

# НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА  
ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

---

Издается с 1961 г.

№ 5

Москва 2020

---

## ОБЩИЙ РАЗДЕЛ

УДК 338.2 : [004:002]

О.В. Сянтюренко

### **Риски развития цифровой экономики: информационные аспекты\***

*Обсуждается многоаспектная проблема выявления, оценки и минимизации угроз и рисков разработки и применения новых технологий в рамках Четвертой производственной революции, стержневым элементом которой являются информационные технологии. На основе системного подхода, с использованием методов наукометрии и многомерного анализа данных, анализируется ряд новых технологических направлений, потенциально порождающих наиболее опасные риски для экономики и социума, зачастую не осознаваемых даже в профессиональном сообществе. Сформулированы некоторые выводы, рекомендации, первоочередные и наиболее актуальные задачи разработки междисциплинарной проблемы рисков развития цифровой экономики.*

**Ключевые слова:** цифровая экономика, киберугрозы, информационные технологии, сетевая инфраструктура, интернет вещей, риски, робототехника, биокиберги, цифровое неравенство, социальное программирование, информационная безопасность

DOI: 10.36535/0548-0019-2020-05-1

---

\* 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».

## ПРОБЛЕМА МИНИМИЗАЦИИ РИСКОВ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

В настоящее время мировая экономика фактически вступила в фазу Четвертой промышленной революции (в политических декларациях и СМИ под лозунгом «Цифровая экономика»). Она характеризуется широким производственным применением целого ряда новых кластеров технологий – прежде всего это технологии Интернета вещей, интеллектуальная робототехника, технологии обработки Больших Данных, 3D-принтинг, нанотехнологии и нанобиосенсорика, искусственный фотосинтез, умные сети электропитания, биотехнология (включая генную инженерию и регенеративную медицину), новые материалы с заранее спроектированными свойствами, мобильный широкополосный Интернет. Информационные технологии, информатика являются основой становления и интеграции отдельных технологических кластеров в формирующемся базовом промышленном комплексе нового технологического уклада. Уже сейчас можно констатировать максимально широкое «вплетение» цифровых информационных технологий в ткань любых производственных, технологических, образовательных и управленческих процессов. На основе глобальной сети Интернет создается единая цифровая среда (инфраструктура) с подключением к ней машин и оборудования, объектов инфраструктуры, транспорта, логистических цепочек, организаций, а также людей.

Правительства многих стран, в том числе и Российской Федерации, разрабатывают и финансируют программы по перестройке своих экономик в соответствии с тенденциями и требованиями цифровой реальности. По версии международного индекса сетевой готовности, представленной в докладе «Глобальные цифровые технологии» Всемирного экономического форума за 2016 г., Россия значительно отстает от мировых лидеров, занимая «по готовности к цифровой экономике» 41-е место, а по экономическим и цифровым результатам использования цифровых технологий – 38-е место. Осознавая важность этой проблематики для развития страны, Правительством РФ была разработана и в июле 2017 г. утверждена Программа «Цифровая экономика Российской Федерации» [1], в которой поставлена задача ускоренного движения по пути инновационного развития как главного средства выживания в условиях глобальной конкуренции. Инновации становятся важнейшим направлением современного промышленного производства, а интенсификация инновационной деятельности в научно-промышленной сфере – приоритетной задачей экономического развития (ежегодный оборот на мировом рынке высоких технологий и наукоемкой продукции в несколько раз превышает оборот рынка сырья, включая нефть, газ и нефтепродукты). При этом возможные негативные последствия использования новых технологий отходят на второй план или вообще не рассматриваются. Однако все технологии и виды современной техники имеют как положительные, так и от-

рицательные для общества последствия и несут в себе технологические, экологические, экономические и социальные риски [2, 3].

Исторический ход научно-технического и индустриального развития показал невозможность предвидеть весь спектр его негативных последствий для человечества. С процессами формирования нового технологического уклада связана фундаментальная неопределенность, поскольку общество, во-первых, просто не готово к столь масштабному расширению пределов возможного, а во-вторых, уже явные возможности влекут за собой и опасные последствия, большинство из которых все еще относится к сфере незнания. В ряде случаев возникает необходимость принимать решения по тем вопросам, по которым – казалось бы – их в принципе принять невозможно. Риск при этом сопряжен с возможным, но в момент принятия решения еще неявным ущербом, по характеру и масштабам которого иногда вовсе нельзя сделать никаких серьезных предположений. Например, только сравнительно недавно стали ясны отдаленные негативные последствия масштабного использования антибиотиков и диоксида титана, применяемого в пищевой и фармацевтической промышленности [4].

Оценка позитивных и негативных последствий развития той или иной технологии, например, для окружающей среды, часто затрудняется недостатком или вообще отсутствием информации и необходимых для принятия решений знаний, что, естественно, увеличивает опасность появления негативных последствий новых технологий. Наиболее показательной в данном случае является нанотехнология, где установка, предназначенные для проведения научных экспериментов, одновременно становятся оборудованием для нанофабрикации. Ученые еще сами до конца не выяснили природу изучаемых ими явлений, а нанопродукты все больше и больше заполняют современный рынок.

Таким образом, по мере развития цифровой экономики, особую важность и актуальность приобретает проблема (междисциплинарная по своему характеру) выявления, оценки и минимизации угроз и рисков разработки и применения новых, и в первую очередь информационных, технологий. Современные представления о риске отличаются многообразием. Существует множество определений риска, в основном в финансово-экономической сфере. Представляется, что в рамках настоящей статьи наиболее приемлемым (и кратким) является следующее определение: «Риск – это потенциальная возможность получить в условиях осознаваемой и будущей неопределенности заранее неизвестный результат негативного характера» [5]. Следует подчеркнуть, что информационная неопределенность (отсутствие информации о возможных состояниях системы, о внешней среде и т.п.) и есть среда появления риска.

Вопрос о классификации и систематизации рисков – это сложная методологическая проблема. При постановке задачи оценки рисков очевидна необходимость стратификации рисков по значимости потенциальных негативных последствий, в первую очередь –

социального характера. Целесообразна кластеризация рисков по сферам предметной деятельности (финансы, военное дело, образование, промышленность и т.д.). В сфере экономики и финансов возможна оценка риска как ожидаемой величины потерь (для каждой  $k$ -й группы рисков) в виде функции  $r_k = f(Dp_k)$ , где  $D$  – финансовая оценка потерь, а  $p_k$  – вероятность реализации риска. В общем случае уровень риска зависит от ряда параметров (зачастую неявных). Теоретический и практический интерес представляет получение количественной оценки уровня риска. При применении  $i$ -й новой технологии уровень риска может, в общем случае, определяться эмпирическим выражением  $r_i = f(S_i, W_j, H_j, D)$ , где  $S_i$  – стратификационный уровень значимости негативных последствий;  $W_j$  –  $j$ -я сфера предметной деятельности, где используется новая технология;  $H_i$  – энтропия среды, определяемая как  $H_i = \log p_i$ , где  $p_i$  – вероятность реализации риска;  $D$  – объем вероятных финансовых потерь [5].

В общем случае однозначное и точное описание будущих состояний социотехнических систем, в состав которых входят новые технологии, часто остается недостижимым. Это обусловлено рядом причин, которые действуют и изолировано, и в комплексе: недостаточностью наших знаний; критически большим числом факторов, определяющих динамику исследуемого (прогнозируемого) процесса; открытым и эмерджентным характером изучаемых систем. Сложность современных социотехнических систем связана в первую очередь не с техническими, а с социальными факторами. В этом и состоит особенность очередного витка эволюции сложности технических систем в условиях роста технологических рисков. Система становится настолько сложной, что не в состоянии не только управлять своей деятельностью и развитием, но и предсказывать негативные сценарии такого развития и способы их преодоления. И здесь уже часто не работает традиционное математическое моделирование. Необходимо принимать во внимание, что при использовании математических вычислений учитываются лишь те отношения, которые доступны математической обработке, т. е. могут быть количественно выражены или выразимы. Кроме того, определение вероятности того или иного события, которое может привести к аварии, катастрофе, другим негативным последствиям, затрудняется тем, что это событие часто лежит за пределами познаваемого, а его последствия измеряются (оцениваются) не только в аспекте нанесенного материального ущерба (как показали Чернобыльская катастрофа и авария на АЭС Фукусима).

Многоаспектная проблема выявления, качественной и/или количественной оценки рисков, разработки подходов к их минимизации является чрезвычайно важной междисциплинарной и, в определенной степени, трансдисциплинарной проблемой. В рамках настоящей статьи рассматривается, на содержательном уровне, ограниченный континуум зачастую неявных рисков и угроз использования новых информационных

технологий, значимых с точки зрения возможных негативных последствий научно-технического и индустриального развития цифровой экономики.

## СТРУКТУРНЫЙ АНАЛИЗ ПОТЕНЦИАЛЬНЫХ РИСКОВ

Борьбу с угрозами и минимизацию рисков необходимо начинать с их выявления, классификации, ранжирования и оценки (количественной и/или качественной). В короткой статье невозможно уделить достаточного внимания всему множеству {IT-рисков}. Далее с системных позиций проанализируем ряд новых развивающихся технологических направлений {A,B,C,D,E,F,G,H,I}, потенциально порождающих наиболее опасные риски для экономики и социума, зачастую не вполне осознаваемые даже в профессиональном сообществе.

**A.** По интенсивности и широте проникновения во все сегменты научно-промышленной сферы интернет-технологии сегодня занимают главенствующее место. Развитие интернет-технологий сопровождается расширением континуума риск-факторов. Необходимо также отметить выраженный тренд роста деструктивных сетевых социальных структур. Наиболее значимые риск-факторы связаны с быстрым развитием так называемого Интернета вещей (*IoT – Internet of Things*).

По существу *IoT* – это сеть физических предметов (вещей), которые оснащены встроенной технологией взаимодействия друг с другом и внешней телекоммуникационной средой. Именно *IoT* обеспечивает лавинообразное увеличение доли автоматически генерируемых данных в глобальной цифровой среде.

Создание и развитие таких сетей рассматривается как технология, способная перестроить как экономические, так и общественные процессы посредством исключения из части действий и операций необходимость участия человека [6]. По данным кампании *Strategy Analytics* [7], количество *IoT*-устройств в мире достигло 22 млрд в 2018 г. По результатам прогнозных исследований кампании *Amazon*, в США в 2020 г. будет 25 млрд подключенных устройств (энергетических установок, общественных зданий, плотин, дамб, роботов, медицинских имплантов, городской и транспортной инфраструктуры и т.п.). Для большинства из них уровень защищенности близок к нулю. К 2025 г. число таких устройств вырастет до 50 млрд (с минимум 2500-3025 млрд связей ежедневно – согласно закону Меткалфа [8]). По оценкам специалистов, технология Интернет вещей уже к 2022 г. приведет к созданию телекоммуникационных сетей такой сложности и запутанности, что они будут не только не управляемыми, но и априори ненадежными. Проблема осложняется тем, что в последнее десятилетие активно развивается глобальная широкополосная сеть Интернет, которая теперь рассматривается как перспективный базовый элемент информационной инфраструктуры. Глобальная сеть, включающая разнообразные сегменты: иерархические и одноранговые сети, коммуникации по оптоволоконным сетям и подключение через ретрансляторы и спутники, чрезвычайно уязвима. В связанной цифровой среде даже

незначительные сбои, отказы, нештатные состояния различных приборов, датчиков, программного обеспечения могут привести к целому каскаду непредсказуемых негативных последствий. В 90-х годах прошлого века именно эти факторы-детерминанты стали одной из основных причин отказа от реализации США Программы СОИ. Согласно исследованиям, проведенным в Массачусетском технологическом институте, веерные отключения и отказы в результате ошибок и несовершенства *software* станут повседневной практикой и будут измеряться десятками и сотнями в год [9].

**Таким образом, основные потенциальные риски IoT для экономики и социума состоят не столько в его преднамеренном использовании злоумышленниками, а сколько в самом факте его существования и дальнейшего развития.**

**В.** По данным Международной федерации робототехники (*International Federation of Robotics – IFR*), объем мирового рынка промышленных роботов в 2018 г. достиг рекордных 422 тыс. единиц, что на 6% больше показателей годичной давности [8]. Примерно 30% продаж промышленных роботов в мире пришлось на китайский рынок по итогам 2018 г. Такие данные приводят в *IFR* в июле 2019 г. Ожидается, что к 2020 г. Китай войдет в десятку самых автоматизированных наций мира. К этому времени количество роботов на производстве должно возрасти до 150 единиц [10]. Кроме того, Китай планирует продать в общей сложности 100 тыс. промышленных роботов местного производства [11]. При этом США производят ~ 75% мирового выпуска роботов, оснащенных вычислительным интеллектом и способных к многофункциональной деятельности. По экспоненте растет число транспортных и бытовых роботов. В цифровой экономике именно человек становится наиболее непредсказуемым, а значит ненадежным звеном автоматизированных производств. Уже в настоящее время роботы вызывают страх у рабочих, юристов, работников транспорта, торговли, представителей других профессий с повторяющимися операциями [6]. Международная консалтинговая компания *McKinsey* предсказывает, что около 20% рабочей силы по всему миру – или 800 млн рабочих – могут потерять работу из-за автоматизации процессов [9]. В будущем до 15 млн. россиян могут лишиться работы, которая не требует серьезной квалификации, т.к. их профессия вымрет. Об этом заявил член комитета Государственной Думы РФ по труду, социальной политике и делам ветеранов Олег Шеин порталу «URA.RU» (04.08.2019). В этой связи следует отметить, что, несмотря на масштабность и важность проблемы, в научном сообществе, в настоящее время, не разрабатываются какие-либо подходы и методы оценки рисков и оценки (переоценки) ценности человеческого капитала с учетом трендов процесса роботизации хотя бы на период до 2025 г.

**С учетом современных тенденций следует констатировать, что весьма динамично актуализируются риски, обусловленные ростом социальной напряженности (в различных социальных слоях) вследствие быстрого прогресса робототехники.**

**Технологическая безработица уже в глобальной «повестке дня».**

**С.** В перспективе весьма вероятной следует рассматривать **актуализацию рисков, связанных с конвергенцией биомедицинских и компьютерных технологий.** В интервале 15-25 лет синтетическая биология, генетическая инженерия, практическое применение нанороботов, способных действовать внутри кровеносной системы человека, совершенно поменяют лицо медицины. На горизонте 15-25 лет реальностью станет биотехнологическая интеграция человека и искусственного интеллекта, формирование своего рода биокибергов. Искусственный интеллект, который превзойдет человека – упрощение сложного феномена. Психика человека, его интеллект работает одновременно в трех сферах: цифровой, аналоговой или модальной, и образной. Воображение, распознавание закономерностей и сложные формы коммуникаций – это когнитивные области, где у людей до сих пор имеется неоспоримое преимущество, которое наверняка сохранится и в будущем. Таким образом, «синтезированные люди» будут обладать высокими креативными способностями, крепким здоровьем и высокой трудоспособностью в течение многих десятков и, возможно, сотен лет. Это будет новый вид людей, живущих в полной, включая цифровую и дополненную, реальности, здоровых и работоспособных от рождения до смерти. Этот новый человеческий вид будет неразрывно связан с искусственным, вычислительным интеллектом (прямой интерфейс мозг-компьютер), базами данных различного целевого назначения, системами поддержки принятия решений и распознавания.

**Развитие синтетических технологий создания биокибергов (суперлюдей) неизбежно трансформирует современную человеческую цивилизацию, т.е. возникнет новая, нечеловеческая цивилизация с непредсказуемыми рисками и, возможно, глобальными негативными последствиями для антропосферы (ноосферы) в целом.**

**Д.** Объем генерируемой и передаваемой в мировых сетях информации экспоненциально растет и специалисты констатируют нарастающие информационные перегрузки. Д. Боуден и Л. Робинсон в исследовании 2008 г., названном «Темная сторона информации: перегрузка, тревожность и другие парадоксы и патологии» [12] определили информационную перегрузку как «состояние цивилизации, при котором объем потенциально полезной и актуальной информации, превышает возможность ее обработки средним человеком (т.е. когнитивные способности) и становится помехой, а не подспорьем». Наглядным примером информационной перегрузки являются оценочные данные *Alphabet* (группы компаний, в которую входит и Google): от начала цивилизации и до 2003 г. было создано около 5 экзбайт ( $5 \cdot 10^9$  Гб) информации; сейчас человечество создает столько данных всего за 2 дня.

Огромное количество информации зачастую ведет к невозможности ее воспринять и усвоить. Объективно существует противоречие между ограниченными психофизиологическими возможностями по-

требителя информации по восприятию новых знаний и большими потоками насущно необходимой научно-технической и экономической информации. Перегруженность информацией приводит к снижению когнитивных (познавательных) функций мозга (возникает также информационно-коммуникативная зависимость). Вследствие этого человеку приходится постоянно делать выбор в огромном многообразии новой информации. Проблема переизбытка информации несет в себе также и другую проблему, именуемую «информационным шумом». Перенасыщение каналов восприятия детерминирует способность индивидуального сознания справиться хотя бы с первичным анализом массивов поступающей информации. Следующий аспект «информационного шума» – это потеря определенного рабочего времени и интеллектуальных ресурсов человека, затраченных при поиске необходимых данных или же в процессе их сортировки и анализа, ведущих, в итоге, к переутомляемости. Специалист, стремящийся иметь информацию о всех новых достижениях в своей области, должен тратить до трети своего рабочего времени на её поиск, анализ и изучение, иначе существует опасность непроизводительных затрат до 45% средств, выделенных на исследования и/или разработку. Следует отметить, что в настоящее время теория научно-технической информации не располагает методами индустриальной интеграции знаний, представленных в разнородных источниках. Именно это определяет тенденции развития информационно-поисковых систем и технологий аналитической обработки данных.

По данным *IDC (International Data Corporation)*, в американских компаниях сотрудники, имеющие дело с информацией, в среднем тратят 14,5 часа в неделю на обработку электронной почты, 9,6 часа – на поиск документов и 9,5 часа – на их анализ [13]. Однако лавинообразное нарастание количества информации не столько характеризует прогресс информационных технологий, сколько отражает их проблемы. В 2016 г. в англоязычном Интернете в течение года не было ни одного посетителя (посещения) на более чем 89% сайтов, а в 2018 г. – уже почти на 90%. Сходные процессы идут и в научной сфере. В настоящее время более 94% статей, опубликованных в научных журналах, ни разу не цитировались в других источниках. Почти 90% научных публикаций имели не более пяти прочтений [14].

**Таким образом, вследствие нарастающей информационной перегрузки возрастают риски торможения научно-технического прогресса, так как даже важнейшие научные открытия и инновационные разработки могут оказаться просто незамеченными научно-технологическим сообществом.**

Е. Информационно-цифровое неравенство представляет собой сложную проблему, которая имеет социально-экономические, политические и культурные аспекты.

Из-за постоянного развития информационных технологий информационно-цифровое неравенство является актуальной и динамической проблемой. Развитие информационно-коммуникационных технологий дает толчок интеграционным процессам в эко-

номике и обществе, но в то же время усиливаются процессы поляризации различных групп населения, регионов и стран. Возникает опасность формирования новой «информационной элиты», а также увеличения определенной страты людей, оказавшихся в маргинальном положении по отношению к информационно-компьютерным технологиям. Основными факторами риска, способствующими появлению информационно-цифрового неравенства, являются: недостаточно развитая информационно-коммуникационная инфраструктура; высокая стоимость интернет-услуг; низкий уровень развития образования и информационной культуры населения; отсутствие социальной поддержки в освоении информационных технологий; слабая мотивация и готовность разных групп населения к использованию информационно-компьютерных технологий.

Проблема информационно-цифрового неравенства, в ближайшей перспективе будет быстро нарастать и активно проявит себя, прежде всего в экономическом и социальном аспектах. Основания для такого вывода дает анализ тенденций развития глобального процесса информатизации, а также степени его воздействия на положение той или иной страны в мировом сообществе [15-17]. Этот анализ показывает, что в геополитическом плане процесс информатизации осуществляется крайне неравномерно и резко усиливает технологическую стратификацию стран мирового сообщества. Выступая в качестве мощного катализатора научно-технического прогресса, информатизация существенным образом ускоряет развитие передовых стран, обрекая тем самым другие страны на все большее и большее отставание. Именно поэтому принимать меры по ослаблению негативных последствий развития глобальной проблемы информационного неравенства необходимо уже сегодня, так как информационное неравенство усиливает социальное расслоение общества и поэтому является угрозой для его стабильности. Исторический опыт свидетельствует о том, что усиление любых форм социального неравенства опасно для развития общества, так как именно оно является первопричиной многих социальных и международных конфликтов. Поэтому своевременное осознание обществом новой для него глобальной проблемы — информационного неравенства – является одной из важных задач мирового сообщества.

