ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ
(ВАК – 05.13.00)
6. 2021 (МАРТ)

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

www.c3da.org

№6
МАРТ 2021

ISSN 2686-9373

Издатель: *Ассоциация специалистов в области развития криптовалют и цифровых финансовых активов*
Центр развития криптовалют и цифровых финансовых активов
Адрес редакции и издателя: 125315, Москва, Усиевича, 20, каб. 207
Тел/факс: *8 (499) 155-43-26*
E-mail: accda@c3da.org
info@c3da.org

Подписано в печать 25.03.2021 г.

Тираж 500 экз.

Подписной индекс в каталоге «Пресса России»: 79111

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

РЕДАКЦИОННЫЙ СОВЕТ

СОДЕРЖАНИЕ

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Шестой номер «Вестника современных цифровых технологий» в основном посвящен темам искусственного интеллекта, цифровой медицины и безопасности промышленных технологий.

В разделе «Государство и цифровые технологии» опубликован материал **«Три года Центру развития криптовалют и цифровых финансовых активов: достижения, размышления и перспективы»**, прозвучавший в виде сообщения руководителя ЦРКЦФА Щербакова А.Ю. на Ученом совете ВИНИТИ РАН 26 января 2021 г.

Материал подводит промежуточные итоги работ по государственному заданию 2019-2020 гг. и описывает методологию научных работ по теме «Исследования в области перспектив развития технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации (тема 0003-2019-0007)».

В традиционном разделе «Фундаментальные проблемы цифровых технологий» представлена статья **«Доказательства с нулевым разглашением и их применения при обработке информации в недоверенных средах»** Сергея Запечникова, посвященная анализу методических и практических аспектов использования доказательств с нулевым разглашением в компьютерных системах различного назначения. В статье рассматриваются типовые модели вычислений в недоверенных средах, дается обзор применения доказательств с нулевым разглашением в системах распределенного реестра и системах конфиденциального машинного обучения, приводятся актуальные проблемы теории доказательств с нулевым разглашением и практики их применения.

Раздел «Цифровые технологии в промышленности» представлен статьей **«Тенденции развития и практические реализации решений по обеспечению безопасности криптографических сетей»**. В статье рассмотрены современные тренды в обеспечении безопасности сетей передачи данных и обеспечения безопасности бизнес-процессов, сформулированы понятия и свойства криптографических сетей, рассмотрены понятия сервисной модели и ключевых контейнеров с опорой на развитие квантово-защищенных сетей, описано практическое решение и его архитектура.

В разделе «Цифровые технологии в биологии и медицине» представлена работа **«Новые подходы к акустическому анализу состояния организма человека»** коллектива авторов. Статья посвящена формулированию и обсуждению нового подхода к изучению акустической картины организма человека при помощи регулярной структуры микрофонов, представляющих собой аналог фазированной приемной антенной решетки, и дальнейшей обработки информации при помощи математических методов цифровой медицины. Особое внимание уделяется пассивным методам получения информации о внутренних процессах в организме человека, связанных с излучением акустических колебаний от внутренних органов.

Как мы уже отмечали, основные тренды цифровой медицины направлены на разработку и продвижение неинвазивных решений.

Раздел **«Беседы с основоположниками»** рассматривает очень интересную и актуальную тему современной науки и техники - искусственный интеллект, его место в создании новых технологий, перспективы и пути его развития. С главным редактором нашего журнала беседует Светлана Алексеевна Бородулина, Председатель Правления Евразийского Делового совета, в недавнем прошлом - министр топлива и энергетики Республики Крым.

Раздел «Философские проблемы цифровых технологий» продолжается статьей Олега Тихоненко **«Семантика языка как источник откровения»** из цикла исследований по смыслу букв первичного языка, на котором были записаны тексты Библии.

Рассказ **«Гросс»** белорусского прозаика Егора Федорова в разделе «Литература о цифровых технологиях» завершает наш номер. Затейливые сюжетные линии рассказа переплетают цифровые медицинские технологии, изучение склонностей детей и тонкости шахматной игры. Вместе с автором рассказа редакция полна оптимизма во взглядах на будущее, на таланты и назначение человека.

Три года Центру развития криптовалют и цифровых финансовых активов: достижения, размышления и перспективы

А.Ю. Щербаков

Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник ЦРКЦФА, ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: x509@ras.ru

Данный материал, прозвучавший в виде сообщения начальника ЦРКЦФА Щербакова А.Ю. на Ученом совете ВИНИТИ РАН 26 января 2021 г., подводит промежуточные итоги работ по государственному заданию 2019-2020 гг. и описывает методологию научных работ по теме «Исследования в области перспектив развития технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации (тема 0003-2019-0007)».

Напомним кратко об истории, области деятельности и миссии Центра развития криптовалют и цифровых финансовых активов.

Центр был создан в апреле 2018 года в рамках ВИНИТИ РАН при поддержке ФАНО РФ. Основной задачей Центра является выполнение программы «Цифровая экономика Российской Федерации, утвержденной распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 1632-Р, в части научно-методологического обеспечения работ в области разработки и использования цифровых финансовых активов и технологий распределенных реестров.

В рамках Центра собран коллектив ведущих российских ученых и практиков, занимающихся решением актуальных теоретических проблем цифровой экономики, организацией и координированием научных работ, в том числе и с международным участием.

Стратегическими партнерами Центра являются Российская ассоциация криптоиндустрии и блокчейна (РАКИБ), Российский государственный университет нефти и газа имени И. М. Губкина (Факультет комплексной безопасности ТЭК), Сберегательный банк РФ, Ассоциация кластеров и технопарков России (ООО «Техпромбизнес»), Институт точной механики и вычислительной техники им. С.А.Лебедева, группа компаний «Инфовотч», институт точной механики и оптики (ИТМО, г. Санкт-Петербург), Федеральный центр образовательного законодательства, Ресурсный центр универсального дизайна и реабилитационных технологий ФГАУ «РЦУД и РТ».

Основная миссия Центра - создание благоприятной научно-образовательной среды в области цифровой экономики, выполнение и поддержка научных и практических национально-значимых проектов, обеспечивающих стратегический паритет отечественной науки в области информационных технологий, искусственного интеллекта, систем обработки больших данных и распределенных реестров, цифровых активов - в течение трех лет работы ЦРКЦФА успешно выполнялась.

Центр также успешно проводил работы по поддержке сертификации безопасности решений в области цифровой экономики в сотрудничестве с уполномоченными организациями РФ.

При ЦРКЦФА действует Координационный совет, предназначенный для определения стратегии развития и координации усилий Центра с другими государственными и общественными организациями.

При участии Центра развития криптовалют и цифровых финансовых активов издается жур-

нал «Вестник современных цифровых технологий».

В 2020 г. была создана Ассоциация специалистов в области развития криптовалют и цифровых финансовых активов, которая также сотрудничает с ЦРКЦФА.

В течение 2020 года ЦРКЦФА продолжал выполнение работ по государственному заданию «Исследования в области перспектив развития технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации».

Необходимо отметить, что работы по государственному заданию связаны с принципиальными особенностями - рассмотрение перспектив развития указанных технологий определяет мультидисциплинарность исследований, а также требует постоянного учета отечественного и зарубежного опыта и тенденций.

В свою очередь применение результатов исследований в сфере цифровой трансформации технологий и экономики, в частности, путем практической реализации разработанных алгоритмов и методов, обуславливает поддержание контактов с технологическими лидерами и уполномоченными государственными органами-регуляторами, участие в законодательной и нормотворческой работе.

«Карта мультидисциплинарности» работ по государственному заданию тесно связана с понятием платформ, которые изучались как в рамках государственного задания, так и в рамках самостоятельных грантов РФФИ. Понятийные вопросы цифровых платформ, включая их основные понятия и свойства, а также их интегративный потенциал, позволяют создать общую методологическую основу для проведения фундаментальных исследований.

В новейшее время, после перехода коммуникаций в цифровую плоскость, понятие платформы появилось также и в области информационных технологий (коммуникационная платформа или цифровая платформа). При этом "платформа" в узком смысле представляет собой сочетание аппаратного и связующего программного обеспечения (операционной системы) персонального компьютера, необходимое для воспроизведения прикладных программ, или аппаратно-программный комплекс с базовым набором сервисов, выполняющих определённые задачи.

Кроме того, платформы выделяют также по отдельным функциональным признакам, в таком случае они составляют основу для обеспечения выполнения функций субъектами (передача данных для транспортной платформы, управление сетью для административной платформы, исполнение программного кода для процессора и др.).

Платформа в сфере цифровой трансформации технологий и экономики может представлять собой единый научно-обоснованный технологический комплекс, который, кроме обеспечения целевой функции платформы, позволит расширить ее сервисы в рамках разрабатываемой сервисной модели. Одной из базовых функций современных цифровых платформ является функция безопасной передачи данных.

В связи с этим в рамках фундаментальных исследований Центра была подробно рассмотрена проблема интеграции систем квантовых коммуникаций в платформенные решения цифровых технологий, которые используют криптографические механизмы для обеспечения собственно функциональности, а также проиллюстрирован тезис о том, что трендом развития парадигмы безопасности распределенных недоверенных систем является переход от алгоритмической безопасности к синергии технических и криптографических решений.

Для придания платформам «активного статуса» предложена концепция выполнения смарт-контрактов. Считается, что неотъемлемой частью общего пула блокчейн-технологий является технология смарт-контрактов. Однако можно полагать, что применение смарт-контрактов как механизма расширения функциональности и интеграции платформ не относится только к блокчейн-технологиям и может быть спроецировано на более широкий класс платформенных решений.

Весьма важным для цифровой трансформации является недавно возникшая проблема обеспечения конфиденциальности в машинном обучении. Актуальность проблемы опре-

деляется возрастающими потребностями в использовании методов машинного обучения для хранения и обработки персональных данных в рамках платформенных решений, а также данных, составляющих коммерческую, медицинскую, финансовую и иные охраняемые законом виды тайн.

Цели данных работ заключаются в систематизации моделей обеспечения безопасности машинного обучения, выявлении алгоритмических инструментов, которые могут быть использованы для обеспечения конфиденциальности в процессе обучения и применения моделей, сравнительном анализе систем конфиденциального машинного обучения.

В рамках работ Центра в 2020 г. был рассмотрен и новый подход к обеспечению безопасности бизнес-процессов, гарантирующий невозможность передачи конфиденциальной информации за периметр безопасности организации, опирающийся на применение модулей хранения пользовательских ключей. Эта проблема также тесно связана с цифровыми платформами, поскольку необходимо обеспечить такие базовые свойства платформ, как замкнутость и защищенность.

Одной из важных методологических проблем в работах Центра является рассмотрение платформы как киберфизической системы. В истекшем году исследовались вопросы описания функционирования киберфизических систем с целью получения их различных характеристик.

Была выдвинута гипотеза о том, что обнаружение негативного воздействия на работу киберфизических систем и платформ возможно через выявление отклонения от стационарных характеристик, описываемых квазианалитической зависимостью. На основании обработки результатов эксперимента было показано, что для киберфизических систем характеристики имеют периодическую зависимость. Предложена реализация полученного метода на платформе «Прогнотех», описаны ее преимущества. «Киберфизичность» системы или платформы важна не только с точки зрения того, что в рамках платформы циркулирует или обрабатывается информация о производственных процессах, но и с той точки зрения, что аппаратная компонента платформ сама является киберфизической системой.

В рамках практической апробации задач в сфере цифровой трансформации технологий часть работ Центра посвящена проблеме повышения надежности и безопасности протекания бизнес-процессов организаций топливно-энергетического комплекса (ТЭК) и в частности - нефтегазовой отрасли. Работы проводились в научно-методическом сотрудничестве с Университетом нефти и газа им. Губкина. Рассмотрены возможности применения технологий распределенных реестров в основных сферах нефтегазового производства. Проанализированы сферы, в которых их применение может привести к повышению безопасности. Сделаны выводы о том, что технологии распределенных реестров обладают большим потенциалом для роста, усовершенствования в области ТЭК действующих механизмов и создания новых, более эффективных.

Необходимость мультидисциплинарного синтеза указанных выше тем в рамках выполнения государственного задания объясняется влиянием на технологии распределенных реестров как информации, обрабатываемой в конкретной киберфизической системе, так и процессов обеспечения информационной безопасности, связанных с технологией обработки и хранения информации. Данные темы позволят дополнить системный подход к развитию технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации.

Весьма важным научным достижением является разработка нового подхода к реализации трансграничной проверки электронных подписей (ЭП). Задача взаимной проверки ЭП, сформированных по различным алгоритмам в различных юрисдикциях, является в настоящее время весьма актуальной и, к сожалению, пока технически нерешенной.

Предполагается, что несколько участников системы относятся к различным государствам (юрисдикциям) и имеют различные алгоритмы и ключи электронной подписи. Для них необходима общая возможность подтвержде-

ния документов, подписанных электронными подписями. Классическое решение вопроса, связанное с созданием единого доверенного удостоверяющего центра практически невозможно, поскольку затруднительно выработать общие технические и юридические регламенты его работы.

Кроме того, в силу закрытости процедур оценки качества криптографических механизмов, стороны находятся в весьма затруднительном положении относительно опубликования результатов криптографических исследований качества ЭП. При этом оценке подвергаются как совокупность алгоритмов ЭП, так и свойства удостоверяющего центра, который формирует сертификаты - подписывает своей ЭП открытые ключи пользователей (участников системы).

Решение этой весьма актуальной задачи находится в сфере применения технологий распределенного реестра для участников системы.

Специалистами Центра рассмотрены также экономические основы виртуальных платежных систем на основе распределенных реестров. Актуальность этой темы определяется тем, что системы распределенных реестров проектируют в мире по большей части, как приватные и корпоративные сети с ограниченным числом участников, имеющих доступ к общей системе журналирования или организации обмена сообщениями, а также определенные правила и инструменты внесения и хранения записей, включающие протоколы консенсуса, верификационные ноды, инфраструктуру. Показано, что важнейшей проблемой в использовании приватных (корпоративных распределенных реестров) является обеспечение безопасности транзакций.

Исследования Центра в области криптографических технологий носили в истекшем году интегрирующий характер и были посвящены криптографическим методам защиты информации в системах распределенного реестра. Проведен анализ практики применения криптографических методов защиты информации в современных системах распределенного реестра. Выделены основные задачи обеспечения безопасности информации в системах распределенного реестра и средства их решения.

Важное место в работах Центра занял процесс развития и апробации технологии управления цифровыми активами. В соответствии с ФЗ «О цифровых финансовых активах вводится понятие «цифровой финансовый актив» – это имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств. Права собственности на данное имущество удостоверяются путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта и токен.

Далее вводится понятие оператора обмена цифровых финансовых активов, который является юридическим лицом, осуществляющим сделки по обмену цифровых финансовых активов одного вида на цифровые финансовые активы другого вида и/или обмену цифровых финансовых активов на рубли или иностранную валюту.

Кроме того, согласно терминам, предлагаемым в законе, вводится понятие «цифровой кошелек». Цифровой кошелек - программно-техническое средство, позволяющее хранить информацию о цифровых записях и обеспечивающее доступ к реестру цифровых транзакций.

Цифровой кошелек открывается оператором обмена цифровых финансовых активов только после прохождения процедур идентификации его владельца в соответствии с Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». В предлагаемой концепции цифровой кошелек фигурирует в виде «криптовалютного кошелька». Требование процедур идентификации владельца предопределяет необходимость шагов по формированию процедур управления цифровым активом, связанных с выпуском соответствующих цифровых сертификатов. Все требования закона были интегрированы ЦРКЦФА в виде концепции и макета системы управления цифровыми активами, отраженными в отчете по государственному заданию и публикациях.

Резюмируя, можно заметить, что мультидисциплинарный синтез указанных выше тем, рассмотренных ЦРКЦФА в течение 2020 года в рамках выполнения государственного задания,

обусловлен влиянием на технологии распределенных реестров как информации, обрабатываемой в конкретной системе, так и процессов обеспечения информационной безопасности, связанных с технологией обработки и хранения информации, включая специфичные цифровые активы.

Данные темы позволят развить и дополнить системный подход к развитию технологий цифровых финансовых активов (криптовалют) и распределенных реестров (блокчейн) для их применения в сфере цифровой трансформации технологий и экономики Российской Федерации.

Наиболее значимые научные публикации сотрудников Центра

Правиков Д.И., Щербаков А.Ю. Изменение парадигмы информационной безопасности // Системы высокой доступности. 2018. Т. 14. № 2. С. 35-39.

Домашев А.В., Щербаков А.Ю. Реализация инфраструктуры процессинга цифровых активов // Системы высокой доступности. 2018. Т. 14. № 2. С. 23-28.

Щербаков А.Ю. О разработке средств для формирования корпоративного распределенного реестра (блокчейн) // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2018. № 4. С. 30-34.

Гриняев С.Н., Злотин Р.А., Милушкин А.И., Правиков Д.И., Селионов И.А., Щербаков А.Ю., Щуко Ю.Н. К вопросу о создании универсального защищенного доверенного цифрового актива (токена) // Научно-техническая информация. Серия 2: Информационные процессы и системы. 2018. № 10. С. 20-28.

Касперская Н.И., Кузьменко В.В., Мананников Д.А., Хайретдинов Р.Н., Щербаков А.Ю. К проблеме оценки и обеспечения корректности бизнес-процессов // Безопасность информационных технологий, том 26, № 3, 2019. С. 8-21.

Касперская Н.И., Кузьменко В.В., Хайретдинов Р.Н., Щербаков А.Ю. О подходах к созданию универсального доверенного распределенного реестра, обеспечивающего неразглашение данных о системе // Безопасность информационных технологий = IT Security. Том 26. № 1. 2019. С. 6-19.

Щербаков А.Ю., Булыгин А.И., Рябков В.Е., Елизарова А.С. Исследование вопросов применения технологий цифровизации на примере цифрового рейтинга студента // Вопросы кибербезопасности. 2019. №3 (30). С. 33-38.

Щербаков А.Ю. Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН как инструмент решения научно-методических проблем в сфере цифровой трансформации // Вестник современных цифровых технологий. 2019. №1. С. 54-55.

Домашев А.В., Щербаков А.Ю. Международный консенсус как развитие парадигмы консенсуса // Вестник современных цифровых технологий. 2019. №1. С. 48-53.

Рязанова А.А., Щербаков А.Ю. Искусственный интеллект как феномен имитации // Вестник современных цифровых технологий. 2019. №1. С. 56-61.

Гриняев С.Н., Правиков Д.И., Щербаков А.Ю., Фомин А.Н. Основы общей теории киберпространства // Электронные финансы и новая экономика. Автономная некоммерческая организация "Центр стратегических оценок и прогнозов", Москва. ISBN: 978-5-906661-22-7

Гостев С.С., Гриняев С.Н., Щербаков А.Ю., Правиков Д.И. К развитию методологии создания доверенных и защищенных информационных систем, построенных с использованием технологии распределенных реестров // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. 2019. № 3-2. С. 10-15.

Запечников С.В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий = IT Security. Том 27. № 1. 2020. С. 51-67.

Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра // Научно-техническая информация, сер. 2 Информационные процессы и системы. 2020. №1. С. 11-18.

Рязанова А.А. Концепция цифровых платформ как подход к интеграции научно-информационных процессов // Научно-техническая информация, сер. 2 Информационные процессы и системы. 2020. №12. С. 9-15.

Запечников С.В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций // Безопасность информационных технологий. 2020. Том 27. №4. С. 108-123.

Bobrysheva J., Zapechnikov S. Post-quantum group key agreement scheme // Advances in Intelligent Systems and Computing. Springer, Cham. 2020. 6 pp. (Scopus)

Щербаков А.Ю. Перспективы современной криптографии // Проектирование будущего. Проблемы цифровой реальности. 2020. № 1 (3). С. 227-233.

Щербаков А.Ю. Комплексный подход к созданию платформы доверенного документооборота с электронной подписью // Научно-техническая информация, сер. 2 Информационные процессы и системы. 2020. №11. С. 24-29.

Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Об одном способе хранения и управления ключами в системах квантовых коммуникаций // Вестник современных цифровых технологий. 2020. № 2. С. 14-20.

УДК: 004.75, 004.41

Доказательства с нулевым разглашением и их применения при обработке информации в недоверенных средах*

S. Zapechnikov

Zero-Knowledge Proofs and Their Applications for Information Processing into Untrusted Environments *

Abstract. *The article is devoted to the analysis of methodological and practical aspects of using in computer systems one of the most important cryptographic primitives – zero-knowledge proofs. A brief description of the main stages of zero-knowledge concept, the typology and characteristics of the properties of the most commonly used zero-knowledge proof systems are given. The article discusses typical models of computing in untrusted environments, and describes the information security requirements for these models. As examples, applications of zero-knowledge proofs in two areas are given: in distributed registry systems and privacy-preserving machine learning systems. In the final part of the article, current problems of the theory of zero-knowledge proofs and the practice of their application are considered.*

Keywords: *probabilistic proofs, zero-knowledge proofs, cryptography, distributed ledgers, blockchain, privacy-preserving machine learning.*

С.В. Запечников [1,2]

[1] Доктор технических наук, профессор, главный научный сотрудник Института интеллектуальных кибернетических систем, Национальный исследовательский ядерный университет «МИФИ»

[2] Вице-президент по научной работе Ассоциации специалистов в области криптовалют и цифровых финансовых активов

E-mail: SVZapechnikov@mephi.ru

Аннотация. *Статья посвящена анализу методических и практических аспектов использования в компьютерных системах различного назначения одного из важных криптографических примитивов – доказательств с нулевым разглашением. Приводится краткая характеристика основных этапов развития концепции нулевого разглашения, типология и характеристика свойств наиболее употребительных систем доказательства с нулевым разглашением. В статье рассматриваются типовые модели вычислений в недоверенных средах, дается характеристика требований по информационной безопасности для этих моделей. В качестве примеров дается обзор применения доказательств с нулевым разглашением в двух сферах: в системах распределенного реестра и системах конфиденциального машинного обучения. В заключительной части статьи рассматриваются актуальные проблемы теории доказательств с нулевым разглашением и практики их применения.*

Ключевые слова: *вероятностные доказательства, доказательства с нулевым разглашением, криптография, системы распределенного реестра, блокчейн, конфиденциальное машинное обучение.*

ВВЕДЕНИЕ

В последнее время во многих сферах человеческой деятельности резко возрастают масштабы дистанционного предоставления информационных услуг. Используемые для этого технические решения: облачные центры обработки данных, системы распределенного реестра, системы федеративного машинного обучения и др. – как правило, не пользуются доверием со стороны пользователей, а часть обрабатываемой информации содержит сведения, относимые к персональным данным, а также к охраняемым законом видам тайны: коммерческой, банковской, врачебной и пр. Как следствие, такая информация может обращаться в распределенных системах лишь в зашифрованном виде, что подразумевает не только хранение и передачу, но и обработку зашифрованных данных и метаданных. Современные криптографические методы защиты информации позволяют реализовать модель полного жизненного цикла обращения зашифрованных данных для многих частных задач, однако общая проблема обработки зашифрованных данных пока находится в стадии решения [1]. К данной проблеме относится обеспечение гарантий конфиденциальности, корректности, достоверности обработки зашифрованных данных. Одним из основных инструментов обеспечения таких гарантий выступают веро-

* Благодарности. Работа выполнена при поддержке Министерства науки и высшего образования РФ (проект государственного задания № 0723-2020-0036).

*Acknowledgement. This work was supported by the Ministry of Science and Higher Education of the Russian Federation (state assignment project No. 0723-2020-0036)

ятностные криптографические доказательства, и в первую очередь, доказательства с нулевым разглашением (zero-knowledge proofs).

ИСТОРИЯ РАЗВИТИЯ ТЕОРИИ ДОКАЗАТЕЛЬСТВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Теория вероятностных криптографических доказательств появилась в середине 1980-х гг. как одна из ветвей теории криптографических протоколов и за 35 лет своего развития превратилась в одну из важнейших алгоритмических стратегий решения сложных задач криптографии. Вероятностные криптографические доказательства, наряду со схемами шифрования, схемами электронной цифровой подписи, схемами аутентификации сообщений, стали одним из фундаментальных криптографических примитивов – «строительных блоков» более сложных алгоритмических конструкций. Отличительной особенностью вероятностных криптографических доказательств, в отличие от классических детерминированных доказательств математической логики, является возможность строить системы доказательства фактов и отношений для задач, не решаемых за полиномиальное время. При этом допускается пренебрежимо малая вероятность пропуска ложных утверждений, что, однако, не влияет на возможности применения таких доказательств для решения прикладных задач обеспечения информационной безопасности. Среди вероятностных криптографических доказательств особенно важное место занимают доказательства, обладающие свойством нулевого разглашения (англ. zero-knowledge proofs). В таких доказательствах лицо, проверяющее доказательство, убеждается в достоверности сформулированного математического утверждения, не получая от доказывающего никакой дополнительной информации, раскрывающей причины истинности утверждения, кроме самого доказываемого факта.

