ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

12. 2022 (СЕНТЯБРЬ)

Издание включено в перечень ВАК (специальности: 2.3.2, 2.3.6, 2.3.8, 5.2.4)

ВЕСТНИК

СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

№12
СЕНТЯБРЬ 2022

www.c3da.org

ISSN 2686-9373

Издатели: *Российский государственный социальный университет*
Ассоциация РКЦФА

Адрес редакции и издателя: 129226, Москва,
ул. Вильгельма Пика, д.4, стр.1
E-mail: accda@c3da.org, info@c3da.org
www.c3da.org

Подписано в печать 30.09.2022 г.
Тираж 500 экз.
Подписной индекс в каталоге «Пресса России»: 79111

Свидетельство о регистрации СМИ
ПИ № ФС 77-76187 от 08.07.2019 г.

Журнал включен в перечень рецензируемых научных изданий ВАК, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук.
(2.3.2) Вычислительные системы и их элементы
(2.3.6) Методы и системы защиты информации, информационная безопасность
(2.3.8) Информатика и информационные процессы
(5.2.4) Финансы

РЕДАКЦИОННЫЙ СОВЕТ

СОДЕРЖАНИЕ

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Двенадцатый выпуск нашего журнала выходит на фоне замечательного события – включения «Вестника современных цифровых технологий» под номером 667 в перечень рецензируемых научных изданий ВАК, в которых должны быть опубликованы основные результаты диссертаций на соискание ученой степени кандидата наук и на соискание ученой степени доктора наук по специальностям в сфере информационных технологий (2.3.2) Вычислительные системы и их элементы, (2.3.6) Методы и системы защиты информации, информационная безопасность и (2.3.8) Информатика и информационные процессы, а также в области экономики по специальности (5.2.4) Финансы.

Включение в перечень ВАК – признание и высокая оценка качества журнала, научной емкости статей и авторитета ученых, входящих в состав Редакционного совета с момента его создания как научно-практического издания. Это итог большой работы главного редактора, ученого секретаря, редакции и всех членов Редакционного совета, которым мы выражаем глубокую благодарность.

Мы поздравляем наших уважаемых членов Редакционного совета, авторов и читателей с этим значительным событием и надеемся на новые успехи и свершения в нашем новом качестве.

К выходу в свет двенадцатого выпуска мы с большой радостью отмечаем новый этап сотрудничества с организациями науки и образования, связанный с включением в редакционный совет в качестве сопредседеталя Джомарта Фазыловича Алиева, видного российского деятеля науки и образования, доктора философии в области бизнес-права (PhD), кандидата экономических наук, доктора делового администрирования в области финансов (DBA), первого проректора Российского государственного социального университета (РГСУ).

Также очень позитивно отмечаем и то, что в рамках активного сотрудничества РГСУ стал соиздателем нашего журнала.

Новый выпуск Вестника включает раздел, посвященный крайне актуальным для современного общества вопросам определения роли, целей и задач, стоящих перед российским высшим образованием в эпоху цифровой трансформации. В статье **«Развитие прорывных технологий в социальной сфере как сверхзадача Российского государственного социального университета»** декан факультета политических и социальных технологий Светлана Бородулина и руководитель Научно-образовательного центра социальной аналитики РГСУ Елена Малькова рассказали о структуре нового факультета и его задачах, а также об интересном проекте «Сетка социальной безопасности».

В разделе «Фундаментальные проблемы цифровых технологий» опубликован концептуальный материал Андрея Щербакова **«О новом методе обеспечения безопасности семантических вычислений»**. В статье предлагается принципиально новый способ раздельного обмена ключами и информацией между абонентами, заинтересованными в совместной обработке нераскрываемой информации. Взамен методов гомоморфного шифрования предлагается новая концепция применения для данных целей симметричных криптоалгоритмов.

Раздел «Цифровые технологии в образовании» предлагает нашему вниманию статью коллектива авторов **«Актуальные подходы к квалиметрии и наукометрии»**. В статье рассматриваются проблемы современной квалиметрии и наукометрии и пути их решения при помощи современных отечественных технологий. В качестве комплексного решения предлагается создать наукометрическую платформу с применением семантически-естественной шкалы анализа научных текстов на основе технологий распределенных реестров. Представлены рамки минимальной жизнеспособности платформы, предложен предварительный концептуальный дизайн платформы, включая основные подсистемы и информационные процессы на базе платформы.

Поскольку в современных реалиях все более актуальными становятся проблемы искусственного интеллекта, в этом номере вводится раздел «Вопросы методологии и технологий искусственного интеллекта». В интересной и отчасти полемической статье Джомарта Фазыловича Алиева **«Логические и методологические аспекты проблематики искусственного интеллекта»** рассматриваются

актуальные тенденции, проблемы и перспективы развития области искусственного интеллекта (ИИ), описывается зависимость сценария развития ИИ от применения бинарной и тринарной логики в вычислительной технике. По мнению автора, вычислительной техники на основе бинарной логики, а также существующих заделов в области информационных технологий недостаточно для создания искусственного интеллекта и необходимо совершенствование стратегии научно-образовательной деятельности в области ИИ.

Тему искусственного интеллекта продолжает статья Сергея Запечникова **«Об актуальной научно-исследовательской повестке в сфере искусственного интеллекта»**. В ней выделяется и анализируется ряд проблем и тенденций, определяющих развитие методов и моделей искусственного интеллекта в современных условиях. Рассматриваются актуальные общеметодологические и прикладные проблемы ИИ, анализируется позитивный эффект от использования ИИ как инструментария научных исследований, в том числе фундаментальных. Автор приводит обзор методов и средств ИИ для решения сложноструктурированных задач и обработки сложноструктурированных данных. Показано, что наиболее актуальными являются проблемы обеспечения доверия к ИИ и его информационной безопасности.

Раздел завершает интересная статья наших уважаемых коллег-математиков из Северо-Кавказского федерального университета **«Применение системы остаточных классов для повышения эффективности операции умножения с накоплением»**. Операция умножения с накоплением является одной из основных для цифровой обработки сигналов и искусственных нейронных сетей. В статье рассмотрена аппаратная реализация этой операции для позиционной системы счисления и предложено её использование для увеличения скорости вычислений системы остаточных классов.

Развитие прорывных технологий в социальной сфере как сверхзадача Российского государственного социального университета

С.А. Бородулина
Декан Факультета политических и социальных технологий РГСУ
Е.В. Малькова
Руководитель Научно-образовательного центра социальной аналитики РГСУ

В 2022 г. в Российском государственном социальном университете был создан Факультет политических и социальных технологий, который начинает подготовку специалистов в области применения новейших технологий в социальной сфере для решения актуальных проблем, касающихся социальных сетей, цифровой гигиены, социальных аспектов применения искусственного интеллекта, социально-политических процессов. В настоящее время организовано привлечение на факультет и его кафедры ведущих российских специалистов по данным направлениям.

На факультете образовано шесть базовых кафедр, которые обеспечивают полный охват перспективных направлений для отклика на актуальный социальный запрос:

- Кафедра общественно-социальных институтов и социальной работы;
- Кафедра когнитивно-аналитических и нейро-прикладных технологий;
- Кафедра информационных технологий, искусственного интеллекта и общественно-социальных технологий цифрового общества;
- Кафедра социально-политических институтов, процессов и технологий;
- Кафедра квалиметрии, коммуникационного менеджмента и управления отношениями;
- Кафедра методов и технологий современной пропаганды и контрпропаганды.

В дополнение к структуре кафедр для решения практических задач в области технического, публикационного, нормативно-методического обеспечения и организации процессов разработки программных и программно-аппаратных средств внедрения социальных технологий создан Научно-образовательный центр социальной аналитики (НОЦ СА).

В ближайшее время силами кафедр и Центра планируется как разработка и внесение на утверждение новых образовательных программ, так и проведение фундаментальных и прикладных научно-исследовательских работ, ориентированных на создание систем и технологий социального сектора, опирающихся на отечественные программные и аппаратные средства и алгоритмы обеспечения информационной безопасности. В области информационных технологий для социальной сферы предполагается создание свободного от заимствований и надежного программного кода, а также в рамках когнитивно-аналитических технологий – процедур мышления, оценки и суждений, основанных на традиционных национальных философских и нравственных ценностях.

В процессе разработки когнитивно-аналитических технологий для политической и социальной сферы особое внимание будет уделяться созданию результативных, определенных, прозрачных и понятных алгоритмов, в отличие от систем непрогнозируемых и непрозрачных решений, как правило, характерных для направления развития искусственного интеллекта, включающего нейросетевые технологии.

С каждым годом объем генерируемой человеком информации увеличивается, поэтому весьма рискованно не учитывать значимость новейших цифровых технологий в социальной сфере. В организации учебного процесса будет применен принципиально новый подход к ознакомлению студентов с практической стороной реализации их профессиональных навыков в трудовой деятельности, моделирование в рамках НОЦ СА различных ситуационных взаимодействий будущих специалистов и различных социальных групп.

Одним из наиболее перспективных проек-

тов Факультета может быть проект под названием «Сетка социальной безопасности», направленный на предотвращение отката в нижний слой нижнего класса («социальное дно») любой значимой группы населения.

В связи с формированием «сетки социальной безопасности» необходимо решить целый комплекс научно-практических задач. Может быть представлена следующая последовательность выполнения задач:

а) на начальном этапе производится выявление тех групп населения, которые уже находятся или скоро будут находиться в зоне риска;

б) далее по каждой из этих групп выделяются проблемные точки (доходы, занятость, доступ к социальной инфраструктуре);

в) на основе полученных в рамках задач а) и б) результатов проводится сводный анализ и мэппинг существующих и потенциальных социальных рисков в целом по России и по отдельным региональным кластерам;

г) обеспечивается персонификация социальной помощи (категориальный подход дополняется индивидуальным): каждая семья, попавшая в зону социального риска, подключается (с ее согласия) к системе непрерывного мониторинга ее материального и социального положения (доходы, занятость, состояние здоровья);

д) разрабатывается система минимально допустимых значений социальных параметров, которые позволяют разным категориям семей не только поддерживать обеспечение базовых потребностей, но и иметь ресурсы для развития;

е) на основе социальных параметров (при участии муниципальных органов управления, некоммерческих организаций и частных компаний) формируется пакет предложений для попавшей в зону социального риска семьи с целью минимизации риска и предоставления возможностей для социального развития;

ж) формируется система общественно-государственного контроля для наблюдения за выработанными в рамках «сетки социальной безопасности» процедурами и мониторинга результатов реализации этого проекта;

з) производится необходимая корректировка бюджетной политики с учетом финансирования проекта «Сетка социальной безопасности» как приоритетного направления социальной политики. При этом некоммерческие организации и частные компании, которые несут расходы на эти цели, частично или полностью освобождаются от налогообложения.

Необходимо заметить, что структурная трансформация экономики на практике нередко приводит к окончательному закрытию производств во многих отраслях. Это может вызвать локальные (в регионах, городах) крайне негативные социальные тенденции, к которым относятся в т.ч. массовая скрытая или открытая безработица, всплеск бедности, разрушение социальной инфраструктуры и т.п., с точки зрения безопасности страны способные в своей совокупности привести к критически высокой скорости роста неблагополучия и криминализации общества.

Возможные негативные последствия трансформации экономики для социального развития и благополучия обуславливают необходимость проведения новой социальной политики и принятия особых мер, адекватных актуальным вызовам, которые стоят перед нашей Родиной.

Научно-образовательная деятельность нового Факультета политических и социальных технологий РГСУ направлена на подготовку специалистов высокой квалификации, востребованных в области решения широкого спектра указанных социальных проблем при помощи отечественных надежных инструментов и технологий в рамках комплекса мер, направленных на благополучие всех категорий населения и развитие возможностей социально-экономического роста.

Раскрытие научно-образовательного потенциала РГСУ в области социальных и политических технологий, безусловно, будет способствовать как созданию новых эффективных, в том числе когнитивно-аналитических, технологий, так и повышению эффективности подготовки квалифицированных кадров с позиции навыков применения обширного инструментария, соответствующего сложности актуальных социальных проблем.

УДК: 004.8

О новом методе обеспечения безопасности семантических вычислений

A.Yu. Shcherbakov

On a New Method for Securing Sematic Computations

Abstract. *In this article a new method for the separate exchange of keys and information between subscribers interested in the joint processing of undisclosed information is proposed, which includes set-theoretic operations on encrypted data. A new concept of using symmetric cryptographic algorithms for these purposes is considered.*

Keywords: *homomorphic encryption, set-theoretic comparison, intruder, separate key management.*

А.Ю. Щербаков
Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий РГСУ, ведущий научный сотрудник Государственного университета управления, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева).
E-mail: x509@ras.ru

Аннотация. *В статье предлагается новый способ раздельного обмена ключами и информацией между абонентами, заинтересованными в совместной обработке нераскрываемой информации, включая теоретико-множественные операции над зашифрованными данными. Рассматривается новая концепция применения для данных целей симметричных криптографических алгоритмов.*

Ключевые слова: *гомоморфное шифрование, теоретико-множественное сравнение, нарушитель, раздельное управление ключами.*

ВВЕДЕНИЕ. МОДЕЛЬ СЕМАНТИЧЕСКОЙ ОБРАБОТКИ ИНФОРМАЦИИ

В современной научной литературе в качестве конструктивной модели семантической обработки информации утвердилась модель, предполагающая первичное рассмотрение некоторых текстов, понимаемых как последовательности слов [1].

Для решения различных задач обработки текстов и их оптимизации используется процедура индексации – небиективное (неоднозначное) преобразование, заменяющее каждое слово текста двоичным вектором фиксированной длины.

В качестве примера индексации рассмотрим процедуру, в которой слова длины меньшей, чем MAX_WORD, заменяются вектором длины 8 байт. При этом преобразуемое слово устанавливается в качестве ключа в криптографическом алгоритме ГОСТ 28147-89 и происходит одна итерация этого алгоритма [2], при этом исходным вектором является фиксированный вектор, получаемый по процедуре for(i=0; i<8; i++) x[i]=0x88^(char)i.

```
#define MAX_WORD 512
int xb(char *wd, unsigned char *x)
 {
int i, j, len, part, ost;
unsigned char wd1[32];

len=strlen(wd);
if(len>MAX_WORD) return(-1);
part=len/32;
ost =len%32;
for(i=0;i<32 ;i++) wd1[i]=0;
for(i=0;i<ost;i++) wd1[i]=wd[i];

for(i=0;i<part;i++)
  for(j=0;j<32;j++) wd1[j]=wd1[j]^wd[i*32+j];

for(i=0; i<8; i++) x[i]=0x88^(char)i;
 imit_fast((unsigned long *)x,(unsigned long *)
wd1);
return(0);
 }
```

В данной статье не рассматриваются свойства описанного небиективного преобразования. Отметим только, что в приведенном примере совпадение индексов x для различных слов зависит от числа байт, которые выбираются для формирования индекса из восьми байт массива x. Это связано с тем, что рассматриваемый алгоритм в большой степени статистически совпадает со случайным отображением. На-

пример, если выбрать 4 байта, то вероятность совпадения векторов x для различных слов (вероятность коллизий) составит порядка 2^{-32}.

Таким образом, предлагается заменить тексты со словами различной длины массивами индексов одинаковой длины (практически длинными числами) и рассматривать различные операции уже с индексированными текстами.

СРАВНЕНИЕ ТЕКСТОВ

В самом простом случае рассмотрим два текста: T и R. Задача ставится следующим образом: необходимо конструктивно и вычислительно нетрудоёмко сравнить тем или иным образом эти тексты. Например, теоретико-множественное сравнение выполняется по «облаку» слов, входящих в эти тексты.

Используя диаграммы Эйлера для условно пересекающихся множеств, рассмотрим три множества: 1 – множество слов, входящих только в текст T, 2 – множество слов, входящих только в текст R и 3 – пересечение текстов T и R. Заметим, что множество 3 может быть и пустым. Объединение множеств 1, 2 и 3 совпадает с объединением текстов T и R, понимаемых как множества слов (упорядоченные или неупорядоченные).

Принимая априорно, что чем больше мощность множества 3, тем более возможно говорить о том, что тексты «сходны» между собой, конструктивно для оценки сходства текстов ввести следующие меры [3].

Обозначим m(i) – мощность множества i.

“Нулевая” мера (исторически введенная первой)

M0= 2m(3)/((m(1)+m(2))

«Верхняя» мера

M=0.5(m(3)/m(1)+m(3)/m(2))

«Нижняя” мера

M=m(3)/(m(1)+m(2)+m(3))

Несмотря на простоту, эта конструкция достаточно универсально работает для решения различных семантических задач.

Задавая в качестве R некоторые эталонные тексты и оценивая значения введенных мер на множествах 1-3, возможно решать задачи не только простого, но и расширенного поиска (по длинному нечеткому произвольному словесному описанию), определения принадлежности текста к некоторой тематике, делать выводы об авторстве текста, а также оценивать по множеству 1 (возможно, даже по его мощности в первом приближении) оригинальность текста и его новизну.

ЗАКРЫТЫЕ ВЫЧИСЛЕНИЯ НА ТЕКСТАХ

В настоящее время весьма актуальной является задача закрытых вычислений, когда зашифрованные данные обрабатывается неким методом без их расшифрования. В этом смысле уместно привести пример с системой электронного голосования, когда подаваемый в закрытом (зашифрованном) виде голос суммируется без его раскрытия с другими голосами, также без их раскрытия (расшифрования), для получения итогов голосования. В этом случае весьма уместно использовать различные методы гомоморфного шифрования [4].

Согласно этому источнику под гомоморфным шифрованием понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций (op) над открытыми текстами.