**Следует констатировать, что развитие цифровой экономики неизбежно обострит проблему информационно-цифрового неравенства и, как следствие, проблему экономического неравенства, что будет приводить к возникновению рисков, обусловленных ростом социальной и политической напряженности.**

Ф. По мере становления цифровой экономики все более начинает осознаваться новый (и, возможно, самый опасный) вид угроз – разрушение способов и форм идентификации личности в результате длительного информационно-психологического воздействия – так называемая концентриальная война (от лат. *conscientia* – сознание) [18–20], что означает переструктуризацию внутреннего мира личности (социальное программирование).

В рамках процессов глобализации и становления цифровой экономики мир вступил в новый этап борьбы – конкуренцию не только технологий, товаров и услуг, но и форм и методов организации общественного сознания. С этой целью используют массовую культуру, транслируемую средствами массовой информации (в том числе и Интернет) и разрушающую ценности традиционного общества, т.е. используют информационное оружие, для которого нет преград в век спутниковой глобальной связи. Предметом трансформирующего воздействия являются определенные типы сознания, имея в виду, прежде всего, его традиционные, этические, культурные, религиозные аспекты и ценности. В результате длительного информационно-психологического воздействия определенные типы сознания могут быть изменены, стерты, перестать существовать. Традиционные типы сознания – объекты воздействия (поражения) в концептуальной войне – должны быть вытеснены за рамки цивилизационно допустимых и приемлемых. Это происходило и раньше, когда один тип сознания вытеснял другой (как, например, христианство сменило язычество). Но с развитием информационных технологий эта конкуренция и борьба принимают тотальный характер. Очень важно понимать, что изменение и/или уничтожение определенных типов сознания предполагает разрушение и реорганизацию общностей, которые конституируют эти типы сознания [16]. Можно выделить несколько основных технологий социального программирования, которые ориентированы на трансформацию (или разрушение) сознания. Во-первых, дезинтеграция и примитивизация информационно-коммуникативной среды, где функционирует и развивается сознание, приводит к понижению уровня ее организации. Во-вторых, распространение образов и текстов, разрушающих работу сознания на основе специальных методов (психотехнологий) по каналам коммуникаций. Сейчас сформировалась устойчивая тенденция, у все более растущей доли пользователей, замены понятийно-логического мышления образно-ассоциативным (клиповым). Клиповый тип мышления на порядок повышает внушаемость людей их склонность к некритическому восприятию информации. В-третьих, разрушение способов и форм идентификации личности по отношению к фиксированным общностям, что приводит к смене форм самоопределения и к деперсонализации.

В социальном программировании используются также стереотипы и привычки, особенности восприятия, характеристики психических состояний (тревожность, агрессия) и т.п. Основной вектор – это целенаправленное изменение общественного сознания и поведенческих предпочтений больших групп с использованием активных методов, в том числе психометрических алгоритмов. Деструктивные социальные сети, новые технологии мультимедиа и виртуальной реальности вовлекают человека в новые формы существования и в определенной мере могут оказывать воздействие на формирование личности. Как результат – рост угроз социальной и личностной дезадаптации и разрушение психики человека. Возрастает уровень угроз деформации общественной нравственности

и морали. Как экспериментально показал российский нейропсихолог и нейрофизиолог С.В. Савельев, автоматизация познавательной поведенческой активности ведет к морфологическим изменениям в головном мозге. Вследствие высокой пластичности мозга церебральное закрепление алгоритмического поведения может происходить в значительно более сжатые временные периоды, чем считалось ранее [21, 22].

***Все это, в итоге, ведет к росту рисков целенаправленного негативного воздействия современной цифровой сетевой среды (инфосферы) на когнитивные способности и поведение людей.***

**Г.** По мере развития цифровой экономики неизбежно будут расти риски, обусловленные все более широким использованием цифровых технологий в сфере вооружений и, прежде всего, в военнокосмической области. Основные риски связаны с тем, что существуют фундаментальные причины, в силу которых программное обеспечение нельзя сделать настолько надежным, чтобы не сомневаться в том, что не возникнут нештатные ситуации и несанкционированного применения ракетно-ядерного оружия. Причем уровень угроз растет с ростом масштабов и сложности военных системотехнических комплексов. В настоящее время проблема усугубляется активной разработкой и широким внедрением суперкомпьютерных технологий, роботизированных систем и систем искусственного интеллекта в различные военнотехнические комплексы.

О высоком уровне потенциальных угроз и рисков свидетельствует тот факт, что, по появившейся информации, в Китае по решению руководства, начиная с 2007 г. проводится оцифровка массивов знаний, инженерной и конструкторской документации по всем ключевым технологиям и научным направлениям. КНР создает крупнейшую в мире базу семян и генного материала не только по сельскохозяйственным животным, птицам и рыбам, но и в целом генную библиотеку обитателей Земли [14].

***По сути, с учетом рисков санкционированного и/или несанкционированного применения ядерного оружия, речь идет о беспрецедентном проекте создания хранилища знаний, технологий, биоматериалов, которое гипотетически может понадобиться выжившим после катастрофы китайцам.***

**Н.** Наряду с интенсивным развитием информационных систем и сетей передачи данных все более актуальной становится проблема обеспечения информационной безопасности.

Широкое применение современных информационных технологий потенциально создает предпосылки таких угроз, как утечки, хищения, утраты, искажения, подделки, копирования и блокирования информации и, как следствие – экономического, экологического, социального и других видов ущерба [17, 23–25]. В разных странах регулярно регистрируются попытки несанкционированного проникновения в информационные системы органов государственной власти и управления, факты кражи и уничтожения экономической и финансовой информации, программного обеспечения систем электронных платежей и т.д. Несанкционированно вторгаясь в компьютерные сети, нарушители

способны не только копировать хранящуюся в них информацию, но и вводить в них вирусы, разрушающие прикладные (или системные) программы, которые срабатывают спустя определенное время (или при возникновении определенных условий), что значительно усложняет их обнаружение. Такие действия могут приводить к функциональному нарушению информационных систем, систем защиты критической инфраструктуры, объектов управления, возникновению социальной напряженности (например, в случае утечки и несанкционированного использования персональных данных, лжеминирования авиационного и железнодорожного транспорта и т.п.). По оценочным данным компании *Positive Technologies*, в 2018 г. статистика киберугроз имела следующий вид: доля целенаправленных атак составила 62%; доля атак, направленных на кражу персональных данных, – 30%, учетных данных – 24% и данных платежных карт – 14%; вредоносный *software* используется в 56% кибератак [26].

Информационная безопасность фактически становится одной из характеристик информационных систем и технологий. С позиций информатики здесь следует выделить два аспекта. Во-первых, реализация функций защиты требует все увеличивающихся информационных и вычислительных ресурсов, что влечет временные задержки и снижение производительности поиска и обработки информации. Во-вторых, быстрый рост глобальной сети, количества компьютерных систем, лавинообразный рост цифровых данных объективно влекут возрастание рисков и различного рода угроз целостности информации.

Помимо этого специалисты отмечают тревожную закономерность быстрого нарастания рисков, связанных с тем, что отдельный человек или малая группа могут получить и даже разработать оружие массового поражения (например, программируемые биовирусы, кибероружие, нановоружение и др.). Следует отметить, что современные методы и средства компьютерного моделирования позволяют значительно сокращать цикл «исследование – разработка» (за счет виртуализации лабораторных исследований и натуральных испытаний). По мере развития цифровой экономики физический объем ущерба, который теоретически способен нанести всего один человек или небольшая группа, становится все больше и больше.

**С высокой степенью вероятности можно прогнозировать, что такие факторы, как внедрение новых информационных технологий (в том числе суперкомпьютинга и систем искусственного интеллекта), расширение мировой сети телекоммуникаций, развитие семантического Интернета и массмедиа будут все более актуализировать проблему роста традиционных угроз и рисков в цифровой сетевой среде.**

I. Риски развития цифровой экономики в России имеют определенную специфику.

1. **Постоянным и высоким фактором риска в сфере энергетики, промышленности, телекоммуникаций является широкое использование импортной электронной элементной базы.** Значительны риски, связанные с использованием в сложных системах и критических приложениях им-

портной микроэлектроники. По разным оценкам, до 75% реализуемого на мировом рынке программного обеспечения (в первую очередь, системного software – ОС и СУБД) и 85% процессоров производится компаниями под американской юрисдикцией. Ряд крупных IT-компаний встраивают в производимые чипы целевые закладки в интересах спецслужб. Принципиальные схемы и исходные коды «зашитого» в чипах программного обеспечения известны только фирме разработчику. По некоторым оценкам существует потенциально высокий уровень рисков нарушения функционирования для ~90% отечественных энергосетей (невосстановимое отключение системы, перехват управления энергосистемой и т. п.) как из-за атак компьютерных вирусов (типа *Dugu* или *Stuxnet*), так и от внешних несанкционированных действий, осуществляемых за пределами их возможного обнаружения и идентификации. Прецеденты – длительное нарушение функционирования энергосетей на Кубе в 2012 г. и в Венесуэле в 2019 г.

2. Критически важные для безопасности *RuNet* ресурсы и функции управления инфраструктурой (корневые серверы системы доменных имен, распределение адресного пространства, маршрутизация трафика) находятся и осуществляются за пределами России. **Риски неустойчивой работы Интернета на территории России в случае недружественных целенаправленных действий достаточно высоки.** Доступ (к сайту) может быть заблокирован на любом этапе: корневые серверы могут неправильно перевести адрес сайта в машинную форму, не отвечать на запросы, физически отключить сегмент сети от Интернета. Таким образом *RuNet* может быть заблокирован целиком. Прецедент – отключение Сирии от Интернета в 2012 г. [15]. Именно в силу этих причин гипотетически существуют риски отключения российского сегмента Интернета от международных платежных систем *Visa* и *Mastercard*, а также от международной межбанковской системы передачи информации и совершения платежей *SWIFT*. Экономические последствия вывода *RuNet* из строя будут катастрофическими, несопоставимыми по тяжести с любыми санкциями. Страна не просто вернется в технологическое прошлое – этот возврат будет сопровождаться выводом из строя, в частности, авиа- и железнодорожного сообщения, системы безналичных платежей и коммуникаций, включая сотовую связь. Американские компании являются производителями львиной доли повсеместно используемых мультиплекторов, маршрутизаторов, серверной инфраструктуры. Некоторые страны, например Китай, осознавая риски уязвимости интернет-трафика, приступили к созданию национальных сегментов Интернета. Ставя вопрос о полном отказе от пользования системами *Microsoft*, Китай добился передачи ему исходного программного кода операционной системы *Windows*, а также исходных текстов программного обеспечения маршрутизаторов фирмы *Cisco*, которые обеспечивают работу большинства мировых сетей и серверов (и, кстати, производятся в Китае) [27]. Следует также отметить, что практически все ведущие компании, специализирующиеся на разработке программных

решений по информационной безопасности сети Интернет, имеют американскую юрисдикцию так же как и все крупнейшие провайдеры (*Twitter, Google, Amazon, eBay, Facebook* и др.) [16].

## НЕКОТОРЫЕ ВЫВОДЫ И АКТУАЛЬНЫЕ ЗАДАЧИ

Цифровая экономика и лежащие в ее основе технологии обладают огромным и уже бурно реализующимся потенциалом влияния на жизнь человека и общества. Является ли это влияние заведомо позитивным; помогает ли оно автоматически выводу на траектории устойчивого развития цивилизации, не содержит ли в себе развитие новых технологий (прежде всего информационных) дополнительных источников неустойчивости и *рисков* – эти вопросы приобретают все большую актуальность в условиях кризисной динамики мировой экономики и политической турбулентности в системе международных политических отношений.

По мнению многих экспертов [14, 17], одной из междисциплинарных сверхзадач XXI века является управление *риском* и безопасностью сложных систем в экономике и социуме. Сформулируем некоторые выводы, рекомендации, первоочередные и наиболее актуальные задачи разработки проблемы рисков развития цифровой экономики.

1. Четкое осознание основных целей и задач: а) раннее предупреждение *рисков* новых технологий и их конвергентных вариантов; б) разработка методологии их многокритериальной оценки (по сегментам экономики); в) разработка рекомендаций и комплексных мер по минимизации *рисков* и улучшение основы поиска решений (с позиций междисциплинарного и трансдисциплинарного подхода).

2. Разработка методов классификации и систематизации рисков на основе таксономии. Потребность в таксономии в данном случае возникает из-за сложности предметной области, не позволяющей провести ее систематизацию на основе некоторой достаточно просто выводимой классификации объектов, ее составляющих [28]. Роль таксономии рисков на этапах создания и реализации технологий состоит в том, что она должна позволять разным категориям специалистов, экспертов, программистов оценивать риски в самых разных аспектах: а) по значимости потенциальных негативных последствий; б) по различным факторам риска (сложности, времени и др.); в) по структурным и функциональным составляющим; г) по категориям потерь.

3. Разработка принципов, методов и рекомендаций по определению и оценке рисков на основе системного подхода, системного анализа, методов социотехнического проектирования, социальной инженерии, имитационного моделирования, теории «нечетких» множеств (с использованием технологии *Big Data*).

4. Создание международной системы сбора (и Бнд), анализа и систематизации данных по реализовавшимся рискам, прежде всего связанных с управлением больших системотехнических комплексов (таких как Чернобыль, Фукусима, Шушенская ГРЭС и т.п.). Организация международного сотрудничества и обобщение

международного опыта, ознакомление с уже имеющимися результатами исследований в этой области, организация конструктивного взаимодействия и совместной работы с зарубежными междисциплинарными группами ученых по данной проблематике.

## ЗАКЛЮЧЕНИЕ

Несколько выходя за рамки рассматриваемой проблематики, хотелось бы сделать три замечания более общего характера.

1. В научных публикациях и СМИ постоянно используется термин «четвертая производственная (промышленная) революция», своеобразным синонимом которого является термин «цифровая экономика». Строго говоря, данный термин не вполне корректен. Важнейшей характеристикой современной мировой экономики является долговременное падение многофакторной эффективности производства, а любая производственная революция предполагает ускорение темпов роста производительности труда и эффективности производства. Этого в последние 20 лет не произошло. Среднегодовые темпы роста производительности труда в 2009–2017 годы были ниже, чем в период с 2000 по 2008 год, а в 2010-х гг. они были в свою очередь ниже средних показателей за последние 20 лет XX в. Это верно не только для глобальной экономики в целом, но и для таких экономически развитых стран как США, Германия, Великобритания, Франция, Япония [14, 29].

2. С начала 70-х гг. прошлого века из пятилетия в пятилетие снижаются темпы экономического роста, повышения эффективности производства (прежде всего производительности труда) и нормы прибыли. Несмотря на наращивание энерго- и механовооруженности, повсеместное внедрение информационных технологий, переломить тенденцию к снижению темпов роста производительности труда и многофакторной эффективности производства так и не удалось. В значительной степени это связано с постоянным неуклонным падением эффективности добычи энергии, а соответственно и снижением энергоэффективности производства. Сопоставительный анализ энергоемкости производства основных видов продукции в натуральном выражении показывает, что в процессе замены рабочей силы (как фактора производства) роботами она только растет. Ключевой показатель энергоэффективности – *EROEI* (*Energy returned on energy investement*) – соотношение полученной к затраченной энергии или энергетическая рентабельность [14, 30, 31]. Этот показатель характеризует отношение количества пригодной к использованию энергии, полученной из определенного источника, к количеству энергии, затраченной на получение этого энергетического ресурса. Если  $EROEI \leq 1$ , то источник энергии не может быть экономически выгодным в использовании. Падение *EROEI* не может быть компенсировано развитием интернет-технологий, внедрением роботов или обработкой больших данных. В структуре цифровой экономики развитие атомной энергетики также имеет свои риски и детерминанты. Основные опасения по поводу современной ядерной энергетики породили



аварии на АЭС Три-Майл-Айленд (США) в 1979 г., Чернобыле в 1986 г. и на Фукусиме в 2011 г. Катастрофа на Фукусиме разрушила миф об энергетических реакторах с нулевым риском. Но кроме значительных рисков для безопасности, эти реакторы имеют проблемы с утилизацией отходов и перекачивают огромное количество воды. Другой важный момент заключается в том, что основным источником топлива для современных атомных реакторов служит Уран-235, запасов которого вряд ли хватит на ближайшее столетие. Будущее с управляемым термоядерным синтезом, над технологиями стабильного использования которого работают ученые уже более 60 лет, представляется сейчас более чем призрачным [32].

По экспертным оценкам, снижение энергоэффективности на горизонте по крайней мере до 2035 г. будет иметь безусловно непрерывный и всеобъемлющий характер. Оно будет происходить темпами, не позволяющими повышать общую эффективность производства за счет внедрения новых технологий.

Таким образом, значимым риск-фактором является то, что долговременное снижение *EROEI* на фоне накладывающихся друг на друга финансово-экономического, природно-климатического и технологического кризисов, возможно на интервале 15-20 лет, вынудит глобальную цифровую экономику перейти к фазе сжатия со значительными отрицательными темпами роста, т.е. абсолютным сокращением производства и потребления товаров и услуг.

3. Стихийное, неуправляемое техническое развитие, преследующее цели экономического роста, может привести к тому, что на определенном этапе техника для своего дальнейшего формирования потребует больше затрат, чем может позволить себе человечество – или отрицательные последствия технологических решений остановят рост, или же, наконец, возникнут проблемы, не имеющие технического решения. Взаимоотношения общества, природы и техники в современных условиях характеризуются приближением к порогу качественных изменений, сам процесс которых может оказаться неконтролируемым и необратимым.

