МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ВИНИТИ РАН)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. **№ 2** **Москва 2020**

ОБЩИЙ РАЗДЕЛ

УДК 004.021.056:001.103–047.44

О.В. Сюнтюренко

Использование методов аналитической постобработки данных для защиты ресурсов в системах коллективного пользования*

Исследуются теоретические и прикладные аспекты использования методов аналитической постобработки данных с помощью многомерного анализа данных, для защиты ресурсов в системах коллективного пользования. Рассматриваются новые подходы, алгоритмы и процедуры этого процесса на основе регистрационной статистики и многомерного анализа данных, позволяющие противодействовать реализации неявных, косвенных методов несанкционированного доступа (или иных действий) к информации. Предлагается методика оценки качества контролируемых показателей, а также стационарности состояния системы показателей, характеризующих «образ» пользователя в системе. Анализируются вопросы восприятия результатов постобработки данных лицом, принимающим решения (администратором службы безопасности). Представлена методика графической визуализации результатов регистрационно-аналитической обработки зафиксированных данных.

Ключевые слова: *аналитическая постобработка данных, система коллективного пользования, информационные ресурсы, анализ данных, риски и угрозы, несанкционированный действия, информационная безопасность, визуализация*

DOI: 10.36535/0548-0019-2020-02-1

* Статья подготовлена в рамках работ по гранту РФФИ № 20-07-00014 «Разработка методологии использования наукометрических данных для решения задач целеполагания, прогнозирования и управления научными исследованиями».

ВВЕДЕНИЕ

Лавинообразный рост цифровой среды, развитие телекоммуникационной инфраструктуры, широкое применение современных информационных технологий – все это потенциально создает предпосылки возникновения таких угроз, как утечка, хищение, искажение, подделка, копирование и блокирование информации и, как следствие – экономический, экологический, социальный и другие виды ущерба [1–7]. В разных странах регулярно регистрируются многочисленные попытки несанкционированного проникновения в информационные системы органов государственной власти и управления, факты кражи и компрометации экономической и финансовой информации, программного обеспечения систем электронных платежей и т.д. Уровень развития оперативных средств защиты системного программного обеспечения, особенно в современных СУБД типа *Oracle*, позволяет говорить о достаточно надежной защите информационных ресурсов от непосредственных попыток несанкционированного доступа. Однако возможна реализация неявных, косвенных методов несанкционированного доступа (или иных действий) к информации. Как правило, эти методы базируются на определенной априорной осведомленности потенциального нарушителя о характеристиках средств оперативной защиты и возможности логического вывода интересующих данных при применении продуманных стратегий работы с базами данных.

В корпоративных системах коллективного пользования (банки, научно-исследовательские организации, медицинские центры, промышленные корпорации, федеральная налоговая служба, госавтоинспекция и другие правительственные структуры) актуализируются риски несанкционированного использования информационных ресурсов, имеющие свою специфику. Следует отметить, что по оценкам *International Data Corporation* (IDC), цифровая корпоративная информация ежегодно растет на ~40% [6]. Особую напряженность в Социуме вызывают факты хищения и несанкционированного использования персональных данных, которые в последние годы имеют устойчивую тенденцию роста. В подавляющем большинстве случаев эти факты являются следствием противоправных, несанкционированных действий кадровых сотрудников организаций, прежде всего связанных с эксплуатацией, поддержкой и развитием компьютерных систем. Человеческий фактор представляется наиболее слабым и уязвимым звеном при решении задач обеспечения безопасности информационных систем. Далее мы рассмотрим подходы и методы противодействия неявным, скрытым несанкционированным действиям персонала с использованием методов постобработки данных на основе регистрационной статистики и многомерного анализа данных [8].

МЕТОДИКА ОЦЕНКИ КАЧЕСТВА ПОКАЗАТЕЛЕЙ УЧЕТА И КОНТРОЛЯ ПОДСИСТЕМЫ АНАЛИТИЧЕСКОЙ ПОСТОБРАБОТКИ ДАННЫХ

Регистрационно-аналитические средства подсистемы постобработки могут использоваться в двух основных направлениях – в плане защиты информации в локальных интерактивных информационных системах коллективного пользования (СКП) и в плане оптимизации использования информационных и вычислительных ресурсов СКП. Сформулируем принципы разработки и функционирования подсистемы аналитической постобработки регистрационной информации.

Первый принцип – заключается в автоматическом принятии решений о доступе к информации или о автоматической выдаче, в определенных ситуациях, рекомендаций лицу, ответственному за принятие решения. Он состоит в том, что регистрационно-аналитическая подсистема должна отслеживать квазиустойчивые параметры. Рассмотрим пример. Для случайной величины, распределенной по нормальному закону, квазиустойчивыми параметрами являются, например, математическое ожидание и дисперсия. Если вдруг они значимо изменяются, то это означает, что возникли причины, повлиявшие на характер распределения. Таким образом, если регистрационно-аналитическая подсистема определила, что произошло значимое изменение хотя бы одного параметра, то она вырабатывает санкционные процедуры и/или сообщение об этой ситуации для лица, принимающего решения. В качестве параметров такого типа могут использоваться значения определенных показателей или обобщенных факторов, например центроиды кластеров, частоты появления тех или иных признаков, тренды показателей и т.д.

Второй принцип состоит в модульности и программной независимости регистрационно-аналитических средств от программного обеспечения защищаемой системы. Сопряжение этих элементов обеспечивается программами, которые записывают информацию, поставляемую штатными средствами регистрации (на внешнем носителе в определенном формате). Остальные модули регистрационно-аналитической подсистемы работают только с этими форматированными данными. В силу значительного разнообразия состава решаемых функциональных задач, программно-технических средств, структур построения реальных систем коллективного пользования, не представляется возможным разработать унифицированные средства аналитической постобработки. Однако в настоящей статье представлен подход к реализации концептуального проектного решения регистрационно-аналитической подсистемы на основе использования методов многомерного анализа данных [9]. Виртуальная модель гипотетической подсистемы включает в себя комплекс функционально-ориентированных программных модулей, компонуемых со штатными средствами СКП в соответствии с целевыми задачами защиты информации.

Подсистема постобработки обеспечивает учет деятельности пользователя как в ходе сеанса, так и в течение более длительного периода его работы в рамках системы. Для формирования «образа» пользователя базы данных (банка данных, электронной библиотеки, архива) может использоваться ряд показателей, включающих, например, такие параметры, как: 1) число запросов (общее, за сеанс); 2) промежуток времени между запросами; 3) время между поступлениями разных задач (частота сменяемости задач); 4) число ошибок при идентификации; 5) число

нарушений полномочий; 6) время работы процессора для одного задания; 7) число операций чтения; 8) число операций корректировки; 9) число выполненных запросов; 10) число технических сбоев, приходящихся на задачу; 11) число записей (файлов), к которым пользователь обратился за время наблюдения.

Все эти показатели выбираются из системы средств регистрации. Наличие массива данных регистрационных программных средств позволяет реализовать следующие свойства и функциональные задачи подсистемы аналитической постобработки:

- отслеживать псевдоустойчивые параметры пользователя и определять значимость их значений по сравнению с базовыми временными интервалами;
- синтезировать показатели, описывающие информационное поведение пользователей на основе данных, предоставляемых штатными средствами регистрации;
- сжимать и подготавливать информацию к долговременному хранению;
- автоматически приводить в действие механизм принятия санкций и/или формировать рекомендации администратору службы безопасности.

Для выполнения этих функций подсистема аналитической постобработки должна реализовывать ряд статистических методов (процедур), позволяющих решать указанные задачи. Одна из важнейших задач – это формирование представительной системы показателей, характеризующих поведение пользователя. Учитывая значительный объем регистрируемых показателей, решение данной задачи состоит из двух частей:

1. Фильтрация малозначащих показателей. Необходимость фильтрации объясняется тем, что среди показателей могут встречаться равномерно распределенные, которые не влияют на функционирование системы и могут быть исключены из рассмотрения и анализа. Для проверки на равномерность может быть предложен такой метод: проверяется статистическая гипотеза о равенстве средних двух совокупностей, на которые разбита первоначальная совокупность. Они характеризуются средними $\overline{z}$, и дисперсиями σ_z^2, σ_u^2. Выдвигается гипотеза, что эти средние равны, т. е. $H_0 : \overline{z} = \overline{u}$. Для проверки этой гипотезы из каждой совокупности производится выборка: из первой – объемом a_1, в результате получаются $\overline{z^*}$ и G_z^2, из второй – объемом a_2, в результате получаются $\overline{u^*}$ и G_u^2, где G_z^2 и G_u^2 – дисперсии в двух выборках. По этим данным необходимо проверить основную гипотезу, для чего используется статистика:

$$\Phi = \left(\overline{z^*} - \overline{u^*}\right) \cdot \sigma^{-1} \left(\overline{z^*} - \overline{u^*}\right)^{-1}. \qquad (1)$$

Поскольку матожидание $M\left(\overline{z^*}\right) = \overline{z}$ и $M\left(\overline{u^*}\right) = \overline{u}$, то при справедливости гипотезы H_0 будем иметь M(Ф) = 0. Используя свойства дисперсии и полагая выборки независимыми, получим

$$\sigma^2\left(\overline{z^*} - \overline{u^*}\right) = \sigma^2\left(\overline{u^*}\right) + \sigma^2\left(\overline{z^*}\right) = \sigma_z^2 \cdot a_1^{-1} + \sigma_u^2 \cdot a_2^{-1}. \qquad (2)$$

При предположении равенства дисперсий, т.е. $\sigma_z^2 = \sigma_u^2 = \sigma^2$, получаем

$$\sigma^2\left(\overline{z^*} - \overline{u^*}\right) = \sigma^2\left(a_1^{-1} + a_2^{-1}\right). \qquad (3)$$

Подставляя в формулу (1) выражение (3) получим

$$\Phi = \left(\overline{z^*} - \overline{u^*}\right)\left(a_1^{-1} + a_2^{-1}\right)^{-1/2}. \qquad (4)$$

При выборках достаточно большого объема $\overline{z^*}$ и $\overline{u^*}$ распределены нормально, поэтому нормально будет распределена и Ф. Заменив неизвестную дисперсию генеральной совокупности σ^2 ее несмещенной выборочной оценкой

$$G^2 = \left[\sum\left(z_i - \overline{z^*}\right)^2 + \sum\left(u_i - \overline{u^*}\right)^2\right] \cdot (a_1 + a_2 - 2)^{-1} =$$
$$= \left(a_1 G_z^2 + a_2 G_u^2\right) \cdot (a_1 + a_2 - 2)^{-1}$$

приходим к нормально распределенному критерию

$$Y = \left[\left(\overline{z^*} - \overline{u^*}\right) \cdot \left(a_1 G_z^2 + a_2 G_u^2\right)^{-1/2}\right] \cdot \left[(a_1 + a_2 - 2)^{1/2} \cdot \left(a_1^{-1} + a_2^{-1}\right)^{-1/2}\right]. \qquad (5)$$

В общем случае для проверки равномерности могут быть использованы и другие статистические критерии.

Равенство средних является признаком равномерности распределения, и этот показатель исключается из дальнейшего рассмотрения.

2. Выделение групп сильно коррелирующих факторов. После отсеивания равномерно распределенных параметров встает задача выделения групп сильно коррелирующих факторов, каждая из которых может быть заменена одним новым «синтетическим» фактором. Таким образом осуществляется сокращение размерности системы показателей. Для этого мы предлагаем использовать метод главных компонентов, выделяющий некоторые скрытые закономерности, представляющие собой линейные комбинации исходных параметров. Метод главных компонентов заключается в следующем. Некая гипотетическая система описана с помощью n характеристик. Предполагается, что изменения этих характеристик есть реализация случайных величин $x_i, \left(i = \overline{1,n}\right)$, о распределении которых нет никаких предположений, кроме равенства нулю средних. Предполагается также, что система подвергается воздействию таких скрытых, но объективно существующих закономер-

ностей. Отыскание этих закономерностей является *первой задачей* метода главных компонентов. *Вторая задача* – описание изучаемой системы числом главных компонентов *m*, значительно меньшим, чем число первоначально выбранных характеристик *n*. Практические возможности решения этих задач могут быть реализованы в следующих направлениях: 1) сжатие исходной информации; 2) классификация объектов наблюдения; 3) ранжирование объектов или наблюдений по главным компонентам.

В нашем случае метод главных компонентов обладает определенным преимуществом перед другими методами факторного анализа. Он не требует никаких гипотез о переменных, является линейным и аддитивным.

Алгоритмически метод реализуется следующим образом.

Шаг 1 – по заданным наблюдениям рассчитывается корреляционная матрица.

Шаг 2 – матрица корреляций приводится к виду ортогонально подобной ей диагональной, где элементы по главной диагонали есть собственные числа матрицы корреляций.

Шаг 3 – определяется факторная матрица, т.е. матрица, где выявляются нагрузки на выбранные главные компоненты.

Шаг 4 – с помощью итерационной процедуры (алгоритма Хотеллинга) производится вращение матрицы для ориентации ее в направлении главных компонентов, имеющих наибольшие факторные нагрузки.

С точки зрения классификации и отсеивания незначащих показателей методом главных компонентов могут быть рекомендованы три направления:

- если в главные компоненты те или иные показатели входят с высокой факторной нагрузкой (например, более 0,75), то эти показатели связаны между собой и значимы для описания объекта;
- выделяются главные компоненты, имеющие наибольшую факторную нагрузку (например, более 80%), и анализируются определяющие их исходные показатели;
- если те или иные показатели входят в главные компоненты с высокой факторной нагрузкой, но сами главные компоненты не вносят значительного вклада в суммарную дисперсию, то эти параметры не являются важными для описания объекта и могут быть отсеяны.

Для решения задач сокращения размерности исходной системы показателей и формирования их представительной совокупности, имеется ряд методов, в определенной степени связанных с факторным. К таким методам могут быть отнесены:

кластерный анализ – его задача состоит в разбиении множества точек так, чтобы каждая точка принадлежала одному и только одному подмножеству разбиения. При этом в каждом подмножестве разбиения точки лежат плотно друг к другу и являются сходными, в то время как точки, принадлежащие разным подмножествам, разнородны. В качестве меры близости точек в кластерном анализе обычно используются следующие критерии:

а) евклидово расстояние

$$d_{ij}^2 = \sum_{l=1}^{P} \left(x_{il} - x_{jl}\right)^2 \ ;$$

б) взвешенное евклидово расстояние

$$d_{ij}^2 = \sum_{l=1}^{P} \omega_i \left(x_{il} - x_{jl}\right)^2 ;$$

в) расстояние Махалонобиса (оно отличается от евклидова расстояния) тем, что учитывает корреляции между переменными и инвариантно к масштабу)

$$d_{ij}^2 = \left(x_i - x_j\right)^T S^{-1} \left(x_i - x_j\right) ,$$

где S^{-1} – матрица, обратная ковариационной;

г) коэффициент корреляции

$$d_{ij}^2 = \left\{ \left[\left(x_{il} - \overline{x_l}\right)\left(x_{jl} - \overline{x_l}\right) \right] \cdot \left(\sigma_i \cdot \sigma_j\right)^{-1} \right\}^{1/2} .$$

В общем случае задача кластерного анализа сводится к разработке определенного правила или алгоритма, с помощью которого можно осуществлять разбиение точек на группы. При этом остается неизвестно, действительно ли найденные группировки являются наилучшими. В кластерном анализе при построении процедуры группировки используется *R* – коэффициент или коэффициент принадлежности

$$R = 100 \left(\frac{\begin{array}{c}\textit{средний коэффициент корреляции между} \\ \textit{переменными одной группы}\end{array}}{\begin{array}{c}\textit{средний коэффициент корреляции переменных} \\ \textit{этой группы с остальными переменными}\end{array}} \right) \quad (6)$$

При этом не разработано никакого удовлетворительного статистического критерия, который позволял бы оценить приведенное разбиение и принадлежность точки к определенной группе.

анализ образов – это изучение структуры количественных данных, исходя из коэффициентов множественной регрессии. Каждую переменную предлагается оценивать с помощью метода множественной регрессии по остальным (*m*-l) переменным. Основная цель множественной регрессии – построить модель с большим числом факторов, определив при этом влияние каждого из них в отдельности, а также совокупное их воздействие на моделируемый показатель [10].

В некоторых случаях, в связи с относительно большой вычислительной сложностью изложенных процедур, средства программной поддержки целесообразно использовать в виде стандартных программ в соответствующих пакетах [11, 12].

МЕТОДИКА ОЦЕНКИ СТАЦИОНАРНОСТИ СОСТОЯНИЯ СИСТЕМЫ ПОКАЗАТЕЛЕЙ, ХАРАКТЕРИЗУЮЩИХ ПОЛЬЗОВАТЕЛЯ

Подсистема постобработки данных должна отслеживать квазиустойчивые параметры. Например, для случайной величины, имеющей нормальный закон распределения, такими параметрами являются математическое ожидание и дисперсия. Значительное изменение этих параметров означает, что возникли причины, изменившие характер распределения. В свою очередь, стабильность параметров соответствует определенной модели поведения пользователя. Изменение этой модели может быть вызвано, в частности, попыткой несанкционированного доступа. Таким образом, если регистрационно-аналитическая подсистема определила, что произошло значимое изменение хотя бы одного из таких параметров, то она реализует санкционные процедуры и/или формирует сообщение об этой ситуации для лица, принимающего решения. Отсюда вытекает необходимость оценки стационарности системы показателей, которая позволит определенным образом делать выводы о поведении пользователей. Под стационарностью понимается устойчивость статистических характеристик системы во времени. Поскольку показатели, выбираемые из системных средств защиты, представляют собой реализацию случайных величин, то для проверки на стационарность предлагается использовать гипотезу о сравнении долей признака в двух совокупностях.

Пусть $\frac{m_1}{n_1}$ и $\frac{m_2}{n_2}$ – частности одного и того же признака в двух совокупностях из n_1 и n_2. Гипотезой H_0 является предположение, что обе совокупности представляют собой две выборки из одной генеральной совокупности с некоторой долей признака ρ, а отмеченное расхождение выборочных частностей есть результат случайностей, сопровождающих отбор. При построении критерия проверки различаются большие и малые выборки.

1. Большие выборки. Если n_1 и n_2 – большие числа (примерно более 30), то распределение выборочных частностей будет близко к нормальному с параметрами

$$M\left(m_1 n_1^{-1}\right) = M\left(m_2 n_2^{-1}\right) = \rho,$$

и дисперсиями

$$\sigma^2\left(m_1 n_1^{-1}\right) = \rho(1-\rho)\cdot n_1^{-1},\ \sigma^2\left(m_2 n_2^{-1}\right) = \rho(1-\rho)\cdot n_2^{-1}.$$

Введем для проверки гипотезы статистику

$$\theta = \left(m_1 n_1^{-1}\right) - \left(m_2 n_2^{-1}\right).$$

При справедливости гипотезы H_0 значение θ может лишь случайно отличаться от нуля. Статистика θ также подчиняется нормальному закону с параметрами:

$$M(\theta) = M\left[\left(m_1 n_1^{-1}\right) - \left(m_2 n_2^{-1}\right)\right] =$$
$$= M\left(m_1 n_1^{-1}\right) - M\left(m_2 n_2^{-1}\right) = \rho - \rho = 0;$$

$$\sigma^2(\theta) = \sigma^2\left[\left(m_1 n_1^{-1}\right) - \left(m_2 n_2^{-1}\right)\right] =$$
$$= \sigma^2\left(m_1 n_1^{-1}\right) - \sigma^2\left(m_2 n_2^{-1}\right) = \rho(1-\rho)\left(n_1^{-1} - n_2^{-1}\right).$$

Далее переходим к проверке нулевой гипотезы с помощью двустороннего критерия, который диктуется смыслом проверки. Задавшись уровнем значимости $\propto$, найдем $z_{\propto/2}$ из уравнения

$$\rho\left\{|\theta| < z_{\propto/2}\sigma(\theta)\right\} = 2\Phi(t) = 1 - \propto. \qquad (7)$$

Исходя из уравнения (7) получим критические точки

$$\theta_1 = -z_{\propto/2}\left[\rho(1-\rho)\right]^{1/2}\left(n_1^{-1} + n_2^{-1}\right)^{1/2},$$
$$\theta_2 = z_{\propto/2}\left[\rho(1-\rho)\right]^{1/2}\left(n_1^{-1} + n_2^{-1}\right)^{1/2},$$

где величину ρ заменяем ее оценкой на основании данных двух выборок

$$\rho = (m_1 + m_2)\cdot(n_1 + n_2)^{-1}.$$

Правило проверки: если выборочное значение θ^* лежит в интервале (θ_1, θ_2), то гипотеза H_0 не отклоняется, т.е. расхождение между $\frac{m_1}{n_1}$ и $\frac{m_2}{n_2}$ несущественно; если θ^* окажется вне этого интервала, то H_0 отклоняется, т.е. расхождение между $\frac{m_1}{n_1}$ и $\frac{m_2}{n_2}$ можно рассматривать как значимое.