Пусть *E(k,m)* — функция шифрования, где *m* — открытый текст, *k* — ключ шифрования. Заметим, что для данных фиксированных *k* и *m* криптограмма (зашифрованный текст) *E(k,m)* может быть, вообще говоря, случайной величиной. В таких случаях говорят о вероятностном шифровании. Функция *E* гомоморфна относительно операции op над открытыми текстами, если существует эффективный алгоритм *M*, который, получив на вход любую пару криптограмм вида *E(k,m1)*, *E(k,m2)*, выдает такую криптограмму *c*, что при расшифровании *c* будет получен открытый текст *m1opm2*.

Как правило, рассматривается следующий важнейший частный случай гомоморфного шифрования. Для данной функции шифрования *E* и операции *op1* над открытыми текстами существует операция *op2* над криптограммами такая, что из криптограммы *E(k,m1)op2E(k,m2)* при расшифровании извлекается открытый

текст *m1op1m2*.

В случае сравнения текстов методы вычисления «под шифром» не подходят, поскольку необходимо производить теоретико-множественное сравнение.

ТЕОРЕТИКО-МНОЖЕСТВЕННОЕ СРАВНЕНИЕ ЗАКРЫТЫХ ДАННЫХ

Рассмотрим формальную постановку задачи, связанную с работой по сравнению текстов и расширенному поиску. Под расширенным поиском как раз будем понимать поиск по максимальной величине одной из мер ранее введенного сходства текстов – поискового запроса и массива информации, в которой ведется поиск.

Введем владельца информации (целевых данных) V достаточно большого объема и текстового вида. Это могут быть списки покупок (от торговой сети), списки клиентов, перечень медицинских симптомов и показаний и т.д. Важно, что в любом случае у владельца есть персональные данные, нуждающиеся в защите по закону, либо конфиденциальная информация. Пусть также есть потенциальный потребитель (интересант) I, который нуждается в некоторой выборке этих данных. Потребитель I также может рассматриваться в качестве нарушителя (может проявить интерес к раскрытию или переносу в свои хранилища данных владельца V).

Рассмотрим также посредника P (владельца вычислительных ресурсов), принимающего поисковый запрос от I и обрабатывающий данные от владельца V. В нашей модели он также является потенциальным нарушителем, поскольку может проявить интерес как к содержанию запроса I, так и информации, которой владеет V. Посредник не имеет ключа K и не имеет доступа к индексам.

Напомним также, что в классической криптографии для установления связи между абонентами необходимо обменяться ключами (или иметь одинаковые или ассиметричные ключи для шифрования и расшифрования информации), а также обменяться зашифрованной на этих ключах информацией.

Предлагается «разорвать» эту парадигму отдельно на обмен ключами и обмен информацией. Очевидно, что обменявшись ключами, но не обменявшись никакой информацией, стороны не могут нарушить конфиденциальность друг друга.

Соответственно, предлагается проиндексировать текстовые массивы владельца V и получить вместо слов или текстовых данных массив B индексов. Аналогично, поисковый запрос X от I также индексируется в Y. После этого стороны зашифровывают каждый индекс на общем для I и V ключе K.

Сформулируем важное утверждение.

При реализации шифрующего преобразования y=E(k, x) мощности множеств 1, 2 и 3 (введенные выше), используемые для сравнения текстов B и Y, будут совпадать с соответствующими мощностями множеств 1, 2 и 3 для E(K, B) и E(K, Y).

Верность этого утверждения следует из однозначности алгоритма шифрования при фиксации каждого ключа K.

Тогда зашифрованные владельцем информации и интересантом индексы от массива, по которому ведется поиск и поискового запроса могут быть направлены посреднику, где над ними будет произведено сравнение в теоретико-множественном смысле и результат сходства может быть сообщен одной или обеим сторонам.

Поскольку каждый индекс шифруется отдельно, то посредник, рассматриваемый в качестве нарушителя, может статистически анализировать шифр простой замены, заданный на отдельных словах (полагаем, что язык текстов ему известен).

При этом очевидно, что поисковый запрос имеет не очень большую длину и такая атака неконструктивна. Опасение представляет массив B владельца, который может быть достаточно большим.

ЗАКЛЮЧЕНИЕ

Предложенный алгоритм раздельного обмена ключами и информацией, а также теоретико-множественные операции над зашифрованными данными позволяют решить задачу обработки текстов без нарушения их конфиденциальности.

СПИСОК ЛИТЕРАТУРЫ

1. Рязанова А.А., Анисимова А.Э. О методике сравнительного квалификационного анализа требований к профессиональным навыкам с целью коррекции национальных образовательных программ // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационный процессы и системы, 2019. № 2. С. 29-35.

2. ГОСТ Р 34.12 – 2015. Информационная технология. Криптографическая защита информации. Блочные шифры. Национальный стандарт РФ: утвержден и введен в действие Приказом Федерального агенства по техническому регулированию и метрологии от 19 июня 2015 г. № 749-ст.: введен впервые: дата введения 01.01.2016. – Москва: Стандартинформ, 2018.- 25 с.

3. Рязанова А.А., Щербаков А.Ю. К вопросу о метриках сходства текстов для методов их автоматизированного сравнения // Приоритетные задачи и стратегии развития технических наук. Выпуск II. Сборник научных трудов по итогам международной научно-практической конференции (25 мая 2017 г.), г. Тольятти. С. 66-69.

4. Варновский Н.П., Шокуров А.В. Гомоморфное шифрование // Сборник трудов ИСП РАН №12. Т.27. 2007. С. 27-35.

УДК: 004.8, 001.38

Актуальные подходы к квалиметрии и наукометрии

D.F. Aliev, A.Yu. Shcherbakov, S.A. Borodulina

Current Approaches to Qualimetry and Scientometrics

Abstract. *The article deals with the problems of modern qualimetry and scientometrics and ways to solve them with the help of modern homegrown technologies. As an integrated solution, it is proposed to create a scientometric platform using a semantically natural scale for the analysis of scientific texts based on distributed registry technologies. Methodology for assessing the professional qualities and achievements of platform participants, which is potentially effective in the scientometrical activity is given. The framework of the minimum viability of the platform is given, a preliminary conceptual design of the platform is proposed, including the main subsystems and information processes based on the platform.*

Keywords: *scientometrics, qualimetry, scientometric platform, self-regulating community, dynamic rank.*

Д.Ф.Алиев[1]
А.Ю.Щербаков[2]
С.А.Бородулина[3]

[1]Доктор философии в области бизнес-права (PhD), доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет».
E-mail: kharchenkoDD@rgsu.net

[2]Доктор технических наук, профессор кафедры комплексной безопасности критически важных объектов РГУ нефти и газа (НИУ) имени И.М. Губкина, заведующий кафедрой когнитивно-аналитических и нейро-прикладных технологий РГСУ, ведущий научный сотрудник Государственного университета управления, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева).
E-mail: x509@ras.ru

[3]Декан факультета политических и социальных технологий РГСУ, первый вице-президент Ассоциации специалистов в области криптовалют и цифровых финансовых активов
E-mail:BorodulinaSA@rgsu.net

Аннотация. *В статье рассматриваются проблемы современной квалиметрии и наукометрии и пути их решения при помощи современных отечественных технологий. В качестве комплексного решения предлагается создать наукометрическую платформу с применением семантически-естественной шкалы анализа научных текстов на основе технологий распределенных реестров. Приводится потенциально эффективная в рамках наукометрической практики методика оценки профессиональных качеств и достижений участников платформы. Представлены рамки минимальной жизнеспособности платформы, предложен предварительный концептуальный дизайн платформы, включая основные подсистемы и информационные процессы на базе платформы.*

Ключевые слова: *наукометрия, квалиметрия, наукометрическая платформа, саморегулируемое сообщество, динамический ранг.*

ВВЕДЕНИЕ

В последние полгода проблема отечественной наукометрии, полностью основанной на международных (англосаксонских) метриках с доминированием триумвирата «Scopus/WoS/Hirsch», прочно закрепилась в дискуссионном поле. С явными признаками «культуры отмены» западные научные сообщества фактически исключили российскую науку из своих наукометрических баз, положив предел нашей от них зависимости.

Проблема количественного оценивания научных качеств всегда стояла в повестке дня, а с ростом тренда на научную глобализацию и развитием технологических возможностей обмена научными знаниями только усугубилась. На сегодняшний день она связана с фундаментальной сущностью наукометрии и субъект-субъектными отношениями и не имеет универсального решения, с высокой вероятностью не будет иметь его и в будущем.

Количество публикаций, к примеру, в верхнем квартиле Scopus отражает лишь количество научных публикаций, принятых редакторами по критериям, которые часто нам не известны. В отдельных случаях рецензентами западных журналов к некоторым нашим гуманитарным исследователям предъявлялись

требования (например, требование поместить в статью критику государственного строя), не имеющие никакого отношения к оценке научных качеств исследований.

Подобные требования приводят к незаинтересованности российских ученых в наукометрии, которая делает попытки свести их в конкуренции с западными учеными, выдвигающими гипотезы, часто очевидно не выдерживающие критики научного сообщества. При этом труды таких ученых не только публикуются в первой квартили и Scopus'a, и WoS'a, но и устанавливают правила и планки западной наукометрии.

Несмотря на явно выраженные проблемы наукометрии, направление мыслей исследователя, стремящегося к публикации своих работ, по-прежнему по прошествии 75 лет можно выразить как «publish or perish» («Публикуйся или погибни») (фраза американского генетика Кимбола Атвуда III). Научная деятельность исторически имеет, с одной стороны, очень сильную репутационную сторону, а с другой – отражает уровень тщеславия, часто в позитивной коннотации. В постиндустриальную эпоху к мотивациям ученого к исследователям добавился материальный интерес. В сочетании с интересами созидания и идеалами чистого познания получается непростой психологический профиль.

Психология специалиста редакции, принимающего или отклоняющего рукопись, имеет существенные отличия от психологии ученого. Как говорилось выше, мотивы и коллизии часто не связаны с научным содержанием работы, непрозрачны и непонятны. Но нас интересует прежде всего, насколько в действительности велика необходимость изучать проблему мотиваций принимающей рукописи стороны и в целом участвовать в иностранных наукометрических системах по установленным в них правилам.

Следует отметить, что отечественная наукометрия имеет, также как и западная, длинную историю, и достаточно долгое время до распада СССР отличалась высоким качеством. Однако на сегодняшний день, в свете происходящих в геополитической плоскости событий с одной стороны и очевидных тенденций, связанных с масштабной информатизацией,- с другой, невозможно не только участвовать в западной, но и вернуться к советской модели наукометрии. Это дает основание полагать, что единственно верной стратегией будет создание современной наукометрической системы в России, основанной на отечественных технологиях.

Наиболее актуальным вопросом, стоящим сегодня перед российской наукой, является вопрос существования потенциально эффективной модели управления научной деятельностью и исследованиями, от которой зависит и эффективность расходования бюджетных средств. В соответствии с общедоступными данными ОЭСР, финансирование НИОКР для России выросло с 30 млрд.$ до 48 млрд.$, или на 60%[1]. Для сравнения, в Японии рост составил менее 17%, а в Израиле – не достиг 20 млрд.$.

Объем затрат на науку в ВВП в России в 2019 г. составил 0,7%, в Японии - 0,5%; Израиле - 0,5%; Китае - 0,5%; Чехии - 0,7%; США - 0,7%, в отличие от Германии с 0,9% и Кореи с 1,1%. Таким образом, в целом отечественная наука получает хорошую поддержку от государства, в связи с чем наличие качественной предиктивной наукометрии и квалиметрии начинает приобретать особое значение.

Приведенные выше показатели касаются государственного финансирования. Совокупное государственное и частное финансирование меняет позиции государств не в пользу России. Общие расходы на НИОКР к ВВП в России равны приблизительно 1,04%., при этом в Японии они составляют около 3,2%, в Израиле - 5,1%, в Китае - 2,2%, в Чехии - 1,9%, в США - 3,2%, в Германии - 3,2%, а в Корее - 4,6%. В данном случае последняя группа показателей выявляет активность частных корпораций в отношении финансирования научных исследований, зависящую в т.ч. как от уровня научных результатов, так и от качества их представления, а также от объективности, точности и прозрачности квалиметрии в науке.

ОСНОВНЫЕ ТЕРМИНЫ

Напомним читателю основные термины, ре-

[1] Источник: официальный сайт Организации экономического сотрудничества и развития. URL: https://www.oecd.org/

левантные для настоящей работы.

Квалиметрия – это научная область, в рамках которой изучаются методология и проблематика комплексного количественного оценивания качества объектов любой природы (одушевленных или неодушевленных, предметов или процессов, продуктов труда или продуктов природы), имеющих материальный или духовный характер, искусственное или естественное происхождение [1].

Наукометрия (англ. scientometrics) — область науковедения, проводящая исследование науки количественными методами; научная дисциплина, изучающая эволюцию науки через многочисленные измерения и статистическую обработку научной информации (количество научных статей, опубликованных в данный период времени, цитируемость и т. д.). Термин «наукометрия» был впервые введён 1969г. В. В. Налимовым и З. М. Мульченко в монографии [2].

Научно-исследовательские и опытно-конструкторские работы (НИОКР) включают в себя творческую работу, проводимую на систематической основе с целью увеличения объема человеческих знаний и разработки новых технологий на их основе. Термин НИОКР охватывает следующие виды деятельности: научно-исследовательские, опытно-конструкторские и технологические работы.

ОБ ЭФФЕКТИВНОСТИ МЕТОДОВ ОЦЕНИВАНИЯ ПРОФЕССИОНАЛЬНЫХ КАЧЕСТВ И ЗАСЛУГ УЧЕНЫХ

Данные об основных видах финансирования, позволяют, как указано выше, предполагать, что от качества и объективности отечественной наукометрии зависит и размер финансирования научных исследований со стороны крупнейших российских корпораций, и их результативность. Поэтому очевидно, что управление наукой и научными исследованиями в современных реалиях необходимы, кроме того, представляется вполне обоснованной позиция некоторых государственных деятелей о необходимости воссоздать Государственный комитет по науке и технике СССР (ГКНТ).

Следует отметить, что для организации наукометрии необходимо определить круг целей, задач, объектов и субъектов наукометрии и в зависимости от них разработать систему эффективных инструментов. При этом в независимости от конечного получателя и дальнейшего использования наукометрических данных для конкретных целей (принятие решений о дальнейшем финансировании, присуждение наград, расстановка приоритетов в отдельной области науки), наукометрия должна давать объективную картину развития научного направления, его актуальности, потенциальных возможностей, законов формирования информационных потоков и распространения научных идей [2].

Стратегия Российского государственного социального университета (РГСУ) включает весомые аргументы в пользу глубокого анализа и практического применения лучших бизнес-практик для организации менеджмента научно-образовательного пространства. В соответствии с этим подходом рассмотрим ниже надежный и потенциально эффективный в рамках наукометрической практики метод оценки «360 градусов».

Термин «Метод оценки 360 градусов» был введен Уордом в 1987 году. Уорд определял данный метод как систематический сбор информации относительно результатов индивидуума или группы, получаемый от окружения [3]. Активно применять метод начали за рубежом в 1990-е гг., а в начале 2000-х гг. российские HR-специалисты стали перенимать этот опыт у западных коллег, и сейчас этот метод является популярным средством оценки персонала в России.

Суть метода «360 градусов» заключается в том, что оценку сотрудника проводит все его рабочее окружение: руководители, подчиненные, коллеги и клиенты. Результат оценки — рейтинг качеств сотрудника (оценивается мера соответствия занимаемой должности по списку определенных характеристик). Также благодаря блоку самооценки данный метод может быть использован в качестве источника обратной связи. Если к оценке присоединяются иные лица (потребители, клиенты, поставщики, партнеры), то «метод 360 градусов» трансформи-

руется в методику «540 градусов».

В специальные анкеты вносятся баллы по знаниям, навыкам и личностным качествам. Анкетирование может проводиться анонимно с указанием категории оценщика (коллега, руководитель, клиент) либо не анонимно. Затем определяется средний арифметический балл по каждому навыку, умению или личностному качеству и строится график.

На последнем этапе результаты оценки представляются оцениваемому сотруднику. На основе этих результатов могут быть сделаны выводы для саморазвития сотрудника, для развития конкретных навыков, умений, качеств, для улучшения отношений с коллегами, а также приняты решения об обучении, занесении в список кадрового резерва и др. Решения о повышении квалификации сотрудника, повышении/понижении в должности и другие кадровые решения на основании данных результатов не могут быть приняты, поскольку для этого применяется процедура аттестации.

Весьма конструктивно распространить такой подход к наукометрической базе научных персоналий. Однако его прикладное применение связано с рядом субъективных по своей природе сложностей, которые проявляются объективно и достаточно часто. Источником этих сложностей может быть в т.ч. феномен «fraud&plunder» (англ. «мошенничество и грабёж»).

Это явление, к сожалению, встречается в научной-исследовательской среде, оно упоминается как в зарубежной литературе («Эррозумит» Синклера Льюиса), так и в отечественной (повесть «Кафедра» И.Грековой), и тесно связано с проблемой плагиата, хотя понятие «fraud&plunder» является более широким и включает, в отличие от понятия «плагиат», денежный и карьерный интерес. В этом смысле научные работы, отчёты о НИР, отдельные содержащиеся в них идеи, а также в некоторых случаях тематики и/или названия становятся «фрод-активами», которые при использовании административного ресурса или других преимуществ становятся «пландер-активами».

Одним из эффективных способов решения описанной проблемы является достижение объективности в оценке научных исследований при помощи анонимизации участников наукометрической платформы в сочетании с механизмом случайного выбора рецензентов и авторов.

Рассмотрим механизм применения этих способов на основе платформы «Сешат».

ОСНОВНЫЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ НАУКОМЕТРИЧЕСКОЙ ПЛАТФОРМЫ «СЕШАТ»

Платформа «Сешат» (Семантически-естественная шкала анализа текстов (Трудов)) регистрирует всех желающих к ней присоединиться специалистов в качестве экспертов. Любой участник с ученой степенью сможет зарегистрироваться на платформе в индивидуальном порядке, а начинающий учёный - по представлению какого-либо корпоративного участника платформы (института, университета, издания, компании, проектного офиса и т.п.).

Очевидно, что регистрация экспертов будет проходить по научным профилям, по их уровням, по режимам доступа к информации, с правом выбора предметных областей, а также на основе простых, понятных и публичных норм и правил. После первичной регистрации все эксперты платформы получат свои уникальные ID, не изменяемые в дальнейшем.

При каждом приглашении эксперта к участию в процедуре оценивания он выбирается случайным образом. Для проведения оценки он получает одноразовый идентификатор, действие которого по завершении процедуры прекращается с фиксацией в системе бальных метрик.

Помимо общего механизма анонимизации экспертов, в системе также будет применяться редакционный инструмент анонимизации - в оцениваемых материалах будет отсутствовать информация об авторах и представляемых ими организациях. Этот инструмент, очевидно, не даст полной объективности в оценивании, но в сочетании с анонимностью экспертов и случайностью их выбора он рассматривается нами как обязательный третий способ достижения объективности.

Безусловно, в ходе практической работы по

созданию, документированию и развёртыванию платформы предстоит решить множество открытых вопросов- от структур секций/подсекций платформы и библиотек стандартных запросов/отчётов до ролей администрирования запросов и моделей финансирования/монетизации. Очень важны также вопросы доверия к анонимности платформы, реферирования оцениваемых материалов, их депонирования, фиксирования приоритетов, подготовки статистических материалов и аналитических обзоров.

Формула проекта «Сешат»: создание современной квалиметрической платформы наукометрического оценивания на принципах саморегулируемой организации с пилотным проетом в Российском государственном социальном университете и с потенциалом масштабирования и тиражирования в российском научном сообществе.

Базовая гипотеза «Сешат»: лучше самих учёных и исследователей никто не оценит качественные характеристики научных работ; надо лишь создать для такого оценивания надлежащие условия и возможности.

Ниже приведем исходные позиции для развития проекта «Сешат».

СТРУКТУРА СЕКЦИЙ ПЛАТФОРМЫ

На старте включаются 24 научные отрасли (правый столбец Приказа №118 Минобрнауки от 24.02.21). В дальнейшем эксперты платформы высокого ранга самостоятельно добавят структуре объёмность, установив список подсекций («Сешат» будет поддерживать функции голосования).

Возможные запросы оценивания на платформе:

1. адекватность реферата содержанию работы;
2. качество обзора литературы к работе (если есть);
3. научная новизна работы;
4. научное качество работы;
5. фундаментальность работы;
6. целостность работы;
7. завершённость работы;
8. прикладные аспекты работы;
9. конкурентность работы/программы/тематики;
10. перспективность программы/тематики;
11. наличие научного задела программы/тематики;
12. соответствие государственным программам.

Административные роли платформы. В подсекциях, секциях и на платформе в целом будут включены следующие роли – администраторы, модераторы, референты и лигалы. Их функции будут соответствовать сложившимся обычаям делового оборота (в детерминантах платформы), а статусы будут определяться уровнями платформы (специалисты- в подсекциях, старшие- в секциях, главные- на платформе в целом).

Динамический ранг экспертов платформы. Любой специалист, регистрируясь экспертом платформы, получает на входе от 1 до 10 баллов стартового ранга, в зависимости от его научных заслуг и статуса (правила будут разработаны и опубликованы). Для его получения эксперт должен просто заполнить анкету мастер-данных (с подтверждениями; возможно через ЕПГУ (Единый портал государственных услуг) и ряд других профессиональных порталов), сформировать запрос на выбранные для участия секции/подсекции, ознакомиться с правилами платформы и принять их. «Сешат» в разумные сроки обработает запрос (порядки и нормативы будут опубликованы) и вернёт участнику сертификат эксперта с ID и текущим рангом (либо мотивированный отказ).

Далее динамика ранга поддерживается автоматически: каждое оценивание может принести эксперту от «плюс 1» до «минус 1» балла к его рангу. Максимальный плюс эксперт получает в случае, если его оценка совпадает с медианой (величина среднеквадратичного отклонения во всех случаях- расчётная величина от предмета, характера и уровня оценивания; также будут опубликованы). Максимальный минус- если его оценка является выпадающей (выходит за доверительный интервал). Для калькуляции изменения ранга внутри границ интервала (от 0 до +1) используется простая дисперсия. Изменения ранга возвращаются эксперту по завершении каждого оценивания,

к которому он был приглашён платформой. В случае мультиоценки (множественный запрос) платформа проводит взвешивание и возвращает эксперту среднюю динамику ранга.

Саморегулирование сообщества на платформе. Экспертный ранг является не только метрикой для определения (установления) уровня оценивания. Ранг эксперта является метрикой его авторитета на платформе и открывающим маркером полномочий. Максимальное значение ранга на платформе составляет 100.

На старте (когда продукт протестирован в РГСУ и предлагается к широкому использованию научной общественностью) предлагаемая панель полномочий в сообществе приблизительно такова (далее она может быть переустановлена экспертами самостоятельно):

Ранг до 10. Участие в процедурах оценивания.

10+ до 20. Переписка с подсекцией «Сешат». Чаты подсекции.

20+ до 30. Переписка с секцией «Сешат». Чаты секции.

30+ до 40. Возможность сопровождать оценки краткими текстами.

40+ до 50. Переписка с платформой «Сешат». Чаты платформы.

50+ до 60. Предложение новаций 1-й категории. Форматы и процедуры.

60+ до 70. Предложение новаций 2-й категории. Функции голосования секции.

70+ до 80. Предложение новаций 3-й категории. Функции голосования платформы.

80+ до 90. Любые экспертные активности в секции «Сешат». Краудфандинг.

Ранг 90+. Любые экспертные активности на платформе «Сешат». Апелляция.

MVP (Minimum Viable Product, «минимально жизнеспособный продукт») платформы «Сешат» - это рамки её минимальной жизнеспособности, или минимальный набор функций, достаточный для ее презентации и проверки функционирования. Сегодня MVP ограничивается 18 элементами. Вероятность их коррекции на инвестиционной фазе проекта нами оценивается как низкая, но не нулевая. Очевидно, что продуктивная и, тем более, тиражная рамки платформы будут шире минимальных. Свод элементов MVP, как они видятся сегодня, представлен в таблице 1.

Техническое решение платформы. В качестве базовой технологии исполнения «Сешат» мы предлагаем блокчейн.

Главными недостатками блокчейна считаются потеря единого контроля, низкая скорость транзакций, дефицит специалистов, отсутствие стандартов, проблемы безопасности и сложные решения вопросов доверия. Названные недостатки не лишены оснований, но на них уже есть содержательные ответы и конкретные решения.

На практике блокчейн уже имеет достаточный портфель юзкейсов и в научной литературе хорошо освещена данная тема [4].

Несмотря на определенные тонкости применения технологий блокчейн, их применимость подтверждена эмпирическим опытом, и они уже стали реальностью, которую необходимо признать. Факты, свидетельствующие о недостатках блокчейна, являются проявлениями фазы роста технологии. IT-аналитики прогнозируют до 2026 года новую фазу инвестирования в блокчейн (технология есть, инфраструктуры нет), после чего начнётся фаза генерации добавленной стоимости.

Считаем важным затронуть вопрос о перспективном раскрытии предлагаемой функциональности платформы, в рамках которой будет качественно организована квалиметрия и создан задел для содержательной работы с научными материалами. Возможна интеграция на новой технологической основе с аналогом функционала ВИНИТИ, который уже 70 лет выделяет его среди всех родственных ему системных решений в реферировании научных знаний.

Синергетический эффект от такой интеграции может превысить даже самые высокие ожидания, в особенности, если проводить её в прямой корреспонденции с задачами новации нашей системы интеллектуального права, обеспечивая, к примеру, процедурную инициацию РИД-активностей по неисключительным безвозмездным лицензиям для госзаказов [5].

Задачи организации такой интеграции, очевидно, не входят в рамки предлагаемого к запуску проекта, однако при структурировании мастер-данных, выборе экспертов, организа-

ции поточности на платформе, формировании очередей/запросов, разработке системных тикетов и управлении смарт-контрактами их (задачи интеграции), безусловно, следует иметь в виду.

Таблица 1

Проект «Сешат»
Квалиметрия в наукометрии — рамки платформы

№	Наименование	MVP	Готовый продукт	Тираж
1	Ведение индивидуальных эккаунтов; тематики	да	да	да
2	Защита персональных данных; управление ими	да	да	да
3	Ввод исходных материалов; варианты загрузки	да	да	да
4	2-х серверный ИТ-ландшафт; «тонкий клиент»	да	да	да
5	ИТ-ландшафт с «песочницей»; приложение	—	да	да
6	Доверенная платформа; смарт-контрактинг	—	—	да
7	Динамика экспертного ранга; баллы; учёт	да	да	да
8	Типы квалиметрических процедур; библиотека	да	да	да
9	Поддержка режимов доступа; работа с тайнами	да	да	да
10	Ранжирование исследования; лупинг и выбор	—	да	да
11	Ордеры квалиметрии; уведомления; акцепты	да	да	да
12	Поддержка рецензий и суждений; деанон	да	да	да
13	Управление научными приоритетами; прувы	да	да	да
14	Анонимайзер экспертов-квалиметристов	да	да	да
15	Рандомайзер экспертов-квалиметристов	да	да	да
16	Анонимайзер работ, программ и тематик	да	да	да
17	Кью-менеджмент; дюрации; экспрессы	—	—	да
18	Бизнес-модель проекта B2B; институты	да	да	да
19	Бизнес-модель проекта B2C; исследователи	да	да	да
20	Бизнес-модель проекта B2G; ведомства	—	да	да
21	Модель монетизации «абонемент»; области	да	да	да
22	Модель монетизации «транзакция»; запросы	да	да	да
23	Модель монетизации «гибрид»; зачёты/неттинг	—	да	да
24	Отчётность в формате pdf; обзор и документ	да	да	да
25	Отчётность в формате xml; фактура и загрузка	—	да	да
26	Аналитическая отчётность; библиотека	—	да	да
27	Конструктор отчётности; инфокуб; объёмы	—	—	да

ПРЕДВАРИТЕЛЬНЫЙ КОНЦЕПТУАЛЬНЫЙ ДИЗАЙН

Проект «Сешат» предлагается на следующих принципах.

Первый принцип – для стадии MVP реализовать на базе веб-интерфейса с пользователями.

Второй принцип – минимизация функциональности на рабочем месте пользователя (т.е. пользователь на рабочем месте генерирует только свои индивидуальные данные и коды безопасности, включая электронную подпись (ЭП) (аналог собственноручной подписи) и коды аутентификации для распределенной БД или блокчейна). Все функции работы со статьями, статистика и семантические алгоритмы, реализованы на серверной платформе, находящейся за веб-интерфейсом.

Третий принцип – использование апробированных метрик для работы тестами. При поступлении статьи на рецензию для нее вычисляется набор метрик и далее сравнение текстов с корпусом текстов в одинаковых тематиках происходит с линейной трудоемкостью, поскольку все предыдущие статьи уже проиндексированы.

Четвертый принцип – опора на отечественные и специально программно-реализованные алгоритмы, позволяющие проводить последующую сертификацию у государственных регуляторов.

Пятый принцип – потенциальная монетизация – на платформе существуют токены, которыми оплачиваются функции системы (авторы платят токены за рецензии, эксперты их получают, токены также отчисляются административному персоналу платформы).

Принципы организации данных

Каждый пользователь при регистрации получает анонимное имя (UserX), однозначно связанное с реальным именем, но по которому невозможно восстановить его реальное имя, а также ключ для выполнения действий (подписания рецензии, выставления рейтинга и т.д.)

Пример

Первый пользователь

Ok Test Random

UserName: AndreyShcherbakov

UserPIN: 1234

UserX:**5cd6e237c6d71e25**

Ok Test Random

Successful UserFile create!

Creation UserKey Time-> 12:50:57 02.09.2022

Второй пользователь

Ok Test Random

UserName: Andrey_Shcherbakov

UserPIN: 1234

UserX:**8255dca3ef0fb938**

Ok Test Random

Successful UserFile create!

Creation UserKey Time-> 12:51:29 02.09.2022

Данные статей организованы в виде структуры директорий. Имя директории – десятичный номер по порядку поступившей на рецензирование статьи.

Данные пользователей хранятся в директориях с именами UserX.

Все генерируемые пользователями объекты подписаны их ЭП.

В блокчейн данные помещаются с двумя подписями – оператора и автора, для обеспечения консенсуальных процедур и работы смарт-контрактов.

На этапе MVP смарт-контракты организованы в виде собственной исполняющей машины-интерпретатора.

Роли пользователей и сценарий работы

Роль «автор» – пользователь загружает статьи.

Роль «эксперт» – пользователь откликается на статьи по своему профилю и генерирует рецензии и/или оценки.

Роль «администратор» – пользователь контролирует и организует работу сервисов (например, администратор верификации).

Роль «лигал» – пользователь участвует в разрешении конфликтов и высказывает мнение третейского судьи.

Роль «внешний заказчик» - пользователь, ищущий в системе интересующих его ученых или информацию.

Основные подсистемы

1. Подсистема регистрации и ведения профиля пользователя

2. Подсистема аутентификации и разграничения доступа (полномочий).

3. Подсистема индексации и сравнения текстов.

4. Подсистема оперативной деятельности (рассылка статей и обработка отзывов).

5. Подсистема журналов и статистики

6. Подсистема внешних интересантов (которые сообщают в систему свои научные интересы, а система подбирает им ученых и статьи – обеспечивает коммерциализацию и развитие «частной» науки).

Основные информационные (бизнес) процессы

При установке и разворачивании системы (платформы) в виде сайта и работающего за ним сервера регистрируется администратор системы (возможно, два и более администратора). Один из администраторов производит верификацию регистрирующихся пользователей и экспертов (администратор верификации).

Также в систему вводится словарь тематик – текстовые наборы терминов, сравнение которых с текстами-кандидатами определяет принадлежность текста к тематике.

1. Регистрация пользователей

Пользователь вводит свое имя, получает UserX, вырабатывает свой ключ в ключевом контейнере, защищенном паролем. Загружает в систему свои квалификационные документы (диплом об образовании, ученом звании и степени, список трудов, некоторые труды, которые он считает важными). Далее пользователь заполняет анкету, где указывает свои тематики (если он претендует на роль эксперта).

Администратор верификации производит верификацию загруженных документов и самого пользователя и завершает его регистрацию. При этом возможен голосовой звонок или общение с пользователем в мессенджере. Также возможна кросс-верификация на Госуслугах (в продуктовой версии). Пользователь получает статус – одну или несколько ролей и перечень тематик, в которых он компетентен. Параметры пользователя отражены в его профиле.

2. Загрузка статей

Статьи загружаются в систему для рецензирования или депонирования (в этом случае рецензирование не требуется, фиксируется приоритет; депонированию также подвергаются статьи или работы с требованиями конфиденциальности).

При загрузке производится индексирование статьи и установление ее принадлежности к тематике.

Также предпринимаются меры по предотвращению загрузки уже загруженных статей (например, путем сравнения с уже загруженными).

Хорошей практикой было бы сравнение индексированной статьи с уже загруженными и определение списка имеющих максимальную меру сходства статей для направления этой информации экспертам или накопление данной информации для автоматизации патентного поиска или антиплагиата.

После успешной загрузки администратор рецензий направляет ее на рецензирование или депонирование.

Направление на рецензирование происходит тремя возможными способами: всем экспертам тематики, избранным экспертам тематики, желающим экспертам тематики. Это выбор делается автором при загрузке и оплачивается внутренними токенами платформы. Соответственно, эксперт тематик выставляет в своем профиле параметр, желает ли он в текущее время участвовать в рецензировании.

При загрузке и поиске работает ядро семантического сервиса – процессы индексирования и сравнения текстов.

3. Рецензирование статей

Рецензент по публичной методике выставляет оценки статье и обосновывает их в виде рецензии, которую подписывает своей ЭП.

Рецензии и оценки модерируются администратором рецензий (например, в целях дополнительной анонимизации эксперта для исключения выяснения его личности и исключения давления на него).

Возможен режим без модерации, когда собираются оценки и рецензии не менее трех экспертов и автору направляется только усредненное мнение (оценка).

Весь документооборот на платформе выполняется в виде файловых операций между соответствующими директориями пользователей и статей.

4. Начисление токенов за рецензии и статистика

После формирования рецензии и оценки эксперты получают токены в соответствии с их

рейтингом.

Возможна ситуация, когда реальных токенов (начисленных авторами или спонсорами) не хватает для оплаты работы экспертов, в этом случае начисленные токены маркируются как кредитные (вексель) и учитываются по мере появления реальных токенов в хронологической очередности оплаты услуг экспертов.

Все действия в системе регистрируются в журналах.

5. Работа внешних заказчиков

Внешний заказчик регистрируется отдельно и также проходит процедуру верификации как физическое или юридическое лицо. Он также является донором (поставщиком) токенов в систему.

Он имеет возможность знакомиться со статистикой поступления статей, оценками за них, а также отдельно оплачивать процедуры развернутого поиска – когда его текстовый запрос сравнивается со статьями тематики с учетом заданного порога их рейтинга (средней экспертной оценки). Поиск может происходить и только по рейтингу статей.

