом ТК (блок 7). Более развернуто блок 6 представлен на рис. 3.

Далее подготовленный наблюдателем проект аудиотекста должен пройти, в рамках продолжающейся когнитивной работы, через когнитивный корректор (блок 8). Поясним необходимость когнитивной коррекции, как неотъемлемой части процесса ТК. В рамках теории познания и выдвинутой ранее гипотезы о наличии тифлореальности при формализации процесса ТК следует учитывать, что когнитивные фильтры на-

блюдателя (реальность 1) и аудитории (реальность 2), могут отличаться настолько существенно, что вербальное описание портрета объекта, данные без учета этих отличий, не создаст у аудитории предпосылок для возникновения портрета объекта, приближенного к визуальному оригиналу, т.е. процесс ТК не достигнет своих целей. Неизбежно возникнет диссонанс между системой понятий наблюдателя и аудитории, что разрушит процесс ТК.

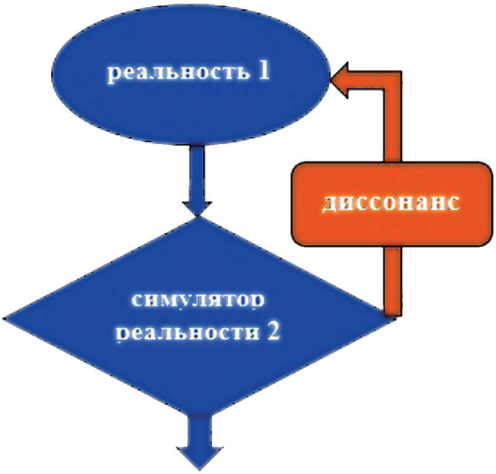

Рис. 3. Модель когнитивной коррекции тифлокомментария

Вводя в процесс когнитивный корректор, мы возлагаем на наблюдателя дополнительную когнитивную работу — пользуясь профессиональными понятиями о тифлореальности, он должен в процессе формирования тифлокомментария проверять вербальные фрагменты аудиотекста на их пригодность для инициации когнитивного фильтра аудитории. Для этого профессиональные знания тифлокомментатора должны содержать симулятор тифлореальности, что позволит ему проводить когнитивную коррекцию проекта аудиотекста.

В предельном случае тифлокомментатор (в результате применения профессионального навыка) в процессе ТК полностью переключается на реальность 2, тем самым резко повышая эффективность и сокращая время обращения к симулятору другой реальности и устранению возникающих диссонансов, т.е. проводя когнитивную коррекцию с доступной для профессионала скоростью.

Именно в этой части процесса ТК применение технологий ИИ выглядит наиболее перспективно, т.к. в когнитивной коррекции скорость обработки информации и доступность соответствующих информационных массивов, симулирующих тифлореальность, и позволит проводить качественный процесс тифлокомментирования, в том числе в режиме реального времени без искажений, задержек и диссонансов.

Заключение

Разумеется, более детальная формализация процесса ТК, учитывающая особенности применения ИИ в качестве когнитивного корректора, должна быть продолжена до внятного практического применения, согласованного тифлокомментаторами, лингвистами и специалистами по технологиям ИИ.

Список источников

1. Тарский А. Введение в логику и методологию дедуктивных наук. М.: ГИИЛ. 1948. 327 с.

2. Паскаль Б. Мысли. М.: Издательство имени Сабашниковых, 1995. 480 с.

Об авторе

Гроховский Марк Ильич — студент 3-го курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва)
E-mail: markgrokhovskii@gmail.com

Научный руководитель

Демина Дарья Аркадьевна — кандидат педагогических наук, доцент, директор Центра поддержки инклюзивного образования Московского государственного лингвистического университета (Россия, Москва)
E-mail: d.a.demina@linguanet.ru

About the author

Mark I. Grokhovskii —3nd year student
(Bachelor's degree)
Moscow State Linguistic University
(Russia, Moscow)
E-mail: markgrokhovskii@gmail.com

Scientific supervisor

Darya A. Demina — Candidate of Pedagogical Sciences, Associate Professor, Director of the Center for Inclusive Education Support at Moscow State Linguistic University (Moscow, Russia)
E-mail: d.a.demina@linguanet.ru

УДК 004.82+81`221.2

ЦИФРОВИЗАЦИЯ ПЕРЕВОДА ЖЕСТОВОГО ЯЗЫКА

Батракова С. В.
Московский государственный лингвистический университет
(Россия, Москва)
batsvik@mail.ru

Веденеева М. В.
Московский государственный лингвистический университет
(Россия, Москва)
mvvedeneeva@mail.ru

Научный руководитель:
Толстых М. Ю.
Московский государственный лингвистический университет (Россия, Москва);
Московский университет МВД России им. В. Я. Кикотя (Россия, Москва)
marina_lion@mail.ru

Аннотация
В статье выполнен ретроспективный анализ средств перевода в области русского жестового языка, а также обзор современных цифровых технологий, ресурсов и их инструментария в части перевода с жестового языка и на него. Характеристика сопровождается примерами с иллюстрацией технологий. В заключении приведены гипотезы о векторах развития процессов цифровой трансформации в сфере жестового языка.

Ключевые слова: цифровая трансформация, информационные технологии, перевод, жестовый язык, лингвистика

DIGITALIZATION OF SIGN LANGUAGE TRANSLATION

Svetlana V. Batrakova
Moscow State Linguistic University (Russia, Moscow)
batsvik@mail.ru

Maria V. Vedeneeva
Moscow State Linguistic University (Russia, Moscow)
mvvedeneeva@mail.ru
Scientific supervisor:

Marina Yu. Tolstykh
Moscow State Linguistic University (Russia, Moscow);
Vladimir Kikot Moscow University of the Ministry of Internal Affairs of Russia (Russia, Moscow)
marina_lion@mail.ru

Abstract
The article provides a retrospective analysis of translation tools in the field of Russian sign language, as well as an overview of modern digital technologies, resources and their tools in terms of translation from and into sign language. The description is accompanied by examples illustrating the technologies. In conclusion, hypotheses about the vectors of development of digital transformation processes in the field of sign language are presented.

Keywords: digital transformation, information technology, translation, sign language, linguistics

Первый разработанный курс переводчиков русского жестового языка (РЖЯ) появился лишь в 1960-е годы, благодаря колоссальной работе основателя и руководителя Ленинградского восстановительного центра для лиц с нарушениями слуха И. Ф. Гейльмана. Разумеется, первые переводчики появились ранее: часто и сегодня переводчиками жестового языка становятся слышащие дети глухих родителей (children of deaf adults, CODA). Однако, если рассуждать именно о первом организованном курсе, то важно понимать, что, когда отсутствовали компьютеры и книги по теории языка, в распоряжении имелись лишь бумажные словари, а число носителей языка, у которых можно уточнить тот или иной жест, было критически мало.

Ранее в словарях было либо описание жеста, либо схематическая его рисовка, отсутствовала как таковая система записи, поэтому понять, как должен показываться жест, было крайне сложно (Рисунок 1).

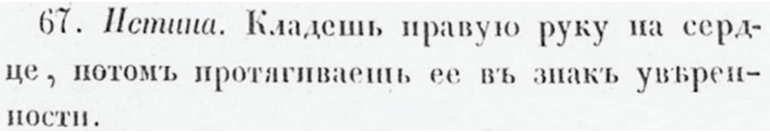
67. *Истина.* Кладешь правую руку на сердце, потомъ протягиваешь ее въ знакъ увѣренности.

Рисунок 1. Пример перевода из книги 1835 года Виктора Флери

Словарь Гейльмана 1957 года стал по сравнению с предыдущими источниками куда более систематизирован и понятен: структурно схож с советским толковым словарем, а также содержал фото (Рисунок 2).

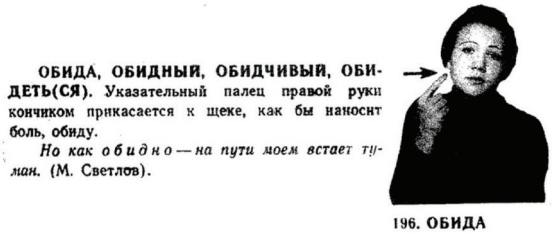

Рисунок 2. Пример перевода из словаря 1957 года Иосифа Гейльмана

Появление компьютеров изначально не облегчило задачу переводчикам: в девяностые и двухтысячные изучение РЖЯ не было приоритетом. Однако, если сравнивать с шестидесятыми, то можно уверенно отметить скачок вперед в развитии РЖЯ по ряду оснований.

Во-первых, появление качественных веб-камер позволило переводить речь дистанционно. Например, в последние несколько лет на вокзалах начали появляться стойки информации [1], с помощью которых глухие могут получить помощь на родном языке (Рисунок 3): на самом вокзале может физически и не быть сотрудника, знающего РЖЯ, но в наличии будут доступны камера и интернет-соединение, чего весьма достаточно для коммуникации.

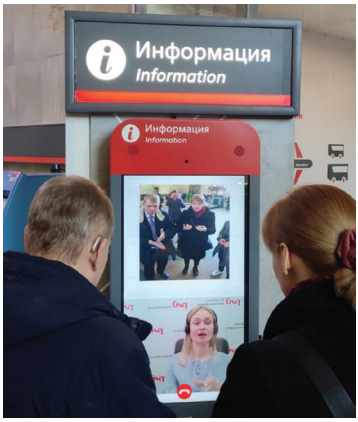

Рисунок 3. Информационный терминал на РЖЯ

Во-вторых, цифровая трансформация в текущих процессах осуществляется и в отношении словарей, что сильно помогает специалистам в данной области, потому что бумажные словари просто неудобны для использования, особенно для жестовых языков.

Наиболее популярный и используемый современный словарь — spreadthesign (рисунок 4) [2]. Как отмечают специалисты, он максимально удобный в использовании, однако не единственный. В 2019 году был разработан агрегатор словарей РЖЯ, в котором поиск ведётся сразу по всем

имеющимся в базе словарям [3]. При этом, интерфейс сервиса трудно назвать «дружественным», но качество перевода весьма высокое (рисунок 5).

В-третьих, интеграция сервисов машинного перевода. На данный момент жестовикам доступен лишь переводчик с русского на РЖЯ, но для обратного перевода цифровые ресурсы не разработаны, либо не являются общедоступными. В интернете размещен «Компьютерный переводчик на русский жестовый язык» (рисунок 6) [4]. Такое название заявлено разработчиками, вместе с тем ввести фразу и получить перевод на данном сервисе нельзя.

По нашему мнению, это очередной словарь, при чем не весьма достоверный: не всегда с первого раза открывается вкладка «Категории»; сервис заявлен как словарь слов и популярных фраз, но число словосочетаний в базе очень мало; изображение аватара не передаёт эмоции, а мимика, как известно, является принципиальной составляющей жестового языка.

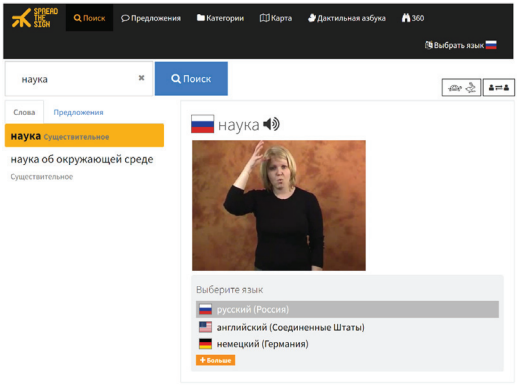

Рисунок 4. Интерфейс словаря spreadthesign

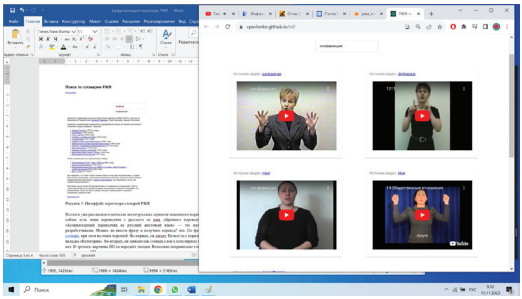

Рисунок 5. Интерфейс агрегатора словарей РЖЯ

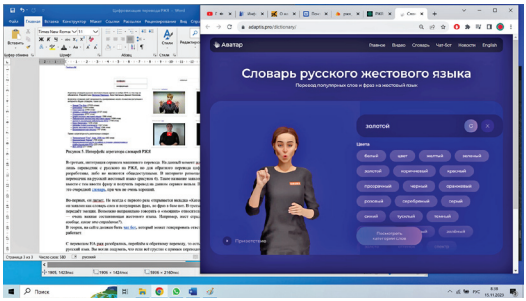

Рисунок 6. Интерфейс приложения «Аватар РЖЯ»

Относительно обратного перевода, то есть трансформации текста с РЖЯ на русский язык, важно упомянуть о появившейся примерно год назад новости [5] о том, что ученик московской школы создал первый прототип перчатки (рисунок 7), которая распознает жестовый язык.

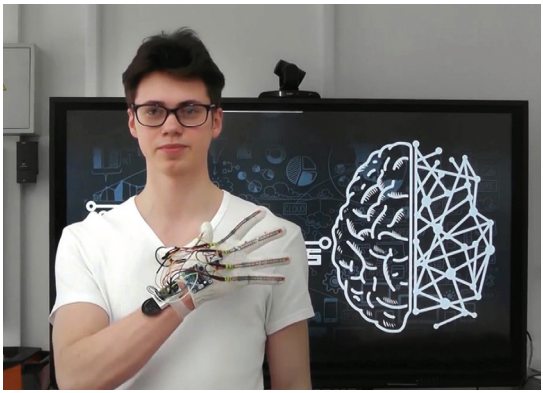

Рисунок 7. Данила Фоминиченко и разработанная им сурдоперчатка

Технология работы устройства заключается в следующем. К перчатке монтируются датчики сгиба, положения в пространстве, динамик и контроллер. С помощью специального программного обеспечения изобретение распознает некоторые жесты и по беспроводной связи Bluetooth транслирует (отображает и озвучивает) на смартфоне перевод жеста на русский язык.