2. Малые выборки. На практике это более сложный случай. Если n_1 и n_2 – малые числа, то использование нормального распределения для статистики $\theta = \left(m_1 n_1^{-1}\right) - \left(m_2 n_2^{-1}\right)$ становится некорректным. В этом случае пользуются критерием χ^2, с помощью которого оценивается расхождение между теоретическими и выборочными частотами. Критерий χ^2 вычисляется следующим образом: через $\overline{m_1}$

и $\overline{m_2}$ обозначается число элементов, не обладающих признаком *A*. Если это выборки из одной и той же генеральной совокупности с долей признака ρ, то можно определить теоретические частоты ρn_1, $(1-\rho)n_1$, ρn_2, $(1-\rho)n_2$. При этом для ρ принимается оценка $\rho = (m_1 + m_2)\cdot(n_1 + n_2)^{-1}$. Вычисляем χ^2 по формуле

$$\chi^2 = (m_1 - \rho n_1)^2 (\rho n_1)^{-1} +$$
$$+\left[m_1 - (1-\rho)n_1\right]^2 \left[(1-\rho)n_1\right]^{-1} +$$
$$+\left[(m_2 - n_2\rho)\right]^2 (\rho n_2)^{-1} +$$
$$+\left[m_2 - (1-\rho)n_2\right]^2 \left[(1-\rho)n_2\right]^{-1}$$

При этом, так как между четырьмя теоретическими частотами существуют три независимых соотношения, то независимой является только одна величина, т.е. в распределении χ^2 следует учесть одну степень свободы $(\nu = 1)$.

Если нулевая гипотеза (согласно которой обе совокупности есть выборки из одной генеральной совокупности) верна, то расхождение между теоретическими и опытными частностями можно отнести только к случайностям отбора. Поэтому, определив для данного уровня значимости $\propto$ значение χ_0^2, примем решение об отклонении гипотезы H_0, если $\chi^2 > \chi_0^2$, и о не значимости расхождений, если $\chi^2 \le \chi_0^2$.

Такая проверка позволяет определить стационарность представленной системы показателей и делать выводы о поведении пользователей, не проводя объемных расчетов всех показателей.

МЕТОДИКА ВИЗУАЛИЗАЦИИ РЕЗУЛЬТАТОВ РЕГИСТРАЦИОННО-АНАЛИТИЧЕСКОЙ ОБРАБОТКИ ДАННЫХ

В системах с постобработкой одной из важнейших задач является восприятие информации лицом, принимающим решения (администратором службы безопасности). Это связано с тем, что данные, выдаваемые системными средствами, имеют большой объем и представлены не в наглядной форме. Одной из задач постобработки является визуализация имеющихся данных, т.е. представление их в форме, удобной для восприятия человеком. Для этой цели используются методы математической статистики (метод главных компонентов, кластер-анализ), которые решают задачу визуализации путем сокращения размерности системы исходных показателей и выявления внутри ее скрытых закономерностей. Большое значение имеют также методы графического представления системы исходных показателей как с помощью обычных графиков, так и с помощью разного рода гистограмм [13].

В различных пакетах прикладных программ используются разные средства визуализации исходной системы показателей. С помощью графиков возможно визуализировать информацию о поведении пользователя в процессе работы с базами данных. Например, может быть дана оценка разнообразия информационных потребностей пользователя.

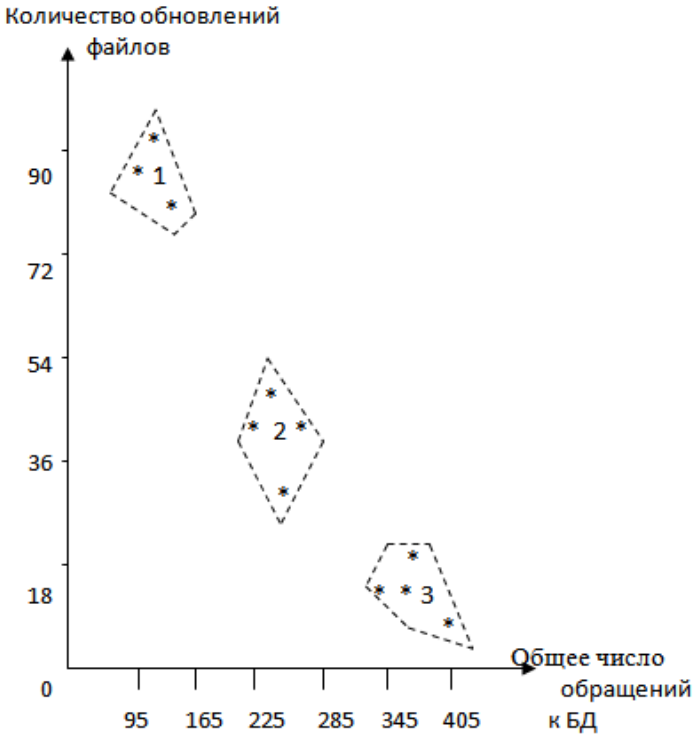


Рис. 1. Визуализация взаимосвязи количества обновлений файлов и общего числа обращений к БД

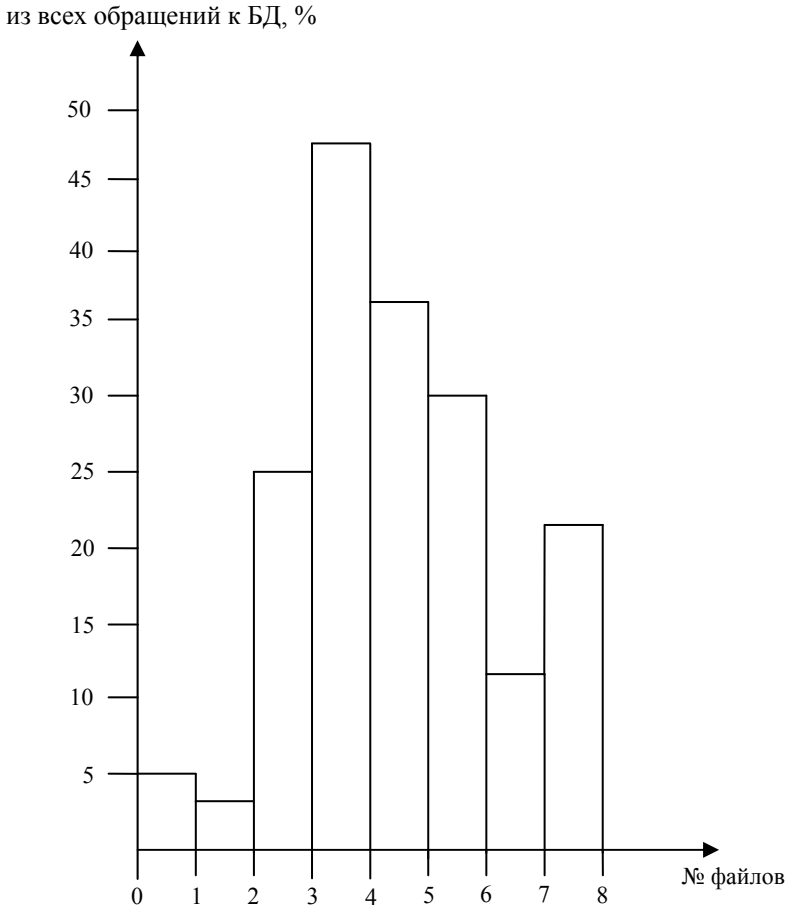


Рис. 2. Распределение по файлам общего количества обращений к БД

Значительный интерес представляет распределение во времени количества обращений к информационным ресурсам системы. Визуализация распределения результатов регистрационно-аналитической обработки информации дает возможность наглядно представлять и группировать пользователей по количеству обращений к базам данных. Такая информация позволяет анализировать взаимность продолжительности работы и ее интенсивность, что может косвенно указывать на попытки доступа к запрещенной информации. Важно также выявить взаимосвязи между количеством обновлений файлов и общим числом обращений к базе данных (рис. 1). Установление такой взаимосвязи позволяет создать «образ» пользователя и по нему делать выводы о способе действий с БД. Например, пользователь, который мало обращается к базе и часто обновляет файлы, может представлять собой потенциального нарушителя. Определенный интерес при анализе деятельности пользователей имеет оценка частоты обращения к файлам (записям) базы данных. Возможность такой оценки связана с тем, что важность файлов, с точки зрения сохранения конфиденциальности (секретности) информации, может быть неодинакова, что можно показать на гистограмме распределения общего количества обращений к базе данных по файлам (рис. 2).

Применение перечисленных методов визуализации результатов аналитической постобработки информации позволяет облегчить анализ накопленной регистрационной информации, повысить эффективность процессов принятия решений администратором службы безопасности организации.

ЗАКЛЮЧЕНИЕ

Несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей не уменьшается, а имеет тенденцию к нарастанию различного рода рисков и угроз. Основными факторами, способствующими повышению уязвимости информации, являются: рост объемов информации в интегрированных базах данных, представляющей интерес для значительного числа пользователей (как легитимных, так и не имеющих права доступа к ней); развитие телекоммуникационных режимов обработки информации (в сетях Интернет и Интранет); расширение круга пользователей банков данных систем коллективного пользования.

В последнее время в России повышение интереса к проблематике информационной безопасности объясняется главным образом интенсификацией процессов информатизации государственных органов (в том числе МВД, вооруженных сил) [14], банковского и страхового бизнеса, развитием крупных коммерческих структур, а также повышением уровня криминогенной обстановки и террористических угроз в сетевой среде.

Рассмотренные в настоящей статье методы постобработки регистрационной информации позволяют реализовывать выявление скрытых, неявных несанкционированных действий в системах коллективного пользования, осуществляемых сотрудниками организаций (связанных с эксплуатацией, поддержкой и развитием компьютерных систем) и которые не обнаруживаются обычными оперативными программными средствами разграничения доступа к информации. Процедуры и алгоритмы, реализуемые на основе рассмотренных методов многомерного анализа данных, имеют хорошую перспективу применения в различных приложениях в системах компьютерной логики, искусственного интеллекта, в рамках развития аналитических технологий Больших Данных.

В области оперативных средств перспективное направление разработок состоит в создании «безопасных» аппаратных средств, «безопасных» операционных систем (например, на базе *Unix*) и СУБД, т.е. в автоматизации средств защиты на всех уровнях доступа к информационным и вычислительным ресурсам систем коллективного доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Хоффман Л.Дж. Современные методы защиты информации. – М.: Советское радио, 1980. – 263 с.
2. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности // Вестник РФФИ. – 1999. – № 3(17). – С. 63–68.
3. Siountiourenko O. The Problems of Providing Information Security: The Case of Information Infrastructure / ed. Gerhard Banse // Studies in Eastern Europe. Technological and nvironmental Policy. – Berlin, 2007. – P. 161–179.
4. Акопян Д.А., Еляков А.Д. Киберпреступления в информационной инфраструктуре общества (Обзор) // Научно-техническая информация. Сер. 1. – 2009. – № 12. – С. 1-14.
5. Сюнтюренко О.В. Социальные и экономические риски развития информационных технологий // Научно-техническая информация. Сер.1. – 2012. – № 6. – С. 1-5; Syuntyurenko O.V. The Social and Economic Risks of the Development of Information Technologies // Scientific and Technical Information Processing. – 2012. – Vol. 39, № 2. – P. 113-116.
6. Сюнтюренко О.В. Цифровая среда: тренды и риски развития // Научно-техническая информация. Сер. 1. – 2015. – № 2. – С. 1 -7; Syuntyurenko O.V. The Digital Enviroment: The Trends and Risks of Development // Scientific and Technical Information Processing. – 2015. – Vol. 42, № 1. – P. 24-29.
7. Арутюнов В.В. О некоторых результатах приоритетных исследований в области информационной безопасности // Научно-техническая информация. Сер. 1. – 2016. – № 2. – С. 8-13.
8. Сюнтюренко О.В. Теоретические и прикладные аспекты автоматизации процедур многомерного анализа данных // Научно-техническая информация. Сер. 2. – 2018. – № 11. – С. 1-8; Syuntyurenko O.V. Theoretical and Applied Aspects of Automating Multivariate Analysis Procedures // Automatic Documentation and Mathematical Linguistics. – 2018. – Vol. 52, № 6. – P. 275-281
9. Сюнтюренко О.В. Цифровая среда: аналитическая постобработка информации с использованием методов наукометрии и анализа данных // Научно-техническая информация. Сер. 1. – 2019. – № 4. – С. 8-16; Syuntyurenko O.V. Digital Enviroment: Information Analytical Postprocessing Using the Scientometric and Data Analysis Methods // Scientific and Technical Information Processing. – 2019. – Vol. 46, № 2 – P. 59-66.
10. Множественная линейная регрессия. Улучшение модели регрессии. – URL: https://function-x.ru/statistics_regression2.html (дата обращения 12.06.2019).
11. Шарстнев В.Л., Вардомацкая Е.Ю. и др. Пакеты прикладных программ для статистического анализа данных. – URI: https://rep.vstu.by/handle/123456789/1746 (дата обращения 06.06.2019).
12. Величко В.В. Сравнительный анализ статистических пакетов программ. – URL: https://cyberleninka.ru/article/n/sravnitelnyy-analiz-statistiches-kin-paketov-programm (дата последнего обращения 06.03.2019).
13. Клышинский Э.С., Рыасков С.В., Шихов А.И. Обзор методов визуализации многомерных данных. – URL: https://cyberleninka.ru/article/n/obzor-metodov-visualizatsii-mnogomernyh-dannyh (дата последнего обращения 07.03.2019).
14. Национальная Программа «Цифровая экономика Российской Федерации»; утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. N 1632-р. – URI: static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf(дата обращения 27.12.2019).

Материал поступил в редакцию 17.01.20.

Сведения об авторе

СЮНТЮРЕНКО Олег Васильевич – доктор технических наук, профессор, ведущий научный сотрудник ВИНИТИ РАН, Москва
e-mail: olegasu@mail.ru

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ РАБОТЫ

УДК 336.563.1(470):[002:004.65]-047.44

И.А. Стерлигов, Т.Ф. Савина, А.О. Чичкова

Исследование грантовой поддержки российскими научными фондами отечественных публикаций в ведущих международных журналах (по материалам *Scopus* и *Web of Science*, РФФИ и РНФ)*

Представлен наукометрический анализ информации о грантах в публикациях с российской аффилиацией в ведущих научных журналах, проиндексированных одновременно в этих ведущих базах: Scopus и Web of Science. На основе метаданных массива российских публикаций в журналах Nature Index за 2014-2017 гг. проведено сравнение полноты данных о грантовых фондах в двух базах и выделены фонды и организации России с наибольшим числом таких публикаций. Проанализирована грантовая поддержка публикаций ведущих вузов России, исследована динамика активности как российских, так и зарубежных фондов, а также международное соавторство. Сделаны выводы о существенном превосходстве Web of Science по полноте индексации информации, а также о том, что число публикаций с указанием РФФИ в качестве грантодателя ранее превышало число публикаций с указанием РНФ, но в последнее время тенденция поменялась: РНФ стал заявляться в большем числе публикаций при сохранении значимой роли иностранных грантодателей. Дополнительно намечены направления сравнительного анализа цитируемости в зависимости от грантодателя.

Ключевые слова: *база Scopus, база Web of Science, грантовые фонды, Nature Index, университеты, Российский научный фонд, Российский фонд фундаментальных исследований, наукометрия*

DOI: 10.36535/0548-0019-2020-02-2

ВВЕДЕНИЕ

Грантовое финансирование – важнейший канал поддержки научных исследований, крайне значимый для фундаментальной науки. Для России развитие этого инструмента особенно важно: исторически в период СССР гранты в нынешнем понимании фактически отсутствовали, но после слома советской модели организации науки сразу были определены как один из наиболее перспективных форматов финансирования [1, 2]. К началу 2010-х гг. они превратились в систему фондов и программ, которые – во всяком случае гранты Российского фонда фундаментальных исследований (РФФИ) и Российского научного фонда (РНФ) – высоко оцениваются самими учеными и научными организациями [3].

Для анализа работы грантовых фондов и их роли в развитии российской и мировой науки особое значение в последние годы приобретает наукометрия. Современные базы научного цитирования индексируют названия грантодателей и номера грантов в конкретных публикациях. Это позволяет связать финансирование и результативность исследований, которая для фондов, сконцентрированных на поддержке фундаментальной науки, фактически определяется характеристиками рецензируемых научных публикаций, прежде всего индексируемых этими базами данных. Наукометрия позволяет выявлять не только количество статей, но и сравнивать их цитируемость, уровень журналов, наличие и состав соавторов, тематику и многое другое, а эти объективные данные очень важны для выработки и корректировки стратегий фондов и государственной научной политики в целом. Соответствующий прикладной анализ, как

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-311-00289\18.

правило на данных базы *Web of Science* (*WoS*), проводился ведущими грантодателями Европы и США [4], но для России это направление фактически является новым, об опубликованных докладах российских грантодателей, аналогичных приведенному, нам неизвестно.

В мировом академическом науковедении изучение финансирования науки через метаданные публикаций развивается достаточно активно в силу большой практической и фундаментальной значимости. За последние годы можно выделить серию исследований в этой области, но все они, кроме работы [5], базируются на иностранных массивах данных, преимущественно взятых из базы данных (БД) *WoS*. Все эти статьи можно разделить на две большие группы: 1) предлагающие новый подход к методологии и 2) прикладные, использующие инструменты работы с базами данных для предоставления новых результатов по статистике или же описывающие интересные, замечательные чем-либо отдельные случаи.

Выделим сначала труды технического характера, анализирующие текстовую информацию о наличии грантовой поддержки в графе *Funding Acknowledgments* (*FA*). В статье [6] введен новый подход к обнаружению текстовых паттернов в разделе о финансовой поддержке на примере вышедших в 2010 г. и проиндексированных в БД *WoS* англоязычных публикаций испанских исследователей. Для таких статей были выявлены различия по предметной области, числу авторов и импакт-фактору журналов. Авторы публикации [7] анализируют наличие и распределение данных об источнике проектного финансирования на основе данных *WoS* в разрезах типов документов и трех индексов цитирования: *SCIE*, *SSCI*, *A&H*, входящих в *WoS Core Collection*. В статье [8] дается наиболее полная картина разнообразия спонсоров, участвующих в системах финансирования, на примере 7510 публикаций 2011 г. об исследованиях рака, проиндексированных в базах *Web of Science* и *MEDLINE/PubMed* и выполненных британскими авторами, и делается вывод о том, что база *WoS* корректно отражает информацию о грантовой поддержке публикаций с хотя бы одним грантодателем в 93% случаев и ошибочно приписывает данные о грантодателях для публикаций с отсутствующими записями о грантовой поддержке в полном тексте почти в 6% случаев.

Из более прикладных можно выделить несколько основных работ. Целью исследования [9] было изучение взаимосвязи количества источников финансирования, указанного в публикации, и цитируемостью публикаций на примере статей журналов «*Cell*» и «*Physical Review Letters*», вышедших в 2009 г. Для статей журнала «*Physical Review Letters»* выявлена относительно слабая положительная взаимосвязь исследуемых объектов, для статей журнала «*Cell*» такая связь не выявлена. В статье [10] составлен запрос по поиску *Funding Acknowledgements* в базе данных *WoS*, и дано распределение числа публикаций в индексах *SCIE*, *SSCI*, *A&H* по языку и типу *acknowledgement*. С целью изучения полноты и точности *WoS* при извлечении и обработке данных об источнике проектного финансирования в работе [11] анализируется случайная выборка статей с аффилиацией Испании, опубликованных в 2014 г. по восьми тематическим областям. Авторы [12] используют свойства сети цитирований академических статей, чтобы классифицировать направления исследований по нескольким категориям в зависимости от их цели и новизны основной литературы по теме. Затем, используя информацию о грантовых фондах, авторы рассматривают их участие в каждой из категорий исследования. Статья примечательна еще и тем, что рассматривает дополнительно базу *PubMed*. В [13] представлена динамика распределения фондовых средств в сфере аналитики данных о пациентах в медицине. В [14] рассматривается финансирование масштабных исследований в университетах стран коалиции *G*9 и сопоставляются государственные и частные фонды. Авторы [15] на примере небольшого числа публикаций, имеющих грантовую информацию и индексируемых в трех базах *Scopus*, *Web of Science* и *MEDLINE* за 2015 г. из 28 престижных медицинских журналов, показывают, что различия в покрытии грантовой информации между этими тремя базами статистически значимы, а наиболее полную индексацию обеспечивает *WoS*.

России посвящена лишь работа [5], в которой анализируется массив публикаций с российской аффилиацией за 2009 г., отраженных в двух индексах базы *WoS* (*SCIE, SSCI*) и содержащих информацию о грантодателе. На основе метаданных 14471 публикации было выделено 1975 грантодателей, среди которых 145 представляют собой российские грантовые фонды или организации. По результатам этого анализа Российский фонд фундаментальных исследований является безоговорочным лидером в поддержке отечественных научных исследований и на него приходится 62% публикаций, а почти 46% статей содержат информацию об иностранном грантодателе.

Более свежих публикаций, посвященных России, нами не найдено, и наша работа призвана восполнить этот пробел. С момента выхода указанной статьи В.А. Маркусовой с коллегами произошло много изменений, а в нашем контексте наиболее важные – повсеместное распространение в российской научной политике и менеджменте науки конкурента *WoS* – БД *Scopus*, и создание Российского научного фонда, претендующего на роль главного грантодателя в отечественной фундаментальной науке [16]. Поэтому в своем исследовании мы ставим цель не просто *выявить и сравнить основных грантодателей*, упоминаемых в российских публикациях, но и *сопоставить эти публикации по полноте индексирования их метаданных FA в WoS и Scopus*.

База *Scopus* широко используется в оценке исследований во всем мире наряду с *Web of Science* и *Google Scholar*, являясь одним из общепринятых источников библиометрических данных [17]. Авторы статьи [18] установили, что *Scopus* демонстрирует «более широкий охват журналов во всех областях науки», и именно охват – scope – является основным маркетинговым преимуществом системы. Несмотря на то, что *Web of Science* представляется более избирательной с точки зрения количества проиндексированных журналов, она позиционирует себя как «тщательно отобранная, активно курируемая база данных

журналов, которые сами исследователи считают самыми важными и полезными в своих областях»[1]. *Scopus*, благодаря своему более широкому охвату, заменила *WoS* в качестве источника данных для влиятельных рейтингов университетов *Times Higher Education* и используется в этом качестве в рейтингах университетов *QS*, на которые ориентируются ведущие российские вузы. Значимость этой базы как инструмента анализа публикационной активности в российском контексте особенно велика, что отражает и вхождение индикаторов *Scopus* в состав официального Мониторинга эффективности деятельности организаций высшего образования[2].