К внешним заказчикам также относятся эксперты государственных учреждений и сервисов, которые обращаются за фактами приоритета или плагиата, различными характеристиками научных достижений авторов или экспертов.

ВЫВОДЫ

На сегодняшний день становится очевидной необходимость создания на базе ведущих научно-образовательных организаций отечественной наукометрической системы, позволяющей максимально точно, объективно и полно оценивать развитие направлений науки и качественно депонировать научные работы, а также проводить их объективное рецензирование и оценку. В связи с этим наиболее целесообразно создание квалиметрической платформы наукометрического оценивания на принципах саморегулируемой организации оценивания качественных характеристик научных работ участниками научного сообщества с возможностью масштабирования и тиражирования платформы в российском научном сообществе.

В данной статье архитектура, принципы построения и концептуальный дизайн платформы представляются достаточно проработанными.

СПИСОК ЛИТЕРАТУРЫ

1. Шапошников В.А. Квалиметрия: учебное пособие. Екатеринбург: Изд-во Рос. гос. проф.-пед. ун-та, 2016. 134 с. URL: http://elar.rsvpu.ru/handle/123456789/20925

2. Налимов В. В., Мульченко З. М. Наукометрия: Изучение науки как информационного процесса. Физико-математическая б-ка инженера. ФМБИ.- Москва : Наука, 1969.- 191 с.

3. Уорд П. Метод 360 градусов. М.: ГИППО, 2006. 352 с.

4. Рязанова А.А. Технология распределенных реестров: накопленный опыт и потенциал // Научно-технический сборник "Научно-техническая информация", сер. 2 Информационные процессы и системы, 2018. № 11. С.16-22.

5. Время деколонизации. URL: https://rgsu.net/platform/vremya-dekolonizatsii.html (дата обращения: 12.09.2022).

УДК: 004.8

Логические и методологические аспекты проблематики искусственного интеллекта

D.F. Aliev

Logical and Methodological Aspects of the Field of Artificial Intelligence

Abstract. *The article discusses current trends, problems and prospects for the development of the field of artificial intelligence. The level of AI technologies utilization among the fields of economics is presented. A description of the main development scenarios is given based on the socio-economic effects of the latest developments. The dependence of the AI development scenario on the use of binary and trinary logic in computer technology is shown. It is assumed that the development of computer technology based on binary logic, as well as the existing groundwork in the field of information technology, is not enough to create artificial intelligence, as a result of this it is necessary to improve the strategy of scientific and educational activities in the field of AI with the participation of leading teams of scientists, taking into account the interdisciplinary nature of research.*

Keywords: *artificial intelligence, artificial consciousness, algorithm, trust, binary logic, trinary logic.*

Д.Ф.Алиев

Доктор философии в области бизнес-права (PhD), доктор делового администрирования в области финансов (DBA), кандидат экономических наук, первый проректор Федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный социальный университет».

E-mail: kharchenkoDD@rgsu.net

Аннотация. *В статье рассматриваются актуальные тенденции, проблемы и перспективы развития области искусственного интеллекта (ИИ). Представлен уровень распространенности технологий ИИ по отраслям экономики. Дается описание основных сценариев развития исходя из социально-экономических эффектов от новейших разработок и зависимости сценария развития ИИ от применения бинарной и тринарной логики в вычислительной технике. Предполагается, что развития вычислительной техники на основе бинарной логики, а также существующих заделов в области информационных технологий недостаточно для создания искусственного интеллекта, вследствие чего необходимо совершенствование стратегии научно-образовательной деятельности в области ИИ с участием ведущих коллективов ученых с учетом междисциплинарного характера исследований.*

Ключевые слова: *искусственный интеллект, искусственное сознание, алгоритм, доверие, бинарная логика, тринарная логика.*

ВВЕДЕНИЕ

В феврале 2018 года журнал MIT Technology Review (Журнал инноваций Массачусетского технологического института) опубликовал обзор большого исследования за авторством 26-ти представителей от Оксфордского университета, Кембриджского университета, Фонда электронных рубежей (Electronic Frontier Foundation), а также некоторых других известных некоммерческих организаций и частных компаний, под названием «Вредоносное использование искусственного интеллекта (ИИ): прогнозирование, предотвращение и смягчение» [1]. Основным содержанием обзора было описание основных негативных сценариев применения искусственного интеллекта. Достаточно высоко оценив успехи в области ИИ и позитивность его практического применения, авторы отметили, что создаваемые наработки являются потенциальными инструментами в руках «преступников, оперативников и деспотов». Наличие подобных рисков позволяет полагать, что некоторые исследования в области ИИ необходимо проводить под грифом секретности.

Уже через год, в феврале 2019-го, один из директоров компании OpenAI Джек Кларк (Jack Clark) заявил MIT Technology Review, что их компания разработала и запустила языковый алгоритм общего назначения, обучив его на сетевом объёме более 45 млн. страниц обычного текста из Reddit (одного из самых посещаемых сайтов мира, сочетающего черты социальной сети, форума и системы голосования).

Отметим, что практически у всех конкурентов OpenAI на тот момент времени, а у многих – и по сей день, необходима специальная подготовка обучающей фактуры, которая требу-

ет больших затрат времени и денежных средств, увеличивает риски калибровки, и при этом качество готового продукта снижается. После обучения на нескольких миллиардах слов алгоритм OpenAI оказался пригоден не только для использования в переводах и ответах на вопросы, но и показал эффективность в генерации фантастических рассказов и новостей о событиях, которые никогда не происходили.

Дж. Кларк так оценивал перспективы разработанной технологии: *«совершенно очевидно, что если эта технология созреет – а я бы дал ей один или два года – она может быть использована для дезинформации или пропаганды»*, однако продолжение цитаты *«we're trying to get ahead of this»*, можно понять диаметрально противоположно, и как «мы постараемся помешать», и как «мы её возглавим».

Подсказку к смыслу сказанного даёт то, что даже MIT, одному из крупнейших исследовательских институтов Америки, команда разработчиков Илона Маска передала на тестирование версию своего алгоритма с усечённой функциональностью. Ещё через год, весной 2020-го года, компания OpenAI опубликовала свой знаменитый алгоритм обработки естественного языка третьего поколения GPT-3 (Generative Pre-trained Transformer) на 175 млрд. параметров (для сравнения- лучшая цифра Сбербанка – 13 млрд. для ruGPT-3) [2].

Летом того же года OpenAI открыла клубный API-доступ, объяснив ограничения желанием контролировать использование технологии и ограничивать доступ тем, кто ей «злоупотребляет». А осенью 2020 г. Microsoft получил от OpenAI эксклюзивную полную лицензию на использование GPT-3 в своих продуктах и доступ к исходному коду технологии.

Рассмотренный кейс комментирует лишь один, причём объективно средний по важности, взгляд на проблематику искусственного интеллекта. Как заявил Дж. Кларку его коллега Ричард Сочер (Richard Socher), научный руководитель другого калифорнийского ИТ-гиганта – компании Salesforce, «для создания фальшивых новостей не нужен искусственный интеллект; люди сами могут легко это делать». Однако, безусловно, в текущих обстоятельствах этот литературотворческий аспект искусственного интеллекта представляет, пожалуй, наибольший интерес и является предметом активного научного дискурса.

СТЕПЕНЬ ОХВАТА ОТРАСЛЕЙ ЭКОНОМИКИ ТЕХНОЛОГИЯМИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

С позиции основного содержания данной работы наибольший интерес представляет собой фундаментальная суть тематики искусственного интеллекта, а также вопросы его фактического распространения и отдельные прикладные аспекты.

Группа экспертов американской компании McKinsey & Company еще в 2017 опубликовала своё исследование распространённости систем искусственного интеллекта в индустриях нашей жизни [3], в котором приводится рыночная доля компаний, использующих в своей основной или перспективной деятельности как минимум одну систему ИИ, и траектории спроса на системы ИИ в оценке средних ожиданий в предстоящие 3 года. Все данные взвешены по размеру компаний и, поскольку заявленный в исследовании период уже прошёл, можно с уверенностью говорить, что сегодня уровень оснащения технологиями ИИ нашей жизни точно превышает приведенные в исследовании ожидаемые показатели.

Нам же важно, что системы ИИ уже в 2019-м году были материальны в 7-ми отраслях:

- хайтек и телекоммуникации;
- финансовая сфера;
- машиностроение и конструкторская деятельность;
- энергетическая сфера и природные ресурсы;
- средства массовой информации и масс-культура;
- транспорт, перевозки и логистика;
- товары народного потребления.

Также уже на тот момент появилось еще 6 отраслей, рассматривающих технологии ИИ в качестве перспективных: розничная торговля, образование, здравоохранение, строительная индустрия, профессиональные сервисы, туристическая индустрия и пассажирские перевозки (Рис. 1).

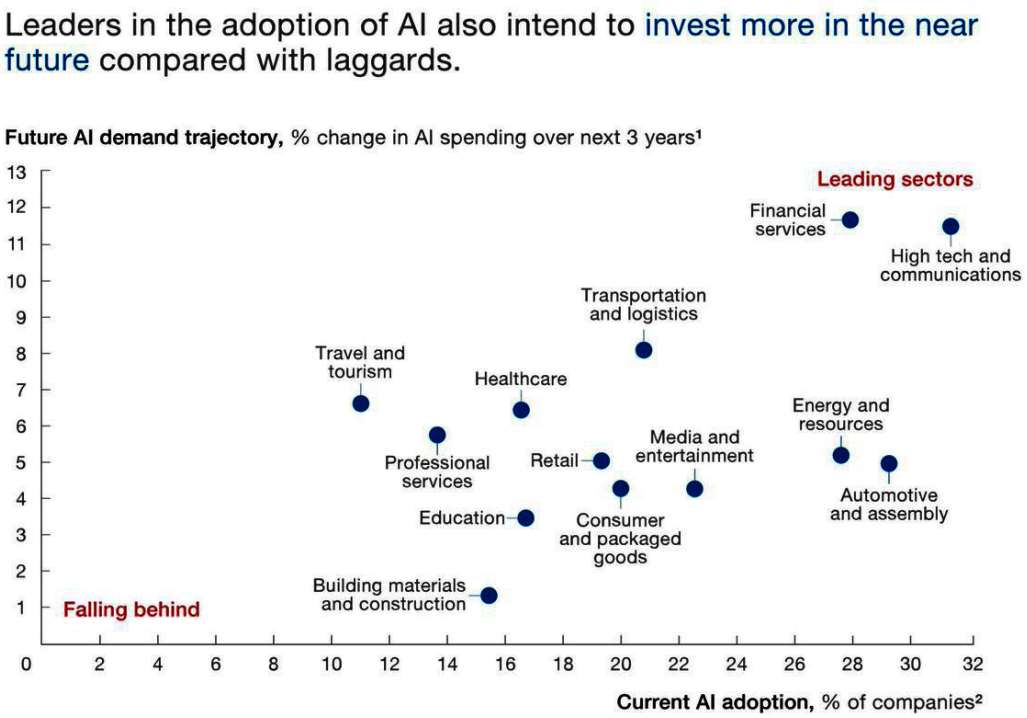


Рис. 1. Вовлеченность компаний в сферу технологий ИИ (по отраслям)[1]

Таким образом, можно утверждать, что сфера использования искусственного интеллекта, при всех его недостатках и проблемах (о которых будет сказано ниже), уже сложилась, приобрела все признаки социального феномена, становится общественно и социально значимой и нуждается в институционализации. Российский государственный социальный университет обязан, согласно его уточнённой стратегии развития, участвовать в этом социально-экономическом процессе.

ОСНОВНЫЕ ТЕНДЕНЦИИ И ПРОБЛЕМЫ В ОБЛАСТИ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА, РОЛЬ УЧАСТИЯ ЛИДИРУЮЩЕГО УНИВЕРСИТЕТА В ПРОЕКТАХ ПО ИИ

Приведем тезисно основные соображения касательно присутствия Российского государственного социального университета (РГСУ) в сфере ИИ.

1. Цифровая экономика охватывает все новые сферы жизни и общественного производства. Оценки мировых годовых прямых инвестиций в развитие ИИ не опускаются ниже 75 млрд. $ и варьируются в пределах 100 млрд. $, а эффекты от ИИ уже составляют приблизительно 20% от прибыли;

2. Российские цифровые индустрии, при серьёзной заявленной поддержке федерального руководства, пока только частично присутствуют в области ИИ;

3. Отечественный рынок технологий ИИ очень амбициозен, весьма конкурентен, имеет высокий, но не сбалансированный потенциал развития при общей текущей слабости технологических и инфраструктурных ресурсов;

4. Несмотря на наличие конкуренции вхождение в рынок в условиях недостаточной зрелости некоторых аспектов ИИ вполне возможно при выверенной стратегии и наличии качественных перспективных проектов;

5. В российских потенциалах, в т.ч. в нашем научном наследии, имеются уникальные возможности теоретического и практического свойства, которые позволяет рассчитывать на прорывные достижения;

6. Исторически сложившееся предметное научно-образовательное содержание дисци-

[1] Источник: https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx

плин в РГСУ вполне соответствует уровню задач позиционирования РГСУ не только в российской, но и в мировой науке и практике в области ИИ.

С учётом первых трех позиций сосредоточим своё внимание на трех последних, а точнее – проблемах, связанных с ними. Считаем, что на сегодняшний день невозможно представить весь спектр существующих проблем ИИ, поэтому следует ограничиться рассмотрением тех проблем, для решения которых целесообразно активное участие Университета. Укажем основные десять проблем.

1. Проблема исходных данных. Любая модель для своего практического применения требует данных. ИИ не является исключением, поскольку без нужного количества данных создать практически полезное решение с ИИ невозможно. Сегодня известны успешные примеры распознавания лиц при помощи чемпионской технологии FindFace российской компании NtechLab. Все подобные ИИ обучаются на датасетах с десятками и сотнями тысяч лиц, причем в данном случае это легко достижимо благодаря хорошему цифровому видеосигналу.

Однако результативность и качество моделей ИИ падает с возникновением проблем недостаточности, плохой подготовленности, недостоверности, нерелевантности данных. Так, в Новой Зеландии периодически возникают сложности с въездом в страну азиатских граждан, которых не распознаёт система, обученная на изображениях местных жителей преимущественно европейской внешности. Обучение идёт на исторических данных, на основе которых ИИ создает свою реальность, часто несоответствующую объективной, поэтому существуют проблемы с предиктивностью ИИ.

2. Проблема динамических данных. В отработке динамических данных ИИ бывает сложно и даже невозможно понять или отследить их логическую цепочку, в соответствии с которой система делает выводы. Существуют успешные проекты, как ИИ Deep Patient (США, 2015), который был обучен на данных о состоянии здоровья 700 тыс. человек. При проверке на новых пациентах система показала весьма хорошие результаты, включая обнаружение скрытых закономерностей, свидетельствующих о высокой вероятности появления каких-либо заболеваний, в том числе диагностировала шизофрению в случаях, когда «живые» медики не находили решения. Однако, имея все признаки «черного ящика», система принимала необъяснимые решения и не давала логических обоснований этих решений [4].

Кроме того, если такой проект как распознавание лиц российской системой FindFace требует больших денежных затрат (200 тысяч московских камер для потокового видео достаточного разрешения обошлись в 5 млрд.₽), принося требуемый предсказуемый результат, то для предсказания землетрясений или предотвращения логистических коллапсов необходимо решать множество дополнительных задач доступа, транспорта, синхронизации и тому подобных.

3. Проблема цифровой гигиены. За последние годы цифровизации практически во всех сферах жизни общества сформировались и существенные киберугрозы и проблемы сетевой безопасности, такие как неконтролируемые и несанкционированные утечки данных, противодействие которым даже в условиях статичных систем затруднительно, а в случае применения новых технологий ИИ может стать невозможным.

4. Проблема дезинформации и пропаганды. Сегодня ИИ не является интеллектом в общепринятом смысле и не способен различить правду и вымысел. Существуют отдельные способы и инструменты решения этой проблемы. Например, Facebook отключил в части фейк-анализа свои ИИ и нанял 10 тысяч модераторов только для оценивания «культурных нюансов публикаций». Когда об этом стало известно, ИТ-сообщество оценило такое решение как некий проигрыш. С марта этого года стало понятно, что причина решения заменить программное обеспечение живыми модераторами была, вероятно, совсем иной, но в целом такая переоценка не отменяет проблему дезинформации для перспектив внедрения ИИ.

5. Проблема оценочных суждений. Когда Facebook нанял на работу «модераторов правды», большинство участников рынка отнеслись к этому действию как одному из прочих неудачных экспериментов М. Цукерберга в так на-

зываемой борьбе с насилием и жестокостью. Однако оно объясняется тем, что ИИ сегодня, умея отчасти распознавать эмоции, не умеет их оценивать. При этом некоторые исследователи сомневаются в том, что это в целом решаемая задача. Нашу позицию на этот счёт приведём чуть позже, а здесь отметим, что эмоционально-основанные суждения искусственному интеллекту сегодня действительно не по возможностям. Более того, при современных технологиях создания и обучения в технологиях ИИ отражаются образ мышления и ценности их разработчиков. Часто у разработчиков недостаточно глубоких знаний в области психологии, социологии и других ключевых гуманитарных дисциплин, что провоцирует появление этических проблем. Таким образом, без коррекции базовых предпосылок и технологий ИИ не будет объективным и беспристрастным.

6. Проблема прав и ответственности. На сегодняшний день ИИ показывает весьма хорошие результаты в области медицины. ИИ-онколог Watson, разработанный IBM, с совпадением до 93% рекомендует протоколы лечения, аналогичные мнению лучших американский врачей для 13-ти разновидностей рака. Однако нельзя забывать о существовании достаточно большой вероятности ошибки, которая может послужить причиной смерти, а не излечения [5].