## СПИСОК ЛИТЕРАТУРЫ

1. Национальная Программа «Цифровая экономика Российской Федерации»; утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-р. – URL: [static.government.ru/media/files/9gFM4FHj4PsB7915v7yLVuPgu4bvR7M0.pdf](http://static.government.ru/media/files/9gFM4FHj4PsB7915v7yLVuPgu4bvR7M0.pdf)
2. Bechmann G. Risk and Rationality in a Future-oriented Society // Rationality in an Uncertain World / eds. G. Banse, I. Hronszky, G. Nelson. – Berlin: Edition Sigma, 2005. – P. 59-75.
3. Lenk H. Global TechnoScience and Responsibility. Schemes Applied to Human Values, Technology, Creativity and Globalisation. – Berlin: LIT, 2007.
4. Сютнюрэнко О.В., Ефременко Д.В. Проблемы информационно-аналитического обеспечения социальной оценки технических и технологических рисков // Научно-техническая информация. Сер. 1. – 2017. – № 10. – С. 1-10; Syuntyurenko O.V., Efremenko D.V. Aspects of Analytical Information Support of the Social Assessment of Technical and Technology Risks // Scientific and Technical Information Processing. – 2017. – Vol. 44, № 4. – P. 227-235.
5. Сютнюрэнко 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. Бриньольсон Э., Макафи Э. Вторая эра машин. Работ, прогресс и процветание в эпоху новейших технологий / пер. с англ. П. Миронова. – М.: АСТ. 2017 – 384.
7. Петров В.Ю., Рудашевская Е.А. Технология «интернета вещей» как перспективная современная информационная технология // Фундаментальные исследования. – 2017. – № 9-2. – С. 471-476.
8. С. 471-476.
9. Закон Меткалфа сорок лет спустя после рождения Ethernet // Открытые системы. СУБД, 2014 – № 01. – URL: <https://www.osp.ru/05/2014/01/13039684>
10. Что такое интернет вещей. – URL: [www.tadviser.ru/index.php/Статья: Что такое интернет вещей \(Internet of Things, IoT\)](http://www.tadviser.ru/index.php/Статья:Что_такое_интернет_вещей_(Internet_of_Things,_IoT))
11. Промышленные роботы. – URL: [www.tadviser.ru/index.php/Статья: Промышленные роботы](http://www.tadviser.ru/index.php/Статья:Промышленные_роботы)
12. Международная федерация робототехники представила список самых роботизированных стран мира. – URL: <https://rb.ru/story/countrits-with-greaest-density-of-robots/>
13. Факты и только факты: информационная перегрузка. – URL: <http://lpgenerator.ru/blog/2014/01/07/fakty-i-tolko-fakty-informacionnaya-peregruzka/>
14. Сютнюрэнко О.В. Факторы-детерминанты неэффективного использования информационных ресурсов в научно-технической деятельности // Научно-техническая информация. Сер.1. – 2017. – № 7. – С. 1-12; Syuntyurenko O.V. Determinants of the Ineffective Use of Information Resources in Scientific and Technological Activities // Scientific and Technical Information Processing. – 2017. – Vol. 44, № 3. – P. 159-169.
15. Ларина Е.С., Овчинский В.С. Час волка. Введение в хронополитику. («Коллекция Изборского клуба») – М.: Книжный мир, 2019. – 416 с.
16. Как отключили Интернет в Сирии. – URL: [d-russia.ru/otklyuchenie-strany-ot-interneta-precident-by.html](http://d-russia.ru/otklyuchenie-strany-ot-interneta-precident-by.html)
17. Сютнюрэнко О.В. Сетевые технологии информационного противоборства и манипуляции общественным сознанием // Научно-техническая информация. Сер. 1. – 2015. – № 10. – С. 1-7; Syuntyurenko O.V. Network Technologies for Information Warfare and Manipulation of Public Opinion // Scientific and Technical Information Processing. – 2015. – Vol. 42, № 4. – P. 205-210.
18. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии // Информа-

- ционные технологии и вычислительные системы. – 2002. – № 4. – С. 83-108.
19. Громыко Ю. Оружие, поражающее сознание, – что это такое? // Альманах «Россия-210». – М., 1997.
  20. Смирнов И., Безносюк Е., Журавлев А. Психотехнологии. – М., 1996. – URL: <http://www.pereplet.ru/text/grom0.html>.
  21. Горохов В.Г., Сянтюренко О.В. Технологические риски: информационные аспекты безопасности общества // Программные системы и вычислительные методы. – 2013. – № 4(5). – С. 344-353.
  22. Савельев С.В. Социальная психология в действии! – URL: [www.feliced.ru/2012/05/blog-post\\_3554.html](http://www.feliced.ru/2012/05/blog-post_3554.html)
  23. Савельев С.В. Нищета мозга. – М.: ВЕДИ, 2014. – 192 с.
  24. Хоффман Л. Дж. Современные методы защиты информации. – М.: Советское радио, 1980. – 263 с.
  25. Смолян Г.Л. Сетевые информационные технологии и проблемы безопасности личности // Вестник РФФИ. – 1999. – № 3(17). – С.: 63-68.
  26. Siountiurenko O. The Problems of Providing Information Security: The Case of Information Infrastructure // Studies in Eastern Europe. Technological and Environmental Policy / ed. Gerhard Banse. – Berlin, 2007. – P. 163-178. 4
  27. Актуальные киберугрозы – 2018. Тренды и прогнозы. – URL: <https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/>
  28. Сянтюренко О.В. Цифровая среда: тренды и риски развития // Научно-техническая информация. Сер. 1. – 2015. – № 2. – С.1-7; Syuntyurenko O.V. The Digital Environment: The Trends and Risks of Development // Scientific and Technical Information Processing. – 2015 – Vol. 42, № 1. – P. 24-29.
  29. Советский энциклопедический словарь. – М.: Советская энциклопедия, 1982.
  30. Замедление темпов роста в развитых странах: основные причины. – URL: <https://popecon.ru/573-zamedlenie-ekonomicheskogo-rosta-v-razvityh-stranah-osnovnye-prichiny.html>
  31. EROI и пирамида энергетических потребностей человечества. – URL: <https://horsesman5th.wordpress.com/источники/eROI-и-пирамида-энергетических-нужд/>
  32. EROEI. – URL: <https://habr.com/ru/post/100525/>
  33. Пара слов об управляемом термоядерном синтезе. – URL: [https://pikabu.ru/story/para\\_slov\\_ob\\_upravlyаемом\\_termoyadernom\\_sinteze\\_6305487](https://pikabu.ru/story/para_slov_ob_upravlyаемом_termoyadernom_sinteze_6305487)

*Материал поступил в редакцию 03.02.20.*

#### **Сведения об авторе**

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

# ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ РАБОТЫ

---

УДК 004.056:316.776

Л.В. Астахова

## Сотрудник организации как субъект управления её информационной безопасностью\*

*Выявлено противоречие между ростом количества инцидентов информационной безопасности организации по вине ее сотрудников и стабильной неэффективностью мер, предпринимаемых работодателем по их снижению. Сделан вывод о недостаточном внимании науки к современным тенденциям менеджмента организации (управления качеством, персоналом, знаниями, рисками), связанным с активизацией участия персонала в процессах управления. На примере обнаружения социоинженерных атак обоснована необходимость усиления роли пользователя информационной системы организации как субъекта управления её информационной безопасностью. Приведены организационные и программно-технические средства вовлечения пользователя в этот процесс.*

**Ключевые слова:** информационная безопасность, управление, организация, сотрудник, вовлеченность, социоинженерная атака, риски, человек как сенсор

**DOI:** 10.36535/0548-0019-2020-05-2

Знание и интеллект все более становятся средством производства, и человек стремительно усиливает свои позиции в информационном пространстве общества. Однако он по-прежнему является «самым слабым звеном» любой системы информационной безопасности [1]. Эта проблема изучается много лет, но становится все более актуальной. Согласно аналитическим отчетам, в мире объем данных, скомпрометированных по вине внутреннего нарушителя в 2017 г., показал 10-кратный рост по сравнению с 2016 г. При этом на утечки, случившиеся в результате умышленных или непредумышленных действий внутренних нарушителей, приходилось 58% от их общего числа [2], а в России в 2018 г. эта цифра составила 77,9% [3]. Впервые с 2004 г. внутренние утечки показали более высокую «мощность», чем внешние: в результате одной внутренней утечки оказался скомпрометированным гораздо больший объем данных, чем в результате одной внешней [4].

Организации пытаются предотвращать угрозы со стороны человека. Сегодня мы постепенно преодолеваем стереотип об информационной безопасности

(ИБ) как сугубо технической области деятельности. Стало очевидно, наконец, что даже самые новые, сильные технические средства защиты не могут гарантировать полной ИБ организации.

В международных и национальных стандартах серии ИСО/МЭК 27000 по управлению ИБ уделено определенное внимание безопасности, связанной с персоналом [5]. Для предотвращения деструктивных действий сотрудников в этих документах приводятся некоторые организационные меры на этапах их трудоустройства, занятости и увольнения, в том числе – требование повышения осведомленности сотрудников об информационной безопасности. Однако следует признать, что далеко не все организации выстраивают свои системы защиты информации согласно названным стандартам, поскольку последние носят рекомендательный характер. Организации, системы информационной безопасности которых проходят дорогостоящие процедуры сертификации на соответствие стандартам, все же не могут похвастаться снижением числа инцидентов по вине сотрудников. Логично полагать, что причиной тому выступает недостаточность, уязвимость декларируемых способов, методов и средств работы с персоналом, и требуется усиление его позиций в обеспечении ИБ, как и в других отраслях информационной экономики. Целый

---

\* Статья выполнена при поддержке Правительства РФ (постановление от 16.03.2013 № 211, соглашение № 02. А03.21.0011).

ряд факторов требует пересмотра роли сотрудника организации в управлении её информационной безопасностью.

**Во-первых**, человек во все времена – это сложная система, объединяющая не только знания, но и личностные качества, исследование которых лежит в психологической плоскости. Поэтому одни лишь знания сотрудника, полученные в процессе повышения его осведомленности об ИБ, – это далеко не единственный фактор, способный предотвратить его деструктивное поведение в информационной среде организации.

Причины и обстоятельства дестабилизирующих информационных воздействий со стороны людей связаны с характером воздействий – преднамеренным или непреднамеренным. К причинам, вызывающим умышленное (преднамеренное) дестабилизирующее воздействие, относят: стремление получить материальную выгоду; отомстить руководству или коллеге по работе, а иногда и государству; оказать бескорыстную услугу приятелю из конкурирующей фирмы; продвинуться по службе; показать свою значимость. Обстоятельствами (предпосылками), способствующими появлению этих причин, могут быть: тяжелое материальное положение, финансовые затруднения; корыстолюбие, алчность; склонность к развлечению, пьянству, наркотикам; зависть, обида; недовольство государственным строем, политическое или научное инакомыслие; личные связи с представителями конкурента; недовольство служебным положением, карьеризм; трусость, страх; тщеславие, самомнение, завышенная самооценка, хвастовство. Причинами непредумышленного (непреднамеренного) дестабилизирующего воздействия на информацию со стороны людей могут быть: неквалифицированное выполнение операций; халатность, безответственность, недисциплинированность, недобросовестное отношение к выполняемой работе; небрежность, неосторожность, неаккуратность; физическое недомогание. К обстоятельствам (предпосылкам) появления этих причин можно отнести: низкий уровень профессиональной подготовки; излишнюю болтливость, привычку делиться опытом, давать советы; незаинтересованность в работе, отсутствие стимулов для ее совершенствования; разочарованность в своих возможностях и способностях; перезагруженность работой, срочность ее выполнения, нарушение режима работы; плохое отношение со стороны администрации [6]. Зарубежные исследования показывают, что процесс принятия управленческих решений в области ИБ зависит от различных организационных и психологических факторов [7]. Поэтому все изложенные причины и обстоятельства деструктивных воздействий работников на информационную сферу организации должны быть в фокусе внимания руководителя по ИБ.

**Во-вторых**, человек сегодня, в обществе знания – это специфический объект управления. Особенности культуры этого общества заключены в расширении возможностей самореализации и саморазвития человека, в углублении интеллектуализации его профессиональной деятельности, в усилении его роли в управленческих процессах. В XXI веке долгосрочными трендами менеджмента и управления персона-

лом называют следующие: готовность сотрудников привносить свою инициативу, изобретательность, увлеченность; открытость, гибкость, сотрудничество, ориентация управления на заслуги сотрудника, а не на звания [8]; принятие научно-обоснованных решений на основе анализа полной и доброкачественной информации, собранной и обработанной с помощью современных методов; отказ от авторитарного стиля руководства и переход к лидерству (способность руководить не силой административного права, а авторитетом знаний, умений и человечности – вместо управления по целям или по результатам систем аттестации и ранжирования персонала, количественных норм и заданий, массового контроля качества продукции); как можно более глубокое и полное делегирование полномочий на всех уровнях управления, сопровождаемое соответствующим наделением ответственностью; постоянное обучение всех, везде и всегда; работа компании по принципу “мы все вместе делаем одно дело”; признание почти полной ответственности менеджеров за работу системы [9]; ориентация на человека, персонализация (от стандартизации – к индивидуальным потребностям, желаниям и возможностям кандидатов и сотрудников организации); повышение уровня доброты и доверия на рабочем месте к подчиненным, руководителям, коллегам; выявление и развитие талантливых сотрудников; обратная связь с сотрудниками; переход от аналитики людей (контроля) к аналитике для людей; микрообучение в процессе работы; использование блокчейна в работе с персоналом и др. [10]; переход от классической модели компании к модели «освобожденной» компании (она предполагает, что все работники могут предлагать решения и проекты для всей компании, свободны и ответственны за все действия, которые, по их мнению, будут необходимыми и лучшими для развития их организации) [11]; Agile-подход, который «возвращает ценность человеческого и профессионального общения, дает ощущение того, что человек влияет на то, что происходит с ним и вокруг него, повышает ощущение определенности и последовательности происходящего и помогает поддерживать баланс во взаимодействии людей и организаций» [12].

Особо пристальное внимание уделяется вовлечению сотрудников в работу организации – их готовности целиком вкладывать когнитивную, эмоциональную и физическую энергию [13–15].

**В-третьих**, усиление позиций сотрудников в системе ИБ организации диктуется принципами менеджмента качества. В разделе 3. «Взаимодействие работников» ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь [16], идентичного международному стандарту ISO 9000:2015 "Quality management systems – Fundamentals and vocabulary", указывается: «Для организации крайне важно, чтобы все работники были компетентными, наделены полномочиями и вовлечены в создание ценности. Компетентные, наделенные полномочиями и взаимодействующие работники на всех уровнях организации повышают ее способность создавать ценность. Поэтому для того чтобы эффективно и результативно управлять организацией, очень важно уважать

и вовлекать всех работников на всех уровнях организации». Следовательно, управленческая деятельность в области информационной безопасности, если она нацелена на снижение деструктивных инцидентов, должна развиваться в русле названных общих тенденций управления персоналом. Для этого необходимо обеспечивать более тесное взаимодействие работников и руководства организации. Как и в сфере менеджмента качества, для практической реализации этого принципа в сфере информационной безопасности требуется: углубление понимания работниками целей организации в области информационной безопасности; усиление мотивации по достижению этих целей; повышение вовлеченности работников в обеспечение информационной безопасности; усиление личностного развития, проявления инициативы и креативности; повышение удовлетворенности работников; развитие доверия и сотрудничества во всей организации; повышение внимания к общим ценностям и культуре во всей организации.

**В-четвертых**, вовлечение сотрудников в управление ИБ обусловлено современным трендом управления знаниями в организации. В основе трансформационной модели SECI (SECI model of knowledge dimensions) И. Нонака и Х. Такеучи лежат различные способы трансформации знаний (спирали знаний): социализация, экстернализация, комбинирование, интернализация. В частности, экстернализация (*externalization*) предполагает преобразование неявных знаний в явные, извлечение смыслов и их передачу другим субъектам [17]. Проблема, обсуждаемая в настоящей статье, находится в русле этого процесса: пользователь корпоративной информационной системы должен быть способен трансформировать неявное знание об угрозах информационной безопасности в явное и передавать его лицам, принимающим управленческие решения.

**В-пятых**, усиление субъектных позиций сотрудников организации в системе защиты информации соответствует концепциям духовного развития человека в обществе знания. Самореализация и личностное развитие человека невозможны сегодня без интеграции информационно-потребительской (чувственное восприятие, рациональное познание и оценка потребляемых текстов и других носителей информации), информационно-репродуктивной (воспроизведение, передача информации) и информационно-созидательной (создание нового знания) составляющих [18]. Поэтому требование участия человека во всех видах информационной деятельности является аргументом в пользу сотрудника как субъекта управленческой деятельности организации по ИБ.

**В шестых**, участие человека в управлении информационной безопасностью необходимо и с позиций теории управления рисками. Один из лучших способов решения проблем информационной безопасности в корпоративном мире основан на оценке риска [19]. При этом еще в 1950-х гг. теоретики заявили, что риск не может быть определен за пределами человеческого восприятия [20]. К сожалению, сегодня наиболее распространенным методом оценки рисков ИБ является их экспертная оценка исключительно директором или специалистом по защите ин-

формации, пользователи информационной системы организации к этой работе не допускаются.

На практике директор по информационной безопасности (в западных странах – Chief Information Security Officer – CISO) традиционно рассматривает сотрудников как угрозу, поэтому занимает авторитарную позицию, пытается реализовать свои должностные функции. Поэтому он, как правило, использует одностороннюю модель связи с конечным пользователем информации без обратной связи с ним [21]. Однако сегодня становится ясно, что этот подход может хорошо работать только в жестких организационных иерархиях (особенно в вооруженных силах и полиции), и ему противоречит рост более открытых организационных структур. Автократизм препятствует эффективной информационной безопасности.

Возможности сотрудника в управлении ИБ организации проиллюстрируем на примере защиты от социоинженерных атак. К ним относятся атаки разной направленности воздействий: прямые (осуществляемые через физический, зрительный, аудиальный контакт, присутствие злоумышленника в рабочей зоне жертвы для выполнения атаки) и косвенные (запущенные удаленно с помощью вредоносного программного обеспечения, передаваемого через вложения электронной почты или СМС сообщения). Примеры прямых атак: физический доступ, «серфинг на плечах», дайвинг, телефон и др.; примеры косвенных атак: фишинг, фальшивое программное обеспечение, всплывающие окна, вымогатели, *SMSishing*, онлайн социальная инженерия и обратная социальная инженерия [22].

В последние годы конечные пользователи признаны самым слабым звеном в цепи безопасности, и теперь защита информации в значительной степени зависит от убеждения сотрудников в необходимости вести себя безопасно. Уже начинает складываться стереотип, что работник будет поступать правильно и заботиться о защите информации, если он осведомлен о проблемах организации. Однако этого не всегда достаточно. Так, в Нидерландах в результате эмпирического исследования была показана неэффективность двух методов, направленных на защиту пользователей от атак социальной инженерии: повышение осведомленности об опасностях социальных и кибератак и предостережение от раскрытия личной информации. У участников эксперимента запрашивался адрес электронной почты, 9 цифр из их 18-значного номера банковского счета, а также перечень покупок в интернет-магазине. В результате были получены относительно высокие показатели раскрытия информации: 79,1% участников заполнили свой адрес электронной почты, а 43,5% предоставили информацию о банковском счете. Среди онлайн-покупателей 89,8% респондентов указали тип продукта, который они приобрели, а 91,4% – название интернет-магазина, в котором они совершили эти покупки [23].

В последнее время появились инструментальные средства защиты от социоинженерных атак. Самые популярные сегодня – это автоматические сканеры уязвимостей социальной инженерии, которые могут быть использованы для тестирования устойчивости организации к потенциальным атакам социальной

инженерии, возникающим в результате использования открытых источников [24, 25]. Многие зарубежные компании проводят симулированные фишинговые атаки, имея четко определенные цели снижения имитируемых фишинговых кликов ниже 5–10% [26]. Аналитические задачи решаются в процессе разработки и внедрения программных комплексов анализа защищенности пользователей компьютерных сетей от социоинженерных атак [27], а также программных продуктов, моделирующих злоумышленника и профиль его компетенций для оценки защищенности информационной системы от социоинженерных атак, выявления ее наиболее уязвимых звеньев [28] и др. Однако во всех этих продуктах сотрудник по-прежнему остается пассивным объектом, что не меняет сути его взаимоотношений с руководством в процессе управления ИБ организации.

Кроме того, на фоне динамики технологических достижений, следует указать на негативные психологические последствия излишнего контроля за сотрудниками организации (в том числе в форме пентестирования): стрессы, озлобленность, утрата доверия к руководству и другие причины и обстоятельства, которые могут привести не к ожидаемому снижению, а, напротив, – к повышению их уязвимости в системе защиты информации [29]. Особенно это относится к лояльным сотрудникам, которые могут стать источниками угроз ИБ не умышленно, а из-за неосведомленности или невнимательности. Тестирование таких сотрудников на устойчивость к социоинженерным атакам может вызвать у них обратную реакцию [30].

Таким образом, становится очевидным, что для достижения эффективности управленческих усилий по обеспечению ИБ требуются альтернативные методы, основанные на более активных, доверительных (а потому – позитивных) двусторонних связях руководителя с сотрудниками. Упор должен делаться на делегирование и расширение прав и возможностей последних. Мы согласны с экспертами [31] в том, что сотрудники могут быть уполномочены брать на себя ответственность за информационную безопасность организации. Люди часто способны выявлять проблемы и решать их так, как не могут даже самые передовые технологии. Когда брандмауэры, системы предотвращения вторжений и другие средства защиты выходят из строя, люди становятся последней линией защиты. Но это работает только в том случае, если обеспечить им необходимую подготовку и поддержку, а также управление со стороны высших руководителей [26].

Если раньше приходилось нанимать лучших математиков, взломщиков кодов и секретных агентов для отчета о безопасности организации, то сегодня обработка, анализ и более доступная информация стали значительно более эффективными. Вскоре машинное обучение, программная робототехника, автоматизация процессов и центры слияния станут средствами, способными революционизировать сбор информации для отделов безопасности организаций. Прогресс, который мы наблюдали предыдущие 30 лет, теперь будет происходить шагом в 5 лет [32].

Полагаем, что в ближайшее время одним из таких новых источников информации и технологий ее об-

работки станет сотрудник организации. Одним из перспективных методов реализации человеческого потенциала в сфере управления ИБ, по нашему мнению, может быть вовлечение сотрудника в обнаружение кибератак на основе развиваемой сегодня в зарубежной науке и практике концепции, что человек есть датчик (сенсор) безопасности (The Human-as-a-Security-Sensor paradigm). За последние несколько лет эта концепция находит все большее применение для выявления угроз и неблагоприятных условий в физическом пространстве: аварийных ситуаций [33], шума и загрязнения окружающей среды [34], мониторинга наличия воды [35]. Успехи в физическом пространстве послужили мотивацией для применения и оценки концепции обнаружения угроз в киберпространстве. Особенно это актуально для раскрытия семантических социально-инженерных атак, где технические механизмы безопасности изначально ограничены в объеме и точности. Так, авторы [36] разработали приложение, предназначенное для того, чтобы пользователи могли активно обнаруживать такие атаки и сообщать о них.