Для сравнения *WoS* и *Scopus* мы выбрали наиболее избранные журналы мира, отобранные внешними экспертами: во-первых, эти журналы индексируются в обеих базах, во-вторых, именно в них как в наиболее престижных и читаемых изданиях должны публиковаться результаты лучших исследований, поддержанных грантами, в-третьих, все эти журналы издаются на высоком технологическом уровне, их отличает внимание к структуре научного текста и его оформлению, в том числе – тщательное указание интересующих нас *Funding Acknowledgements*.

Оценив применимость *Scopus* и *WoS*, мы проанализировали публикации не только по грантодателям, но и по ведущим университетам, т.е. организациям, на которые сейчас направлен основной фокус отечественной государственной политики по развитию науки [16].

Но прежде чем перейти к описанию нашей методики исследования и полученным результатам, необходимо кратко представить основных российских грантодателей и показать использование ими библиометрии, так как именно грантовые фонды здесь являются главными игроками.

ОСНОВНЫЕ РОССИЙСКИЕ ГРАНТОДАТЕЛИ

Грантовая система финансирования науки в России находится в стадии совершенствования и ее функционирование связано со спецификой экономической, политической и культурной ситуации в стране. Российский фонд фундаментальных исследований и Российский научный фонд составляют основу национальной грантовой системы, роль и известность остальных участников гораздо меньше [3]. В последние годы оба фонда в своей работе активно применяют библиометрические показатели в качестве как входных барьеров, так и в качестве требований к отчетности и результатам.

РФФИ создан в 1992 г. по инициативе крупнейших ученых страны по модели *National Science Foundation* (США). Фонд проводит разнообразные конкурсы по поддержке фундаментальных научных исследований, по организации российских и международных научных мероприятий, по изданию научных трудов, экспедициям и полевым исследованиям. Объем грантового финансирования варьируется в зависимости от проекта. Например, с 2018 г. объем финансирования конкурса проектов фундаментальных научных исследований, выполняемых молодыми учеными («Мой первый грант»), составляет 500 тыс. руб. ежегодно, а максимальный объем финансирования конкурса на лучшие научные проекты, выполняемые ведущими молодежными коллективами («Стабильность»), – 6 млн руб. на срок два года. Больше всего грантов выдается в рамках «Конкурса на лучшие проекты фундаментальных научных исследований» (от 700 тыс. до 1 млн руб. в год на коллектив в 2018 г.).

Российский научный фонд создан гораздо позднее, в 2013 г. Средний объем финансирования каждого проекта существенно выше, чем РФФИ (1,5 млн руб. ежегодно по мероприятию «Проведение инициативных исследований молодыми учеными», 30 млн руб. ежегодно по мероприятию «Проведение исследований научными лабораториями мирового уровня в рамках реализации приоритетов научно-технологического развития Российской Федерации»)[3]. Такой беспрецедентный для России объем грантов вызвал большой интерес ученых: согласно социологическому опросу 2015 г. [19] (порядка 500 участников), почти 40% респондентов подали заявки на участие в конкурсах РНФ в 2014 г., т. е. в первый год его функционирования. По данным [20] в 2014 г. средняя стоимость одного проекта в РНФ составляла 7 млн руб., в РФФИ – 0,55 млн руб. По данным отчетов фондов[4] в 2018 г. средняя стоимость одного проекта в РНФ по сравнению с 2014 г. снизилась и составила 5,35 млн руб., в РФФИ – 1,01 млн руб.

По официальным и открытым данным объем финансирования конкурсов РФФИ составил 10,99 млрд руб. в 2016 г. и 18 млрд руб. в 2017 г.[5], для РНФ в 2016 г. объем финансирования был более 15 млрд руб.[6], а в 2017 г. – 18,5 млрд руб.[7]. Согласно закону 459-ФЗ «О федеральном бюджете на 2019 год и на плановый период 2020 и 2021 годов», ассигнования на РФФИ составят в 2019 г. 22,22 млрд руб. По Программе деятельности РНФ на 2019-21 гг. ассигнования составят в 2019 г. 20,8 млрд руб.

Резюмируя, сейчас фактически можно говорить о примерно одинаковом размере общего финансирования двух фондов, при этом РФФИ дает много небольших грантов, а РНФ – мало больших, что согласуется с нашими предварительными результатами о частоте упоминаемости фондов в публикациях в топовых журналах (табл. 1).

---

[1] См. http://clarivate.com/?product=web-of-science

[2] Документация и результаты мониторинга размещены на портале http://indicators.miccedu.ru/monitoring/

[3] Сам фонд в информационном буклете, размещенном на сайте http://www.rscf.ru/ru/activity/, сообщает: «Гранты РНФ являются одними из самых крупных среди распределяемых государственными фондами – от 2 до 150 млн рублей ежегодно, что создает комфортные условия для ученых и позволяет проводить исследования без привлечения дополнительных средств. При этом ученый берет на себя обязательство опубликовать результаты своих исследований в высокорейтинговых научных журналах. Количество таких публикаций ученый определяет сам на стадии подачи заявки».

[4] См. «Отчет Президенту Российской Федерации о деятельности Российского фонда фундаментальных исследований в 2018 году» (https://www.rfbr.ru/), «Информация о деятельности Фонда в 2018 году» (http://www.rscf.ru/fondfiles/documents/otchet-RSF-2018.pdf),

[5] См. https://tass.ru/nauka/2714633

[6] См. рнф.рф/ru/node/2318, https://tass.ru/nauka/5087376

[7] См. https://tass.ru/nauka/5087376

Таблица 1

Основные характеристики РНФ и РФФИ

	РФФИ	РНФ
Дата создания	1992	2013
Декларируемая цель работы	поддержка научно-исследовательских работ по всем направлениям фундаментальной науки на конкурсной основе, направленная на построение новых отношений между учеными и государством	финансовая и организационная поддержка фундаментальных научных исследований и поисковых научных исследований, подготовки научных кадров, развития научных коллективов, занимающих лидирующие позиции в определенной области науки
Объем финансирования в 2018 г. (тыс. руб.)	19126608,80	21400000
Общее количество грантов за 2018 г.	18904	4000

Еще один важный для России источник грантового финансирования, нацеленный на публикации в лучших журналах – так называемые мегагранты, т.е. гранты Правительства РФ для государственной поддержки научных исследований, проводимых под руководством ведущих ученых, инициированные Постановлением Правительства от 9 апреля 2010 г. №220. Конкурс мегагрантов проводился с 2010 по 2017 гг. включительно[8]. Основными задачами стало привлечение ученых с мировым именем, создание научных лабораторий и получение научных результатов мирового уровня. В разные годы финансирование проектов составляло от 120 до 90 млн руб. на три года, число победителей – порядка 40 в каждой из шести волн.

Крупных иностранных грантодателей, напрямую системно выделяющих средства российским ученым на проведение фундаментальных исследований, в настоящее время нет. При этом и РФФИ, и РНФ активно проводят совместные конкурсы с иностранными грантовыми фондами, преимущественно государственными, и ставят своей целью расширение международного сотрудничества российских ученых. Кроме того, многие российские ученые сотрудничают с иностранными коллегами, которые получают иностранные гранты, поэтому соответствующие фонды упоминаются в российских публикациях таких ученых.

После прекращения работы фонда «Династия» заметных частных российских грантовых фондов в настоящее время нет.

ИСПОЛЬЗОВАНИЕ ФОРМАЛЬНЫХ НАУКОМЕТРИЧЕСКИХ ПОКАЗАТЕЛЕЙ В РАБОТЕ ГРАНТОВЫХ ФОНДОВ

Поскольку мы изучаем грантовые фонды с точки зрения научных публикаций, очень важно представлять, как сами фонды регламентируют работу грантополучателей. Для этого были изучены официальные сайты крупнейших российских (РФФИ, РНФ, конкурс «Мегагранты») и иностранных (*European Research Council*, *Deutsche Forschungsgemeinschaft*) грантодателей на предмет соответствующих упоминаний.

В зависимости от конкурса РФФИ руководитель научного проекта может как иметь ученую степень кандидата или доктора наук, так и не иметь ее, однако в этом случае при подаче заявки необходимо предоставить от одной публикации по теме проекта в журнале, индексируемом в одной из баз научного цитирования Российского индекса научного цитирования (РИНЦ) или *Web of Science*[9]. Как правило, результатами проекта выступают опубликованные статьи и доклады на конференциях, по ряду конкурсов – издание монографий, проведение конференций. Например, результатом первого года реализации проекта 2018 г. фундаментальных научных исследований, выполняемых молодыми учеными («Мой первый грант»), является публикация минимум одной статьи в рецензируемом журнале, индексируемом в одной из систем научного цитирования (*Web of Science* или РИНЦ). В отчетах по «Конкурсу на лучшие проекты фундаментальных научных исследований» следует указывать импакт-факторы *WoS* для журналов, в которых опубликованы результаты.

С 1 января 2014 г. при подаче заявки на конкурсы РНФ руководитель проекта должен иметь от 2-х до 10-ти публикаций, индексируемых в базах *Web of Science* или *Scopus*, в зависимости от конкурса и области науки. Например, для совместных с иностранными фондами конкурсов у руководителя по отрасли «Гуманитарные и социальные науки» должно быть не меньше 5-ти публикаций, а для всех остальных отраслей – не менее 10-ти. В зависимости от конкурса и области науки к результатам проекта предъявляются различные требования. Например, результатом конкурса «Проведение инициативных исследований молодыми учеными» является выпуск не менее одной публикации в *WoS Core Collection* или *Scopus* для отрасли «Гуманитарные и социальные науки» и не менее двух публикаций для всех остальных областей. Для

[8] Официальный сайт программы http://www.p220.ru

[9] Информация о конкурсах и требованиях РФФИ (https://www.rfbr.ru/) и РНФ (http://www.rscf.ru/) получена с их официальных сайтов в феврале 2019 г.

конкурсов поддержки лабораторий мирового уровня в ходе реализации проекта необходимо опубликовать не менее 25-ти публикаций в изданиях, индексируемых в *WoS* или *Scopus* для гуманитариев, и не менее 40 – для остальных. При этом одна публикация в журнале первого квартиля по значению импакт-фактора *WoS* или по показателю *ScimagoJR* (рассчитывается по *Scopus*) при оценке степени выполнения проекта учитывается как две публикации в иных журналах.

Согласно конкурсной документации к конкурсу мегагрантов, для заявителей по естественным, медицинским и техническим наукам введены пороговые значения по индексу Хирша (по данным *Web of Science*) и числу публикаций типов *article* и *review* в журналах первого квартиля *WoS*. Как следует из этой документации «обязательными результатами научного исследования являются публикация не менее 3 статей по направлению исследования в научных изданиях, индексируемых в базе данных *WoS* … по истечению 18 месяцев после начала осуществления научного исследования, а также публикация не менее 5 статей по направлению научного исследования в научных изданиях, индексируемых в базе данных *WoS* … по истечению 30 месяцев после начала осуществления научного исследования».

В отличие от ведущих российских государственных фондов иностранные грантодатели практически вовсе не прибегают к формализации и обязательности публикаций по итогам поддержанных проектов. Более того, они не используют формализованные наукометрические пороги и на входе. Так, основной грантовый фонд Евросоюза *European Research Council* (*ERC*) подчеркивает, что оценка проводится только международными экспертами и только по содержательному критерию *excellence* (превосходство): «Proposals are evaluated by selected international peer reviewers who evaluate proposals on the basis of excellence as the sole criterion. It will be applied to the evaluation of both the research project and the Principal Investigator in conjunction»[10]. На сайте *ERC* в требованиях для любых типов грантов нам не удалось найти никакой информации про обязательное число публикаций, квартили, цитируемость, уровень, статус индексации журналов и т.д. Единственное формальное требование совсем другого рода: все публикации должны быть в открытом доступе.

Ведущий германский фонд *Deutsche Forschungsgemeinschaft* (*DFG*) в информации, размещенной на своем сайте, также не оперирует формальными характеристиками публикаций. Единственное упоминание, которое удалось найти, касается разрешения тратить средства гранта на оплату публикаций и сформулировано так: «Publications may be in any form, with the exception of grey literature»[11]. Еще в 2010 г. DFG в официальном комментарии своего президента Матиаса Клейнера, озаглавленном «Quality, not Quantity» подчеркнул приверженность принципу содержательной оценки: «increasing importance has been given to numerical indicators such as the H-index and the impact factor… This is not in the interest of science»[12]. В частности, фонд запретил заявителям указывать в заявках более пяти своих публикаций. В официальных сообщениях 2018 г. фонд подтвердил свое стремление освободить науку от упрощенных оценок по импакт-фактору журналов[13].

Таблица 2

Требования к отчетности российских и иностранных грантовых фондов

Фонд	Критерии результативности (показатели)
РФФИ	Публикация минимального количества статей (в зависимости от конкурса) в рецензируемых журналах, индексируемых в одной из систем научного цитирования (*Web of Science* или РИНЦ). В отчетах некоторых конкурсов необходимо указать импакт-факторы *WoS* для журналов, в которых опубликованы результаты.
РНФ	В зависимости от конкурса и области науки публикация минимального количества статей в журналах, проиндексированных в *WoS Core Collection* или *Scopus*. Число публикаций для отрасли «Гуманитарные и социальные науки», как правило, в два раза ниже, чем для остальных отраслей. При этом одна публикация в журнале первого квартиля по значению импакт-фактора *WoS* или по показателю *ScimagoJR* (рассчитывается по *Scopus*) учитывается как две другие публикации.
Мегагранты	Публикация не менее 3 статей по направлению исследования в научных изданиях, индексируемых в базе данных *WoS*, по истечению 18 месяцев после начала осуществления научного исследования, а также публикация не менее 5 статей по направлению научного исследования в научных изданиях, индексируемых в базе данных *WoS*, по истечению 30 месяцев после начала осуществления научного исследования.
Иностранные фонды (*ERC*, *DFG*)	Публикации типа *Open Access* с их последующей содержательной оценкой.

[10] https://erc.europa.eu/funding/starting-grants (Здесь и далее цитаты по официальным сайтам упоминаемых грантовых фондов).
[11] https://www.dfg.de/formulare/52_01/52_01_en.pdf
[12] https://www.dfg.de/en/service/press/press_releases/2010/pressemitteilung_nr_07/
[13] https://www.dfg.de/en/research_funding/announcements_proposals/2018/info_wissenschaft_18_56/index.html

В целом можно заключить, что западные фонды в своей политике в этой части противоположны российским: если РНФ и РФФИ и на входе, и на выходе требуют соблюдение жестких и предельно формализованных обязательств по числу публикаций, то *ERC* и *DFG* максимально избегают такой формализации и упирают на важность содержательной оценки специалистами (табл. 2). Если западные фонды активно требуют *Open Access* для публикации научных результатов поддержанных проектов, то российские фонды этого вопроса не касаются вовсе.

МЕТОДЫ И ДАННЫЕ ИССЛЕДОВАНИЯ

На первом этапе исследования нами была поставлена задача выделения ведущих мировых журналов: такой подход, ограничивающий список источников, широко используется в наукометрии как соотносящийся с эмпирическими законами Гарфилда [21], а публикации в ведущих изданиях являются основным символическим капиталом современного ученого уже не только в естественных, но и в общественных науках [22].

За основу нами был взят перечень *Nature Index* (*NI*, список и описание процедуры отбора приведены на официальном сайте https://www.natureindex.com/), состоящий из 82 журналов с безупречно высокой репутацией, высокой цитируемостью и низким *acceptance rate* по физике, химии, биологии и наукам о Земле, т.е. наиболее представленным в международных базах тематикам российских публикаций [23]. Попадание журнала в этот список происходит после отбора ведущими независимыми учеными под руководством *Nature Research* – исследовательского подразделения издательства *Springer Nature* – мирового лидера, выпускающего, помимо прочих, журнал «*Nature*». Журналы, входящие в список *Nature Index*, соответствуют высоким редакционным стандартам, поэтому, как правило, имеют полноценную информацию о *FA* и хорошее качество индексирования в базах *Scopus* и *WoS*.

Выбор экспертного списка вместо наукометрических показателей (импакт-фактор и т.п.) был сделан в силу ряда причин: во-первых, использование импакт-факторов (ИФ) вместо экспертного отбора сейчас активно критикуется самим исследовательским сообществом [24], во-вторых, подход *Nature Index* (*NI*) хорош для выбранных нами целей из-за соблюдения селективности при равномерном охвате различных областей естественных наук, который трудно гарантировать, используя формальные показатели. При этом следует отметить, что журналы списка *NI* в подавляющем большинстве относятся к первому децилю распределений по ИФ в соответствующих предметных категориях, т.е. противоречия между экспертной и наукометрической оценкой с этой стороны нет. *NI* используется в библиометрии с целями, аналогичными нашей [25]. Наконец, важным было и то, что число публикаций России в этих журналах достаточно велико.

Временными рамками для анализа мы выбрали 2014-2017 гг. Год начала совпадает с годом фактического запуска РНФ, а год окончания – последний полный проиндексированный рассматриваемыми базами на момент проведения исследования (выгрузка осуществлялась летом 2018 г., затем массив метаданных публикаций был обновлен 15 февраля 2019 г.). Для анализа через соответствующие веб-интерфейсы была вручную выгружена библиографическая информация публикаций с российской аффилиацией за 2014-2017 гг. в журналах *Nature Index* из баз *Scopus* и *WoS*, содержащая все доступные поля из *WoS*, *Scopus* и дополнительные показатели из *SciVal* и *InCites*[14]. Таким образом, на 15 февраля 2019 г. за 2014-2017 гг. всего проиндексировано одновременно в обеих базах (*WoS* и *Scopus*) 8412 публикаций всех типов с российской аффилиацией (при этом 2 статьи с пометкой *Retracted* не учитывались). В силу различия в индексировании при расхождениях годом публикации признавался указанный в базе *WoS*, информации об аффилированности с Россией было достаточно хотя бы по одной из баз. Полный массив публикаций был использован для сравнения аналогичных публикаций других стран.

Для того чтобы картина относительного соотношения присутствия различных фондов была более отчетливой, на третьем этапе исследования были исключены публикации с числом авторов более 100 – это публикации, выполненные в мегаколлаборациях (таких, как *ATLAS* в физике высоких энергий или *Global Burden of Disease* в эпидемиологии). Исключение таких публикаций связано со сложностями их учета и неоднозначностью оценки вклада отдельных авторов, организаций, стран и грантодателей [26]. После исключения работ с 100+ авторами остается 6898 публикаций, из которых на типы *article* и *review* (тип публикации *article* и *review* определяется в соответствии с данными хотя бы одной из баз) приходится 6811 публикаций. Выбор публикаций только типов *article* и *review* традиционен для наукометрии [26] и обусловлен существенно лучшим качеством индексирования информации и существенно большей однозначностью в трактовке показателей на их основе. Кроме того, сами требования фондов ограничивают отчетность данными типами[15].

Массив, состоящий из 6811 публикации, и является основным объектом исследования в настоящей статье.

Для распределения полученного массива публикаций по грантодателям, необходимо изучить, как устроены полные выгрузки библиографического описания из баз научного цитирования. В табл. 3 приведены названия полей в *Scopus* и *WoS*, содержащие информацию о *FA* в полных выгрузках.

Пример грантовой информации в выгрузках *Scopus* и *WoS* по отдельной статье представлен в *Приложении 1*.

Следует отметить, что по предварительным данным *Scopus* внутри своей базы может в ряде случаев

[14] Официальные платные аналитические надстройки над *Scopus* и *WoS*, содержащие показатели нормализованной различными способами цитируемости публикаций, отсутствующие в стандартных версиях этих баз.

[15] http://rscf.ru/upload/iblock/a60/a60d5fb59e0bbe7ad38e41f23e60af52.pdf, http://rscf.ru/upload/iblock/918/91889812133774a3ff4d215b329a3ba6.pdf (пункт 1.11 формы 1)

Таблица 3

Грантовая информация в полных выгрузках из *Scopus* и *WoS*

Информация о *FA* в полных выгрузках	**Поля в *Scopus***	**Поля в *WoS***
Номера грантов и названия организаций – грантодателей	Funding details	FU
Слова о грантовой поддержке и слова благодарности в статье	Funding Text (1, 2, …)*	FX

*Библиографическое описание может как не содержать совсем поле *Funding text*, так и содержать более одного поля с грантовой информацией

фиксировать в формате *XML* информацию о *FA* более полно и структурировано[16], но она по неясным причинам недоступна через стандартный веб-интерфейс, которым пользуется львиная доля ученых и администраторов, и которым в связи с этим воспользовались и мы.

Сведение публикаций *WoS* и *Scopus* осуществлялось по *DOI* и по названиям публикаций (по *DOI* сошлось свыше 99% работ). Затем было проведено сравнение *FA*, сразу показавшее наличие очень существенных лакун в *Scopus* (см. далее), в силу чего дальнейшая работа велась с базой *WoS*.

Первоначальная привязка исследуемого массива публикаций к российским грантодателям осуществлялась с помощью скрипта на языке *Python* с использованием ряда открыто доступных данных. В скрипте реализован поиск по разным используемым учеными вариантам названий упомянутых выше трех основных государственных фондов и программ, а также фонда «Династия», а также по номерам грантов для конкурса «мегагрантов» в полях *FU* и *FX* выгруженных метаданных публикаций из *WoS*. Суть работы кода заключалась в следующем: проверить наличие хотя бы одной из возможных комбинаций номеров, используемых в конкурсе мегагрантов, с помощью регулярных выражений или вхождение каждого названия фонда (без учета регистра) в полях *FU* и *FX* (*Приложение 2*). Для установления точности привязки по скрипту и поиска в *WoS* были разработаны механизмы идентификации фондов, представляющие собой текстовые запросы с использованием операторов *WoS Advanced Search*. Эти запросы включают как официальные полные названия фондов, так и менее распространенные варианты или аббревиатуры (*Приложение 3*).