В настоящее время не разработаны многие фундаментальные вопросы, связанные с вероятностными и теоретико-сложностными свойствами криптографических доказательств, а также протоколов, в которых они используются в качестве примитивов, что, в частности, сдерживает дальнейшее развитие многих новых информационных технологий, например, технологий распределенного реестра и конфиденциального машинного обучения. Все известные криптографические доказательства, обладающие свойством нулевого разглашения, позволяют доказывать математически сформулированные факты либо отношения, выраженные теоретико-числовыми зависимостями, булевыми либо арифметическими схемами. Для криптографических доказательств на основе теоретико-числового аппарата характерна относительно низкая вычислительная и коммуникационная сложность, но серьезно ограничен диапазон доказываемых утверждений. Криптографические доказательства на основе булевых и арифметических схем универсальны, но отличаются очень высокой вычислительной и коммуникационной сложностью, так как представляющие практический интерес функции, как правило, описываются очень сложными булевыми (арифметическими) схемами. Основным недостатком существующих криптографических доказательств является низкая производительность и большой объём данных, представляющих доказательство. Преодоление этих недостатков путем поиска нового математического аппарата, разработки методов, алгоритмов и протоколов криптографических доказательств позволит приблизиться к созданию универсальных систем доказательства с приемлемыми для практического применения теоретико-сложностными оценками.

МОДЕЛИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЫЧИСЛЕНИЙ В НЕДОВЕРЕННОЙ СРЕДЕ

Центральным вопросом обеспечения информационной безопасности в условиях обработки данных в недоверенной среде является создание условий для возможности выполнения произвольного программного кода над массивом данных, представленным в зашифрованном виде, без раскрытия этого кода для стороны (участника), выполняющей такие вычисления. Причиной невозможности выполнения программного кода той же стороной, которая является заказчиком решения задачи, может быть недостаточная вычислительная мощность имеющегося у неё оборудования, недостаточный

объем оперативной памяти либо накопителей для долговременного хранения информации, мобильность пользователя, связанная с невозможностью выполнения большого объема вычислений на одном и том же оборудовании. Это приводит к необходимости передавать исходные данные для решения задачи другой стороне вычислительного процесса – исполнителю, обладающему достаточными ресурсами. Однако исполнитель может не пользоваться доверием со стороны заказчика. Описанная ситуация получила название аутсорсинговых вычислений.

Конфигурацию, в которой происходят защищенные аутсорсинговые вычисления, можно представить архитектурной моделью, изображенной на рис. 1.

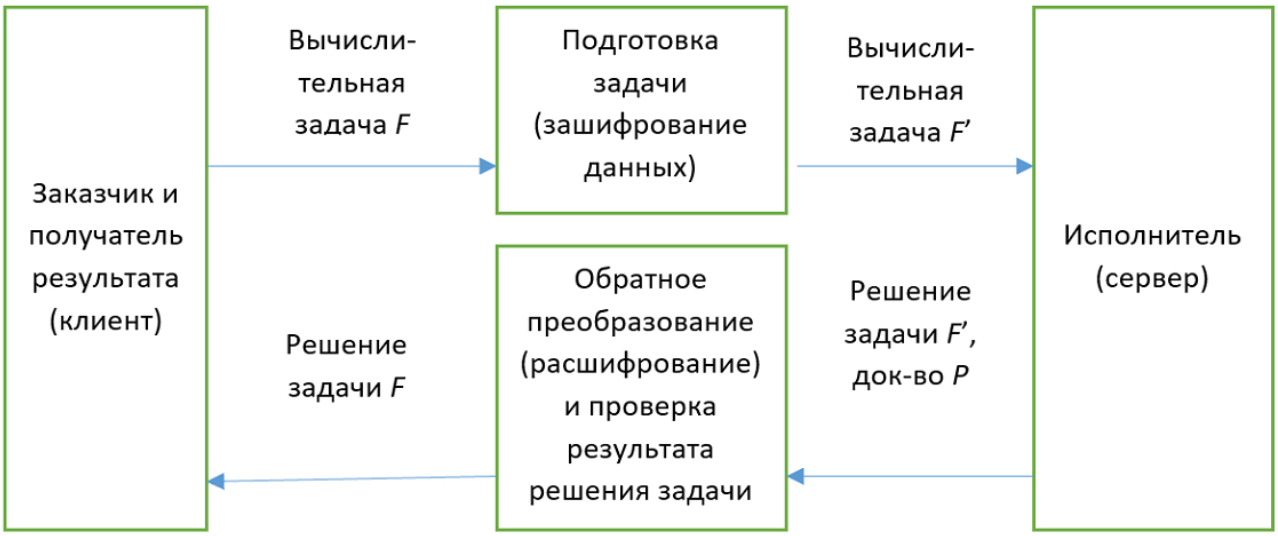


Рис. 1 Архитектурная модель защищенных аутсорсинговых вычислений

Модель включает в себя три основных функциональных блока:

- блок генерации задачи, передаваемой на аутсорсинг, и получения результата решения задачи;
- блок преобразования (трансформации) задачи и проверки результата решения задачи;
- блок решения задачи.

Размещение функциональных блоков по физическим участникам вычислительного процесса может быть неоднозначным. Наиболее предпочтительной является схема, когда первые два блока расположены на доверенной системе-клиенте, третий блок – на недоверенной системе-сервере. Такая конфигурация обеспечит максимальные гарантии защищенности информации, однако может быть связана с достаточно высокой вычислительной нагрузкой на клиента. В связи с этим второй возможной конфигурацией является размещение первого блока на доверенной системе-клиенте, второго блока – на доверенной системе-шлюзе, третьего блока – на недоверенной системе-сервере. Такая модель позволяет удобно разместить по блокам всю основную функциональность, обеспечивающую безопасность информации,

От недоверенных компонентов модели требуется следующая функциональность:

- выполнение алгоритмов обработки данных без раскрытия открытого текста данных;
- генерация доказательств корректного выполнения требуемых алгоритмов обработки данных.

От доверенных компонентов модели требуется следующая функциональность:

- подготовка исходных данных решаемой задачи для передачи недоверенным компонентам;
- прием результатов решения задачи от недоверенных компонентов и преобразование их в формат, пригодный для восприятия заказчиком вычислений;
- проверка корректности решения задачи недоверенным компонентом.

В связи с этим наиболее подходящими инструментами реализации функций, требуемых

от недоверенных компонентов, выглядят следующие криптографические методы:

- полностью и частично гомоморфные схемы шифрования (в части алгоритмов выполнения арифметических операций над зашифрованными данными);
- GC-схемы (garbled circuits);
- схемы разделения секрета;
- протоколы безопасных многосторонних вычислений (SMPC – secure multi-party computations);
- криптографические доказательства с нулевым разглашением (в части алгоритмов генерации доказательства).

Наиболее подходящими инструментами реализации функций, требуемых от доверенных компонентов, представляются следующие криптографические методы:

- полностью и частично гомоморфные схемы шифрования (в части алгоритмов зашифрования и расшифрования данных);
- криптографические доказательства с нулевым разглашением (в части алгоритмов проверки доказательства).

Развитием модели аутсорсинговых вычислений является модель федеративных вычислений, широко используемая во многих практических ситуациях. Основной особенностью федеративных вычислений является участие значительного числа клиентов, каждый из которых обладает частью массива обрабатываемой информации и обращается к одному общему серверу (иногда один логический сервер может быть представлен несколькими физическими, совместно обрабатывающими одни и те же данные и в процессе обработки обменивающимися между собой промежуточными результатами вычислений). Архитектурная модель федеративных вычислений показана на рис. 2.

Отличительной чертой модели федеративных вычислений является невозможность получения полноценного результата решения задачи ни одним из клиентов без получения достаточно полных исходных данных для ре-

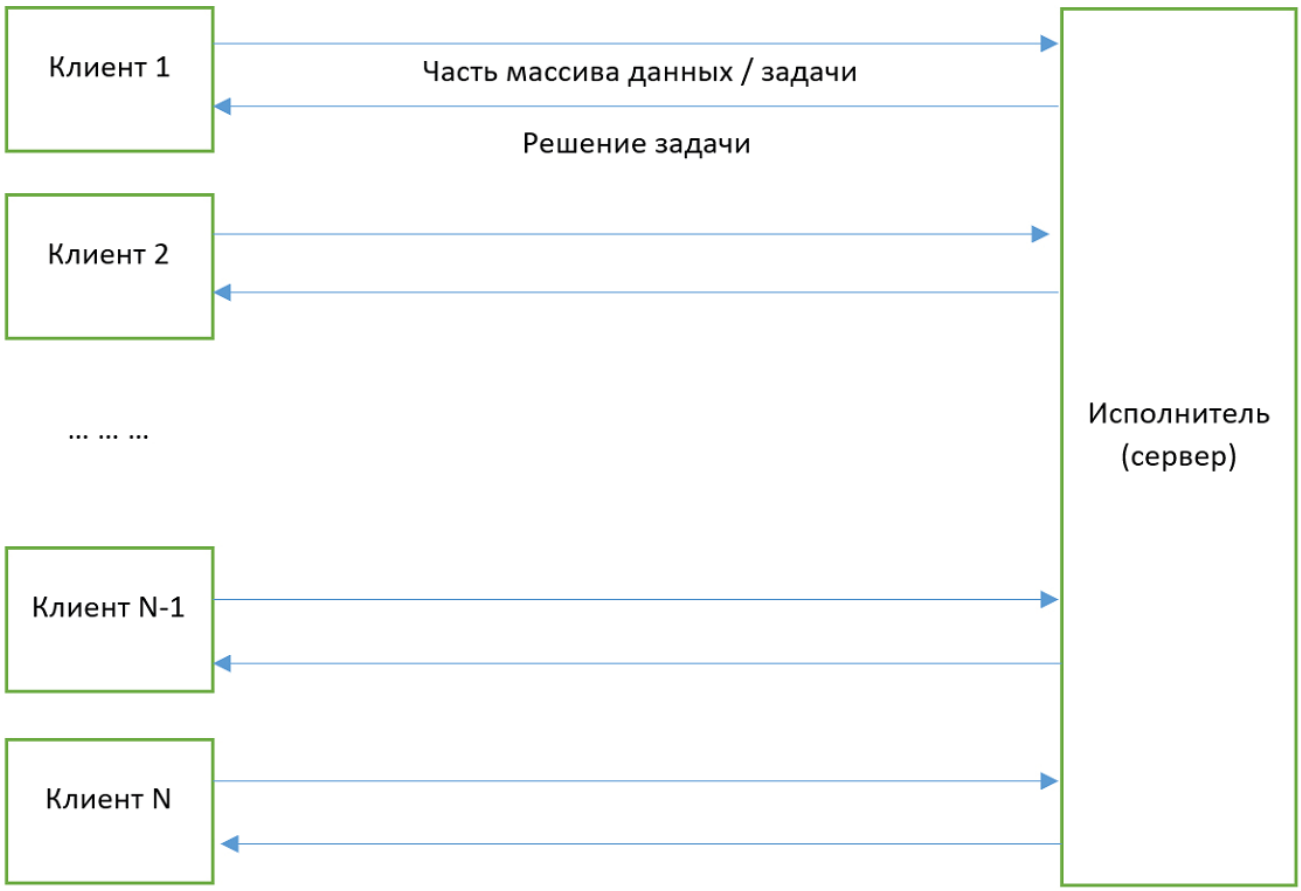


Рис. 2 Архитектурная модель федеративных вычислений

шения задачи от большинства клиентов, которые одновременно являются поставщиками исходных данных и потребителями результатов решения задачи.

Модель федеративных вычислений чаще всего применяется в сфере машинного обучения [2], когда признаки объектов находятся во владении множества разных лиц и в силу этого пространственно распределены. Выделяют несколько конфигураций федеративного машинного обучения:

- небольшое число участников, разделенные между ними данные, примерно равные вычислительные ресурсы у каждого из них, все вычисления выполняются самими участниками в ходе выполнения протоколов, отсутствует третья сторона, которой передавались бы данные для вычислений;
- большое число клиентов, малое число обрабатывающих центров, данные поставляются от клиентов, обучение и применение моделей осуществляется на серверах (например, в облаке).

Функции обеспечения безопасности информации для модели федеративных вычислений в основном аналогичны модели аутсорсинговых вычислений. Как следствие, аналогия наблюдается и в распределении функций криптографической защиты информации между клиентскими и серверными компонентами.

ТИПОЛОГИЯ И СВОЙСТВА ДОКАЗАТЕЛЬСТВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Доказательства с нулевым разглашением – криптографические протоколы, которые позволяют одной стороне – доказывающему *P* – доказать второй стороне – проверяющему *V* какое-либо утверждение, не сообщая проверяющему никаких дополнительных сведений, кроме факта истинности этого утверждения. Например, можно доказать, что в двух шифртекстах зашифрован один и тот же открытый текст, не разглашая сам открытый текст. В самом общем виде доказательства с нулевым разглашением позволяют доказывать истинность утверждений *st* вида:

st: {(a,b,c,…; x,y,z,…): f(a,b,c, … ,x,y,z, …)=true},

где *a,b,c,…* – общеизвестные величины, *x,y,z,…* – секретные величины, известные только доказывающему. Современные доказательства с нулевым разглашением позволяют доказывать любые факты и отношения, которые могут быть выражены арифметической схемой над конечным полем, в частности, булевой схемой.

Среди доказательств с нулевым разглашением выделяется множество взаимопроникающих классов протоколов. Одним из важнейших классов доказательств являются Σ-протоколы [3]. Это интерактивные протоколы специального вида, которые позволяют конструировать доказательства для очень широкого класса алгебраических отношений. Методика Фиата – Шамира [4] позволяет стандартным образом преобразовывать Σ-протоколы в неинтерактивные доказательства с нулевым разглашением. В некоторых системах распределенного реестра удается использовать такие относительно простые классы доказательств, однако в большинстве случаев интерес для создания конфиденциальных систем распределенного реестра представляют протоколы, позволяющие построить доказательства для функций произвольного вида, представимых в виде булевой или арифметической схемы.

Среди систем доказательства, представляющих наибольший теоретический и прикладной интерес, следует отметить, в частности, неинтерактивные доказательства Грота – Сахаи (Groth – Sahai) на основе билинейных отображений, краткие неинтерактивные доказательства знания с нулевым разглашением (zk-SNARK), доказательства типа Bulletproof, масштабируемые прозрачные доказательства знания с нулевым разглашением (zk-STARK).

В качестве примера рассмотрим систему доказательства zk-SNARK [5]. Это криптографическая схема, состоящая их четырех алгоритмов, выполнимых за полиномиальное время: $П_z$=(Setup,KeyGen,GenProof,VerProof), которая обладает свойствами полноты (completeness), состоятельности (soundness), краткости (succinctness) и совершенно нулевого разглашения (perfect zero-knowledge). Она позволяет создать доказательство с нулевым разглашением для произвольного утверждения вида $\vec{x}$ =C($\vec{a}$), где C – арифметическая схема, описывающая функцию, которая принимает на вход вектор $\vec{a}$ и вы-

даёт на выходе вектор $\vec{x}$.

Алгоритм генерации начальных параметров Setup(λ)→pp_Z по заданному параметру безопасности λ генерирует список открытых параметров pp_Z. Все остальные алгоритмы по умолчанию используют pp_Z как открытые общедоступные параметры.

Алгоритм генерации ключей KeyGen(C)→(pk_Z,vk_Z) по заданной арифметической схеме C, используя общедоступные параметры pp_Z, генерирует пару ключей (pk_Z,vk_Z), где pk_Z – открытый ключ генерации доказательства, vk_Z – секретный ключ проверки доказательства.

Алгоритм генерации доказательства GenProof(pk_Z, $\vec{x}$, $\vec{a}$)→π по заданному открытому вектору $\vec{x}$, называемому утверждением (statement), который является входом для арифметической схемы C, секретному вектору $\vec{a}$, называемому свидетельством (witness), который служит дополнительным входом для схемы C, используя ключ генерации доказательства pk_Z, создаёт совокупность данных, называемую криптографическим доказательством π со свойством нулевого разглашения, которое доказывает, что векторы $\vec{x}$ и $\vec{a}$ связаны алгебраическим отношением, задаваемым схемой C: $(\vec{x},\vec{a}) \in R_C$. Здесь $\vec{x}$ и π являются общедоступными наборами данных.

Алгоритм проверки доказательства VerProof(vk_Z, $\vec{x}$, π)→b позволяет, используя ключ проверки доказательства vk_Z и открытый вектор $\vec{x}$, использованный для генерации доказательства π алгоритмом GenProof, проверить это доказательство. Алгоритм вырабатывает бинарный ответ вида b=1, если проверка прошла успешно, и b=0 в противном случае.

Недостатком систем доказательства zk-SNARK является слишком большой для большинства практических применений объем данных, представляющих доказательство, который для сложных арифметических схем может доходить до десятков и даже сотен гигабайтов.

В связи с этим для целого ряда практических случаев большой интерес представляет система доказательства Грота – Сахаи [6]. Она позволяет конструировать весьма эффективные и по времени выполнения, и по объему данных доказательства, однако лишь для тех случаев, когда доказываемые утверждения могут быть представлены в виде спаривания либо композиции спариваний. Спариванием (pairing) называется эффективно вычислимое невырожденное билинейное отображение ê:G×G→G', где G – аддитивная группа, G' – мультипликативная группа. Требование эффективной вычислимости означает, что для ∀P, Q преобразование ê(P,Q) вычислимо за полиномиальное время. Требование невырожденности означает, что если P – образующий элемент G, то ê(P, P) – образующий элемент G'. Иными словами, ê(P, P) ≠1. Свойство билинейности означает, что для ∀R, S∈G ê(Q,R + S) = ê(Q,R) · ê(Q, S) и ê(Q + R, S)= ê(Q, S) · ê(R, S) (в левых частях равенств операции выполняются в группе G, в правых частях – в группе G').

Из билинейности сразу можно вывести следующее свойство парных отображений:

ê(2P, P)= ê(P+P, P)= ê(P, P) · ê(P, P)= ê(P, P)^2 = ê(P, P+P)= ê(P, 2P).

Аналогично можно показать, что

ê(3P, P)=...= ê(P, 3P),

ê(aP, bP)= ê(P, P)^{ab}= ê(abP, P)= ê(P, abP).

Ценное для криптографии свойство спариваний заключается в том, что задача распознавания Диффи–Хеллмана (DDHP) решаема в G за полиномиальное время тогда и только тогда, когда ê(aP, bP) = ê(P, cP).

Таким образом, спаривание – это функция, которая отображает пары элементов Q, R∈G в элементы ê(Q, R)∈G'. Спаривания удобны тем, что все аналитические выражения, в которых они используются, достаточно просты. Реализуются они в виде специальных дробно-рациональных функций над группами точек эллиптических кривых.

Недостатком всех вышеупомянутых систем доказательства является требование наличия доверенной третьей стороны при генерации начальных параметров системы доказательства. Это ограничение было преодолено в работах [7], где предложена система доказательства Hyrax, и [8], где представлена система Bulletproofs. Вторая система доказательства показывает лучшие результаты по объему данных, представляющих доказательство, при асимптотически одинаковом времени проверки доказательства. Однако и эти системы доказательства не вполне удовлетворяют современным

требованиям. Все они основаны на теоретико-числовых предположениях о вычислительно сложных задачах и оказываются нестойки к атакам нарушителя, обладающего доступом к квантовым компьютерам. Это обстоятельство породило требование постквантовой стойкости систем доказательства с нулевым разглашением.

В работах [9–11] предложены три неинтерактивные системы доказательства с нулевым разглашением, не требующие доверенной третьей стороны при генерации начальных параметров и обладающие постквантовой криптостойкостью: Ligero, zk-STARK и Aurora. Системы доказательства различаются между собой последовательно улучшающимися параметрами объема доказательств, времени их генерации и проверки, но имеют свои недостатки и ограничения, обсуждение которых выходит за рамки настоящей статьи. В настоящее время наиболее перспективной выглядит система доказательства Aurora, которая нашла практическое применение при решении ряда прикладных задач.

ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ В СИСТЕМАХ РАСПРЕДЕЛЕННОГО РЕЕСТРА

К настоящему времени накоплен опыт использования доказательств с нулевым разглашением в системах распределенного реестра. Как известно, в ныне существующих системах распределенного реестра распространены две модели представления балансов участников: UTXO-модель (Unspent Transaction Output) и модель аккаунтов (account model) [12]. В обеих моделях, если рассматривать их в базовых вариантах исполнения, отсутствуют встроенные механизмы обеспечения конфиденциальности информации, обрабатываемой при выполнении транзакций и записываемой в распределенный реестр. Таким образом, любой нарушитель может получить все данные транзакций, просто скопировав себе копию реестра, и прослеживать взаимосвязи между транзакциями и учетными записями, анализируя данные транзакций в реестре. Новые транзакции непрерывно добавляются в реестр, прежние при этом не удаляются в течение всего жизненного цикла реестра. Как только какая-либо транзакция раскрывает личность её участника, информация о нём будет раскрыта во всей цепочке транзакций, которая может быть прослежена от этой транзакции. Помимо данных из реестра, злоумышленники могут использовать любую внесистемную, косвенную информацию для определения личности владельцев аккаунтов.

Самый простой способ обеспечения конфиденциальности транзакций в UTXO-модели – генерация участником системы множества случайных или псевдослучайных адресов электронных кошельков. В идеале для каждой новой транзакции следует открывать новый кошелёк, но поддержание большого числа кошельков неудобно для пользователя и создает в конечном итоге риск утраты контроля над движением цифровых финансовых активов. Для решения проблем конфиденциальности в системах распределенного реестра на основе UTXO-модели в разное время было предложено множество решений с использованием доказательств с нулевым разглашением, в том числе реализованных на таких известных криптовалютных платформах как Dash, Zerocoin, Zerocash, Monero, CoinJoin и др. Обзор этих решений приведен в статье автора [12].

В то же время существует относительно немного решений по обеспечению конфиденциальности транзакций для модели аккаунтов. Баланс аккаунта обновляется каждый раз при добавлении в реестр новой транзакции, связанной с этим аккаунтом. При этом баланс аккаунта в любой момент равен накопленному результату всех связанных с ним операций, что приводит к большей концептуальной сложности защиты аккаунтов по сравнению с защитой графа транзакций в UTXO-модели и к существенно большей сложности реализации такой системы. Требования к защищённости аккаунтов значительно выше по той простой причине, что раскрытие личности отправителя или получателя хотя бы в одной из транзакций за все время существования аккаунта приводит к утрате анонимности владельца аккаунта. Функции обеспечения конфиденциальности аккаунтов с использованием доказательств с пулевым разглашением реализованы в таких системах,

как DSC, ZETH, Zether, BlockMaze. Их обзор также можно найти в статье [12].

ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ В КОНФИДЕНЦИАЛЬНОМ МАШИННОМ ОБУЧЕНИИ

Применение доказательств с нулевым разглашением в сфере конфиденциального машинного обучения – сравнительно новая идея, поэтому литература по этой теме пока немногочисленна. Общая идея заключается в следующем: если процессы обучения и применения модели происходят дистанционно (т.е. владелец данных, получатель результата и владелец модели – разные лица, взаимодействующие по дистанционным каналам) и обе взаимодействующие стороны заинтересованы в сохранении конфиденциальности своей информации, они, скорее всего, будут использовать одну из схем конфиденциального машинного обучения (privacy-preserving machine learning). Поэтому в настоящее время разработке методов защиты, которые могли бы использоваться при обучении и применении моделей, уделяется большое внимание.

Рассмотрим случай, когда обучающая выборка может содержать конфиденциальную информацию, в частности, персональные или медицинские данные. В этом случае владельцы данных могут быть заинтересованы в том, чтобы они были использованы при обучения какой-либо модели, но по вполне понятным причинам не желают терять контроль над ними и передавать их владельцу модели. Владелец модели также может не желать, чтобы параметры модели (например, синаптические веса нейронной сети) стали известны другим лицам, в том числе тем, кто предоставляет данные для обучения модели. Тем не менее, обе стороны заинтересованы в обучении и последующем применении модели. Добиться реализации этой цели позволяют протоколы конфиденциального машинного обучения.