В ряде случаев объяснение отказу врачей делегировать решение медицинских вопросов искусственному интеллекту было в том, что мы озвучили как первую проблему - выборки данных, на которых обучали Ватсона, были американскими и ориентировались на их врачебные практики и методы. Однако глубинная проблема прав и ответственности связана и с неминуемыми ошибками ИИ, такими как трагедия в 2015 году на заводе Volkswagen, когда робот принял рабочего за автодеталь, ошибка интеллектуального ассистента Wallmart'a, повлекшая за собой сбой в производстве и поставках и 3-х кратный рост цен на детское питание в США (стране, в которой крайне критична зависимость от этого продукта), возможные аварии с участием робомобилей и многие другие.

Поэтому еще больше вопросов вызывает, кто будет нести ответственность за ошибки и последствия решений, принятых ИИ, кто и какие свои права готов делегировать искусственному интеллекту и на каких условиях и т.д.

7. Проблема доверия и контроля. Эта острая проблема ИИ психологического свойства корреспондирует с тремя первыми. Пользователи не обязаны понимать, как устроена та или иная технология искусственного интеллекта, кроме того, в некоторых случаях сами разработчики не могут объяснить, как функционирует их продукт. Поэтому при наличии возможности выбора люди скорее откажутся от использования «чёрного ящика».

Возможная вовлеченность в донастройки ИИ могла бы позитивно отразиться на доверии к ИИ, однако для того, чтобы обеспечить вовлеченность, необходимо иметь определенные цели и задачи, а главное – технологию с заданными прозрачными и прогнозируемыми функциями.

Проблема доверия тесно связана с проблемой контроля систем ИИ, к исследованию которой призывали еще Стивен Хокинг и нобелевский лауреат Фрэнк Вильчек из MIT [6]. Напомним, что, ссылаясь на попытки сориентировать ИИ на работу с намерениями людей против буквального выполнения команд, два президента Ассоциации развития искусственного интеллекта (AAAI) Том Диттерих и Эрик Хорвиц предупреждали о проблеме внезапного зарождения суперинтеллекта, которое может произойти независимо от воли разработчиков [7].

8. Проблема креатива и творчества. Искусственный интеллект на сегодняшний день лишь подражает человеку. Технологии ИИ уже давно используются в СМИ для написания спортивных новостей и криминальной хроники, однако задачи, связанные с творчеством, ими по-прежнему практически не выполняются.

Летом 2018-го известный ИИ-эксперт Джанель Шейн (Janelle Shane) из AI WEIRDNESS провела обучение общедоступного инструмента ИИ TextGenRNN из MIT-портфеля на датасете Kaggle, содержащем 231 657 американских шуток «тук-тук» от лучших артистов в жанре стендап-комедии. На рисунке 2 представлены некоторые результаты его отработки. Очевидно, что невозможно назвать эти шутки смешными.

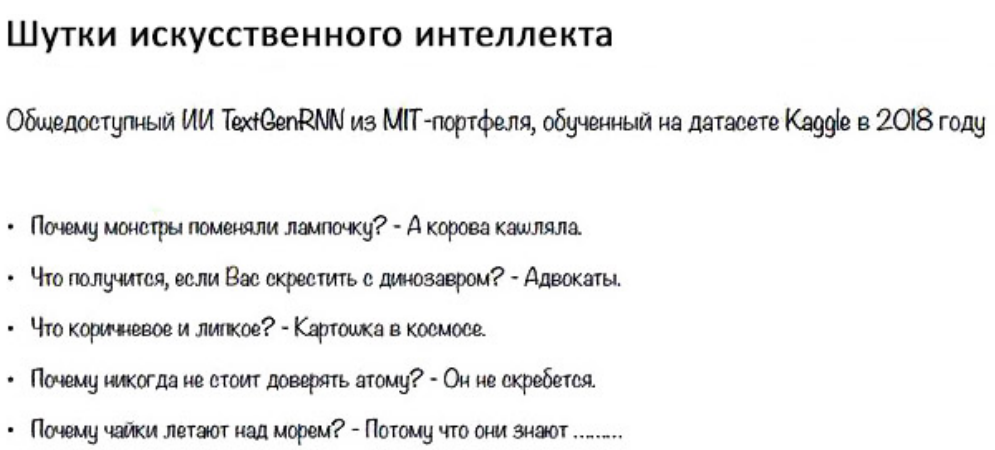


Рис. 2. Выборка из результатов генерации шуток модели ИИ TextGenRN

Через три года Дж. Шейн протестировала версии чемпионской технологии GPT-3 – в частности продвинутую (DaVinci), базововую (Curie) и облегчённую (Ada), поручив им производство шуток к 1-му апреля с учетом КОВИДных ограничений. Результаты представлены на рисунках 3 и 4 [8].

Рис. 3. Выборка из результатов генерации шуток версии DaVinci GPT-3

Рис. 4. Выборка из результатов генерации шуток версий Curie и Ada GPT-3

В ходе анализа восьми проблем, рассмотренных выше, обнаруживаем ещё одну комплексную проблему.

9. Проблема детерминации ИИ

Современный технологический уровень цифровизации и автоматизации процессов уже позволяет выполнять множество функций, которые ранее выполнялись только с применением человеческого ресурса, включая тестирование, прогнозирование, операции по расчетам, решение подчинённых оборонных задач и многие другие. Несмотря на то, что ни одной системе не удалось пройти «кофейный тест» С. Возняка (робот должен войти в незнакомую квартиру и приготовить кофе, выполнив все сопутствующие задачи), все совершенствующийся ИИ представляет собой угрозу для рынка труда. Так, еще 4 года назад в Великобритании предсказывали, что до конца 2020-х гг. ИИ-автоматизация сократит 4 млн. рабочих мест в частном секторе и 850 тыс. – в государственном [9].

Не стоит забывать, что указанная социально-экономическая тенденция наблюдается на фоне отсутствия четкой детерминированности понятия искусственного интеллекта. Основатель образовательной платформы Курсера Эндрю Ын уверен, что автоматизировать системами ИИ можно только те интеллектуальные задачи, с которыми человек справляется быстрее секунды. Во внеэкспертном обществе долгие годы маркером интеллекта была игра в шахматы. Сегодня ПК выигрывает у мировых гроссмейстеров, при этом даже лучшие чат-боты и голосовые ассистенты в осмысленных разговорах не показывают результатов более высоких, чем пятилетний ребёнок.

Представляется, что и сегодня мы можем говорить лишь о перспективе автоматизации рутинных операций. В этом смысле требования к компетенциям специалистов изменятся. С внедрением новых ИИ-систем будут требоваться специалисты, незаменимые на каждом этапе – от обучения до сопровождения и текущей деятельности. Так ИИ, подбирающему кадры, нужен консультант, системе рекомендательного сервиса – апдейтер, а военному комплексу - командир. Этот список можно продолжать до полного охвата всех существующих и перспективных систем искусственного интеллекта. При этом можно предполагать, что объем занятости в новых профессиях, связанных с применением ИИ, будет существенно ниже объема, сокращенного по причине внедрения новых инструментов ИИ.

Таким образом, описание всего круга проблем позволяет делать следующие выводы:

- необходимо четко разграничивать понятия искусственного интеллекта и искусственного сознания;

- на текущем технологическом уровне позитивные перспективы есть только у сбалансированного альянса искусственного интеллекта и человеческого;

- для обеспечения позитивной динамики развития области ИИ необходимо эффективное решение прикладных вопросов применения уже созданных систем;

- чтобы достичь эмпатии в исполнении ИИ, его суждениях и, возможно, отношениях с ним, необходимо обратиться к исходным позициям, движущим силам и механизмам ИИ, а также к глубинным мотивирующим факторам его развития.

Четвёртая позиция является одновременно и отражением десятой проблемы – проблемы аппетита, означающей, какой путь выберет человечество в точке бифуркации – искусственный интеллект или искусственное сознание.

О МЕТОДОЛОГИИ МЫШЛЕНИЯ. СИСТЕМЫ СЧИСЛЕНИЯ, ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ, ИСКУССТВЕННОЕ СОЗНАНИЕ

Аристотель в своих «Аналитиках» изложил теорию логики, приведя её законы и силлогизмы. Эта логика, как и все его физические представления, в том числе постулат «природа не терпит пустоты», оставались основой научного мышления вплоть до XX века несмотря на наличие противников в лице Галилея, Торричелли, Паскаля и др.

Считается, что и сегодня мы живём в аристотелевой логике.

В 1903-м году британец Бертран Рассел открыл парадокс, показывающий, что теория множеств в существовавшем виде приводит к противоречию. Это известный парадокс брадобрея: «он бреет всякого, кто сам не бреется; и

не бреет того, кто бреется сам; кто бреет брадобрея?» Парадокс Рассела привёл к тяжёлому кризису математики, её расколу и резкому ускорению развития в трёх направлениях: интуиционизм, логицизм и формализм.

Интуиционисты во главе с голландцем Яном Брауэром критиковали классическую математику за её опору на парадоксальную теорию множеств; их новая математика рассматривала мир мысленных процессов как последовательность элементарных шагов. А ещё они исключили понятие бесконечности из науки. Как говорил Сигизмунд Врублевский, «если тебе трудно сразу понять всю бесконечность, постарайся понять ее хотя бы наполовину».

Логицисты во главе с немецким математиком, логиком и философом Готлобом Фреге и самим Бертраном Расселом обнаружили, что парадоксы типа расселовского связаны не столько с их математическим содержанием, сколько со свойствами языка. Итогом стало утверждение о сводимости математики к логике и знаменитый труд в трёх томах «Principia Mathematica».

Формалистов собрал вокруг себя немецкий ученый Давид Гильберт. В этот круг входили такие видные ученые, как Герман Вейль, Эмануил Ласкер, Пауль Бернайс, Вильгельм Аккерман. К ним относился и Джон фон Нейман – автор фундаментальных трудов по математике, квантовой физике, информатике, автор архитектуры большинства современных компьютеров.

Д. Гильберт провозгласил своей целью возвращение математике её строгости и начал разрабатывать математический аппарат формализма. В 1934-м и 1939-м годах вышли два знаменитых тома «Оснований математики» Гильберта и Бернайса, в которых были представлены аксиоматическая теория доказательств и основы современной математической логики. Но предшествовала им более ранняя публикация 1928 года «Основ теоретической логики», подготовленная в соавторстве с Вильгельмом Аккерманом, в которой Гильберт и подверг уничтожающей критике логику Аристотеля.

Смысл противоречия заключается в том, что отвергнутое положение «Все А суть В» у Аристотеля трёхзначно, а у Гильберта – двухзначно. В этот момент математика оторвалась от реальности, а логика двух немецких ученых заменила всеобщую формулу «да»/«нет»/«не знаю» на чёрно-белую «да»/«нет». Однако наша жизнь тринарна, а бивалентная логика ведет к логическому фатализму.

Лучше всех эту историю прокомментировал известный математик позднего СССР, автор задачки «о мятом рубле» Владимир Игоревич Арнольд: «Гильберту принадлежит формальная точка зрения на математику как на дедуктивный вывод логических следствий из заданных аксиом. Эта точка зрения, безусловно, справедлива, но лишь в той мере, в какой поэзия сводится к последовательностям букв определенных алфавитов».

Вернёмся к проблемам искусственного интеллекта. Полагаем, что на современном уровне возможно создать даже суперинтеллект. Но понять эмоции человека по сообщениям в соцсетях или создать вирусное приложение, покоряющее мир остроумными шутками, системы

Рис. 5. Пример базовой записи в системах счисления[2]

[2] Источник: https://dev.to/buntine/the-balanced-ternary-machines-of-soviet-russia

ИИ не смогут до тех пор, пока они бинарны. Для решения сверхзадачи искусственного сознания нужна тринарная (троичная, тернарная) (рис.5) информатика, основанная на логике Аристотеля.

Первый и единственный серийный компьютер на живой трёхзначной логике назывался «Сетунь» и был создан Николаем Петровичем Брусенцовым и его коллективом.

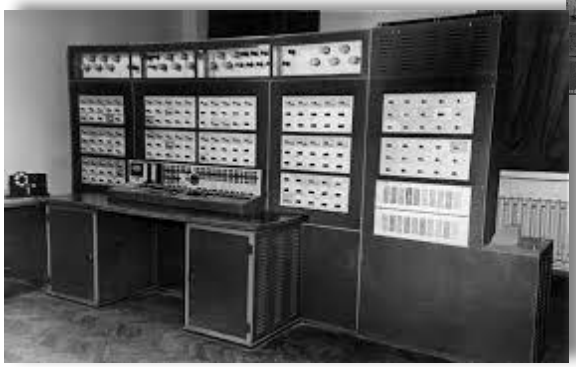
Николай Петрович Брусенцов

Николай Петрович Брусенцов - фронтовик, кавалер орденов Красной Звезды, Отечественной войны, Знак Почёта, За Заслуги перед Отечеством; был награждён медалями «За отвагу», «За взятие Кенигсберга», «За победу над Германией», «За доблестный труд», Большой золотой медалью ВДНХ.

Николай Петрович бессменно руководил лабораторией ЭВМ ВМК МГУ с 1958-го по 2014-й год.

Коллектив Н.П. Брусенцова

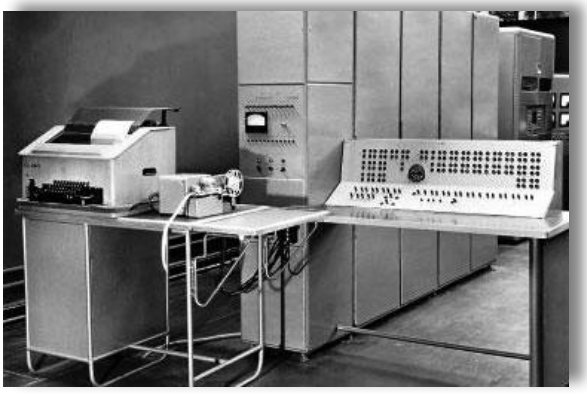
В 1959 году команда Брусенцова собрала и запустила опытный образец троичного компьютера «Сетунь», которых за 6 лет на Казанском заводе собрали 56 шт.



Опытный образец ЭВМ «Сетунь», 1959 г.

В 1970-м году, к столетию со дня рождения Ленина, была выпущена версия ЭВМ под названием «Сетунь-70», исполненная на новых элементах.

Троичная ЭВМ «Сетунь-70»



Серийный образец «Сетуни», 1961 г.

После того, как разработка ЭВМ «Сетунь» была остановлена, Н.П. Брусенцов занялся прикладным применением вычислительных машин и создал автоматизированную систему обучения "Наставник", предназначенную для поточного обучения студентов, проведения коллоквиумов и тестов. «Наставник» в 1972-м году (!) на практике реализовал нейро-подход к обучению.

Трудно предположить, каким был бы мир сегодня, если бы 60 лет назад политика партийно-промышленного руководства Госкомитета по радиоэлектронике была иной и команда Брусенцова получила бы поддержку. По мнению нидерландского ученого Эдсгера Дейкстру, автора концепции структурного программирования, «решение советского правительства о переходе советской промышленности к копированию модельного ряда IBM/360 стало величайшей победой Запада в Холодной войне».

Таким образом, тринарная информатика не получила такого развития, как бинарная, но несмотря на это некоторые исследования в этой области по-прежнему ведутся. В МГУ продолжает работать лаборатория троичной информатики Брусенцова. В США со времён появления американского аналога «Сетуни» PDP-8 создаются эмуляторы, исследуются элементы с промежуточными состояниями, на несложных задачах тестируется тринарная логика. Некоторые университеты Индии, Франции и Израиля также проводят исследования в области вычислительной техники на основе тринарной логики.

Изучаются сильные и слабые стороны тринарной логики, причем можно обоснованно утверждать, что большинство сильных сторон фундаментальны, в то время как недостатки связаны с проблемой технической реализации троичного состояния первичных элементов.

Для ЭВМ на основе тринарной логики есть варианты реализации долговременной памяти, при этом оперативная память и первичные элементы процессора требуют исследований. Однако исследования в рамках данной тематики не проводятся, несмотря на многие преимущества тринарности, такие как большая близость к основанию нормального логарифма или возможность записывать цвет одним тритом. На сегодняшний день для разработчиков вполне комфортна среда бинарной вычислительной техники, однако именно в ней представляется принципиально невозможным создание искусственного разума, в отличие от искусственного интеллекта.

В настоящее время весьма сомнительна также возможность получить поддержку исследований в области вычислительной техники, реализующей тринарную логику, но тем не менее, если в точке бифуркации наш выбор между искусственным интеллектом и искусственным сознанием будет в пользу ИС, необходимо пересмотреть перспективы разработки и тестирования вычислительной техники на основе тринарной логики в применении к созданию ИИ и ИС.

ВЫВОДЫ

Исследования в области искусственного интеллекта в силу сложности и многоплановости проблем, связанных с их внедрением и влиянием на общество, должны носить междисциплинарный характер, а также вовлекать ученых, занимающихся как фундаментальными вопросами ИИ, так и прикладными аспектами, и проходить в тесном взаимодействии с высшим образованием.

Российский государственный социальный университет обладает большим потенциалом для проведения таких исследований, прежде всего имеются достаточные заделы в юридической, психологической, медицинской, социологической и информационно-технологической научно-образовательных предметных областях.

Целесообразно установить приоритетными стартовыми содержательными компонентами деятельности РГСУ в проблематике искусственного интеллекта пять укрупнённых групп тем по правовым вопросам ИИ, цифровой гигиене ИИ, этическим аспектам ИИ, медицинским применениям ИИ и тринарной информатике ИИ.