Для устранения возможных пробелов в привязке публикаций к грантодателю по скрипту и текстовым запросам для грантов РФФИ и РНФ дополнительно был проведен поиск по номерам грантов, представленных на сайтах фондов. При этом, общий принцип работы с данными был следующим: предпочитался риск потери некоторых публикаций в множестве, допустим, поддерживаемых РФФИ, чем включение в это множество лишних публикаций.

В силу возможного недостаточного охвата публикаций с помощью текстовых запросов для ведущих иностранных фондов, чаще всего упоминаемых в российских публикациях – *Deutsche Forschungsgemeinschaft* (*DFG*, Германия), *National Science Foundation* (*NSF*, США), *European Research Council* (*ERC*), *National Natural Science Foundation of China* (*NSFC*, Китай), – привязка публикаций осуществлялась по официальным профилям грантодателей в *WoS\InCites*.

После выделения массивов публикаций, упоминающих ведущие фонды в своих *Funding Acknowledgments*, они были исследованы с применением стандартных наукометрических средств (наличие иностранных аффилиаций, распределение по организациям, цитируемость и т.д.).

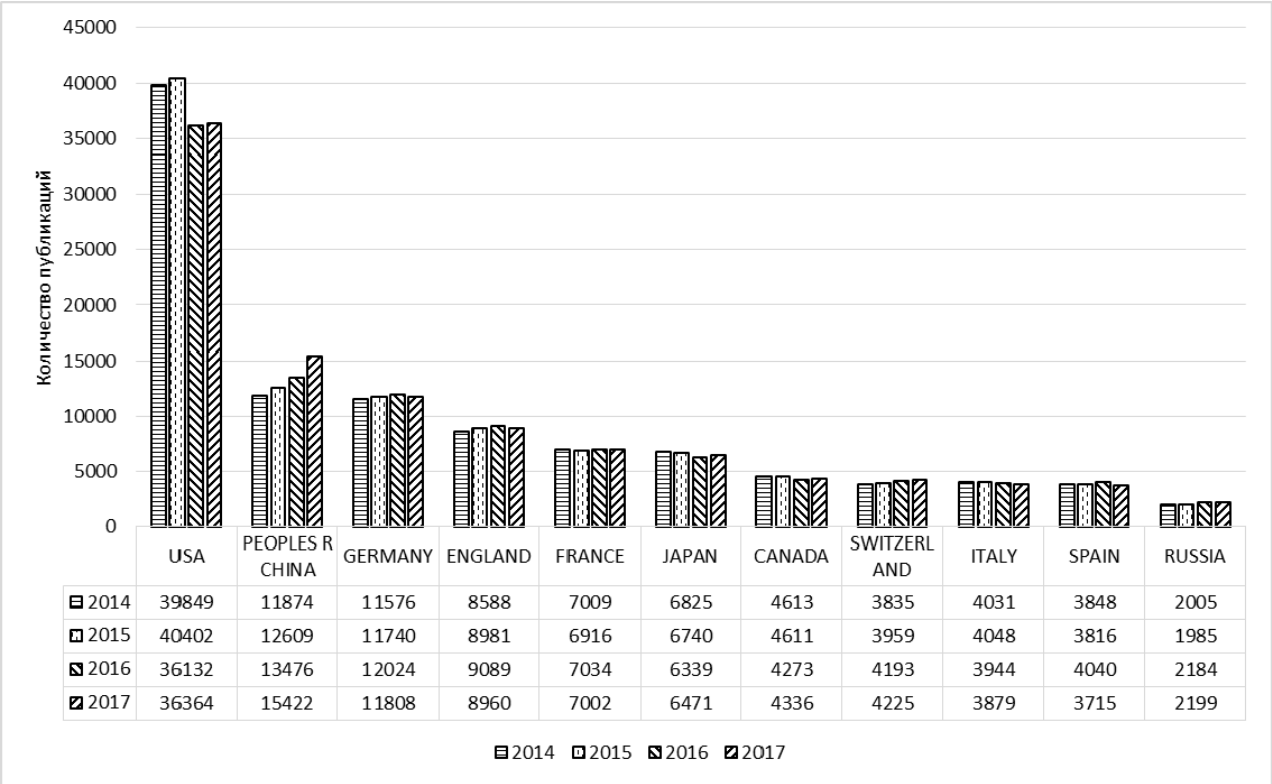
РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Российские публикации в журналах списка *Nature Index*

Прежде чем переходить непосредственно к результатам исследования *FA*, необходимо кратко остановиться на характеристиках изучаемого массива публикаций (в данном случае речь пойдет о массиве 8412 публикаций всех типов с любым числом соавторов). По количеству публикаций в журналах списка *Nature Index* за период с 2014 по 2017 гг. (рис. 1) безоговорочным лидером является США, Российская Федерация не входит в первую десятку, а разрыв между остальными странами наблюдается не такой серьезный. Существенный рост числа публикаций за исследуемый период демонстрирует прежде всего Китай, на фоне которого увеличение числа российских публикаций в *Nature Index* практически незаметно. При этом число публикаций США в 2016-2017 гг. существенно снизилось.

Большая часть российских публикаций, отраженных в *WoS* относится к естественным наукам [23], т.е. именно тем, которым посвящены входящие в список *Nature Index* журналы. В этом смысле тематическое распределение публикаций в топовом сегменте журналов не отличается кардинально от соответствующего распределения всех публикаций в *WoS*.

[16] В частности, для ряда публикаций при доступе через *API* выделяются грантодатели, которые привязываются к сводным профилям в рамках проекта *FundRef* (*CrossRef Funding* – Глобальный проект международного консорциума *CrossRef*, объединяющий грантовые фонды по всему миру. Подробнее на сайте *CrossRef*: https://www.crossref.org/services/funder-registry)



	USA	PEOPLES R CHINA	GERMANY	ENGLAND	FRANCE	JAPAN	CANADA	SWITZERLAND	ITALY	SPAIN	RUSSIA
2014	39849	11874	11576	8588	7009	6825	4613	3835	4031	3848	2005
2015	40402	12609	11740	8981	6916	6740	4611	3959	4048	3816	1985
2016	36132	13476	12024	9089	7034	6339	4273	4193	3944	4040	2184
2017	36364	15422	11808	8960	7002	6471	4336	4225	3879	3715	2199

Рис. 1. Количество публикаций всех типов в журналах списка *Nature Index* по странам по данным базы *Web of Science*

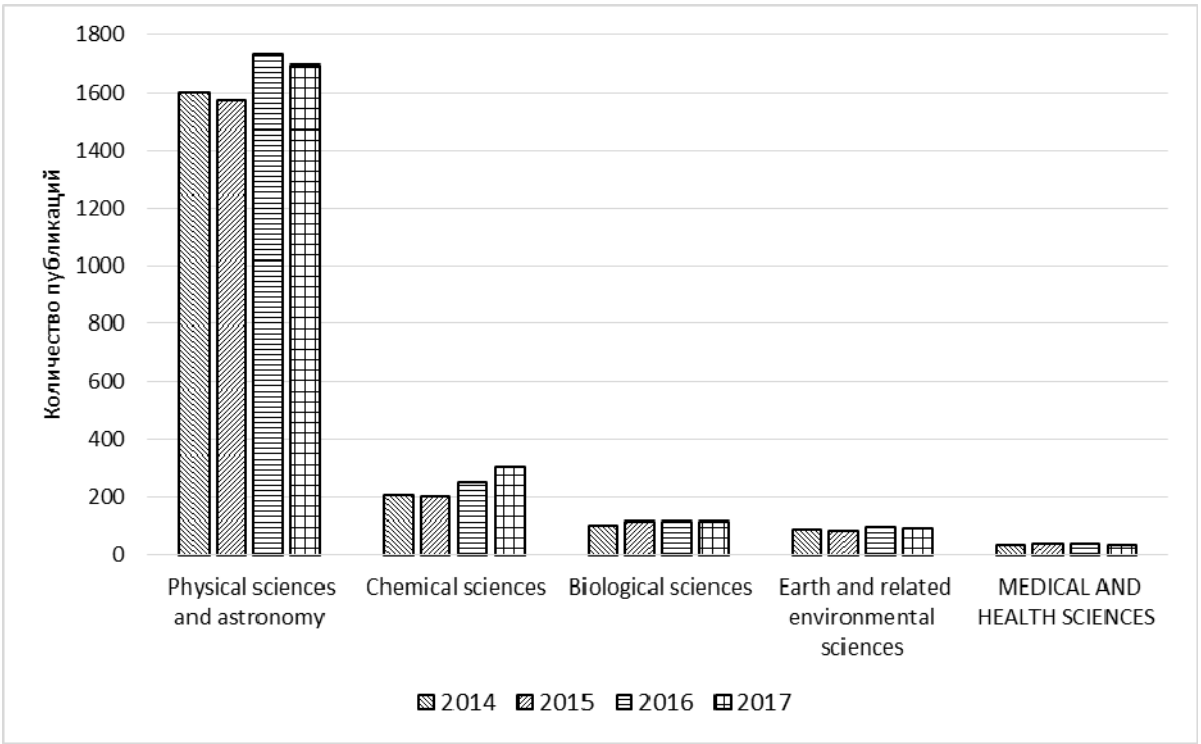


Рис. 2. Распределение публикаций всех типов с российской аффилиацией по основным разделам естественных наук и медицине (ОЭСР [27]) по данным базы *Web of Science*

Таблица 4

Топ-10 журналов по количеству российских публикаций всех типов за 2014-2017 гг.

Название журнала	Кол-во публикаций с российской аффилиацией	Общее кол-во публикаций (по миру, WoS)	Доля публикаций с российской аффилиацией, %
«Physical Review B»	1415	20953	7
«Physical Review D»	1173	14094	8
«Physical Review Letters»	730	10638	7
«Journal of High Energy Physics»	693	8387	8
«Physical Review A»	610	10861	6
«Applied Physics Letters»	475	14576	3
«European Physical Journal C»	475	2774	17
«Astronomy and Astrophysics2	450	7234	6
«Nature Communications»	222	14419	2
«Inorganic Chemistry»	197	6076	3

Таблица 5

Динамика числа публикаций типов article и review с российской аффилиацией в журналах списка *Nature Index*

Год	Всего публикаций	Первая волна, МГУ, СПбГУ, %	Первая волна, %
2014	1633	54,6	36,9
2015	1600	59,6	43,6
2016	1778	60,9	44,5
2017	1800	60,3	43,6
Всего	6811	58,9	42,2

Как видно из рис. 2, число публикаций с российской аффилиацией в журналах *Nature Index* растет в первую очередь по химии.

Распределение публикаций России по журналам также неравномерно. Журнал «*Physical Review B*», посвященный физике конденсированного состояния – крупнейшей области физики, сохраняющей центральное значение не только в России, но и в мире [28], предсказуемо лидирует по числу российских публикаций в списке *NI*. Из табл. 4 видно, что 8 из 10 журналов с наибольшим числом публикаций посвящены физике (кроме мультидисциплинарного «*Nature Communications*» и химического «*Inorganic Chemistry*»).

Наибольшая относительная концентрация статей с российской аффилиацией предсказуемо наблюдается в журналах по физике высоких энергий («European Physical Journal C»).

Для анализа на уровне организаций уместно ограничиться только типами публикаций *article* и *review*, как основными видами реферируемых публикаций (такое ограничение традиционно для наукометрии [26]), и исключить публикации с 100+ авторами в силу их специфики. В соответствующем массиве из 6811 работ на ведущие вузы, под которыми мы в данном случае понимаем МГУ им. М.В. Ломоносова, СПбГУ и вузы первой волны программы 5-100, приходится порядка 60% (табл. 5), что согласуется со ставкой правительства России на университетскую науку [16].

Отдельно уместно остановиться на работах с 100+ соавторами, так как их число и важность для науки Российской Федерации велики. Если в целом для ведущих стран (членов *OECD*) доля работ с 100+ соавторами в списке *NI* за рассматриваемый период составляет 0,66%, то для РФ доля таких работ равна 17,2%. Особенно велика роль таких публикаций для многих ведущих университетов, которым необходимо быстро наращивать число статей в лучших журналах, чтобы продвигаться в рейтингах. У целого ряда российских университетов и НИИ на публикации в составе мегаколлабораций приходится свыше половины всех статей в списке *NI* (МГУ им. М.В. Ломоносова, МИФИ, СПбГПУ, ТГУ, НГУ), у других (СамГУ, ИТМО, МИСиС и т.д.) – эта доля минимальна или нулевая (*Приложение 4*).

Различия в индексировании грантовой информации в базах научного цитирования

Полнота охвата информации о грантах в базах научного цитирования *Web of Science* (наличие непустых полей *FU* и *FX*) и *Scopus* (наличие непустых полей *Funding details* и *Funding Text*) на примере выгрузок исследуемого массива из 6811 публикаций отражена в табл. 6.

Таблица 6

Число (верхняя часть таблицы) и доля (нижняя часть таблицы) публикаций с наличием информации в *Funding Acknowledgments* в *WoS* и *Scopus*

2014		**2015**		**2016**		**2017**	
Всего	1633	Всего	1600	Всего	1778	Всего	1800
WoS +	**1525**	**WoS +**	**1512**	**WoS +**	**1683**	**WoS +**	**1715**
Scopus +	127	Scopus +	179	Scopus +	867	Scopus +	1083
Scopus -	1398	Scopus -	1333	Scopus -	816	Scopus -	632
WoS -	**108**	**WoS -**	**88**	**WoS -**	**95**	**WoS -**	**85**
Scopus +	3	Scopus +	1	Scopus +	7	Scopus +	10
Scopus -	105	Scopus -	87	Scopus -	88	Scopus -	75
2014		**2015**		**2016**		**2017**	
WoS +	**93,4**	**WoS +**	**94,5**	**WoS +**	**94,7**	**WoS +**	**95,3**
Scopus +	7,8	Scopus +	11,2	Scopus +	48,8	Scopus +	60,2
Scopus -	85,6	Scopus -	83,3	Scopus -	45,9	Scopus -	35,1
WoS -	**6,6**	**WoS -**	**5,5**	**WoS -**	**5,3**	**WoS -**	**4,7**
Scopus +	0,2	Scopus +	0,1	Scopus +	0,4	Scopus +	0,6
Scopus -	6,4	Scopus -	5,4	Scopus -	4,9	Scopus -	4,2

Массив всех этих публикаций был поделен на две группы: первая группа содержала публикации с указанием *FA* в выгрузках *WoS* (отмечено знаком *WoS*+ в табл. 6) и вторая группа не содержала публикаций с информацией о *FA* в выгрузках *WoS* (отмечено знаком *WoS*-). Внутри каждая группа была поделена еще на два непересекающихся множества публикаций: первое содержало информацию о *FA* в выгрузках *Scopus* (*Scopus*+), а второе – нет (*Scopus*-). Например, число 127 в ячейке на пересечении строки «Scopus+» и года «2014» означает, что 127 публикаций из 1525 публикаций с указанием *FA* в выгрузках *WoS* имеют информацию о *FA* в выгрузках *Scopus*.

Одним из ключевых результатов стало выявление существенной разницы в полноте индексации *FA* в *WoS* и *Scopus*: если для первой базы доля статей с *FA* стабильно составляет около 95%, то для второй колеблется от 7,8% до 60,2% в зависимости от года. Фактически, несмотря на серьезный прогресс в индексировании *Scopus*, использовать на практике пока следует только базу *Web of Science*, так как лакуны в *Scopus* еще заведомо слишком велики. Тем не менее, важно отметить, что некоторые лакуны присутствуют и в *WoS*.

Качество индексирования *Scopus*, хотя и остается низким, с годами резко улучшается и по единичным статьям превосходит *WoS*: так, в 2017 г. из 85 публикаций, по которым в *WoS* отсутствовали *FA*, у 10 они присутствовали в *Scopus* (двумя годами ранее из 88 работ без *информации о грантах* в *WoS* в *Scopus FA* найдены лишь у одной). *WoS* за рассмотренный период также несколько улучшила индексирование: ежегодно доля работ с *FA* незначительно увеличивался и к 2017 г. превысила 95%, что на наш взгляд вполне достаточно для содержательного анализа. Следует учитывать, что среди статей в *NI* есть небольшое число работ, действительно не содержащих *FA*. Если экстраполировать покрытие в *Scopus* за 2017 г. (60,2%), то уместно предположить, что в *WoS* отсутствует информация о *грантах* по примерно 16-20 публикациям, содержащим *FA*, а у остальных 65-70 публикаций *FA* отсутствуют в оригинале, т. е. доля проиндексированных *FA* по журналам списка *NI* по российским статьям может достигать 98-99%. Наконец, необходимо отметить, что для тех публикаций, *FA* которых проиндексированы обеими базами сразу, длина этих *FA* различается слабо: среднее по *Scopus* – 1365 символов, медиана – 664 символа, по *WoS* – 1330 и 770 соответственно.

Результат сравнения двух рассматриваемых баз данных обусловил наше использование *WoS* и отказ от *Scopus* во второй части работы.

Привязка FA к грантодателям

Для уточнения привязки *Funding Acknowledgments* и публикаций к грантовым фондам на массиве данных *WoS* для ряда ведущих отечественных грантодателей нами был проведен описанный выше расширенный поиск, заключающийся в нахождении всевозможных названий фондов с помощью скрипта на *Python* с дополнением по номерам грантов, по полям *FU* и *FX* для выгруженных из *WoS* 6811 публикаций.

Прежде всего, выяснилось, что для двух основных отечественных грантовых фондов количество работ, где в *WoS* есть номера грантов, но нет названий фондов, минимально: 18 статей для РФФИ и 17 для РНФ.

Из-за отсутствия в открытом доступе полной информации о номерах грантов РФФИ оценить точность соотнесения грантовых номеров и названия удалось только для РНФ. В его случае число публикаций, которые нам удалось соотнести с фондом по *FA* одновременно по номеру гранта и по названию, составило 95,4%, что представляется очень хорошим результатом. Фактически, это позволяет проводить средствами *WoS* широкомасштабный анализ публикаций по отдельным грантам данного фонда.

Таблица 7

Сравнение точности привязки публикаций в *WoS* на примере РФФИ

Число публикаций *article* и *review* с российской аффилиацией в журналах *Nature Index*	Год				Всего
	2014	2015	2016	2017	
Расширенный поиск по выгрузке из *WoS* (по названию и номерам грантов)	684	611	608	569	2472
Профиль РФФИ в системе *InCites*	622	563	562	530	2277
Разница	62	48	46	39	195
Разница, %	9,06	7,86	7,57	6,85	7,89

Дополнительно на примере РФФИ была проведена проверка корректности привязки к встроенному в *WoS* профилю грантового фонда (табл. 7). Доля непривязанных к официальному профилю публикаций существенна: в 2014 г. теряется 9% публикаций, в 2017 г. – около 7%, но динамика скорее положительная и эта доля сокращается из года в год.

Готовые профили фондов есть и в базе *Scopus*, но их качество тоже не идеально. Так, сравнив публикации, приписанные к РНФ в этой базе и *WoS*, мы выявили 43 публикации, которые алгоритмами *Scopus* были ошибочно отнесены к *Robert Schalkenbach Foundation*, по сокращенному названию, совпадающему с РНФ.

Важно отметить, что для ряда грантодателей полноценные профили в *WoS* отсутствуют, а варианты наименования в *FA* крайне разнообразны и не содержат аббревиатур, позволяющих надежно связать их с источниками финансирования. В первую очередь это относится к мегагрантам, федеральным целевым программам, программам РАН. Фактически, для мегагрантов единственным приемлемым вариантом поиска является поиск по номерам грантов, а для федеральных целевых программ затруднен и такой вариант.

Представленность грантовых фондов в Funding Acknowledgments

В табл. 8 представлен результат выделения основных грантовых фондов по расширенному поиску названий и номеров грантов в выгрузках исследуемого массива публикаций типов *article* и *review* с российской аффилиацией в журналах списка *Nature Index* из *WoS* и по профилям грантодателей в *InCites*.

Прежде всего, нужно подчеркнуть быстрое развитие РНФ: уже в 2014 г., т. е. на старте работы фонда, в лучших мировых журналах опубликовано свыше 100 работ, упоминающих его поддержку. К 2017 г. РФФИ и РНФ практически сравнялись в уровне поддержки российских публикаций в ведущих журналах. РФФИ за исследуемый период наоборот снизил не только долю, но и абсолютное число поддержанных публикаций, но пока сохранил статус лидера, чья поддержка упоминается в трети всех работ России в *NI*.

Специально отметим, что с 2014 г. постепенно увеличивалось количество работ, поддержанных одновременно обоими фондами: если в 2014 г. это всего лишь 3,4% от проектов РФФИ, то в 2016 г. было достигнуто максимальное значение доли публикаций с поддержкой двух фондов, что составляет 21,2%. За 2017 г. этот показатель незначительно снизился (до 20,9%). В табл. 9 отражено число публикаций, поддержанных одновременно двумя ведущими грантовыми фондами РФ.

Доля работ, упоминающих иностранные грантовые фонды, за рассмотренные четыре года существенно не изменился. Традиционно [5] лидирует DFG, давно сотрудничающий с российскими учеными и имеющий представительство в России. Число публикаций частного фонда «Династия», закрытого в 2015 г., предсказуемо быстро снижается.