Изложенное позволяет утверждать, что для эффективного управления ИБ организации необходимо учреждение правового статуса сотрудника как субъекта обнаружения социоинженерных атак. В организации должна быть создана стабильная система взаимодействия сотрудников и руководителей, основанная на формализованных, документированных правилах, нормах, статусах и ролях, которые способны обеспечить снижение человеческих угроз ИБ. При этом новая информационно-функциональная роль сотрудника должна быть подкреплена системой морального или материального вознаграждения. Это будет способствовать укреплению доверия между руководством и работником, усилению мотивации работника по достижению целей ИБ, личностному развитию, повышению его инициативности и креативности. В итоге максимально вероятно достижение целей не только работодателя (обеспечение ИБ), но и работников (удовлетворенность работой, самореализация и саморазвитие).

Обоснованная трансформация ролей пользователей информационных систем организации способна привести к активизации факторов повышения уровня культуры информационной безопасности организации и ее работников: их осведомленности, формированию ценностей, ответственности и лояльности; взаимного доверия и гармонизации потребностей работодателя и работников и др. Так, в процессе правового учреждения управленческой функции сотрудника он получает знания об опасности различных типов и видов кибератак, о технологиях реализации и защиты от их деструктивного воздействия. Самостоятельная обработка фишинговых писем, пришедших на персональный ящик электронной почты сотрудника, усиливает осознание им опасности рисков ИБ и повышает его ответственность в этой области. Это подтверждают постулаты психологии рисков, согласно которым персонифицированные риски считаются более опасными, чем анонимные [37]. Как правило, человек больше боится опасности, которая затрагивает его лично и поэтому более внимательно

относится к ней и предпринимает больше усилий для её устранения, чем опасности, которая угрожает другим [38]. Уверенности в информационной безопасности придаёт сотруднику реальная возможность управления рисками (контроля над ними, реализации технологий их обработки), ведь большинство людей меньше опасаются рисков, над которыми они чувствуют некоторый контроль, и больше опасаются рисков, которые они не контролируют [37].

Усиление роли сотрудника в управлении информационной безопасностью особенно актуально для небольших организаций, не имеющих достаточных ресурсов на приобретение дорогостоящих средств защиты информации. Для такого типа организаций мы разработали специальное программное приложение HUMAN FIREWALL, которое нацелено на техническое обеспечение процесса обнаружения человеком социоинженерной атаки, её классифицирование (отнесение к определенному типу атак), цифровую передачу информации о ней в отдел информационной безопасности, получение и обработку обратной связи.

\* \* \*

На фоне возрастания роли человека в обществе информации и знания слишком много организаций все еще верят в технологические решения проблем обеспечения информационной безопасности. И это несмотря на то, что отчет за отчетом, нарушение за нарушением показывают, что злоумышленники больше внимания уделяют конечным пользователям. Поэтому актуальная задача работодателей сегодня – оценить важность сотрудника в управлении ИБ. Именно человек может быть последней линией защиты и предохранить организацию от атак в случае отказа всех других технологий.

Потребность наделения сотрудника организации полномочиями обнаружения кибератак и оперативного оповещения о них руководства обусловлена достижениями таких разных отраслей науки и практики, как управление информационной безопасностью, менеджмент качества, управление персоналом, управление знаниями, психология рисков, информационно-психологическая теория информационной деятельности. Сотрудник должен быть не только объектом управления, но и его активным субъектом, вовлеченным в процесс управления ИБ и организационного сотрудничества, не только потреблять знания об ИБ и репродуцировать его на практике, но и создавать новое знание об угрозах ИБ организации, уметь трансформировать неявное знание об угрозах ИБ в явное, выступать в роли первичного преобразователя и отправителя информации для принятия управленческих решений в области ИБ.

В управлении информационной безопасностью сотрудник организации имеет широкие возможности как датчик социоинженерных атак. Существующие инструментальные средства часто способствуют предотвращению угроз ИБ, связанных с социоинженерными атаками. Однако на практике требуется разработка программных продуктов, которые могли бы реализовать человеческий потенциал для обнаруже-

ния этих атак, информирования о них руководства и обработки рисков ИБ на основе обратной связи.

Участие конечных пользователей в обнаружении кибератак повышает общий уровень их культуры информационной безопасности. Если люди достаточно умны, чтобы защищать себя на работе, то они охраняют себя и дома, делятся знаниями с членами семьи и знакомыми, и тогда мы действительно добиваемся хорошего прогресса в развитии культуры ИБ. Персональное участие сотрудника организации в управлении ИБ повышает его ответственность, уверенность в причастности к решению серьезных корпоративных задач. Реализация сотрудником функции обнаружения социоинженерных атак способствует не только оперативному реагированию на угрозы ИБ организации, но и гармонизации взаимодействия работодателя и работника, усилению организационной мотивации и лояльности, самореализации и саморазвитию.

Активизация роли человека в управлении информационными процессами организации и реализация этой усиливающейся тенденции в сфере ИБ становятся возможными благодаря цифровой трансформации общества в глобальном масштабе, в том числе – развитию цифровых компетенций человека. Это – ключевая особенность современной, цифровой культуры. Поэтому проблемы, поставленные в настоящей статье, имеют широкие перспективы исследования. К ним мы относим изучение различных стратегий вовлечения сотрудников в управление ИБ и оценку уровня их вовлеченности в рамках каждой из стратегий. В настоящее время существуют разные стратегии вовлечения сотрудников и более десяти шкал, которые были разработаны для их измерения [13]. Однако в сфере информационной безопасности эти стратегии и метрики имеют специфические особенности, требующие специального изучения.

В ближайшем будущем предметом научного анализа должно стать использование блокчейн-технологий и технологий машинного обучения в процессе обработки пользовательской информации о кибератаках разных видов.

## СПИСОК ЛИТЕРАТУРЫ

1. Caldwell T. Training – the weakest link // Computer Fraud & Security. – 2012. – Vol. 2012, Issue 9. – P. 8-14.
2. Исследование утечек конфиденциальных данных коммерческих компаний и государственных организаций, произошедшие по вине или неосторожности внутреннего нарушителя. Сравнительное исследование. 2013-2017 гг. – URL: <https://www.infowatch.ru/resources/analytics/reports/15194> © InfoWatch (дата обращения – 17.12.2019).
3. Утечки данных. Россия. 2018 год – URL: <https://www.infowatch.ru/resources/analytics/reports/russia2018> © InfoWatch (дата обращения: 17.12.2019).
4. 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 – 17.12.2019).
5. Астахова Л.В. Проблемы культуры информационной безопасности в условиях цифровой экономики // Научно-техническая информация. Сер. 1. – 2020. – №2. – С. 28-37.
  6. Алексенцев А.И. Понятие и структура угроз защищаемой информации // Безопасность информационных технологий. – 2000. – № 3. – С. 10–17.
  7. Dor D., Elovicci Y. A model of the information security investment decision-making process // Computers & Security. – 2016. – Vol.63. – P.1-13.
  8. Хэмел Г. Менеджмент XXI века: Новые открытия. Перевод на русский язык: Наталья Коношенко // Электронная публикация: Центр гуманитарных технологий. – URL: <https://gtmarket.ru/library/articles/4246> (дата обращения: 17.12.2019).
  9. Менеджмент 21 века – краткий обзор основных тенденций. – URL: <https://mirznanii.com/a/165547-4/medzhment-21-veka-kratkiy-obzor-osnovnykh-tendentsiy-4> (дата обращения: 17.12.2019).
  10. Naak T. 12 HR Trends for 2020. – URL: <https://hrtrendinstitute.com/2019/11/26/12-hr-trends-for-2020/> (дата обращения: 17.12.2019).
  11. Костенко Е.П. Современные тренды в управлении персоналом: отечественный и зарубежный опыт // Journal of Economic Regulation. – 2018. – Т. 9, № 4. – С. 107-123.
  12. Чухно Ю. Управление изменениями в VUCA-мире: как вовлечь людей и помочь им стать лидерами новых решений. – URL: <http://novaterra-coaching.ru/change-management-in-vuca> (дата обращения – 17.12.2019).
  13. Saks A.M. Translating Employee Engagement Research into Practice // Organizational Dynamics. – 2017. – Vol.46, Iss. 2. – P.76-86.
  14. Employee engagement and motivation. Understand the concept of employee engagement and learn how to build an engaged and motivated workforce / Chartered Institute of Personnel and Development. – 2018. – URL: <https://www.cipd.co.uk/> (дата обращения – 17.12.2019).
  15. Веретковская О.В. Вовлеченность персонала организации как актуальная задача современных компаний // Экономика и бизнес: теория и практика. – 2019. – № 4-2. – С. 40-43.
  16. ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь (с Поправкой). Утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 28 сентября 2015 г. № 1390-ст. – URL: <http://docs.cntd.ru/document/1200124393> (дата обращения: 17.12.2019).
  17. Нонака И., Такеучи Х. Компания – создатель знания. Зарождение и развитие инноваций в японских фирмах. – М.: Олимп-Бизнес, 2003. – 320 с.
  18. Астахова Л.В. Информационно-психологическая теория духовного развития личности в эпоху цифровой культуры. К 95-летию со дня рождения Ю.С. Зубова // Научно-техническая информация. Сер. 1. – 2019. – № 5. – С. 1-7.
  19. Shameli-Sendi A., Aghababaei-Barzegar R., Cheriet M. Taxonomy of information security risk assessment (ISRA) // Computers & Security. – 2016. – Vol. 57. – P.14-30.
  20. Munteanu A.-B., Fotache D. Enablers of Information Security Culture // Procedia Economics and Finance. – 2015. – Vol.20. – P. 414-422.
  21. Albrechtsen E. A qualitative study of users' view on information security // Computers & Security. – 2007. – Vol. 26, Iss. 4. – P.276-289.
  22. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey. April 2019 // Future Internet 11(89). – URL: [https://www.researchgate.net/publication/332151597\\_Social\\_Engineering\\_Attacks\\_A\\_Survey](https://www.researchgate.net/publication/332151597_Social_Engineering_Attacks_A_Survey) (дата обращения: 17.12.2019).
  23. Junger M., Montoya L., Overink F. -J. Priming and warnings are not effective to prevent social engineering attacks // Computers in Human Behavior. – 2017. – Vol. 66. – P.75-87.
  24. Edwards M., Larson R., Green B., Rashid A., Baron A. Panning for gold: Automatically analysing online social engineering attack surfaces // Computers & Security. – 2017. – Vol. 69. – P. 18-34.
  25. Faircloth J. Chapter 8: Client-side attacks and social engineering // Penetration Tester's Open Source Toolkit (Fourth Edition). – 2017. – P.273-318.
  26. Mansfield-Devine S. Raising awareness: people are your last line of defence // Computer Fraud & Security. – 2017. – Vol. 2017, Issue 11. – P. 10-14.
  27. Абрамов М.В. Автоматизация анализа социальных сетей для оценивания защищенности от социоинженерных атак // Автоматизация процессов управления. – 2018. – № 1(51). – С. 34-40.
  28. Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищенности персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. – 2016. – № 4(83). – С.77-84.
  29. Астахова Л.В. Онтологический статус доверия в информационной безопасности // Научно-техническая информация. Сер. 1. – 2016. – № 3. – С. 1-9; Astakhova L.V. The ontological status of trust in information security // Scientific and Technical Information Processing. – 2016. – Vol. 43, № 1. – С. 58-65.
  30. Hatfield J.M. Virtuous human hacking: The ethics of social engineering in penetration-testing // Computers & Security. – 2019. – Vol. 83. – P.354-366.
  31. Ashenden D., Sasse A. CISOs and organisational culture: Their own worst enemy? // Computers & Security. – 2013. – Vol. 39, Part B. – P. 396-405.
  32. Allen M. Chapter 1: Corporate security today // The Chief Security Officer's Handbook. – 2019. – P. 1-18.
  33. Avvenuti M., Cimino M.G., Cresci S., Marchetti A., Tesconi M. A framework for detecting unfolding emergencies using humans as sensors // SpringerPlus. – 2016. – Vol. 5(1). – P.1-23.
  34. Zheng Y., Liu T., Wang Y., Zhu Y., Liu Y., Chang E. Diagnosing new york city's noises with



- ubiquitous data // ACM International Joint Conference on Pervasive and Ubiquitous Computing. – 2014. – P.715-725.
35. Jurrens E.H., Broring A., Jirkai S. A human sensor web for water availability monitoring // OneSpace 2009 - 2nd International Workshop on Blending Physical and Digital Spaces on the Internet, Berlin, Germany. – URL: <https://www.researchgate.net/publication/228886237> (дата обращения: 17.12.2019).
36. Heartfield R., Loukas G. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework // Computers & Security. – 2018. – Vol.76. – P.101-127.
37. Schneier B. The Psychology of Security. – URL: <https://www.schneier.com/academic/paperfiles/paper-psychology-of-security.pdf> (дата обращения: 17.12.2019).
38. Ropeik D., Gray G. M. Risk: A Practical Guide for Deciding What's Really Safe and What's Really Dangerous in the World Around You. – Boston, New York: Houghton Mifflin Harcourt, 2002. – 485 p.

*Материал поступил в редакцию 17.12.19.*

#### **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](mailto:astakhovalv@susu.ru)

Н.С. Редькина, О.М. Ударцева, Л.Б. Шевченко

## Российские библиотеки сквозь призму мирового веб-пространства: по данным опроса 2019 г.

*С целью выявления тенденций развития библиотек в веб-пространстве проведен опрос, в котором приняли участие 387 библиотек разных видов из 39 стран мира (211 российских и 176 зарубежных). Результаты исследования демонстрируют тренды в области стратегий развития библиотечных веб-ресурсов, внедрения систем оценки их эффективности с помощью инструментов веб-аналитики, практик юзабилити тестирования, методов организации и управления веб-представительскими библиотек разных организационно-правовых форм.*

**Ключевые слова:** библиотеки, веб-пространство, веб-ресурсы, социальные сети, управление сайтом, юзабилити, веб-аналитические инструменты, вебметрические показатели

DOI: 10.36535/0548-0019-2020-05-3

### ВВЕДЕНИЕ

Современные библиотеки активно создают и ведут сайты, применяют различные интернет-платформы и публичные социальные сети для организации профессионального общения и взаимодействия с пользователями, а также библиотечно-информационного и справочно-библиографического обслуживания, обучающей деятельности и рекламы мероприятий. Использование веб-технологий позволяет адаптировать библиотечно-информационные услуги к потребностям пользователей, в том числе не являющихся читателями библиотек, способствует формированию благоприятного имиджа, положительной репутации библиотек в виртуальном мире и привлечению новых пользователей. Учитывая возрастающее значение виртуального обслуживания, связанное с ростом числа пользователей Интернета, увеличением количества веб-ресурсов и усилением их влияния на общество, целью настоящего исследования стало определение современных тенденций развития библиотек в веб-пространстве. В контексте анализа/сравнения с зарубежными библиотеками большее внимание уделено российским библиотекам.

### ОБЗОР ЛИТЕРАТУРЫ ПО ТЕМЕ

Результаты контент-анализа профессиональной литературы по исследуемой проблеме свидетельствуют, что библиотековеды и библиотечные специалисты-практики все большее внимание уделяют вопросам развития библиотек в веб-пространстве, так как веб-технологии позволяют библиотекам переходить к новым моделям взаимодействия с пользователями, используя различные каналы, включающие собственные и сторонние веб-платформы (*Facebook*,

*Instagram*, *RSS*, *Twitter*, *YouTube*, мгновенные сообщения и др.) [1–3]; способствуют созданию нового контента, включающего разнородные документы [4, 5], в том числе полученные непосредственно от пользователей [6]; содействуют развитию сервисов [7]. Особый акцент приходится на анализ соответствия библиотечных сайтов стандартным практикам развития сайтов [8] с учетом разнообразия сегментов пользователей и их информационных потребностей [9]. Исследователи рассматривают удобство использования сайтов [10–14]. I.C. Drivas, D. P. Sakas и P. Reklitis, проанализировав посетителей с целью изучения их восприятия сайта, сделали вывод, что, следуя представлениям и предложениям пользователей веб-сайта об удобстве его использования, общее количество просмотров страниц, органический трафик, а также реферальный трафик сайта значительно выросли [15]. Вместе с тем, помимо сильных сторон J. Miller рассматривает и слабые стороны методов юзабилити, которые обычно используются в библиотеках [16].

Что касается контента, то основные тенденции в области создания веб-ресурсов собственной генерации связаны с расширением их типо-видового состава (видео, мультимедиа, вебкасты; звуковые файлы, подкасты; результаты исследований, Большие Данные, Big Data); фото, графика; модели, в том числе 3D-модели; программное обеспечение; веб-архивы и др.) [17–19]. Этот тренд просматривается при анализе ресурсов конкретных библиотек. Например, в 2019 г. в American Libraries Collection (<https://archive.org/details/american>) было представлено 3 029 688 различных объектов, включая 1740 коллекций различных материалов, 2993588 текстовых документов, 15773 изображений, 10442 видео, 8132 аудио, 11 массивов данных, 2 ресурса с программным обеспечением. Часть

контента находит отражение в электронных каталогах библиотек, часть – в цифровых (электронных) библиотеках, которые становятся все более популярными. Разные виды документов (аудио, видео, изображение, текст) вошли в состав *Deutsche Digitale Bibliothek* (<https://www.deutsche-digitale-bibliothek.de/>) [20] и др.

Вопросы управления и поддержки библиотечных сайтов не часто рассматриваются в профессиональной печати. Отмечается, что библиотечные сайты в основном разрабатывались и управлялись библиотекарями в рамках их профессиональной деятельности [10]. Российские авторы упоминают, что сайты разрабатываются библиотечными специалистами, «людьми, информированными во всех сферах библиотечной деятельности» [21-23]. В публикациях сформулировано несколько подходов к организации ведения сайтов: распределение функций по обслуживанию сайта между подразделениями и сотрудниками; создание специального подразделения; комбинация этих подходов; аутсорсинг. В основном, сайты российских библиотек поддерживаются их сотрудниками путем распределения ответственности между подразделениями [24-27].

Развитию библиотек в веб-пространстве помогают веб-аналитические инструменты (счетчики, лог-анализаторы, маркетинговые инструменты), которые позволяют как анализировать поведение пользователей, так и определять общую производительность веб-ресурса [28, 29]. Сегодня рынок веб-аналитики предлагает значительное количество веб-аналитических инструментов [30]. Существующие современные веб-аналитические решения имеют довольно широкий функционал, потому многие исследователи уделяют

внимание анализу плюсов и минусов использования инструментов веб-аналитики с той или иной технологией сбора данных [28, 29, 31-34]. По мнению специалистов, какая бы из технологий ни была бы принята в качестве основной, для анализа эффективности сайта библиотеки важно понять, с какой целью пользователи приходят на сайт, что позволит в дальнейшем прогнозировать их поведение [35, 36]. Чаще всего изменения на сайте библиотеки проводились с использованием веб-аналитических данных в области структуры, навигации, дизайна, отражая тем самым обратную связь сайта с пользователем [35, 37, 38].

Можно констатировать, что в библиотечной сфере есть понимание значения веб-представительств библиотек, необходимости выработки подходов к оценке эффективности их деятельности, организации системы виртуального обслуживания и создания востребованных ресурсов. Определить векторы развития библиотек в указанных направлениях позволяет наше исследование.

## МЕТОДИКА ИССЛЕДОВАНИЯ

Онлайн опрос выбран в качестве подходящей стратегии, проводимой с помощью онлайн-инструмента Google Forms [39, 40]. Ссылка на онлайн опрос отправлялась по электронной почте в 900 библиотек мира (450 российских и 450 зарубежных) в два этапа (весной и осенью 2019 г.). Список рассылки был сформирован на основании информационно-справочного портала *Library.ru*, просмотра веб-сайтов библиотек и библиотечных ассоциаций разных стран мира.