Описанная ситуация хорошо вписывается в рассмотренную выше модель аутсорсинговых вычислений. Применительно к машинному обучению она включает два уточнения: модель процесса обучения модели и модель процесса её применения к тестовой выборке. Соответствующие модели показана на рис. 3 и 4.

Из литературы известны по крайней мере

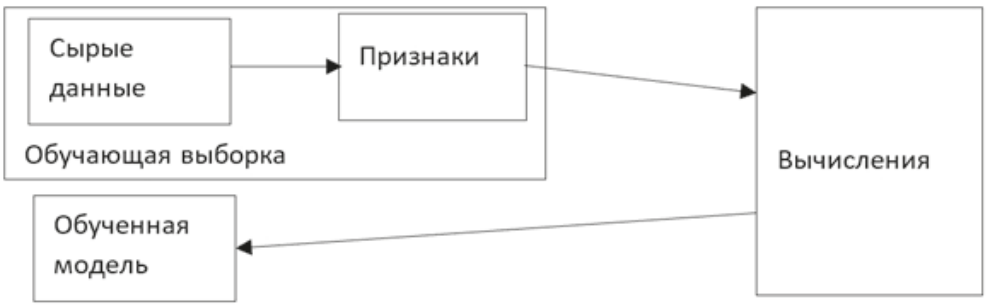


Рис. 3 Модель аутсорсинговых вычислений для этапа обучения

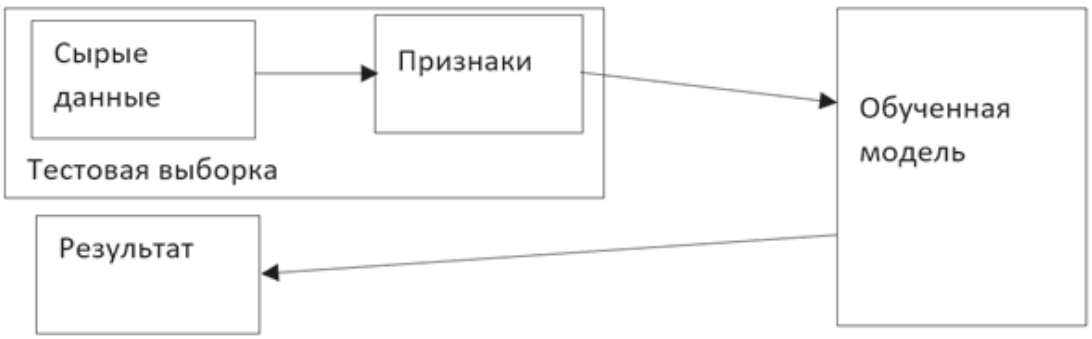


Рис. 4 Модель аутсорсинговых вычислений для этапа применения

три системы конфиденциального машинного обучения с нулевым разглашением.

В работе [13] предложена система VeriML, которая позволяет на этапе применения модели машинного обучения составить, передать от доказывающего к проверяющему и проверить доказательство факта корректного применения модели и получения достоверного результата. В качестве основного инструмента доказательства используется система zk-SNARK. Система VeriML применима для широкого спектра моделей: линейной регрессии, логистической регрессии, нейронных сетей, метода опорных векторов, кластеризации методом K средних и для решающих деревьев. Недостатком системы является избирательный характер проверки: для сокращения временных затрат проверяется не полный алгоритм получения ответа на запрос к модели, а лишь некоторые его элементы, например, для нейронных сетей проверяются операции на подмножестве слоев нейронов, которые случайно выбрал проверяющий.

Ещё одна разработка описана в статье [14], где предлагается система конфиденциального машинного обучения с нулевым разглашением для сверточных нейронных сетей, названная vCNN. В качестве основного инструмента используется система доказательства zk-SNARK. Однако, по заявлению самих авторов, производительность системы пока еще слишком низка для того, чтобы быть использованной в разработках, представляющих практический интерес.

В статье [15] описана система конфиденциального машинного обучения с нулевым разглашением для решающих деревьев. На этапе обучения модели авторы предлагают строить не обычное, а аутентифицированное решающее дерево, что позволит скрыть от посторонних наблюдателей практически все параметры дерева, за исключением малозначительных (таких как максимальная глубина пути от корня до вершин). На этапе применения модели доказывающий строит доказательство с нулевым разглашением для совокупности утверждений, состоящих в том, что он в самом деле воспользовался некоторым путём от корня до вершины, проходящим через все уровни дерева, что этот путь совпадает с одним из путей аутентифицированного дерева и что множество признаков, которыми помечены вершины этого пути, образуют перестановку множества признаков объектов обучающей и тестовой выборок. Все эти утверждения в комплексе позволяют проверяющему в случае положительного результата проверки доказательства убедиться в том, что предъявленный ему результат применения модели корректен. Построенное таким образом доказательство обладает свойствами полноты, состоятельности и нулевого разглашения.

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ТЕОРИИ ДОКАЗАТЕЛЬСТВ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ И ПРАКТИКИ ИХ ПРИМЕНЕНИЯ

Анализ положения дел в сфере прикладной криптографии позволяет выделить актуальную исследовательскую повестку в виде ряда научно-практических задач, развивающих теорию и практику применения доказательств с нулевым разглашением.

Во-первых, это анализ математических основ, существующих методов и моделей синтеза основных классов криптографических доказательств с нулевым разглашением, выявление их достоинств, недостатков, ограничений и областей эффективного применения. Для решения этой задачи необходимо уточнить типологию и исследовать все известные типы и виды криптографических доказательств, обладающих свойством нулевого разглашения, включая интерактивные и неинтерактивные системы доказательства, теоретико-числовые системы доказательства и системы доказательства на основе булевых (арифметических) схем, доказательства на основе вычислительно сложных задач в алгебраических структурах (в частности, задачи дискретного логарифмирования, задач над целочисленными решетками и др.) и вычислительно сложных задач, порождаемых отображениями между алгебраическими структурами (в частности, задач на основе билинейных отображений между группами точек эллиптических кривых и др.).

Во-вторых, это поиск математических моделей и методов синтеза новых криптографических доказательств, обладающих большей эффективностью по соотношению стойкость/

скорость. Развитие этого направления позволит определить перспективные математические и формально-логические основания синтеза криптографических доказательств, обладающих сбалансированными стойкостными и сложностными характеристиками. Для этого должны быть выделены и обоснованы критерии оценки криптографических доказательств, исследованы свойства систем доказательства, обладающих наилучшими известными на сегодня показателями по различным критериям.

Третьей актуальной задачей является поиск и исследование закономерностей проявления криптографическими доказательствами алгебраических, комбинаторных, теоретико-вероятностных, теоретико-сложностных и иных свойств в зависимости от выбора математического аппарата, классов доказательств, формы представления функций, вычисляемых при генерации доказательств. Решение этой задачи позволит сформулировать и доказать необходимые и достаточные условия наличия у криптографических доказательств основных свойств, определяющих их ценность для обеспечения информационной безопасности: корректности, состоятельности (полноты), экстракции знания, независимости от свидетельства и др.

В качестве четвёртой задачи можно выделить поиск и исследование закономерностей синтеза криптографических доказательств с заданными показателями криптографической стойкости (в том числе асимптотическими), вычислительной, коммуникационной и емкостной сложности. Исследования в этом направлении позволят сформулировать критерии достижения криптографическими доказательствами заданных количественных показателей стойкости и сложности. Представляет интерес сравнительное экспериментальное исследование перспективных систем доказательства с целью подтверждения теоретических оценок вычислительной, коммуникационной и емкостной сложности и выявления наиболее эффективных из них по соотношению различных показателей.

Пятая задача – разработка методов синтеза криптографических доказательств для обеспечения свойства нулевого разглашения в задачах аутсорсинговых вычислений, верифицируемых вычислений, безопасных многосторонних вычислений. Для решения задачи требуется формализация соответствующих криптографических схем и их свойств, выделение роли и функций в них криптографических доказательств, обладающих свойством нулевого разглашения, поиск математического аппарата и синтез криптографических доказательств для этих криптосхем. Наиболее предпочтительной для обоснования стойкости криптографических схем, протоколов и алгоритмов выглядит модель универсальной компонуемости (UC-модель, от англ. universally composable), которая позволяет использовать криптографические конструкции с доказанными оценками стойкости при модульном конструировании криптосхем. Представляет интерес экспериментальное исследование разработанных криптосхем с целью определения их стойкостных и сложностных характеристик, а также исследование производительности систем обработки информации, использующих криптосхемы, как систем массового обслуживания.

Наконец, шестая задача – это разработка методов синтеза криптографических доказательств для обеспечения свойства нулевого разглашения в задачах конфиденциального доступа к информационным массивам и базам данных, конфиденциального машинного обучения и смежных областях. Для этого необходимо формализовать исследуемые криптографические схемы и их свойства, определить место и функции криптографических доказательств в этих схемах, провести поиск математического аппарата и сконструировать криптографические доказательства для соответствующих криптосхем.

ЗАКЛЮЧЕНИЕ

Доказательства с нулевым разглашением являются одним из важнейших криптографических инструментов решения прикладных задач обеспечения безопасности информации. Подытожим важнейшие сферы практического применения доказательств с нулевым разглашением, какими они представляются на сегодняшний день и в обозримой перспективе:

• создание подсистем криптографической защиты информации в перспективных компьютерных информационно-коммуникационных, информационно-аналитических системах, цифровых системах управления, системах поддержки принятия решений, создание новых, изначально защищенных информационных технологий в интересах различных сфер деловой деятельности.

• создание новых средств и систем обеспечения безопасности информации в сфере цифровой экономики и государственного управления.

• оценка производительности существующих и прогнозирование производительности вновь создаваемых средств и систем криптографической защиты информации, осуществляющих дистанционную обработку конфиденциальной информации.

• создание высокозащищенных облачных систем информационного обслуживания и дистанционной обработки зашифрованных данных, защищенных систем распределенного реестра и иных защищенных компьютерных систем.

• создание систем управления зашифрованными базами данных, защищенных систем федеративного машинного обучения и иных защищенных компьютерных систем, а также многофункциональных систем, требующих выполнения указанных функций.

Представляется, что развитие теории и практики доказательств с нулевым разглашением позволит в ближайшем будущем создавать информационные системы и сервисы с принципиально новыми свойствами защищённости.

СПИСОК ЛИТЕРАТУРЫ

1. Запечников С.В. Криптографическая защита процессов обработки информации в недоверенной среде: достижения, проблемы, перспективы // Вестник современных цифровых технологий, 2019. № 1. С. 6–18.

2. Запечников С.В. Модели и алгоритмы конфиденциального машинного обучения // Безопасность информационных технологий, 2020. Т. 27, Вып. 1. С. 51–67.

3. Hazay C., Lindell Y. Sigma protocols and efficient zero-knowledge // Efficient secure two-party protocols. Information security and cryptography. Springer, 2010. P. 147–175.

4. Fiat A., Shamir A.How To Prove Yourself: Practical Solutions to Identification and Signature Problems // Advances in Cryptology — CRYPTO' 86. Lecture Notes in Computer Science. Springer. Vol. 263. P. 186–194.

5. Bitansky N., Canetti R., Chiesa A., et al. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again // ITCS '12: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, January, 2012. P. 326–349.

6. Groth J., Sahai A. Efficient non-interactive proof systems for bilinear groups // SIAM Journal on Computing. Vol. 41(5). P. 1193-1232, 2012.

7. Wahby R., Tzialla I., Shelat A., et al. Doubly-Efficient zkSNARKs Without Trusted Setup // 2018 IEEE Symposium on Security and Privacy, San Francisco, 2018. P. 926-943. doi: 10.1109/SP.2018.00060.

8. Bunz B., Bootle J., Boneh D. et al. Bulletproofs: Short Proofs for Confidential Transactions and More // Proc. of IEEE Symposium on Security and Privacy, 2018. P. 315–334.

9. Ames S., Hazay C., Ishai Y. et al. Ligero: Lightweight Sublinear Arguments Without a Trusted Setup // Proceedings of the 24th ACM Conference on Computer and Communications Security. CCS ’17. 2017. P. 2087–2104.

10. Ben-Sasson E., Bentov I., Horesh Y., Riabzev M. Scalable, transparent, and post-quantum secure computational integrity // IACR cryptology eprint archive, 2018. 83 pp. URL: https://eprint.iacr.org/2018/046.pdf (датаобращения: 18.01.2021).

11. Ben-Sasson E., Chiesa A., Riabzev M. et al. Aurora: Transparent Succinct Arguments for R1CS // Advances in Cryptology – EUROCRYPT 2019. Lecture Notes in Computer Science. Springer.Vol. 11476. P. 103-121.

Doi: 10.1007/978-3-030-17653-2_4

12. Запечников С.В. Системы распределенного реестра, обеспечивающие конфиденциальность транзакций // Безопасность информационных технологий. Том 27, №4 (2020). С. 107 – 122.

13. Zhao L., QianWang, CongWang, et al. VeriML: Enabling Integrity Assurances and Fair Payments for Machine Learning as a Service.- URL: https://arxiv.org/pdf/1909.06961v1.pdf

14. Lee S., Ko H., Kim J., Oh H. vCNN: Verifiable convolutional neural network based on zk-SNARKs.- URL: https://eprint.iacr.org/2020/584 (дата обращения: 18.01.2021).

15. Zhang J., Fang Z., Zhang Y., Song D. Zero knowledge proofs for decision tree predictions and accuracy // CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020. P. 2039–2053. Doi: 10.1145/3372297.3417278.

УДК: 004.75, 004.41

Тенденции развития и практические реализации решений по обеспечению безопасности криптографических сетей

V. Kuzmenko, V. Makarov, K. Razgulyaev, D. Khan, P. Cherkashin, A. Shcherbakov

Development Trends and Practical Implementation of Solutions to Ensure the Security of Cryptographic Networks

Abstract. *Modern trends in ensuring the security of data transmission networks and ensuring the security of business processes are considered, the concepts and properties of cryptographic networks are formulated, the concepts of a service model and key containers are considered based on the development of quantum-protected networks, a practical solution and its architecture are described.*

Keywords: *cryptographic networks, service model, protocol, keys, key containers, electronic signature, key exchange, security, encryptor, HSM (hardware security module) - module for trusted storage of keys.*

***В.В. Кузьменко*[1]**
***В.Л.Макаров*[2]**
***К.А. Разгуляев*[3]**
***Д.В. Хан*[4]**
***П.А.Черкашин*[5]**
***А.Ю.Щербаков*[6]**

[1] Вице-президент Ассоциации РКЦФА по направлению Финтех.
v.kuzmenko@c3da.org
[2] Президент Некоммерческого партнерства разработчиков программного обеспечения «Руссофт»
[3] Центр научно-технологического форсайта Университета ИТМО, Санкт-Петербург.
E-mail: kirill.razgulyaev@gmail.com
[4] ООО «Финдинамика», Санкт-Петербург.
E-mail: dkhan@findinamika.com
[5] Научный сотрудник Ассоциации РКЦФА.
E-mail: pcherkashin@gmail.com
[6] Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник ЦРКЦФА, ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: x509@ras.ru

Аннотация. *Рассмотрены современные тренды в обеспечении безопасности сетей передачи данных и обеспечения безопасности бизнес-процессов, сформулированы понятия и свойства криптографических сетей, рассмотрены понятия сервисной модели и ключевых контейнеров с опорой на развитие квантово-защищенных сетей, описано практическое решение и его архитектура.*

Ключевые слова: *криптографические сети, сервисная модель, протокол, ключи, ключевые контейнеры, электронная подпись, обмен ключами, безопасность, шифратор, HSM (hardware security module) – модуль доверенного хранения ключей.*

ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ И СОВРЕМЕННЫЕ ТРЕНДЫ

В последние годы наметилось несколько примечательных и принципиально важных мировых трендов в области интернет-технологий.

Это в первую очередь повсеместное использование облачных сервисов. Благодаря развитию персональных мобильных устройств и всё большему распространению Интернета, сервисы все чаще переходят на облачную архитектуру для работы в непрерывном режиме. Однако развитие таких бизнес моделей как Iaas, PaaS, SaaS приводит к увеличению нагрузки на сеть, а огромное количество подключенных устройств повышает риск кибератак.

Криптографические сети (Cybersecurity Mesh, сети кибербезопасности). Подключения к облачным сервисам все большего количества устройств повышает риски отказа всей системы при внешних киберугрозах. Для того, чтобы не фокусироваться на построении единого «периметра» вокруг всех устройств и узлов ИТ-сети, а установить меньшие индивидуальные периметры вокруг каждой точки доступа, используются специальные криптографические сети, целью которых является обеспечение не только безопасности передаваемой и хранимой в сети информации, но и эффективного управле-

ния безопасностью каждой точки доступа (узла сети) из центра управления без предоставления доступа к более широкой части сети в случае нарушения безопасности данного узла. Такой подход позволяет устанавливать более надежные и гибкие модульные системы сетевой безопасности, дифференцируя уровни доступа к различным частям сети и предотвращая использование слабых мест данного узла для доступа к другим сетям и информации пользователей.

Цифровые активы. Благодаря применению технологии распределенных реестров пользователь получил инструменты контроля за перемещением информации и её состоянием, что в сочетании с безопасными криптографическими решениями позволило превратить любую информацию в цифровой актив. Вместе с тем эволюционировали учетно-расчетные системы данных: объединенные с платежными сервисами и инструментами цифровых подписей, они представляют собой легитимную для большинства юрисдикций цифровую среду полного цикла для работы с практически любым типом документов.

Сквозная аутентификация и универсальные аккаунты. Повсеместное использование открытых программных интерфейсов (API) позволило сделать бесшовную интеграцию приложений и сервисов для конечного пользователя и выстроить интерфейсы взаимодействия вокруг единого идентификатора пользователя. На основе этого тренда крупнейшие мировые и российские технологические платформы строят свои экосистемы, собирая персональные данные и подстраиваясь под потребительские особенности каждого клиента.

Сервисные модели. Сервисная модель (СМ), применяемая в первую очередь для квантово-защищенных сетей (КЗС) передачи данных, представляет собой инфраструктурное понятие, необходимое для целостного описания и моделирования процессов оказания услуг клиентам, в первую очередь связанных с защищенной передачей данных и защитой информации.

Принципиальное отличие квантово-защищенной сети от произвольной сети передачи данных – наличие механизма выработки и распределения квантовых и связанных с ними ключей, соответственно, основа СМ – процедуры распределения и хранения ключевой информации пользователей и построенные на их основе разнообразные сервисы [1].

СВОЙСТВА КРИПТОГРАФИЧЕСКИХ СЕТЕЙ

Таким образом, главным в новом технологическом укладе в сфере кибербезопасности является получение безопасного доступа к любому цифровому активу, независимо от того, где находится актив или человек. По прогнозам компании Gartner[1], к 2025 году криптографические сети будут поддерживать более половины запросов на управление цифровым доступом и станут главной архитектурой систем кибербезопасности.

Учитывая изложенные выше тренды, криптографические сети должны выполнять следующий минимальный набор функций:

- **Регистрация пользователя по его персональному идентификатору.** Не требуется специальный интерфейс для использования привычных приложений, система аутентификации автоматически подключается ко всем доступным сервисам. Пользователю должна быть предоставлена возможность реализации входа в систему без удостоверяющих центров и посредников.
- **Использование КЗС.** Вследствие повышения требований к безопасности инфраструктуры информационных систем, а также в связи с участившимися случаями компрометации классических методов шифрования, использование квантовой криптографии становится обязательным не только для защиты критически важной инфраструктуры, но и в массовом сегменте корпоративных систем обмена данных. Появление квантового компьютера в среднесрочной перспективе (3-5 лет) только ускоряет имплементацию данной технологии.
- **Необратимая или «сингулярная» загрузка ключей.** Все процессы управления ключами осуществляются по их номеру или идентификатору в хранилище, понимаемом как изоли-

[1] https://www.gartner.com/en/newsroom/press-releases/2020-10-19-gartner-identifies-the-top-strategic-technology-trends-for-2021 - Top Industry Trends at Gartner IT Symposium/Xpo 2020 Americas, October 19-22

рованное техническое устройство, в котором нет возможности прочитать загруженный или сформированный ключ ввиду отсутствия программных и технических интерфейсов извлечения ключа во «внешний мир» [2].

• **Использование безопасных ссылок для передачи файлов.** Хранение и передача файлов осуществляется внутри защищенного контура, доступ к которому имеют только авторизованные пользователи. Обмен файлами строится на передаче не самих исходных данных, а защищенных ссылок, доступ к которым в реальном времени регулируется владельцем.

• **Безопасное хранение ключей шифрования.** Внешний доступ к информации и ключам внутри хранилища ограничен благодаря использованию специального физического модуля хранения ключей (HSM). Данное оборудование позволяет использовать квантовые ключи шифрования без смены архитектуры всей системы.

• **Симметричное шифрование.** В основе криптографических сетей преимущественно используются симметричные алгоритмы шифрования и контроля целостности (имитовставки), являющиеся стойкими к квантовым вычислениям и значительно менее ресурсоемкими по сравнению с ассиметричными алгоритмами шифрования (на основе пар приватный – открытый ключ).

• **Низкая стоимость.** Общая стоимость издержек значительно снижается за счет отсутствия необходимости устанавливать сертифицированное средство криптографической защиты (СКЗИ) на каждое пользовательское устройство.

• **Легитимность.** Обеспечение корректной национальной регуляции в части использования криптографических средств.

АРХИТЕКТУРА КЗС И КЛЮЧЕВЫЕ КОНТЕЙНЕРЫ

В силу того, что обмен квантовыми ключами физически возможен только для смежных узлов квантовой сети, для обмена информации транзитного характера (для произвольной топологии КЗС, подключения к другим сетям и обеспечения работы абонентов без квантового оборудования) необходимо использовать другие виды ключей, последовательно используя защищенные каналы, образованные между смежными узлами.

Кроме того, передача ключей абонентам или в оконечные узлы сети, не содержащие квантового оборудования, должна происходить в зашифрованном виде, для чего используется конструкция ключевого контейнера.

Ключевой контейнер – информационный объект КЗС и СМ, использующийся для защищенной (обеспечивающей целостность и конфиденциальность) передачи ключей между элементами КЗС.

Ключевой контейнер (КК) состоит из совокупности открытых и закрытых полей, целостность которых зафиксирована.

КК в обязательном порядке содержит ключи, которые зашифрованы таким образом, чтобы обеспечить их безопасную передачу и хранение внутри или вовне КЗС (для этого используется шифрование на квантовых ключах, на паролях, на ключах аппаратных хранилищ и т.д.). Кроме того, КК содержит дополнительную информацию, обеспечивающую функционирование в рамках сервисной модели: назначение ключа, владельца ключа, количество использований ключа и др.

Перечень возможных сервисов криптографических сетей

Таким образом, возможные виды защищенных сервисов определяются полем «назначение ключа»:

1. Ключи транзитной передачи данных между узлами криптографической сети.
2. Ключи клиентов для связи с опорными узлами.
3. Ключи клиентов для связи между собой (для поддержания режима конфиденциальности абонентской связи).
4. Ключи инициализации датчиков случайных чисел (ДСЧ) для программных ДСЧ, расположенных у клиента или в опорных узлах.
5. Ключи оконечных сервисов (IP-телефония, видеосвязь).
6. Ключи корпоративных хранилищ и облаков.
7. Ключи внутрисетевых и корпоративных распределенных реестров.

8. Ключи для работы с аппаратными хранилищами данных.

9. Ключи для взаимодействия со сторонними сервисами и другими системами защищенной передачи данных.

СЦЕНАРИИ ПРИКЛАДНОГО ИСПОЛЬЗОВАНИЯ

Для прикладного использования системы в качестве типовой задачи защиты бизнес-процессов рассматривается защита данных в открытых сервисах, используемых в бизнес-процессе, включая мессенджеры и открытую почту. Практика показала, что даже при работе с конфиденциальной информацией, приоритет отдаётся в пользу удобства, а не безопасности.

Корпоративные решения неудобны и сложны в использовании, а их ставка на безопасную передачу данных - зачастую лишь маркетинговый ход. Поэтому у многих компаний сформировалась потребность в обеспечении защиты информации при использовании открытых сервисов.

Специалистами российской компании ApiQ был реализован новый подход к обеспечению безопасности бизнес-процессов, который может гарантировать невозможность передачи конфиденциальной информации за периметр организации и связанный с применением модулей хранения пользовательских ключей (подход реализован в виде решения «QuantGuard»). Теоретическая модель и протокол решения рассмотрены в [3, 4].

Под «открытыми сервисами» понимаются абонентские программные средства и обеспечивающая их инфраструктура (например, общедоступные почтовые клиенты Gmail, Outlook, Mail.ru, Yandex mail), обслуживающие их сервера, а также различного рода мессенджеры, например, Telegram, Whatsapp и другие.