Проблематику искусственного интеллекта необходимо позиционировать в качестве приоритетной научной-образовательной тематики Российского государственного социального университета, имея в виду комплексное вовлечение заделов пяти приведенных предметных областей с использованием пяти представленных ресурсных потенциалов для решений по десяти изложенным в данной работе проблемам искусственного интеллекта.

СПИСОК ЛИТЕРАТУРЫ

1. The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation. URL: https://arxiv.org/ftp/arxiv/papers/1802/1802.07228.pdf (дата обращения: 12.09.2022).

2. OpenAI Presents GPT-3, a 175 Billion Parameters Language Model. URL: https://developer.nvidia.com/blog/openai-presents-gpt-3-a-175-billion-parameters-language-model/ (дата обращения: 12.09.2022).

3. Artificial Intelligence. The next digital frontier? URL: https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/how%20artificial%20intelligence%20can%20deliver%20real%20value%20to%20companies/mgi-artificial-intelligence-discussion-paper.ashx (дата обращения: 12.09.2022).

4. Зловещий секрет в самом сердце искусственного интеллекта. URL: https://habr.com/ru/post/370445/ (дата обращения: 12.09.2022).

5. ИИ-онколога IBM Watson уличили во врачебных ошибках. URL: https://hightech.plus/2018/07/27/ii-onkologa-ibm-watson-ulichili-vo-vrachebnih-oshibkah- (дата обращения: 12.09.2022).

6. Stephen Hawking: 'Transcendence looks at the implications of artificial intelligence - but are we taking AI seriously enough?'. URL: https://www.independent.co.uk/news/science/stephen-hawking-transcendence-looks-at-the-implications-of-artificial-intelligence-but-are-we-taking-ai-seriously-enough-9313474.html (дата обращения: 12.09.2022).

7. Dietterich T., Horvitz E. "Rise of Concerns about AI: Reflections and Directions". Communications of the ACM 58 (10): 38–40. doi:10.1145/2770869. URL: http://erichorvitz.com/CACM_Oct_2015-VP.pdf (дата обращения: 12.09.2022).

8. Шутки, придуманные нейросетью, показали, как у ИИ обстоит дело с чувством юмора. URL: https://naukatv.ru/news/nejrosetyam_predlozhili_pridumat_pervoaprelskie_rozygryshi (дата обращения: 12.09.2022).

9. Robots 'could take 4m UK private sector jobs within 10 years'. URL: https://www.theguardian.com/technology/2017/sep/19/robots-could-take-4m-private-sector-jobs-within-10-years (дата обращения: 12.09.2022).

УДК: 004.8

Об актуальной научно-исследовательской повестке в сфере искусственного интеллекта

S. Zapechnikov

On the Current Research Agenda in the Field of Artificial Intelligence

Abstract. *The article highlights and analyzes a number of problems and trends that currently determine the development of methods and models of artificial intelligence. The current general methodological and applied problems of AI are considered. The positive effect of using AI as a tool for scientific research, including fundamental ones, is analyzed. An overview of AI methods and tools for solving weakly structured problems and processing complicated big data is given. It is shown that one of the most pressing problems is the problem of ensuring trust in AI and information security of AI.*

Keywords: *artificial intelligence technologies, machine learning, deep learning, complicated big data, trustworthy artificial intelligence, information security of artificial intelligence.*

С.В. Запечников
Доктор технических наук, профессор Института интеллектуальных кибернетических систем, Национальный исследовательский ядерный университет «МИФИ», Вице-президент по научной работе Ассоциации специалистов в области криптовалют и цифровых финансовых активов
E-mail: SVZapechnikov@mephi.ru

Аннотация. *В статье выделяется и анализируется ряд проблем и тенденций, определяющих развитие методов и моделей искусственного интеллекта в современных условиях. Рассматриваются актуальные общеметодологические и прикладные проблемы ИИ. Анализируется позитивный эффект от использования ИИ как инструментария научных исследований, в том числе фундаментальных. Дается обзор методов и средств ИИ для решения сложноструктурированных задач и обработки сложноструктурированных данных. Показано, что одними из самых актуальных проблем являются обеспечение доверия к ИИ и информационной безопасности ИИ.*

Ключевые слова: *технологии искусственного интеллекта, машинное обучение, глубокое обучение, сложноструктурированные данные, доверенный искусственный интеллект, информационная безопасность искусственного интеллекта.*

ВВЕДЕНИЕ

В наши дни наблюдается заметный всплеск интереса к технологиям искусственного интеллекта (ИИ). Это обстоятельство обусловлено как уже достигнутыми успехами во внедрении ИИ в самые различные сферы человеческой деятельности, так и ожиданиями ещё большего позитивного эффекта от ИИ в будущем. В этой связи представляет интерес сделать своеобразный «срез» нынешнего этапа исследований и разработок в области ИИ. Поскольку наука всегда выступает локомотивом гораздо более обширного проникновения создаваемых новых технологий в самые разные сферы человеческой жизни, можно спрогнозировать наиболее заметные изменения в экономическом укладе и повседневной жизни человеческого общества в недалёком будущем.

Технологии ИИ почти всегда имеют прикладной и междисциплинарный характер. В настоящей статье предпринимается попытка анализа исследовательских и внедренческих трендов в тех областях, которые, как представляется, уже сейчас наиболее затронуты технологиями ИИ, претерпевают под его влиянием наиболее заметные и быстрые изменения и, следовательно, являются самыми многообещающими.

Статья имеет следующую структуру. В первом разделе рассматриваются наиболее заметные из актуальных общеметодологических проблем ИИ. Последующие разделы посвящены некоторым конкретным областям развития ИИ. Так, во втором разделе рассматриваются возможности использования ИИ как инструмента научных исследований, в первую очередь, фундаментальных. В третьем разделе рассматривается проблема применения ИИ для решения сложноструктурированных задач и обработки сложноструктурированных данных. Четвертый раздел посвящён проблемам создания доверенного ИИ и обеспечения информационной безопасности ИИ.

1. ОБЩЕМЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ИИ

ИИ как комплексная научно-техническая область имеет обширное теоретическое ядро, которое в настоящее время представлено, прежде всего, методами статистического обучения и интеллектуального анализа данных, а также смежными областями: методами оптимизации, численными методами, теорией автоматического управления и пр. Дисциплины, составляющие теоретическое и методологическое ядро ИИ, перечислены и охарактеризованы, например, в [1].

Ключ к пониманию общих тенденций развития технологий ИИ даёт, в первую очередь, анализ направлений развития теоретико-методологического базиса ИИ. С этой целью попытаемся систематизировать актуальные общеметодологические проблемы ИИ.

1. Решение внутренних проблем науки об ИИ:

• появление и развитие новых разделов компьютерных наук (непрерывное обучение, самообучение, автоматизация синтеза архитектур нейронных сетей, геометрическое глубокое обучение и др.);

• постановка новых массовых задач, решаемых методами ИИ;

• развитие высокопроизводительных вычислений с данными большой размерности (тензорные вычисления, новые численные методы решения задач оптимизации);

2. Создание инструментов решения новых научных проблем, вовлечение в орбиту применения ИИ новых сфер человеческой деятельности.

В качестве примеров принципиально новых теорий и методологических идей в сфере ИИ, появившихся в недавнем прошлом и бурно развивающихся в настоящее время, назовём следующие.

• *Федеративное машинное обучение*, в том числе горизонтальное, вертикальное и трансферное федеративное обучение. Федеративное машинное обучение позволяет обучать модели на обучающих выборках, составленных из данных множества владельцев без необходимости передачи этих данных в общее пользование, тем самым позволяя сохранять конфиденциальность. При этом можно добиться качества обучения моделей не худшего, чем при традиционном подходе.

• *Обучение нейросетей методом прямого вычисления градиента*. В настоящее время на практике для обучения нейросетей используется почти исключительно алгоритм обратного распространения ошибок, реализующий метод градиентного спуска. Этот алгоритм требует двукратного прохода графа вычислений для каждого обучающего примера. Метод прямого вычисления градиента позволит как минимум в 2 раза ускорить вычисления при обучении нейросетей. Недостатком метода является его ограниченная применимость.

2. ИИ КАК ИНСТРУМЕНТАРИЙ НАУЧНЫХ ИССЛЕДОВАНИЙ

Позитивный эффект использования ИИ как инструмента научных исследований обусловлен, прежде всего, способностью ИИ существенно усиливать или углублять человеческие способности, особенно важные для исследователя. Функции ИИ, позволяющие говорить об этом, включают следующие:

• обнаружение ранее неизвестных закономерностей в сверхбольших массивах данных;

• возможность конструирования (преимущественно при помощи генеративного моделирования) новых, не наблюдавшихся ранее объектов, комбинирующих свойства известных объектов, на основе выделенного латентного пространства признаков;

• перебор экспоненциально большого количества состояний системы с целью выявления оптимальных по каким-либо критериям состояний.

ИИ в качестве инструментария научных исследований применим в целях развития как фундаментальных научных исследований, так и прикладной науки.

Перечислим некоторые известные сферы и примеры применения ИИ как инструментов фундаментальной и прикладной науки:

• в физике элементарных частиц – для обнаружения элементарных частиц, образующихся

при столкновениях частиц в ходе физических экспериментов с целью подтверждения физических гипотез;

• в физике плазмы – для долговременного удержания плазмы в ходе экспериментов по созданию термоядерных реакторов;

• в астрофизике и космологии – для обнаружения ранее не наблюдавшихся объектов, выдвижения и подтверждения гипотез;

• в материаловедении – для предсказания свойств создаваемых материалов, создания материалов с заранее заданными свойствами;

• в физике твёрдого тела – для моделирования поведения тела при внешних воздействиях на него;

• в математической физике – для проведения сложных многошаговых численных экспериментов;

• в хемоинформатике – для проведения численных химических экспериментов, поиска химического состава веществ с искомыми свойствами, предсказания свойств химических соединений;

• в биоинформатике – для геномных исследований;

• в криптографии и криптоанализе – для исследования вероятностных свойств стойкости существующих и перспективных криптосистем, а также стойкости их реализаций к атакам по побочным каналам, обнаружения скрытых каналов утечки информации;

• в математике – для решения дифференциальных уравнений, доказательства теорем в топологии, геометрии, комбинаторике;

• в биологии – для моделирования конформаций всех известных белков, создания цифровых моделей участков мозга животных и человека;

• в фармакологии – для синтеза новых лекарственных форм, поиска новых антибиотиков и пр.;

• в экологии – для моделирования углеродного следа, прогнозирования воздействия человеческой деятельности на окружающую среду;

• в исторической науке – для реконструкции исторических артефактов, расшифровки забытых письменностей.

Приведенные примеры свидетельствуют о достаточно широкой распространенности методов ИИ в современной науке, успешности применения их для получения новых исследовательских результатов и позволяют прогнозировать ещё более широкое распространение их в недалеком будущем.

3. ИИ ДЛЯ РЕШЕНИЯ СЛОЖНОСТРУКТУРИРОВАННЫХ ЗАДАЧ И ОБРАБОТКИ СЛОЖНОСТРУКТУРИРОВАННЫХ ДАННЫХ

Имеется устойчивый круг задач, в которых ИИ был успешно применён ещё на ранних этапах его развития и которые на сегодняшний день уже немыслимы без ИИ. Это компьютерное зрение, обработка естественных языков, робототехника, рекомендательные системы, компьютерная графика и многое другое. Однако все перечисленные сферы характеризуются относительной упорядоченностью, регулярностью данных, с которыми работают алгоритмы ИИ. Так, например, в обработке естественных языков тексты и аудиопотоки – это всегда линейно упорядоченные массивы, в компьютерном зрении и робототехнике фотоизображения и видеопотоки – это матрицы и тензоры. Таким образом, для традиционных задач характерны:

• простые типы данных: числовые, символьные, двоичные строки;

• базы данных, преимущественно реляционные (таблицы);

• данные регулярной структуры (текст, аудио- и видеопотоки, цифровые изображения и пр.).

Однако современные задачи требуют умения обрабатывать всё более и более сложные совокупности данных, да и структура самих задач становится комплексной, они включают в себя подзадачи, образующие конвейеры или иерархию.

Таким образом, новые задачи требуют от ИИ умения работать с новыми структурами данных, такими как:

• графы, гиперграфы, сети;

• алгебраические абстракции: группы, кольца, поля, векторные пространства, многообразия;

• скалярные и векторные поля;

Это обстоятельство, в частности, привело к появлению такого нового раздела ИИ как геометрическое глубокое обучение [2].

Приведем несколько примеров, которые, несмотря на некоторую произвольность в их выборе, дают неплохое представление о сложности структуры таких задач и сложности обрабатываемых в них данных.

• *Проблема установления конформаций белковых молекул*. Для решения этой проблемы был реализован проект AlphaFold [3]. Исследование пространственных конфигураций белковых молекул осуществляется на протяжении нескольких десятилетий физическими методами, которые характеризуются дороговизной и длительными сроками проведения экспериментов. За период проведения таких исследований накопилась значительная база данных известных результатов, которую можно использовать в качестве обучающей выборки для обучения моделей ИИ, способных предсказывать конформацию новых молекул по известным последовательностям их аминокислотных остатков. Проблема создания такой модели и была решена в ходе реализации проекта AlphaFold, выполненного компанией DeepMind (на сегодняшний день эта модель уже не единственная). С помощью модели за короткое время была предсказана конформация большинства известных науке белковых молекул.

• *Создание компьютерной программы для игры в го*. Проект AlphaGo [4]. Давно известны компьютерные программы для игры в шахматы, шашки и другие классические игры, однако игра го до недавних пор не поддавалась усилиям разработчиков компьютерных программ. Это объясняется тем, что го – сложная игра, требующая нескольких уровней стратегического мышления. Количество вариантов партий этой игры практически необозримо, на много порядков превышает число комбинаций шахматных партий, и их невозможно перебрать методом построения дерева поиска. Все предыдущие попытки приводили к созданию компьютерных программ, играющих на весьма посредственном уровне. Для создания компьютерной программы, способной на высоком уровне соперничать с человеком в этой игре, пришлось применить методы обучения с подкреплением в соединении со стратегией поиска на основе метода Монте-Карло, что было реализовано в проекте AlphaGo.

• *Реалистичный синтез человеческого голоса в реальном масштабе времени* был целью реализации проекта WaveNet [5]. Цель проекта состояла в создании инструмента, способного в режиме реального времени преобразовывать текст в речь на естественном языке. Ранее известные модели либо не могли выполнять эту функцию в режиме реального времени, либо синтезируемая ими речь была низкого качества.

• *Исследование тактики игры в футбол* [6]. Целью проекта является выработка оптимальной тактики футбольной команды в игре с другими командами на основе изучения записей прошедших матчей обеих команд. Для этого используются данные, собираемые при помощи видеокамер, о местоположениях игроков и мяча, снятые через небольшие интервалы времени, позволяющие сформировать траектории и рассчитать многочисленные пространственные и числовые характеристики отдельных игроков и команды в целом.

• *Модель обработки поисковых запросов, заданных на естественном языке* (на основе языковой модели BERT) [7]. Суть задачи состоит в создании модели, обучаемой восприятию естественного человеческого языка, способной высококачественно транслировать речь в запросы к поисковой системе и выполнять поиск релевантной информации.

Как видим, эти примеры очень разнообразны и связаны с решением разнородных, весьма нетривиальных задач и с использованием данных совершенно разных типов и разной структуры.

Рассмотрим также два комплексных примера, относящихся к важным традиционным отраслям человеческой деятельности.

• *Цифровое сельское хозяйство*. Идея состоит в реализации «безлюдных» сельскохозяйственных предприятий, где поля и фермы оснащаются многочисленными IoT-устройствами, фиксирующими параметры внешней среды, состояние сельскохозяйственных растений и животных, а робототехнические комплексы осуществляют все основные технологические

операции по обслуживанию и уходу за сельскохозяйственными растениями и животными.

• *Цифровое строительство*. Идея заключается в создании «безлюдных» строительных площадок, на которых все этапы работ, традиционно выполняемые человеком с использованием средств механизации, от освоения стройплощадки до сдачи в эксплуатацию законченного сооружения, были бы полностью автоматизированы. С этой целью предполагается использовать аддитивные технологии, включая технологии 3D-печати для изготовления элементов строительных конструкций, а также многочисленные автономные робототехнические устройства и даже рои роботов для подготовки строительной площадки, доставки и монтажа строительных конструкций, отделки готовых сооружений.

Несмотря на достаточно полную теоретическую проработку этих концепций, их полномасштабная реализация и практическое внедрение пока сдерживаются в основном экономическими причинами, связанными с высокой стоимостью реализации при наличии относительно дешёвой рабочей силы.

4. ДОВЕРЕННЫЙ ИИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИИ

Повсеместное применение технологий ИИ выдвигает высокие требования к инструментам ИИ по доверию и безопасности. Несмотря на различия в подходах к определению понятия доверенного ИИ, наблюдаемые в разных источниках, а также списку требований, входящих в понятие доверия, можно попытаться выделить основные составляющие доверенного ИИ:

• использование доверенной, т.е. обладающей предсказуемой функциональностью, свободной от недекларированных возможностей, аппаратной базы;

• использование доверенной (в аналогичном смысле) программной среды;

• надёжность систем ИИ (в традиционном смысле, который вкладывается в понятие надёжности в технических науках);

• обеспечение функциональной безопасности систем, использующих технологии ИИ;

• обеспечение качества предоставления сервисов;

• обеспечение доверия между бизнес-партнёрами, если интеллектуальная система предназначена для выполнения бизнес-функций.