Таблица 1

Распределение библиотек – участников опроса по странам

№ п/п	Страна	Число библиотек, принявших участие в опросе	№ п/п	Страна	Число библиотек, принявших участие в опросе
1	Армения	3	21	Португалия	2
2	Беларусь	4	22	Республика Гана	1
3	Болгария	2	23	Республика Маврикий	1
4	Великобритания	12	24	Республика Уганда	1
5	Германия	13	25	Россия	211
6	Греция	4	26	Сербия	1
7	Дания	4	27	США	29
8	Израиль	3	28	Турция	2
9	Ирландия	1	29	Узбекистан	4
10	Испания	6	30	Украина	3
11	Италия	5	31	Финляндия	5
12	Казахстан	6	32	Франция	9
13	Канада	14	33	Хорватия	2
14	Китай	9	34	Чехия	6
15	Латвия	2	35	Швеция	4
16	Намибия	1	36	Шотландия	1
17	Нидерланды	5	37	Эстония	2
18	Нигерия	1	38	Эфиопия	1
19	Норвегия	2	39	Южно-Африканская республика	1
20	Польша	7	<b>Итого:</b>		<b>387</b>

Основные задачи исследования заключались в том, чтобы определить, какие веб-ресурсы ведут библиотеки и как осуществляется управление веб-сайтом библиотеки, интересуется ли специалистов библиотек юзабилити их сайтов, а также какие современные инструменты веб-аналитики и метрики используют для оценки их эффективности. Были сформулированы следующие вопросы анкеты.

1. Имеется ли в Вашей библиотеке сайт?
2. Какие веб-ресурсы создает Ваша библиотека?
3. Какие виды документов включены в генерируемые библиотекой БД, представленные на сайте?
4. Кто занимается управлением и ведением сайта Вашей библиотеки?
5. Проводили ли Вы тестирование на удобство пользования сайтом?
6. Какие аналитические инструменты используются для анализа сайта библиотеки?
7. Какие показатели для оценки сайта Вы используете?
8. В каких социальных сетях Ваша библиотека имеет аккаунт / группу / сообщество?
9. Какие аналитические инструменты используются для анализа аккаунта библиотеки?
10. Какие показатели для оценки социальных аккаунтов Вы используете?

На вопросы анкеты ответили 211 российских и 176 зарубежных респондентов, из них 204 (52,7%) – представители вузовских библиотек; 128 (33,1%) – публичных; 29 (7,5%) – академических; 26 (6,7%) – детских и юношеских библиотек. В табл. 1 показано распределение библиотек – участников опроса по странам.

## РАЗВИТИЕ БИБЛИОТЕЧНЫХ ВЕБ-ПРЕДСТАВИТЕЛЬСТВ

Сегодня большая часть библиотек имеет официальный сайт – 380 из 387 библиотек, принявших участие в опросе, подтвердили это. Данные о наличии сайтов в российских и зарубежных библиотеках раз-

ных организационно-правовых форм (академические, вузовские, публичные, детские и юношеские библиотеки) распределились неоднозначно (табл. 2). Российские и зарубежные академические библиотеки, как правило, располагают сайты на собственном сервере. Такая же ситуация наблюдается в российских и зарубежных публичных библиотеках – большинство опрошенных публичных библиотек (115) отметили наличие сайта на собственном сервере или на внешнем хосте. И лишь незначительная часть зарубежных публичных библиотек ответили, что размещают информацию на корпоративном сайте, а 7 библиотек не имеют на данный момент сайта вообще. В свою очередь для вузовских библиотек характерно размещение информации на корпоративных сайтах, особенно явно это выделяется у российских библиотек: 72 библиотеки из опрошенных не имеют отдельного от университета сайта. Сайты большинства зарубежных вузовских библиотек (69 респондентов) располагаются либо на собственных серверах, либо на внешних хостах, и только 25 вузовских библиотек размещают информацию на корпоративных сайтах университетов. Все опрошенные российские детские и юношеские библиотеки подтвердили наличие своих отдельных сайтов на внешних хостах.

Основными ресурсами, генерируемыми библиотеками, остаются электронные каталоги (табл. 3). В создании цифровых коллекций и навигаторов по ресурсам значительный перевес наблюдается у зарубежных библиотек, при этом российские библиотеки большее внимание уделяют полнотекстовым и библиографическим БД (76% и 75% соответственно).

Текстовая информация остается наиболее популярной. Однако, как видно из данных табл. 4, зарубежные библиотеки более активны с другими видами информации – фото (85%), веб-архивы (51%), подкасты (47%) и вебкасты (45%), научные данные (43%). Российские библиотеки в меньшей степени уделяют внимание работе с такими видами информации.

Таблица 2

Наличие сайтов у библиотек разных организационно-правовых форм

Библиотеки	Собственный сервер (физически находящийся в библиотеке)		Отдельный сайт на внешнем хосте		Как часть корпоративного сайта		Нет сайта	
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные
Академические	4	8	7	-	10	-	-	-
Вузовские	38	34	-	35	72	25	-	-
Публичные	23	34	31	27	-	6	-	7
Детские/юношеские	-	-	26	-	-	-	-	-

## Основные ресурсы, создаваемые библиотеками в веб

Ресурсы	Российские библиотеки		Зарубежные библиотеки	
	количество	доля от опрошенных, %	количество	доля от опрошенных, %
Навигаторы	13	6	41	23
Электронные каталоги	207	98	159	90
Фактографические БД	37	18	34	19
Библиографические БД	159	75	103	59
Полнотекстовые БД	161	76	96	55
Коллекции оцифрованных изданий	114	54	159	90
Другое	6	3	7	4

Таблица 4

## Виды информации, отраженные в ресурсах библиотек

Виды информации	В российских библиотеках		В зарубежных библиотеках	
	количество	доля от опрошенных, %	количество	доля от опрошенных, %
Текстовые	194	92	172	98
Звуковые (подкасты)	32	15	82	47
Видео (вебкасты)	53	25	80	45
Фото	91	43	150	85
Мультимедиа	65	31	89	51
Научные данные	61	29	75	43
Веб-архивы	23	11	89	51
Другое	4	2	7	4

Таблица 5

## Популярные социальные сети в российских и зарубежных библиотеках

Социальная сеть	Библиотеки (количество (доля от опрошенных, %))								Число библиотек, принявших участие в опросе
	академические		вузовские		публичные		детские/юношеские		
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные	
Facebook	7 (3,3%)	7 (3,9%)	38 (18,0%)	93 (52,0%)	52 (24,6%)	66 (36,9%)	17 (8,1%)	-	280 (72,4%)
YouTube	-	7 (3,9%)	24 (11,4%)	53 (29,6%)	49 (23,2%)	33 (18,4%)	17 (8,1%)	-	183 (47,3%)
ВКонтакте	7 (3,3%)	-	90 (42,7%)	-	54 (25,6%)	-	24 (11,4%)	-	176 (45,5%)
Twitter	-	-	24 (11,4%)	66 (36,9%)	24 (11,4%)	40 (22,3%)	10 (4,7%)	-	164 (42,4%)
Instagram	3 (1,4%)	-	28 (13,3%)	33 (18,4%)	45 (21,3%)	33 (18,4%)	21 (10,0%)	-	163 (42,1%)
Одноклассники	-	-	17 (8,1%)	-	24 (11,4%)	-	10 (4,7%)	-	51 (13,2%)
Другие	-	-	7 (3,3%)	13 (7,3%)	10 (4,7%)	13 (7,3%)	4 (1,9%)	-	47 (12,1%)

Значительное повышение активности библиотек в социальных сетях было отмечено в 2016 г.: 275 (81,8%) российских библиотек подтвердили наличие аккаунтов в социальных сетях [41]. В нашем исследовании собственное веб-представительство в социальных сетях в 2019 г. подтвердили 379 (97,9%) библиотек. Это доказывает тот факт, что с каждым годом библиотеки усиливают свое присутствие в сетях. Анализируя популярность социальных площадок для библиотек, мы пришли к выводу, что библиотеки во всем мире отдают предпочтение социальным сетям: *Facebook*, *YouTube*, ВКонтакте, *Twitter*, *Instagram* и т. д. (табл. 5). Рассмотрим подробно предпочтения социальных площадок библиотек разных организационно-правовых форм.

По результатам нашего опроса российские академические библиотеки для ведения своей деятельности в социальной сети выбирают 3 социальные площадки: ВКонтакте, *Facebook* и *Instagram*. Зарубежные академические библиотеки: *Facebook* и *YouTube*. Российские вузовские библиотеки имеют аккаунты в разных социальных сетях, однако наблюдается явное предпочтение социальной сети ВКонтакте – 90 (42,7%) библиотек подтвердили наличие собственных аккаунтов в этой сети. В свою очередь, зарубежные вузовские библиотеки предпочитают *Facebook* – именно здесь 93 (52,0%) вузовские библиотеки ведут работу. Схожая тенденция среди публичных библиотек: большая часть российских публичных библиотек имеет аккаунты во ВКонтакте (25,6%), а зарубежные публичные библиотеки – в *Facebook* (36,9%). Еще один вид библиотек представлен только российскими библиотеками – это детские/юношеские библиотеки, которые работают на разных социальных площадках, в частности, во ВКонтакте (11,4%), *Instagram* (10,0%), *Facebook*

(8,1%) и *YouTube* (8,1%). Таким образом, явным фаворитом среди российских библиотек является социальная сеть «ВКонтакте», а среди зарубежных – *Facebook*.

Многие библиотеки расширяют свою деятельность в веб-пространстве за счет создания и ведения сразу нескольких аккаунтов в разных социальных сетях (табл. 6). Это вызвано необходимостью охвата аудитории в глобальном масштабе и оперативного распространения информации в виртуальном пространстве [42]. С другой стороны, работа на разных социальных площадках требует дополнительных трудовых ресурсов. Результаты опроса показали, что число аккаунтов в социальных сетях у библиотек так или иначе связано с количеством сотрудников библиотек. Так, наибольшее количество российских и зарубежных респондентов (51 библиотек), имеющих один аккаунт в социальной сети, располагают штатом сотрудников от 10 до 50 человек. Тогда как штат сотрудников библиотек, которые ведут активную деятельность в социальных сетях, имея четыре и более аккаунтов для этих целей, состоит из 100 и более человек (99 библиотек). Библиотеки, которые указали, что вообще не представлены в социальных сетях, имеют небольшой штат сотрудников – до 10 человек. Таким образом, мы наблюдаем прямую зависимость активности деятельности на разных социальных площадках и штата сотрудников библиотеки.

Несмотря на то что за короткий промежуток времени библиотеки значительно расширили сферу своей деятельности в социальных сетях, 3,8% российских библиотек (из 46,9% ответивших российских респондентов) не имеют представительств в социальных сетях, тогда как все зарубежные респонденты подтвердили абсолютное присутствие в социальных медиа.

Таблица 6

#### Аккаунты российских и зарубежных библиотек

Количество аккаунтов у библиотеки	Количество сотрудников в библиотеках (количество библиотек (доля от опрошенных, %))									
	до 10		от 10 до 50		от 50 до 100		от 100 до 300		более 300	
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные
Один	3 (1,4%)	26 (14,8%)	38 (18,0%)	13 (7,4%)	10 (4,7%)	-	3 (1,4%)	-	-	13 (7,4%)
Два	-	7 (4,0%)	17 (8,1%)	7 (4,0%)	3 (1,4%)	7 (4,0%)	-	-	-	-
Три	-	-	14 (6,6%)	7 (4,0%)	7 (3,3%)	7 (4,0%)	3 (1,4%)	33 (18,8%)	3 (1,4%)	-
Четыре и более	-	-	31 (14,7%)	-	9 (4,3%)	7 (4,0%)	39 (18,5%)	34 (19,3%)	12 (5,7%)	14 (8,0%)

## УПРАВЛЕНИЕ БИБЛИОТЕЧНЫМИ САЙТАМИ

Опрос показал, что большинство российских библиотечных сайтов управляется и ведется несколькими специалистами из разных отделов библиотеки – 86 ответов (40,9%). Следующая группа – это ИТ-специалисты – 52 ответа (24,6%), затем специализированный отдел – 35 ответов (16,6%). В рамках дополнительной работы библиотекарь занимается ведением сайта в 31 библиотеке (14,7%), в качестве основной работы – в 7 библиотеках (3,3%). В зарубежных библиотеках несколько иная ситуация. В большинстве опрошенных библиотек веб-сайтом управляет библиотекарь и делает это как часть своей работы – 54 ответа (30,7%). Исследование, проведенное в 2013 г., представляет результаты подобного опроса – большинство веб-сайтов библиотеки управлялось библиотекарями, которые работают на веб-сайте неполный рабочий день в рамках своей постоянной работы, т. е. это не единственная их работа (50%) [10]. Одинаковым количеством сайтов управляют специализированные отделы библиотеки или не библиотечные сотрудники (ИТ-специалисты) – по 41 ответу (23,3%). В 28 библиотеках (15,9%) управлением сайтов занимаются несколько специалистов из разных отделов. Внешние компании ведут библиотечные сайты в 6 случаях, и в 6 же случаях библиотекарь выполняет это как свою основную работу.

Анализ ответов различных типов библиотек на вопрос по управлению сайтами (табл. 7) показал, что веб-сайты российских вузовских библиотек, как правило, ведутся либо несколькими специалистами, либо библиотекарем в рамках дополнительной работы, управление сайтом специализированным отделом или ИТ-специалистом встречается реже; в зарубеж-

ных вузах сайтами, в основном, занимается библиотекарь как дополнительной работой. Веб-сайты российских академических библиотек ведут либо ИТ-специалисты, либо несколько специалистов из разных отделов, за рубежом это делает специализированный отдел. В российских публичных библиотеках управлением сайтов чаще всего занимаются несколько специалистов, почти треть сайтов ведут ИТ-специалисты, около 25% сайтов управляет специализированный отдел; в зарубежных публичных библиотеках представлены все типы управления сайтами. В рамках основной деятельности библиотекари занимаются ведением сайтов только в российских вузовских библиотеках и публичных зарубежных.

Результаты опроса показали, что российские сайты вузовских и публичных библиотек чаще всего управляются несколькими специалистами из разных отделов, академических – ИТ-специалистами.

Более детальный анализ ответов респондентов – представителей российских библиотек на данный вопрос с позиции штатного количества сотрудников в библиотеке показал, что в небольших библиотеках, со штатом от 10 до 50 человек ведением и управлением сайтов в основном, занимается библиотекарь как дополнительной работой, либо несколько специалистов из разных отделов, в небольших библиотеках – ИТ-специалист, что можно объяснить недостаточным штатным обеспечением. В библиотеках со штатом до 300 человек данной работой в большинстве случаев занимается несколько человек из разных отделов. Только в средних и больших по численности сотрудников библиотеках управлением сайтов занимаются в основном специализированные отделы.

Таблица 7

Управление сайтами российских библиотек

Управление сайтом	Библиотеки (количество (доля от опрошенных, %))						
	академические		вузовские		публичные		детские/ юношеские
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские
Несколько специалистов из разных отделов	11 (52,4%)	-	42 (38,2%)	14 (14,6%)	24 (44,4%)	13 (17,2%)	11 (42,3%)
ИТ-специалист	10 (47,6%)	-	14 (12,7%)	20 (20,8%)	16 (29,7%)	21 (27,6%)	11 (42,3%)
Специализированный отдел	-	8 (100%)	16 (14,5%)	27 (28,1%)	14 (25,9%)	7 (9,2%)	4 (15,4%)
Библиотекарь (дополнительная работа)	-	-	31 (28,2%)	35 (36,5%)	-	21 (27,6%)	-
Библиотекарь (основная работа)	-	-	7 (6,4%)	-	-	7 (9,2%)	-
Внешняя компания	-	-	-	-	-	7 (9,2%)	-

Распределение обязанностей по работе с сайтом, когда наполнение и ведение сайта осуществляется специалистами из разных отделов, программистами, сотрудниками, информированными во всех сферах библиотечной деятельности, представляется перспективным, однако это может быть проблемной, так как понимание того, как интерпретировать, использовать и внедрять изменения на веб-сайт требует навыков, которыми библиотекари, не выполняющие эти задачи на постоянной основе, могут не обладать и не иметь достаточно времени [10, 43, 44].

## ЮЗАБИЛИТИ-ТЕСТИРОВАНИЕ В БИБЛИОТЕЧНОЙ ПРАКТИКЕ

Результаты опроса свидетельствуют о том, что тестирование на удобство использования веб-сайтов не является важным приоритетом для большинства библиотек. Так, 62,1% российских библиотек не проводили юзабилити-тестирование, что подтверждает выводы других исследователей [10, 45], несмотря на то, что удобству использования библиотечных сайтов придается большое значение [15, 16, 46].

Примечательно, что вузовских библиотек, принявших участие в опросе, было больше всех (110), но юзабилити-тестирование эти библиотеки проводили меньше (40%), чем публичные (47,5%). Данные анализа свидетельствуют о том, что детско-юношеские библиотеки уделяют больше внимания удобству использования своих сайтов (8,7%), а академические библиотеки это практически не интересуется (3,8%).

Зарубежные библиотеки в 50% случаев проводили юзабилити-тестирование. Свои сайты на удобство использования проверяли все ответившие академические библиотеки, большинство вузовских библиотек (64,6%) и только 27,6% публичных.

Таким образом, удобство сайтов для пользователей большинства опрошенных библиотек остается неизвестным, библиотеки не занимаются активно изучением предпочтений пользователей, мало взаимодействуют с ними для достижения высокого уровня обслуживания.

## ВЕБ-АНАЛИТИКА САЙТОВ БИБЛИОТЕК

Веб-представительства – это сложные ресурсы, для эффективного развития которых применяются современные методы веб-аналитики. Web-технологии позволяют реализовать управление ресурсами, используя статистические данные о посетителях и посещаемости сайта библиотеки. Данные опроса показали, что из существующего разнообразия аналитических инструментов российские и зарубежные библиотеки выбирают аналитические системы Яндекс.Метрика (ЯМ) и *Google Analytics* (GA). Основная цель использования данных инструментов – это анализ: посещаемости; источников трафика; аудитории (интересы, география посетителей, демографические характеристики, лояльность той или иной группы посетителей); поведения посетителей; контента; технологий, используемых посетителями; производительности сайта; конверсии.

Таблица 8

Популярные инструменты веб-аналитики в российских и зарубежных библиотеках, используемые для оценки сайта

Инструменты веб-аналитики	Библиотеки (количество (доля от опрошенных, %))								Число библиотек, принявших участие в опросе
	академические		вузовские		публичные		детские/ юношеские		
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные	
Google Analytics	7 (3,3%)	7 (4,0%)	17 (8,1%)	91 (51,7%)	28 (13,3%)	52 (29,5%)	7 (3,3%)	-	209 (54,0%)
Яндекс.Метрика	3 (1,4%)	-	52 (24,6%)	-	48 (22,7%)	-	21 (10,0%)	-	124 (32,0%)
Лог-анализаторы	10 (4,7%)	7 (4,0%)	42 (19,9%)	20 (11,4%)	7 (3,3%)	-	-	-	86 (22,2%)
Рейтинг@mail.ru	-	-	7 (3,3%)	-	21 (10,0%)	-	10 (4,7%)	-	38 (9,8%)
WordPress Stats	-	6 (3,4%)	-	20 (11,4%)	-	7 (4,0%)	-	-	33 (8,5%)
LiveInternet	3 (1,4%)	-	7 (3,3%)	-	10 (4,7%)	-	7 (3,3%)	-	27 (7,0%)
Спутник аналитика	-	-	-	-	10 (4,7%)	-	3 (1,4%)	-	13 (3,4%)
Piwik	-	-	-	-	-	7 (4,0%)	-	-	7 (1,8%)
Siteimprove	-	-	-	7 (4,0%)	-	-	-	-	7 (1,8%)
HotLog	-	-	3 (1,4%)	-	3 (1,4%)	-	-	-	6 (1,6%)



Среди используемых аналитических инструментов в российском библиотечном сегменте лидирующую позицию занимает ЯМ: предпочтение данной системе отдают 124 библиотеки или 58,8% от общего числа опрошенных российских респондентов. В свою очередь, зарубежные библиотеки почти единогласно выбирают GA – 150 библиотек или 85,2% от числа принявших участие в опросе зарубежных респондентов. В топе популярных веб-аналитических инструментов эти системы занимают первые места. Первенство принадлежит системе GA, именно этому инструменту отдают предпочтение 209 из 387 библиотек во всем мире, на втором месте ЯМ – 32,0 % от общего числа библиотек, принявших участие в опросе. Третье место библиотеки во всем мире отдают лог-анализаторам – 86 библиотек (22,2%).

В выборе аналитических инструментов российские академические и вузовские библиотеки, прежде всего, отдают предпочтение трем инструментам: ЯМ, GA и лог-анализаторам (табл. 8). Академические библиотеки чаще всего устанавливают на собственные сайты лог-анализаторы, тогда как вузовские библиотеки предпочитают счетчик ЯМ. Публичные библиотеки для оценки сайтов используют разные инструменты, чаще всего это ЯМ, GA и Рейтинг@mail.ru. Детские и юношеские библиотеки явное предпочтение отдают аналитической системе ЯМ, но при этом не используют для сбора данных лог-анализаторы. Зарубежные библиотеки независимо от вида отмечают равнозначный выбор таких аналитических инструментов, как GA, лог-анализатор и WordPress Stats.