Предлагаемая технология позволяет существенно снизить риски ИБ и не нагружать пользователей неудобными и непривычными им сервисами. Кроме того, корпоративная сеть становится замкнутой и нет необходимости устанавливать сертифицированное СКЗИ на каждое устройство, что позволяет снизить издержки и обеспечить корректную национальную регуляцию в части использования криптографических средств.

В данном случае речь идет о модели внешнего нарушителя, т.е. нарушителя, который может читать и изменять информацию в каналах связи (в телекоммуникационной компоненте информационно-телекоммуникационной системы). Полагаем, что владелец системы (организатор бизнес-процессов) является лицом доверенным и не заинтересован в нарушении свойств безопасности.

Угроза безопасности выглядит следующим образом: пользователь использует различные открытые сервисы для передачи служебной информации, что приводит к систематическим инцидентам информационной безопасности (ИБ), связанным с утечками корпоративных данных за периметр безопасности (т.е. к лицам, не участвующим в бизнес-процессах, прямым конкурентам и нарушителям информационной безопасности).

Использование решения «QuantGuard» (рис.1) позволяет нейтрализовать данную угрозу и не допустить попадания защищенной информации за периметр криптографической сети. Кроме того, предложенный подход в сочетании с квантовыми коммуникациями (реализацией сервисов на базе квантового HSM) позволяет решить множество актуальных проблем, например, уйти от зависимости от управляющих ключами электронной подписи удостоверяющих центров, а также вообще уйти от влияния человеческого фактора в вопросах управления безопасностью, создать современную надежную инфраструктуру, обеспечивающую на корпоративном уровне управление доступами и безопасный обмен информацией внутри корпоративного периметра на основе симметричных криптографических алгоритмов, исключая человеческий фактор, при формировании паролей, криптографических ключей, сертификатов открытого ключа.

Использование квантовой криптографии особенно актуально в связи с принятием дорожной карты по созданию в России квантовой сети. Сейчас реализуется первый сегмент сети между Москвой и Санкт-Петербургом, что позволит заинтересованным игрокам использовать уникальные свойства квантовых криптографических ключей в своих сервисах и решениях.

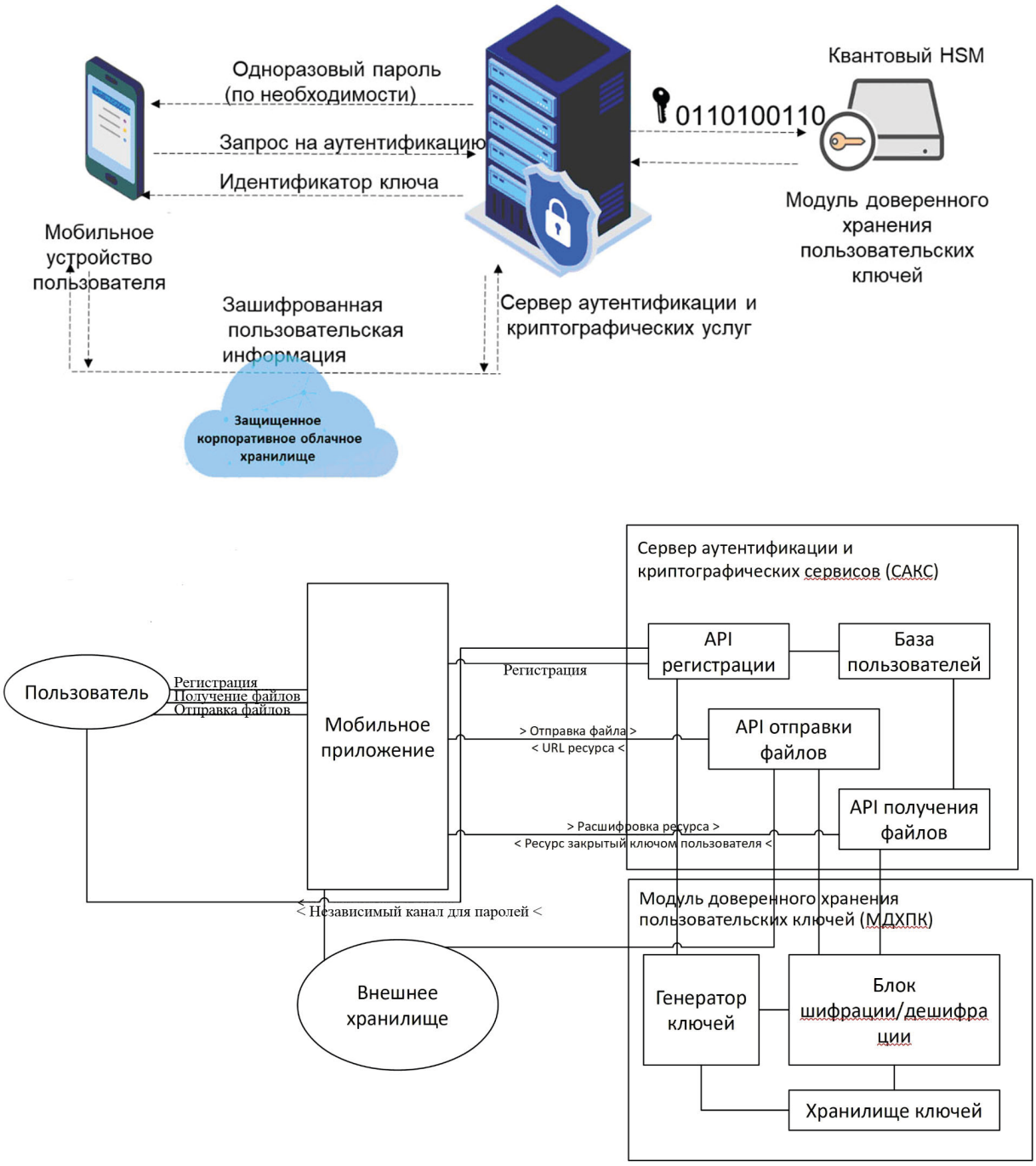


Рис. 1. Варианты архитектуры решения «QuantGuard»

Таким образом, данная система криптографических сетей с применением симметричного шифрования и квантовых коммуникаций способна организовать устойчивую к внешним угрозам безопасную среду работы с файлами и обмена информацией. Учитывая вектор технологического развития, данная архитектура имеет серьезный задел на будущее и отвечает всем современным требованиям как мировых, так и национальных стандартов безопасности.

ВЫВОДЫ

Для реализации сервисной модели криптографической сети необходимо создание подсистемы, обеспечивающей ее функционирование и опирающейся на механизм ключевых

контейнеров, который позволит реализовать и изолировать различные сервисы на базе поля назначения ключа.

Этот же фактор облегчит коммерциализацию СМ, поскольку селектирование и билинг сервисов может быть достаточно просто реализован.

Кроме того, механизм контейнеров позволяет легко добавлять различные сервисы, реализовывать механизмы конвертации ключевых форматов для других систем защищенной передачи данных.

Дополнительными преимуществами использования КК будет повышение устойчивости и надежности сети за счет хранения контейнеров (исключая ключи ЭП) как минимум у пары подсистем или пользователей, а также возможность проведения мониторинга информации о сервисах (с использованием информации в контейнерах, например, об объеме трафика, закрытого на данном ключе) и восстановления КК при сбоях или поломках оборудования.

СПИСОК ЛИТЕРАТУРЫ

1. Щербаков А.Ю. Перспективы современной криптографии // Проектирование будущего. Проблемы цифровой реальности. – 2020. – № 1 (3). – С. 227-233.

2. Гриняев С.Н., Правиков Д.И., Разгуляев К.А., Рязанова А.А., Хан Д.В., Щербаков А.Ю. Основные методологические подходы к формированию и обоснованию архитектуры и протокола квантового распределенного реестра // Научно-техническая информация. Серия 2: Информационные процессы и системы. – 2020. – № 1. – С. 11-18.

3. Кузьменко В.В., Макаров В.Л., Разгуляев К.А., Хан Д.В., Щербаков А.Ю. Новый подход к обеспечению безопасности периметра бизнес-процессов и аутентификации пользователей в корпоративной системе // Вестник современных цифровых технологий. – 2020. – №3. – С. 10-13.

4. Бородулина С.А., Гриневич В.Е., Тихоненко О.О., Щербаков А.Ю. О новом подходе к реализации трансграничной проверки электронных подписей // Вестник современных цифровых технологий. – 2020. – №4. – С. 20-25.

УДК: 616-071

Новые подходы к акустическому анализу состояния организма человека

D. Tikhonenko, O. Tikhonenko, P. Cherkashin, G. Shipitsina, I. Shushkevitch, A. Shcherbakov

New Approaches to Acoustic Analysis of the State of the Human Body

Abstract. *The article is devoted to the formulation and discussion of a new approach to the study of the acoustic picture of the human body using a regular structure of microphones, which are analogous to a phased receiving antenna array, and further processing of information using mathematical methods of digital medicine. Particular attention is paid to passive methods of obtaining information about internal processes in the human body associated with the emission of acoustic vibrations from internal organs (heart, lungs).*

Keywords: *acoustics, stethoscope, auscultation, ultrasound scan, digital antenna array (DAA), phased acoustic antenna array (PhAAA).*

Д.О. Тихоненко[1]
О.О. Тихоненко[2]
П.А.Черкашин[3]
Г.Н. Шипицина[4]
И.Ю. Шушкевич[5]
А.Ю. Щербаков[6]

[1]Руководитель проекта BodyVo,
E-mail: t.daniil@bodyvo.com.
[2]Кандидат философских наук, председатель совета директоров ООО «Прогнотех».
E-mail: fzr@bk.ru, t.oleg@ bodyvo.com.
[3]Научный сотрудник Ассоциации РКЦФА.
E-mail: pcherkashin@gmail.com
[4]Главный специалист ЦРКЦФА, ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: info@c3da.org
[5]Главный специалист ЦРКЦФА, ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: info@c3da.org.
[6]Доктор технических наук, профессор, главный научный сотрудник РАН (ИТМиВТ им.С.А.Лебедева), начальник ЦРКЦФА, ВИНИТИ РАН, Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).
E-mail: x509@ras.ru

Аннотация. *Статья посвящена формулированию и обсуждению нового подхода к изучению акустической картины организма человека при помощи регулярной структуры микрофонов, представляющих собой аналог фазированной приемной антенной решетки, и дальнейшей обработки информации при помощи математических методов цифровой медицины. Особое внимание уделяется пассивным методам получения информации о внутренних процессах в организме человека, связанных с излучением акустических колебаний от внутренних органов (сердца, легких).*

Ключевые слова: *акустика, стетоскоп, аускультация, ультразвуковое исследование (УЗИ), цифровая антенная решетка (ЦАР), фазированная акустическая антенная решетка (ФААР).*

ВВЕДЕНИЕ

Как неоднократно отмечалось [1], реализация цифровых технологий в медицине в первую очередь связана с «оцифровкой» данных и накоплением больших данных. Это отражает вполне объяснимый тренд медицинской цифровизации, связанный прежде всего с количественными изменениями, а не с появлением нового подхода к диагностике различных состояний. Кроме того, необходимо отметить, что акустический анализ медицинских состояний, как правило, выполняется профессиональными врачами, для ультразвука – узкими специалистами, в то время как проведение аускультации с использованием стетоскопа доступно широкому кругу медицинских работников.

В силу своей универсальности акустический анализ – весьма эффективный метод как врача общей практики, так и узкого специалиста. Выделим два направления акустического анализа: активное исследование (ультразвуковая диагностика, локация) и пассивное прослушивание (аускультация). В дальнейшем мы остановимся на пассивных методах анализа,

поскольку воздействие их на организм минимально. Необходимо отметить, что на применение новых методов анализа звуковых сигналов оказывают влияние такие факторы, как консервативность методов ультразвукового обследования и аускультации, отсутствие моделей и практики приема и анализа звуков, требующих высокой вычислительной мощности. Рассмотрим естественные результаты развития акустических технологий – УЗИ-сканеры и цифровые стетоскопы.

УЛЬТРАЗВУКОВЫЕ СКАНЕРЫ

Одним из лидеров в сфере ультразвуковой диагностики является компания Signostics, которая в 2009 году разработала свой первый ручной УЗИ-сканер. Устройство **Signos RT**, отличающееся неплохим качеством изображения при размере экрана 2,7 дюймов, компания определяет как самое маленькое и удобное ручное ультразвуковое устройство в мире, предназначенное для использования в акушерских исследованиях, сканирования органов брюшной полости и сердца, отдельных периферических сосудов, определения пневмоторакса и плеврального выпота (рис. 1).

Рис. 1. Устройство ультразвуковой диагностики Signos RT

Вариант миниатюрного УЗИ-сканера **Sonimage P3** представила компания Konica Minolta Medical Imaging в 2013 году. Данное устройство, аналогичное описанному выше Signos RT, производится по лицензионному соглашению.

ЦИФРОВЫЕ СТЕТОСКОПЫ

Прогресс наблюдается и в консервативной области электронных стетоскопов. На сегодняшний день с помощью новейших устройств возможно обнаружение подозрительных характеристик работы сердца. Таким неинвазивным, безрадиационным, быстрым и портативным инструментом для оказания помощи клиницистам в оценке звуков, связанных с клинически значимой обструкцией коронарных артерий, застойной сердечной недостаточностью и аномалиями сердечных клапанов, является система **CADence**, состоящая из цифрового стетоскопа, используемого для записи сердечных тонов, встроенных датчиков для записи электрической активности сердца (ЭКГ) и программного приложения CADence (рис. 2). Последнее представляет собой инструмент поддержки клинических решений, предназначенный для оказания помощи квалифицированному клиницисту в анализе нормальных/физиологических и патологических шумов сердца после записи сердечных тонов и ЭКГ.

Автоматизированный анализ сердечных тонов системой CADence должен производиться в сочетании с наблюдением врача, а также с учетом всей другой релевантной информации о пациенте, обязательной для постановки диагноза. Система CADence не предназначена для использования в качестве автономного диагностического устройства.

Функции записи и сравнения звуков сердца, легких и других органов выполняет стетоскоп **Stethee** с помощью приложения Stethee. Данное устройство подключается непосредственно к любым проводным или беспроводным наушникам, возможно подключение к мобильному устройству. Устройство Stethee (рис. 2), оснащено двухъядерным процессором, обработкой сигналов в реальном времени, двухквадратными сердечными и дыхательными фильтрами, а также технологией шумоподавления воздушного шлюза. Сочетание данных функций обеспечивает высокое качество прослушивания и позволяет повысить эффективность и производительность медицинской помощи.

Цифровой стетоскоп **Thinklabs One** также

упрощает медицинское обслуживание (рис. 2). Это эффективный инструмент аускультации, используемый, в частности, в ведущих медицинских учебных заведениях для эффективного обучения практическим навыкам аускультации и позволяющий в режиме реального времени наблюдать пациента одновременно преподавателем и студентами (в том числе удаленно), использовать возможности визуализации, внешние микрофоны, мобильные устройства.

CADence: автоматический анализатор звуков сердца

Стетоскоп Stethee

Стетоскоп Thinklabs One

Рис. 2. Примеры аппаратов пассивного прослушивания звуков от внутренних органов

ИСТОРИЯ ПРОЕКТА ОТ КАРДИОМА (CARDIOM) ДО ГОЛОСА ТЕЛА (BODYVO)

Первоначально развитием модели цифрового стетоскопа фактически являлся проект **CARDIOM**. Суть проекта заключалась в прослушивании звуков работы сердца через микрофон мобильного устройства и сохранении аудиозаписей, соответствующих звукам сердца. Далее производилось установление соответствия звуков сердца и ЭКГ. Первичные данные собирались у кардиологов. Пациент приходил на ЭКГ к врачу, который через электронный стетоскоп записывал звук работы сердца и соответствие в текущий момент ЭКГ сердца пациента. Для формирования качественной базы соответствий необходимы были данные десятков тысяч пациентов. Поскольку один врач мог обеспечить данные 30-50 пациентов, проект оказался технически трудно реализуем.

Далее развитие проекта было в сторону устройства с тремя микрофонами эхографа **RuCore 24/7** для размещения его на животе беременной женщины. С помощью полученных звуков была построена 3D-модель плода ребенка и его положение в утробе матери. Данный универсальный пассивный эхограф с широким кругом применения - от личного до специализированных клиник - предоставляет врачу записанную звуковую информацию для прослушивания, дает максимально полный набор сведений для врача и пациента (при домашнем использовании).

Следующий макет прибора (бандаж или высокие трусы) содержит три микрофона с несферической диаграммой направленности (для точного определения направления на звук с учетом фазы), датчик сверхнизких частот, датчик контакта с телом, колесико-курвиметр для определения перемещения по телу, датчики положения блока в пространстве и блок передачи данных, кнопку "начать измерения".

Все измерения отображаются на трехмерной фигуре человека, а цветом выделяются места рекомендуемого прикладывания прибора.

Измерения ведутся с перемещением прибора по телу. По мере накопления данных на фигуре начинает динамически отображаться сердце и легкие, а также крупные сосуды, дающие звук и эхо, отображается сердце плода, положение которого позволяет моделировать положение всего плода в пространстве. Дополнительно измеряется корреляции пульса плода

и матери и строится допплер-модель кровотока. Первично прибор калибруется - передвигается по телу и придает макету реальные размеры, что дает возможность зафиксировать изменения фигуры при течении беременности.

Отличием прибора от существующих является визуализация работы органов (включая работу сердца матери и плода - для беременных) в виде понятной неспециалисту графической модели.

Технические отличия – определение направления на источник звука, учет положения прибора в пространстве, высокая частота дискретизации для сохранения особенностей сигнала.

Проект фазированной акустической антенной решетки

Дальнейшим развитием проекта является высокоточное изучение параметров акустических сигналов. Техническая реализация выполнена при помощи размещения на облегающей тело футболке решетки из n на m компактных микрофонов. Звук от этих микрофонов передается на смартфон и обрабатывается на нем.

Первично для приёма акустических сигналов, используется плотно соприкасающаяся с телом микрофонная решётка 7×3 микрофонов (рис.3).

Полученное устройство представляет собой фазированную антенную акустическую решетку (ФААР) для акустического сигнала – аналог цифровой антенной решетки (ЦАР). Сигнал снимается с частотой не менее 44 кГц с разрядностью 8 и сохраняется на внешнем хранилище. Объем данных равен приблизительно 1 Мбайт/мин.

Переход от небольшого числа микрофонов, позволяющих определить направление на источник звука с антенной решетки, связан с возможностью высокоточной локации источников звука, а также звуковой локации, когда синтезированная диаграмма направленности позволяет последовательно сканировать источники звука без перемещения приемных устройств по телу. Кроме того, ЦАР позволяет обеспечить разрешение так называемого сверхрэлеевского типа.

Анализ спектра (в первую очередь - фазы сигнала) позволяет установить направление и расстояние до всех источников звука [20]. Таким образом, можно определить следующие важные параметры внутренних органов:

- основной сердечный ритм и вариабельность пульса;
- работа желудочков сердца;
- основной цикл дыхания для каждого легкого;

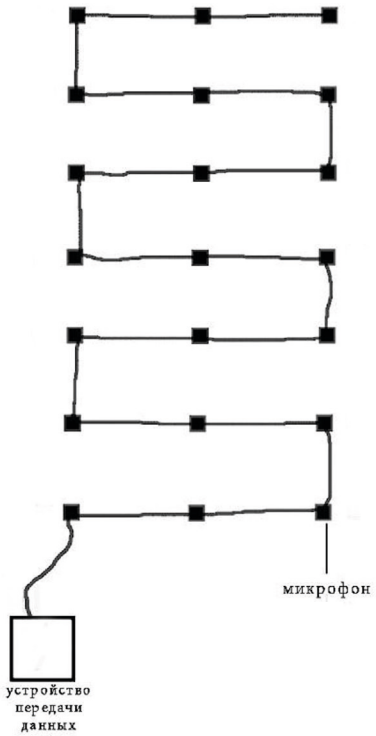


Рис. 3 Реализация применения микрофонной решетки для приема акустических сигналов

- неоднородности и наличие жидкости в легких;
- движение крови в аорте и артериях.

После обработки сигналов можно построить:

- динамическую 3D модель работы сердца и легких;
- модель кровообращения с вычислением функции артериального давления.

Для беременных возможно определить сердцебиение плода и его положение.

В перспективе, изучая гармоники спектра акустических сигналов ФААР, можно установить места отражения звуковых волн и определить:

- места появления опухолей;
- проблемы с кишечником,
- тромбы в сосудах.

Анализ источников акустических сигналов

Как мы заметили выше, фазированная антенная акустическая решётка позволяет с высокой точностью установить направление на звуковой сигнал, а оперирование с частью решётки - вычислить точки пересечения направлений в пространстве. Для этого необходимо разделить ФААР на три (минимум) подрешетки. Тогда пересечение трех лучей в пространстве точно даст расположение источника звука.

Такими источниками будут:

- желудочки и клапаны сердца;
- бронхиальные каналы;
- зоны звуковых аномалий кровеносных сосудов (сужение или расширение), которые дают перепад пульсовой волны и также являются источниками звука.

При движении тела (ходьба, бег, физические упражнения) положение источников звука (сердца и его частей) меняется, и это дает материал для создания динамической объёмной модели, что также является принципиально новым.

Для беременных можно создать уникальную картину изменения положения плода в течение времени, ориентируясь на положение его сердца как источника звука.

Весьма важным является синфазность работы сердца матери и плода. По этому параметру на ранней стадии можно диагностировать множество проблем роста и развития плода, а также спрогнозировать посперинатальный период его жизни.

Отражения звуковых волн идентифицируются по изменению фазы и позволят увидеть:

- жидкость в лёгких;
- неоднородности в тканях;
- уплотнения в печени и почках.

Тем самым решается задача ранней диагностики:

- опухолей;
- непроходимости кишечника и спаек;
- наличие кист.

ОСНОВЫ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ АНТЕННОЙ РЕШЕТКИ

Напомним, что антенная решётка [2] — это совокупность излучающих (в нашем случае – принимающих) элементов, расположенных в определённом порядке, ориентированных и возбуждаемых так, чтобы получить заданную диаграмму направленности.

Будем рассматривать ФААР как аналог цифровой антенной решётки (ЦАР) - антенной решетки с поэлементной обработкой сигналов, в которой сигналы от излучающих элементов подвергаются аналого-цифровому преобразованию с последующей обработкой по определённым алгоритмам [3].

Более общее определение ЦАР предполагает формирование диаграммы направленности как на прием, так и на передачу сигналов: в случае ФААР в первую очередь нас интересует проблема приема сигнала, однако нельзя отрицать возможность и активного воздействия на организм источниками акустических колебаний как с целью диагностики, так и терапии.

Таким образом, цифровая антенная решётка (ЦАР) — пассивная или активная антенная система, представляющая собой совокупность аналого-цифровых (цифро-аналоговых) каналов с общим фазовым центром, в которой формирование диаграммы направленности осуществляется в цифровом виде, без использования фазовращателей [3]. В зарубежной литературе используются эквивалентные термины digital antenna array или smart antenna [4].

В нашем случае ЦАР работает в акустическом диапазоне и на прием.

Различие между ЦАР и разновидностью активной фазированной антенной решётки (АФАР) заключается в методах обработки информации. В основе АФАР лежит приёмопередающий модуль (ППМ), включающий в себя два канала: приёмный и передающий. В каждом канале установлен усилитель, а также по два устройства управления амплитудно-фазовым распределением: фазовращатель и аттенюатор.

В ЦАР в каждом канале установлен цифровой приёмопередающий модуль, в котором аналоговая система управления амплитудой и фазой сигнала заменена системой цифрового синтеза и анализа сигналов [3, 5- 8].

Теория цифровых антенных решёток (ЦАР) зарождалась как теория многоканального анализа (Multichannel Estimation) [9, 10]. Исторически проблема начала обсуждаться и изучаться в 20-х годах XX века для определения направлений прихода радиосигналов при помощи совокупности двух антенн по разности фаз или амплитуд их выходных напряжений [11].

В конце 1940-х годов подход анализа разности фаз привёл к появлению теории трёхканальных радиолокационных антенных анализаторов, обеспечивавших решение задачи разделения сигналов воздушной цели и отражённого от подстилающей поверхности (земли, воды) «антипода» путём решения системы уравнений, сформированных по комплексным напряжениям трёхканальной сигнальной смеси [12]. Результаты экспериментальных измерений с помощью аналогичного трёхантенного устройства были опубликованы Фредериком Бруксом в 1951 г. [13].