Таким образом, можно заключить о том, что в сфере РЖЯ также происходит цифровая трансформация основных процессов профессиональной переводческой деятельности. В качестве перспективных направлений развития можно отметить следующие: формирование качественного корпуса РЖЯ, улучшение функционала и инструментария онлайн-словарей (поиск по конфигурации или локализации), создание общедоступных переводчиков с РЖЯ.

Список источников

1. Информация на РЖЯ на вокзалах России / Общероссийская общественная организация инвалидов «Всероссийское общество глухих» (ВОГ). 04 апреля 2022 г. [Электронный ресурс] // URL: https://voginfo.ru/society/2022/04/04/informacija-na-rzhja-na-vokzalah-rossii (дата обращения: 14.11.2023)

2. Spreadthesign. О нас / European Sign Language Center [Электронный ресурс] // URL: https://www.spreadthesign.com/ru.ru/about (дата обращения: 14.11.2023)

3. Поиск по словарям РЖЯ / Агрегатор словарей русского жестового языка. 2019. Разработчики: Виталий Павленко, Лиза Свитанько, Даниил Охлопков [Электронный ресурс] // URL: https://vpavlenko.github.io/rsl (дата обращения: 14.11.2023)

4. Компьютерный переводчик на русский жестовый язык / Аватар. Технологии и продукты для глухих и слабослышащих «Адаптис» [Электронный ресурс] // URL: https://adaptis.pro/ (дата обращения: 14.11.2023)

5. Московский школьник изобрел перчатку, озвучивающую язык жестов // Москвич Mag. 29.06.2022. [Электронный ресурс] // URL: https://moskvichmag.ru/gorod/moskovskij-shkolnik-izobrel-perchatku-ozvuchivayushhuyu-yazyk-zhestov (дата обращения: 14.11.2023)

Об авторах

Батракова Светлана Викторовна — студентка 3-го курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва)
E-mail: batsvik@mail.ru

Веденеева Мария Владиславовна — студентка 3-го курса (бакалавриат) Московского государственного лингвистического университета (Россия, Москва)
E-mail: mvvedeneeva@mail.ru

Научный руководитель

Толстых Марина Юрьевна — кандидат технических наук, доцент кафедры международной информационной безопасности Московского государственного лингвистического университета (Россия, Москва);
доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России им. В. Я. Кикотя (Россия, Москва)
E-mail: marina_lion@mail.ru

About the authors

Svetlana V. Batrakova —3nd year student (Bachelor's degree)
Moscow State Linguistic University (Russia, Moscow)
E-mail: batsvik@mail.ru

Maria V. Vedeneeva—3nd year student (Bachelor's degree)
Moscow State Linguistic University (Russia, Moscow)
E-mail: mvvedeneeva@mail.ru

Scientific supervisor

Marina Yu. Tolstykh — Candidate of Technical Sciences, Associate Professor of the Department of International Information Security at the Moscow State Linguistic University (Russia, Moscow);
Associate Professor of the Department of Special Information Technologies of the Educational and Scientific Complex of Information Technologies at the V. Ya. Kikot Moscow University of the Ministry of Internal Affairsof Russia (Russia, Moscow)
E-mail: marina_lion@mail.ru

УДК 37+130.3

РЕСТАВРАЦИЯ ЦЕННОСТНОЙ И ИДЕОЛОГИЧЕСКОЙ СОСТАВЛЯЮЩИХ ВОСПИТАТЕЛЬНОГО ПРОЦЕССА В ОТЕЧЕСТВЕННОМ ОБРАЗОВАНИИ

Коханая О. Е.
Московский гуманитарный университет
(Россия, Москва)
kokhanaya@mail.ru

Аннотация

В статье анализируется российская система гуманитарного образования и подготовки научно-преподавательских кадров, трансформацию механизмов коммуникации в учебной, научной деятельности и самоподготовке современных студентов российской высшей школы. Восстановление и обновление отечественной системы образования и воспитания как элемента национальной безопасности российского общества, идеологическая наполненность представляется крайне актуальным, что необходимо в краткосрочной перспективе как инструмент отстаивания традиционных духовно-ценностных координат нашего Отечества. Автору представляется важным возвращения авторитета в обществе и семье к личности учителя и преподавателя.

Ключевые слова: фундаментальные ценности, медиа-коммуникации, система образования, личность, учитель, преподаватель, научная работа студентов, нейросети, Болонская система,

RESTORATION OF THE VALUE SYSTEM AND IDEOLOGICAL COMPONENTS THE EDUCATIONAL PROCESS IN DOMESTIC EDUCATION

Olga E. Kokhanaya
Moscow University for the Humanities (Russia, Moscow)
kokhanaya@mail.ru

Abstract

The article analyzes the Russian system of humanitarian education and training of scientific and teaching staff, the transformation of communication mechanisms in educational, scientific activities and self-training of modern students of Russian higher education. The restoration and renewal of the national education and upbringing system as an element of the national security of Russian society, ideological fullness seems extremely relevant, which is necessary in the short term as a tool for defending the traditional spiritual and value coordinates of our Fatherland. The author considers it important to return the authority in society and the family to the personality of the teacher and the teacher.

Key words: fundamental values, media communications, education system, personality, teacher, teacher, scientific work of students, neural networks, Bologna system

Введение

В современном российском обществе нетрудно заметить пренебрежение традициями беспрекословного уважения к учителю, преподавателю, межпоколенный разрыв, даже где-то конфликт поколений. Этот культурный феномен современности доходчиво описан еще в 2010 году выдающимся российским педагогом, крупнейшим организатором киноклубного движения в Воронеже, доцентом Воронежского государственного университета Сталем Никаноровичем Пензиным (1932–2011) и его соавтором, исследователем Ю. А. Кульченко: «Причины геронтофобии (неуважения к старости) связаны с духом времени. Почтение к «преклонным летам» и «сединам» сменилось пренебрежением к старости. Сумасшедшие скорости обновления технологий, навыков, образа жизни обесценили в глазах большинства опыт и знания пожилых.

Господство принципа потребления и удовольствия неизбежно ведет к пренебрежительному отношению к старости, которая явно проигрывает молодежи в потребностях. Пожилой человек не может, да и не хочет придерживаться высокоскоростных стандартов в потреблении товаров, услуг, информации. Таким образом, старики, не способные следовать «молодежному образу жизни», не вправе рассчитывать на уважение» [1, с. 50]. Тем более, что одним из основных постулатов Болонской системы, которую внедряли в отечественное воспитание и образование два десятилетия, является тезис, что ребенок с двухлетнего возраста сам себе эксперт, он самодостаточен!

Избыточная формализация образовательного процесса

В данный момент российская научно-педагогическая школа похожа на русского богатыря, стоящего на развилке дорог. И важно выбрать единственно верный путь: у нас нет времени для ошибок [2, с. 85]. Когда нашим детям, подросткам враги звонят и вкрадчиво предлагают включить газовую плиту (чтобы руками доверчивого ребенка взорвать его же дом и его самого) или поджечь военкомат и т.п., и дети это совершают, очевидно, настала пора оторваться от бумаготворчества и перспективных планов по бесконечной реорганизации обучения обучающихся, читай, окончательного разрушения, отечественной высшей школы, и дать возможность преподавателям взглянуть вновь в глаза студентов, вернуть воспитательную составляющую деятельности педагога в школы и вузы!

Хотя, как мы видим, не только нашу кафедру журналистики Московского гуманитарного университета тревожит проблема нехватки высококвалифицированных преподавательских кадров в сфере высшего образования, а проще говоря, иссяк тот источник, который каким-то неведомым образом существовал последние четверть века, когда, подняв личные связи и приложив некоторые усилия, можно было найти педагога, профессионала, отлично знающего свой предмет, яркую личность, которая несомненно увлечет своими мыслями, творческими проектами, научными идеями студентов. Преподаватели, соответствующие высоким критериям традиционного российского, советского образования, теперь как-то не находятся. Новомодные термины «человеческий капитал», «человеческий ресурс» есть, а людей нет!

Похоже, количество ударов, нанесенных отечественной высшей школе, перешло в качество, с отрицательным результатом, естественно. Нищенские зарплаты преподавателей, соответственно, необходимость работать в нескольких местах или в одном вузе, но на полторы ставки (при объеме — только учебной нагрузки на одну ставку — 900 часов (!) для любой преподавательской должности), бесконечные изменения Федеральных государственных стандартов, переписывание по новым чиновничьим требованиям, не имеющих никакого отношения к реальному учебно-воспитательному процессу документов, ежегодно обновляемых: основных образовательных программ по каждому направлению и профилю подготовки, рецензий на них работодателей, учебных планов, учебно-методических комплексов по каждой дисциплине с новыми компетенциями и индикаторами по регулярно обновляемым вышестоящими организациями шаблонам, фондов оценочных средств и т.д., и т.п.

Тонны и тонны бумаг, иссушающих мозг, отупляющих и энергетически выхолащивающих каждого конкретного преподавателя, доцента, профессора, — это учебная работа!

А есть еще вторая обязательная половина нагрузки остепененного преподавателя высшей школы — научно-исследовательская работа, которая превратилась в гонку за индексом Хирша, количеством публикаций и цитирований; за публикациями в научных журналах, рецензируемых в российских и международных системах, а также необходимо обязательное участие с публикациями в международных и всероссийских научных конференциях, написание монографий, учебных пособий и т.п. При этом последние годы вузы на научной деятельности пытаются активно «зарабатывать»! То есть бедный, в буквальном смысле, профессор, доцент за участие в конференции и свою, авторскую публикацию еще и деньги свои собственные платит, чтобы выполнить некие индивидуальные рейтинговые показатели. Все эти длинные перечисления автор осуществил, не упоминая таких понятий, как студент и научный интерес. А именно они были самыми важными в советской, да и дореволюционной системе образования! С водой выплеснули ребенка…

К тому же и уважение в обществе к профессии педагога уже давно кануло в лету. Ходил он, голодный, оборванный в 1990-е годы (основная масса преподавателей в это время просто покинула профессию: ушла, куда глаза глядят, семьи кормить!), а потом обществу сообщили, что он и есть главный коррупционер. И куда в него только влезают букеты цветов и конфеты? Это в знак благодарности? Какой еще благодарности? Ничего этому коррупционеру не дарить! О фактах коррупции сообщать: на сайте каждого университета появился раздел о противодействии коррупции, нужные телефоны. Результат налицо.

Превращение морально-нравственных ориентиров в проблему

Когда при встрече Нового 2022 года кто-то остроумный запустил акцию: подарок чиновника высокого ранга остро нуждающемуся, больному школьнику, подростку, что транслировалось по федеральным каналам: из десятком «счастливчиков», с их самыми экзотическими, но исполненными «слугами народа» желаниями, только от одного мальчика (больного, которому устроили полет на вертолете) телезрители услышали «спасибо». От одного. Остальные детки с невозмутимым видом принимали как должное (из рук Президента РФ!), бесплатные — для всей семьи счастливчика — спектакль в Большом театре, экскурсию в Санкт-Петербург всей семьей и т.д. А ведь именно чувство благодарности, на мой взгляд, отличает человеческую личность от человеческой особи, от массового

человека, которому, как он абсолютно уверен, и так все обязаны! Разве душевная щедрость, благодарность измеряются букетиком цветочков?.. Не просчитывая морально-нравственные потери, вытравили в нашем Отечестве традиционное уважение к Учителю. А зря старались! Время и без того жестоко.

Массовые ценностные ориентации и установки, десятилетиями преподносимые аудитории медиа-профессионалами, видными представителями сетевой журналистики, политтехнологами через печатные, электронные СМИ и Internet-ресурсы, стирая традиционные национально-этнические и прочие различия индивидов и социальных групп, уже сформировали новый вид Homo sapiens — массового человека, который постепенно обезличивается, утрачивает самостоятельность, личностное начало. «Разрыв коммуникации, атомарность и дискретность сознания… разрушение социальных связей и традиционных форм коммуникации в современном обществе», — справедливо выделяет в качестве основных черт современного человека исследователь Т. В. Болдырева [3, с. 52].

«При этом социальная и духовная самоидентификация… выстраивается на основе обсуждения медийной повестки (того, о чем говорят в СМИ, рассказывают люди) и на основе пережитого опыта. По сути — это классическая схема самоидентификации через социальные коммуникации. Мы — то, о чем говорят другие люди, о чем пишут в медиа» [3, с. 53]. Психологическая зависимость массового сознания от, как правило, неподконтрольных ему информационных воздействий формирует у индивидуально-личностного сознания приверженность доминирующему общественному мнению, конформизм, инфантилизм, некритичность мышления.

В научном сообществе, в СМИ, в профильных министерствах активно обсуждается дипломная работа, точнее ВКР (надо же всё обезличить и обездушить аббревиатурами), студента РГГУ, которую он изготовил за сутки, применив возможности искусственного интеллекта, нейросеть ChatGPT [4]. К обсуждению прецедента на федеральных каналах подключились it-специалисты. Один из них, конечно, защищает студента, парируя журналистке на ее вопрос: «Когда-то нам учителя запрещали пользоваться калькуляторами. И где они сейчас, и где Я». Как не правы учителя, которые искренне хотели научить школьников складывать числа, вычитать в уме!