Кроме того, многие российские библиотеки отметили использование сразу нескольких инструментов (3 и более) – 83 респондента (39,3%), где самым по-

пулярным сочетанием инструментов (27,5%) является использование ЯМ, GA и лог-анализатора. И ЯМ, и GA относятся к счетчикам посещений (внешние программы), тогда как лог-анализаторы – внутренние программы. Таким образом, мы наблюдаем общую тенденцию в использовании библиотеками обеих технологий измерения, что представляется оптимальным решением для получения достоверных данных.

## ОЦЕНКА ДЕЯТЕЛЬНОСТИ БИБЛИОТЕКИ В СОЦИАЛЬНЫХ СЕТЯХ ИНСТРУМЕНТАМИ ВЕБ-АНАЛИТИКИ

Как показали результаты опроса, для оценки эффективности развития аккаунтов в социальных медиа 242 библиотеки чаще всего используют встроенные в аккаунт инструменты. Также было установлено, что в дополнение к данному виду инструментов библиотеки используют GA и некоторые маркетинговые инструменты (*Followerwonk*, *Hootsuite*, *Sprout Social* и др.) (табл. 9). При этом группу маркетинговых инструментов используют только зарубежные библиотеки (12% респондентов от зарубежных библиотек). Цель использования этой группы инструментов – оценка деятельности собственных аккаунтов в социальных сетях, в частности, *Followerwonk* является узкоспециализированным инструментом для анализа аккаунта в социальной сети *Twitter*. Среди существующего разнообразия маркетинговых инструментов библиотеки выбирают также *Hootsuite* и *Sprout Social*, что может объясняться уникальными возможностями этих инструментов, например, с их помощью планируются дата и время суток выхода постов.

Таблица 9

Популярные инструменты веб-аналитики в российских и зарубежных библиотеках, используемые для оценки аккаунта

Инструменты веб-аналитики	Библиотеки (количество (доля от опрошенных, %))								Число библиотек, принявших участие в опросе
	академические		вузовские		публичные		детские/ юношеские		
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные	
Встроенные в аккаунт инструменты	7 (3,3%)	7 (4,0%)	55 (26,1%)	65 (36,9%)	45 (21,3%)	39 22,2%	24 (11,4%)	-	242 (62,5%)
Hootsuite	-	-	-	7 (4,0%)	-	-	-	-	7 (1,8%)
Follower-wonk	-	-	-	-	-	7 (4,0%)	-	-	7 (1,8%)
Sprout Social	-	-	-	7 (4,0%)	-	-	-	-	7 (1,8%)
Google Analytics	3 (1,4%)	-	-	-	-	-	-	-	3 (0,8%)

Однако значительная часть респондентов, как в российском, так и зарубежном библиотечном сегменте, не осуществляют аналитику собственных аккаунтов – 125 библиотек (32,3% от общего числа респондентов, принявших участие в опросе), демонстрируя тем самым самую слабую заинтересованность, что может свидетельствовать о незнании возможностей указанных инструментов.

## ПОКАЗАТЕЛИ ОЦЕНКИ ВЕБ-РЕСУРСОВ БИБЛИОТЕК

Аналитический потенциал современных веб-инструментов довольно широк, что позволяет собирать разнообразные вебметрические показатели. На вопрос: «Какие показатели для оценки сайта Вы используете?», респонденты назвали вебметрические показатели, которые являются ключевыми для оценки эффективности деятельности конкретной библиотеки в веб-пространстве. На основании анализа полученных ответов от российских и зарубежных респондентов выявлен следующий список ключевых метрик: посетители – 301 библиотека (77,8%); визиты – 257 библиотек (66,4%); уникальные посетители – 203 библиотеки (52,5%); география посетителей – 165 библиотек (42,6%); источники трафика – 144 библиотеки (37,2%); среднее время, проведенное на сайте – 129 библиотек (33,3%); новые посетители – 115 библиотек (29,7%). Менее значимы для библиотек показатели: глубина просмотра – 98 библиотек (25,3%); количество зарегистрировавшихся пользователей на сайте – 85 библиотек (22,0%); показатель отказов – 68 библиотек (17,6%); количество повторных посещений – 64 библиотеки (16,5%); гендерный анализ пользователей – 57 библиотек (14,7%); количество положительных отзывов – 35 библиотек (9,0%).

109 из 387 библиотек для оценки сайта используют 1-2 показателя (табл. 10). Это может свидетельство-

вать о нехватке собственных трудовых ресурсов для решения аналитических задач, и косвенно подтверждается тем, что большинство библиотек, использующих 1-2 показателя для оценки сайтов, имеют в штате до 50 человек. Более того, библиотеки, не занимающиеся оценкой сайтов, также входят в эту группу библиотек. В свою очередь, библиотеки со штатом сотрудников от 100 до 300 и более – это 98 библиотек – как правило, используют для оценки сайтов четыре и более показателей, что подтверждает выдвинутую выше гипотезу. Однако некоторые библиотеки демонстрируют заинтересованность в развитии сайта с использованием аналитических возможностей инструментов, несмотря на небольшой штат сотрудников. Так, ряд зарубежных библиотек, штат сотрудников которых состоит от 1 до 10 человек, выбирают для оценки сайта библиотеки 4 и более показателей. Например, Объединенная библиотечная служба Университета Коимбры (*University of Coimbra Joint Libraries Service*) (Португалия) выбирает 4 ключевые метрики для оценки сайта: посетители; визиты; источники трафика; показатель отказов. Следует отметить, что 62 российские библиотеки с количеством сотрудников от 10 до 100 человек выбирают четыре и более показателей. При этом максимальное число показателей среди российских и зарубежных библиотек варьируется от 4 до 12.

Для получения объективных результатов важно брать во внимание разные показатели, в том числе для большей конкретизации информации проводить сегментирование данных, сравнивая сегменты между собой. В качестве вывода, следует отметить, что наиболее популярными для оценки эффективности библиотечного сайта представляются метрики посещаемости [47], которые являются ключевыми для библиотек, позволяя оценивать эффективность/неэффективность их деятельности в веб-пространстве.

Таблица 10

Количество показателей, используемых для оценки сайтов библиотек

Количество показателей	Количество сотрудников в библиотеках (количество библиотек (доля от опрошенных, %))									
	до 10		от 10 до 50		от 50 до 100		от 100 до 300		более 300	
	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные	российские	зарубежные
Один	-	7 (4,0%)	21 (10,0%)	7 (4,0%)	3 (1,4%)	-	3 (1,4%)	7 (4,0%)	-	7 (4,0%)
Два	3 (1,4%)	-	17 (8,1%)	7 (4,0%)	7 (3,3%)	-	-	20 (11,4%)	-	-
Три	-	13 (7,4%)	17 (8,1%)	7 (4,0%)	10 (4,7%)	7 (4,0%)	10 (4,7%)	7 (4,0%)	-	-
Четыре и более	3 (1,4%)	13 (7,4%)	49 (23,2%)	-	10 (4,7%)	13 (7,4%)	31 (14,7%)	33 (18,8%)	14 (6,6%)	20 (11,4%)

На основании полученных данных мониторинга ключевых показателей принимаются важные решения по оптимизации веб-ресурса. Сравнивая показатели за предшествующий и текущий периоды можно сделать выводы о том, насколько эффективно развивается ресурс. Результаты опроса показали, что ключевыми показателями для оценки эффективности аккаунтов библиотек в социальных медиа являются: посетители – 253 библиотеки (65,4%); активность пользователей (количество оценок – «лайков» и «перепостов») – 198 библиотек (51,2%); визиты – 196 библиотек (50,6%); новые подписчики – 155 библиотек (40,1%); охват пользовательской аудитории – 131 библиотека (33,9%); рекомендации и отзывы в социальных медиа – 129 библиотек (33,3%); упоминания – 106 библиотек (27,4%). Меньшее внимания библиотеки уделяют показателям: количество положительных отзывов – 91 библиотека (23,5%); уникальные посетители – 88 библиотек (22,7%); новые посетители – 71 библиотека (18,3%); количество переходов из социальных сетей – 68 библиотек (17,6%); география посетителей – 61 библиотека (15,8%); гендерный анализ аудитории – 54 библиотеки (14,0%); источники трафика – 36 библиотек (9,3%); среднее время, проведенное на сайте – 29 библиотек (7,5%); количество повторных посещений – 21 библиотека (5,4%); показатель отказов – 14 библиотек (3,6%); глубина просмотра – 14 библиотек (3,6%). Исходя из того, что основной функцией веб-представительств в социальных сетях является продвижение контента, библиотекам следует обращать внимание не только на социальные метрики, но и на метрики вовлечения и лояльности [47].

В качестве ключевых показателей эффективности аккаунта многие библиотеки выбирают 1-3 показателя – 127 библиотек (32,8%), 4 и более показателей – 224 библиотек (58,1%), 36 библиотек (9,3%) от общего числа ответивших респондентов не осуществляют анализ собственных аккаунтов. Максимальное количество метрик для оценки аккаунтов использует Библиотека Российской академии наук – 16 метрик. Однако это исключительный случай. Для других библиотек максимальное число метрик, как правило, варьируется от 4 до 7 показателей, что свидетельствует об экономном использовании возможностей веб-аналитических инструментов.

## ВЫВОДЫ

Важная тенденция современного развития библиотек – это выход в глобальное веб-пространство. Библиотеки активно формируют собственные веб-представительства, создавая официальные сайты (на собственном сервере, внешнем хосте или корпоративном портале) и аккаунты в социальных сетях, размещают там информацию о проводимых мероприятиях и услугах, ресурсы, включающие разнородную информацию (текст, видео, аудио, данные и др.), тем самым пытаясь повысить собственную конкурентоспособность на рынке информационных услуг, который стремительно развивается за счет не-

прерывного внедрения новых информационных технологий, а также стать ближе современному пользователю, который «уходит» в Интернет. Многие библиотеки сегодня имеют сразу несколько аккаунтов на разных социальных площадках, среди которых наиболее популярными являются *Facebook*, *YouTube*, *ВКонтакте*. Вместе с тем, отмечена разница в выборе социальных площадок для библиотек разных видов, что вполне объяснимо работой с целевой аудиторией, представленной в той или иной сети.

Для эффективного развития ресурсов библиотек в веб-пространстве уже недостаточно просто создать сайт, эффективность таких ресурсов напрямую зависит от своевременного управления и оптимизации удобства использования. Однако не все библиотеки осознают важность оценки имеющихся веб-ресурсов. Около двух третей респондентов сообщили, что никогда не проводили тест на удобство использования, и примерно в половине библиотек обязанности веб-дизайнера и веб-менеджера выполняют специалисты из разных отделов. Это может вызвать проблемы при управлении сайтом, так как понимание того, как интерпретировать, использовать и внедрять изменения на веб-сайт для улучшения удобства использования, требует навыков, которые специалисты, не выполняющие эти задачи на постоянной основе, могут не иметь. Выявлена также зависимость числа специалистов, занятых управлением и ведением сайтов библиотек разных видов, от количества сотрудников библиотек.

Важную роль в эффективном развитии веб-ресурсов сегодня играют аналитические инструменты, поэтому особое внимание в нашем исследовании было уделено использованию веб-технологий для оценки эффективности собственных ресурсов. Определены популярные инструменты веб-аналитики среди российских и зарубежных библиотек: зарубежные библиотеки независимо от типа отмечают *GA*, лог-анализаторы и *WordPress Stats*; российские академические и вузовские библиотеки отдают предпочтение *ЯМ*, *GA* и лог-анализаторам. Аналитика создаваемых веб-ресурсов не только отнимает много времени от другой, как правило, основной деятельности сотрудника, но и требует соответствующих профессиональных знаний и навыков. На сегодняшний день библиотеки для развития создаваемых веб-ресурсов используют лишь незначительную часть предоставляемых веб-аналитикой возможностей – экономное использование ключевых показателей для выявления их эффективности: оценивают эффективность сайта по 1-2 показателям – 109 библиотек (28,2%); эффективность деятельности веб-представительства в социальных медиа по 1-3 показателям – 127 библиотек (32,8%).

Более детальный анализ веб-представительств российских и зарубежных библиотек – предмет дальнейшего анализа, который позволит не только выявить тенденции развития библиотек в веб-пространстве, но и детально проанализировать лучшие практики работы, а также выработать рекомендации по повышению эффективности деятельности библиотек в веб-пространстве.

## СПИСОК ЛИТЕРАТУРЫ

1. Balaji B.P., Vinay M.S., Shalini B.G., Mohan J.S. Web 2.0 use in academic libraries of top ranked Asian universities // *Electronic Library*. – 2019. – Vol. 37(3). – P. 528-549. DOI: 10.1108/EL-12-2018-0248.
2. Wusteman J. The potential of web components for libraries // *Library Hi Tech*. – 2019. – Vol. 37, № 4. – P. 713-720. DOI: 10.1108/LHT-06-2019-0125.
3. Soohyung Joo, Namjoo Choi, Tae Hyun Baek. Library marketing via social media: The relationships between Facebook content and user engagement in public libraries // *Online Information Review*. – 2018. – Vol. 42, № 6. – P. 940–955. DOI: 10.1108/OIR-10-2017-0288.
4. Hopkins P., Hare J., Donaghey J., Abbott W. Geo, audio, video, photo: How digital convergence in mobile devices facilitates participatory culture in libraries // *Australian Library Journal*. – 2015. – Vol. 64, № 1. – P. 11-22. DOI: 10.1080/00049670.2014.984379.
5. Scardilli B. Streaming Video in Public Libraries // *Information Today*. – 2014. – Vol. 31, № 6. – P. 1-37.
6. Baggett M., Gibbs R. HistoryPin and Pinterest for Digital Collections: Measuring the Impact of Image-Based Social Tools on Discovery and Access // *Journal of Library Administration*. – 2014. – Vol. 54, № 1. – P. 11–22. DOI: 10.1080/01930826.2014.893111
7. Gavit B.K. Web based library services // *Library Philosophy and Practice (e-journal)*. – 2019, September. – URL: <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?Article=6178&context=libphilprac> (дата обращения: 18.02.2020).
8. Al-Qallaf C.L., Ridha A. A Comprehensive Analysis of Academic Library Websites: Design, Navigation, Content, Services, and Web 2.0 // *Tools International Information and Library Review*. – 2019. – Vol. 51, № 2. – P. 93-106. DOI: 10.1080/10572317.2018.1467166.
9. Rosenfeld L., Morville P., Arango J. *Information Architecture: For the Web and Beyond*, 4th edition. – Sebastopol, USA: Published by O'Reilly Media, 2015. – 486 p.
10. Chow A.S. et al. The Website Design and Usability of US Academic and Public Libraries // *Reference & User Services Quarterly*. – 2014. – Vol. 53, № 3. – P. 253–265.
11. Garrett J.J. *The elements of user experience: User-Centered design for the web and beyond*. – Berkeley, CA: New Riders, 2011.
12. Lazar J. *Web Usability: A User-Centered Design Approach*. – Boston: Pearson Education, 2006.
13. Nielsen J. *Usability 101: Introduction to Usability*. Nielsen Norman Group. – 2012. – URL: <https://www.nngroup.com/articles/usability-101-introduction-to-usability> (дата обращения: 12.12.2019).
14. Круг С. Не заставляйте меня думать: веб-юзабилити и здравый смысл: лучшая книга по юзабилити для начинающих / пер. с англ. М.А. Райтмана. – 3-е изд. – М.: Изд-во «Э», 2017. – 253 с.
15. Drivas I.C., Sakas D.P., Reklitis P. Improving Website Usability and Traffic Based on Users Perceptions and Suggestions – A User-Centered Digital Marketing Approach // *Strategic Innovative Marketing. IC-SIM 2017. Springer Proceedings in Business and Economics*. – Cham: Springer, 2019. – P. 255-266.
16. Miller J. The Design Cycle and a Mixed Methods Approach for Improving Usability: A Case Study // *Journal of Web Librarianship*. – 2019. – URL: <https://www.tandfonline.com/doi/pdf/10.1080/19322909.2019.1600451?needAccess=true> (дата обращения: 09.12.2019).
17. Sotnikov A.N., Sobolevskaya I.N., Kirillov S.A., Cherednichenko I.N. Subject-oriented and interdisciplinary digital collections in the electronic environment knowledge // *CEUR Workshop Proceedings*. – 2018. – № 2260. – P. 448-453.
18. Ahammad N. Open source digital library on open educational resources // *Electronic Library*. – 2019. – Vol. 37, № 6. – P. 1022-1039. DOI: 10.1108/EL-11-2018-0225.
19. Li S., Hao Z., Ding L., Xu X. Research on the application of information technology of Big Data in Chinese digital library // *Library Management*. – 2019. – Vol. 40, № 8-9. – P. 518-531. DOI: 10.1108/LM-04-2019-0021.
20. Frischmuth F., Schauerte G. Deutsche digitale bibliothek – Eine erste bilanz 2011-2015 // *Zeitschrift für Bibliothekswesen und Bibliographie*. – 2015. – Band 62, № 5. – S. 232-237.
21. Рогозникова О.А. Модель библиотечного сайта на основе Web-ИРБИС // *Науч. и техн. б-ки*. – 2016. – № 11. – С. 131–135.
22. Соколинский Е.К. Разговоры с сайтом // *Национальная библиотека*. – 2016. – № 2. – С. 70–73.
23. Ткачева Е.В. Создание и наполнение сайта научной библиотеки (на примере библиотеки Главного ботанического сада им. Н. В. Цицина РАН) // *Науч. и техн. б-ки*. – 2017. – № 1. – С. 88–95.
24. Потехина Ю.В. Управление официальным сайтом библиотеки как предмет научных исследований: постановка проблемы // *Библиосфера*. – 2011. – № 4. – С. 85–89.
25. Редькина Н.С. Службы информационных технологий в научных библиотеках // *Науч. и техн. б-ки*. – 2010. – № 11. – С. 34–44.
26. Редькина Н.С. Эффективность библиотечных сайтов // *Науч. и техн. б-ки*. – 2010. – № 9. – С. 56–66.
27. Шевченко Л.Б. Организация и ведение сайта библиотеки. Опыт Государственной публичной научно-технической библиотеки Сибирского отделения Российской академии наук // *Труды ГПНТБ СО РАН. Вып. 8: Новые направления деятельности традиционных библиотек в электронной среде : материалы межрегион. науч.-практ. конф. (22-26 сент. 2014 г., г. Красноярск)*. – Новосибирск, 2015. – С. 224–227.
28. Клифтон Б. *Google Analytics для профессионалов / пер. с англ.* – 3-е изд. – М.: Диалектика: Вильямс, 2017. – 607 с.