Гранты в *Funding Acknowledgments* списка *Nature Index* и ведущие вузы России

Доля публикаций ведущих вузов Российской Федерации (в том числе входящих в программу 5-100), поддержанных грантовыми фондами РФФИ и РНФ, указана в табл. 10. Из нее видно, что доля публикаций, поддержанных РФФИ, сократилась практически для каждого вуза, а доля публикаций с поддержкой РНФ, наоборот, почти для всех выросла. Особенно активно выросла доля публикаций с поддержкой РНФ у ННГУ, но это больше именно относительный, а не абсолютный рост (общее количество публикаций в журналах списка *Nature Index* уменьшилось, а количество публикаций, финансированных грантами РНФ, наоборот, возросло).

Публикации с международным соавторством

Наибольшее число публикаций с международным сотрудничеством выполнено в рамках конкурса «Мегагрантов», что соотносится с идеей этого конкурса, многие из победителей которого – иностранные ученые. В отличие от уменьшающейся доли публикаций с международным участием при поддержке РФФИ за период 2014-2017 гг., доля таких публикаций при поддержке РНФ растет, однако в обоих случаях изменения незначительны (рис. 3).

Важно, что в ведущих журналах публикации, как правило, выполнены крупными международными коллективами, поэтому доля интернациональных работ существенно выше, чем в среднем публикаций России, отраженных в *WoS Core Collection* (*article+review*).

Таблица 8

Распределение числа публикаций с российской аффилиацией по основным грантодателям России и ведущим иностранным фондам

Число публикаций	Год				Всего
	2014	2015	2016	2017	
Всего	1633	1600	1778	1800	6811
«Династия»	103	103	69	29	304
РФФИ	684	611	608	569	2472
РНФ	110	296	453	513	1372
Мегагранты	132	130	112	105	479
DFG (по профилю в InCites)	231	169	211	228	839
NSF (по профилю в InCites)	193	139	155	188	675
ERC (по профилю в InCites)	80	80	73	85	318
NSFC (по профилю InCites)	39	60	63	56	218
Доля публикаций, %	**2014**	**2015**	**2016**	**2017**	**Всего**
«Династия»	6,3	6,4	3,9	1,6	4,5
РФФИ	41,9	38,2	34,2	31,6	36,3
РНФ	6,7	18,5	25,5	28,5	20,1
Мегагранты	8,1	8,1	6,3	5,8	7
DFG (по профилю в InCites)	14,1	10,6	11,9	12,7	12,3
NSF (по профилю в InCites)	11,8	8,7	8,7	10,4	9,9
ERC (по профилю в InCites)	4,9	5	4,1	4,7	4,7
NSFC (по профилю InCites)	2,4	3,8	3,5	3,1	3,2

Таблица 9

Взаимосвязь публикаций с поддержкой РФФИ и РНФ

Научный фонд	Год				Всего
	2014	2015	2016	2017	
	Число публикаций				
РФФИ +	684	611	608	569	2472
РНФ +	23	84	129	119	355
РНФ -	661	527	479	450	2117
РФФИ -	949	989	1170	1231	4339
РНФ +	87	212	324	394	1017
РНФ -	862	777	846	837	3322
Доля РНФ+РФФИ в общем количестве публикаций РФФИ, %	3,4	13,7	21,2	20,9	14,4

Таблица 10

Сотрудничество РФФИ и РНФ с ведущими вузами Российской Федерации (%)

ВУЗ	РФФИ				РНФ			
	2014	2015	2016	2017	2014	2015	2016	2017
ВШЭ	75,00	50,00	61,76	31,58	6,25	5,00	29,41	39,47
ДВФУ	69,23	60,00	31,03	30,00	0,00	26,67	17,24	30,00
ИТМО	40,00	41,86	37,89	33,63	8,89	16,28	22,11	27,43
КФУ	48,84	48,08	29,23	25,40	0,00	3,85	16,92	15,87
ЛЭТИ	73,33	57,14	80,00	50,00	0,00	28,57	0,00	25,00
МГУ	57,87	47,57	46,03	40,38	10,21	23,79	30,95	38,46
МИСиС	55,22	24,64	38,46	32,74	8,96	8,70	17,31	24,78
МИФИ	52,00	47,27	42,17	39,51	0,00	34,55	33,73	22,22
МФТИ	63,91	51,39	45,96	37,24	11,28	32,64	45,34	44,83
НГУ	58,97	51,09	50,44	41,00	16,67	28,26	32,74	35,00
ННГУ	56,45	52,63	54,29	40,00	6,45	22,81	48,57	70,00

ВУЗ	РФФИ				РНФ			
	2014	2015	2016	2017	2014	2015	2016	2017
СамГУ	40,00	63,64	50,00	33,33	0,00	18,18	0,00	40,00
СПбГПУ	50,00	39,13	41,67	20,69	9,09	21,74	27,78	31,03
СПбГУ	51,59	40,58	44,59	44,59	7,14	18,12	18,24	21,62
ТГУ	24,07	35,06	25,45	32,84	3,70	10,39	14,55	19,40
ТПУ	13,33	40,00	37,04	18,42	0,00	4,00	14,81	23,68
УрФУ	52,00	50,88	44,44	37,04	10,00	26,32	26,98	27,78

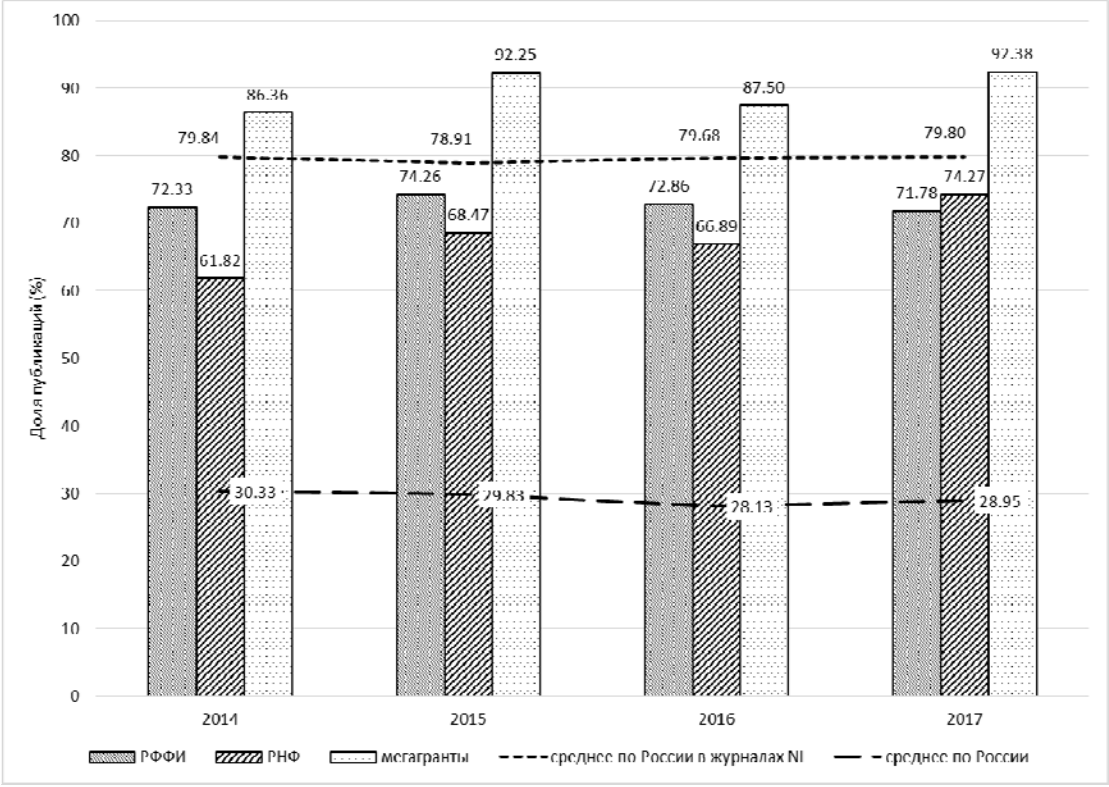


Рис. 3. Доля публикаций с международным соавторством (доля со средней тренд-линией по Российской Федерации)

Цитируемость публикаций

Детальное изучение взаимосвязи цитирований и грантов [9] выходит за рамки настоящей работы, однако обойти вниманием этот ключевой аспект мы не можем. Так как журналы списка *Nature Index* относятся к разным тематикам[17], для изучения цитирований требуется нормализация по журналу или по тематике [26]. Средняя нормализованная по журналу цитируемость российских публикаций (*JNCI, Journal-Normalized Citation Impact*) в *NI* выше, чем в среднем по миру (единица) и составляет 1,19, но при исключении статей со 100+ соавторами снижается до 0,9, однако эти данные по понятным причинам (сложность учета мегаколлабораций) трактовать сложно. Гораздо интереснее сравнивать, есть ли значимые отличия в цитируемости российских работ в списке *NI*, поддержанных ведущими российскими грантодателями и не поддержанных ими. Для такого сравнения мы выбрали РФФИ и РНФ.

Мы рассмотрели четыре группы публикаций, относящиеся к типам *article* и *review* и имеющие 100 и менее соавтров. В первую группу входят публикации, у которых указан фонд РФФИ в качестве одного из грантодателей, во вторую – все публикации с грантовой информацией без указания РФФИ, в третью – все публикации с поддержкой РНФ, в четвертую группу – все публикации с грантовой поддержкой без указания РНФ. Таким образом, для анализа были рассмотрены две группы публикаций попарно: РФФИ/не РФФИ (при этом, другие фонды, в том числе РНФ, не исключались), и РНФ/не РНФ (при этом, другие фонды, в том числе РФФИ, не исключались).

В качестве показателей цитируемости мы помимо *JNCI* выбрали *Field-Weighted Citation Impact* (*FWCI*, вариант нормализующего цитируемость на тип документа и тематику «Лейденского индикатора» в *SciVal\Scopus*) и *Category-Normalized Citation Impact* (*CNCI*, аналогичный индикатор в *InCites\WoS*). Дополнительно мы установили среднее число авторов на публикацию, которое для РФФИ\РНФ и не-РФФИ\не-РНФ оказалось соответственно очень близким.

[17] https://www.natureindex.com/faq#subjects

Таблица 11

Сравнение нормализованной цитируемости в публикациях с поддержкой РФФИ\РНФ и без нее

Научный фонд	Количество публикаций с *FA*	Среднее значение *JNCI*	Среднее значение *FWCI*	Среднее число авторов на статью	Среднее значение *CNCI*
РФФИ	2472	0,84	1,58	7,34	1,38
не РФФИ	3963	0,96	2,18	9,18	2,06
РНФ	1372	0,93	2	7,28	1,84
не РНФ	5063	0,88	1,9	8,5	1,77

Из табл. 11 видно, что по всем метрикам цитирований не-РФФИ выглядит лучше РФФИ, а РНФ, напротив, выглядит лучше не-РНФ. Однако для РНФ эти различия гораздо менее выражены.

По критерию U-Манна-Уитни (расчеты в *Приложении 5*) получаем, что на уровне значимости 0,05 публикации, поддержанные РФФИ, по сравнению с публикациями тех же лет с поддержкой других фондов, будут иметь значимые различия по всем трем показателям цитирования. Напротив, на уровне значимости 0,05 публикации 2014-2017 гг., поддержанные РНФ, по сравнению с публикациями тех же лет с поддержкой других фондов, не будут иметь значимые различия по этим показателям.

Таким образом, можно достаточно уверенно утверждать, что российские публикации с поддержкой РФФИ в ведущих журналах цитируются хуже, чем российские публикации в тех же журналах без упоминания этого фонда, а для РНФ такой зависимости не прослеживается.

ВЫВОДЫ И ОБСУЖДЕНИЕ

Основной результат нашего исследования в плане применимости наукометрических инструментов для оценки механизмов проектного финансирования науки заключается в том, что были выявлены существенные пропуски в индексации *Funding Acknowledgments* в ведущих научных журналах мира в базе *Scopus*, что в целом близко к (немногочисленным) выводам других исследователей по данному вопросу [15]. С учетом масштабности этих пропусков использование *Scopus* для прикладного анализа грантовой информации в публикациях в настоящее время следует считать преждевременным.

При этом мы отмечаем стремительный рост полноты индексирования *Scopus* за рассмотренный период: на протяжении всего четырех лет доля работ с *FA* в российских журналах списка *Nature Index* выросла с 8% до свыше 60%. При сохранении таких темпов уже через несколько лет Scopus может приблизиться по полноте индексироваия к *WoS*.

В смысле полноты информации в *WoS* наши данные подтверждают результаты [8] и других работ: покрытие фактически составляет 95% всех публикаций и может составлять до 99% работ с *FA*, что вполне достаточно для анализа. При этом отдельные лакуны остаются, а причина их возникновения неясна, особенно в случаях, когда в *Scopus* у той же работы *FA* присутствуют. Что касается полноты индексации самого текста *FA*, то здесь по тем работам, *FA* которых представлены сразу в обоих базах, существенной разницы в длине текста не наблюдается, хотя медиана числа символов у *WoS* все же больше, чем у *Scopus*.

Использование готовых профилей фондов в *WoS* и *Scopus* по нашим данным следует проводить осторожно, так как потери от недоучета могут быть достаточно велики.

Значимым результатом нашего исследования представляется продемонстрированный на примере Российского научного фонда высокий уровень индексирования номеров конкретных грантов. Это позволяет достаточно надежно и, что важно для прикладных изысканий, просто и быстро связывать результаты (публикации) с конкретными проектами. Кроме того, используя поиск *Advanced Search* по маске номера (в номере кодируется год выдачи гранта, тематика, конкурс), можно выявлять все публикации, поддержанные грантами РНФ, выданными в конкретном году по конкретной тематике[18]. Примечательно, что нами было найдено несколько грантов (около 10), номера которых в индексах РФФИ и РНФ полностью совпадают. Очевидно, что фондам требуется лучшая координация в этом вопросе.

Установив, что для выбранного нами массива покрытие *FA* в *WoS* достаточно велико, мы смогли изучить в динамике вопрос о поддержке публикаций с российской аффилиацией в лучших мировых журналах. Основной результат уже описан выше: РФФИ остается лидером, но его стремительно догоняет РНФ. В сумме на эти два фонда приходится около 51% всех публикаций. При этом в абсолютном выражении число публикаций РФФИ незначительно падало на всем протяжении рассмотренного периода, а РНФ – существенно росло.

Для организаций мы видим отражение той же тенденции, причем для некоторых ведущих вузов она проявляется сильнее: рост по РНФ и снижение по РФФИ у них больше, чем в среднем по стране.

[18] Один из авторов в период работы в системе Минобрнауки РФ в 2012 г. предложил единый формат номеров грантов и проектов из средств федерального бюджета именно с целью облегчить такой анализ в разрезе грантодателей и тематик. В настоящее время, насколько можно судить, предложенный формат начинает внедряться в системе федеральных целевых программ, что в перспективе облегчит учет соответствующих публикаций.

Отметим, что доля публикаций, упоминающих оба фонда, довольно высока: в 2016-2017 гг. примерно 21% статей РФФИ упоминали также и РНФ. Такое сотрудничество (по крайней мере, в наукометрическом смысле) продолжается, несмотря на установку РНФ по недопущению двойного финансирования[19].

Выявленные существенные различия в цитируемости публикаций в одних и тех же журналах в зависимости от наличия или отсутствия поддержки РФФИ требуют дальнейшего изучения, однако уже сейчас очевидно, что и здесь между двумя основными российскими фондами есть разница. Более низкую цитируемость публикаций, поддержанных РФФИ, возможно, отчасти объясняет существенно меньший размер гранта, однако это лишь предположение.

Иностранные фонды продолжают играть важную роль в науке России, однако не демонстрируют ни положительной, ни отрицательной динамики: сотрудничество с ними остается на одном уровне. К тому же, в отличие от РНФ\РФФИ, по которым мы можем достаточно уверенно предполагать, что их средства пошли именно российским соавторам, в случае иностранных фондов речь, вероятно, чаще идет о поддержке иностранных соавторов. Доля работ с иностранным соавторством, поддержанных РНФ и РФФИ, меньше, чем в среднем по массиву статей России в списке *Nature Index*, но значительно больше, чем в среднем по всем публикациям России, отраженных в *WoS Core Collection*. Для мегагрантов, как и ожидалось, доля международных работ существенно выше среднего по списку *Nature Index*, при этом абсолютное число поддержанных этими грантами публикаций снижается. То же касается и публикаций с поддержкой «Династии», но в отличие от мегагрантов, в данном случае причина очевидна.

Напоследок, нельзя не остановиться на одном принципиальном моменте: уже в первый год работы РНФ мы наблюдаем более ста публикаций в ведущих мировых журналах с поддержкой этого фонда. Широко известно, что один только процесс рассмотрения рукописей в журналах может составлять многие месяцы и годы [29], не говоря уже о непосредственном проведении сложных изысканий, приводящих к опубликованию в этих топовых изданиях. Соответственно, мы можем утверждать, что ученые вставляют упоминание о грантовой поддержке в том числе в работы, выполненные не за счет средств данных грантов, и по всей видимости это происходит из-за требований отчетности.[20]

Такой подход, который, вероятно, получает всё большее распространение на фоне роста использования формализованных систем оценки [30], заставляет крайне осторожно подходить к трактовке чисто наукометрической информации о грантах. Фактически, есть основания говорить о быстром развитии модели гибкого публикационого пайплайна, когда у исследовательского коллектива есть поток публикаций в работе, а указания на ту или иную поддержку (а также, например, аффилиации организаций) могут подставляться в конкретные статьи в зависимости от ситуации и требований отчетности, а вовсе не реального вклада.

ЗАКЛЮЧЕНИЕ

Проведенное нами изучение грантовой поддержки научных публикаций (*Funding Acknowledgments*) стало первым российским исследованием такого рода за многие годы и впервые включило прямое сравнение полноты индексирования *FA* в *WoS* и Scopus, причем в качестве объекта сопоставления были выбраны публикации России в наиболее престижных научных журналах мира. Помимо этого были получены актуальные для научной политики сравнительные данные по крупнейшим грантовым фондам, активным в России, показывающие, насколько они важны для ведущих российских ученых. Такое сравнение особенно актуально в свете продолжающихся обсуждений[21] о реформе крупнейших отечественных грантовых фондов.

Надеемся, что своим исследованием мы внесли вклад как в изучение применимости *FA* для прикладного и теоретического науковедения, так и в непосредственное картирование грантового ландшафта России 2010-х гг. Несмотря на обозначенные нами ограничения в трактовках, данные *FA* являются уникальным источником, позволяющим связать расходы и результаты как по грантам и странам, так и по отдельным проектам, и отражающим быстрое изменение каналов финансирования. В дальнейшем мы рассчитываем продолжить начатое изучение *Funding Acknowledgments* в российских публикациях, распространив его на весь массив статей страны, а также на уровень отдельных грантов и их взаимосвязи.

* * *

Авторы благодарят Александра Балышева (НИУ ВШЭ) за консультации и помощь в сборе данных о номерах грантов РФФИ и РНФ.

[19] Характерна цитата руководителя РНФ А.В. Хлунова: «Ограничение источников финансирования – абсурд? Нет, это не абсурд. Вот [на пресс-конференции рядом со мной] сидит Геннадий Андреевич Месяц. Достаточно странно, если Г. А. на протяжении пяти лет будет платить заработную плату лаборатории, которая в дальнейшем получит деньги РНФ на этот же проект. Кроме того, этот же проект получит деньги в Российском фонде фундаментальных исследований, Национальной технологической базе и Федеральной целевой программе по приоритетным направлениям. Это уже называется мошенничеством». Источник: https://trv-science.ru/2014/04/08/rnf-teoriya-vs-praktika/

[20] Например, статья Capela F., Pshirkov M., Tinyakov P. Adiabatic contraction revisited: Implications for primordial black holes // Physical Review D - Particles, Fields, Gravitation and Cosmology. – 2014. – № 90(8). DOI:10.1103/PhysRevD.90.08350, изначально опубликованная на arxiv.org 27 марта 2014 г. и полученная журналом 10 апреля 2014 г., содержит указание на грант РНФ 14-12-00146, победивший в конкурсе на получение грантов по приоритетному направлению деятельности РНФ "Проведение фундаментальных научных исследований и поисковых научных исследований отдельными научными группами" с дедлайном по приему заявок до 11 марта 2014 г.

[21] См., например, публикацию «Ученым денег не видать: уничтожают самый демократичный научный фонд РФФИ» в газете «Московский комсомолец» от 9 сентября 2019 г.

Приложение 1

Пример формата данных в выгрузках

Пример	**Title**	Muon polarization in the MEG experiment: Predictions and measurements
	Source title	European Physical Journal C
	DOI	10.1140/epjc/s10052-016-4047-3
Scopus	**Funding Details**	Ministry of Education and Science of the Russian Federation, Minobrnauka: RFBR 14-22-03071 22000004, 26000004 Ministero dell'Istruzione, dell'Università e della Ricerca, MIUR Physicians' Services Incorporated Foundation, PSI Instituto Nazionale di Fisica Nucleare, INFN Schweizerischer Nationalfonds zur Förderung der Wissenschaftlichen Forschung, SNF: CH, 200021_137738, DOE DEFG02-91ER40679
	Funding Text 1	We are grateful for the support and cooperation provided by PSI as the host laboratory and to the technical and engineering staff of our institutes. This work is supported by SNF Grant 200021_137738 (CH), DOE DEFG02-91ER40679 (USA), INFN (Italy) and MEXT KAKENHI 22000004 and 26000004 (Japan). Partial support of the Italian Ministry of University and Research (MIUR) Grant RBFR08XWGN, Ministry of University and Education of the Russian Federation and Russian Fund for Basic Research Grants RFBR 14-22-03071 are acknowledged.
WoS	**FU**	SNF (CH) [200021_137738]; DOE (USA) [DEFG02-91ER40679]; INFN (Italy); MEXT KAKENHI (Japan) [22000004, 26000004]; Italian Ministry of University and Research (MIUR) [RBFR08XWGN]; Ministry of University and Education of the Russian Federation; Russian Fund for Basic Research [RFBR 14-22-03071]
	FX	We are grateful for the support and cooperation provided by PSI as the host laboratory and to the technical and engineering staff of our institutes. This work is supported by SNF Grant 200021_137738 (CH), DOE DEFG02-91ER40679 (USA), INFN (Italy) and MEXT KAKENHI 22000004 and 26000004 (Japan). Partial support of the Italian Ministry of University and Research (MIUR) Grant RBFR08XWGN, Ministry of University and Education of the Russian Federation and Russian Fund for Basic Research Grants RFBR 14-22-03071 are acknowledged.