К концу 1950-х годов возрастающая сложность решения радиолокационных задач обусловила необходимость применения электронной вычислительной техники [9, 10].

В 1957 г. Бен С. Мелтонт и Лесли Ф. Бейли в своей статье [14] предложили способы реализации алгебраических операций по обработке сигналов с помощью электронных схем, являющихся их аналогами, с целью создания машинного коррелятора (a machine correlator) или машинного вычислителя обработки сигналов на основе аналоговой вычислительной машины.

В результате замещения аналоговых вычислительных средств цифровыми буквально через несколько лет возникла идея использования быстродействующего компьютера для решения пеленгационной задачи, первоначально в отношении определения местоположения эпицентра землетрясения [9, 10]. Б. А. Болт стал одним из первых, кто реализовал эту идею на практике [15], написав программу для IBM 704 по сейсмопеленгации на основе метода наименьших квадратов. Сотрудник Австралийского национального университета Е.А. Флинн использовал аналогичный подход [16].

В Советском Союзе потенциальные возможности многоканальных анализаторов впервые оценил Поликарпов Б. И. [17] в 1961 г. Им были изучены анализаторы фазового типа с равными или кратными расстояниями между фазовыми центрами приёмных каналов, на выходах которых напряжения подвергаются корреляционной обработке. С помощью вычислительных машин определяются угловые координаты источников сигналов. Поликарпов Б. И. указал на принципиальную возможность разрешения источников сигналов с угловым расстоянием, меньшей ширины главного лепестка диаграммы направленности антенной системы (сверхрэлеевское разрешение) [9, 10].

Конкретное решение задачи сверхрэлеевского разрешения источников излучения было предложено в 1962 году Варюхиным В.А. и Заблоцким М.А., которыми был изобретён соответствующий способ измерения направлений на источники электромагнитного поля [18]. Данный способ основывался на обработке информации, содержащейся в распределении комплексных амплитуд напряжений на выходах амплитудных, фазовых и фазово-амплитудных многоканальных анализаторов, и позволял определять угловые координаты источников, находящихся в пределах ширины главного лепестка приёмной антенной системы [9, 10].

В дальнейшем Варюхиным В.А. была разработана общая теория многоканальных анализаторов, основанная на обработке информации, содержащейся в распределении комплексных амплитуд напряжений на выходах антенной решётки [10]. Эта теория рассматривает способы определения угловых координат источников в зависимости от угловых расстояний между

ними, фазовых и энергетических соотношений между сигналами, а также функциональные схемы устройств, реализующих теоретические выводы. Определение параметров источников производится непосредственным решением систем трансцендентных уравнений высокого порядка, описывающих функцию отклика многоканального анализатора. Трудности, возникающие при решении систем трансцендентных уравнений высокого порядка, были преодолены Варюхиным В.А. путём «сепарации» неизвестных, при которой определение угловых координат сводится к решению двух или даже одного уравнения, а определение комплексных амплитуд — к решению систем линейных систем уравнений порядка N [19].

Кратко рассмотрим приёмный канал ЦАР и ФААР. Основа приёмного канала — аналого-цифровой преобразователь (АЦП) [21-23]. Аналого-цифровой преобразователь заменяет в аналоговом варианте реализации активного модуля два устройства: фазовращатель и аттенюатор. АЦП позволяет перейти от аналогового к цифровому представлению сигнала для дальнейшего его анализа в схеме цифровой обработки сигнала.

Для корректной работы АЦП в канале также присутствует ещё малошумящий усилитель (МШУ) [21-23]. МШУ поднимает амплитуду сигнала до требуемого уровня для дальнейшей оцифровки.

Несколько слов необходимо сказать о преобразовании частоты в ЦАР. При работе с сигналами, оцифровка или цифро-аналоговое преобразование которых на несущей частоте является неэффективной (недостаточная разрядность и канальность имеющихся АЦП/ЦАП, их высокое энергопотребление и т. п.), в ЦАР может выполняться одно или несколько промежуточных преобразований частоты [21-23]. Следует отметить, что всякое преобразование частоты вносит дополнительные погрешности в обработку сигналов и снижает потенциальные характеристики ЦАР. Для акустического сигнала это также верно.

ВЫВОДЫ

Новый подход к акустическому анализу позволяет решить массу проблем в области медицинской диагностики. В частности, для акустической ЦАР и ФААР возможны выявление и локация внутри организма объектов, размер которых гораздо меньше ширины диаграммы направленности, что является впечатляющим результатом.

Преимущество цифровой медицины, опирающейся на математические методы, в том числе в области обработки сигналов, заключается в возможности получать результаты высокой точности и глубины диагностики, что позволит не только улучшить качество диагностических процедур, но и сделать их более понятными и доступными как для врачей, так и для пациентов.

На описанный способ подана патентная заявка «Способ акустического анализа состояния организма» [24].

СПИСОК ЛИТЕРАТУРЫ

1. Тихоненко З.О., Тихоненко О.О., Щербаков А.Ю. Цифровые технологии анализа крови // Вестник современных цифровых технологий, 2020. №5. С. 44-48.

2. ГОСТ 23282-91. Решётки антенные. Термины и определения. – URL: http://gostrf.com/normadata/1/4294830/4294830746.pdf

3. Слюсар В.И. Основные понятия теории и техники антенн. Антенные системы евклидовой геометрии. Фрактальные антенны. SMART-антенны. Цифровые антенные решётки (ЦАР). MIMO–системы на базе ЦАР // Разделы 9.3 - 9.8 в книге «Широкополосные беспроводные сети передачи информации». Вишневский В.М., Ляхов А.И., Портной С.Л., Шахнович И.В. – М.: Техносфера. – 2005. С. 542 – 563.

4. Слюсар В.И. Smart-антенны пошли в серию // Электроника: наука, технология, бизнес, 2004. № 2.

С. 62 – 65.
5. Слюсар В.И. Цифровое диаграммообразование- базовая технология перспективных систем связи // Радиоаматор, 1999. № 8. С. 58 – 59.
6. Слюсар В.И. Цифровое формирование луча в системах связи: будущее рождается сегодня // Электроника: наука, технология, бизнес. 2001. № 1. С. 6-12.
7. Слюсар В.И. Цифровые антенные решётки: будущее радиолокации // Электроника: наука, технология, бизнес. 2001. № 3. С. 42- 46.
8. Слюсар В.И. Цифровые антенные решётки: аспекты развития // Специальная техника и вооружение, 2002.- № 1,2. С. 17- 23. Дата обращения: 4 июня 2014. Архивировано 23 декабря 2018 года.
9. Slyusar V. I. Origins of the Digital Antenna Array Theory // International Conference on Antenna Theory and Techniques, 24-27 May, 2017, Kyiv, Ukraine. Pp. 199—201.
10. Слюсар В. И. Развитие схемотехники ЦАР: некоторые итоги. Часть 1 // Первая миля. Last mile. Приложение к журналу «Электроника: наука, технология, бизнес», 2018. №1. С. 72 — 77.
11. Friis H. T. Oscillographic Observations on the Direction of Propagation and Fading of Short Waves // Proceedings of the Institute of Radio Engineers. — May 1928. — Vol. 16, Issue 5. Pp. 658—665.
12. Hamlin E. W., Seay P. A., Gordon W. E. A New Solution to the Problem of Vertical Angle-of-Arrival of Radio Waves // Journal of Appllied Physics. — 1949. Vol. 20. Pp. 248—251.
13. Frederick E. Brooks. A Receiver for Measuring Angle-of-Arrival in a Complex Wave // Proceedings of the I.R.E.- April, 1951. Pp. 407—411.
14. Ben S. Meltont and Leslie F. Bailey. Multiple Signal Correlators // Geophysics. — July, 1957. Vol. XXII. No. 3. Pp. 565—588.
15. Bolt B. A. The Revision of Earthquake Epicentres, Focal Depths and Origin-Times using a High-speed Computer // Geophysical Journal. — 1960. Vol. 3, Issue 4. Pp. 433—440.
16. Flinn E. A. Local earthquake location with an electronic computer // Bulletin of the Seismological Society of America. — July 1960. Vol. 50. No. 3. Pp. 467—470.
17. Поликарпов Б. И. О некоторых возможностях применения независимых каналов приема сигналов и использования электронно-вычислительной техники для повышения помехоустойчивости и разрешающей способности радиолокационных измерений // Сборник «Экспресс-информация», БНТ. № 23, 1961.
18. Варюхин В. А., Заблоцкий М. А. Авторское свидетельство СССР № 25752 «Способ измерения направлений на источники электромагнитного поля». 1962.
19. Варюхин В. А., Касьянюк С. А. Об одном методе решения нелинейных систем специального вида // Журнал вычислительной математики и математической физики. Издание АН СССР, 1966. № 2.
20. Марпл С. Л. Цифровой спектральный анализ и его приложения. Пер. с англ. — Москва, Мир, 1990. 265 стр.
21. Миночкин А. И., Рудаков В. И., Слюсар В. И. Основы военно-технических исследований // Теория и приложения. Том. 2. Синтез средств информационного обеспечения вооружения и военной техники // Под ред. А. П. Ковтуненко. — Киев: «Гранмна». — 2012. С. 7 — 98; 354—521.
22. Слюсар В.И. Идеология построения мультистандартных базовых станций широкополосных систем связи // Известия вузов. Сер. Радиоэлектроника, 2001. Том 44. № 4. С. 3- 12.
23. Слюсар В.И. Многостандартная связь: проблемы и решения // Радиоаматор, 2001. № 7. С. 54 – 54. № 8. С. 50- 51.
24. Патентная заявка №2020135943 от 02.11.2020 «Способ акустического анализа состояния организма».

Беседа С.А. Бородулиной и А.Ю.Щербакова о проблемах искусственного интеллекта

Сделаем небольшое вступление.

Искусственный интеллект, являясь по сути неоднородной областью, постепенно проникает во все сферы жизни человека и общества – от транспортных систем и систем здравоохранения до систем информационной безопасности. Методы, разрабатываемые на основе математического анализа, теории вероятностей, физики, машинного обучения, компьютерного зрения, психологии, лингвистики и биологии, обучения вычислительной техники мыслить подобно человеку, чтобы решать многочисленные задачи реального мира, заменяя человека, дают некоторые результаты.

Компьютер способен анализировать данные, программировать, писать романы и даже побеждать чемпиона по игре в го. Искусственный нейрон, как математическая функция, принимает или обрабатывает информацию, полученную от других искусственных нейронов, затем на выход подается результат. Данный результат может собой представлять большую загадку, с учетом того, что обрабатывающий искусственный нейрон связан с большим количеством входных и выходных нейронов. Предполагается, что такая структура взаимосвязей, соответствующая структуре взаимосвязей живого мозга человека, станет залогом создания человекоподобного искусственного интеллекта. Однако тот факт, что искусственная нейронная сеть обучается на определенном массиве данных, уже ощутимо ограничивает ее область применения. Можно сказать, что речь идет об узкоспециализированной программе. Кроме того, практически невозможно обеспечить полную достоверность обучающих данных, что, разумеется, отражается и на качестве результатов обработки данных нейросетью, поскольку алгоритмы заимствуют ошибки из исходного массива данных.

Умение обучаться на основе полученных данных, а затем принимать решение, безусловно, является важными функциями, присущими и человеческому мозгу, и нейросети, однако это не дает оснований назвать последнюю интеллектуальной по Тьюрингу, так как она, в силу сказанного выше, по-прежнему не обладает разумом, который трудно было бы отличить от человеческого.

О перспективах развития искусственного интеллекта и его месте в развитии современных технологий беседуют Светлана Алексеевна Бородулина, Председатель Правления Евразийского Делового совета, в недавнем прошлом- министр топлива и энергетики Республики Крым, и главный редактор журнала «Вестник современных цифровых технологий»- Андрей Юрьевич Щербаков.

Светлана:

Летом 2017 года Правительством РФ была утверждена программа «Цифровая экономика РФ». Все отмеченные в ней сквозные технологии я бы условно разделила на три части – аппаратно-информационные (компоненты робототехники и сенсорика, квантовые технологии, новые производственные технологии, промышленный интернет), информационно-транслирующие (технологии беспроводной связи, технологии виртуальной и дополненной реальностей) и информационно-формирующие (большие данные, нейротехнологии и искусственный интеллект, системы распределенного реестра).

О последних я и хотела бы задать Вам свой вопрос. Однако начнем с самого загадочного явления, регулярно взрывающего информационное пространство, но, тем не менее, по-прежнему непостижимого для большинства – искусственного интеллекта.

Начиная с середины прошлого века, ученые, писатели, сценаристы и кинорежиссеры говорят о возникновении искусственного интеллекта и даже искусственного разума, но мы можем видеть, что ничего подобного не происходит. Как Вы можете это объяснить и что Вы думаете относительно наступления этого долгожданно-

го события?

Андрей:

Мировые лидеры в области цифровых технологий демонстрируют нам впечатляющие, иногда гротескные успехи по созданию текстов (включая поэзию), портретов несуществующих людей и даже произведений изобразительного искусства, однако мы видим беспомощность этих технологий в критически важных областях общественного производства. Использование подобных алгоритмов в этих областях может привести к плачевным результатам - как если бы за дело взялся интеллект растущего ребенка или психически неустойчивого человека, с той лишь разницей, что объем вмещаемой информации, вероятно, в миллион раз превышает возможности человека. Таким образом, сегодня мы не наблюдаем существенного прогресса в развитии искусственного интеллекта, потому что еще не определены верные средства и методы достижения цели. Да и сам образ, назначение искусственного интеллекта по-прежнему видятся, честно говоря, в весьма абстрактных очертаниях.

Светлана:

Человеку всегда было свойственно мечтать, а в своих мечтах - моделировать будущее. При этом самыми отчаянными романтиками были математики, физики, техники. Как, по Вашему мнению, реализовались их мечты?

Андрей:

Безусловно, многие цели известных ученых достигнуты. Человечество научилось ездить, летать, использовать заряд электрона и преодолевать земное тяготение, но с изменением научной картины мира также, часто неожиданно и непредсказуемо, менялись и средства для достижения целей.

В истории технического прогресса известен эффект имитации - когда техническую задачу предлагалось решить методом подобия, например, полет - при помощи взмаха крыльями, а движение по поверхности земли- за счет имитации ходьбы. Вспомните гениальные рисунки летательного аппарата («махолета») Леонардо Да Винчи.

Но как мы знаем, современные автомобиль и самолёт работают по другим принципам. Аналогичный эффект возник и при разработке искусственного интеллекта (ИИ) - первым этапом создания ИИ стала именно имитация работы мозга при помощи модели нейронов и нейронных сетей.

Классическая диалектика в лице нескольких законов, в первую очередь - закона перехода количественных изменений в качественные, дает нам оптимистичную надежду, что усилия ученых и инженеров когда-нибудь найдут правильное русло, переболев «детскими болезнями».

Светлана:

Действительно, можно сказать, что темпы развития цифровых технологий избаловали современного человека, и его зависимость от информационного комфорта уже не может быть удовлетворена при помощи имитационных методов. В своих выступлениях и работах Вы неоднократно говорили о принципиальных ошибках моделирования интеллекта в современной технике и науке. На сегодняшний день, в чем они, по Вашему мнению, заключаются?

Андрей:

Один из персонажей классической фантастики говорил: «это меня не пугает – это слишком человеческое».

В пьесе Карела Чапека «R.U.R.», написанной в 1920 году, впервые появилось слово «робот», обозначающее искусственного человека, созданного из выращенных тканей и органов для выполнения тяжелой монотонной работы. С этого момента вот уже на протяжении века наука и философия подходят к креативному, созданному человеком интеллекту или человекоподобному роботу слишком по-человечески – оно наделяет его тем же «алгоритмом мышления» и той же структурой органов и чувств.

При этом методы мышления и картины мира могут быть разными. К примеру, совершенно другую картину мира мы можем видеть в геометрии Лобачевского. Расскажу об одном эпи-

зоде из моего личного опыта. Будучи школьником старших классов, я задался вопросом: что может сделать «искусственный ум» (ИУ), который располагает только единицами измерений, размерностями величин? Например, ИУ знает, что время измеряется в секундах, а скорость - в метрах, деленных на секунду. Сможет ли он оценить параметры Вселенной? Например, оттолкнувшись от мировых констант и их размерностей: скорости света, постоянной Хаббла, заряда электрона. Оказалось, что сможет. Для этого он должен составить такие формулы из мировых констант, варьируя их с разными степенями. Получилась совсем несложная программка, но с полностью другой, неклассической логикой. Наука так не привыкла делать. Кстати, эти формулы до сих пор дают довольно реалистичные оценки параметров нашего мира.

Светлана:

Из Вашего личного опыта следует, что принципиально важно для развития искусственного интеллекта - не присваивать ему черты антропоморфного, верно? Может ли этот принцип избавить нас от многолетних опасений, связанных с вероятным негативным и даже пагубным влиянием искусственного интеллекта на ход истории цивилизации?

Андрей:

Да, уже сейчас понятно, что ИИ может и должен иметь различные алгоритмы, а лучше сказать – механизмы мышления, даже шире – разные механизмы преобразования информации.

И весьма ошибочно примеривать к ИИ человеческую этику, которая является продуктом не только нашего разума, но и истории, общества. Многим из нас известны законы робототехники Айзека Азимова, но строить на их основе техническую систему невозможно.

Трудности, с которыми сталкиваются и разработчики ИИ (конкретнее – нейросетей), и те, кто занимаются их (нейросетей) обучением, лежат именно в этой сфере. Например, существующие выборки данных, по которым тренируют нейросеть, отражают как раз текущее состояние общества на современной стадии его развития, и после обучения по ним нейросеть «усваивает», например, расовые предрассудки или представления о женской красоте. Эта проблема, конечно, в большей степени волнует западных инженеров (вопросы расизма более актуальны для американского общества), однако как ее существование, так и внимание к ней показывают, что модели далеко не совершенны и особенно зависимы от социальных и исторических условий.

Принцип «робот не должен причинить вред человеку» звучит однозначно, но в своей сути он противоречив. Для нас же нет сомнений, что топор не должен причинить вред человеку, а Федор Михайлович Достоевский на эту тему написал большой роман, который имеет самостоятельную, но отнюдь не техническую ценность. Подобно любому другому инструменту, искусственный интеллект, вне зависимости от того, на какой основе он работает, способен как приносить пользу, так и разрушать. Например, к какому результату может привести неконтролируемое увеличение количества генерируемых нейросетью изображений человека и их использование?

Оценивая в целом возможности современных информационных технологий, мы видим, что они часто негативно сказываются на человеческом интеллекте, причем вычислительные процедуры могут быть вовсе не обязательно интеллектуальными. Вспомните, что в прежние времена приближение непогоды за несколько дней чувствовали деревенские жители, чуть позже, но тоже заранее – городские жители. Современные люди все чаще обращаются к смартфону, не наблюдая за погодой. Даже на простом примере доступного в любой момент прогноза можно проследить постепенное внедрение мобильного устройства как интерфейса между человеком и окружающим миром. И если человек не может без этого интерфейса сформировать свое мнение (например, о погоде), а затем и модель действий, то «интерфейс», снабженный некоторыми дополнительными алгоритмами, сможет сформировать их сам. В конце концов, заменить человеческий интеллект, подвергнутый определенному влиянию информационных технологий, может оказаться

несколько проще, чем мы себе представляем.

Кроме того, на этапе борьбы с «детскими болезнями» исследований в области ИИ мы, возможно, будем наблюдать настоящие «соревнования в некомпетентности». Известный античный философ говорил, что человек – это животное о двух руках и ногах, лишенное перьев, на что другой философ – его современник - предъявил ему ощипанного петуха. Возникает концептуальный вопрос: не будет ли и ИИ так же оценивать человека? Безусловно, он сможет дополнительно предложить и «широкие ногти», и множество других характеристик объекта «человек», однако не совсем ясна цель создания этой бесконечной цепочки умножения сущностей.

Светлана:

Немецкие специалисты привели пример неразрешимой проблемы для ИИ, который управляет движением железнодорожных стрелок. На одном пути стоит поезд с пассажирами, на другом – уснул пьяный обходчик. В какую сторону направить поезд?

Андрей:

Это как раз логический тупик, навязанный человеческой, даже больше – гуманитарной этикой, которая подсказывает, что поезд куда-то надо направлять. На самом деле никуда поезд направлять не нужно. Его нужно остановить. И оперативно перестроить при этом большое расписание движения, чтобы не допустить опозданий или аварий. А это - задача как раз для ИИ.

Светлана:

Значит ли это, что все философы и футурологи ошибались и не видели совершенно иного, альтернативного сценария развития ИИ?

Андрей:

Не всегда. Бывали и достаточно интересные, даже пугающие прозрения, например, Станислав Лем в романе «Непобедимый» (написанном в 1964 г.) говорил о распределенных системах из простых компонент. Там же эти системы довольно успешно боролись с интеллектуальными системами в лице человека и его техники.

Относительно причинения вреда мне вспомнилось, что по этому поводу сказал в интервью Владимиру Познеру один из основателей фирмы Apple, Стивен Возняк. Он говорил, что на данном этапе скорее человек может причинить вред высокоорганизованным машинам, если, например, будет произвольно стирать данные из их «памяти» или просто выдергивать их из розетки, когда ему заблагорассудится. Следовательно, замешательство поводу того, какая будет (если это понятие уместно) этика у искусственных интеллектуальных систем, не только преждевременно, но и смещает фокус внимания с людей, для которых работа над этикой естественна и обеспечивает их социальное взаимодействие, на неких других, пока еще не существующих действующих лиц, которым этическое измерение не присуще.

Светлана:

Насколько велико влияние искусственного интеллекта на развитие современных технических трендов?

Андрей:

Здесь необходимо учитывать следующие особенности развития науки и техники.

Человеческая техника развивается по принципу «отчуждаемой инфраструктуры». Воин восемнадцатого или девятнадцатого века мог сам сделать порох и пулю, зарядить оружие и выстрелить.

Современный автомат можно сделать и в домашней мастерской, но патроны к нему самому делать сложно и невыгодно. И некий Игрок может в любой момент блокировать или по меньшей мере контролировать применение оружия, производя или не производя патроны.

Второй момент указан в повести «За миллиард лет до конца света». Для специалиста нет сомнений, что в истории техники действует «фактор икс», который сдерживает или просто ликвидирует целые направления науки и техники. Можно даже для первого приближения назвать его «бизнес»: продвигаются только те решения, которые способны принести выгоду,

причем весьма узкому кругу лиц.

Заметил бы еще, что разработчики искусственного интеллекта могут почерпнуть многое из области социальных наук. Еще в 1970-х гг. структуралисты показали, что в «новое время», то есть примерно с начала XVII в., развитие наук, в том числе точных и естественных, самого их понятийного аппарата и методов, не было «нейтральным» или «объективным» и испытывало значительные изменения в зависимости от политического контекста, было частью системы власти и управления. Примечательно, что почти объективный характер носило развитие советской науки.

Однако если, например, вернуться к широко известной, но надуманной «войне СССР с кибернетикой», то в сухом остатке победа школы Норберта Винера привела к ликвидации отечественной школы аналоговых вычислительных машин и в откате советской школы вычислительной математики точно в «хвост» американской системы программирования и разработки вычислителей.

В том случае, если мы видим ИИ не как инструмент власти, а как универсальный инструмент познания, стоит обратить внимание на саму структуру предпосылок, которые привели к его разработке. Это поможет осознать, какие из них несут в себе следы слияния знания с властью.

Светлана:

Исходя из аналогий с романом «Непобедимый», Вы полагаете, что ИИ должен иметь совсем простую структуру, чтобы каждый, по вашим словам, «мог выстрелить сам»?

Андрей:

Именно так. Сейчас мы на тонкой грани. Представим, что Интернет выключен. У него же нет даже формального владельца, и никто нам юридически ничего не обещал, тем более что юридические обещания в современном мире – это особенно пустой звук.

Куда денется вся современная цивилизация? Человек (даже ученый) повседневно использует не очень большой объем информации, он может сохранить его, как говорят программисты, «на локальном ресурсе». А потом, в случае каких-то проблем, восстановить в единую сеть.

Кроме того, «доступность» информации, как мы видим, не приводит к повышению образованности и к появлению стимулов для развития.

Таким образом, решение состоит в том, чтобы остановить безудержную «информационную экспансию», уменьшить накопление отчужденных от владельца данных, уделять время обеспечению их доступности и сохранности, а также постепенно переходить к более «прозрачным», повторяемым решениям по обработке и анализу данных.