29. Кошик А. Веб-аналитика 2.0 на практике: тонкости и лучшие методики / пер. с англ. – М.: Диалектика : Вильямс, 2017. – 526 с.
30. Hassler M. Web Analytics – Metriken auswerten, Besucherverhalten verstehen, Website optimieren. 3 Auflage. – Heidelberg, 2012. – 562 s.
31. Amthor A., Brommund T. Mehr Erfolg durch Web Analytics. Ein Leitfaden für Marketer und Entscheider. – München: Hanser, 2010. – 287 p.
32. Turner S.J. Website statistics 2.0: Using Google analytics to measure library website effectiveness // Technical Services Quarterly. – 2010. – Vol. 27, № 3. – P. 261-278.
33. Кожушко О.А. и др. Интернет-маркетинг и digital-стратегии: принципы эффективного использования : учеб. пособие / М-во образования и науки РФ, Новосиб. нац. исслед. гос. ун-т, Компания Intelsib. – Новосибирск : НГУ, 2015. – 313 с.
34. Кулева О.В. Инструменты веб-аналитики в библиотечной практике (на примере Государственной публичной научно-технической библиотеки Сибирского отделения Российской академии наук) // Труды ГПНТБ СО РАН. – 2017. – № 12-1. – С. 369–381.
35. Manuel S., Dearnley J., Walton G. Strategic development of UK academic library websites: A survey of East Midlands university libraries // Journal of Librarianship and Information Science. – 2010. – Vol. 42, № 2. – P. 147-155.
36. Wilson A. Paula. Library Web sites : creating online collections and services. – Chicago: American Library Association, 2004. – 146 p.
37. Sapateiro C., Gomes J. Leverage Web Analytics for Real Time Website Browsing Recommendations // Recent Advances in Information Systems and Technologies. WorldCIST: World Conference on Information Systems and Technologies. – 2017. – Vol. 2. – P. 538–548.
38. Шевченко Л.Б. Методы поисковой оптимизации: опыт применения в ГПНТБ СО РАН // Науч. и техн. б-ки. – 2018. – № 3. – С. 24–32.
39. Case D. Looking for information: A survey of research on information seeking, needs and behavior (3rd ed.). – Bingley: Emerald, 2012.
40. Pickard A. Research methods in information. – London: Facet, 2012. – 384 p.
41. Редькина Н.С., Васильева Н.В., Коломенская А.С. Использование облачных сервисов в библиотеках России: результаты исследования // Научно-техническая информация. Сер. 1. – 2017. – № 6 – С. 21–30.
42. Павлюченко Г.В., Карауш А.С. Виртуальные представительства муниципальных библиотек Томска в социальных сетях // Материалы Третьего Международного профессионального форума «КНИГА. КУЛЬТУРА. ОБРАЗОВАНИЕ. ИННОВАЦИИ "КРЫМ-2017"». – М.: Гос. публич. науч.-тех. б-ка России. – 2017. – С. 97–102.
43. Шевченко Л.Б. Тенденции развития библиотечных сайтов: обзор публикаций // Труды ГПНТБ СО РАН. Вып. 13: Библиотеки в контексте социально-экономических и культурных трансформаций : материалы всерос. науч.-практ. конф. (Кемерово, 25–29 сент. 2017 г.) – Новосибирск, 2018. – Т. 2. – С. 224–236. DOI: 10.20913/2618-7575-2018-2-224-236.
44. Шевченко Л.Б. Дизайн и удобство библиотечных веб-сайтов // Научно-техническая информация. Сер. 1. – 2019. – № 11. – С.21–33; Shevchenko L.B. Design and Usability of Library Websites // Scientific and Technical Information Processing. – 2019. – Vol. 46, № 4. – P. 248-260. DOI: 10.3103/S0147688219040087
45. Connell R.S. Survey of Web Developers in Academic Libraries // Journal of Academic Librarianship. – 2008. – Vol. 34, № 2. – P. 121–129.
46. Rennick B. Library Services Navigation: Improving the Online User Experience // Information Technology and Libraries. – 2019. – Vol. 38, № 1. – P. 14–26. DOI:10.6017/ital.v38i1.10844
47. Ударцева О.М., Рыхторова А.Е. Использование инструментов веб-аналитики в оценке эффективности способов продвижения библиотечных ресурсов // Библиосфера. – 2018. – № 2. – С. 93–99. DOI: 10.20913/1815-3186-2018-2-93-99.

*Материал поступил в редакцию 20.02.20.*

#### Сведения об авторах

**РЕДЬКИНА Наталья Степановна** – доктор педагогических наук, заместитель директора по научной работе Государственной публичной научно-технической библиотеки Сибирского отделения Российской академии наук (ГПНТБ СО РАН), г. Новосибирск  
e-mail: to@spsl.nsc.ru

**УДАРЦЕВА Ольга Михайловна** – младший научный сотрудник научно-технологического отдела ГПНТБ СО РАН  
e-mail: Udartseva@spsl.nsc.ru

**ШЕВЧЕНКО Людмила Борисовна** – кандидат педагогических наук, старший научный сотрудник ГПНТБ СО РАН  
e-mail: shevchenkol@spsl.nsc.ru

# ДОКУМЕНТАЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

---

УДК 002–047.44

Е.В. Бескаравайная, Т.Н. Харыбина

## О факторах, влияющих на цитируемость научной статьи

*Показатель цитирования учитывается при мониторинге деятельности научной организации, обязательно включается в заявку на получение гранта или участия в конкурсе, лежит в основе стимулирующих надбавок. Приводятся результаты анализа публикаций одного из институтов научного центра по физико-химической биологии, которые не были процитированы ни разу, начиная с 2014 г. Показано изучение влияния различных потенциальных факторов на число цитирований. Представлены рекомендации, способствующие повышению видимости публикации в научных кругах.*

**Ключевые слова:** библиометрический анализ, библиометрия, научная продуктивность, научные исследования, библиометрические базы данных, публикационная активность, индексы цитирования

DOI: 10.36535/0548-0019-2020-05-4

### ВВЕДЕНИЕ

Результаты изучения такого библиометрического показателя, как цитируемость, дают возможность администрации научного учреждения оценивать общую продуктивность научного коллектива, получать информацию о динамике и тенденциях развития той или иной научной области, расширить научные связи, выявлять круг перспективных изданий. Используя такой показатель в качестве маркеров важнейших идей при «картографировании» науки [1] руководители получают инструмент для формирования эффективной системы научных подразделений. Особенно привлекательно выглядит применение данных цитирования для оценки научного труда, поскольку не требует личного взаимодействия с респондентом и может проводиться сторонними независимыми экспертами [2]. Понимая всю важность выбора критериев оценки научно-исследовательской деятельности, сотрудники информационных подразделений организаций считают, что количество публикаций и их цитирование в большей степени демонстрируют активность ученого и его коммуникативные связи, но не его научные достижения. Сам факт цитирования часто является благодарностью к своим коллегам, чьи знания позволили автору публикации осуществить исследование, поэтому список литературы к статье – это перечень наиболее важных источников по теме. Однако на выбор цитируемого документа влияет огромное количество различных факторов [3], часто не

относящихся к их научным достоинствам, например: физическая доступность документа [4], определенный тип публикации [5], личные отношения [6], дань традиционного уважения к цитируемому автору [7]. По результатам исследований российских и зарубежных библиографов прослеживается положительная корреляция между частотой цитирования публикаций и числом соавторов работы [8], тиражом журнала и базами индексирования [9], объемом статьи [10]. Зарубежные коллеги рассматривают вариант, когда число ссылок в публикации зависит от ее расположения в выпуске журнала [11–13] и даже личных знакомств в социальных сетях [14, 15]. Нельзя исключать и фактор случайности: статья вполне могла быть прочитана, только потому, что она оказалась в поле зрения ученого, а не была наиболее важной для его исследования. Кроме того, на цитирование влияет время опубликования: вторичные ссылки играют заметную роль в цитировании, затеяя первоначальные исследования и заставляя использовать наиболее «свежую» информацию. Собирая литературу по исследуемой проблеме, нам стоило немалых усилий найти ранние публикации, затрагивающие выбор цитат, и сослаться на авторов, получивших первоначальные результаты, исключая подтверждающие и обзорные статьи.

С практической точки зрения высокое цитирование действительно служит свидетельством официального признания учёного научным сообществом и официальным подтверждением его научного авторитета.

**Общие показатели публикационной активности и цитируемости  
Институт Белка РАН за 2014-2018 гг.**

БД	Показатель	Год					Всего
		2014	2015	2016	2017	2018	
WoS CC	Количество публикаций ИБ РАН	43	73	70	41	76	302
	Цитирование в год публикации <sup>1</sup>	29	25	19	12	39	124
	Цитирование всех публикации института в 2014-2018 гг.	2015	2119	2067	1948	2210	10359
	Количество цитирующих статей за 2014-2018 гг.	29	93	153	222	278	775
Scopus	Количество публикаций ИБ РАН	79	132	123	118	162	614
	Цитирование в год публикации <sup>1</sup>	36	31	56	70	71	264
	Цитирование всех публикации института в 2014-2018 гг.	1969	2151	2119	2310	2556	11105
	Количество цитирующих статей за 2014-2018 гг.	36	140	275	513	625	1589

<sup>1</sup> Данный критерий учитывает количество цитирований статьи на год ее выхода. Такие публикации называются «быстроцитируемые» и свидетельствует об актуальности тематики исследований

Однако цитирование – процесс сложный и неоднозначный, тем более в сфере науки, где закономерен вопрос: Действительно ли не цитируемые работы не заслуживают внимания? В нашем исследовании мы не ставим задачу оценить научную значимость таких статей, но, на примере практического анализа по материалам БД *WoS CC* и *Scopus*, предлагаем рассмотреть отсутствие ссылок в некоторых публикациях как результат технологических недочетов, исправив которые, можно повысить видимость публикации в научном сообществе и получить заслуженный отзыв в дальнейшем.

В качестве анализируемого объекта нами был выбран Институт Белка РАН (ИБ РАН), имеющий высокие показатели публикационной активности и цитируемости по БД *WoS CC* и БД *Scopus* (табл. 1), обширные связи с иностранными коллегами, высокую долю молодых исследователей.

Определив среднее количество ссылок на одну статью в год ее выхода, мы выяснили, что 60% публикаций Института Белка РАН по БД *Scopus* были оценены как быстроцитируемые в 2017 г.; по БД *WoS CC* 51% таких публикаций отмечены в 2018 г.; а 2014 г. стал плодотворным для института по обеим базам: 46% и 67% быстроцитируемых работ, соответственно. Высокие показатели, хорошее цитирование, многоплановые международные связи являются для ИБ РАН нормой [17,18]. Именно поэтому интерес вызывают работы этого института, которые не были процитированы ни разу за 5 лет.

Сотрудниками Библиотеки Пуштинского научного центра разработана и опробована на практике модель мониторинга научных исследований на основе ежегодного анализа патентной и публикационной активности всех институтов Центра [19]. В 2019 г. впервые в нашей практике, помимо сведений о высокоцитируемых статьях и рейтинговых изданиях, для администрации ИБ РАН был проведен анализ публикаций, которые не получили ни одной ссылки с 2014 по 2019 гг.

## ЦЕЛЬ И МЕТОДЫ ИССЛЕДОВАНИЯ

В настоящем исследовании была поставлена цель выяснить: как публикации, прошедшие рецензирование, опубликованные в рейтинговых журналах, попавшие в международные библиографические базы данных, не привлекли внимание научных сообществ и не получили ни одного упоминания – цитаты (на момент сбора данных). Изначально, можно предположить, что такая ситуация складывается, если:

- а) тема статьи является новой, малоизученной и неизвестной в мире;
- б) представленное в статье научное направление является специфичным для конкретного института;
- в) научная область, к которой относится тема статьи, устарела, интерес к ней в мировом сообществе снизился;
- г) статья написано неграмотно, либо трудна к пониманию.

Из опыта изучения возможностей зарубежных баз данных, мы знаем, что по сравнению с другими иностранными системами БД *Scopus* шире охватывает публикации именно российских авторов и оперативнее отслеживает цитирование в российских изданиях. Используя поиск по тематическому профилю организации и ограничение по годам, на 1 августа 2019 г в базе данных *Scopus* нами было выявлено 247 работ ИБ РАН, опубликованных в 2014-2018 гг. По количеству цитирований эти публикации были условно разделены на 4 части подобно квартилям: в первую группу включены высокоцитируемые публикации с цитированием от 31 до 97, в 4-ю группу – статьи, не процитированные ни разу (на 1 августа 2019 г.). Остальные статьи были распределены в группы с малым цитированием (1 до 10 цитат) и средним цитированием (от 10 до 30 цитат). В табл. 2 показано, что каждая группа включала разное количество публикаций.

**Условное распределение публикаций по рейтинговым группам  
в зависимости от цитирования**

Рейтинговая группа	Количество цитирований	Количество публикаций в группе	Доля в общем числе публикаций, %
1	31–97	13	5,2
2	10–30	47	19,0
3	1–10	150	60,5
4	0	37	15,3

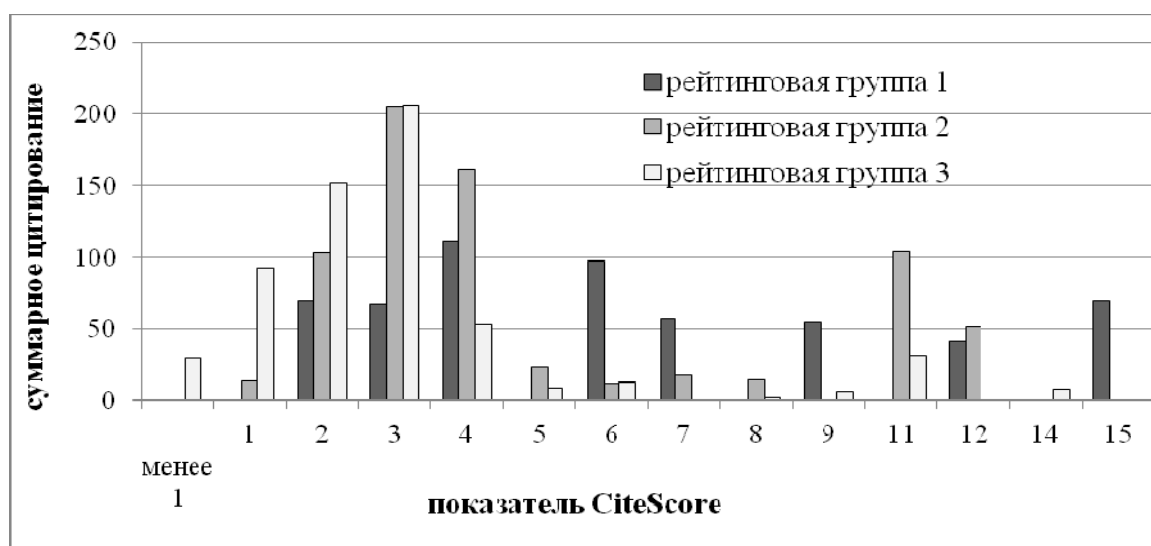


Рис. 1. Распределение суммарного цитирования публикаций 2014-2018 гг. по каждой рейтинговой группе относительно показателя цитируемости журнала CiteScore.

### ЗАВИСИМОСТЬ ЦИТИРУЕМОСТИ СТАТЕЙ ОТ ИМПАКТ-ФАКТОРА ЖУРНАЛА

Предположим, что цитирование статьи напрямую зависит от источника, в котором она опубликована, следовательно, наибольшее количество цитирований будет в журналах с высоким импакт-фактором (что вытекает из самого определения импакт-фактора). Проверим это на практике: расположим журналы, в которых опубликованы работы сотрудников ИБ РАН в порядке убывания их цитирования, и параллельно те же журналы в порядке убывания *CiteScore* (бесплатный и общедоступный сервис от *Scopus*, рассчитывающий среднее цитирование публикаций издания за 3-летний период). Как видно на рис. 1, публикации с высоким цитированием, входящие в рейтинговую группу 1, встречаются в журналах с различным *CiteScore* и не тяготеют к изданиям с высоким индексом цитируемости. Не прослеживается такой зависимости и у прочих рейтинговых групп, а наибольшее количество работ публикуется в журналах с показателем *CiteScore* от 1 до 4, независимо от их цитирования. Таким образом, предположение, что наибольшее количество цитирований получает публикация в журнале с наибольшим показателем цитируемости самого журнала – на практике не подтвердилось.

### ЗАВИСИМОСТЬ ЦИТИРУЕМОСТИ СТАТЕЙ ОТ ТЕМАТИКИ ЖУРНАЛА

Возможно, отсутствие цитирования публикации связано с тематикой исследования. Сравним публикации, процитированные высоко и выше среднего уровня, с публикациями, которые не были процитированы ни разу по их тематике. Такие научные области, как биохимия, аналитическая химия, молекулярная биология, цитология, фармакология, прикладная микробиология, кристаллография – встречаются в публикациях любой цитируемости. Тем не менее, исследования по биоинформатике, структурной биологии, ядерной физике, палеонтологии – присутствуют только в группе 4 (без цитирования). Наиболее вероятным объяснением не цитируемости таких публикаций будет неверное определение тематики издания, в которой была представлена статья. Для проверки этого предположения мы воспользовались системой управления библиографической информацией *EndNote*, в частности, функцией *Match*, которая, основываясь на многолетних исследованиях, предлагает помощь в определении нишевых изданий для публикации научных статей. В соответствующие поля нами были введены названия и рефераты статей и определен список журналов, наиболее соответ-



вующих тематике каждой из них. Затем, журналы отобранные программой, были проанализированы с точки зрения научных областей. В результате нами выявлена следующая закономерность: для 46% публикаций с нулевым цитированием, программой были предложены издания по другой тематике. Что касается высокоцитируемых статей, то они составляют всего 8%. Нами зарегистрированы случаи, когда публикации сотрудников ИБ РАН с одними и теми же ключевыми словами не имели цитирования в журналах по молекулярной биологии, биохимии и биомедицине, однако хорошо цитировались в научных ресурсах по генетике. *Таким образом, внимательное отношение к выбору издания, в которое направляется статья – одно из условий ее успешного научного пути.*

### КОРРЕЛЯЦИЯ ИСПОЛЬЗОВАНИЯ КЛЮЧЕВЫХ СЛОВ И ВИДИМОСТИ СТАТЕЙ

Более пристально разобраться с тематическим направлением нам позволит анализ публикаций по ключевым словам. Исключив общие термины (биология, клетка, белок, энзимы, ферменты, рибосомы, бактерии, биохимия) как неинформативные для нашего исследования, мы воспользовались функцией БД *Scopus*, позволяющей проводить поиск непосредственно по **авторским** ключевым словам. Первое, что привлекает внимание при анализе публикаций

без цитирования – это отсутствие авторских ключевых слов у 32% таких статей. Совершенно очевидно, что эти публикации не находятся при поиске, не попадая в массив данных, отбираемых учеными, работающими по схожим направлениям. Таким образом, на наш взгляд, *серьёзной причиной не цитируемости статьи становится отсутствие авторских ключевых слов, что приводит к ухудшению её видимости в научной среде независимо от тематики исследования.*

Для остальных публикаций из группы 4 (с нулевым цитированием) мы взяли ключевые слова в том виде, в котором их предоставляют авторы самих статей, и провели по ним поиск отдельно для каждой статьи.

В трех случаях в итоге были найдены только работы самих авторов, ключевые слова которых состояли из названия конкретного химического вещества, строго определенного метода или частного биохимического процесса. Следовательно, *использование специфических ключевых слов, описывающих слишком узкую тематику, ограничивает поиск и снижает видимость публикации, так же, как и полное их отсутствие.*

Оставшиеся статьи группы 4 обнаружили достаточное количество сторонних публикаций с теми же словосочетаниями (с учетом морфологии) в качестве ключевых слов (табл. 3).

Таблица 3

Соотношение публикаций ИБ РАН с нулевым цитированием и статей с точным повторением ключевых слов по БД *Scopus* за 2014-2018 гг.

ID статьи с цитированием = 0	Количество публикаций с точным повторением ключевых словосочетаний	Максимальное цитирование публикаций с точным повторением ключевых словосочетаний
11	1647	1543
31	471	315
20	325	333
19	190	111
14	189	248
32	98	159
17	90	158
6	86	65
10	53	104
3	52	267
15	48	58
13	34	225
33	25	60
35	21	87
18	20	82
8	16	20
36	11	14
27	9	30
4	7	12
12	7	6
9	6	30
5	5	5
21	5	8
2	2	14
28	2	20

Как видно из табл. 3, в каждой публикации сотрудников ИБ РАН, отраженной в БД *Scopus*, работы с такими же авторскими ключевыми словами не просто присутствовали, но и имели различную степень цитирования. Сравнение ключевых слов в публикациях ИБ РАН с нулевым цитированием и статей, отраженных в БД *Scopus*, с высоким цитированием, выявило общие биологические термины в качестве ключевых слов (*adenosine phosphate, amyloid protein, initiation factors*). При этом в процитированных работах имели место и другие термины, более ориентированно описывающие области исследований авторов, отсутствующие в статьях сотрудников института. Таким образом, использование ключевых слов, общих для всех публикаций по тематике (например: синтез протеина, амилоиды, рибосомальные протеины и пр.), не позволяет отобрать публикации института из всей массы научных трудов по данной теме, снижает видимость статьи и ее цитирование.

В процессе работы нам встретилась ситуация, когда автор использует одни и те же общие ключевые слова (например, «влияние УФ – излучения на клетку», «адаптационное изменение химического состава мембран») в нескольких своих публикациях и в различных журналах. В таких случаях невозможно проследить закономерность между тематикой исследования и цитированием работы, так как статьи с одинаковыми ключевыми словами встречаются как в группе нецитируемых публикаций, так и в группе с высоким цитированием.

Ещё один вариант, затрудняющий анализ – это отражение в БД *Scopus* одновременно и русского, и переводного издания, когда в базе оказываются сразу две версии статьи, одна из которых (как правило, переводной) имеет цитирование, а другая (как правило, в русском издании) не имеет. Такая ситуация интересна с точки зрения самоцитирования, когда сами авторы предпочитают ссылаться на свою переводную публикацию, игнорируя её первичный русский вариант. Возможной причиной такой практики может быть требование издателей к оформлению списков литературы к статье на английском языке или в транслитерации. Именно этот вариант и цитируется соавторами в последующих работах.