Приложение 2

Фонды и маски номеров мегагрантов

РФФИ	'RUSSIAN FOUNDATION FOR BASIC RESEARCH' 'RFBR' 'RUSSIAN FOUNDATION OF BASIC RESEARCH' 'RUSSIAN FOUNDATION FOR BASIC RESEARCH RFBR' 'RFBR RUSSIA' 'RUSSIAN FOUNDATION FOR BASIC RESEARCHES' 'RUSSIAN FUND FOR BASIC RESEARCH' 'RFFI' 'RUSSIAN FOUNDATION FOR FUNDAMENTAL RESEARCH' 'RUSSIAN FUND OF BASIC RESEARCH' 'RFBR GRANT' 'RFBR CNRS' 'DFG RFBR' 'RUSSIAN FOUNDATION OF BASIC RESEARCH RFBR' 'RUSSIAN BASIC RESEARCH FOUNDATION' 'RUSSIAN FOUNDATION OF BASIC RESEARCHES' 'Russian Foundation of Fundamental Research' 'Russian Foundation Basic Research' 'Russian Foundation for Basic Reseach' 'RFBR (Russia)'
РНФ	'Russian Science Foundation' 'Russian Scientific Foundation' 'Russian Scientific Fund' 'Russian Science Fund' 'russian research fund' 'russian research foundation' 'RSF ' 'RSCF'

Династия	'dynasty' 'dinasty' 'dinasti' 'dynasti' 'dinastiya' 'dinastia' 'dynastia'
Мегагранты	import re result = re.findall(r'\d{2}.\w\d{2}.31.00\d{2}', string) result1 = re.findall(r'\d{2}.\d{3}.31.00\d{2}', string)

Приложение 3

Текстовые запросы с использованием операторов *WoS Advanced Search*

Грантодатель	Расширенный поисковый запрос для базы данных *WoS*
РФФИ	ft=(RUSSIAN FOUNDATION FOR BASIC RESEARCH or RFBR or RUSSIAN FOUNDATION OF BASIC RESEARCH or RUSSIAN FOUNDATION FOR BASIC RESEARCH RFBR or RFBR RUSSIA or RUSSIAN FOUNDATION FOR BASIC RESEARCHES or RUSSIAN FUND FOR BASIC RESEARCH or RFFI or RUSSIAN FOUNDATION FOR FUNDAMENTAL RESEARCH or RUSSIAN FUND OF BASIC RESEARCH or RFBR GRANT or RFBR CNRS or DFG RFBR or RUSSIAN FOUNDATION OF BASIC RESEARCH RFBR or RUSSIAN BASIC RESEARCH FOUNDATION or RUSSIAN FOUNDATION OF BASIC RESEARCHES or RFBR (Russia) or Russian Foundation of Fundamental Research or Russian Foundation Basic Research or Russian Foundation for Basic Reseach)
РНФ	(ft=(Russian Science Foundation or Russian Scientific Foundation or Russian Scientific Fund or Russian Science Fund) or fg=(Russian Science Foundation or Russian Scientific Foundation or Russian Scientific Fund or Russian Science Fund) or ft=(russian research fund) or fg=(russian research fund) or ft=(russian research foundation) or fg=(russian research foundation) or ft=(rscf) or fg=(rscf))
Мегагранты	ft=(14-a??-31-00*) or ft=(14-b??-31-00*) or ft=(14-c??-31-00*) or ft=(14-d??-31-00*) or ft=(14-e??-31-00*) or ft=(14-f??-31-00*) or ft=(14-g??-31-00*) or ft=(14-h??-31-00*) or ft=(14-i??-31-00*) or ft=(14-j??-31-00*) or ft=(14-k??-31-00*) or ft=(14-l??-31-00*) or ft=(14-m??-31-00*) or ft=(14-n??-31-00*) or ft=(14-o??-31-00*) or ft=(14-p??-31-00*) or ft=(14-q??-31-00*) or ft=(14-r??-31-00*) or ft=(14-s??-31-00*) or ft=(14-t??-31-00*) or ft=(14-u??-31-00*) or ft=(14-v??-31-00*) or ft=(14-w??-31-00*) or ft=(14-x??-31-00*) or ft=(14-y??-31-00*) or ft=(14-z??-31-00*) or fg=(14-a??-31-00*) or fg=(14-b??-31-00*) or fg=(14-c??-31-00*) or fg=(14-d??-31-00*) or fg=(14-e??-31-00*) or fg=(14-f??-31-00*) or fg=(14-g??-31-00*) or fg=(14-h??-31-00*) or fg=(14-i??-31-00*) or fg=(14-j??-31-00*) or fg=(14-k??-31-00*) or fg=(14-l??-31-00*) or fg=(14-m??-31-00*) or fg=(14-n??-31-00*) or fg=(14-o??-31-00*) or fg=(14-p??-31-00*) or fg=(14-q??-31-00*) or fg=(14-r??-31-00*) or fg=(14-s??-31-00*) or fg=(14-t??-31-00*) or fg=(14-u??-31-00*) or fg=(14-v??-31-00*) or fg=(14-w??-31-00*) or fg=(14-x??-31-00*) or fg=(14-y??-31-00*) or fg=(14-z??-31-00*) or ft=(11-G??-31-00*) or fg=(11-g??-31-00*) or ft=(14.641.31.00*) or fg=(14.641.31.00*) or ft=(11.634.31.00*) or fg=(11.634.31.00*)
Династия	ft=(d?nast*)

Приложение 4

Доля публикаций в журналах списка *Nature Index* с 100+ авторами ряда ведущих вузов и НИИ РАН (%)

Университет	2014	2015	2016	2017
ВШЭ	0	0	0	3
ДВФУ	0	0	0	0
ИБХ РАН	0	0	0	0
ИОНХ РАН	0	0	0	0
ИОХ РАН	0	0	0	0
ИТМО	0	0	0	0
ИФЗ РАН	0	0	0	0
КФУ	10	7	36	2
ЛЭТИ	0	0	0	0

Университет	2014	2015	2016	2017
МГМУ	0	0	0	0
МГУ	48	53	50	51
МИСиС	0	0	0	0
МИФИ	82	76	73	73
МФТИ	44	53	48	57
НГУ	69	69	62	72
ННГУ	0	0	0	0
СамГУ	0	0	9	0
СПбГПУ	62	72	81	82
СПбГУ	10	12	12	14
СФУ	0	0	0	0
ТГУ	40	61	66	58
ТПУ	0	0	0	28
УрФУ	0	0	0	2
ФИ РАН	73	72	75	73
ФТИ РАН	1	0	1	2

Приложение 5

Критерий U-Манна-Уитни для публикаций 2014-2017 гг. с поддержкой РФФИ и РНФ и без нее

Ранги		Средний ранг			Сумма рангов		
Фонд	N	JNCI	FWCI	CNCI	JNCI	FWCI	CNCI
РФФИ	2472	3119,00	3004,19	2974,33	7710170,00	7426357,00	7352533,00
не РФФИ	3963	3279,75	3351,37	3370,00	12997660,00	13281473,00	13355297,00
Всего	6435						
РНФ	1372	3218,00	3214,92	3211,41	4415093,00	4410871,50	4406052,00
не РНФ	5063	3218,00	3218,83	3219,79	16292737,00	16296958,50	16301778,00
Всего	6435						

Статистики критерия (группирующая переменная: фонд)			
РФФИ/не РФФИ	JNCI	FWCI	CNCI
Статистика U Манна-Уитни	4653542,000	4369729,000	4295905,000
Статистика W Уилкоксона	7710170,000	7426357,000	7352533,000
Z	-3,376	-7,292	-8,310
Асимпт. знч. (двухсторонняя)	0,001	0,000	0,000
РНФ/не РНФ	JNCI	FWCI	CNCI
Статистика U Манна-Уитни	3473215,000	3468993,500	3464174,000
Статистика W Уилкоксона	4415093,000	4410871,500	4406052,000
Z	0,000	-0,069	-0,148
Асимпт. знч. (двухсторонняя)	1,000	0,945	0,882

СПИСОК ЛИТЕРАТУРЫ

1. Дежина И.Г. Государственное регулирование науки в России. – М.: Магистр, 2008. – 430 с.
2. Гохберг Л.М., Заиченко С.А., Китова Г.А., Кузнецова Т.Е. Научная политика: глобальный контекст и российская практика. – М.: Изд. дом ВШЭ, 2011. – 308 с.
3. Деловой климат в российской науке – Doing Science / С.В. Бредихин, В.В. Власова, М.А. Гершман и др.; науч. ред. Л.М. Гохберг; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2019. – 212 с.
4. Robitaille J.P., Macaluso B., Pollitt A., Gunashekar S., Larivière V. Comparative Scientometric Assessment of the Results of ERC-Funded Projects. Bibliometric Assessment Report (D5). European Commission: ERC Executive Agency [отчет]. – 2015. – URL: https://erc.europa.eu/sites/default/files/document/file/ERC_Bibliometrics_report.pdf (дата обращения 15.02.2019).
5. Markusova V.A., Libkind A., Aversa E. Impact of competitive funding on research output in Russia // Collnet Journal of Scientometrics and Information Management. – 2012. – Vol. 6, №1. – P. 61–69.
6. Díaz-Faes A., Bordons M. Acknowledgments in scientific publications: Presence in spanish science and text patterns across disciplines // Journal of the Association for Information Science and Technology. – 2014. – Vol. 65, № 9. – P. 1834-1849.
7. Paul-Hus A., Desrochers N., Costas R. Characterization, description, and considerations for the use of funding acknowledgement data in web of science // Scientometrics. – 2016. – Vol. 108, № 1. – P. 167-182.

8. Grassano N., Rotolo D., Hutton J., Lang F., Hopkins M.M. Funding data from publication acknowledgments: Coverage, uses, and limitations // Journal of the Association for Information Science and Technology. – 2017. – Vol. 68, № 4. – P. 999-1017.
9. Rigby J. Systematic grant and funding body acknowledgement data for publications: New dimensions and new controversies for research policy and evaluation // Research Evaluation. – 2011. – Vol. 20, № 5. – P. 365–375.
10. Tang L., Hu G., Liu W. Funding acknowledgment analysis: Queries and caveats // Journal of the Association for Information Science and Technology. – 2017. – Vol. 68, № 3. – P. 790-794.
11. Álvarez-Bornstein B., Morillo F., Bordons M. Funding acknowledgments in the web of science: Completeness and accuracy of collected data // Scientometrics. – 2017. – Vol. 112, № 3. – P. 1793-1812.
12. Mejia C., Kajikawa Y. Using acknowledgement data to characterize funding organizations by the types of research sponsored: The case of robotics research // Scientometrics. – 2018. – Vol. 114, № 3. – P. 883-904.
13. Kokol P., Vošner H.B. Nursing informatics research: A bibliometric analysis of funding patterns // Online Journal of Nursing Informatics. – 2017. – Vol. 21, № 2.
14. Huang M., Huang M. An analysis of global research funding from subject field and funding agencies perspectives in the G9 countries // Scientometrics. – 2018. – Vol. 115, № 2. – P. 833-847.
15. Kokol P., Vošner H.B. Discrepancies among Scopus, Web of Science, and PubMed coverage of funding information in medical journal articles // Journal of the Medical Library Association. – 2018. – Vol. 106, № 1. – P. 81-86.
16. Dezhina I.G. Science and innovation policy of the russian government: A variety of instruments with uncertain outcomes? // Public Administration Issues. – 2017. – Vol. 5. – P. 7-26.
17. Wouters P., Thelwall M., Kousha K., Waltman L., de Rijcke S., Rushforth A., Franssen T. The Metric Tide: Literature Review (Supplementary Report I to the Independent Review of the Role of Metrics in Research Assessment and Management). – HEFCE, 2015. DOI: 10.13140/RG.2.1.5066.3520
18. Mongeon P., Paul-Hus A. The journal coverage of Web of Science and Scopus: a comparative analysis // Scientometrics. – 2016. – Vol. 106, № 1. – P. 213–228.
19. Лазар М.Г., Стрельцова Е.А. Грантовая система финансирования российской науки: итоги одного социологического опроса // Социология науки и технологий. – 2015. – № 6(3). – С. 38-49.
20. Ильина И.Е. Анализ деятельности научных фондов, обеспечивающих поддержку фундаментальных исследований в России // Науки. Инновации. Образование. – 2015. – № 18. – С. 179-203.
21. Garfield E. The Mystery of the Transposed Journal Lists—Wherein Bradford's Law of Scattering Is Generalized According to Garfield's Law of Concentration // Current Content No. 75 (August 4, 1971) Reprinted in Essays of an Information Scientist; ISI Press: Philadelphia, PA, USA. – 1977. – Vol. 1. – P. 222–223.
22. Heckman J., Moktan S. Publishing and Promotion in Economics: The Tyranny of the Top Five (№ w25093). – Cambridge, MA: National Bureau of Economic Research, 2018.
23. Moed H.F., Markusova V., Akoev M. Trends in Russian research output indexed in Scopus and Web of Science // Scientometrics. – 2018. – Vol. 116, № 2. – P. 1153-1180.
24. Hicks D., Wouters P., Waltman L., de Rijcke S., Rafols I. Bibliometrics: The Leiden Manifesto for research metrics // Nature. – 2015. – Vol. 520, № 7548. – P. 429–431.
25. Bendels M.H.K., Müller R., Brueggmann D., Groneberg D.A. Gender disparities in high-quality research revealed by Nature Index journals // PLOS ONE. – 2018. – Vol. 13, № 1: e0189136.
26. Waltman L. A review of the literature on citation impact indicators // Journal of Informetrics. – 2016. – Vol. 10, № 2. – P. 365–391.
27. Frascati Manual 2015: Guidelines for Collecting and Reporting Data on Research and Experimental Development, The Measurement of Scientific, Technological and Innovation Activities. – OECD Publishing, Paris, 2015. DOI: 10.1787/9789264239012-en
28. Battiston F., Musciotto F., Wang D., Barabási A.-L., Szell M., Sinatra R. Taking census of physics // Nature Reviews Physics. – 2019. – Vol. 1, № 1. – P. 89–97.
29. Björk B.-C., Solomon D. The publishing delay in scholarly peer-reviewed journals // Journal of Informetrics. – 2013. – Vol. 7, № 4. – P. 914–923.
30. Wilsdon J., Allen L., Belfiore E., Campbell P., Curry S., Hill S., Johnson B. The Metric Tide: Report of the Independent Review of the Role of Metrics in Research Assessment and Management. – HEFCE, 2015. DOI: 10.13140/RG.2.1.4929.1363.

Материал поступил в редакцию 12.11.19.

Сведения об авторах

СТЕРЛИГОВ Иван Андреевич – директор Наукометрического центра Национального исследовательского университета «Высшая школа экономики», Москва
e-mail: isterligov@hse.ru

САВИНА Татьяна Федоровна – кандидат физико-математических наук, ведущий эксперт Наукометрического центра Национального исследовательского университета «Высшая школа экономики»
e-mail: tsavina@hse.ru

ЧИЧКОВА Александра Олеговна – независимый исследователь, Москва
e-mail: chichkova.aleksandra@gmail.com

УДК 338.2(470):[004.056:316.776]

Л.В. Астахова

Проблемы культуры информационной безопасности в условиях цифровой экономики*

Выявлено противоречие между мировыми тенденциями развития компетенций человека (сотрудника организации в области информационной безопасности и гражданина), отраженными в международном праве и в зарубежной социальной науке и практике, и содержанием задач федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (2018). Показана ограниченность реализации системы повышения грамотности в области кибербезопасности как планируемого результата этой программы. Обоснована активная субъектная роль пользователя цифровых ресурсов в обеспечении информационной безопасности в условиях культуры цифрового общества и цифровой экономики. Изложены требования культурологического подхода к этой роли. Выявлены содержание понятия культуры информационной безопасности, факторы, влияющие на её уровень, а также проблема её развития в новых условиях.

Ключевые слова: *культура информационной безопасности, осведомленность, грамотность, сотрудник, организация, цифровая экономика, цифровая культура, цифровая безопасность, информационный центр, библиотека, машинное обучение*

DOI: 10.36535/0548-0019-2020-02-3

Цифровая трансформация общества актуализировала проблемы информационной безопасности личности, социума и государства в глобальном масштабе. Её технологии стремительно развиваются вслед за новыми угрозами, среди которых особую опасность занимают угрозы со стороны человека. Понимание их критичности пришло не сразу, долгое время доминировали технократические представления об этой сфере. Человек как главный источник угроз информационной безопасности изучается много лет, но по-прежнему остается критически важной областью теоретических и эмпирических исследований. Согласно отчету *PriceWaterhouseCoopers*, в 2018 г. основными источниками угроз безопасности были люди: сотрудники (30%), бывшие сотрудники (27%) и неизвестные хакеры (23%). Основные воздействия заключаются в компрометирующих записях о клиентах и сотрудниках, и в потере или повреждении личных данных [1]. Парадоксально, но при доминирующем числе инцидентов по вине человека только у 34% участников исследования внедрена программа повышения осведомленности сотрудников о различных аспектах безопасности. При этом обязательное обучение политике защиты данных и ее применение на практике организовано всего лишь у 31% респондентов [2].

В процессе решения проблемы снижения рисков информационной безопасности из-за человека используются разные термины: повышение осведомленности, грамотности, культуры информационной безопасности (ИБ), культуры кибербезопасности, культуры цифровой безопасности и др. Правда, последние два термина (культура кибербезопасности и культура цифровой безопасности) еще не вошли в число широкораспространенных.

В международных стандартах по обеспечению информационной безопасности широко используется понятие осведомленности – *Security Awareness*. Самое раннее упоминание «осведомленности» встречается в документе американского Национального института стандартов и технологий (*The National Institute of Standards and Technology – NIST*) NIST 800-16-1998 Information Technology Security Training Requirements: A Role- and Performance-Based Model (Требования к обучению безопасности информационных технологий: модель на основе ролей и производительности). В 2003 г. в NIST SP 800-50-2003 Building an Information Technology Security Awareness and Training Program (Создание программы повышения осведомленности в области безопасности информационных технологий) появляется понятие *Security Awareness* [3].

Международные стандарты серии ISO/IEC 27000 (и их российские национальные аналоги ГОСТ Р ИСО/МЭК 27000) по управлению информационной безопасностью содержат как требования, так и реко-

* Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г., соглашение № 02.A03.21.0011).

мендации для организаций по обучению персонала вопросам информационной безопасности с целью повышения их осведомленности.

Согласно стандарту ISO/IEC 27000:2012 Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary (Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Общий обзор и терминология), на реализацию и успешное внедрение системы менеджмента информационной безопасности (СМИБ), позволяющей организации достигать своих бизнес-целей, влияет большое количество факторов. Один из них – эффективная программа повышения осведомленности, обучения и подготовки по ИБ, доводящая до сведения всех сотрудников их обязанности по обеспечению ИБ, сформулированные в политиках и стандартах ИБ, и побуждающая их к соответствующим действиям [4].

Вопросам осведомленности по ИБ в стандарте ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements («Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента ИБ – Требования») посвящен подраздел 7.3. *Awareness* (Осведомленность). В нем приведены **требования** к лицам, осуществляющим работу под контролем организации: они должны быть осведомлены о политике ИБ; о своем вкладе в обеспечение эффективности системы менеджмента ИБ, включая выгоды от улучшения функционирования ИБ; о последствиях несоблюдения требований системы менеджмента ИБ [5].

Стандарт ISO/IEC 27002:2013 Information Technology – Security Techniques – Code of Practice for Information Security Controls (Информационная технология – Методы и средства обеспечения безопасности – Свод правил по мерам и средствам контроля и управления информационной безопасностью) содержит **рекомендации** по осведомленности, обучению и тренингам в области информационной безопасности. В разделе 8.2. «В период занятости» этого стандарта отмечается, что в организации необходимо обеспечить уверенность в том, что сотрудники и сторонние пользователи осведомлены о своих обязанностях в отношении ИБ и выполняют их. В пункте 8.2.2 *Information Security Awareness, Education and Training* (Осведомленность, обучение и подготовка в области ИБ) указано, что все сотрудники организации и при необходимости пользователи сторонних организаций должны проходить соответствующую программу информирования, обучение и подготовку и получать на регулярной основе обновленные варианты политик и процедур организации, необходимых для выполнения их рабочих функций. В этом же стандарте приведены конкретные рекомендации по разработке программы осведомленности и обучения в области ИБ [6].

Рекомендации по разработке программы информирования и обучения информационной безопасности представлены в п. 9.4.2 стандарта ISO/IEC 27003:2010 Information technology – Security techniques – Information security management systems implementation guidance (Информационная технология – Методы и средства обеспечения безопасности – Руководство по реализации системы менеджмента информационной безопасности) [7]. В новой версии этого стандарта приведенные рекомендации отражены в п.7.3. *Awareness* [8].