Сегодня задайте элементарный пример сложения двух чисел студентам: первый их жест — к мобильному телефону. А если этот порыв пресечь, то из 30 человек в группе, максимум один сможет дать ответ! То

есть эти поколения — легкая добыча любого нечистоплотного торговца, они ничего ни за кем не пересчитывают, не умеют! А уж если какая-то финансовая простейшая комбинация «по отъему денег у населения», например, в сетевом магазине «Пятерочка», так они ее никогда и не заподозрят, и обнаружить не смогут: математическая логика отсутствует. Но при этом, какое небрежное отношения к учителям: «где они, и где Я». Они всё там же: в неуважение общества, родителей и детей, соответственно, ведь родители сегодняшних школьников и студентов уже учились в 1990-е годы и позднее.

Молодых же преподавателей в высшей школе крайне мало, о чем свидетельствуют как существующие реалии, так и минимум защищенных кандидатских диссертаций за последние годы: например, если в 2011 году в РФ было защищено 22 827 кандидатских, то в 2020 году — 5 115, — эти впечатляющие данные прозвучали на Научном профессорском форуме «Научные исследования в современном мире: проблемы, тренды, перспективы» на площадке Российской академии образования (7 февраля 2023 года, организатор — Российское профессорское собрание) в докладе директора Департамента аттестации научных и научно-педагогических работников Министерства науки и высшего образования РФ С. И. Пахомова. Падение подготовки кандидатов наук для отечественной высшей школы за 9 лет в 4,5 раза. Это закономерный результат еще одного заграничного новшества: с 2013 года обучение в аспирантуре не предполагала на финале защиты диссертации.

Тогда зачем аспирантура вообще нужна, да еще, как правило, на платной основе? Даже если кто-то в эти годы диссертацию и написал, попробуй найти функционирующий диссовет, ведущую организацию, оппонентов — по новым требованиям! Пока вникаешь в требования конкретного диссовета, его уже закрыли… С 2022 года вновь защиту вернули, может, и диссоветов станет как-то побольше, но годы потеряны, интерес к научной деятельности у молодых исследователей угас. По нашему опросу, магистранты 2023 года выпуска (январь), защитив магистерские диссертации, категорически не хотят продолжать образование в аспирантуре. Они не собираются связывать жизнь с педагогической и научно-образовательной деятельностью. Кроме вышеперечисленных причин, надо отметить, что сами по себе гуманитарные научные исследования как бакалаврам, так и магистрам, в их критическом большинстве, не интересны.

Отложим в сторону нерешенную проблему, в чьи обязанности в высшей школе входит системная, кропотливая научная работа со студентами, выявление более одаренных, имеющий научный склад ума. Думается,

опять это отдано на откуп вымирающему поколению энтузиастов, бессеребренников. Но ведь была же выстроена именно система данного вида работы в вузах при советской власти!..

Девальвация ценностей авторского творчества

Обратимся к «всезнающей» системе «Антиплагиат», которой с первого курса пугают студентов. И на это есть основания. Если автор сам формулирует мысли, то система безапелляционно может выдать «перефразирование»: кого, чего, тебя ли самого из прошлого, твоё ли национальное происхождение (мне на днях выдала: «Украинский перефраз»!), но это определяется как плагиат! Если автор ВКР под руководством научного руководителя долго, методично, скрупулезно читает и анализирует исследования ведущих ученых по изучаемой теме, да еще по неопытности не всегда аккуратно ставит сноски, кавычки в своем тексте, это всё, возможно, будет плагиатом. То есть основная цель научного исследования — анализ авторитетных авторов по избранной теме и свои суждения на этот счет, может привести к скорбным последствиям: избыточный процент заимствований, плагиат.

И студенты не только, как выпускник РГГУ, используют нейросети, покупают готовые дипломные работы в Интернете, но и находят статьи на других языках по данной теме, а автопереводчик им эти тексты переводит, и т.п. Процент оригинальности по системе Антиплагиат 82–90%. Читать эти бездушные, обезличенные, подчас бессмысленные тексты невозможно, прибавления научного знания — ноль. Изучение выпускником вуза фундаментального научного наследия по теме отсутствует. Правда, мелькают в тексте дипломной работы какие-то малоизвестные исследователи со случайными цитатами, но это подобрал, как мы теперь понимаем, искусственный интеллект случайным методом подбора.

Далее, когда магистрант, вчерашний бакалавр, пишет обязательную научную статью для конференции, научный руководитель видит, что это односложные предложения уровня шестого класса средней школы, с множеством грамматических и пунктуационных ошибок, наивно-примитивного содержания и практически отсутствующими списком научной литературы и цитированием ученых. Если даже фамилии известных ученых по данной теме упомянуты, то после одного-двух вопросов научный руководитель понимает, что студент этот источник не читал. Дипломники, как правило, по нашему опыту, даже не считают нужным прочитать хотя бы одну научную статью научного руководителя. Естественно, если человек не увлечен научным исследованием, но в дальнейшем он этим заниматься не будет.

Можно возразить: а как же выполнение студентами во время обучения рефератов, курсовых работ? А самостоятельная работа студента по заданиям, прописанным преподавателем, по списку обязательной и дополнительной литературы по каждой дисциплине? Всё происходит там же: в интернет-пространстве.

Изначально Интернет предполагался как огромная библиотека с качественной, научной информацией, охватывающей все времена и народы. Возможность упрощённого изучения предметов мирового искусства (музыки, литературы, полотен великих мастеров), научной литературы и безграничного общения привлекает своей функциональностью (электронные библиотеки, электронная почта, электронный бизнес, СМИ, социальные сети, блоги) [5, с. 393], интерактивностью, свободным управлением информацией, согласно духовным и интеллектуальным потребностям массовой аудитории. Но где существует возможность для роста, развития и получения знаний, неминуемо найдется место опасности, обману, психологическим манипуляциям.

Обилие некачественной информации в Интернете способствует дезинформации, которая происходит при «переадресации сведений, не с помощью ссылки-переноса, а в виде свободного пересказа» [6, с. 90]. Этот вариант дезинформации схож со слухами, сплетнями или так называемым «сарафанным радио», когда часть информации не доходит до получателя в своём первоначальном виде, теряет основную суть, приобретает новые оттенки. Кроме того, в сети часто используется «прием «передергивания» — смещение акцентов при подаче новости, чтобы привлечь больше внимания» [6, с. 90] к информационным материалам. Посредством манипулятивных технологий, из-за потребления неполной, некачественной информации, вырванной из контекста, массовая аудитория, к которой относятся и наши студенты образца Болонской системы, не имеющая представления о реальной, целостной картине мира, конкретного явления или события, хватается за случайно найденные ею обрывки действительности, не всегда подлинные данные и, следовательно, строит неправильное суждение о происходящем.

Материал, представленный в Интернете, зачастую не проверенный и не правдивый, так как многие источники информации в виртуальном пространстве не являются официальными изданиями, не несут ответственности за распространение какой-либо информации. Таким образом, разнообразная псевдонаучность сообществ, проектов, авторских постов в социальных сетях порождает усредненный тип студента, потребителя информации, которую он при отсутствии начальных знаний по предмету проверить не в состоянии. Обязательная учебная литература,

указанная преподавателем дисциплины, как и уважение к преподавателю, также не является императивом. То есть подчас студенты читают совсем не те учебники (всевозможных открытых обществ, фондов, например, Сороса), ими используются публичные страницы, блоги, аккаунты в социальной сети, видеохостинги, «Википедия», всевозможные «эксперты» в интернет-среде: разве они не могут заменить, реального преподавателя? Правда, пандемия ковида-19 многим доказала, что живое человеческое общение, обмен эмоциями с педагогом — это величайшая роскошь, которую мы недооценивали ранее, но процесс расчеловечивания личности преподавателя запущен давно, как минимум с 2003 года, когда российское высшее образование перешло на Болонскую систему обучения.

Задача реставрации идеологии воспитательной работы

Таким образом, посредством легкого нахождения необходимых материалов для докладов, рефератов, курсовых работ вырабатывается пассивность в получении знаний, инфантильность, студент не считает нужным самостоятельно изучать, анализировать какую-либо информацию, запоминать и в последствии творчески, ответственно использовать ее в жизни, так как у него сложилось твердое убеждение, что он всегда может открыть нужный сайт или всем широко известную Википедию, сервер которой был безвозмездно предоставлен компанией Bomis, основанной в 1996 году и расположенной в Сан-Диего, штат Калифорния.

Насколько информация Википедии, в принципе, требующая дополнительной проверки, соответствует национальным интересам нашей страны, вопрос риторический. Помимо этого, непрерывный контакт с интернет-ресурсами подчас вызывает у молодого поколения безоговорочное доверие к информации, развивается психологическая зависимость от интернет-среды. Таким образом, потребление массовой информации в интернет-пространстве предполагает превращение сознания — одной из самых главных тайн человечества, — в объект слива информационных отходов.

Высокой степенью эффективности в распространении массовой культуры обладают и различные поучающие и мотивирующие тренинги на просторах социальных сетей, которыми увлеклись наши студенты в годы пандемии, находясь на дистанционном обучении. Видео-уроки характера «Как стать лидером в своей жизни» [7] или «10 простых методов саморазвития» [8] содержат в себе различные рекомендации того, как надо строить свою жизнь. Довольно часто в них проповедуются мысли о том, что надо быть жёстче с окружающими людьми, добиваться успехов в ка-

рьерном росте, желаемой должности любой ценой, лавировать в отношениях с начальством и т.д. Такие рекомендации укореняют в сознании массовой аудитории культ успешности любой ценой, богатства, славы и достатка вне зависимости от моральных принципов [9].

Из этого следует, что новые медиа сегодня являются самым эффективным инструментом информационно-психологического воздействия на молодое поколение и активным популяризатором массовой культуры. Посредством их влияния происходит внедрение в российский менталитет западных принципов и моделей поведения: индивидуализма, эгоцентризма, инфантильности, прокрастинации и др. Культивируются — комфорт, гедонизм, значимость денег, достатка, благосостояния, успеха и славы. При этом умаляются традиционные ценности — родины, семьи, образования, развития интеллектуальных способностей, свободы, чести, пользы труда и т.д.

Первые шаги в сторону возвращения идеологических, ценностных скреп нашего государства и общества делаются, но ведь важно, как и кем! Для примера: теперь утром в московских школах исполняется по понедельникам гимн и поднимается российский флаг. Идея прекрасная. Но в некоторых школах дети приходят в этот день на 15 минут раньше. Казалось бы мелочь! Но ранним утром в понедельник расписание жизни всей семьи, работающих родителей, полусонного школьника сбивается на 15 минут. И подсознательно возникает раздражение, недовольство, возмущение…

Любая хорошая идея может быть погублена бесчувственностью, бездарностью исполнителя. «Хотелось, как лучше, а получилось, как всегда», — вспоминаются слова незабвенного В. С. Черномырдина. Пока мы не вернем в отечественную высшую школу фундаментальные дисциплины в приемлемых объемах (философия, эстетика, этика, литература, современный русский язык и т.п.), благодаря которым человек способен научиться самостоятельно анализировать, чувствовать, мыслить, некому будет воспитывать новые поколения граждан, искренне любящих свою землю, природу, семью, Родину.

Заключение

Должен быть остановлен длительный процесс «разрушения системы традиционных ценностей и механизмов социализации поколений, «активного навязывании российскому обществу западных ценностей, означающего попытку духовного покорения России «мирным» путем» [10, с. 232], в том числе под видом «улучшения человека» глобальным

картелем FAGMA (Facebook, Apple, Google, Microsoft) [11, с. 48], а также нанесения военного поражения нашей Родине странами НАТО. Пришло время перехвата инициативы западных «благожелателей», десятилетиями формирующих у россиян чуждые нашему обществу ценностные ориентиры, пришло время возрождения России, как птицы Феникс из пепла, посредством возвращения к принципам фундаментальности отечественного образования в лучших его традициях, а именно подготовки и воспитания не только профессионала, но и личности, имеющей широкие знания, взгляд исследователя и творца, морально-нравственную устойчивость патриота и гражданина, что невозможно без возвращения уважительного, бережного отношения к личности Учителя, преподавателя, педагога, наставника и крайне необходимо российскому народу на пути к справедливому мироустройству.

Список источников

1. Пензин С. Н., Кульченко Ю. А. Уроки воспитания // Вестник Воронежского государственного университета. Серия: Проблемы высшего образования. 2010. № 1. С. 45–52.

2. Головин Ю. А., Коханая О. Е. Формирование нового медиапространства в эпоху социальных и технологических трансформаций // Челябинский гуманитарий. 2020. № 2 (51). С. 81–88.

3. Болдырева Т. В. Новая театральность в эпоху медиатизации // Сфера культуры. 2023. № 2 (12). С. 48–56.

4. Абрамов А. Нейросеть за один вечер написала диплом за российского студента. Преподаватели в шоке — как теперь проверять знания? [Электронный ресурс] // Комсомольская правда. 2023. 1 февраля. URL: https://www.msk.kp.ru/daily/27460/4714947 (дата обращения: 12.12.2023).

5. Акимова Е. М. Информационная безопасность личности в контексте технологических и социокультурных изменений // Высшее образование для XXI века: роль гуманитарного образования в контексте технологических и социокультурных изменений: XV Международная научная конференция. Доклады и материалы: в 2 ч. Ч. 1. / под общ. ред. И. М. Ильинского. Москва, 2019. С. 392–398.

6. Акимова Е. М. Современные тенденции медиаобразования в эпоху цифровизации и манипулирования сознанием личности // Высшее образование для XXI века: роль гуманитарного образования в контексте технологических и социокультурных изменений: XV Международная научная конференция. Доклады и материалы: в 2 ч. Ч. 1. / под общ. ред. И. М. Ильинского. Москва, 2019. С. 85–92.

7. Хакамада И. Эксклюзив [Электронный ресурс] // YouTube. 2016. 02 июля. URL: https://youtu.be/LunNI09QuA4 (дата обращения: 26.05.2022).

8. 1000 секретов силы. 10 простых методов саморазвития [Электронный ресурс] // YouTube. 2022. 04 августа. URL: https://youtu.be/oBeeEzuxO9I (дата обращения: 12.12.2023).