Инструментами обеспечения доверия к технологиям ИИ выступают следующие решения и инструменты:

• отечественная аппаратная база;

• отечественные программные решения и аппаратно-программные комплексы;

• прошедшие верификацию программные средства с открытым исходным кодом;

• системы распределенного реестра и др.

Детальный анализ проблемы обеспечения информационной безопасности ИИ проводился в [8]. Для полноты изложения перечислим здесь основные классы задач обеспечения информационной безопасности технологий ИИ, которые возникают помимо чисто технических задач обеспечения безопасности ИТ-систем:

• обеспечение безопасности персональных данных;

• обеспечение конфиденциальности данных, содержащих охраняемые законом виды тайны (коммерческую, банковскую, врачебную и др.);

• разграничение доступа к информационным и аппаратно-программным ресурсам;

• предотвращение утечки информации по скрытым и побочным каналам.

Как видим, они не имеют ярко выраженных отличий от задач обеспечения безопасности иных информационных технологий. В то же время специфическими являются инструменты обеспечения информационной безопасности:

• конфиденциальное машинное обучение (privacy-preserving machine learning), реализуемое преимущественно на основе протоколов безопасных многосторонних вычислений (secure multi-party computations), которые, в свою очередь используют в качестве примитивов гомоморфное шифрование, схемы разделения секрета, искаженные схемы (garbled circuits), доказательства с нулевым разглашением (zero-knowledge proofs);

• концепция статистической неразличимости (differential privacy);

• аппаратные средства доверенного испол-

нения кода;

• эвристические решения.

Из перечисленных направлений наибольшее влияние на развитие технологий безопасного ИИ имеет, как представляется, конфиденциальное машинное обучение и смежные технологии конфиденциального выполнения иных необходимых для систем ИИ функций, таких, как конфиденциальная выборка информации из баз данных (private information retrieval), конфиденциальное вычисление пересечения множеств (private set intersection) и др.

ЗАКЛЮЧЕНИЕ

В статье выделены и проанализированы основные направления развития идей и технологий в области ИИ на современном этапе. Показано, что исследовательская повестка в сфере искусственного интеллекта чрезвычайно обширна и включает ряд принципиально новых направлений. Отмечены актуальные общеметодологические и прикладные проблемы ИИ. В частности, показан позитивный эффект от использования ИИ как инструментария научных исследований, в том числе фундаментальных, приведены многочисленные примеры успешного использования ИИ в сфере научных исследований. Дан обзор новых технологий ИИ, применяемых для решения сложноструктурированных задач и обработки сложноструктурированных данных, приведены примеры таких задач, в том числе комплексных, из разных областей человеческой деятельности. Показано, что одними из самых актуальных проблем являются проблемы обеспечения доверия к ИИ и информационной безопасности ИИ, указаны развивающиеся в настоящее время методы создания доверенных и безопасных интеллектуальных ИТ-систем.

СПИСОК ЛИТЕРАТУРЫ

1. Запечников С.В. Актуальные зарубежные образовательные практики в области искусственного интеллекта: содержательное наполнение образовательных программ / С. Запечников // Вестник современных цифровых технологий. Вып. 11. 2022. С.5 – 26.

2. Bronstein M., Bruna J., Cohan T. Geometric Deep Learning: Grids, Groups, Graphs, Geodesics, and Gauges. URL: https://geometricdeeplearning.com/ (дата обращения: 07.09.2022)

3. Jumper J. Highly accurate protein structure prediction with AlphaFold / J. Jumper, R. Evans, D. Hassabis // Nature. Vol. 596, pp. 583 – 589 (2021). URL: https://www.nature.com/articles/s41586-021-03819-2

4. Silver D. Mastering the game of Go with deep neural networks and tree search / D. Silver, A. Huang, C. Maddison et al. // Nature. Vol. 529. 20 pp. (2016) URL: https://storage.googleapis.com/deepmind-media/alphago/AlphaGoNaturePaper.pdf

5. van den Oord A. WaveNet: A generative model for raw audio / A. van den Oord, S. Dieleman, H. Zen et al. arXiv preprint. 2016. 15 pp. URL: https://arxiv.org/pdf/1609.03499.pdf (дата обращения: 07.09.2022)

6. Omidshafiei S. Multiagent off-screen behavior prediction in football / S. Omidshafiei, D. Hennes, M. Garnelo et al. // Nature. 2022. 12:8638. DOI: https://doi.org/10.1038/s41598-022-12547-0 (дата обращения: 07.09.2022)

7. Li J. Graph enhanced BERT for query understanding / Li J., Ma Y., Zeng W. et al. arXiv preprint. 2022. 10 pp. URL: https://arxiv.org/pdf/2204.06522.pdf (дата обращения: 07.09.2022)

8. Запечников С.В. К вопросу определения предметной области информационной безопасности технологий искусственного интеллекта / С. Запечников, А. Щербаков // Вестник современных цифровых технологий. № 8. 2021. С.5 – 16.

УДК: 004.315.5

Применение системы остаточных классов для повышения эффективности операции умножения с накоплением[1]

V.A. Kuchukov, N.N. Kucherov

The Application of a Residue Number System to Improve the Efficiency of Multiplication with Accumulation

Abstract. *Multiplication with Accumulation (MAC) is one of the basic operations of digital signal processing, artificial neural networks. The paper considers the hardware implementation of this arithmetic operation for the positional number system and proposes the use of a residue number system (RNS) to increase the speed of computation. The non-positional structure of RNS at the expense of absence of transfers between discharges allows to carry out calculations in parallel. We consider the process of finding the remainder of division by modules of a special form 2^n-1, 2^n, 2^n+1 using the period and half-period of numbers, as well as a neural network of a finite ring. Using a modification of the method based on the period and half-period of a number allows to obtain a complete system of least nonnegative residues, necessary for further multiplication and addition. A MAC simulation has been performed for various sets of RNS modules from 8 to 64 bits with different numbers of modules. It is shown that on a range from 16 bits the RNS allows a 1.5-fold reduction in computation time, required power, and used area.*

Keywords: *residue number system, multiplication with accumulation, application-specific integrated circuits.*

В.А.Кучуков[1]
Н.Н.Кучеров[2]
[1]Северо-Кавказский центр математических исследований, Северо-Кавказский федеральный университет.
E-mail: vkuchukov@ncfu.ru
[2]Северо-Кавказский федеральный университет.
E-mail: nik.bekesh@mail.ru

Аннотация. *Умножение с накоплением (Multiplication with Accumulation, MAC) является одной из основных операций цифровой обработки сигналов, искусственных нейронных сетей. В статье рассмотрена аппаратная реализация данной арифметической операции для позиционной системы счисления и предложено использование для увеличения скорости вычисления системы остаточных классов (СОК). Непозиционная структура СОК за счет отсутствия переносов между разрядами позволяет проводить вычисления параллельно. Рассмотрен процесс нахождения остатка от деления на модули специального вида 2^n-1, 2^n, 2^n+1 с использованием периода и полупериода чисел, а также нейронной сети конечного кольца. Использование модификации метода на основе периода и полупериода числа позволяет получить полную систему наименьших неотрицательных вычетов, необходимую для дальнейшего умножения и сложения. Моделирование MAC было проведено для различных наборов модулей СОК от 8 до 64 бит с различным количеством модулей. Показано, что на диапазоне от 16 бит СОК позволяет в 1,5 раза сократить время вычислений, требуемую мощность и используемую площадь.*

Ключевые слова: *система остаточных классов, умножение с накоплением, интегральные схемы специального назначения.*

1. ВВЕДЕНИЕ

Многие современные высокоскоростные двоичные процессоры используют специализированные инструкции, такие как умножение и накопление. Кроме того, специальные методы реализации функций умножения и накопления существуют для двоичных компьютеров, например, "объединенные" блоки умножения и накопления (MAC). Причина в том, что многие компьютерные вычисления требуют умножения двух операндов и добавления третьего операнда к результату умножения. Выполнение операции

$$P=C+A\times B \quad (1)$$

является основной операцией для задач цифровой фильтрации [1, 2], таких как очистка от шума, эквализация, при реализации нейронных сетей [3] и др.

В статье [4] рассмотрена реализация усеченного MAC для конвейерного выполнения умножения со сложением в рамках цифровой фильтрации. Для получения итогового результата, согласно формуле (1), нет необходимости выполнять полное умножение $A\times B$. Вместо этого достаточно использовать генератор k частичных произведений, где $k=\lceil \log_2 B \rceil$ бит

[1] Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации в рамках стипендии Президента СП-3186.2022.5 и гранта Президента МК-1203.2022.1.

– размерность коэффициента B, и дерево сумматоров с сохранением переноса (CSA) [5], без использования на каждом шаге конвейера конечного сложения сумматором Когге-Стоуна (KSA) [6].

В статье [3] рассмотрен блок MAC, сокращенно называемый ASM, который способен выполнять три режима умножения: (1) четыре умножения 4-бита × 16-бит, (2) два умножения 8- бит × 16-бит, и (3) одно умножение 16-бит × 16-бит. Несмотря на то, что ASM полностью использует свои внутренние ресурсы для таких операций, как умножения 4-бита × 16-бит, 8-бит × 16-бит, и 16-бит × 16-бит, выполнение умножения с 16-бит × n-бит, n=8,7,… является неэффективным, так как оно не полностью использует внутреннюю логику, соответствующую старшим разрядам точности или старшим битам операнда с фиксированной точностью.

Более того, в структуре ASM, при умножении происходит существенная трата вычислительных ресурсов даже при незначительной разнице между размерами входных битов (например, умножение 9 бит × 7 бит).

Аппаратная реализация MAC доступна, в частности, в рамках среды разработки Vivado Design Suite фирмы Xilinx и поддерживает умножение беззнаковых чисел размерностью от 1 до 52 бит и знаковых от 2 до 53 бит, а также сложение или вычитание беззнаковых чисел размерностью от 1 до 105 бит и от 2 до 106 для чисел со знаком. При этом размерность выхода может быть задана вручную и быть меньше необходимой [7]. В общем случае же размерность результата умножения равна сумме размерностей операндов, а размерность результата сложения равна максимальной размерности операнда, увеличенной на один.

Повышение эффективности вычисления умножения с накоплением возможно за счет использования непозиционных систем счисления, в которых нет необходимости учитывать межразрядные переносы. При выборе системы счисления можно непосредственно снизить количество операций, длину операндов, количество и/или длину глобальных соединений, что может привести к снижению площади, задержки и рассеивания мощности [8]. Далее статья организована следующим образом. В разделе 2 описаны основные положения системы остаточных классов. В разделе 3 рассмотрена реализация операции нахождения остатка от деления на модули специального вида. В разделе 4 рассмотрено моделирование операции умножения с накоплением для двоичной системы счисления и системы остаточных классов.

2. ОСНОВЫ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ

Одним из наиболее перспективных представлений чисел при параллельной обработке является использование непозиционных систем счисления, таких как система остаточных классов (СОК).

Если задан ряд положительных целых чисел $p_1,p_2,\ldots,p_n$, называемых модулями или основаниями системы, то под системой остаточных классов понимается система, в которой целое положительное число представляется в виде набора остатков по выбранным основаниям $X=(\alpha_1,\alpha_2,\ldots,\alpha_n)$, где $\alpha_i=X \bmod p_i$ для $i=1,2,\ldots,n$ [9].

Из теории чисел известно, что если модули p_i взаимно простые, то представление числа $X=\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ является единственным. При этом $X < P = p_1\, p_2 \ldots, p_n$, где P – динамический диапазон представления чисел.

Набор модулей СОК существенно влияет на сложность реализации арифметических операций, при этом есть несколько подходов к выбору модулей. Подход, рассмотренный в [10] и используемый при вычислениях на GPU, заключается в использовании в качестве модулей всех простых чисел из некоторого диапазона. Также часто используют модули специального вида, к которым можно отнести:

- чётные модули, которые являются степенями числа 2, т.е. $p=2^n$, которые, к сожалению, могут быть использованы только один раз;
- числа Мерсенна $p=2^n-1$, которые среди нечетных модулей легче всего реализовать аппаратно;
- числа вида $p=2^n+1$.

Выбор модулей должен учитывать комплексно операции прямого (из позиционной системы счисления (ПСС) в СОК) и обратного (из СОК в ПСС) преобразований, сложность выпол-

нения арифметических операций. Желательно, чтобы выбранные модули имели эффективные аппаратные реализации основных модулярных операций (по площади, времени, энергопотреблению).

Особенностью системы остаточных классов является возможность выполнения операций сложения, вычитания и умножения параллельно и независимо по каждому из модулей.

Для чисел $A=(a_1,a_2,...,a_n)$ и $B=(b_1,b_2,...,b_n)$ выполняется

$$C=A*B=(a_1*b_1,a_2*b_2,...,a_n*b_n),$$

где $\in\{+,-,\times\}$.

Однако столь удобной в одном отношении системе остаточных классов присущ ряд недостатков в других отношениях: трудность определения соотношений чисел по величине, определения выхода результата операции из диапазона и т.д.

Для того чтобы в системе остаточных классов можно было строить вычислительные машины, необходимо найти принципиальные пути преодоления этих трудностей и найти эффективные способы построения машинной арифметики.

3. РЕАЛИЗАЦИЯ ОПЕРАЦИИ НАХОЖДЕНИЯ ОСТАТКА ОТ ДЕЛЕНИЯ

Рассмотрим реализацию операции нахождения остатка от деления на специальные модули 2^n, 2^n-1, 2^n+1.

Нахождение остатка по модулю 2^n при аппаратной реализации не требует использования какой-либо логики. На вход подается число X размерности N бит, а на выход подаются младшие n бит входного числа.

В статье [11] показан следующий метод вычисления остатка по модулю p, названный нейронной сетью конечного кольца. Пусть входное число X задано в двоичной форме в следующем виде:

$$X=\sum_{i=0}^{N-1}2^i\{x_i\},$$

где $\{x_i\}$ – есть i-ый бит двоичного представления X. Тогда, используя свойства конечного кольца, можно получить, что

$$|X|_p=\left|\sum_{i=0}^{N-1}\left|2^i\right|_p\{x_i\}\right|_p. \quad (2)$$

Поскольку $|2^i|_p$ имеют период, (например, для модуля 3: $|2^0|_3=1$, $|2^1|_3=2$, $|2^2|_3=1$ и т.д. вычисление остатка можно свести к сложению с несколькими повторяющимися коэффициентами. Например, для модуля 3 коэффициентами будут 1 перед x с четными индексами и 0 перед x с нечетными индексами:

$$|X|_3=||8|_3\cdot x_3+|4|_3\cdot x_2+|2|_3\cdot x_1+|1|_3\cdot x_0|_3=$$
$$|2\cdot x_3+1\cdot x_2+2\cdot x_1+1\cdot x_0|_3.$$

Развитие этой идеи связано с периодом и полупериодом чисел [12].

Периодом $P(p)$ нечетного модуля p является минимальное расстояние между двумя последовательными степенями 2, для которых модуль равен единице, т.е.

$$P(p)=\min\{k\,|\,k>0 \text{ и } |2^k|_p=1\}.$$

Для заданного нечетного модуля p, если существует целое число k такое, что $|2^k|_p=-1$, то полупериодом $HP(p)$ является минимальное расстояние между последовательной парой чисел 1 и $p-1$ в последовательности $|2^k|_p$, т.е. $HP(p)=\min\{k\,|\,k>0 \text{ и } |2^k|_p=-1\}$.

Обратим внимание, что $|p-1|_p=-1$. Практическая значимость этих понятий заключается в следующих выражениях, где j – любое неотрицательное целое число:

$$|2^{jP(p)+i}|_p=|2^i|_p, \quad (3)$$
$$|2^{j\cdot HP(p)+i}|_p=(-1)^j\,|2^i|_p. \quad (4)$$

Используя формулу (2) и свойство $P(2^n-1)=n$, можно разбить исходное число X на $r=\lceil N/n\rceil$ блоков B_i, начиная с младшего значащего бита, т.е. $X=(B_{r-1}...B_1B_0)$, где $B_0=(x_{n-1}...x_1x_0)$, $B_1=(x_{2n-1}...x_{n+1}x_n)$ и т.д. Если N не делится на n, то блок B_{r-1} может быть дополнен нулями [12]. Тогда из (3) $|2^{jn}|_{2^n-1}=1$ и формулу (2) используя группировку по n бит вместо 1, можно переписать в следующем виде:

$$|X|_{2^n-1}=\left|\sum_{j=0}^{r-1}2^{j\cdot n}\cdot\{x_{2jn-1}\dots x_{jn+1}x_{jn}\}\right|_{2^n-1}=$$
$$=\left|\sum_{j=0}^{r-1}2^{j\cdot n}\cdot B_j\right|_{2^n-1}=\left|\sum_{j=0}^{r-1}B_j\right|_{2^n-1}. \quad (5)$$

Для модуля 2^n+1 также можно воспользоваться формулой, аналогичной (5), однако при использовании периода размеры блоков будут равны $P(2^n+1)=2n$. Это позволит уменьшить размерность числа, но не даст искомого результата. Для модуля 2^n+1 возможно использование полупериода, т.е. используя формулу (4) в формуле (2), получим:

$$|X|_{2^n+1} = \left|\sum_{j=0}^{r-1} 2^{j\cdot n}\cdot B_j\right|_{2^n+1} = \left|\sum_{j=0}^{r-1} (-1)^j B_j\right|_{2^n+1} \quad (6)$$

При этом в аппаратной реализации у каждого B_i необходим дополнительный бит для знака.

Вычисления по формулам (2), (5), (6) не всегда дают искомый результат в диапазоне $[0,p)$. Например, $|3|_3$ по формуле (2):

$3=1\cdot0+2\cdot1+1\cdot1=3$,

т.е. результат выполнения попадает в диапазон $[0,6)$, т.е. $[0,2p)$, а не в диапазон $[0,3)$.