Повышение осведомленности сотрудников организации по вопросам ИБ – это также предмет различных рекомендаций и руководств. В 2008 г. силами агентства Европейского Союза по сетевой и информационной безопасности (ENISA) разработан документ «Information Security Awareness in Financial Organisations» («Осведомленность об информационной безопасности в финансовых организациях»), в котором приведены конкретные рекомендации для финансовых организаций [9]. В 2010 г. разработаны новые рекомендации, которые распространяются на все сферы деятельности и содержат подробное описание действий по организации процесса осведомленности в компании, а также советы и инструкции по созданию собственной программы по осведомленности [10].

Исследованиями и практикой в области *Security Awareness* активно занимается европейская научно-образовательная организация The SANS Institute, деятельность которой связана с исследованиями и образовательными программами в области ИБ, системного администрирования, аудита. В 2011 г. она разработала «Модель зрелости осведомленности по вопросам безопасности» (*Security Awareness Maturity Model*), которая позволяет организациям определить, на каком этапе находится их программа повышения осведомленности о безопасности в настоящее время и в каком направлении в дальнейшем организация должна продвигаться в данном направлении [11].

Сегодня активно развивается рынок сервисов повышения осведомленности по ИБ. Самыми крупными мировыми провайдерами платформ *Security Awareness* являются: PhishMe Knowbe4 Wombat Security MediaPro Inspired eLearning и др. [12].

Для повышения осведомленности широких масс в области ИБ проводятся специальные мероприятия. Так, в США ежегодно, начиная с 2004 г., проводится месячник под эгидой Департамента внутренней безопасности США совместно с Альянсом национальной кибербезопасности (National Cyber Security Alliance (NCSA)), куда входят такие компании, как Google, Cisco, Microsoft, Intel, SANS, Symantec, Facebook, Raytheon. Мероприятие называется National Cyber Security Awareness Month (NCSAM – Национальный месяц осведомленности о кибербезопасности). В его рамках рассматриваются такие темы, как: простые шаги к онлайн-безопасности; кибербезопасность на рабочем месте — дело каждого; сегодняшние прогнозы для завтрашнего Интернета; защита критической инфраструктуры от киберугроз и др. [13]. Целевой аудиторией месячника в США являются: дети (от 3-х до 7-ми лет); школьники; родители и учителя; молодые работники; пожилые американцы; сотрудники государственных органов, различных бизнес-структур, малого бизнеса, правоохранительных органов [14].

В Европе с 2012 г. ежегодно под эгидой ENISA тоже проходят подобные мероприятия под названием

European Cyber Security Month (ECSM). ECSM — это компания по повышению осведомленности по ИБ в ЕС, которая содействует кибербезопасности граждан и организаций и подчеркивает простые шаги, которые могут быть предприняты для защиты личных, финансовых или профессиональных данных. Основная цель этого мероприятия – повышение осведомленности, изменение поведения и предоставление ресурсов для всех о том, как защитить себя в Интернете. Действия по пропаганде осведомленности в области кибербезопасности регулируются правительством и распространяются на всех граждан, начиная от госорганов и корпораций и заканчивая простыми гражданами [15].

Наряду с понятием осведомленности (*Awareness*) в начале XXI в. в обиход вошло понятие культуры информационной безопасности (Information Security Culture – ISC). Ключевым стал 2002 г., когда Генеральная Ассамблея ООН в Резолюции «Создание глобальной культуры кибербезопасности» предложила государствам – членам развивать культуру кибербезопасности при применении и использовании информационных технологий [16]. Большая работа была проведена также Организацией по экономическому сотрудничеству и развитию (OECD), которая в 2002 г. опубликовала Рекомендации Совета по созданию глобальной культуры информационной безопасности «Безопасность информационных систем и сетей – на пути к культуре безопасности» [17].

В последние годы активно разрабатывается концепция цифровой среды как киберпространства, а также концепции культуры кибербезопасности (Cyber Security Culture –CSC) и цифровой безопасности (*digital security*) как частей культуры информационной безопасности. В 2015 г. OECD мотивирует создание культуры цифровой безопасности, в которой заинтересованные стороны должны учитывать риск своей собственной деятельности в цифровой среде [18]. Под эгидой ENISA, которое является центром экспертизы сетевой и информационной безопасности ЕС, в 2017 г. выходит документ «Cyber Security Culture in organisations», в котором представлены рекомендации по созданию и запуску программы повышения культуры кибербезопасности, а также описывается передовой опыт, выявленный в тех организациях, которые уже внедрили зрелые программы CSC, и которые специально распределены по категориям и адаптированы к разным аудиториям внутри организации, от высшего руководства до команды по информационной безопасности. Для облегчения разработки и реализации программы по культуре кибербезопасности в этом документе представлено восемь этапов реализации, а также дано подробное руководство по каждому из этих этапов. Кроме того, в нем обоснованы методы создания CSC для организации, показатели для измерения воздействия деятельности CSC, а также стратегии для создания надежного экономического обоснования для распределения внутренних ресурсов на будущие мероприятия по культуре кибербезопасности. В этом исследовании определены методологические инструменты и пошаговые инструкции для тех, кто хочет начать или усовершенствовать собственную программу культуры кибербезопасности в своих организациях, включая ресурсы для разработки бизнес-обоснования обеспечения финансирования такой программы [19].

Повышенный интерес к проблеме культуры информационной безопасности на организационном уровне привел к росту ее теоретических и эмпирических исследований. В настоящее время количество зарубежных публикаций по теме исчисляется сотнями. Ученые работают над определением термина «культура информационной безопасности» [20, 21 и др.], методами ее оценки [22 и др.] и др. Уже появились зарубежные исследования в виде обзоров. Так, европейские ученые выполнили исследование культуры информационной безопасности в период с 2000 по 2013 гг. [23]. Обзор определений и структур культуры информационной безопасности за период с 2003 по 2016 гг. был проведен малазийскими экспертами [24]. Члены еще одного научного коллектива [25] провели систематический обзор 405 публикаций, изданных с 2000 по 2017 гг., с использованием метода Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Все исследователи делают выводы об отсутствии единого подхода к определению культуры информационной безопасности, о несогласованности в определении обусловливающих ее факторов и т.д.

В научных публикациях нашли отражение и проблемы соотношения культуры информационной безопасности и кибербезопасности [26]. Культура кибербезопасности связана с тем, как люди воспринимают кибербезопасность и каково их поведение в киберпространстве, что влияет на защиту цифровой информации, систем и людей [27]. Сделана попытка определения культуры информационной безопасности, включающей в себя культуру кибербезопасности [28]. Иными словами, не только практика, но и наука о культуре ИБ находятся сегодня на пике своего развития.

В России гораздо позже стали уделять внимание вопросам человеческих (кадровых) рисков для информационной безопасности организации. Это связано с тем, что чрезвычайно «живучим» в нашей стране оказался стереотип об информационной безопасности как сугубо технической сфере деятельности, далекой от гуманитарных проблем. Опираясь на зарубежный опыт, в России обратили внимание на осведомленность в области информационной безопасности лишь в начале XXI в., когда началась гармонизация вышеупомянутых стандартов ИСО/МЭК по управлению информационной безопасностью. Затем требования по осведомленности в области информационной безопасности были приведены в Федеральном законе Российской Федерации № 152-ФЗ от 27 июля 2006 г. «О персональных данных». Статья 18.1 пункт 1 подпункт 6 «Ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников»[1] относит обучение и ознакомление работников опера-

[1] Федеральный закон Российской Федерации № 152-ФЗ от 27 июля 2006 года «О персональных данных». – URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения 02.10.2019)

тора персональных данных с требованиями о защите персональных данных к возможной, но все же частной мере. На практике это ознакомление и обучение заканчиваются росписью в акте ознакомления с документами в организации.

Требования к повышению осведомленности работников в области информационной безопасности содержатся в приказе Федеральной службы по техническому и экспортному контролю (ФСТЭК) России по защите информации в автоматизированных системах управления производственными и технологическими процессами (от 14 марта 2014 г. № 31)[2], в котором требования к мерам повышения осведомленности сформулированы в виде класса мер «XVIII. Информирование и обучение персонала (ИПО)». Этот блок включает требования к разработке правил и процедур (политик) информирования и обучения персонала, а также требования к обучению и информированию персонала по вопросам защиты информации. К сожалению, требования этого приказа выполняются только на основе решения владельца автоматизированной системы.

В приказе «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (от 25 декабря 2017 г. № 239) приводится блок требований «XVII. Информирование и обучение персонала (ИПО)», как и в Приказе №31. Отличием является лишь включение нового требования к контролю осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы[3].

Эти вопросы отражены и в отраслевых стандартах России. Так, в п. 8.9 СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» изложены требования к разработке и организации реализации программ по обучению и повышению осведомленности в области информационной безопасности [29]. Весьма оптимистичны в настоящее время планы ЦБ РФ преобразовать рекомендательный статус этого стандарта в разряд обязательного для всех финансовых организаций РФ.

В Доктрине информационной безопасности Российской Федерации (2016) «низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности» названа одной из угроз ИБ, указана необходимость поддержки образовательных программ и организаций, работающих в данной области [30]. Таким образом, в содержании концептуальных и нормативных документов России требование наличия программы повышения осведомленности не является обязательным, способы и пути ее решения не конкретизируются.

Несмотря на недостаток нормативного регулирования, в России развивается практика в этой области. Например, как и на Западе, ежегодно с 2008 г. проводится «Неделя безопасного Рунета». Эта серия мероприятий, приуроченных к Международному Дню безопасного Интернета, проводится по инициативе Региональной общественной организации «Центр интернет-технологий» (РОЦИТ) и российского офиса Microsoft. Однако, в отличие от западных мероприятий, «Неделя безопасного Рунета» ориентирована только на детей и их родителей [15]. Начал развиваться российский рынок сервисов повышения осведомленности по ИБ среди вендоров – «Лаборатория Касперского», Phishman, «Антифишинг», UBS, «Системный софт», DeteAct, «Ростелеком» и др. [12].

Параллельно с проблемами осведомленности в России концептуализируется культурологический подход к решению проблемы человеческих рисков – с помощью повышения культуры информационной безопасности. Отрадно, что мероприятия федерального проекта «Информационная безопасность» национальной программы «Цифровая экономика Российской Федерации» (утверждена президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. N 16) направлены на реализацию 4-х ключевых направлений: повышение уровня защищенности личности, информационной безопасности и устойчивости сетей связи общего пользования; создание новых сервисов (услуг) для граждан, гарантирующих защиту их персональных данных; профилактика и выявление правонарушений с использованием информационных технологий против общества и бизнеса; разработка новых механизмов поддержки отечественных разработчиков программного обеспечения и компьютерного оборудования в сфере информационной безопасности. Наряду с прочими мероприятиями, в рамках этих направлений планируется осуществить «развитие подходов к повышению грамотности и практико-ориентированной подготовке в области кибербезопасности для представителей бизнеса и государства на базе опыта ведущих компаний цифровой экономики». До 31 декабря 2021 г. планируется «**разработать предложения** по популяризации добровольного страхования рисков информационной безопасности и **повышению киберкультуры»** (п.1.35)[4].

[2] Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868- (дата обращения 02.10.2019)

[3] Приказ ФСТЭК от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (в ред. приказа ФСТЭК России от 26 марта 2019 г. n 60)». – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239 (дата обращения – 02.10.2019

[4] Паспорт национальной программы "Цифровая экономика Российской Федерации" (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. N 16). – URL: https://base.garant.ru/72190282/ (дата обращения: 24.09.2019).

К сожалению, в Паспорте этого проекта термин «киберкультура» заменен на **«систему повышения грамотности в области информационной безопасности»** (п.1.55)[5].

В рамках этой системы планируется разработать «не менее 10 учебных курсов по 4 направлениям, связанным с ИБ; ввести в эксплуатацию платформу управления обучением, включающую разработанные учебные курсы по ИБ; подготовить не менее 10 специальных практических комплексов для проведения семинаров и практикумов; провести не менее 100 образовательных мероприятий (лекций, семинаров, вебинаров и пр.) для слушателей, включая представителей МВД России, Следственного комитета, Генпрокуратуры и бизнес-структур; для организации обучения привлечь не менее 3 ведущих отечественных компаний в сфере информационной безопасности».

С сожалением можно констатировать, что массовый характер мероприятий по повышению осведомленности в области ИБ в этом документе не планируется. Да и неожиданный отказ от понятия «киберкультура» – это шаг назад. Невольно вспоминается, как недопустимо долго в нашей стране происходило переформатирование установки с информационной грамотности на информационную культуру, их отождествление. От первого упоминания термина «информационная культура» [31] до сегодняшнего дня прошло почти полвека, однако многочисленные исследования показывают, что и до сих пор уровень этой культуры низок. Российские ученые справедливо называют концепцию информационной грамотности рациональной, ибо она выросла из американских стандартов информационной грамотности и традиций американской системы образования с присущими ей утилитаризмом и практицизмом. Однако, в связи с тем, что невозможно формировать информационную грамотность без мотивирования человека, не обращаясь к его духовной сфере, в России появилась концепция информационной культуры личности как «грань общей культуры человека, которая включает в себя в качестве неотъемлемого компонента информационную грамотность» [32]. Информационную культуру личности невозможно рассматривать вне информационного мировоззрения и ценностных аспектов, вне норм информационного поведения человека в сети и др. [33]. Поэтому «информационная культура личности» – более широкое понятие, чем «информационная грамотность». Оно, в отличие от информационной грамотности, включает в свой состав информационное мировоззрение и характеризуется интегрированностью в сферу культуры. Это позволяет обеспечить синтез и целостность традиционной книжной (библиотечной) и новой (компьютерной) информационной культуры, дает возможность избежать в информационном обществе конфронтации двух полярных культур – технократической и гуманитарной [34].

Ценностная составляющая поведения человека в цифровом пространстве – это ключевой компонент, который, тесно связывает информационную культуру и культуру ИБ. Именно наличие ценностей отличает культуру от грамотности (осведомленности) и в области информации, и в области ИБ. Осведомленный – сведущий, знающий, знакомый с чем-либо, компетентный, грамотный, информированный, наслышанный о чем-либо и др. [35, с. 258]. Как видим, синонимом слова «осведомленность» является грамотность. А «грамотность», как известно, означает наличие элементарных навыков – умения читать и писать, знаний в какой-либо области [36, с. 337], поэтому грамотный – это осведомленный, умелый [35, с. 81]. Осведомленность, знание чего-либо, знакомство с чем-либо, компетентность, грамотность, информированность – однопорядковые понятия. Логично заключить, что осведомленность в области ИБ – это элементарный уровень грамотности, выражающийся в минимуме знаний об ИБ. Она не предполагает сложных знаний и умений, связанных с обеспечением безопасности информации, информационных систем и имеет семантическую окраску примитивности, самого простого, начального уровня знаний в этой области. Недостатком концепции осведомленности является и то, что в нее не входит необходимость формирования информационного мировоззрения, мотивации деятельности человека к обучению и использованию полученных знаний на практике. В ее рамках человеческий фактор не рассматривается в контексте новой культуры – культуры цифрового общества, основанного на знаниях, и вне ее социальных функций - образовательно-воспитательной, когнитивной, мировоззренческой, ценностной и др. Вот почему нам нужна культура информационной безопасности, а не грамотность или осведомленность в этой области. Учитывая высокий уровень опасности и критичность человеческих угроз информационной безопасности, концентрация на грамотности в этой области чревата отставанием России в развитии цифровой экономики.

В настоящей статье мы не ставим перед собой цели обоснования теории культуры информационной безопасности. Авторские исследования ее сущности, структуры, факторов влияния, методов измерения и др. представлены нами в статьях [21, 37-40 и др.]. По нашему мнению, *культура информационной безопасности организации – это способ целенаправленной созидательной совместной деятельности руководителей и сотрудников по обеспечению и повышению уровня ИБ организации, который выражен в ценностях, потребностях, знаниях и поведении этих руководителей и сотрудников: а) в формировании ценностных моделей их информационного взаимодействия как отправителей и получателей информации; б) в гармонизации потребностей работодателя (в обеспечении ИБ организации) и сотрудников (в самореализации и саморазвитии); в) в непрерывном повышении их знаний, в том числе – осведомленности об ИБ; г) в способности работодателя и сотрудников реализовывать и развивать культурные ресурсы их информационного поведения в процессе совместной профессиональной деятельности.*

[5] Паспорт федерального проекта "Информационная безопасность" (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 28 мая 2019 г. N 9)). – URL: http://www.consultant.ru/document/ cons_doc_LAW_328932/ (дата обращения 02.10.2019)

В процессе формирования и развития культуры ИБ для предприятия важно учитывать все множество факторов и, по возможности, определять степень ее зависимости от каждого из них. Факторы, влияющие на культуру ИБ, можно классифицировать по разным признакам: по уровню влияния (микро- и макроуровень); по среде возникновения (внешние и внутренние); по направлению влияния (защищаемая информация, пользователь информационной системы); по степени важности (важные и менее важные); по степени распространения (факторы общего и локального действия) и др. Среди этих факторов особая роль в формировании и развитии культуры ИБ принадлежит группе факторов внешней и внутренней среды.

Факторы внешней среды (внешние факторы) объективны, от организации не зависят и влияют на культуру ИБ либо способствуя, либо тормозя ее развитие. К ним относятся национально-культурные, политические и правовые, экономические, социально-культурные и технико-технологические факторы.

Иное дело – факторы внутренней среды (внутриорганизационные факторы). Они формируют культуру ИБ внутри организации, поэтому требуют к себе активного деятельностного подхода со стороны организации и им присуща субъективность воздействия. Внутренние факторы – это общеорганизационные, управленческие, человеческие (связанные с персоналом) и факторы доверия между всеми участниками процесса.

К общеорганизационным факторам относятся: внутреннее состояние, стадия жизненного цикла организации, уровень общей организационной культуры, наличие действующей системы защиты конфиденциальной информации в организации. Управленческие факторы – это лидерство руководителя, политика ИБ и управление ИБ (управление рисками, инцидентами угрозы ИБ, изменениями, персоналом, осведомленностью, обучением и др.).

Большое влияние на уровень культуры информационной безопасности организации оказывают факторы, связанные с сотрудниками: их личностные качества и ценности; потребности и установки; эмоциональное состояние; знания об информационной безопасности; соблюдение правил ИБ-поведения. Огромное значение имеет степень взаимного доверия, лояльности (приверженности) сотрудников к организации, их вовлеченности в реализацию ИБ-стратегии предприятия. Степень гармонизации потребностей работодателя (в обеспечении ИБ организации) и сотрудников (в самореализации и саморазвитии) существенно повышает шансы на успех развития КИБ. Высокий уровень лояльности сотрудника к организации предполагает, что он идентифицирует себя с ней, представляет себя и организацию как единое целое, отождествляет себя с ее культурой и способен реализовать все свои личностные характеристики в информационном поведении в процессе профессиональной деятельности. Полагаем, что культура информационной безопасности должна рассматриваться именно в данной, многофакторной интерпретации, иначе проблематично решать задачи по развитию цифровой экономики, в том числе поставленные в федеральном проекте «Информационная безопасность».

Одна из серьезных проблем повышения осведомленности, а значит, и культуры информационной безопасности – недостаток кадров, способных эту проблему решать [41]. Это актуально и на уровне организаций, и на массовом уровне.

В организациях эта функция закреплена за директором и специалистом по защите информации. Сегодня это уже не «технарь», как было раньше, а специалист широкого профиля – со знанием правовых аспектов, бизнеса, финансов, технологий, организационного управления, управления рисками, инцидентами, персоналом и в том числе – культурой ИБ. Поэтому он должен обладать педагогической компетенцией [42]. Как замечают эксперты, за рубежом термин *chief information security officer* (*CISO*) стал постепенно исчезать. Специалисты по ИБ все более становятся специалистами широкого профиля по защите бизнеса, даже буква "*I*" в аббревиатуре *CISO* постепенно исчезает. С сожалением следует констатировать, что пока таких специалистов российские вузы не готовят. Однако совершенно очевидно, что технологии развития культуры информационной безопасности в организациях должны быть обязательным предметом изучения в вузах, а также в системе переподготовки и повышения квалификации кадров.

А как же быть с массовой культурой информационной безопасности, кто будет формировать ее? Мы согласны с мнением экспертов о том, что это острая необходимость [43]. Если дети хоть как-то включены в орбиту внимания государства, то как же быть со всеми остальными гражданами? Может, решению этой проблемы будет способствовать «цифровой куратор»? Профессиональный стандарт, определяющий особенности этой новой специальности, появился в России в 2018 г.[6]

Если мы обратимся к содержанию этого стандарта, то найдем утвердительный ответ на этот вопрос. В рамках трудовой функции «Ознакомительное индивидуальное консультирование граждан в области информационно-коммуникационных технологий» в числе трудовых действий – «информирование о наиболее типичных угрозах при работе в сети, с использованием средств коммуникации», «информирование об основных методах противодействия информационным угрозам». В числе необходимых умений – «отбирать и применять инструменты обеспечения информационной безопасности», необходимых знаний – «требования информационной безопасности». Трудовая функция «Выполнение подготовительных работ по консультированию граждан в области применения информационно-коммуникационных технологий» предполагает умения «обрабатывать пер-

[6] Приказ Минтруда России от 31.10.2018 N 682н «Об утверждении профессионального стандарта "Консультант в области развития цифровой грамотности населения (цифровой куратор)"» (Зарегистрировано в Минюсте России 19.11.2018 N 52725). – URL: http://www.consultant.ru/document/Cons_doc_LAW_311506/ (дата обращения 02.10.2019)

сональные данные с соблюдением требований, установленных законодательством Российской Федерации», «оказывать консультативную помощь, связанную с оперированием персональными данными самими пользователями (и их защитой) при работе с интернет- сервисами».