9. Смеюха В. В. Социальные сети: этические проблемы коммуникации // Реклама и связи с общественностью: традиции и новации: материалы Седьмой Международной научно-практической конференции (Ростов-на-Дону, 11–13 сентября 2019). Ростов-на-Дону, 2019. С. 52–59.

10. Ильинский И. М. Образование, молодёжь, человек(статьи, интервью, выступления). Москва: Издательство Московского гуманитарного университета, 2006. 560 с.

11. Былевский П. Г. Культуроцентричный подход к развитию способностей как альтернатива «техноцентричному» трансгуманизму // Вестник Московского государственного университета культуры и искусств. 2023. № 1(111). С. 41–49. DOI 10.24412/1997–0803–2023–1111–41–49. EDN QPBYVK

Об авторе

Коханая Ольга Евгеньевна —
доктор культурологии,
кандидат философских наук,
доцент, профессор кафедры
журналистики Московского
гуманитарного университета
(Россия, Москва)
E-mail: kokhanaya@mail.ru

About the author

Olga E. Kokhanaya —
Doctor of Cultural Studies,
Candidate of Philosophical Sciences,
Associate Professor, Professor
of the Department of Journalism
at Moscow University for the Humanities
(Russia, Moscow)
E-mail: kokhanaya@mail.ru.

УДК 008

КОРИФЕЙ РОССИЙСКОЙ КУЛЬТУРОЛОГИИ: 100-ЛЕТНИЙ ЮБИЛЕЙ С. П. МАМОНТОВА

Кириллов И. А.
Московский государственный лингвистический университет
(Россия, Москва)
I. A. Kirillov@gmail.com

Аннотация

В статье рассматриваются основные этапы жизненного пути культуролога, историка, лингвиста, переводчика, замечательного человека и патриота Степана Петровича Мамонтова (1923–2001). Приводятся интересные факты его биографии, а также достижения в области науки, литературы и культуры.

Ключевые слова: Степан Петрович Мамонтов, лингвистика, культурология, переводческая деятельность, межкультурные коммуникации, МГЛУ

THE LUMINARY OF RUSSIAN CULTURAL STUDIES: THE 100TH ANNIVERSARY OF STEPAN P. MAMONTOV

Igor A. Kirillov
Moscow State Linguistic University (Moscow, Russia)
I. A. Kirillov@gmail.com

Abstract

The article examines the main stages of the life path of the culturologist, historian, linguist, translator, remarkable man and patriot Stepan Petrovich Mamontov (1923–2001). Interesting facts of his biography are presented, as well as achievements in the field of science, literature and culture.

Key words: Stepan P. Mamontov, linguistics, cultural studies, translation activities, intercultural communications, MSLU

Светлой памяти
Степана Петровича Мамонтова
посвящается

20 сентября 2023 года исполнилось 100 лет со дня рождения Степана Петровича Мамонтова культуролога, историка, лингвиста, переводчика и, более того, замечательного человека и патриота. Степан Петрович родился в Москве в семье, сохранявшей свои глубокие исторические корни. По семейным преданиям, среди предков Степана Петровича по мужской линии было большое количество воинов, защитников Отечества. Один из пращуров, прапрадед Степана Петровича за храбрость и боевые заслуги в Отечественной войне 1812 года получил офицерский чин и дворянское звание. А уже дед, в звании подполковника артиллерии, участвовал во взятии и беспримерной обороне Шипкинского перевала, сыгравшей огромную роль в победоносной русско-турецкой войне 1877–1878 годов.

Школьные годы Степана Петровича связаны со школой-коммуной № 32 имени Пантелеймона Лепешинского (2-й Обыденский переулок, д. 9). В 1930-е годы здесь учились многие в будущем известные люди (летчик-испытатель Степан Микоян, ученый-физик Сергей Капица, писатель Анатолий Рыбаков и многие другие).

Уже в школьные годы проявился талант Степана Петровича к изучению иностранных языков. Началось с того, что мать одного из его друзей, этническая немка и преподавательница немецкого языка, стала проводить с ним регулярные дополнительные занятия. Так, что к окончанию школы в 1941 году Степан Петрович уже в совершенстве владел немецким языком.

С началом Великой Отечественной войны и вплоть до мая 1945 года Степан Петрович — военный переводчик в действующей армии. Конкретно, это 4-я Ударная Армия, которая в разные периоды времени входила в состав Калининского, 1-го Прибалтийского, 2-го Прибалтийского и Ленинградского фронтов.

На войне военный переводчик должен был не только владеть языком противника, но и знать тактику врага, свободно разбираться в трофейной документации и оружие, добывать из открытых радиопереговоров противника важные сведения, вести пропагандистские передачи с передовой линии фронта, при необходимости быть парламентером. И, конечно, пробираться на сторону врага, чтобы взять в плен «языка». Таким об-

разом, военные переводчики, как правило, служили в разведывательных подразделениях.

За героизм и отвагу проявленные в Великой Отечественной войне Степан Петрович был награжден двумя Орденами Отечественной войны, Орденом Красной Звезды, медалями «За отвагу» и «За боевые заслуги». Последнее полученное им воинское звание было звание полковника вооруженных сил Российской Федерации.

Окончание Великой Отечественной войны он встретил в Либаве — городе на юго-западе Латвии, на побережье Балтийского моря (ныне Лиепая). В письме своей маме из Либавы от 10 мая 1945 года он писал: «Наконец-то закончилась эта мировая вакханалия. Ликование было большое. Теперь, видно, будет вскоре решаться участь многих офицеров, остаться или не остаться в армии. Я могу остаться и останусь, лишь при одном условии: только учиться и учиться в Москве во ВИИЯКе (Военный институт иностранных языков). Если нет, то приложу все силы, чтобы уйти на гражданскую работу. Как ты оцениваешь эти мои рассуждения? Я сейчас очень нуждаюсь в твоём совете по жизненным вопросам. Пиши. Привет всем. Всем… Стёпа».

В итоге, выбор был сделан, по окончании войны Степан Петрович Мамонтов стал слушателем Института иностранных языков Советской Армии. В добавок к немецкому он изучает испанский и французский языки. В 1951 году он заканчивает институт и поступает в адъюнктуру ВИИЯ. Его научные изыскания были посвящены проблемам риторики испанского языка, точнее проблеме построения испанской художественной речи. Теоретическая разработка этой проблемы привела его к защите диссертации кандидата филологических наук. Практическая реализация — способствовала тому, что одним из основных направлений для творческой натуры Степана Петровича в этот период становится переводческая и литературоведческая деятельность.

Он много переводит с испанского языка латиноамериканских авторов, и прежде всего Уругвайского писателя, мастера креольского фантастического реализма и короткой прозы Орасио Кирогу. Книга Орасио Кироги (Horacio Quiroga) «Сказки сельвы» (Cuentos de la selva), подавляющее большинство переводов которой были выполнены Степаном Петровичем, увидела свет в 1956 году. Им же была подготовлена и вступительная статья к этому изданию [1]. Общий тираж этой книги изданной Гослитиздатом в 1956 и 1957 году составил 690 000 экземпляров [2]. Эта книга неоднократно переиздавалась и позже: в 1982, 2012 и 2023 годах.

Орасио Сильвестре Кирога Фортеса (1878–1938) признанный классик латиноамериканской литературы. Сказки сельвы (1918) — единственная

детская книга писателя, написанная для детей в маленьком доме посреди бескрайней сельвы, в отдалённой провинции Аргентины [3].

Параллельно с литературно-переводческой деятельностью с 1954 по 1956 год Степан Петрович занимается преподавательской деятельностью. Он служит в должности преподавателя испанского языка кафедры романских языков Военного института иностранных языков.

С 1956 года Степан Петрович становится штатным переводчиком и редактором Гослитиздата (Государственное издательство художественной литературы).

В 1960 году свет увидела очередная переведенная на русский язык книга Орасио Кироги «Анаконда» с предисловием и переводами С. П. Мамонтова.

Вот что писал в предисловии к этой книге Степан Петрович: «Среди писателей Латинской Америки Орасио Кирога — один из наиболее своеобразных и выдающихся мастеров рассказа. Уругваец по рождению и подданству, он прожил почти всю свою жизнь в Аргентине и принадлежал к талантливому поколению писателей, которых выдвинула латиноамериканская литература первой четверти XX века.» [4]. 1960-е годы — удивительное время для нашей страны и всего мира. Юрий Алексеевич Гагарин летит в космос, в прессе идут битвы между «физиками» и «лириками», завершающиеся компромиссом между наукой и искусством. Это годы освободительных движений во всем мире в Африке (1960 год объявлен ООН Годом Африки) и Латинской Америке.

В 1962 году Гослитиздатом издается — первая книга из уникальной серии “Библиотека латиноамериканской поэзии”. Одним из организаторов выпуска этой серии книг явился С. Мамонтов. Эта серия содержала 25 замечательных книг латиноамериканских поэтов. Выпуск книг продлился до 1991 года, и бессменным членом редколлегии был Степан Петрович. 5 февраля 1960 года решением правительства СССР для оказания помощи освободившимся странам (бывшим колониям) в подготовке национальных квалифицированных кадров был учрежден Российский университет дружбы народов им. Патриса Лумумбы.

И не было ничего странного, что Степан Петрович был приглашен в создаваемый университет. Вот что вспоминает его сын, Александр Степанович Мамонтов, советский и российский учёный и преподаватель, доктор филологических наук, профессор, почётный работник высшего профессионального образования РФ, член Экспертного совета ВАК РФ:

«В Университете дружбы народов Степан Петрович работал с 1960 года и имел служебное удостоверение с № 1. Сначала в качестве ученого секретаря по странам Латинской Америки Отдела информации

и приема, позже был избран деканом историко-филологического факультета. За плодотворную работу неоднократно был отмечен почетными грамотами Ректората и награжден медалями Университета».

Этот период биографии Степана Петровича сохранился в воспоминаниях Михаила Викторовича Горбаневского, окончившего московскую языковую спецшколу с преподаванием испанского языка в 1970 году и поступившего на историко-филологический факультет Университета дружбы народов имени Патриса Лумумбы.

На всю жизнь Михаил Викторович запомнил вступительное собеседование с деканом историко-филологического факультета РУДН Степаном Петровичем Мамонтовым. Возможно, именно влияние этих воспоминаний и дальнейшего общения с таким замечательным человеком и ученым способствовало выбору жизненного пути сначала абитуриенту, а потом и студенту, в результате которого Михаил Викторович сам стал крупным лингвистом, историком и культурологом.

Михаил Викторович Горбаневский — советский и российский лингвист; специалист по проблемам общей и русской ономастики, лексикологии, судебных лингвистических экспертиз, славяноведения и культуры речи, русского языка в компьютерных технологиях. Доктор филологических наук, профессор кафедры общего и русского языкознания Российского университета дружбы народов. Председатель правления Гильдии лингвистов-экспертов по документационным и информационным спорам, вице-президент Общества любителей российской словесности.

В 1972 году Степан Петрович защитил докторскую диссертацию по испаноязычной литературе Латинской Америки. Он продолжает совмещать литературную, педагогическую и административную деятельность.

В 1975 году в рамках двухсот томного проекта «Библиотека всемирной литературы» выходит в свет Антология — «Поэзия Латинской Америки». Среди переводчиков с испанского, подготовивших к изданию эту книгу, был и доктор филологии, профессор, декан историко-филологического факультета РУДН Степан Петрович Мамонтов [5].

И вдруг, в том же 1975 году и вплоть до 1979 года он становится советником по культуре Посольства СССР в Португалии?

25 апреля 1974 года в Португалии произошла, так называемая, «Революция гвоздик», которая победила быстро и почти бескровно. Режим диктатора Салазара пал. Нашу страну диктатор Салазар считал злейшим врагом и не поддерживал с ней даже формальные отношения.

9 июня 1974 года в Лиссабоне и Москве было опубликовано совместное коммюнике об установлении дипломатических отношений между

Португалией и СССР. Отношения эти были разорваны еще в 1918 году. До конца 1974 года в Москве побывало несколько официальных португальских делегаций. В декабре было подписано торговое соглашение, а также соглашения о воздушном сообщении и морском судоходстве.

В Советском Союзе до конца его существования свержение режима Салазара считалось главным событием многовековой португальской истории и одним из крупнейших событий всемирной истории XX века.

Обстановка вокруг Португалии накалялась. И СССР, и США стремились взять под свой контроль ход событий в Португалии. В ноябре США назначили нового посла, который прибыл в Лиссабон в январе 1975 года и первым делом сменил весь дипломатический состав посольства. Советский Союз так же предпринял ряд шагов по усилению своего влияния в Португалии [6].

В связи со сказанным выше, назначение советником по культуре Посольства СССР в Португалии в 1975 году доктора филологии, профессора, лингвиста, знатока истории и культуры Иберийского полуострова Степан Петрович Мамонтов, становится не только понятным, но, возможно, и наилучшим решением.

Анатолий Апостолов (Анатолий Геннадьевич Апостолов — русский писатель —прозаик, поэт и публицист, академик Международной Кирилло-Мефодиевской академии славянского просвещения) в своей статье «Помним и чтим культуролога Мамонтова» приводит следующие воспоминания, связанные с «португальским периодом» биографии Степана Петровича [7]:

«О чём бы мы с ним ни говорили, всё носило характер и дух научного исследования, с его методом сравнительного исторического анализа и человеко-сущностным подходом.

История возникновения древней Лузитании непременно сопровождалась у него историей Симферополя времён изгнанника Овидия. Время централизации древле вятских поселений Мосха в славное городище Кучково он хронологически сопрягал с временем возникновения графства Портукале (ныне — Португалия), которое испанский король Альфонс VI пожаловал в 1095 году рыцарю Генриху Бургундскому, мужу своей внебрачной дочери Терезы.»