Это как раз очень резонирует с тем, с какими трудностями встречаются разработчики нейросетей. Чтобы добиться ощутимого результата в их обучении, нужны огромные массивы информации и доступ к ним, который обеспечивает Интернет и в случае отсутствия которого эти модели первыми окажутся нежизнеспособными. При этом хранение на локальных носителях и восстановление в единую сеть уже опробованы на самом массовом уровне - множество людей используют торренты, чтобы скачивать файлы, фрагментарно хранить их и передавать. Это действительно массовое явление, к участию в котором людей никто не принуждает, то есть существует некая форма добровольного сотрудничества. Можно предположить, что если бы системы ИИ работали схожим образом, то многие не просто имели бы к ним доступ, но и пользовались бы ими с большим энтузиазмом.

Светлана:

В чем Вы видите недостатки подхода к имитации искусственного интеллекта в виде нейросети?

Андрей:

Пожалуй, самый существенный недостаток - непрогнозируемый и неповторяемый результат работы нейросети, что сводит к нулю сам смысл и полезность такого ИИ для человека. Кроме того, надо отметить сложность и трудоемкость настройки и обучения в сочетании с высокой вычислительной сложностью эмуля-

ции нейросети на компьютере, невозможность импортозамещения и доверенной разработки (решения в области нейросетей, как правило, импортные и с закрытым кодом).

Все эти факторы делают непривлекательными как зарубежные решения в области ИИ, так и в целом подход к ИИ, основанный на нейросетях.

Искусственная нейронная сеть функционирует по принципу биологической нейронной сети, уникальной для каждого человека. Но люди с различным мозгом могут коммуницировать друг с другом через язык, письменную и устную речь, через семантику. Семантика и есть основа "реального" ИИ.

Светлана:

В чем заключается семантический ИИ?

Андрей:

Семантический ИИ построен на теоретико-множественном сравнении текстов и изучении статистических свойств текстов.

Для решения задач работы с текстами используется технология небиективных преобразований, когда слова преобразуются в вектора (фактически числа) фиксированной длины.

Представим два «облака» слов-чисел. Теоретико-множественное их сравнение даст картину пересекающихся облаков. Пересечение – это общая часть или общий смысл текстов, левая часть – слова, которые есть только в первом тексте, а правая – те, которые есть только во втором тексте. Чем тексты, мысли, понятия ближе друг к другу, тем больше общая часть «облаков». Ценны также и не входящие в пересечение слова, поскольку они позволяют учесть особенности и различия текстов.

Если в поисковой машине для эффективного поиска мы должны задать довольно точный вопрос, чтобы не «утонуть» в результатах поиска, то при семантическом сравнении мы вполне можем оперировать и достаточно развернутым и не очень точным вопросом. Теоретико-множественное сравнение выручит нас и позволит по степени пересечения смыслов определить близость результата поиска к нашему вопросу. Вполне понятно, что на основе постоянно повторяющихся оценок и движения к более точному (будем избегать слова «лучшему») результату мы сможем реализовать работу ИИ.

Светлана:

Как можно наиболее кратко описать преимущества семантического ИИ перед ИИ, основанном на нейросетях?

Андрей:

Получается, что семантический ИИ, основанный на сравнении текстов, по характеристикам является фактическим антиподом имитационного ИИ.

Например, полная повторяемость и детерминированность работы семантического ИИ, а также то, что он работает и настраивается на естественном понятном языке, не свойственны имитационному ИИ. В этом смысле мы всегда можем заглянуть ему в «голову» и понять как его логику, так и ошибки.

Наш семантический ИИ представляет собой отечественное решение с открытым компактным кодом. Он легко встраивается в "ответчики" (системы типа Алиса или Сири), системы диагностики и прогностики.

В вопросе применения семантики мне кажется очень важным то, что такая модель позволяет преодолеть искусственное разделение между «точными» и «гуманитарными» науками и привлечь к работе над ИИ специалистов из самых разных областей, в том числе лингвистов, культурологов, специалистов по переводу, и вывести эти проекты на междисциплинарный уровень, который реально соответствует глобальным задачам, стоящим перед учеными.

Светлана:

Существует ли практический прототип ИИ на основе семантики?

Андрей:

Да, это проект Ария. Читатель может с легкостью «поиграть» с семантикой на сайте.

Светлана:

В свете вышесказанного хотелось бы перей-

ти ко второму вопросу, вскользь упомянутому Вами- относительно больших массивов данных (Big Data), которые представляют собой фактически бесконечный информационный источник для работы искусственного интеллекта. Собственно для анализа больших данных, исследования закономерностей и прогнозирования событий современному человеку и требуется искусственный интеллект. Как мы понимаем, в современном мироустройстве прогнозированию и аналитическому исследованию отведена ключевая роль, в том числе и в национальной безопасности. Какие разработки Вы на сегодняшний день применяете для работы с большими данными?

Андрей:

Вопрос анализа данных- весьма непростой. Есть классические методы и пакеты анализа данных, например, RapidMiner или TensorFlow, основанные на специализированной нейросети. Здесь важна роль статистики и классических статистических методов. Но есть очень большое «но»: большинство статистических оценок корректно для нормальных, гауссовских распределений. В жизни и в технике не так много процессов, распределенных нормально. Задача аналитика – анализировать данные в рамках корректной математической модели, что реализуется далеко не всегда.

Второй момент – мы незаслуженно забываем классический математический анализ и исследование функций. Для дискретных данных возможно перейти к понятиям дискретной производной, периодичности, спектров функций. Например, на этих идеях можно построить прогностику, что мы и используем в проекте PrognoTech.

Светлана:

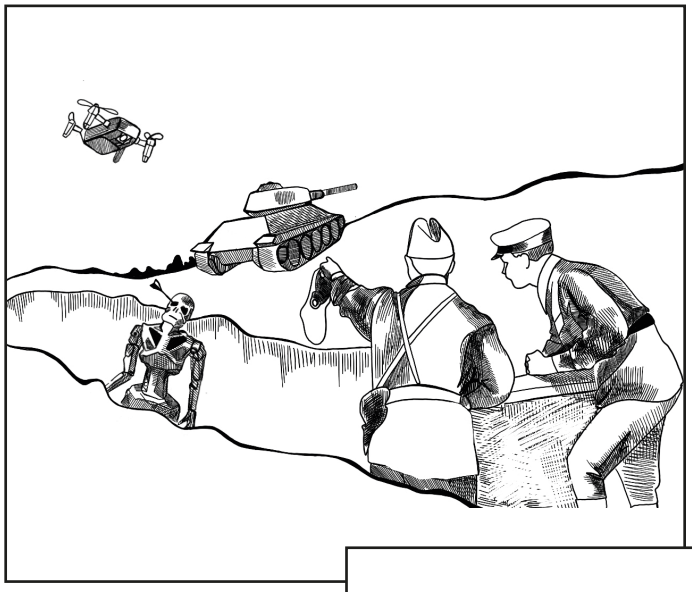
Теперь пришло время задать обещанный вопрос о блокчейне, наверное, самый каверзный и часто вызывающий усмешку. Я читала много Ваших публикаций на эту тему, в частности - Ваше детальное описание различий между технологиями распределенного реестра и технологией блокчейн, направлений их применения, а также среднесрочные прогнозы развития финансовых институтов. Мы хорошо знаем, что важнейшее предназначение распределенного реестра, как способа достоверного хранения информации, понимают далеко не все. Путаница в формулировках, информационный хайп вокруг криптовалют, анекдоты в стиле «по случаю купил у цыган немного биткоинов недорого», исчезновение криптобирж, криминальные сводки про хищения цифровых активов – все это фактически приводит к искажению перспектив технологий распределенных реестров не только в России, но и в мире. Как лично Вы воспринимаете эти тенденции?

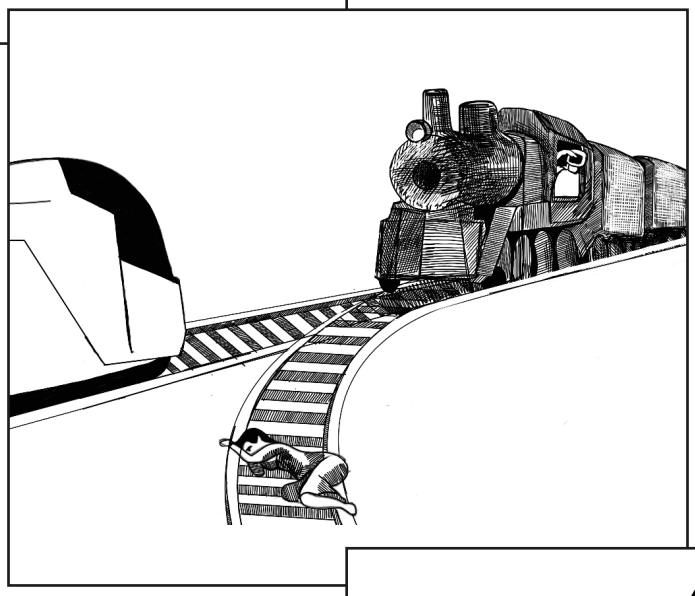
Андрей:

Я думаю, Светлана, что Вы правы – необходимо четко разделять блокчейны для учета криптовалют и распределенные реестры для доверенного хранения данных. Полагаю, что время и объективный подход компетентных ученых все расставит на свои места и мы увидим разумное применение распределенных реестров в финансовой сфере и для решения государственных задач в области экономики и управления. Опять же замечу, что применять зарубежные решения - значит переносить на отечественные системы все те проблемы, которые есть в решениях наших зарубежных коллег и оппонентов, что в основе своей неразумно и нецелесообразно.

Редакция журнала выражает благодарность Светлане Алексеевне за актуальные, интересные, глубоко продуманные вопросы и Андрею Юрьевичу – за содержательные и ёмкие рассуждения на тему перспектив развития искусственного интеллекта.

Иллюстрации на тему искусственного интеллекта





Автор иллюстраций: Мария aka Взломщица

УДК: 279.12

Семантика языка как источник откровения

O. Tikhonenko

Semantics of Language as a Source of Revelation

Abstract. *A semantic and system-analytical approach to the analysis of the sacred texts is applied. This article continues a series of studies on the meaning of the letters of the primary language in which the texts of the Bible were writed. The author used the next two letters of the alphabet as examples, shows that each of the letters is associated with the previous and the next one through large number of semantic, theological and historical meanings and contents.*

Keywords: *Bible, alphabet, letter, digit, meaning, being, mind.*

Тихоненко Олег Олегович
к.филос.н.,
руководитель НКО «Библейская Истина»
E-mail: fzr@bk.ru

Редакционная ремарка: *Олег Олегович Тихоненко, один из оригинальных философов-исследователей и современных богословов, применяет семантический подход к анализу и изучению Священных текстов. Данная статья – продолжение цикла его исследований по смыслу букв первичного языка, на котором были записаны тексты Библии. Приведенный ниже текст содержит мнение автора и не рассматривается в качестве канонического.*

Аннотация. *Применен семантический и системно-аналитический подход к анализу и изучению Священных текстов. Статья является продолжением цикла исследований по смыслу букв первичного языка, на котором были записаны тексты Библии. Автор на примере следующих двух букв алфавита показывает, что каждая буква связана с предыдущей и следующей буквой множеством семантических, богословских и исторических смыслов и содержаний.*

Ключевые слова: *Библия, алфавит, буква, цифра, смысл, бытие, сознание.*

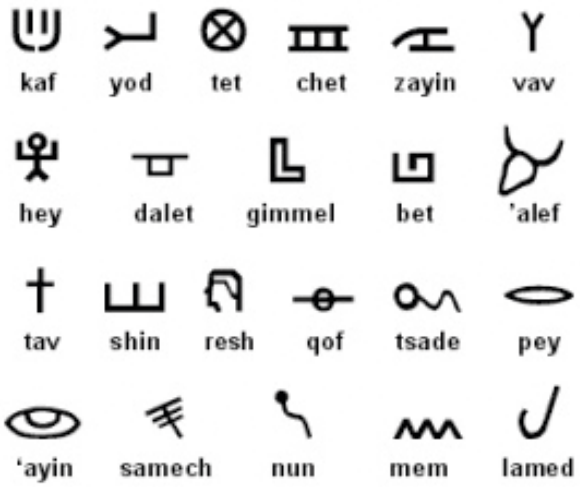
ВВЕДЕНИЕ

В этой статье мы продолжаем открывать для себя глубины смыслов еврейского алфавита, тонкости его влияния на нашу жизнь и наше взаимодействие с окружающей действительностью. Мы последовательно рассматриваем фрагменты еврейского алфавита, и сегодня рассмотрим очередную часть.

АЛФАВИТ ИВРИТА			א 1	ב 2
			а́леф	*бэт*
ג 3	ד 4	ה 5	ו 6	ז 7
ги́мэл	*да́лет*	*hэ*	*вав*	*за́ин*
ח 8	ט 9	י 10	כך 20	ל 30
хэт	*тэт*	*йод*	*каф*	*ла́мэд*
מם 40	נן 50	ס 60	ע 70	פף 80
мэм	*нун*	*са́мэх*	*а́ин*	*пэ*
צץ 90	ק 100	ר 200	ש 300	ת 400
ца́ди	*коф*	*рэш*	*шин*	*тав*

krasnaja-nit.ru

Еврейский алфавит состоит из 22 букв. Каждой еврейской букве соответствует какое-то числовое значение, например, «АЛЕФ»- это 1, а «БЕТ»- это 2. Таким образом, в иврите, чтобы указать число, нужно, по сути, начертать буквы. Каждой букве также соответствует какое-то изображение. Набор таких рисунков, которые использовали четыре тысячи лет назад, называют древнееврейской письменностью.



Проследив историю этих рисунков, можно увидеть, что в каждом из них заключен какой-то смысл. Если мы затем проанализируем

сочетание этих значений в словах, мы увидим глубокие послания, которые описывают наш духовный путь.

Вспомним, какой смысл несет каждая буква, изученная нами в предыдущих статьях.

«АЛЕФ»- это «глава», «вол» или «сила».

«БЕТ»- это «дом».

«ГИМЕЛ» значит «верблюд» или «богач», «щедрый человек».

«ДАЛЕТ» - это «открытая дверь» или «бедняк, принимающий милостыню». «ХЕЙ» - это «откровение». Это пиктограмма в виде подпрыгивающего человека.

«ВАВ»- это «гвоздь» или то, что соединяет.

«ЗАИН»- это «плуг» или «меч духа». Он проникает вглубь земли и разделяет ее. Этот разрез создает ограду, которую символизирует буква «ХЕТ».

«ХЕТ» - это ограда, которая отделяет чистое от нечистого, святое от не святого.

«ТЕТ» обозначает момент принятия решения. Ее пиктограмма - «змея в корзине». Если мы примем неверное решение, эта змея может нас погубить, если же верное - мы перейдем к следующему уровню или следующей букве - «ЙОД».

«ЙОД» - это первая буква Божьего имени и десятая буква по счету. Десять - число совершенства. «ЙОД»- это «правая рука силы».

«КАФ» символизирует помазание и напоминает крылья херувима.

«ЛАМЕД» значит «учить» или «наставлять», а также «жезл власти», «стимул», «наставление».

«МЕМ» значит «открытая утроба», «вода». Она символизирует воду потопа, который создает хаос, а затем приносит новую жизнь («НУН»).

«НУН» означает то, из чего появляется новая жизнь.

«САМЕХ» связывает земное начало и духовное и означает, с одной стороны, гордость и тщеславие, а с другой – Божью благодать и брак.

Продолжим наше исследование еврейского алфавита и узнаем значение следующих букв – «АИН» и «ПЕЙ».

16. «АИН»

ע

Понимание сути этой буквы может преобразить нашу жизнь. Эта буква дарует слепым зрение, а глухим- слух.

Эволюция буквы **«АИН»**.

Пиктограмма **Ктав Иври** **Ктав Ашурит** **Книжный шрифт**

«АИН» - шестнадцатая буква еврейского алфавита. Число 16 символизирует нежную заботу о чем-либо.

Шестнадцать священнических, левитских рангов формировались из глав семейств из сынов Елеазара. Они служили в храме в 24-х чередах наряду с восемью поколениями, принадлежащими к линии Ифамара.

1-я Паралипоменон 24:4 – *И нашлось, что между сынами Елиазара глав поколений более, нежели между сынами Ифамара. И он распределил их так: из сынов Елиазара шестнадцать глав семейств, а из сынов Ифамара восемь.*

Ее гематрия - 70. Мы уже знаем, что, семь - число совершенства, а умножив его на десять, мы получаем полноту совершенства, поэтому 70- это число совершенного духовного порядка.

СМЫСЛ ЧИСЛА 70

Иудеи около семидесяти лет провели в вавилонском плену, потому что они не давали земле покоиться на протяжении семидесяти лет. За это БОГ отправил их в Вавилонский плен, чтобы позволить успокоиться земле, в которой израильтяне не соблюдали Шаббат. Это говорит нам о том, что Бог действительно заботится о Своем творении.

Вспомним о семидесяти старейшинах Израиля, о семидесяти праздничных жертв на Суккот за народы. Семьдесят человек пришли в Египет от Иакова. Иисус отправил на служение

семьдесят учеников.

Луки 10:1 – *После сего избрал Господь и других семьдесят учеников, и послал их по два пред лицом Своим во всякий город и место, куда Сам хотел идти…*

Он послал именно семьдесят учеников, потому что за 1200 лет до этого события на горе Синай жили семьдесят старейшин. Сто лет на каждое колено древнего Израиля, начиная с праздника Шавуот, который мы называем Пятидесятницей. В этот праздник были даны заповеди, и предполагалось, что будет также дан Святой Дух, но израильтяне отвергли Его и отправили Моисея на гору вместо того, чтобы лично встретиться с Богом. Когда были даны заповеди, Моисей находился у подножия горы вместе со всеми остальными. Бог дал всем Свои наставления. Но народ больше не мог выдержать вида грозовых облаков, молний, дождя и грома, и закричал: «Моисей, хватит!». Если бы народ подождал еще немного, то у нас было бы одиннадцать заповедей, но они остановились на десятой, и Моисею пришлось подниматься дальше на гору самому, чтобы получить остальные заповеди. Дух был отвергнут. Через 1200 лет был дан Святой Дух, и на этот раз Его приняли. Началась вторая глава книги Деяний, и она длится по сей день.

Вот почему Отец говорит, что мы должны поклоняться Ему одновременно в Духе и в истине, на обеих временных шкалах. Истина Его заповедей, которая приносит жизнь посредством всех Писаний Библии, и Его Дух, приносящий жизнь воскресения. Мы должны иметь обе эти составляющие.

70 - это число завершения периодов времени.

Даниила 9:24 – *Семьдесят седмин определены для народа твоего и святого города твоего, чтобы покрыто было преступление, запечатаны были грехи и заглажены беззакония,…*

Наши тела на семьдесят процентов состоят из воды. Вода имеет духовную взаимосвязь с нами и с самим Писанием. Почему мы должны быть крещены именно в воде, а не в масле? Мы знаем, что символизирует елей и что было бы гораздо логичнее креститься в нем, а не в воде. Сегодня это выглядит так. Капают масло на палец и изображают им на лбу крест. Однако царей на престол возводили совершенно по-другому. В древние времена елей наливали царю прямо на голову и втирали в волосы. Точно так же поступали с учениками. Если волосы человека были жирными от масла, каждый понимал, что он кем-то любим, потому что помазать может только тот, кто любит. В иврите смысл слова «любовь» гораздо глубже, чем в любом другом языке. Оно не содержит ни малейшей взаимосвязи с сексуальностью. Любовь - это дружба, близость, посвящение, преданность тех, кто любит.

Пиктограмма буквы «аин» символизирует глаз. Она означает «видеть», «понимать» или «быть свидетелем». «Аин» - это внутреннее зрение, живущий внутри нас дух. Это безмолвная буква, которая даже не обязательно передает какой-либо звук.

Сколько было случаев, когда Дух издавал звук? Писание сравнивает Дух с ветром. Мы не можем ощутить Его физически, услышать Его, но мы видим Его влияние, что Он совершает, как появляется и исчезает среди народа Божьего. Все, происходящее в физической сфере, содержит в себе духовное послание.

Бог говорит через Свое Слово, через людей, через Свое творение. Он ежесекундно передает нам послания, в том числе тогда, когда мы еще не приступили к молитве или уже занялись делами. Но мы не знаем, как перевести Его слова. Когда мы смотрим на дерево, мы видим, что оно может раскачиваться, потому что корни его уходят глубоко в землю. Там оно находит воду, Слово, и навсегда остается на этом месте. Одна из самых больших проблем тех, кто находится «под зонтом» Христианства, заключается в том, что они не знают, как укорениться в Божьем Слове и остаться в нем. В действительности мы не ищем Слова, а ищем комфорта, меняем одни формы на другие, более удобные. Мы должны смотреть на все, что нас окружает, и мы увидим послания Божьи.

Матфея 6:22 – *Светильник для тела есть око. Итак, если око твое будет чисто, то все*

тело твое будет светло;

6:23 – *Если же око твое будет худо, то все тело твое будет темно. Итак, если свет, который в тебе, - тьма, то какова же тьма?*

Эта еврейская идиома о глазах говорит о щедрости.

Светильник тела есть око. Итак, если око твое будет щедрым, то все твое тело будет наполнено светом. Если же око твое не будет щедрым, то есть, будет скупым, то все твое тело будет наполнено тьмой. Итак, если свет, который в тебе, - это тьма, то ты скупец, ты мертвой хваткой держишься за свое. Ты не любишь быть в завете. Тебе не нравится, когда кто-то вмешивается в твои дела.

Насколько велика эта тьма? Теперь становится ясно, почему эти слова находятся среди наставлений о деньгах. Может показаться, что этот фрагмент находится вне контекста, но на самом деле в Божьем Слове из контекста ничего не выпадает, напротив, мы не понимаем контекста. Нам надо познавать то, о чем говорят Писания. Мы должны быть щедрыми, как богач, который, как мы знаем, олицетворяет самого Бога. Он щедро благотворит бедняку. Когда вы поступаете так же, Бог дает откровение! Вот почему сказано:

6:24 – *Никто не может служить двум господам: ибо или одного будет ненавидеть, а другого любить; или одному станет усердствовать, а о другом нерадеть. Не можете служить Богу и маммоне (деньгам).*

Мудрецы говорят: доброе око (на иврите «аин това») смотрит в сторону буквы «САМЕХ» (того, кто поддерживает), в то время как злое око смотрит в сторону следующей буквы «ПЕЙ», чтобы насытить собственную алчность.

СЛОВА С БУКВЫ «АИН».

- «Эд (Ed)», что значит «свидетельство».
- «Эда (edah)»- «свидетельница».
- «Амад (Amad)»- «стоять».
- «Амуд (Amud)»- «столб».
- «Эвед (Eved)»- «раб, слуга».
- «Аса (Asah)»- «делать» или «работать».

У нас есть глаза, которые являются воротами нашей души. Все, что мы видим, как в физическом, так и в духовном мире, оказывает непосредственное влияние на наше духовное состояние. Наше восприятие какой-либо ситуации напрямую связано с наставлением, силой, благословением или проклятием Бога в нашей жизни. Если в нашей жизни присутствует проклятие, то, вероятно, мы что-то видим в искаженном свете. Если же наш взгляд не искажен, мы видим только благословение. Мы должны соблюдать величайшую заповедь - «Возлюбите!». Тогда все будет проходить через наш любящий взгляд. Мы не знаем настоящих причин того или иного поведения, истинных источников человеческих пороков. Но даже если мы сталкиваемся с грубостью, неприязнью, несправедливостью, мы должны смотреть на людей так, как на них смотрит Бог- глазами милости, прощения, любви и благословения.

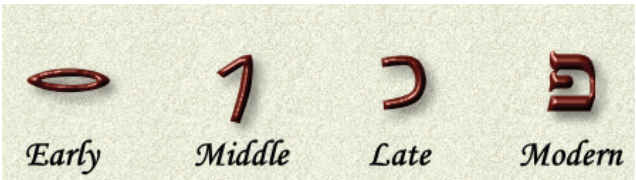
Пророчество, слово, знания, мудрость - все духовные дары приходят через букву «АИН», через духовное понимание. Высочайший из даров – мудрость, названная «кетэр» (вершиной). Она является источником знания и Божьего страха, и Библия говорит, что с ней связано все существующее. Поэтому когда Соломону была дана мудрость, он приобрел и все остальное.

Если у нас добрый взгляд, мы обращаемся к Торе за наставлениями о том, как проявлять щедрость. Если же мы не щедры, нам интересно только то, что люди могут нам дать, но через нас ничто не перетекает к другим.

17. «ПЕЙ»

פ, ף

Так выглядит пиктограмма буквы «ПЕЙ».