Для нахождения остатка в диапазоне $[0,2p)$ в диссертации [13] рассмотрен следующий алгоритм нахождения остатка. Пусть задано число s и модуль p, причем $0\le s<2p$, а также $c=2^n-p$, где $2^n>p\ge2^{n-1}$, т.е. n – размерность модуля. Для нахождения остатка прибавим к s значение с, т.е. $t\leftarrow s+c$ и, если $t\ge2^n$, то $s\leftarrow t \bmod 2^n$. Полученный результат s и будет остатком от деления. Этот метод имеет эффективную аппаратную реализацию, т.к. нахождение остатка сводится к сложению и проверке старшего бита числа. Для модулей вида 2^n-1 значение параметра с будет равным 1, что еще упростит схему.

Сравним построение использование нейронной сети конечного кольца и периода для нахождения остатка по модулю $2^4-1=15$.

Весами нейронной сети для формулы (2) в данном случае будут $|2^{4\cdot i}|_{15}=1$, $|2^{4\cdot i+1}|_{15}=2$, $|2^{4\cdot i+2}|_{15}=4$, $|2^{4\cdot i+3}|_{15}=8$.

Период $P(2^4-1)=4$, таким образом, исходное число при использовании периода разбивается на блоки по 4 бита. Результаты моделирования представлены в таблице 1.

Таблица 1

Результаты моделирования нахождения остатка

	Площадь, μm²				Время, пс			
Размерность, бит	8	16	32	64	8	16	32	64
Нейронная сеть конечного кольца	1152	2424	4997	9990	1245	1893	2570	3505
Период числа	852	2022	4227	8772	1417	2407	2958	3495

При построении нейронной сети конечного кольца используются полусумматоры и сумматоры и площадь устройств получается несколько больше ввиду оптимизации элементной базы средой синтеза при построении устройства нахождения остатка с помощью периода числа.

Рассмотрим применение данных методов для построения умножителя с накоплением, работающего в системе остаточных классов.

4. МОДЕЛИРОВАНИЕ УМНОЖЕНИЯ С НАКОПЛЕНИЕМ

Моделирование умножения с накоплением было произведено на ASIC в среде RTL и физического синтеза Cadence Genus Synthesis Solution с использованием библиотеки osu018_stdcells. В качестве измеряемых показателей были выбраны время прохождения сигнала по схеме (пикосекунды, пс), требуемая мощность (ватт, Вт), а также используемая площадь (квад-

ратные микрометры, μm^2).

Для моделирования и сравнения был взят диапазон от 8 до 64 бит с шагом 8 бит. Для позиционной системы счисления взяты множители размером $n/2$ бит, слагаемое размером n бит, результат n бит для возможности конвейерной обработки с учетом, что старший $n+1$-й бит суммы отбрасывается (т.е. подразумевается, что результат сложения не выходит за диапазон n бит).

В системе остаточных классов наборы модулей выбирались так, чтобы для динамического диапазона P выполнялось условие $\lfloor \log_2 P \rfloor = n$ бит.

В качестве метода нахождения остатка от деления использован период числа ввиду простоты его реализации и масштабируемости. Реализация MAC в СОК использует вычисление умножения с последующим нахождением остатка при вычислении суммы. Псевдокод данной реализации представлен алгоритмом 1, где $A[a:b]$ означает выборку бит с a до b сигнал A.

Алгоритм 1. Умножение с накоплением по модулю $p=2^n-1$.

Input: $A,B,C \in [0,p)$

Output: $P=(A \cdot B+C) \bmod p$

1. $Mult=A \cdot B$
2. $Sum_1=Mult[n-1:0]+Mult[2n-1:n]+C$
3. $Sum_2=Sum_1[n-1:0]+Sum_1[n+1:n]$
4. $Sum_{out}=Sum_2+1$
5. **if** $Sum_{out}[n]=1$
   5.1. **return** $P=Sum_{out}[n-1:0]$
6. **else**
   6.1. **return** $P=Sum_2[n-1:0]$

Преимущества системы остаточных классов связаны с независимостью вычислений по каждому модулю, таким образом, взяты трех-, четырех-, пяти- и т.д. модульные наборы, чтобы максимально раскрыть потенциал параллелизма вычислений. Из таблицы 2 видно, что выигрыш во времени, площади и мощности растет с увеличением количества модулей и как следствие с уменьшением их размера.

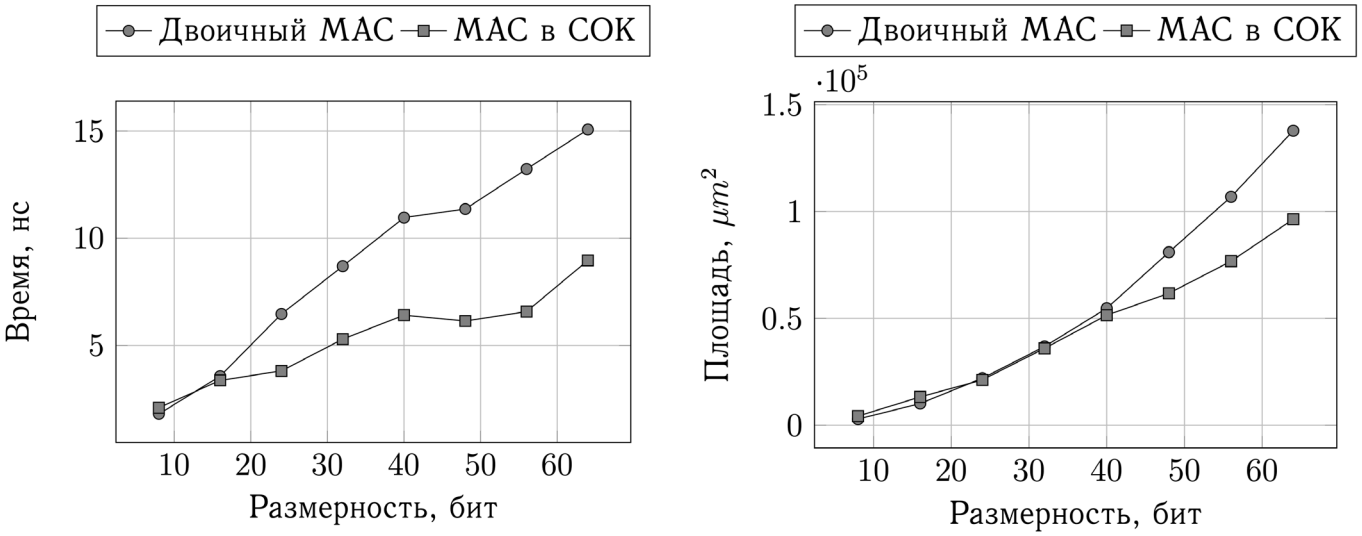
Таблица 2

Результаты моделирования MAC

Представление чисел	Время, пс	Мощность, Вт	Площадь, μm^2
8 бит			
Двоичное представление	1799	2,86E-04	2881
{3,5,32}	2087	4,57E-04	4282
{5,7,8}	2168	5,29E-04	4423
16 бит			
Двоичное представление	3563	1,13E-03	10132
{31,63,64}	4623	1,98E-03	14351
{7,9,17,64}	3366	1,59E-03	13241
24 бита			
Двоичное представление	6461	3,95E-03	22000
{255,257,512}	6576	4,83E-03	32284
{31,63,65,256}	5071	3,51E-03	25825
{5,7,9,17,31,128}	3807	2,66E-03	21229
32 бита			
Двоичное представление	8692	7,00E-03	36806
{1023, 2047, 4096}	9029	1,01E-02	47713

Представление чисел	**Время, пс**	**Мощность, Вт**	**Площадь, μm²**
{127, 255, 511, 512}	6154	6,57E-03	40409
{31, 63, 65, 127, 512}	5290	5,11E-03	35975
40 бит			
Двоичное представление	10959	1,10E-02	54686
{8191, 16383, 16384}	11518	1,80E-02	71198
{511, 1023, 2047, 2048}	9052	1,25E-02	60357
{127, 255, 257, 511, 512}	6576	8,99E-03	55403
{17,31,65,129,511,512}	6410	7,64E-03	51456
48 бит			
Двоичное представление	11359	1,43E-02	80942
{65535, 65537, 131072}	14767	2,49E-02	103205
{2047, 4095, 8191, 8192}	10290	2,08E-02	82370
{257, 511, 1023, 1025, 2048}	9233	1,40E-02	75995
{65, 127, 129, 257, 511, 2048}	6576	1,07E-02	68117
{17,31,65,127,129, 511,1024}	6137	9,24E-03	61729
56 бит			
Двоичное представление	13228	1,86E-02	106871
{262143, 524287, 1048576}	14403	3,37E-02	126156
{8191, 16383, 32767, 32768}	12362	2,75E-02	106798
{511, 1025, 2049, 8191, 16384}	10339	2,20E-02	99219
{127, 257, 511, 513, 2047, 8192}	8915	1,66E-02	88215
{31, 65, 127, 257, 513, 2047, 2048}	8972	1,52E-02	84918
{17, 31, 65, 127, 129, 257, 511, 1024}	6576	1,16E-02	76724
64 бита			
Двоичное представление	15068	2,46E-02	137773
{2097151, 4194303, 4194304}	16771	4,43E-02	162240
{32767, 65535, 131071, 131072	13287	3,63E-02	135746
{2047, 4097, 8191, 16383, 32768}	11539	2,97E-02	120158
{257, 511, 1025, 2049, 8191, 8192}	10386	2,40E-02	112625
{65, 127, 257, 511, 1023, 2047, 8192}	8962	1,80E-02	96373

Сравнение двоичной реализации MAC с реализациями в СОК представлено на рисунке 1, откуда видно, что начиная с 24 бит реализация с использованием системы остаточных классов выигрывает и по времени и площади.



а) Время вычислений, пс

б) Требуемая площадь, мкм^2

Рис. 1. Результаты моделирования MAC

ЗАКЛЮЧЕНИЕ

Применение системы остаточных классов со специальными модулями вида 2^n-1, 2^n, 2^n+1 с использованием периода числа позволяет на диапазонах от 16 бит сократить время выполнения в 1,68 раз, на диапазонах от 24 бит сократить требуемую мощность и площадь в 1,37 и 1,43 раза соответственно.

Как видно из таблицы 1, возможно дальнейшее улучшение за счет применения нейронной сети конечного кольца, которая позволит в некоторой степени объединить вычисления по разным модулям.

Анализ таблицы 2 показывает, что лучшие результаты достигаются СОК с большим количеством модулей, при этом стоит проблема их несбалансированности по размеру. Четырехмодульные наборы со сбалансированными модулями также дают преимущество по сравнению с двоичной реализацией, хотя и не такое явное.

Однако стоит учитывать, что данная реализация построена на стандартных конструкциях Verilog для сложения и умножения, и реализация MAC при помощи методов умножения с предсказанием переноса сократит время вычислений, пожертвовав при этом площадью и размерностью устройства.

Таким образом, показана применимость системы остаточных классов для выполнения умножения с накоплением, при котором вычисления с большими числами разбиваются на блоки, реализующие параллельное выполнение вычислений с числами меньшей разрядности. Так, для 64-битных чисел размеры модулей ограничены 11 битами для нечетных модулей и 13 битами для модуля вида 2^n.

Направлением дальнейших изысканий может быть разработка и исследование методов обратного преобразования для данных наборов модулей, а также реализация немодульных операций, таких как сравнение чисел и определение знака числа.

Благодарность. Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации в рамках стипендии Президента СП-3186.2022.5 и гранта Президента МК-1203.2022.1.

СПИСОК ЛИТЕРАТУРЫ

1. Rakesh, H.; Sunitha, G.S. Design and Implementation of Novel 32-Bit MAC Unit for DSP Applications. In Proceedings of the 2020 International Conference for Emerging Technology, Belgaum, India, 5–7 June 2020; pp. 1–6.

2. Patil, P.A.; Kulkarni, C. Multiply Accumulate Unit Using Radix-4 Booth Encoding. In Proceedings of the 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 14–15 June 2018; pp. 1076–1080.

3. Kang J., Kim T. PV-MAC: Multiply-and-accumulate unit structure exploiting precision variability in on-device convolutional neural networks //Integration. – 2020. – Vol. 71. – pp. 76-85.

4. Lyakhov P. et al. A method of increasing digital filter performance based on truncated multiply-accumulate units //Applied Sciences. – 2020. – Vol. 10. – №. 24. – p. 9052.

5. Parhami, B. Computer Arithmetic: Algorithms and Hardware Designs; Oxford University Press: Oxford, UK, 2010; ISBN 9780195328486.

6. Kogge, P.M.; Stone, H.S. A Parallel Algorithm for the Efficient Solution of a General Class of Recurrence Equations. IEEE Trans. Comput. 1973, 786–793. DOI: 10.1109/TC.1973.5009159

7. Multiply Adder v3.0. LogiCORE IP Product Guide. Vivado Design Suite. Xilinx. URL: https://www.xilinx.com/content/dam/xilinx/support/documents/ip_documentation/xbip_multadd/v3_0/pg192-multadd.pdf

8. Patronik P., Piestrak S. J. Design of Reverse Converters for General RNS Moduli Sets "\\\{"2^k,2^n–1,2^n+1,2^{n-1}–1"\\\}" and "\\\{" 2^k,2^n–1,2^n+1,2^{n+1}–1"\\\}" (n even)}, Circuits and Systems I: Regular Papers, IEEE Transactions on 61.6 (2014), 1687--1700.

9. Акушский И. Я., Юдицкий Д. И. Машинная арифметика в остаточных классах. – Сов. радио, 1968.

10. Phatak, D.S. New distributed algorithms for fast sign detection in residue number systems (RNS)/ D.S. Phatak, S.D. Houston // Journal of Parallel and Distributed Computing. – 2016. – Vol. 97. – pp. 78-95.

11. Zhang D., Jullien G. A., Miller W. C. A neural-like network approach to finite ring computations, Circuits and Systems, IEEE Transactions on 37.8 (1990), p. 1048-1052

12. Piestrak S. J. Design of multi-residue generators using shared logic, Circuits and Systems (ISCAS), 2011 IEEE International Symposium on. IEEE, (2011), p. 1435-1438

13. Plantard T. Arithmetique modulaire pour la cryptographie, Doctoral dissertation, Universite Montpellier II-Sciences et Techniques du Languedoc, 2005

Приглашаем авторов к участию в журнале «Вестник современных цифровых технологий»

ИНФОРМАЦИЯ ДЛЯ АВТОРОВ

Редакция принимает материалы статей, соответствующие тематике журнала, содержащие новые научные результаты, не опубликованные ранее и не предназначенные к публикации в других печатных или электронных изданиях. Проводится независимое внутреннее рецензирование. Статьи в журнале публикуются бесплатно (объем – до 15 тыс. знаков), после получения одобрения Редакционного совета.

Для опубликования статьи в редакцию журнала необходимо направить по адресу *accda@c3da.org, info@c3da.org* **следующие материалы в электронном виде:**

• рукопись статьи в DOC- и PDF-форматах;
• иллюстрации, предоставленные также и отдельными файлами в формате JPG или PNG с разрешением 72 dpi;
• сведения об авторах, содержащие фамилию, имя, отчество, ученые степень и звание, должность, место работы, контактные телефоны или E-mail;
• англоязычную информацию, содержащую название статьи, ФИО авторов, аннотацию и ключевые слова;
• редакция может запросить экспертное заключение о возможности публикации статьи в открытой печати.

ПОСЛЕДОВАТЕЛЬНОСТЬ МАТЕРИАЛОВ ДЛЯ ПУБЛИКАЦИИ:

1. шифр УДК (см. Справочник УДК) в левом верхнем углу;
2. название статьи (полужирным шрифтом по центру) не более 12 слов;
3. инициалы и фамилия автора (полужирным шрифтом по центру), к каждому автору - сноска, содержащая ученое звание, должность, название организации (без сокращений), e-mail;
4. Аннотация, излагающая суть работы и полученные результаты (5-7 строк);
5. ключевые слова (8-10 слов);
6. англоязычная информация по статье (по пп.2-5)
7. текст статьи с учетом указанных далее требований к его оформлению;
8. список литературы, оформленный по ГОСТ Р 7.0.5-2008.

Статья должна быть структурирована, т.е. должна включать разделы с названиями, кратко и точно отражающими их содержание, в том числе:

• введение, содержащее обоснование актуальности и краткий обзор проблематики;
• четкую постановку задачи исследования;
• описание метода решения задачи исследования;
• прикладную интерпретацию и иллюстрацию полученных результатов исследования;
• заключение, включающее обобщение и указание области применения полученных результатов, не повторяющее аннотацию и не ограничивающееся простым перечислением того, что сделано в работе.

С детальными требованиями к рисункам, таблицам, формулам, списку литературы, а также с примерами оформления статьи можно ознакомиться на странице Вестника http://c3da.org/journal.html.

Приглашается к сотрудничеству редактор для работы в редакции журнала по совместительству.
Просьба направлять резюме по электронному адресу *accda@c3da.org, info@c3da.org*

ТРЕБОВАНИЯ К РЕДАКТОРУ:

• отличное знание русского языка;
• свободное владение ПК, в том числе специальными текстовыми и графическими программами;
• опыт работы в издательстве.

Высшее техническое образование и знание английского языка являются существенными преимуществами.

ОБЯЗАННОСТИ

Редактор:
• редактирует рукописи, принятые к изданию;
• оказывает авторам необходимую помощь по улучшению структуры рукописей, выбору терминов, оформлению иллюстраций;
• проверяет, насколько учтены авторами замечания по доработке, предъявленные к рукописям;
• подписывает отредактированные рукописи в печать.