С 1979 по 1983 год Степан Петрович профессор кафедры общественной психологии Института общественных наук (ИОН). ИОН был основан в 1962 году. Институт являлся высшим учебным и научно-исследовательским заведением ЦК КПСС.

Институт готовил кадры для национально-освободительных движений в том числе, находившихся на нелегальном положении.

Основная цель создания ИОН заключалась в поисках эффективных способов влияния на коммунистические и рабочие движения развивающихся стран в после-коминтерновский период. Как правило, преподаватели института владели необходимыми иностранными языками.

Потребность в творчески мыслящих сотрудниках была обусловлена острыми дискуссиями, развернувшимися к началу 1970-х годов в левом движении с одной стороны, а с другой стороны с леворадикалами, создавшими в Латинской Америке коммунистические организации, ориентировавшиеся не столько на Москву, сколько на Гавану [8].

И на работе в ИОН Степан Петрович был как нельзя кстати: ветеран Великой Отечественной войны, Патриот, знаток языков и культур Латинской Америки, культуролог, мудрый и знающий человек.

С 1983 по 1990 год он заведующий отделом стран Латинской Америки и Карибского бассейна международного журнала «Проблемы мира и социализма» в Праге.

В редколлегию журнала входили представители КПСС, всех других правящих братских партий, а также крупнейших компартий мира — итальянской и французской.

Со стороны СССР курировал журнал международный отдел ЦК КПСС, Кадры подбирало руководство отдела на самом высоком уровне.

На страницах журнала высказывались различные точки зрения по самым актуальным мировоззренческим проблемам. Можно утверждать, что в публикуемых материалах преобладало искреннее желание действительно разрешить проблемы мира и социализма.

В лучшие свои годы журнал издавался на 28 языках и распространялся более чем в 100 странах тиражом около 600 тысяч экземпляров

К глубоким познаниям Степана Петровича истории, культуры и литературы ибер-американских стран семь лет работы в Праге добавили поистине глобальное видение цивилизационного развития.

Автору данной статьи, в определенном культурологическом смысле, кажутся символичными, услышанные в 90 годы от Степана Петровича воспоминания, связанные с чешским королем Рудольфом II (1552–1612).

Рудольф II был сыном и преемником императора Священной Римской империи, чешского и венгерского короля Максимилиана II, а также двоюродным братом испанского короля Филиппа II. Он вырос в Мадриде и получил строгое католическое образование. Но по-настоящему он любил Пражский град (старинную крепость на высоком берегу Влтавы), поистине европейский культурный центр, являвшийся резиденцией императоров Священной Римской империи. Вокруг себя Рудольф II собирал художников и учёных. Учёные-естествоиспытатели, среди которых

выдающийся Иоганн Кеплер, трудились при дворе Рудольфа, поражая современников своими феноменальными открытиями.

В 1619 году Иоганн Кеплер публикует книгу «Гармония мира», в которой наряду с ценнейшими научными открытиями, изложены также философские рассуждения о «музыке сфер» и платоновых телах составляющие, по мнению учёного, эстетическую суть высшего проекта мироздания [9]. Подобного рода философско-культурологические рассуждения во многом могли быть присущи и самому Степану Петровичу.

С 1990 года судьба связывает Степана Петровича с Московским государственным лингвистическим университетом (МГЛУ). С главным зданием в старинном особняке по улице Остоженка, 38, с вековыми стенами, со своей домовой церковью (в честь Марии Магдалины), украшенной фресками Васнецова и Нестерова [10]. Думается, не последнюю роль в выборе будущего места работы сыграло то, что он родился, так сказать, в «этих краях» — в расположенном буквально рядом — Хилковом переулке, в старинном деревянном двухэтажном доме, снесённом уже после его кончины, где-то в 2006-м году.

А в здании сегодняшнего МГЛУ, еще до революции, в стенах тогдашнего Коммерческого училища, овладевали знаниями многие достойнейшие граждане нашей страны: писатель, критик и публицист Иван Гончаров — автор знаменитых романов «Обломов» и «Обрыв»; выдающийся русский историк Сергей Соловьев; генетик Николай и его брат физик Сергей Вавиловы. Сама атмосфера и история этого здания располагали к трепетному отношению к славному прошлому и родной культуре. В такой вот плодотворной среде Степан Петрович принялся за создания кафедры Мировой культуры.

Первым сотрудником кафедры стал кандидат исторических наук, преподаватель кафедры второго иностранного языка МГЛУ, потомственный инъязовец Тёмкин Виктор Александрович. Его мама, Российский лингвист-романист, специалист в области теории перевода, доктор филологических наук, профессор, замечательный педагог-испанист — Канонич Софья Иосифовна (1918–2006).

В воспоминаниях Виктора Александровича сохранились свидетельства того энтузиазма и одухотворенности, с которыми Степан Петрович создавал свою кафедру, как радовался успехам сотрудников и студентов.

С первых же дней появления кафедры её заведующий активно занимался и разработкой учебных программ преподаваемых дисциплин, и преподаванием, и научной работой.

В 1992 году автор этих строк был назначен на должность Начальника научно-исследовательского сектора МГЛУ. Из воспоминаний того перио-

да сохранились некоторые детали исследовательской работы, связанной с этно- культурологическими особенностями образовательных лингвистических систем, выполненной под руководством Степана Петровича и заслужившей самые высокие оценки специалистов.

Часто с благодарностью к судьбе вспоминаю 1994 год, когда мне посчастливилось вместе со Степаном Петровичем принимать участие в научной конференции Гранадского университета (Испания).

В той поездке Степан Петрович для меня фактически стал проводником в культуру и искусство Испании. Он показал мне маленький беленький домик в Фуэнте Вакерос (Гранада, Андалузия), где родился Федерико Гарсиа Лорка, великий испанский поэт, и на память читал свои любимые стихотворения Лорки на испанском и на русском.

Степан Петрович был для меня гидом в незабываемой ночной экскурсии по сооружениям одной из жемчужин арабского зодчества, архитектуры, резьбы по камню и парковому искусству — Альгамбре.

В Мадриде, в Прадо он в подлиннике открыл для меня полотна великих Веласкеса и Гойи — и всё это с точными и исчерпывающими фактами, тонкими замечаниями и мудрыми выводами.

К 1994 году Степан Петрович подготовил к первому изданию пособие «Основы культурологии». В 1996 году появилось на свет второе дополненное издание этого пособие, книгу которого с дарственной надписью Степана Петровича автор этой статьи благоговейно хранит среди своих лучших книг. В 2005 и 2016 годах, эта книга, переизданная, дополненная, вышла в свет в несколько ином формате под названием «Культурология. Учебник», уже под грифом Минобрнауки.

Еще одна реликвия — книга с автографом Степана Петровича «Антология культурологической мысли» (увидела свет в 1996 году). Эта антология была также подготовлена им в соавторстве с сыном, Александром Степановичем Мамонтовом, продолжателем семейных научных традиций.

Не стало Степана Петровича Мамонтова 25 апреля 2001 года.20 сентября 2023 года исполнилось бы 100 лет со дня рождения Степана Петровича Мамонтова. Но пока мы живы, Память о нём будет бережно сохраняться в наших сердцах.

Список источников

1. Кирога О. Сказки сельвы». М.: Гослитиздат, 1956. 43 с.

2. Грибанов А. (Вертер де Гёте). Эдгар По Латинской Америки: Орасио Кирога. Из цикла «Как издавали хоррор в СССР». Выпуск 5 / Лаборато-

рия фантастики. 1 июля 2019 г. [Электронный ресурс] URL: https://fantlab.ru/blogarticle61359 (Дата обращения 10.09.2023)

3. Кирога О. Cuentos de la selva, Сказки сельвы. С.-Пб.: Антология, 2016. 96 с.

4. Кирога О. Анаконда. М.: Гослитиздат, 1960. 344 с.

5. Поэзия Латинской Америки. Художественная литература, М. 1975.

6. Поляков А. К. Португалия. Полная история страны. М.: АСТ, 2023. 480 с.

7. Апостолов А. Помним и чтим культуролога Мамонтова / Проза.ру. 07 апреля 2016 г. [Электронный ресурс] URL:. https://proza.ru/2016/04/15/499 (Дата обращения 10.09.2023)

8. Шестопал А. В. Лица и поколения // Вестник МГИМО Университета. 2010, № 6 (15). С. 283–294.

9. Копелевич Ю. Х. К истории приобретения Россией рукописей Кеплера // Историко-астрономические исследования. Вып. XI. 1972. С. 131–145.

10. Гурьянова А. Дом Еропкина на Остоженке / Шагаю по Москве. [Электронный ресурс] URL: https://moscowsteps.com/dom-eropkina. (Дата обращения 10.09.2023)

Об авторе

Кириллов Игорь Алексеевич —
кандидат технических наук,
заслуженный профессор МГЛУ,
доцент кафедры международной
информационной безопасности
Института информационных наук;
Московский государственный
лингвистический университет
(Россия, Москва).
E-mail: I. A. Kirillov@gmail.com

About the author

Igor A. Kirillov —
Candidate of Technical Sciences,
Honored Professor
of Moscow State Linguistic University,
Associate Professor
of the Department of International
Information Security of the Institute
of Information Sciences;
Moscow State Linguistic University
(Russia, Moscow).
E-mail: I. A. Kirillov@gmail.com

УДК 001.89

АНАЛИЗ ПУБЛИКАЦИОННОЙ АКТИВНОСТИ ЧЛЕНОВ ДИССЕРТАЦИОННЫХ СОВЕТОВ: НА ПРИМЕРЕ ДВУХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ

Романова С. А.
Московский государственный лингвистический университет
(Россия, Москва)
s.a.romanova@linguanet.ru

Аннотация

Исследование показало, что для членов диссертационных советов двух образовательных организаций характерно опубликование исследовательских статей в большей степени в научных периодических изданиях, отнесенных ко второй категории Перечня ВАК. Стратегия выбора членом диссертационного совета определяется соответствием издания научной специальности, по которой ученый включен в диссертационный совет. В то же время при анализе выявлены особенности публикационной активности членов диссертационных советов, которые зависят от территориальной принадлежности автора и издательства, научной специальности, соавторства, авторитетности издания. Полученные выводы можно использовать при планировании будущих публикаций членов диссертационных советов.

Ключевые слова: научная публикация, член диссертационного совета, перечень журналов ВАК, цитирование, научное периодическое издание

PUBLICATION ACTIVITY'S ANALYSIS OF MEMBERS OF DISSERTATION COUNCILS: ON THE EXAMPLE OF TWO EDUCATIONAL ORGANIZATIONS

Svetlana A. Romanova
Moscow State Linguistic University (Moscow, Russia)
s.a.romanova@linguanet.ru

Abstract

The study showed that the members of the dissertation councils of two educational organizations are characterized by the publication of research articles to a greater extent in scientific periodicals classified in the second category of the List of Higher Educational Institutions. The strategy for choosing a publication by a member of the dissertation council is determined by the correspondence of the publication to the scientific specialty for which the scientist is included in the dissertation council. At the same time, the analysis revealed the peculiarities of the publication activity of members of dissertation councils, which depend on the territorial affiliation of the author and the publishing house, scientific specialty, co-authorship, and the authority of the publication. The findings can be used when planning future publications by members of dissertation councils.

Key words: scientific publication, member of the dissertation Council, list of Higher Attestation Commission journals, citation, scientific periodical

Введение

Публикационная активность любого ученого тесно связана с предъявляемыми научным сообществом требованиями к содержанию результатов исследований, таких как актуальность и оригинальность исследования, практическая и теоретическая значимость, достоверность результатов, отсутствие неправомерных заимствований и т.п.

Совокупность этих требований регулируется нормативными правовыми актами, касающимися аттестации научных кадров: федеральными законами[1], постановлениями Правительства Российской Федерации, приказами Минобрнауки России, рекомендациями ВАК и др.

В то же время научное сообщество изучает проблемы, связанные с процедурой оценки содержания исследований: обнаружение плагиата [6; 14; 30]; рецензирование [8; 21; 29]; самоцитирование [19; 27; 28]; индекс цитирования [4; 17; 24]; вклад каждого автора [12; 18; 22; 26]; аффилиацию автора [20]; ретракцию статей [7; 13; 15; 16; 25]; информационно-аналитическую систему учета публикаций [23; 31]; взаимодействие

[1] См., например: Федеральный закон от 23 августа 1996 г. № 127-ФЗ «О науке и государственной научно-технической политике» / КонсультантПлюс (Электронный ресурс) URL: https://www.consultant.ru/document/cons_doc_LAW_11507 (дата обращения: 18.10.2023).

между исследователями и редакторами периодических изданий [5; 10]; использование искусственного интеллекта для генерации текста, изображений, графиков, формул [3; 32] и т.д.

Важно не допустить в исследовании неправомерно заимствованную, сфабрикованную, сфальсифицированную информацию, а также сгенерированные нейросетями некорректные данные. Поддержание добросовестности в проведении научных исследований и информировании общественности о достигнутых результатах требует усилий со стороны всего научного сообщества.

Одним из инструментов по оценке качества исследований, наряду с институтом рецензирования, считается государственная система научной аттестации, в частности наделение членов диссертационных советов (далее — ЧДС) правом определять соответствие представленных в совет диссертаций на соискание ученой степени кандидата или доктора наук критериям, таким как новизна, актуальность, практическая и теоретическая значимость и др.[2]

Члены диссертационных советов, созданных на базе образовательной организации, должны являться специалистами по научной специальности, которую они представляют в совете, и иметь ученую степень доктора наук. В состав диссертационного совета могут быть включены лица, имеющие ученую степень кандидата наук, при подтверждении их значительного вклада в развитие отрасли науки. Создание диссертационного совета, его состав или изменения в составе и перечень научных специальностей, по которым в совете разрешено проводить защиты, утверждается приказом Минобрнауки России по ходатайству образовательной организации. В ходатайстве указывается как информация об образовательной организации, так и о публикационной активности каждого кандидата в члены диссертационного совета за 5 лет, предшествующих дате подачи ходатайства (см. пункт 10 раздела II Положения о совете по защите диссертаций[3]).