Пиктограмма **Ктав Иври** **Ктав Ашурит** **Книжный шрифт**

От нее произошла греческая буква «ПИ». «ПЕЙ» - семнадцатая буква алфавита. 17 - это седьмое по счету простое число. Семнадцать - сумма десяти и семи. Десять означает порядко-

вое совершенство, а семь- духовное.

Числовое значение буквы «ПЕЙ» - 80, восемь, умноженное на десять. Восемь - является числом нового начала, а десять - числом порядкового совершенства. Безусловно, 80 - это очень важное число нового правящего, совершенного порядка.

Именно в возрасте восьмидесяти лет Моисей вывел израильтян из Египта.

Значения буквы «ПЕЙ»: «издавать звуки», «дышать», «говорить», «переносить в реальность посредством слов», а также «заповедь» или «предписание».

Малахии 2:6 – *Закон истины был в устах его, и неправды не обреталось на языке его; в мире и правде он ходил со Мною и многих отвратил от греха.*

Своими словами мы формируем реальность. То, что мы провозглашаем о наших друзьях, близких, об окружающем мире, имеет свойство сбываться. В этом заключается сила сказанного слова, в чем мы постоянно убеждаемся на практике.

«ПЕА (Pa,ah)», номер в симфонии Стронга 06284, означает «расщеплять на части». Здесь мы видим слово «рот» в значениях «расщеплять», «разбивать», «дробить», «разрывать на части». Еврейские концепции всегда тесно связаны с сельским хозяйством, с земледелием, с чем-то, что можно понять на физическом уровне, что имеет непосредственно отношение к нашей жизни.

Псалом 36:30 – *Уста (пей) праведника изрекают премудрость, и язык его произносит правду.*

Притчи 31:26 – *Уста (пей) свои открывает (патах) с мудростью, и кроткое наставление на языке ее.*

Псалом 118:131 – *Открываю (паа) уста (пей) мои и вздыхаю, ибо заповедей Твоих жажду.*

Когда мы открываем уста и произносим слова, мы что-то разрушаем. Мы разбиваем силу Божью или силу врага. Мы должны быть осторожны в своих высказываниях, даже, и особенно, если мы говорим что-то за закрытыми дверями. В библейском контексте наши негативные и злые слова в чей-то адрес являются убийством, потому что они способны разрушать этих людей в духовном мире, уничтожать их репутацию, что, согласно Писанию, равноценно убийству. По сути, то же самое определено и нашим законодательством в отношении тех случаев, когда мы подрываем чью-то репутацию.

СЛОВА НА БУКВУ «ПЕЙ»

«Пей (Pey)» означает «рот».

«Патах (Patach)» - «открывать» или «дверь», «открытая дверь».

«Паар (pa,ar)» - «раскрыть широко» или «зевать».

«Пур (pur)» - «ломать», «крушить» или «жребий».

«Парац (paratz)» - «взрывать».

«Парат (parad)» - «рассеивать».

«Парас (paras)» - «разбивать» или «разбрасывать».

«Пазар (pazar)» - «рассыпать».

«Питом (pithom)» - «вдруг».

«Паним (panim)» - «лицо». Господь говорит: «я хочу видеть вас ‘паним эль паним’», а именно- лицом к лицу.

«Паним Эль (Paniel)» - «Божье лицо».

«Порэ (parah)» - «плодородный».

«Парусиа (parousia)» - «приход» или «присутствие».

«Пурим (purim)» - «жребий».

Как правило, слова на букву «ПЕЙ» связаны с устами, которые либо открывают в нашей жизни Слово Божье, либо дают сатане законное право вторгаться в вашу жизнь.

Вся Вселенная возникла благодаря словам, произнесенным Богом. *«И сказал Господь: “Да будет свет!“ И возник свет» (Брейшит, 1:3). В мидраше сказано: «Десятью изреченными повелениями сотворен мир».*

Именно словом был поднят из гроба Лазарь. Именно в словах выражены наставления для нас. Все исходит из Божьих уст. Структуры власти исходят из уст.

Своими устами мы совершаем один из самых опасных грехов, потому что в притчах сказано, что злые слова проникают глубоко в сердца людей и создают засовы, как в крепости. Своими устами мы можем заточить кого-то в рабство, можем сокрушать сердца. Но в то же время

наши слова могут возродить к жизни того, кто был сокрушен.

Мы опираемся на наставления Божьи, дающие нам совершенное понимание. Обретая совершенное понимание, мы можем провозглашать слово в жизнь других людей своими устами. Если мы не видим правильно, не имеем надлежащего понимания и не смотрим Его глазами, мы должны держать уста закрытыми. Анализируя свою жизнь, мы наверняка заметим, что самые лучшие советы в разных ситуациях нам давали именно те, кто имел правильный взгляд на эти ситуации. Они смотрели глазами Бога и были способны наставлять, потому что опирались на Его Слово. Если же мы опираемся не на Божье, а на человеческое слово, мы не сможем иметь правильный взгляд и погубим кого-то, дав ему ошибочные наставления. Мы провозгласим смерть в чью-то жизнь, даже если будем думать, что провозглашаем жизнь, и навредим ему, даже если будем иметь благие намерения.

Наконец, приведенный выше семантический анализ буквы «ПЕЙ» убеждает нас в том, что никогда не следует принимать какие-либо решения, находясь в состоянии страха. Если мы поступаем правильно и пребываем во власти Бога, нам нечего бояться, потому что Бог дает нам не страх, а силу, любовь и самоконтроль. Однако мы не всегда ходим Его путями, поэтому и существует потребность в духовном руководстве. Но когда мы идем Его путями, опираемся на Его слово, Он дает нам способность видеть все безупречно верно и власть провозглашать жизнь.

Гросс

Егор Федоров
Республика Беларусь,
писатель, сценарист, драматург

Человеку было необходимо выжить - и для этого он добыл огонь.
Человек хотел поменьше ходить и изобрел колесо.
Человек мечтал летать и однажды полетел.
Возможно, скоро цифровые технологии
помогут человеку победить саму смерть.
Ведь главное - хотеть добросовестно.
И тогда получится обязательно.

«У них опять салют».

Гроссмейстер посмотрел на разлетающиеся в небе разноцветные огонёчки, а потом снова вернулся к шахматной партии, которая была сейчас на мониторе компьютера.

Он немного подумал, потом отбросил сомнения и передвинул пешку. Компьютер ответил шахматисту почти без раздумий. Станишевский посмотрел на ход машины и задумался. Лимита времени у игры не было и думать над развитием партии сейчас можно было, сколько угодно.

За окном снова прогрохотало.

В то время, когда гроссмейстер был ещё ребенком, салют давали только на День Победы и на юбилеи советской власти.

«И ещё, кажется, на столетие дедушки Ленина»- припомнил Гросс.

Кличку «Гросс» Станишевский заработал, когда ему было семнадцать лет. Его так прозвали в шахматной школе, где он был на голову выше всех обучающихся. Прилипло. И прилипло настолько намертво, что в двадцать пять лет Кирилл Васильевич Станишевский при обмене паспорта стал Гроссом Васильевичем. Настоящим же гроссмейстером Станишевский стал только спустя двадцать лет на турнире в Турине. Последним, решающим был матч с Алексеем Шировым. Боже, как это было давно. Как будто не в этой жизни.

Гроссмейстер сдвинул теперь ферзя. С компьютером они играли почти на равных. Общий счет был даже в пользу Станишевского.

«В этой жизни, не в этой, - размышлял гроссмейстер. Он снова посмотрел за окно. Залпов больше не было. - Если не в этой жизни, то в какой?»

Позиция на доске была какой-то скучной. И потому мысли Гросса растеклись вокруг вопросов жизни и смерти.

«Что там вообще у нас дальше, после смерти? Мгла и покой? Безмолвие и спокойствие?»

Гросс вспомнил: все мировые религии говорили, что смерть - это не конец.

«А знаешь, все ещё будет» - вспомнил Гросс слова старой песни и тихонечко рассмеялся.

«Ерунда это всё, - подумал Гросс. - Будет гроб, кладбище, сырая земля и черви. А больше не будет ничего».

Станишевский привык жить только своим умом. И то, что он в конце концов стал гроссмейстером, давало ему на это основания. Чужим свидетельствам о загробной жизни он не верил, а ничего другого не предлагалось. Только чужие, недостоверные и непроверенные свидетельства.

Вместе с этим, всю сознательную жизнь где-то внутри гроссмейстера существовало убеждение, что что-то внутри него не умрет. Какая-то его часть - может быть, очень маленькая, незримая, будет существовать дальше.

«Или мне так просто хочется?- спросил себя Гросс. - Сейчас. Когда уже совсем скоро помирать?»

За долгих 70 лет своей жизни Гросс научился себя не обманывать. Просто порой очень сложно было понять разницу, где он сам себя пытается обмануть, а где честен.

С загробной жизнью был именно тот случай.

Станишевский то ли знал о том, что никогда не умрет, то ли только хотел этого.

Гросс посмотрел в окно и достал сигарету.

«Нет, всё таки не может быть, чтоб так просто всё закончилось, - подумал он, подкурил и снова посмотрел на доску. - Раз, и нету меня. Как будто и не было меня никогда».

Компьютер, наконец, сделал ход. Гросс посмотрел и не раздумывая снял с доски ферзя противника.

***

- Ты, Маттео, вот сейчас раскачиваешься на стуле. Упадешь, разобьешь себе лоб, а меня потом посадят в тюрьму, - сказал я. - Оно мне надо?

Группа притихла. Эти обезьяны все время заняты чем-то ещё, кроме шахмат. Шахматы не забирают у них весь ресурс, потому что мир ещё так полон, так богат событиями и чем-то новым. Поэтому для того, чтобы овладеть их вниманием, нужен какой-то выпад. Какая-то неожиданность. Вот как сейчас - про тюрьму.

- Оно мне не надо,- закончил я. - Так что прекращай.

Никита пытается бить пешкой назад. Вадим ходит конем, пытаясь сбить по дороге все фигуры противника. Рита однажды сбила мою белую ладью моей же белой пешкой.

Логика новая и любопытная. Простор для создания новых нейронных связей. Жаль, такие нейронные связи вряд ли где-то пригодятся. Для шахмат такой способ мыслей не нужен, а в жизни - ну черт его знает, где такое применять.

Есть вообще мнение, что шахматы не делают умнее.

Я так не думаю. Это мнение опровергают те дети, которые ходят ко мне. Не то, чтобы я проводил какую-то глубокую аналитику с графиками и диаграммами. Нет. Дело здесь было в том, что я очень наблюдательный человек. При входе в комнату вы сможете зафиксировать 15-20 предметов, которые в ней находятся. Я таких предметов могу зафиксировать 30-40. Я не хвастаюсь, я констатирую. Тем более, в моей наблюдательности нет моей личной заслуги, а благодарить можно мою маму, которая развивала это качество во мне чуть ли не с двух лет.

- Ворожун, у нас не урок пения, заканчивай своё «ла-ла-ла». Амброжевич, чего ты смотришь на меня влюбленно, чей там у вас ход? На доску смотри. Майя, ты могла взять бесплатно слона, чего не брала? Ну как ты делаешь рокировку, Леша? Ты ходишь ко мне второй год, уже пора бы запомнить хоть что-то!

История, которую я вам хочу рассказать, как раз касается моей наблюдательности.

Преподаю я действительно только второй год. Но уже со своими первыми группами я заметил одну странность. Некоторым моим детям никто ранее шахмат не преподавал. Родители играть их не обучали. Книг на эту тему они тоже, очевидно, не читали.

Однако некоторые дети откуда-то знали, как ходит та или иная фигура.

Вообще, этому тоже можно было бы не придавать особенного значения. Мало ли, где они могли подсмотреть. Могли случайно ткнуть в видео-ролик на телефоне или пройти какое-то игровое обучающее видео, увидеть, наконец, партию между кем-то из знакомых в гостях. В общем, я особенного значения этому и не придавал.

Пока ко мне в этом году не пришел заниматься мальчик, которого звали Миша Листопад.

***

Гроссмейстер сосчитал очередной вариант на доске. По всему судя, выходила ничья. Но не предлагать же компьютеру ничью. Как-то это было не спортивно, как говорили во времена молодости Станишевского.

Свою молодость, равно как и всю свою жизнь, гроссмейстер помнил на удивление ясно.

Очень много биографических фактов Гросс мог бы перечислить, если бы понадобилось писать мемуары. Другое дело - и Станишевский понимал это прекрасно - жизнь его не тянула на литературное произведение. Не доставало в ней остроты. Какой-то драматургии. Женщин Станишевский выбирал всегда спокойных, без внутренней личной трагедии. Ему всегда хватало борьбы за шахматным столом - дома он предпочитал спокойствие и тишину. Дети тоже не доставляли больших хлопот - были они какими-то очень обычными. Девочка стала нейробиологом, мальчик - музыкантом (он играл на скрипке в оркестре). В перипетии с большими

деньгами Гросс никогда не попадал. Жил всегда безбедно, нужд и лишений не испытывал. Скука, уныние и рутина. Никаких поворотов и коллизий. Вышла бы одна сплошная графомания. Зачем?

Старик посмотрел на часы. Вспомнил, что с утра он ничего не ел. Есть особенно не хотелось и сейчас. Станишевский подумал о копченой осетрине, что прислал на днях сын - они с филармонией выступали сейчас на Дальнем Востоке. Посылки дети слали достаточно часто. Чувствовали такую необходимость, наверное, оттого, что лично Станишевского почти не навещали. Гроссмейстер подумал, что к осетрине можно почистить картошки.

Гросс не заметил, что сидит у ноутбука в полной темноте. Он поднялся со стула, включил свет, потом вышел в коридор, который вел на кухню.

Из коридора Гроссу внезапно показалось, что на кухне произошло какое-то движение.

Станишевский посмотрел на диван - кошка его тихо мирно сопела на своём любимом месте.

Наверное, всё таки показалось.

Однако тут же у гроссмейстера возникло какое-то неприятное чувство тревоги. Кажется, движение на кухне всё-таки было.

Может быть, в дом забрался вор? Гросс подумал, что такое вполне могло случиться. Дом его снаружи сейчас казался нежилым - свет в окнах не горел, машина стояла в гараже. Сейчас, совсем ранней весной, участок выглядел почти заброшенным. Гросс не раз думал о том, что он будет делать, если в квартиру каким-то образом попадет вор. И каждый раз выходило плохо.

У Гросса был пистолет в ящике стола. Его выхлопотала ещё жена, когда они въехали в этот загородный дом. Старинный приятель Станишевского был прокурором и за разрешением дело почти не стало. Жена занялась вопросом и пистолет вскоре был приобретен.

Но решился бы Станишевский стрелять в человека? Очень и очень сомнительно.

Тем не менее Гросс вернулся в комнату, открыл ящик стола и достал оттуда пистолет.

***

На втором году преподавания я уже чувствовал себя гораздо уверенней, чем на первом. Миша Листопад обнаружился в новом наборе. В самой первой группе, которая пришла в 14-00.

Я показал, где брать доски. Когда все расселились, спросил, знает ли кто-то, как расставлять фигуры. Ещё не было такой группы, чтобы в ней не нашелся тот, кто знает. Обычно, знает где-то треть.

Миша Листопад сидел именно с таким вот знающим мальчиком. Он долго молча наблюдал, как сосед расставляет шахматы на доске, потом внезапно сказал:

- Фианкетто.

Первые уроки проходят, как правило, в тишине. Дети пока ещё присматриваются к учителю. Черт его знает, этого учителя. Вдруг это котокчыч, чудовище. Дети пока ещё стесняются учителя. Они пока ещё скромны и не развязны.

В этой тишине термин, который сказал Листопад, я услышал очень отчетливо. Миша сказал именно «фианкетто» - вывод слона по диагонали от ладьи.

Это меня очень удивило. Дело в том, что этот термин проходят где-то на третьем году обучения.

Но Миша Листопад на этом не остановился. Он все также в каком-то трансе смотрел на шахматы.

- Гамбит, - сказал Миша.

Потом ещё немного подумал и добавил.

- Миттельшпиль.

- Молодец, - сказал я Мише. - Ты уже ходил на шахматы раньше?

- Нет, - ответил мне Листопад. - На шахматы раньше я не ходил.

- Откуда же ты знаешь эти слова? - спросил я. - Миттельшпиль, фианкетто?

- Эндшпиль, - добавил Миша к уже сказанному. - Цугцванг.

Я ничего не понимал.

- Так откуда, Миш? - переспросил я.

- Просто знаю, - ответил мне Листопад. - Ниоткуда.

Вечером того же дня я связался с Мишиным папой и спросил у него, занимался ли кто-то с Мишей шахматами? Нет, ответил мне папа Листопад. С Мишей занимались только рисованием. С трёх лет. Я художник, сказал мне папа

Листопад.

Я крепко задумался над вопросом, откуда шестилетний мальчик может знать все эти термины?

Надо сказать, что шахматы Мише Листопаду по душе не пришлись. Рисовать ему нравилось куда больше, и со временем из шахмат он с увлечением художника стал составлять на доске цветочки. Солнышко. Получалось похоже.

Но эта история о том, что маленький мальчик откуда-то знает шахматные термины, сначала натолкнула меня на интересные мысли, а после привела к одному масштабному эксперименту.

Этот эксперимент, вполне возможно, перевернёт все представления человечества о том, что находится за гранью жизни и смерти.

***

Гросс выставил руку с пистолетом вперед и пошел на кухню.

Свет на кухне зажигался из коридора и Станишевский щелкнул выключателем. Когда по кухне разлился свет, стало несколько уютнее и спокойнее. Может быть, оттого, что ни к каким движениям на кухне включение света не привело.

Гроссмейстер, все также не опуская руки с пистолетом, вошел в кухню. Все здесь, вроде бы, было, как всегда. Только что-то мешало сейчас Гроссу. И он через несколько мгновений понял - что. На кухне явственно ощущался запах перегара. Станишевский бросил выпивать лет пятнадцать назад. Запах этот, конечно же, не забыл. И сейчас переработанный алкоголь просто бил по ноздрям Гросса.

Сам по себе запах, конечно же, появиться не мог. И гроссмейстер понял: на кухне кто-то есть. И этот кто-то сейчас прячется. Станишевский вернулся за порог кухни и сказал пропавшим голосом:

- Выходи. Я знаю, ты здесь.

Вышло как-то очень жалко. Поэтому Гросс решил добавить:

- У меня пистолет, - потом еще немного подумал и сказал. - Он заряжен и я умею из него стрелять.

Старик посмотрел на окно в кухне и понял, как вор попал в дом. Видимо, у него были какие-то специнструменты. Самая большая фрамуга теперь была приоткрыта.

На призыв Гросса, между тем, никто не откликнулся.

- Я звоню в полицию, - сказал Гросс.

Тут старик вспомнил, что мобильник лежит даже не в той комнате, откуда он сейчас пришел. Мобильник лежал в спальне на втором этаже. Станишевскому звонили крайне редко и он не имел привычки носить телефон с собой. Старик мысленно обругал себя. Потом он подумал, что вполне может и сблефовать. Преступник очевидно не знает, что телефона у Гросса нет.

- Или ты выходишь, или на счет три я набираю номер, - сказал Гросс и начал отсчет. - Раз. Два.

Станишевский выждал паузу. Потом сказал:

- Три.

Старик сделал вид, что достал из кармана телефон и приложил к уху.

- Алло, полиция?

В этот момент из-за ниши с холодильником на Станишевского выскочил небольшой, но очень крепкий мужчина, в два шага преодолел расстояние, которое отделяло его от шахматиста и страшным ударом статуэтки гипсового шахматного короля, что стоял на угловом диване кухни, сбил Станишевского с ног.

Король, которого Станишевскому подарили на семидесятилетие, разлетелся на части, пистолет отлетел в сторону. Гросс повалился от удара на пол. Из головы старика тут же хлынула кровь и стала заливать кухню. Станишевский упал так, что видел растекающуюся лужу и думал о том, как много в нём, оказывается, крови. Было больно, но это была какая-то странная боль, не пронзительная и не корежащая. И, к удивлению Гросса, какая-то затихающая.

Через секунду Станишевский понял, отчего боль постепенно затихала. Вместе с кровью на пол кухни из гроссмейстера вытекала жизнь.

Невысокий мужчина поставил остатки статуэтки на пол и склонился над гроссмейстером.

- Эй, дед, - вор потряс Гросса за плечо. - Дед, где бинт у тебя? Йод там? Эй?

Станишевский ничего не ответил.

Мужчина взял руку старика, как будто собирался прощупать пульс. Потом прислонил два пальца к его шее. Было очевидно, что действует

преступник совершенно непрофессионально, никаких данных он из своих действий извлечь не смог. Поэтому вор нашел другой выход. Он закрыл Гроссу пальцами нос. А потом и рот. Подождал так что-то около минуты. И только тогда понял, что дед, которому он только что врезал тяжелой гипсовой статуей, мёртв.

***

После случая с Мишей Листопадом я в первую очередь задумался о том, что шахматы - это игра, которая известна больше двух тысяч лет. Также я подумал о том, что термины, которые произносил Миша - международные. И на любом языке мира будут звучать примерно одинаково.

Здесь, наверное, самое время сказать, что человек я не верующий.

Может быть и не лютый атеист, но агностиком меня можно называть смело.

Однако. Ну вот откуда Листопад мог знать эти термины? Заучивал специально? Исключено. Зачем ему их заучивать?

Научили старшие дети во дворе? Абсурд.

Прочитал? Так тоже нет. Листопаду было шесть лет и буквы для чтения он ещё в слова не складывал.

И ничего мне в голову не приходило кроме того, что Миша Листопад знал эти термины откуда-то из другой, ранее прожитой жизни.

И тогда я подумал: а что будет, если расставить шахматы перед ребенком двух лет? А что будет, размышлял я, если ставить этот эксперимент не с одим ребенком, а с сотней, тысячей? Может быть, у детей есть какая-то память, которая стирается со взрослением?

И что же произойдет, размышлял дальше я, если хотя бы один из двухгодовалых детей внезапно возьмет и сходит пешкой с e2 на e4, а потом - слоном на f4 и станет играть итальянскую партию?

И чем больше я думал об этом, тем больше идея захватывала меня.

Тем более, что в реализации этой идеи не было ничего такого уж невыполнимого. В ясли дети ходили с полутора лет. Что мне мешало лично ставить эксперимент, который я придумал?

- Марат, убери телефон. Чувствую, пока я хотя бы одного кого-то из вас не выгоню, вы так и не поймете, что мы здесь занимаемся шахматами и только шахматами. Клим, сколько стоит слон? Правильно, три пешки. А ладья? Правильно, пять. А зачем ты отдал свою ладью за слона? Вика, здесь глухих нет, прекрати так кричать. Спокойнее.

Все это время я, конечно же, преподавал. И искал какой-то случай, похожий на тот, что произошел с Мишей Листопадом. Но таких случаев больше не было.

Параллельно с преподаванием, я стал смотреть в соцсетях, кого и куда разбросала судьба из моих одноклассников и одногруппников по институту.

Говорят, что если хотеть чего-то по-настоящему, вся Вселенная будет тебе помогать. Один из моих одноклассников, Сергей Козловский, после пединститута поступил на работу в Министерство образования. Там он сделал неплохую карьеру и занимался как раз детскими садами. Встретиться со мной Сергей не отказался.

***

Сначала не было ничего. Потом возникло состояние абсолютного покоя.

Следом за этим состоянием появилось состояние сна.

А ещё потом Гросс проснулся.

Станишевский очень удивился этому своему пробуждению.

Он ничего не видел, ничего не слышал и вообще кажется, ничего не чувствовал. Тела, во всяком случае, у него, вроде бы, никакого не было.

Было только сознание.

Самое восхитительное во всем этом было то, что это сознание помнило, что оно - Гросс Васильевич Станишевский, гроссмейстер по шахматам 72-х лет. Что рожден Гросс Васильевич в стране СССР, городе Ленинграде, имя при рождении имел Кирилл. И ещё огромное количество фактов помнило о себе это сознание. Совершенно отчетливо помнил Гросс сосредоточенное лицо невысокого крепкого мужчины, который отводит для удара руку с гипсовым королем, на котором красиво вылеплена большая цифра 70. Помнил Станишевский страшный удар, боль, которую этот удар причинил, и то, как выливалась на пол из тела Гросса Васильевича жизнь.

Потом...А что было потом, после того, как Гросс умер?

После этого все было таким смутным, таким путанным и таким пугающим, что Станишевский понял - сознание его в этом «потом» сжалось в комок и ничего в нем не было кроме страха, ужаса и отчаяния.

Даже то, что оно живо, сознание, кажется, не разобрало. Оно было напугано и ошеломлено происходящим вокруг подобно котенку, попавшему в зоопарк с открытыми вольерами и вольно разгуливающими животными.