Однако в остальном мы будем разочарованы: полное название специальности – "Консультант в области развития цифровой грамотности населения (цифровой куратор)" и, следовательно, будущий специалист ограничен элементарными уровнем грамотности, хоть и цифровой. Ценностные, мировоззренческие и другие гуманитарные аспекты ИБ в стандарте не упоминаются. Впрочем, это понятно: необходимо сначала ликвидировать «безграмотность» в этой области. Однако на подготовку кадров для решения даже этой, более простой задачи уйдет немало времени. А время, как известно, не ждет, и следует искать более оптимальные пути – там, где уже накоплен соответствующий опыт.

Может ли библиотека как главный субъект формирования и развития информационной культуры в нашей стране, справиться с этой задачей? Этим вопросом правомерно задались и библиотечно-информационные специалисты, ведь на данный момент, как это ни печально, библиотека не попала в проект ни как инициатор, ни как площадка для его реализации [44]. У библиотеки, безусловно, есть потенциал в реализации этих функций, есть инициативы, огромный опыт в использовании информационных ресурсов и технологий. Однако библиотечно-информационным специалистам срочно требуются новые компетенции в области ИБ. Эта проблема должна решаться в рамках вопроса о расширении миссии и функций современной библиотеки. Зарубежные эксперты все более склоняются к требованию активной интеллектуально-деятельностной позиции библиотечно-информационного специалиста. По словам экс-президента Американской библиотечной ассоциации С. Фельдмана [45, с. 5], будущая актуальность библиотек и библиотечных специалистов будет зависеть от того, *что они делают* для людей, а не от того, *что они имеют* для людей. Так, роль библиотеки как информационного центра неминуемо снижается из-за расширения возможностей удаленного доступа пользователей к информационным ресурсам, поэтому библиотека все более исследуется с позиций новой функции –учебного центра, в реализации которой она уже накопила большой и ценный опыт [46].

Для реализации своей образовательной функции библиотека, как и любой субъект, вынуждена будет использовать новейшие технологии, в том числе – технологии искусственного интеллекта. С их помощью уже сегодня можно выявлять скрытые закономерности в поведении потребителей, определять вероятность отклика на то или иное рекламное предложение, понимать, кому, когда, как и что лучше предложить, чтобы выстроить максимально персонифицированные коммуникации. Искусственный интеллект дает дополнительные навыки и помогает распознавать тексты, определять тип документа, извлекать значимые данные, чтобы затем передавать их в целевые информационные системы. По мнениям экспертов, искусственный интеллект в ближайшее время охватит все ИТ-сервисы. Наиболее перспективны персонификация предложений клиентам; создание релевантных рекомендательных сервисов нового поколения; автоматическая обработка пользовательского контента и действий: например, анализ отзывов, обращений, выявление ботов и т.д. [47]. Так, компания *Uber Technologies Inc*. использовала машинное обучение для прогнозирования спроса и предложения (алгоритм направляет водителя в ближайшие зоны с повышенным числом клиентов еще до того момента, как они появляются). Крупный финансовый холдинг *JPMorgan Chase* представил платформу *Contract Intelligence* (*COIN*), на которую были возложены задачи по обработке и анализу юридических документов, по извлечению из них ключевой информации, а также по сегментации клиентов на категории, в соответствии с которыми планировалось разрабатывать таргетированные предложения и оказывать услуги и др. [48]. И поскольку «успешность применения технологий искусственного интеллекта зависит главным образом от наличия достаточного объема данных» [47], логично предположить, что информационные центры и библиотеки, такими данными располагающие, могут использовать свой потенциал и опыт участников рынка программных решений по повышению осведомленности в области ИБ.

Но им следует пойти дальше осведомленности и грамотности – по направлению к культуре информационной безопасности, а потому – создавать свои инструментальные средства. Эти средства должны оценивать текущие угрозы ИБ со стороны пользователей; выявлять закономерности в их поведении; понимать, кому, когда, как и что предложить для обучения; создавать релевантные рекомендательные сервисы контента по информационной безопасности нового поколения; прогнозировать информационное поведение пользователей и их ИБ-уязвимости в будущем и др. Некоторые игроки рынка осведомленности уже начинают идти по этому пути. Так, программы повышения осведомленности «Лаборатории Касперского» не только дают знания, но и формируют правильное поведение; для разных категорий сотрудников они создают разные навыки; курс позволяет обучать пользователей в соответствии с ландшафтом угроз и их исходными навыками и т.д. [12].

Развитие культуры информационной безопасности должно стать предметом непрерывного образования в школах, вузах, по месту работы и досуга граждан, а значит – во всех видах и типах библиотек. Цифровые сервисы по повышению культуры ИБ должны размещаться на официальных и поисковых сайтах, в электронных библиотечных системах, в социальных сетях. Безусловно, это новые вызовы для российского информационного и библиотечного образования, и требуются не только государственные решения по этому вопросу, но и готовность специалистов-практиков к профессиональной переподготовке и непрерывному повышению квалификации.

Большим потенциалом для создания и внедрения цифровых сервисов повышения культуры ИБ обладает Всероссийский институт научной и технической

информации Российской академии наук (ВИНИТИ РАН). Согласно его Уставу, утвержденному приказом Министерства науки и высшего образования Российской Федерации № 5 от 06.07.2018, предметами деятельности Института являются, кроме научно-информационного и аналитического обеспечения научных исследований, «разработка научно-методологических основ информатизации общества и осуществление инновационной деятельности, направленной на обеспечение социально-экономического развития и национальной безопасности Российской Федерации; развитие информационных технологий; разработка концептуальных основ и методологических подходов к оценке эффективности процессов информатизации общества»[7]. Обращение к культурологическому методологическому подходу к осведомленности в области ИБ, разработка и внедрение высокотехнологичных инновационных инструментов по повышению культуры ИБ – все это, безусловно, позволит ускорить темпы и улучшить качество цифровизации общества, составляющей основу информационной и национальной безопасности страны.

Что касается кадровой готовности к решению столь нестандартных проблем, то руководство ВИНИТИ РАН так или иначе ставит перед собой задачу «усовершенствовать систему подготовки кадров информационных работников путем проведения соответствующих конференций и особенно семинаров для работников информационной сферы, активизации работы аспирантуры и докторантуры, привлечения студентов и аспирантов к информационной работе в сотрудничестве с вузами» [49, с. 4].

* * *

Предпринятый анализ зарубежной науки и практики показал, что до начала XXI в. доминировал подход к решению проблемы человеческих рисков информационной безопасности через повышение осведомленности о ней. Концепция осведомленности (грамотности) и разработанные на ее основе стандарты информационной безопасности отличаются сугубо прагматической направленностью, отсутствием мотивационно-рефлексивных, мировоззренческих аспектов, что неадекватно в условиях культурной цифровой трансформации. В последние годы в зарубежных странах осознается ограниченность столь прагматичного подхода, поэтому резко увеличился поток публикаций по культуре информационной безопасности, развивается её социальная практика в самых разных отраслях деятельности. Ограниченность науки и практики рамками осведомленности и грамотности в области информационной безопасности свидетельствует об отставании России от мировой тенденции. Нам необходимы широкомасштабные научные междисциплинарные исследования теории культуры информационной безопасности, перестройка системы подготовки кадров для выполнения её функций (специалистов по защите информации, информационных работников, библиотечно-информационных специалистов и др.), повсеместная практика ее развития под эгидой Совета безопасности Российской Федерации с участием образовательных и информационных организаций страны. Акцент на образовательную функцию информационных центров и библиотек согласуется с трансформацией их социальной миссии в цифровой культуре. Главным средством реализации этой функции должны стать многофункциональные цифровые сервисы по развитию культуры информационной безопасности, разработанные на основе машинного обучения.

[7] Устав Всероссийского института научной и технической информации Российской академии наук. Утв. приказом Министерства науки и высшего образования Российской Федерации № 5 от 06.07.2018. – URL: http://www.viniti.ru/viniti-about (дата обращения 02.10.2019).

СПИСОК ЛИТЕРАТУРЫ

1. PriceWaterhouseCoopers. The Global State of Information Security® Survey 2018. – URL: https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html (дата обращения 02.10.2019).
2. PriceWaterhouseCoopers. На пути к цифровому доверию. – URL: https://www.pwc.ru/ru/assets/pdf/digital_trust_insights_russian.pdf (дата обращения 02.10.2019).
3. NIST SP 800-50-2003 Building an Information Technology Security Awareness and Training Program. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf (дата обращения 02.10.2019).
4. ISO/IEC 27000:2012 Information technology – Security techniques – Information security management systems – Overview and vocabulary. – URL: https://www.iso.org/standard/56891.html (дата обращения 02.10.2019).
5. ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements. – URL: https://www.iso.org/standard/54534.html (дата обращения 02.10.2019).
6. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management. – URL: https://www.iso.org/standard/54533.html (дата обращения 02.10.2019).
7. ISO/IEC 27003:2010 Information technology – Security techniques – Information security management systems implementation guidance. – URL: https://www.iso.org/standard/ 42105.html (дата обращения 02.10.2019).
8. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance. – URL: https://www.iso.org/obp/ ui/#iso:std:iso-iec:27003:ed-2:v1:en (дата обращения 02.10.2019).
9. Information Security Awareness in Financial Organisations / ENISA. – URL: https://webcache.googleusercontent.com/search?q=cache:0Us-oaHURyQJ:https://www.enisa.europa.eu/publications/archive/is-in-financial-organisations/at_download/fullReport+&cd=1&hl= ru&ct=clnk&gl=ru (дата обращения 02.10.2019).
10. The new users guide: How to raise information security awareness [Электронный ресурс] / ENISA –

URL:https://www.enisa.europa.eu/publications/ archive/copy_of_new-users-guide (дата обращения 02.10.2019).
11. Spitzner L. Defining the Security Awareness Maturity Model. – URL: https://www.sans.org/security-awareness-training/blog/defining-security-awareness-maturity-model (дата обращения 02.10.2019).
12. Горюнов С.Е. Обзор рынка сервисов повышения осведомленности по ИБ (Security Awareness). – URL:https://www.anti-malware.ru/analytics/Market_ Analysis/Security-Awareness#part3 (дата обращения 02.10.2019)
13. Bonderud D. National Cyber Security Awareness Month: What's New for 2018? – URL: https://securityintelligence.com/national-cyber-security-awareness-month-whats-new-for-2018/ (дата обращения 02.10.2019)
14. National Cybersecurity Awareness Month. – URL: https://www.dhs.gov/national-cyber-security-awareness-month (дата обращения 02.10.2019)
15. Пластунов В.А. Почему у задачи по повышению осведомленности в кибербезопасности нет альтернативы. – URL: https://www.itweek.ru/ security/ article/ detail.php?ID=195601 (дата обращения 02.10.2019)
16. Создание глобальной культуры кибербезопасности: Резолюция, принятая Генеральной Ассамблеей Организации Объединенных Наций [по докладу Второго комитета (A/57/529/Add.3)] 57/239. 31 January 2003. – URL: https://undocs.org/ ru/A/RES/57/239 (дата обращения 02.10.2019)
17. OECD. (2002). Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security: Organisation for Economic Co-operation Development). – URL: https://www.oecd.org/sti/ ieconomy/15582260.pdf (дата обращения – 02.10.2019)
18. OECD. (2015). Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document. – URL: https://www.oecd.org/sti/ieconomy/ digital-security-risk-management.pdf (дата обращения 02.10.2019)
19. ENISA. (2017). Cyber Security Culture in organisations / ENISA. – URL: https://doi.org/10.2824/10543 (дата обращения 02.10.2019)
20. AlHogail A., Mirza A. Information security culture: A definition and a literature review // 2014 World Congress on Computer Applications and Information Systems (WCCAIS). 17-19 Jan. 2014. – URL: https://ieeexplore.ieee.org/document/6916579 (дата обращения 01.10.2019)
21. Астахова Л.В. Понятие культуры информационной безопасности // Научно- техническая информация. Сер. 1. – 2014. – № 2. – С. 1-8; Astakhova L. The concept of the information-security culture // Scientific and Technical Information Processing. – 2014. – № 41, № 1. – P. 22-28.
22. Veiga A. d., Martins N. Information security culture and information protection culture: A validated assessment instrument // Computer Law & Security Review. – 2015. – № 312). – P. 243-256.
23. Karlsson F., Åström J., Karlsson M. Information security culture–state-of-the-art review between 2000 and 2013 // Information & Computer Security. – 2015. – № 23(3). – P. 246-285.
24. Mahfuth A., Yussof S., Baker A. A., Ali N. a. A systematic literature review: Information security culture // 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). – URL: https://ieeexplore.ieee.org/document/8002442 (дата обращения 02.10.2019)
25. Nasir A., Arshah R. A., Ab Hamid M. R., Fahmy S. An analysis on the dimensions of information security culture concept: A review // Journal of Information Security and Applications. – 2019. – № 44. – P. 12-22.
26. Solms B. von, Solms R. von. Cybersecurity and information security–what goes where? // Information & Computer Security. – 2018. – № 26(1). – P. 2-9.
27. Veiga A. d. Comparing the information security culture of employees who had read the information security policy and those who had not // Information and Computer Security. – 2016. – № 24(2). – P.139-151.
28. Veiga A. d., Martins N. Defining and identifying dominant information security cultures and subcultures // Computers & Security. – 2017. – № 70. – P. 72-94.
29. СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». – URL: https://cbr.ru/ Content/Document/File/ 46921/st-10-14.pdf (дата обращения 02.10.2019)
30. Доктрина информационной безопасности Российской Федерации / Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646. – URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения 02.10.2019)
31. Воробьев Г.Г. Информационная культура управленческого труда. – М.: Экономика, 1971. – 108 с.
32. Гендина Н.И. Можно ли измерить информационную грамотность (культуру)? // Образование в документах. – 2009. – № 20(213). – С. 58-62.
33. Астахова Л.В. Информационное мировоззрение: понятие и уровни // Вестник Челябинской государственной академии культуры и искусств. – 2014. – № 4 (40). – С. 9-16.
34. Гендина Н.И. Информационная грамотность и информационная культура личности: международный и российский подходы к решению проблемы // Открытое образование. – 2007. – № 5. – С. 58-69.
35. Словарь синонимов русского языка. – М.: Русский язык, 1993. – 495с.
36. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1990. – 1632 с.
37. Astakhova L.V. Information security culture and information destructiveness counterculture: essence and structure // Socio-cultural aspects of regional development. – Chelyabinsk, 2010. – P. 201-205.
38. Astakhova L.V. Information-psychological security in the region: culturological aspect // Bulletin of the Ural Federal District. Information security. – 2011. – №2. – P. 40-47.

39. Астахова Л.В. Информационная безопасность: риски, связанные с культурным капиталом персонала // Научно-техническая информация. Сер. 1. – 2015. – № 4. – С. 1-13; Astakhova L. V. Information security: risks related to the cultural capital of personnel (review) // Scientific and Technical Information Processing. – 2015. – № 42, № 2. – P. 41-52.
40. Astakhova L.V. From culture to cultural capital information security of the organization // Bulletin of Culture and Arts. – 2018. – №3(55). – P. 85-101.
41. 2018 SANS Security Awareness Report. Building Successful Security Awareness Programs. – URL: https://www.sans.org/sites/default/files/2018-05/2018%20SANS%20Security%20Awareness%20Report.pdf (дата обращения – 02.10.2019)
42. Астахова Л.В. Педагогическая компетенция будущего специалиста по защите информации в вузе: проблема развития и понятие // Вестник Южно-Уральского государственного университета. Серия: Образование. Педагогические науки. – 2014. – Т. 6, № 1. – С. 69-76.
43. Белов Е.Б., Лось В.П., Малюк А.А. Цифровая экономика и актуальные проблемы совершенствования системы подготовки кадров в области информационной безопасности // Безопасность информационных технологий. – 2018. – Т. 25, № 4. – С. 6-22.
44. Цифровой куратор. А при чём здесь библиотека? // Университетская книга. – 2019. – № 4. – С. 31-37.
45. Feldman S. The future of the MLIS: imparting enduring values with changing instruction models // American Libraries. – 2015. –- 46(11/12).
46. Kumar B. Academic Library in Transition from Library as a Place to Library as a Learning Centre: A Case Study of Indian Institutes of Management // Desidoc journal of library & information technology. – 2015. – Vol. 35, № 3. – P. 169-176.
47. Искусственный интеллект 2018. Российский рынок искусственного интеллекта: проблемы и перспективы: Обзор. – URL: http://www.tadviser.ru/index.php/_2018 (дата обращения 02.10.2019)
48. Андреянов Н. Подходит ли опыт западных стран в области машинного обучения для российского рынка? – URL: https://www.anti-malware.ru/analytics/Technology_Analysis/foreign-machine-learning-experience (дата обращения 02.10.2019).
49. Щуко Ю.Н. Некоторые аспекты развития Всероссийского института научной и технической информации // Научно-техническая информация. Сер. 1. – 2018. – № 9. – С. 1-6.

Материал поступил в редакцию 03.10.19.

Сведения об авторе

АСТАХОВА Людмила Викторовна – доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета (национального исследовательского университета), г. Челябинск
e-mail: astakhovalv@susu.ru

ВНИМАНИЕ!

С 9-го номера 2019 г. каждая статья сборника «Научно-техническая информация» сер. 1 и 2 сопровождается цифровым идентификатором объекта – DOI (Digital Object Identifier). См. статью Д.Б. Саркисяна «Цифровой идентификатор *DOI* – инструмент навигации по научным публикациям в Интернете // Научно-техническая информация. Сер. 1 – 2019. – № 8. – С. 27-31.

Научно-техническая информация.
Серия 1: Организация и методика информационной работы.

№ 9 – 2019

Сюнтюренко О.В., Дмитриева Е.Ю. Государственная система научно-технической информации в структуре задач цифровой экономики. – С. 1-11. DOI: 10.36535/0548-0019-2019-09-1

Еркимбаев А.О., Зицерман В.Ю., Кобзев Г.А., Косинов А.В. Курирование цифровых научных данных. – С. 12-24. DOI: 10.36535/0548-0019-2019-09-2

Селиванова И.В., Косяков Д.В., Гуськов А.Е. Влияние ошибок в базе данных *Scopus* на оценку результативности научных исследований. – С. 25-32. DOI: 10.36535/0548-0019-2019-09-3

Джиго А.А., Майстрович Т.В. Новый уровень понимания библиотечно-информационной услуги. – С. 33-37. DOI: 10.36535/0548-0019-2019-09-4

№ 10 – 2019

Соколова И.С. Научно-популярные ресурсы России: журналы и интернет-медиапроекты. – С. 1-5. DOI: 10.36535/0548-0019-2019-10-1

Яшалова Н.Н., Шрейдер Н.В., Яковлева Е.Н. Цифровая грамотность общества: ситуация, проблемы и перспективы на современном этапе научно-технического прогресса. – С. 6-11. DOI: 10.36535/0548-0019-2019-10-2

Сысоев А.Н., Корнилова М.Б., Толмачев А.О. Научная поддержка действующей классификации: на примере УДК. – С. 12-18. DOI: 10.36535/0548-0019-2019-10-3

Гуреев В.Н., Лакизо И.Г., Мазов Н.А. Неэтичное авторство в научных публикациях (обзор проблемы). – С. 19-32. DOI: 10.36535/0548-0019-2019-10-4

№ 11 – 2019

Астахова Л.В., Медведев И.А. Инструментальный мониторинг соответствия веб-сайтов требованиям законодательства в области персональных данных. – С. 1-5. DOI: 10.36535/0548-0019-2019-11-1

Мельникова Е.В. Опыт формирования цифровых коллекций ведущих библиотек России и США. – С. 6-11. DOI: 10.36535/0548-0019-2019-11-2

Алевизаки О.Р., Кара-Мурза Е.С., Ломыкина Н.Ю., Агафонова М.А. Маркетинг в социальных сетях для продвижения брендов средств массовой информации. – С. 12-20. DOI: 10.36535/0548-0019-2019-11-3

Шевченко Л.Б. Дизайн и удобство использования библиотечных веб-сайтов. – С. 21-33. DOI: 10.36535/0548-0019-2019-11-4

№ 12 – 2019

Гоннова С.М., Разуваева Е.Ю. Национальные системы научно-технической информации – потенциал для развития научной дипломатии в СНГ. – С. 1-18. DOI: 10.36535/0548-0019-2019-12-1

Калачихин П.А. Оценка исследователей по критериям репутационной ответственности. – С. 19-27. DOI: 10.36535/0548-0019-2019-12-2

Миралиев К.Х., Алибаева М.М., Азизова Р.Н. Информационная обеспеченность науки в Республике Таджикистан. – С. 28-30. DOI: 10.36535/0548-0019-2019-12-3

№ 1 – 2020

ВНИМАНИЮ ЧИТАТЕЛЕЙ!

ИЗДАНИЕ УДК

УНИВЕРСАЛЬНАЯ ДЕСЯТИЧНАЯ КЛАССИФИКАЦИЯ

АЛФАВИТНО-ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

в 2-х томах

Алфавитно-предметный указатель (АПУ) к 4-му полному изданию УДК на русском языке:

Том I содержит АПУ от буквы А до Н;

Том II содержит АПУ от буквы М до Я и указатель латинских наименований к классам УДК 56 Палеонтология, 57 Биологические науки, 58 Ботаника, 49 Зоология, 61 Медицинские науки.

АПУ содержит около 100 000 понятий, представленных в полных таблицах УДК.

При его составлении были учтены изменения, опубликованные в Выпусках № 1 – 6 «Изменения и дополнения к УДК»

Для подписки необходимо направить заявку для оформления счета по адресу:

125190, Россия, Москва, ул. Усиевича, 20, ВИНИТИ РАН

Телефоны: 499 155-42-85, 499 151-78-61

E-mail: feo@viniti.ru

http://www.udcc.ru