## ЗАВИСИМОСТЬ ЦИТИРОВАНИЯ ОТ ТЕМАТИКИ ИССЛЕДОВАНИЯ

Следующим предположением, от чего отсутствует цитирование, может быть снижение интереса мирового сообщества к данной научной области. Для каждой статьи ИБ РАН, изданной в 2014-2015 гг. и не процитированной ни разу за 5 лет, мы посмотрели связанные записи (*Related Records*) по базе данных *WoS CC* и проследили динамику изменения количества публикаций за 10 лет. Как видно на рис. 2, нет резкого снижения количества публикаций в связанных записях за 10 лет, соответственно, и уменьшения научного интереса к тематике самих публикаций не наблюдается. Более того, для статей *ID* (уникальный номер, позволяющий идентифицировать статью) 1,5,7 заметно стремительное увеличение потока публикаций по теме.

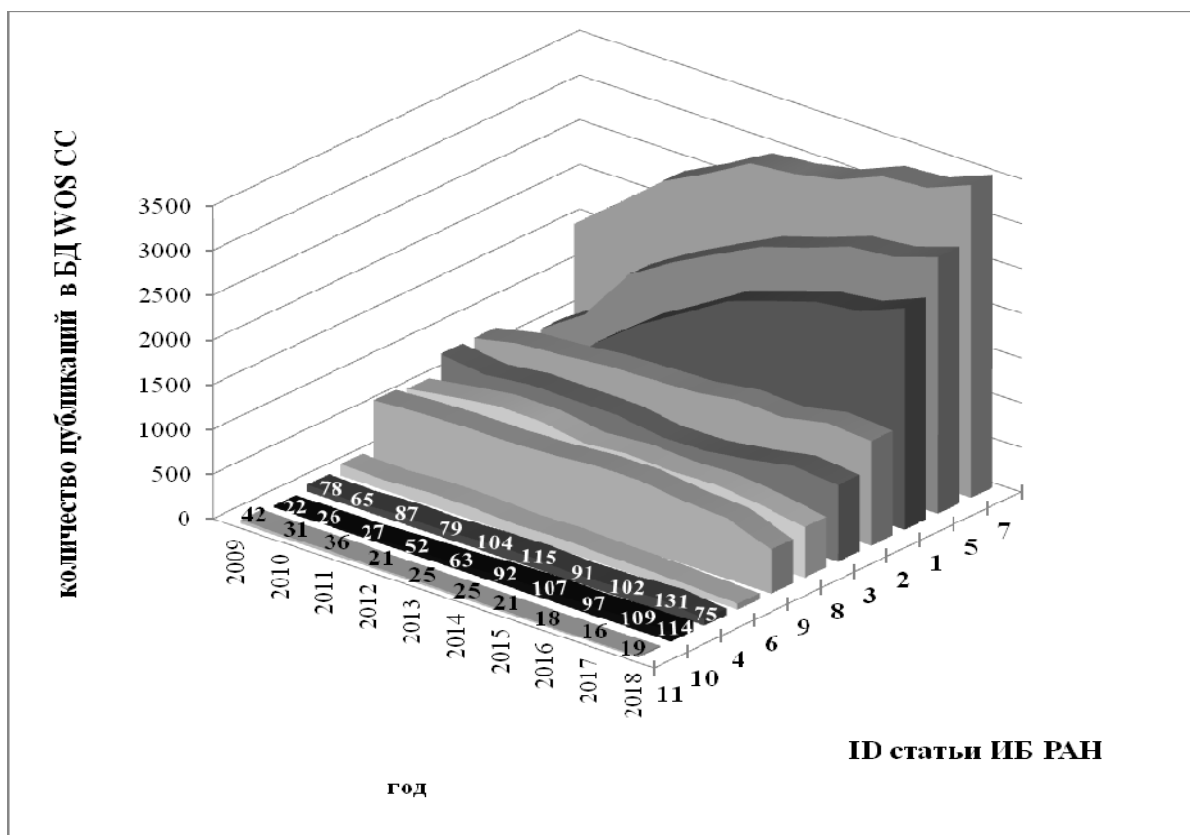


Рис. 2. Динамика связанных публикаций для статей Института Белка РАН с нулевым цитированием по годам.

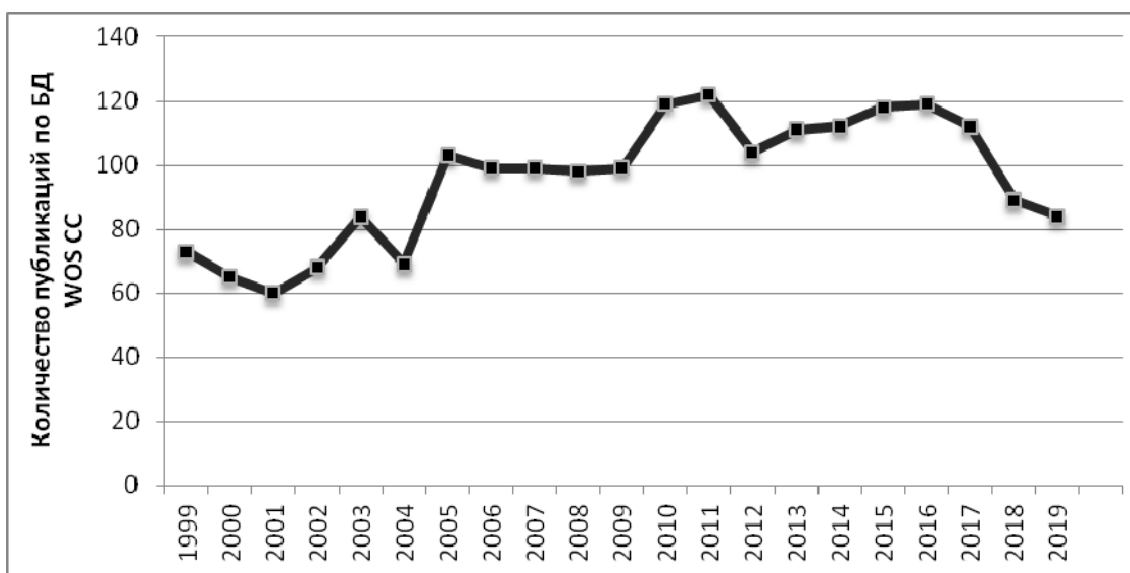


Рис. 3. Динамика публикационной активности по теме "Protein conformation problems" в БД WoS CC за 20 лет.

Из этого следует, что *отсутствие цитирования отдельных работ института не связано с падением интереса мирового сообщества к материалам исследований и не может быть объяснено неактуальностью тематических направлений*. Более того, для публикаций ID 4 и ID 10, мы отметили, что изначально небольшое количество связанных записей имеет тенденцию к росту с течением времени. Администрации ИБ РАН следует взять на заметку тематики этих публикаций как набирающие популярность и, возможно, перспективные области разработок в будущем.

В случае с публикацией ID 11 происходит незначительное снижение количества работ по теме, которое изначально было невелико. Изучив более подробно временную динамику статей по данной тематике («проблемы конформации белковой молекулы»), мы заметили, что пик работ с этими ключевыми словами приходится на более ранний период, а начиная с 2012 г. убывает (рис. 3).

Таким образом, мы можем утверждать, что в данном случае, действительно, *отсутствие цитирования может быть следствием падения интереса к тематике исследований*.

### ИЗУЧЕНИЕ ИНТЕРЕСА К ТЕМАТИКЕ ПУБЛИКАЦИИ ПО КОЛИЧЕСТВУ СКАЧИВАНИЙ

Снижение видимости для пользователя публикации в связи с непредставлением ключевых слов или неверно выбранной тематикой издания, не всегда может объяснить отсутствие ее цитируемости. Это заключение подтверждает функция «Параметры PlumX» от Scopus, позволяющая определять степень интереса к статье посредством просмотров аннотации, ссылок в соцсетях, сохранения библиографиче-

ской записи и т.д. Из 28 публикаций ИБ РАН, оставшихся без ссылок, только у 7 статей нет таких показателей. *Скачивания, или прочтения, на наш взгляд, полезный критерий, который подобно цитированию, может фиксировать интерес к тематике исследования*. Очевидно, что цитирование какой-либо публикации свидетельствует о тщательном ее изучении ученым, в отличие от простого скачивания любым пользователем. Вместе с тем, нельзя игнорировать тот факт, что статьи, ни разу не процитированные в научных изданиях, тем не менее, были просмотрены 18 (ID 26), 40 (ID 15), 79 (ID 28) раз, имеют ссылки на материал в соцсетях, сохранение списков литературы, просмотр полного текста (рис. 4).

Это свидетельствует о том, что тема привлекает внимание сообщества, читающего научную литературу, поэтому, изучая распределение цитирования научных публикаций, не стоит забывать об эффекте «отложенного спроса», описанного в модели М. Симкина и В. Ройчодхури [20] и объясняющего феномен резкого роста ссылок на нецитируемые публикации через несколько лет. Такие статьи, названные «Спящие красавицы» [21], выносят на рассмотрение научной обществу идеи, опережавшие своё время, и не получившие должного внимания на момент опубликования (например: результаты применения новейших методов и методик; впервые опубликованные экспериментальные данные и пр.). «Пробуждаясь» лишь через несколько лет, они начинают активно цитироваться тогда, когда у основного документопотока цитирование идет на спад [22]. На наш взгляд, будет целесообразно вернуться к рассмотрению цитирования этих публикаций несколько лет спустя.

Какие еще причины препятствуют прочтению и внесению статей в списки цитируемой литературы, несмотря на то, что их тематика вызывает живой интерес читателей? По-видимому, включаются такие

Степень использования		Получения	
EBSCO - Просмотры аннотации:	79	Mendeley - Читатели:	5
EBSCO - Ссылки на материал:	3		

Рис. 4. Пример использования статьи (DOI: 10.1134/S0026893315010082) с нулевым цитированием в БД *Scopus* по данным показателя «Параметры PlumX». (Скриншот страницы в БД *Scopus* на 17.02.2020)

факторы, как труднодоступная подача материала, неграмотный перевод, некачественные иллюстрации и пр. Всем, кто пишет и публикует научные статьи, известно, какая кропотливая работа предстоит, начиная от сбора данных и их анализа до оформления статьи и рисунков. Существенная доля критических замечаний рецензента при общей положительной рекомендации затрагивает требования по исправлению стиля изложения и иллюстрационного материала.

## ВЫВОДЫ

Проведенный нами анализ нецитируемых публикаций Института Белка РАН, позволяет сделать следующие заключения:

- для улучшения видимости публикации при поиске необходимо использовать ключевые слова;
- ключевые слова не должны быть слишком общими или специфическими;
- для публикации нужно тщательно выбирать тематику издания, с этой целью разумно использовать автоматические сервисы, позволяющие определять научные журналы, в которых статья по данной теме имеет наилучшие шансы на публикацию, экономя время и сводя к минимуму вероятность получения отказа;
- особое внимание следует уделять оформлению статьи, грамотному переводу, визуализации материалов, формированию библиографических списков и пр.
- для облегчения оценки и проверки результатов представляемой работы статья должна иметь достаточное количество ссылок на литературные источники.

Цитирование не может объективно отражать качество отдельной взятой статьи, так как сам акт цитирования «...является функцией многих переменных, помимо Научного влияния» [23]. Мы уверены, что большинство ученых это понимают, более того, многие администраторы науки тоже. Но пока подходы к оценке научной деятельности носят формальный характер, усилия направлены на увеличение количественного показателя, а сотрудники, разрабатывающие важные, но не «модные» сегодня направления будут проигрывать на этапе первых 1-5 лет, оказываясь обойденными цитированием, и как следствие – финансированием.

## СПИСОК ЛИТЕРАТУРЫ

1. Шарабчиев Ю.Т. Использование наукометрических методов для мониторинга продуктивности научной деятельности // *Международные обзоры: клиническая практика и здоровье*. – 2013. – № 4(4). – С. 118-133.
2. Smith L.C. Citation Analysis // *Library Trends*. – 1981. – № 30(1). – P. 83-110.
3. Bornmann L., Daniel H. What do citation counts measure? A review of studies on citing behavior" // *Journal of Documentation*. – 2008. – Vol. 64, Iss. 1. – P. 45-80. DOI: 10.1108/00220410810844150.
4. Soper M.E. Characteristics and use of personal collections // *Library Quarterly*. – 1976. – Vol. 46. – P. 397-415.
5. Daud Ali, Amjad Tehmina, Siddiqui Muazam Ahmed, et al. Correlational analysis of topic specificity and citations count of publication venue // *Library hi Tech*. – 2019. – Vol. 37, Iss. 1. – P. 8-18.
6. Кара-Мурза С.Г. Цитирование в науке и подходы к оценке научного вклада // *Вестн. АН СССР*. – 1984. – № 5. – С. 68-75
7. Cole S. The growth of scientific knowledge: Theories of deviance as a case study // *The idea of social structure*. – Routledge, 2017. – P. 175-220.
8. Beaver D.B. Does collaborative research have greater epistemic authority? // *Scientometrics*. – 2004. – № 60. – P. 399-408.
9. Soper M.E. Characteristics and use of personal collections // *The Library Quarterly*. – 1976. – Vol. 46, № 4. – P. 397-415.
10. Baldi S. Normative versus social constructivist processes in the allocation of citations: A network-analytic model // *American Sociological Review*. – 1998. – Vol. 63, Iss. 6 P. 829-846.
11. Stewart J. A. Achievement and ascriptive processes in the recognition of scientific articles // *Social Forces*. – 1983. – Vol. 62, № 1. – P. 166-189.
12. Ayres I., Vars F.E. Determinants of citations to articles in elite law reviews // *The Journal of Legal Studies*. – 2000. – Vol. 29, №. S1. – P. 427-450.
13. Laband D.N., Piette M.J. Favoritism versus search for good papers: Empirical evidence regarding

- the behavior of journal editors // Journal of Political Economy. – 1994. – Vol. 102, № 1. – P. 194-203.
14. Smart S., Waldfogel J. A citation-based test for discrimination at economics and finance journals // National Bureau of Economic Research. – 1996. – № w5460.
  15. Mählck P., Persson O. Socio-bibliometric mapping of intra-departmental networks // Scientometrics. – 2000. – Vol. 49, № 1. – P. 81-91.
  16. White H.D. Authors as citers over time // Journal of the American Society for Information Science and Technology. – 2001. – Vol. 52, № 2. – P. 87-108.
  17. Бескаравайная Е.В., Харыбина Т.Н. Консолидация ученых: вклад сотрудников, работающих за рубежом, в тематику Научных школ Института Белка РАН. // Информационные Ресурсы России. – 2014.– № 5.– С. 27-32.
  18. Бескаравайная Е.В., Харыбина Т.Н. Динамика библиометрических показателей сотрудников научных Школ института Белка РАН // Сб. науч. трудов / ред. Н.Е. Каленов, В.А. Цветкова. – М.: БЕН РАН, 2015. – С. 63–73
  19. Бескаравайная Е.В., Харыбина Т.Н. Создание модели мониторинга научных исследований // Научно-техническая информация. Сер. 1. – 2019. – № 5. – С. 19-28; Beskaravainaya E.V., Kharybina T.N. Creating a Model for Scientific Research Monitoring // Scientific and Technical Information Processing. – 2019. – Vol. 46, № 2. – P. 100-109.
  20. Simkin M.V., Roychowdhury V.P. A mathematical theory of citing, 2007, arXiv:physics/0504094v3. – URL: <https://arxiv.org/ftp/physics/papers/0504/0504094.pdf>
  21. Van Raan A.F.J. Sleeping beauties in science // Scientometrics. – 2004. – Vol. 59, № 3. – P. 467-472.
  22. Мохначева Ю.В. Цитируемость научных публикаций: особенности и закономерности // Научные и технические библиотеки. – 2017. – № 6. – С. 3-24. DOI:10.33186/1027-3689-2017-6-3-24
  23. Garfield E. Citation analysis as a tool in journal evaluation // Science. – 1972. – Vol. 178, № 4060. – P. 471-479.

*Материал поступил в редакцию 17.02.20.*

#### **Сведения об авторах**

**БЕСКАРАВАЙНАЯ Елена Вячеславовна** – Старший научный сотрудник, Библиотека по Естественным Наукам РАН  
e-mail: elenabesk@gmail.com

**ХАРЫБИНА Татьяна Николаевна** – заслуженный работник культуры РФ, Старший научный сотрудник, Библиотека по естественным наукам РАН  
e-mail: natsl@vega.protres.ru

**ВНИМАНИЮ ЧИТАТЕЛЕЙ!**  
**УНИВЕРСАЛЬНАЯ ДЕСЯТИЧНАЯ КЛАССИФИКАЦИЯ**  
**(УДК)**

**НОВОЕ ИЗДАНИЕ**  
**УДК. ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ.**

**Выпуск 7**

***Содержание выпуска:***

В настоящем электронном издании помещены **изменения и дополнения**, опубликованные Консорциумом УДК в выпусках 32 и 33 «Extensions and corrections to the UDC»:

**ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ К ТАБЛИЦАМ ОБЩИХ ОПРЕДЕЛИТЕЛЕЙ**

- Опубликовано изменения к **Таблице IG. Общие определители времени**

**ИЗМЕНЕНИЯ И ДОПОЛНЕНИЯ К ОСНОВНЫМ ТАБЛИЦАМ УДК**

Опубликованы изменения к классам:

- **2 Религия. Богословие**
- **33 Экономика. Народное хозяйство. Экономические науки**
- **582 Систематика растений**
- **551.7 Историческая геология.**

Для удобства пользователей издание открывает **Общая методика применения** Универсальной десятичной классификации.

**Для подписки необходимо направить заявку по адресу:**  
*125190, Россия, Москва, ул. Усиевича, 20, ВИНТИ РАН*  
**Телефоны:** 499-155-42-52, 499-155-42-85, 499-151-78-61  
**E-mail:** typo@viniti.ru, feo@viniti.ru  
**<http://www.udcc.ru>**

***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, ВИНТИ РАН*

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

**E-mail:** feo@viniti.ru

<http://www.udcc.ru>

## ***ВНИМАНИЮ ЧИТАТЕЛЕЙ!***

ВИНИТИ РАН, как единственный в России владелец лицензии Консорциума УДК, предлагает издания УДК полного четвертого издания на русском языке в печатном и электронном виде:

### ***1. Таблицы УДК***

**УДК. Том I** Общая методика применения УДК. Вспомогательные таблицы. Основные таблицы. Общий отдел. Алфавитно-предметный указатель к Общему отделу

**УДК. Том II** 1/3 Философия. Психология. Религия. Богословие. Общественные науки (только электронное издание)

**УДК. Том III** 5/54 Математика. Естественные науки (только электронное издание)

**УДК. Том IV** 55/59 Геологические и биологические науки (только электронное издание)

**УДК. Том V** 6/61 Медицинские науки (только электронное издание)

**УДК. Том VI (часть 1) 6/621** Прикладные науки. Технология. Инженерное дело (только электронное издание)

**УДК. Том VI (часть 2) 622/629** Техника. Инженерное дело (только электронное издание)

**УДК. Алфавитно-предметный указатель к т. VI (1 и 2 части)** (только электронное издание)

**УДК. Том VII** 63/65 Сельское хозяйство. Домоводство. Управление предприятием (только электронное издание)

**УДК. Том VIII** 66 Химическая технология. Химическая промышленность. Пищевая промышленность. Металлургия. Родственные отрасли (только электронное издание)

**УДК. Том IX** 67/69 Различные отрасли промышленности и ремесел. Строительство (только электронное издание)

**УДК. Том X** 7/9 Искусство. Спорт. Филология. География. История.

**УДК. АПУ (с в о д н ы й) к полному 4-му изданию**

**УДК. Изменения и дополнения. Выпуск 2** (к т.т. 1–3) (только электронное издание)

**УДК. Изменения и дополнения. Выпуск 3** (к т.т. 1–6) (только электронное издание)

**УДК. Изменения и дополнения. Выпуск 4** (к т.т. 1–7) (только электронное издание)

**УДК. Изменения и дополнения. Выпуск 5** (к т.т. 1–10)

**УДК. Изменения и дополнения. Выпуск 6** (к т.т. 1–10)

**УДК. Изменения и дополнения. Выпуск 7** (к т.т. 1–10), 2017 г. (только электронное издание)

**Для подписки необходимо направить заявку по адресу:**

**125190, Россия, Москва, ул. Усиевича, 20, ВИНТИ РАН**

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

**E-mail:** feo@viniti.ru