Сознание Гросса в тот момент мечтало только об одном - чтобы происходящее прекратилось.

Потом Станишевскому показалось, что сатаны, которые окружали котенка, вовсе не хотели его уничтожить или умучить, а были заняты каким-то сложным процессом, которого котенок постичь и понять был не в состоянии. Сколько длился этот процесс, Гросс не имел представления. Может быть годы. А может быть минуты.

Больше Станишевский не успел подумать ни о чем. Потому что он снова погрузился в сон.

***

- И что, ты во все это действительно веришь?

Мы с Сергеем Козловским сидели в баре неподалеку от Министерства образования. Я пил пиво, Сережа заказал себе двести коньяку. Судя по всему, в этом баре он был завсегдатай. Не исключено, что доза в двести коньяка у него была не по случаю нашей встречи. Просто в этом баре он каждый день так снимал стресс. Делать карьеру в министерстве образования - дело, я думаю, непростое.

- Сергей, ты не подумай ничего такого, - сказал я. - Я не кришнаит и не индуист...

- В переселение душ верят скорее, буддисты, - перебил меня Кэз. Он махнул стопочку коньяку и аккуратно закусил салатиком. Был взрослый Козловский весь какой-то аккуратненький, весь ухоженный, весь напомаженный. Я его помнил совсем другим. Впрочем, без сомнений, передо мной был все тот же Кэз, с которым мы в подъезде пили водку в одиннадцатом классе и с которым получали звездюлей от гопоты в Серебрянке, куда нас однажды занесло глубоко вечером.

- Пусть буддисты, - сказал я. - Не важно. Важно, что я – не они. Я оперирую фактами, понимаешь? Фактами, которые я тебе только что изложил.

- Ну, а что ты, собственно, хочешь отыскать, я не пойму? - Серёжа взял салфетку и промокнул рот.

- Понимаешь... а вдруг кто-то из этой тысячи детей, с которыми я собираюсь ставить эксперимент... Вдруг кто-то возьмет и начнет играть со мной в шахматы?

- Ну ты хватил, - рассмеялся Кэз. - Играть начнет с тобой. Скажи ещё, поставит тебе мат.

- Ну, а если, Сережечка, если? - спросил я. - А если все-таки возьмет и поставит? Ты представляешь тогда, какой случится огромный резонанс из такого вот происшествия?

- Гм, - Козловский прекратил смеяться. Немного подумал. - Честно говоря, мне представить такое как-то ну очень сложно.

- А ты попробуй, - сказал я и понял, что сейчас буду покупать Сережу. - Ну так, на секундочку, просто попробуй. И представь, чья фамилия, кроме моей, будет после такого события во всех газетах мира, во всех новостях?

- Ну, ты скажешь, - Сережа налил себе из графинчика ещё коньяку. - Ты когда последний раз брал в руки газету-то?

Тут я всей своей наблюдательностью понял: Кэз уже в деле. Сейчас мы просто будем говорить о подробностях этого дела.

- Газету последний раз в руки я брал вчера, - я улыбнулся. – Как бишь, её название. Вспомнил. «Целебник»! Бесплатно в ящик кидают. Но тебе, наверное, не кидают. У тебя в доме, поди, сидит злой консьерж.

- У меня частный дом,- тоже с улыбкой ответил Кэз. - Потому да, спам мне не приходит.

- Ну не суть, Серый, - как с можно большим воодушевлением сказал я. - Что ты, в конце концов теряешь, если напишешь мне эту бумагу?

- Думал уже об этом, - сказал мне хитрый и расчётливый чинуша С. Козловский. - Ничего. Вроде как ничего я потерять не могу.

- Вот, - сказал я.

И тут совершенно неожиданно сам для себя я вспомнил отчество Кэза.

- Ну тогда что, Сергей Леонидович. По рукам?

- Давай-ка ещё раз обсудим эту бумагу, кото-

рая тебе нужна, - вздохнул в ответ Козловский. - Но принципиально я ничего против не имею.

***

Когда Станишевский проснулся во второй раз, он уже совершенно явственно ощутил, что находится сейчас не в мире мертвых, а в мире живых.

Ни зрения, ни слуха у Гросса по-прежнему не было. Но теперь он явственно почувствовал, что в нём есть жизнь. Кажется, Гросс теперь даже уловил, как бьется его сердце. Но окружающий мир по-прежнему был не доступен для восприятия.

Станишевский стал размышлять о том, что произошло там, в зоопарке с неведомыми чудищами.

Теперь ему казалось, что это было некое судилище. И эти сатаны, которые его окружали - теперь казались кем-то, кто оценивал, как Станишевский прожил свою жизнь. Кто решал, куда его далее сейчас следует направлять.

Хотя... Гросс подумал о том, что, скорее всего он сейчас фантазирует. По мотивам, так сказать, прочитанного и усвоенного в прошлой жизни. Станишевский покопался в воспоминаниях о том кошмаре, в котором он очутился сразу после смерти и понял, что часть событий из происходящего он сейчас просто не помнит. Гросс удивился. Вполне могло статься, что в следующее своё пробуждение он просто будет иметь лишь какой-то очень слабый след от тех событий. Остальное будет только его домыслами.

Гросс заинтересовался - а помнил ли он остальную свою жизнь? Сейчас, во втором своём пробуждении Станишевский помнил, кажется, гораздо меньше чем тогда, когда проснулся в первый раз. События из жизни Гросса Васильевича очевидно, стирались и блекли. Явственно сейчас Станишевский мог вспомнить только лишь что-то очень уж яркое - например, своё поступление в шахматную школу. Или первую свою девушку.

Затем Гросс подумал, что если начать разматывать свою жизнь, все нормально вспоминается. Он вспомнил беременность жены, рождение Ани, первого своего ребенка. И ему стало несколько спокойнее. Он даже припомнил, как пару часов бродил вокруг больницы, когда жена рожала. А потом вспомнил свою радость в тот момент, когда он вернулся и акушер ему сообщил, что все прошло успешно, что и с женой, и с Аней все в полном порядке. Также вспомнил, как на волне той радости обещал врачу привести пару бутылок коньяку. И с огорчением подумал о том, что так и не привез. Все-таки память стиралась. Но пока как-то очень избирательно.

Тут Гросс почувствовал, что ему нужно что-то сделать. Чувство это ширилось и росло.

Но что надо сделать, до Станишевского долго не доходило.

А потом. Когда, наконец, это стало ясно, Гросс Васильевич Станишевский открыл глаза.

***

Заведующая д/с №400 побарабанила пальцами по столу.

Она снова заглянула в бумагу, что я ей дал.

- Так, - сказала она. - И что, Вадим Аллахиярович, требуется от меня?

- Вадим Аллахияров, - поправил заведующую я. - Если вам угодно по отчеству-то Сергеевич.

- Простите, - сказала заведующая и снова заглянула в бумагу. - Вадим Сергеевич. Но тем не менее... Что требуется от меня?

- Да ничего особенного, - ответил я. - Представить меня воспитателям. Объяснить, что я тренер по шахматам. Хотелось бы, чтобы вы дали мне, так сказать, полномочия.

Я вежливо улыбнулся.

- Ну что ж, - заведующая пожала плечами. - Пойдёмте.

Дело, в общем, закрутилось.

Кэз выдал мне мощный документ из Министерства образования. Я и не ожидал, что эта бумага будет действовать так на всех этих заведующих и их заместителей в детских садах. В каждом из детсадов мне шли навстречу. Где-то даже пытались накормить обедом - от него я всегда отказывался.

Первых сто детей, перед которыми я расставлял на доске фигуры, не принесли ровным счетом никаких результатов. Дети, конечно, интересовались этими куклами, которых видели чаще всего впервые. Но не более того. Никто из них не стал ходить правильно. Никто из них не назвал ни одной фигуры хоть как-нибудь верно. Никто из них не стал вторым Мишей Листопадом - не говорил со мной шахматными терми-

нами.

Ничего не дали и вторые сто детей.

На третьей сотне я задумался, а занимаюсь ли я вообще хоть чем-нибудь полезным?

На четвертой сотне я стал уже думать о том, что скоро закончатся детсады моего Фрунзенского района и надо будет ездить уже гораздо дальше от дома, чтобы продолжить мои научные (а скорее - псевдонаучные) изыскания.

Но на пятой сотне детей, списки которых я уже даже перестал фотографировать, меня, наконец, ждал сюрприз.

***

После того, как Гросс открыл глаза и стал понимать, что день вокруг сменяется ночью, он стал размышлять о том, где он сейчас оказался.

Ощущения тела по-прежнему не было. Слух появился вместе со зрением, но с ним все обстояло ещё хуже, чем со зрением - почти никакой информации о происходящем слух не давал. После третьего пробуждения Станишевский пришел к выводу, что он находится в материнской утробе.

Память, между тем, стиралась уже очевиднее. Гросс помнил ещё события своей смерти, помнил также какие-то самые важные вехи в своей жизни. Матч, после которого ему присвоили гроссмейстера, смерть отца, женитьба дочери. Это все ещё было, но постепенно отдалялось. Радость, которую испытал Гросс когда догадался, что он снова проживет ещё одну жизнь и что сможет в этой своей новой жизни рассказать о том, что никакой смерти-то, оказывается, и нет, постепенно проходила. Она сменялась пониманием того, что примерно к тому моменту, когда он снова выйдет в мир, в котором снова предстояло прожить ещё одну жизнь, ничего такого он о себе помнить уже не будет. И ничего с этим поделать было нельзя. Каждое новое пробуждение в утробе уносило с собой что-то из его памяти. Наверное, и память о том, что он Гросс Васильевич, рано или поздно должно была покинуть его.

Дело ещё осложнялось тем, что моменты пробуждения были очень кратковременными. И на то, чтобы что-то попытаться вспомнить что-то ещё и как-то это зафиксировать – на это попросту не было времени.

В какое-то из своих пробуждений Гросс понял, что и соображать с каждым разом он начинает все хуже. Чувство осознанности, понятийный аппарат куда-то исчезали. Вернее даже было бы сказать по другому - Кириллу Станишевскому понимать что-то становилось попросту не нужно. Кириллу? Станишевский задумался. Кажется, его звали как-то по-другому. Но как? А всё равно. Было очень хорошо, очень уютно и комфортно вот так безмятежно лежать. Наслаждаться теплом материнского тела, получать через него пищу. А вся эта способность что-то понимать... Зачем? Это становилось чем-то неинтересным, скучным. Навязчивым даже, ненужным.

И постепенно осознанность Станишевского смещалась куда-то на периферию сознания.

Эмбрион превращался в человека.

***

- Ну что? Давай поиграем?

Эту фразу я за сегодня, кажется, повторил уже раз двадцать. А за две недели до сегодняшнего дня - уже раз пятьсот.

Я находился в четвертой ясельной группе за сегодняшний день. Последней, по моему плану.

Я уже давно перестал интересоваться именами детей, которым показывал шахматы. На это тупо не было времени. Да и нужды, признаться, в этом не было почти никакой. Выдающихся результатов не показал пока никто.

Безымянный мальчик лет двух, что сидел сейчас на ковре напротив меня, хотя бы не пытался уползти. Он даже проявил интерес, когда я высыпал на ковер шахматы.

Реакция детей на мои потуги делится на три типа - «разрушение и уничтожение», «иди в баню» и «что это за куклы?».

С первым типом реакции вроде все понятно. Бурим и смеемся.

Во втором типе дети пытаются уползти от этого стрёмного лысого дядьки.

В третьем типе дети берут шахматные фигурки в руки и изучают их.

Ходить фигурками пыталось человек десять из всей полутысячи подопытных, то есть ничтожно низкий процент. Ну и ходили они как попало, ничего похожего на шахматные ходы не было.

Я расставил фигуры. Походил пешкой. Сде-

лал приглашающий жест рукой.

- Прошу, - сказал я. - Теперь ты.

Безымянный мальчик сначала стал действовать по третьему типу реакций. Он взял в руки пешку, повертел её в руках. Потом поставил пешку обратно и сделал ею ход наискосок.

Что ж. Хотя бы так. Я походил конем.

Мальчик ответил мне уже другой пешкой и снова наискосок. Мне стало интереснее. Я вывел слона и поставил его наискосок от пешки мальчика. Тот подумал немного. Потом сбил моего слона так, как бьют в шашках. Мой интерес усилился. Кажется, мальчик играл со мной в шашки. Мы сделали ещё по ходу. Мальчик, которому не было и двух лет, действительно пытался играть со мной в шашки. Я достал телефон, чтобы записать нашу игру на видео. Это стало моей фатальной ошибкой. Шахматы сразу перестали интересовать безымянного мальчика. Теперь его интересовал только мой телефон. Я понял, что на сегодня партия для нас окончена и пошел к воспитательнице.

- Закончили уже, Вадим Сергеевич?

- Нет, - ответил я. - Если можно - имя и фамилию вон того мальчика? С телефоном.

- Вы не боитесь, что он вам его разобьет? Сами понимаете, никто за это нести ответственность...

- Нет, не боюсь, - улыбнулся я. Не боялся я только потому, что такая мысль просто не пришла мне в голову. - Он у меня бронированный. Специально для детей. Так все-таки, как его зовут?

- Это Владик Швец.

- Низкий вам поклон. Могу ли я как-то связаться с его родителями?

***

Гросс Васильевич Станишевский почувствовал, что его уютный и безопасный мир перестает быть таковым.

Все в нём, в этом мире, сейчас пришло в движение. Нельзя сказать, что здесь до этого совсем уж все было недвижимо - конечно же нет. Но сейчас, кажется, миру Гросса наступал конец.

Сначала Вселенная Станишевского стала сдавливать и выпихивать Гросса куда-то вниз. Хоть и не было никогда в этом мире такого представления, как «низ» или «верх», Станишевский отчего-то почувствовал, что движется он именно вниз. Затем куда-то пропала жидкость, что окружала Гросса все это время. Сразу после этого Станишевского стало крутить вокруг своей оси и снова толкать, толкать, буквально ввинчивать головой во что-то не очень-то податливое, во что-то упругое и сжатое. Потом что-то стало происходить и с самой головой Гросса - кажется что-то там сжалось в ней, потом голову стало как-то подворачивать и загибать, вместе с этим Станишевский чувствовал, что какая-то непреодолимая сила изгоняет его из этого мира - мира, в котором было так хорошо и так уютно. А следом за этим ... Следом за этим Гросса ослепил яркий свет, потом схватили чьи-то руки и влепили такую пощёчину пониже спины Гросса, что Станишевский просто заорал от этой боли.

Гросс ещё помнил матерные слова и произносил сейчас именно их, но выходило что-то, кажется, совсем другое. Впрочем, Станишевскому было сейчас все равно, что у него там выходило. Он орал и ругался на того, кто причинил ему боль, хотелось обратно туда, где он так чудесно проводил время. Сейчас его слепил яркий свет, обжигал холодный воздух, на Гросса навалилась сразу тысяча звуков - все это горе обрушилось на него одновременно и он орал, орал, орал...

А потом те же руки, что избили его, положили на что-то мягкое и теплое и очень-очень знакомое, а совсем другие руки, очень добрые и ласковые, успокоили Гросса, утешили и уняли. Руки гладили и обнимали его, руки окутывали и обвивали. С этими руками худо-бедно уже можно было жить и мириться с происходящим.

Спустя какое-то время Станишевский снова заснул.

- Марк, - тем временем сказал тёплый, полный любви голос над Гроссом. Руки снова погладили его и обняли. - Марк...

***

- Это все твои результаты? - мы снова сидели с Сергеем Козловским в баре неподалеку от Министерства образования. Он снова взял себе свои двести коньяку и смотрел в лист с отчетом, который я ему предоставил.

- А ты считаешь, это не результаты? - спросил я.

- Ну..., - Кэз перевернул листок, как будто искал на обороте продолжения отчета. Никакого продолжения там, конечно же, не было. - Я бы не сказал, что это какой-то прорыв.

- Если бы у меня был какой-то прорыв, - я сделал глоток своего пива. - Мы бы, Сережа, с тобой сидели не здесь, А созывали бы сейчас пресс-конференции и готовились стать знаменитостями. И, может быть, даже - миллионерами.

- Ладно, - Кэз вернул мне мой листок. Мне не очень-то понравились эти его реакции. Кажется, Сережа больше вообще не верил в мою идею. - Что ты хочешь от меня теперь?

- Теперь я хочу попробовать с детьми ещё младше, - ответил я.

- Ну... - Кэз неопределенно пожал плечами. - А я-то уже здесь при чем?

- Ты здесь при том, что мне нужен доступ в детские дома. К полугодкам. И ещё меньше.

- А, - протянул Кэз. - Вот как... Виталя! Повтори-ка! Да-да, ещё двести.

Тут я обратил внимание, что Серж был сегодня не напомажен и напудрен. Был сегодня Сережа помят и как-то в целом несвеж. Чувствовалось, что Козловский превышает возможности организма по переработке алкоголя. Кэз, видимо, считал эту мысль в моих глазах и решил объясниться.

- Сын у меня родился, - сказал он.

- О, - протянул я с искренней радостью, - поздравляю, Сережа, поздравляю. Ну, не буду оригинальным. Как назвали?

- Марк, - ответил Кэз. - Слушай, Вадя, а тебе не кажется, что ты куда-то не туда бежишь? Может быть у тебя методологическая ошибка?

- Методологическая?

- Ну да, - сказал Сергей. - А что, если дети тебя не воспринимают как партнера по игре? Ты же не папа им, не мама. Чужой лысый дядька. Давай, может быть, попробуем по-другому...

***

Почти вся память Гросса Станишевского смылась после его явления на свет.

Так смывается краска с моющихся обоев. То есть что-то можно было бы ещё разглядеть там, где ещё совсем недавно был такой красивый и четкий рисунок, но для этого уже нужно было очень пристально вглядеться. Вглядываться сейчас в тот, предыдущий рисунок, было некому. Во-первых, у Гросса сейчас появилась масса новых дел. Мир вокруг был нов и удивителен и ум Станишевского был поглощён тем, чтобы разглядеть, впитать и, может быть понять те новые обстоятельства, которые его окружали. Во-вторых, у Гросса теперь появились заботы и хлопоты - ему сейчас приходилось самому себе добывать пищу. Ну и в-третьих, поверх старого рисунка на моющихся обоях постепенно стали наносить новый рисунок, совсем не напоминающий прежний. Согласно этому, новому рисунку, Гросс узнал, что зовут его теперь уже Марк. Очень как-то быстро он привык к своему новому имени и постепенно старое имя «Гросс» стало каким-то далеким и к нему мало относящимся.

Однажды, когда Марку стукнуло три месяца и он уже умел неплохо различать предметы, на столике рядом с тем, где его переодевали, Марк заметил фигурки на доске. Фигурки эти были ему знакомы так, как не был знаком ни один предмет в окружающем его мире. Он потянулся к этим фигуркам своими малюсенькими ручками и стал голосом просить Большое Существо, в котором была пища для него, чтобы Существо ему помогло. Существо почти всегда понимало, чего хочет Марк, не подкачало и сейчас. Оно протянуло ему одну из фигурок - это был шахматный конь. Вместе с этим Существо стало произносить какие-то очень странные звуки, которых до этого не произносило никогда. Марк удивленно посмотрел на Существо. Звуки эти были резкими и противными.

- Иго-го, - старалась мать Марка. - Иго-го.

Марк попросил Существо помолчать. Он разглядывал коня, потом попросил Существо, чтобы оно дало ему возможность рассмотреть поближе остальные фигурки и доску, на которой они стояли. Но теперь Существо не разобралось в просьбе Марка. Даже ту фигурку, что была у Марка в руках, оно теперь забрало и поставило обратно туда, где стояли остальные.

На шахматную доску.

***

17 февраля 2021 года около тысячи жителей города Москва, имеющих младенцев от 3 месяцев до года, получили небольшое письмо.

Часть этих писем так и осталась лежать в по-

чтовых ящиках так и не забранной, часть отправилась прямиком в мусор, как спам. Примерно половина была распечатана и прочитана.

Предложение, содержащееся в письме, было необычным. Суть письма сводилась к тому, что «если у вас есть дома шахматы, расставьте их перед своим ребенком и попробуйте с ним сыграть. Если у вас получится хоть что-то - напишите мне». Далее шел адрес электронной почты.

У примерно половины получателей шахмат дома не оказалось. Половина из тех, кто шахматы имел, сразу же расценили предложение не заслуживающим внимания и выбросили его из головы. Из оставшихся ста человек у половины не оказалось времени для того, чтобы расставить шахматы перед ребенком. Из тех пятидесяти, что расставили, оказался Гросс Станишевский.

Которого теперь звали Марк Эйхбаум.

***

Прошло пять лет.

Я больше не шахматный тренер. Я работаю в корпорации «Клото». Так зовут древнегреческую богиню, что прядет нить жизни.

Мы продаем людям знание о том, есть ли у того или иного младенца активность мозга в материнской утробе. Или её нет.

Зачем?

По тому, есть ли такая активность, можно с большой долей вероятности сказать - является ли младенец «перерожденцем» - человеком, который приходит на Землю не в первый раз.

Или это будет человек, чьей душе только ещё предстоит зародиться.

Если, конечно, вообще предстоит.

По возникшим за последние годы представлениям, так называемая «душа» не выдается без разбора всем и каждому, кто приходит в этот мир.

«Душу» нужно в себе зародить. Затем душу следует взрастить и укрепить так, чтобы она смогла пройти через смерть тела. Удается это, конечно же, далеко не всем.

После того, как обнаружился Марк Эйхбаум, который в четыре месяца откуда-то знал, как играют в шахматы, стало совершенно очевидно, что некоторые люди рождаются на Земле не впервые. Это был не трюк, не фокус и не любая другая мистификация, поскольку четырехмесячного ребенка нельзя научить играть в шахматы.

После появления Марка мои исследования продолжались уже при серьёзной финансовой поддержке. Благодаря этим исследованиям мы стали выявлять «шахматистов» с завидным постоянством. Надо сказать, что мне сильно повезло, когда я делал первые свои шаги. Такие, как Марк Эйхбаум, встречались крайне редко. Из почти ста тысяч наших подопытных мы выявили Марка и всего ещё двух. В меньшей степени, но тоже парадоксально хорошо из этих ста тысяч шахматной игрой владели ещё три десятка детей. А это, я вам скажу, был уже результат.

Этим результатом заинтересовался по-настоящему крупный бизнес. Ничего удивительного - вопросы жизни и смерти всегда приносили и будут приносить колоссальную прибыль. Вы думаете, человеческая жизнь не измеряется в долларах? Ещё как измеряется. Тем более, если речь идет о приобретении ещё одной, следующей жизни. Наши исследования имеют вектор именно такой - если нам рано или поздно удастся отслеживать, в каком месте появляется тот или иной человек при перерождении... О, какие это лютые миллионы и даже миллиарды. Но пока до этого ещё далековато всем участникам «забега» - а в эту область науки устремились очень многие. Подобными исследованиями занимались и раньше, но такого огромного количества денег и, соответственно, такого количества «мозгов», занятых в этой области, не было никогда.

«Шахматистов» конечно же, больше никто не выявляет - с этим вопросом все более или менее уже понятно. Исследования касаются электрического сигнала, который излучает мозг младенца в материнской утробе.

В исследованиях электрических сигналов мозга младенца в утробе раньше заключалась одна большая проблема: их нужно было проводить активным зондированием плавающей частотой. А это - вмешательство с непредсказуемыми последствиями для здоровья младенца. Прежде всего непонятно, что будет происходить с мозгом ребенка в перспективе после такого воздействия.

Современные цифровые технологии позво-

ляют создавать модель развития мозга человеческого эмбриона. И после того, как исследования проведены на моделях, производить такие же эксперименты на живых людях уже становится почти безопасно.

В «Клото» я занимаюсь пресс релизами, PR-кампаниями, продвижением и рекламой. Любой бизнес - это продажи. Мы продаем людям информацию о том, «перерожденец» их будущий ребенок или нет. Спрос есть, а увеличить его - наша с Сережей Козловским задача в корпорации.

Ещё предстоит выяснить, что приводит к зарождению «души», открыть механизмы, которые при этом работают. Но почему-то я не сомневаюсь, что уже лет через двадцать на эту тему будут защищать кандидатские и докторские диссертации.

Человеку было необходимо выжить - и для этого он добыл огонь.

Человек хотел поменьше ходить и изобрел колесо.

Человек мечтал летать и однажды полетел.

Возможно, скоро цифровые технологии помогут человеку победить саму смерть.

Ведь главное - хотеть добросовестно.

И тогда получится обязательно.

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.