[2] Подробно см.: Раздел II постановления Правительства Российской Федерации от 24 сентября 2013 г. № 842 (ред. от 18 марта 2023 г.) «О порядке присуждения ученых степеней» (вместе с «Положением о присуждении ученых степеней») / КонсультантПлюс (Электронный ресурс) URL: URL: https://www.consultant.ru/document/cons_doc_LAW_152458 (дата обращения: 18.10.2023)

[3] Приказ Минобрнауки России от 10 ноября 2017 г. № 1093 (ред. от 14.12.2022) «Об утверждении Положения о совете по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук» (Зарегистрировано в Минюсте России 5 декабря 2017 г. № 49121) / КонсультантПлюс (Электронный ресурс) URL: https://www.consultant.ru/document/cons_doc_LAW_284549/ (дата обращения: 18.10.2023)

Через федеральную информационную систему государственной научной аттестации (далее — ФИС ГНА[4]) ученые секретари диссертационных советов подают отчеты о деятельности диссертационного совета за прошедший год, указывая в отчете данные о публикационной активности его членов за последние 5 лет. В разделе отчета «публикационная активность» перечисляются научные статьи из рецензируемых научных периодических изданий (из Перечня ВАК, из международных баз данных), рецензируемые монографии, доклады на международных конференциях и препринты членов диссертационного совета, а также указывается общее количество ссылок из РИНЦ[5], индекс Хирша по РИНЦ, Scopus, WoS за весь период деятельности каждого из членов совета.

Считается, что временной промежуток в 5 лет достаточен для выявления вклада ученого в развитие отрасли знаний, в которой он специализируется. Например, в работе Пономарева и др. [9] отмечается, что по прошествии пяти лет научная статья может находиться на стадии прироста цитирования, на стадии насыщения цитированием или цитирование спадает. Временной промежуток для оценки цитируемости статьи короче 5 лет может нанести вред процедуре оценки, поскольку велика вероятность пропуска прорывных статей и статей в изданиях с длительным редакционным циклом подготовки. Чтобы статья была в достаточной мере процитирована сторонними исследователями, ее не должны сдерживать длительные редакционные циклы, такие как длительные рецензирование и редактирование, а также согласование с автором и т.п.

Классическая траектория публикационной активности молодого ученого описывается быстрым ростом числа публикаций (во время подготовки к защите кандидатской, затем докторской диссертации), за кото-

[4] Прим.: ФИС ГНА — Федеральная информационная система государственной научной аттестации создана в соответствии с требованиями Федерального закона от 2 июля 2013 г. № 185-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу законодательных актов (отдельных положений законодательных актов) Российской Федерации в связи с принятием Федерального закона «Об образовании в Российской Федерации"» (Электронный ресурс) URL: http://static.kremlin.ru/media/acts/files/0001201307080024.pdf (дата обращения: 18.10.2023), и ведется на основании постановления Правительства Российской Федерации от 18 ноября 2013 г. № 1035 «О федеральной информационной системе государственной научной информации» (Электронный ресурс) URL: http://static.government.ru/media/files/41d4a3e3a46a758e7faf.pdf (дата обращения: 18.10.2023).

[5] Прим.: Российский индекс научного цитирования (РИНЦ) — национальная информационно-аналитическая система учета публикаций и их цитирований, размещенная на платформе Научной электронной библиотеки «Elibrary.ru».

рым следует медленное снижение их числа. Для состоявшихся докторов наук — членов диссертационных советов траектория публикационной активности иная. Чтобы увидеть её отличительные особенности, обратимся к изучению массива публикаций членов диссертационных советов двух образовательных организаций ФГБОУ ВО «Московский государственный лингвистический университет» (далее — МГЛУ) и ФГКОУ ВО «Академия управления Министерства внутренних дел Российской Федерации» (далее — Академия управления МВД России) за 2019–2023 гг. из Научной электронной библиотеки «Elibrary.ru» (далее — НЭБ «Elibrary.ru»), в том числе рассмотрим, в каких рецензируемых изданиях они публиковались и имеются ли у них высокоцитируемые научные работы.

Следует отметить, что цитирование, пусть и с задержкой, обеспечивает признание вклада ученого в развитие области научных знаний. Так, Д. Акснес и А. Рип [1] доказали, что ученому важно иметь не менее одной высокоцитируемой качественной статьи, чтобы быть признанным в своей области научной деятельности.

С другой стороны, отношение к цитированию у научного сообщества двойственное: высокое цитирование может свидетельствовать как о высоком качестве подготовленной статьи [11], так и о «договорном» цитировании в академической среде. Например, исследование Ю. В. Чеховича и А. В. Хазова массива полнотекстовых научных публикаций из НЭБ «Elibrary.ru» раскрыло недостатки в редакционной политике российских журналов, допустивших дублирование научных публикаций российских ученых [2].

Данные и методы исследования

Проанализирована публикационная активность в научных периодических изданиях, включенных в Перечень ВАК и отнесенных к категориям К1, К2 и К3[6], 74 членов 5 диссертационных советов МГЛУ и 52 членов четырёх диссертационных советов Академии управления МВД России за период 2019–2022 год и 10 месяцев 2023 года по открытым данным из НЭБ «Elibrary.ru».

[6] См.: Информационное письмо Высшей аттестационной комиссии при Минобрнауки России от 6 декабря 2022 № 02–1198 «О категорировании Перечня рецензируемых научных изданий» / Высшая аттестационная комиссия при Министерстве науки и высшего образования Российской Федерации [Электронный ресурс] URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=19&name=92263438002&f=15751 (дата обращения: 15.11.2023).

Использован алгоритм поиска публикаций по параметрам: год публикации; автор публикации; «статьи в журналах, включенные в текущий перечень ВАК»; «статьи в журналах, входящих в RSCI»; «статьи в журналах, входящих в Web of Science или Scopus». Публикации, не отраженные в авторском профиле в НЭБ «Elibrary.ru» (например, находящиеся в печати), анализу не подвергались.

Результаты и обсуждение

В Таблицах 1 и 2 приведены данные из НЭБ «Elibrary.ru» о ведущих научных направлениях в МГЛУ и Академии управления МВД России за период 2019–2022 год и 10 месяцев 2023 года.

Для МГЛУ ведущими направлениями исследований являются тематики по филологическим, педагогическим, юридическим, политическим, социологическим наукам, культурологии и литературоведению; для Академии управления МВД России — по юридическим, экономическим, педагогическим, психологическим, социологическим, историческим и техническим наукам. Диссертационные советы, открытые в МГЛУ, принимают к защите диссертации по 9 научным специальностям, отнесенным к следующим отраслям науки: филологические, педагогические, политические, социологические науки и культурология. За рассматриваемый период члены диссертационных советов МГЛУ (внешние и являющиеся сотрудниками этой образовательной организации) публиковались в 264 уникальных научных периодических изданиях. Из них 49 (19%)

Таблица 1. Ведущие направления исследований в МГЛУ за период2019–2022 год и 10 месяцев 2023 года, отраженные в различных публикациях (по состоянию на 15 ноября 2023 г.).

№ п/п	Тематика	Всего публикаций, включенных в РИНЦ	Из них:		
			В изданиях, включенных в Перечень ВАК	В изданиях, включенных в RSCI	В изданиях, включенных в WoS или Scopus
1	Филологические науки	5080	1659	80	175
2	Педагогические науки	854	330	10	16
3	Юридические науки	821	275	15	16
4	Политические науки	729	292	26	23
5	Культурология	497	132	28	30
6	Литературоведение	353	144	23	24
7	Социологические науки	479	102	15	17

изданий включены в международные базы данных и RSCI, 18 (7%) — включены в Перечень ВАК за последние 2 года и не имеют категории, 59 (22%) изданий отнесены к первой категории (К1), 109 (41%) — ко второй (К2), 29 (11%) — к третьей (К3)[7]. Таким образом, в выборе членами диссертационных советов МГЛУ изданий для своих статей лидируют издания, отнесенные ко второй категории Перечня ВАК [8].

Таблица 2. Ведущие направления исследований в Академии управления МВД России за период 2019–2022 год и 10 месяцев 2023 года, отраженные в различных публикациях (по состоянию на 22 ноября 2023 г.).

№ п/п	Тематика	Всего публикаций, включенных в РИНЦ	Из них:		
			В изданиях, включенных в Перечень ВАК	В изданиях, включенных в RSCI	В изданиях, включенных в WoS или Scopus
1	Юридические науки	7105	2676	42	82
2	Экономические науки	1005	181	12	41
3	Педагогические науки	786	213	0	6
4	Психологические науки	632	239	22	25
5	Социологические науки	214	105	18	19
6	Исторические науки	186	97	8	18
7	Технические науки	113	54	2	0

[7] Прим.: Научное периодическое издание отнесено к той или иной категории на основании информационного письма Высшей аттестационной комиссии при Минобрнауки России от 6 декабря 2022 № 02–1198 «О категорировании Перечня рецензируемых научных изданий». В 2024 году планируется введение в действие нового распределения по категориям К1, К2, К3 научных периодических изданий, включенных в Перечень ВАК по результатам наукометрической и экспертной оценки за 2022–2023 гг.

[8] Согласно рекомендации пленума ВАК Минобрнауки России от 22 июня 2023 года № 1-пл/2 «О работе по совершенствованию и оптимизации перечня научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук» / Высшая аттестационная комиссия при Министерстве науки и высшего образования Российской Федерации [Электронный ресурс] URL: https://vak.minobrnauki.gov.ru/uploader/loader?type=35&name=92548041002&f=19033 (дата обращения: 15.11.2023). Издания по категориям распределились в следующих пропорциях: 25% — первая категория, 50% — вторая категория и 25% — третья категория. Следовательно, статей ЧДС в изданиях, отнесенных ко второй категории, будет значительно больше, что и подтверждает проведенное исследование.

Диссертационные советы, открытые в Академии управления МВД России, принимают к защите диссертации по трём научным специальностям, отнесенным к техническим, юридическим и педагогическим отраслям науки.

За рассматриваемый период члены диссертационных советов Академии управления МВД России (внешние и являющиеся сотрудниками академии) публиковались в 268 уникальных научных периодических изданиях: 32 (12%) издания включены в МБД и RSCI, 10 (3%) — включены в Перечень ВАК за последние 2 года и не имеют категории, 69 (26%) изданий отнесены к первой категории (К1), 109 (41%) — ко второй (К2), 48 (18%) — к третьей (К3). Члены диссертационных советов Академии управления МВД России также предпочитают выбирать для опубликования статей научные периодические издания, отнесенные ко второй категории в Перечне ВАК.

Максимальное число научных статей членов диссертационных советов за рассматриваемый период выявлено в изданиях той образовательной организации, в которой они работают.

Для ЧДС МГЛУ максимум статей опубликован в Вестниках МГЛУ (серия «Гуманитарные науки» — 149 статей, серия «Общественные науки» — 68 статей, серия «Образование и педагогические науки» — 66 статей); для ЧДС Академии управления МВД России максимум — в научном периодическом издании «Труды Академии управления МВД России» (100 статей).

Члены диссертационных советов МГЛУ также часто публикуют статьи в сторонних изданиях в разных городах: «Когнитивные исследования языка» (Тамбов) — 100 статей, «Иностранные языки в школе» (Москва) — 21 статья, «Вопросы когнитивной лингвистики» (Тамбов) — 18 статей, «Вестник ВолГУ. Серия 2: Языкознание» (Волгоград) — 14 статей.

Члены диссертационных советов Академии управления МВД России часто публикуются как в ведомственных научных периодических изданиях, так и в гражданских изданиях в разных городах: «Вестник Воронежского института ФСИН России» (Воронеж) — 23 статьи, «Вестник Уфимского юридического института МВД России» (Уфа) — 22 статьи, «Вестник экономической безопасности» (Москва) — 21 статья, «Прикладная психология и педагогика» (Москва) — 20 статей.

Максимум цитирований распределился следующим образом.

Статьи ЧДС МГЛУ по филологическим и педагогическим наукам высоко цитируются в изданиях, отнесенных ко второй категории Перечня ВАК. Статьи ЧДС по политологии, истории, социологии, культурологии и литературоведению цитируются в 4 раза меньше независимо от категории, к которой отнесено издание.

Статьи ЧДС Академии управления МВД России по юриспруденции и техническим наукам высоко цитируются в изданиях, отнесенных как к первой, так и ко второй категории. Тогда как статьи ЧДС по психологии и педагогике цитируются в 6 раз меньше независимо от категории, к которой отнесено издание.

Анализ публикационной активности ЧДС двух образовательных организаций выявил и некоторые другие особенности в выборе изданий для опубликования. Каждый член диссертационного совета за рассмотренный период публиковался в 5–7 разных научных периодических изданиях в пределах города, в котором работает (преподает или приглашен на защиту диссертации), или в городе, в который приехал на тематическую конференцию или защиту диссертации. Если член диссертационного совета ранее работал в другом городе и публиковал научные статьи в научных периодических изданиях этого города (например, в Воронеже, Калининграде, Самаре, Саратове, Уфе, Челябинске) и позже переехал в Москву, то при сохранившихся контактах с редакцией, он продолжает публиковать там свои статьи. Если контакты с издательством из другого города длительно не поддерживаются, член диссертационного совета публикуется в изданиях того города, в котором постоянно проживает и работает, или в который временно приезжает. Член диссертационного совета также чаще публикуется в издании того образовательного учреждения, в котором преподает или состоит в диссертационном совете.

Выбор издания членом диссертационного совета для опубликования результатов своего исследования зависит и от многих других условий: включения издания в Перечень ВАК по его научной специальности, наличия соавтора, включения в международную базу данных или RSCI, налаженных контактов с редакцией издания, бумажный или электронный способ предоставления статьи в издательство и т.п.

Также мониторинг научных публикаций членов диссертационных советов за 2019–2023 гг. не выявил ретрагированных статей по базе данных РИНЦ, что свидетельствует о соблюдении авторами принципов научной этики и подготовки рукописей на высоком профессиональном уровне.

Выводы и рекомендации

Выбор членом диссертационного совета научного периодического издания для опубликования проведенного исследования по-прежнему остается сложным и сопряженным со многими трудностями процессом.

Исследование показало, что члены диссертационных советов публикуются в различных научных периодических изданиях, как включенных

в международные базы данных (Scopus, Web of Science, Chemical Abstract и т.д.), так и включенных в Перечень ВАК и соотнесенных с тремя категориями. В большинстве случаев члены диссертационных советов выбирают издания, включенные во вторую категорию Перечня ВАК.

В ходе исследования было выявлено, что данные о включении издания в Перечень ВАК по новой научной специальности и в международную базу данных (Scopus и Web of Science) могут устаревать по мере проведения переоценки изданий экспертами. Если такая информация своевременно не скорректирована на сайте издания и в его анкете на сайте НЭБ «Elibrary.ru», это приводит к путанице и дезинформации авторов, желающих подать свою рукопись на опубликование. В этом случае именно издатель несет ответственность за своевременную корректировку информации на сайте издания и в анкете на сайте НЭБ «Elibrary.ru» об индексации или прекращении индексации своего издания как в Перечне ВАК по новой номенклатуре научных специальностей, так и в международных базах данных при включении в них ранее.

Одной из рекомендаций по защите автора от подобной неточности может служить введение в договор с автором пункта о возможности отзыва статьи до ее опубликования (на стадии рецензирования и редакторской обработки) при изменении статуса издания в Перечне ВАК или в международной базе данных, и передачи ее в другое издание.

Сотрудники отдела научного менеджмента и наукометрии МГЛУ на сайте вуза[9] ежегодно публикуют списки отечественных научных периодических изданий по профилям подготовки с учетом их текущего статуса в Перечне ВАК и международных базах данных на момент публикации. Эта информация носит рекомендательный характер и помогает членам диссертационных советов рассмотренных образовательных организаций сориентироваться в выборе качественных изданий.

Список источников

1. Aksnes D. W., Rip A. Researchers' perceptions of citations // Research Policy. 2009. Volume 38, Issue 6, Pp. 895–905. ISSN 0048–7333. URL: https://doi.org/10.1016/j.respol.2009.02.001 (accessed 18 October 2023).

2. Chekhovich Y. V., Khazov A. V. Analysis of duplicated publications in Russian journals // Journal of Informetrics. 2022. Volume 16, Issue 1, 101246. URL: https://doi.org/10.1016/j.joi.2021.101246 (accessed 18 October 2023).

[9] См.: Журналы для публикаций / МГЛУ. Наука без границ [Электронный ресурс] // URL: https://science.linguanet.ru/журналы-для-публикации (дата обращения: 18.10.2023).

3. Dien J. Editorial: Generative artificial intelligence as a plagiarism problem // Biological Psychology. 2023. Vol. 181, 108621, ISSN 0301–0511. DOI 10.1016/j.biopsycho.2023.108621.

4. Filippo D. D., Gorraiz J. Is the Emerging Source Citation Index an aid to assess the citation impact in social science and humanities? // Journal of Informetrics. 2020. Vol. 14, Issue 4, 101088, ISSN 1751–1577. URL: https://doi.org/10.1016/j.joi.2020.101088 (accessed 18 October 2023).

5. Fong E. A., Patnayakuni R., Wilhite A. W. Accommodating coercion: Authors, editors, and citations // Research Policy. 2023. Volume 52, Issue 5, 104754, ISSN 0048–7333. URL: https://doi.org/10.1016/j.respol.2023.104754 (accessed 18 October 2023).

6. Gipp B. Citation-based Plagiarism Detection. Detecting Disguised and Cross-language Plagiarism using Citation Pattern Analysis. Springer, 2014. eISBN 978–3–658–06394–8.

7. Kwee R. M., Kwee T. C. Retracted Publications in Medical Imaging Literature: an Analysis Using the Retraction Watch Database // Academic Radiology. 2023. Volume 30, Issue 6. Pp. 1148–1152, ISSN 1076–6332. URL: https://doi.org/10.1016/j.acra.2022.06.025 (accessed 18 October 2023).

8. Nedić O., Dekanski A. Priority criteria in peer review of scientific articles // Scientometrics, 2016. Vol. 107, no 1, pp. 15–26. DOI: 10.1007/s11192–016–1869–6.

9. Ponomarev I. V., Williams D. E., Hackett C. J., Schnell J. D., Haak L. L. Predicting highly cited papers: A method for early detection of candidate breakthroughs // Technological Forecasting and Social Change. 2014. Vol. 81, pp. 49–55.

10. Si K., Li Y., Ma Ch., Guo F. Affiliation bias in peer review and the gender gap // Research Policy. 2023. Vol. 52, Iss.7, 104797, ISSN 0048–7333. URL: https://doi.org/10.1016/j.respol.2023.104797 (accessed 18 October 2023).

11. Tikhonova E., Raitskaya L. Citations and References: Guidelines on Literature Practices // Journal of Language and Education. 2022. Vol. 8, no 3, pp. 5–10. URL: https://doi.org/10.17323/jle.2022.15960 (accessed 18 October 2023).

12. Yang S., Xiao A., Nie Y., Dong J. Measuring coauthors' credit in medicine field — Based on author contribution statement and citation context analysis // Information Processing & Management. 2022 Volume 59, Issue 3, 102924, ISSN 0306–4573. URL: https://doi.org/10.1016/j.ipm.2022.102924 (accessed 18 October 2023).

13. Zilberman T., Margalit I., Yahav D., Tau N. Retracted publications in infectious diseases and clinical microbiology literature: an analysis using the retraction watch database // Clinical Microbiology and Infection. 2023. Jul 29,

ISSN 1198–743X. URL: https://doi.org/10.1016/j.cmi.2023.07.022 (accessed 18 October 2023).

14. Авдеева Н. В., Сусь И. В., Иванова Е. Н. Практики оценки качества научных документов // Информационные ресурсы России. 2020. № 6. С. 11–19.

15. Балякина Е. А. Retraction Watch — инструмент информирования научного сообщества об этических нарушениях в публикациях // Научный редактор и издатель. 2021. Т. 6, № 2. С. 164–174. DOI 10.24069/SEP-21–12.

16. Богустов А. А. Процедура ретракции с точки зрения авторского права // Хозяйство и право. 2021. № 1 (528). С. 80–87.

17. Габараев Б. А., Джалавян А. В. Наукометрия в оценке деятельности российских учёных // Обозреватель. 2022. № 7–8 (390–391). С. 143–150. DOI 10.48137/2074–2975_2022_7–8_143.

18. Грачева Е. Ю. Актуальные вопросы научной экспертизы диссертационных правовых исследований // Юридическое образование и наука. 2019. № 7. С. 14–20. DOI 10.18572/1813–1190–2019–7–14–20.

19. Зайцев В. В., Михайлова И. А. Право автора на самоцитирование среди других авторских прав // Труды по интеллектуальной собственности. — 2023. Т. 46, № 3. С. 76–83.

20. Кириллова О. В. Значение и основные требования к представлению аффилиации авторов в научных публикациях // Научный редактор и издатель. 2016. Т. 1. № 1–4. С. 32–42.

21. Киричек А. В., Морозова А. В., Спасенников В. В. Рецензирование как процедура экспертного оценивания качества научных статей // Эргодизайн. 2018. № 2 (2). С. 3–7.

22. Косычева М. А. Система CRediT для описания авторского вклада // Health, Food & Biotechnology. 2023. Т. 5. № 1. С. 6–9. DOI 10.36107/hfb.2023.i5.s169.

23. Мазов Н. А., Гуреев В. Н. Ведение базы данных публикаций организации с использованием библиографических ресурсов открытого доступа // Научно-техническая информация. Серия 1: Организация и методика информационной работы. 2023. № 9. С. 20–32. DOI 10.36535/0548–0019–2023–09–4.

24. Никулина Ю. В. Возможности и перспективы использования международных систем научного цитирования при оценке эффективности научной работы // Труды БГТУ. Серия 6: История, философия. 2020. № 1 (233). С. 138–142.

25. Пачина Н. Н. Политика издания в сфере ретрагирования статей // Человек. Общество. Наука. 2023. Т. 4, № 2. С. 10–12. DOI 10.53015/2686–8172_2023_4_2_10.

26. Пикало И. А. Поправочный коэффициент в наукометрических базах для оптимального определения рейтинга ученого и организации // Система менеджмента качества: опыт и перспективы. 2021. № 10. С. 286–290.

27. Писляков В. В. Самоцитирование и его влияние на оценку научной деятельности: обзор литературы. Часть I // Научные и технические библиотеки. 2022а. № 2. С. 49–70. DOI 10.33186/1027–3689–2022–2–49–70.

28. Писляков В. В. Самоцитирование и его влияние на оценку научной деятельности: обзор литературы. Часть II // Научные и технические библиотеки. 2022б. № 3. С. 85–104. DOI 10.33186/1027–3689–2022–3–85–104.

29. Раицкая Л. К. О перспективах создания комплексной системы независимого рецензирования российских научных журналов // Научный редактор и издатель. 2017. Т. 2, № 2–4. С. 84–88. DOI 10.24069/2542–0267–2017–2–4–84–88.

30. Сусь И. В., Иванова Е. Н. Зарубежные стратегии анализа качества научных документов (европейские страны) // Образовательные ресурсы и технологии. 2020. № 4 (33). С. 88–98. DOI 10.21777/2500–2112–2020–4–88–98.

31. Шумилин Д. А. Единая государственная информационная система учета научно-исследовательских, опытно-конструкторских и технологических работ гражданского назначения: реалии и перспективы // Временник Зубовского института. 2023. № 1 (40). С. 9–17. DOI 10.52527/22218130_2023_1_9.

32. Янковский Р. М. Способен ли искусственный интеллект написать статью в юридический журнал? // Закон. 2023. № 3. С. 126–133. DOI 10.37239/0869–4400–2023–20–3–126–133.

Об авторе

Романова Светлана Андреевна —
специалист отдела
научного менеджмента и наукометрии,
Московский государственный
лингвистический университет
(Россия, Москва).
E-mail: s.a.romanova@linguanet.ru

About the author

Svetlana A. Romanova —
Specialist of the Department
of Scientific Management
and Scientometrics,
Moscow State Linguistic University
(Russia, Moscow).
E-mail: s.a.romanova@linguanet.ru

УДК: 008: 130.2; 141.319.8

ЕВРОПЕЙСКИЙ ДЕКАДАНС И ВОСХОЖДЕНИЕ ФАУСТОВСКОЙ ТЕМЫ В СОЦИАЛИСТИЧЕСКОМ РЕАЛИЗМЕ

Былевский П. Г.
Московский государственный лингвистический университет
(Россия, Москва).
pr-911@yandex.ru

Аннотация

Автор предлагает применять инструментарий сравнительно-исторической культурологии и субъектно-деятельностный подход к анализу эволюции образа доктора Фауста в культуре после И.-В. Гёте. Предлагаемый метод позволяет выявить две тенденции социально-культурного процесса: с одной стороны — декаданс (нисхождение, нарастание пессимизма), с другой стороны — восходящую, оптимистическую линию развития. Одна преимущественно свойственна западноевропейской культуре, вторая — отечественной, в частности, в искусстве социалистического реализма. Продуктивность предлагаемого подхода проявляется в том, что на основе героической интерпретации «фаустовского типа» выявляются примеры индивидуальных субъектов социально-культурного творчества. Это личности, способные служить прототипами конструктивно-позитивного развития в искусстве «фаустовского образа», а также нормативными ориентирами в современной культурно-воспитательной работе.

Ключевые слова: И.-В. Гёте, доктор Фауст, культурология, преображение, общественно полезный труд, социально-культурная деятельность, фаустовская личность, социалистический реализм

EUROPEAN DECADENCE AND THE RISE OF THE FAUSTIAN THEME IN SOCIALIST REALISM

Pavel G. Bylevskiy
Moscow State Linguistic University (Russia, Moscow)
pr-911@yandex.ru

Abstract

The author suggests applying the tools of comparative historical cultural studies and a subject-activity approach to the analysis of the evolution of the image of Dr. Faust in culture after I.-V. Goethe. The proposed method allows us to identify two trends in the socio-cultural process: on the one hand, decadence (descent, increase in pessimism), on the other hand, an upward, optimistic line of development. One is mainly characteristic of Western European culture, the second is native, in particular, in the art of socialist realism. The productivity of the proposed approach is manifested in the fact that, based on the heroic interpretation of the "Faustian type", examples of individual subjects of socio-cultural creativity are identified. These are individuals who can serve as prototypes of constructive and positive development in the art of the "Faustian image", as well as normative guidelines in modern cultural and educational work.

Keywords: I.-V. Goethe, Dr. Faust, cultural studies, transfiguration, socially useful work, socio-cultural activity, Faustian personality, socialist realism

Введение

Образ доктора Фауста в мистической «трагедии для чтения» И.-В. Гёте оказался рубежным в истории культуры. Его мощь и глубина привели к тому, что сюжет трагедии многократно служил основой художественного переосмысления в ходе дальнейшего развития культуры. Применение сравнительно-исторической культурологии [1] и субъектно-деятельностного подхода [2] к анализу эволюции образа доктора Фауста в культуре после И. В. Гёте позволяет выявить две противоположные линии его «исторических судеб». Их можно условно определяемые как «нисходящую» и «восходящую».

Европейский декаданс: нисходящая тенденция

Фаустовская тема И.-В. Гёте век спустя проявилась в полярном раздвоении социально-культурного процесса: «отмену» героического пафоса в зарубежной культуре и, напротив, появление в отечественном социалистическом реализме жанра «оптимистической трагедии». «Нисходящая» линия, пессимистическая линия свойственна западноевропейской культуре. Она углубляет трагизм образа доктора Фауста, вплоть до безысходности. Происходит ревизия образа, созданного И.-В. Гёте, применяется редукция, рудиментарное воспроизведение в новых условиях прежних

трактовок этого образа, существовавших ранее. Ярким примером пессимистической, нисходящей линии развития [3]служит роман Томаса Манна «Доктор Фаустус. Жизнь немецкого композитора Адриана Леверкюна, рассказанная его другом», начатый в 1943 году и опубликованный в 1947 году. Герой Томаса Манна — композитор, творящий в жанре додекафонии, модернистского направления современной музыки (параллель с композитором Арнольдом Шёнбергом).

Адриан Леверкюн заражается сифилисом, но не лечится. Потому что начавшееся от этого психическое заболевание способствует своеобразному подъёму творческих сил, галлюцинациям. Это явная аллюзия с судьбой Фридриха Ницше, чей философский образ «белокурой бестии» лёг в основу нацистской идеологии «сверхчеловека». Больному композитору привидится Мефистофель, с которым он, подобно доктору Фаусту, заключает договор. В обмен на своеобразное модернистское вдохновение он жертвует душой.

Вместе с тем «доктор Фаустус» Томаса Манна становится неспособен на подлинное, гуманистическое и реалистическое творчество. На пути модернистского разрушения реалистической художественной формы у него созревает маниакальное решение: лишить человечество условной «Девятой симфонии Бетховена». Потому что её оптимистический хоровой финал — это «Ода к радости» на стихи Ф. Шиллера. В настоящее время это официальный гимн Европейского Союза.

Также Адриан Леверкюн теряет способность к любви. Потому что тем, кого он любит, грозит гибель, подобная страшной смерти его любимого племянника, пятилетнего Непомука. В финале романа проводится параллель между творческой и человеческой трагедией композитора Адриана Леверкюна, увлёкшегося модернизмом, — и Германии, которую фашизм довёл до национальной катастрофы [4].

В похожем ключе, на материале того же исторического периода художественно переосмысливается образ доктора Фауста и его контрагента в кинофильме «Мефисто». Это первая часть так называемой «немецкой трилогии» венгерского кинорежиссера Иштвана Сабо, экранизация романа «Мефисто: история одной карьеры» (1936 год) Клауса Манна, кстати, сына Томаса Манна. В основу его книги положена реальная история его друга молодости, знаменитого актёра Густафа Грюндгенса [5]. Сотрудничество с фашистскими властями ради утоления непомерного честолюбия и карьеры закончилось полной деградацией личности.

В обоих произведениях, книгах Томаса Манна и Клауса Манна (по которой снят фильм «Мефисто»), отца и сына, образ доктора Фауста трактуется в духе попятного движения от созданного И. В. Гёте. Их доктор

Фауст вновь действует во имя утилитарной цели, успешной творческой карьеры. Ради этого жертвует самым дорогим, включая собственную душу и близких людей. Прибегает к помощи метафизического зла. В результате же оказывается у разбитого корыта, во «внутреннем аду»: собственная судьба разрушена, личность в руинах.

Обратим внимание: в двух приведённых примерах развитие образа доктора Фауста, классического сюжета, осуществляется не отвлечённо, не «в безвоздушном пространстве». Напротив: в самой тесной связке с социально-культурными процессами, свойственными описываемой эпохе. Особенности художественного образа определяются тенденциями и проблематикой тогдашней культуры в целом. Ради обратного воздействия на аудиторию, а через неё — на гуманистическое переустройство действительности. В наше время человеку, мучающемуся «фаустовским вопросом», трансгуманизм предлагает соблазн «улучшения» (омоложения, бессмертия и т.п.) исключительно посредством новых высоких технологий, взамен утраты души [6].

Социалистический реализм: восходящая линия

В истории отечественной культуры Российской Империи — СССР — Российской Федерации преобладала другая линия развития образа доктора Фауста, которую можно обозначить как восходящую, оптимистическую [7]. Она характеризуется развитием сущностных черт протагониста «Доктора Фауста», продуктивными художественными решениями в контексте социально-культурного творчества.

В 1892 году А. М. Горький написал романтическую поэму-сказку «Девушка и Смерть». По цензурным соображениям опубликовать её удалось лишь в июле 1917 года, в газете «Новая жизнь», которую он сам тогда редактировал. Позже, 11 октября 1931 года, А. М. Горький зачитал это своё юношеское произведение в особняке С. П. Рябушинского в Москве. И. В. Сталин нанёс на последнюю страницу текста издания резолюцию: «Эта штука сильнее, чем «Фауст» Гёте (Любовь побеждает Смерть)» [7].

Эта оценка является не конъюнктурной и не чрезмерной, но пророческой. Вот почему. У героя сентиментального романа в письмах «Страдания юного Вертера» (1774), принесшего молодому И.-В. Гёте литературную славу, быстро появилось немало подражателей. В 1974–1975 годах американский социолог Дэвид Филлипс (Калифорнийский университета, США), исследовавший волну «подражающих самоубийств», ввёл термин «Эффект Вертера», ставший популярным среди психологов [8]. Напротив, почти век после публикации трагедии И.-В. Гёте «Фауст» достойных подражателей и последователей у её главного героя не было.

Деятельно-оптимистическое начало, которое И.-В. Гёте придал образу доктора Фауста, получило качественно новое бытие, многостороннее и обширное развитие в искусстве социалистического реализма в СССР. Впервые в истории культуры было начато интенсивное взаимодействие между прототипом в реальной жизни, художественным образом героя и, что особенно важно, его обратным воздействием на практические социально-культурные процессы.

Первым ярким примером является книга А. Н. Островского «Как закалялась сталь»: сам автор, его судьба лежат в основе образа Павки Корчагина, главного героя. Это герой «фаустовского типа», как и сам автор, положивший в основу книги свою автобиографию. На фронтах Гражданской войны и на стройках социализма он потерял здоровье. Но не смирился с уготованной ему отныне незавидной участью. Напротив, нашёл в себе силы, превозмогая тяжелейшие недуги, написать книгу с огромным воспитательным потенциалом. Роман стал самым издаваемым произведением художественной литературы в стране: на 1 января 1991 года был издан на 75 языках народов СССР 773 раза суммарным тиражом 53,854 млн. экземпляров [9]. Было три экранизации книги: в 1942, 1956 и 1973 годах.

Второй подобный пример — «Повесть о настоящем человеке» (1946) Б. Н. Полевого, прототипом главного героя которой стал лётчик-истребитель, Герой Советского Союза А. П. Маресьев. Став полным инвалидом из-за тяжёлых ранений, полученных на фронте, он сумел вернуться в строй, смог снова совершать боевые вылеты. До 1 января 1990 года повесть была издана 229 раз на 52 языках народов мира общим тиражом свыше 36 млн. экземпляров. В 1948 году по ней сняли одноимённый кинофильм, а Сергей Прокофьев написал оперу с тем же названием.

И «Как закалялась сталь», и «Повесть о настоящем человеке», обладая огромным воспитательным потенциалом, до начала 1990-х годов входили в обязательные программы школьного чтения. Их герои, Павка Корчагин и Алексей Мересьев, служили живыми примерами для подражания десяткам миллионов подростков и молодых людей, образцами «делать жизнь с кого». Как мы видим, в отечественном социально-культурном процессе произошло позитивное, восходящее развитие образа доктора Фауста, созданного И. В. Гёте. Даже не прибегая к прямому цитированию имени героя и сюжетных ходов. Российские, советские «фаусты» носят иные имена, но черты их сходства с протагонистом трагедии И. В. Гёте просматриваются хорошо.

Оказавшись в нечеловечески трудных обстоятельствах, они не сдаются. Находят силы вернуть себя к полноценной жизни. Делают это в про-

цессе напряжённого труда на благо других людей, действуя вместе и заодно с ними, участвую в общем историческом творчестве. Не прибегая к помощи «высших сил», тем более силы нечистой. Не жертвуя близкими людьми, не приходя в итоге к разрушению собственной личности и судьбы. Результат получается созидательный, позитивный.

Современные перспективы развития фаустовского образа

В современной России также есть примеры людей «фаустовского типа», способных послужить прототипами героев грядущих шедевров искусства. Один из них — С. М. Бубновский, среди прочего, «коллега» доктора Фауста, причём дважды. Как медик по профессии и как обладатель учёной степени доктора, только не богословия, а медицинских наук (2007). Закончив в Сургуте Институт физической культуры, С. М. Бубновский во время службы в армии в автокатастрофе получил страшные травмы. 12 дней провёл в коме, пережил клиническую смерть, ряд сложных операций. Потом 27 лет передвигался на костылях, каждое движение вызывало острую боль.

Вердикт врачей был безжалостным: пожизненная инвалидность второй группы, медленное мучительное угасание. Но доктор С. М. Бубновский, не прибегая к помощи коварных «мефистофелей», разработал собственную методику реабилитации. Трудами тяжкими полностью преодолел собственную инвалидность. На основе своей практики разработал новое направление медицины — кинезитерапию, помогающую пациенту решить проблемы со здоровьем, принципиально не решаемые по-другому, в частности — фармакологией и физиотерапией.

С. М. Бубновский не только создал опробованную на себе методику, но и разработал на её основе способы излечения многих заболеваний, возвращения здоровья и полноценной жизни, казалось бы, безнадёжно больным людям. И довёл дело до многопрофильного массового сервиса, в России сейчас действуют около ста медицинских центров, работающих по его методикам [10].

Наши современники — люди, подобные С. М. Бубновскому, — являются представителями «личности фаустовского типа» в её трактовке, выработанной И.-В. Гёте, её наследниками и продолжателями. Это люди, поставленные своей судьбой и обстоятельствами в крайне трудные условия. Говоря термином философии экзистенциализма, в «пограничную ситуацию» [11]. Такой человек совершает героический выбор: не смиряется с, казалось бы, неизбежным. Но находит силы и способы победить судьбу. Не только во имя собственного спасения, но и во благо других людей, участвуя в совместной творческой деятельности.

Выводы

Предлагаемый подход позволяет определить две противоположные тенденции развития образа доктора Фауста в социально-культурной деятельности после И.-В. Гёте. С одной стороны, пессимистическую, нисходящую, с другой — оптимистическую, восходящую. Первая в большей степени развивается в западноевропейской культуре, вторая — в отечественном социально-культурном поле. Вторая тенденция более свойственна отечественной культуре, в особенности искусству социалистического реализма. Что особенно важно, удаётся установить, что не только исторические, но и современные индивидуальные субъекты социально-культурного творчества обладают большим потенциалом. Они могут служить полноценными прототипами для создания художественных произведений в русле конструктивно-позитивного развития тематики «фаустовского образа».

Список источников

1. Бабякина Е. П. Культурная политика социального государства: сущность и модели реализации: автореферат диссертации на соискание ученой степени кандидата культурологии: 24.00.01. М.: РАНХиГС, 2013. 33 с.

2. Циринг Д. А., Яковлева Ю. В. Проблема самостоятельности субъекта в рамках классического университетского образования // Историческая и социально-образовательная мысль. 2012. № 4(14). С. 177–180.

3. Якушева Г. В. Фауст и Мефистофель в литературе XX века: К проблеме кризиса просветительского героя: диссертация на соискание учёной степени доктора филологических наук. 10.01.05. М.: 1998. 319 с.

4. Манн Т. Доктор Фаустус. Жизнь немецкого композитора Адриана Леверкюна, рассказанная его другом / Манн Т. Собр. соч. в 10 томах. Т. 5. М.: ГИХЛ, 1960. 696 с.

5. Ишимбаева Г. Г. Фаустианская тема в немецкой литературе: диссертация на соискание учёной степени доктора филологических наук: 10.01.05. М.: 1999. 444 с.

6. Былевский П. Г. Культуроцентричный подход к развитию способностей как альтернатива «техноцентричному» трансгуманизму // Вестник Московского государственного университета культуры и искусств. 2023. № 1(111). С. 41–49. DOI 10.24412/1997–0803–2023–1111–41–49. EDN QPBYVK

7. Горький Максим / Большая Советская энциклопедия, 2-е издание. М.: ГНИ «Большая Советская энциклопедия», 1952. Т. 12. С. 247.

8. Schmidtke A., Häfner H. The Werther effect after television films: new evidence for an old hypothesis // Psychological Medicine 1988. Vol. 18. Iss.3. Pp. 665–676. DOI: https://doi.org/10.1017/S0033291700008345

9. Книгоиздание СССР. Цифры и факты. 19171987 / Е. Л. Немировский, М. Л. Платова. М.: Книга, 1987. С. 299.

10. Бубновский С. М. Методика Бубновского: краткий путеводитель. М: Издательство «Э», 2017. 128 с.

11. Ясперс Карл. Разум и экзистенция. М.: «Канон+», РООИ «Реабилитация», 2013. 336 с.

Об авторе

Былевский Павел Геннадиевич —
кандидат философских наук,
доцент кафедры международной
информационной безопасности,
Московский государственный
лингвистический университет
(Россия, Москва).
E-mail: pr-911@yandex.ru.

About the author

Pavel G. Bylevskiy —
Candidate of Philosophical Sciences,
Associate Professor
of the Department of International
Information Security,
Moscow State Linguistic University
(Russia, Moscow).
E-mail: pr-911@yandex.ru.