ISSN 2686-9373

ВЕСТНИК СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ
(ВАК – 05.13.00)
1. 2019 (ОКТЯБРЬ)

ВЕСТНИК
СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ
НАУЧНО-ПРАКТИЧЕСКИЙ ЖУРНАЛ

www.c3da.org

№1
ОКТЯБРЬ 2019

ISSN 2686-9373

Издатель: *Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН*
Адрес редакции и издателя: 125315, Москва, Усиевича, 20, каб. 207
Тел/факс: 499-155-43-26
E-mail: info@c3da.org

Подписано в печать 30.10.2019 г.
Тираж 500 экз.

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

РЕДАКЦИОННЫЙ СОВЕТ

СОДЕРЖАНИЕ

Редакционное примечание.....4

1. ФУНДАМЕНТАЛЬНЫЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

С.В. Запечников – Криптографическая защита процессов обработки информации в недоверенной среде: достижения, проблемы, перспективы
S. Zapechnikov – Cryptographic Protection of Information Processing in an Untrusted Environment: Achievements, Challenges and New Perspectives.....6

Д.И. Правиков, А.В. Петухов – Кибербезопасность как новое фундаментальное направление в области информационной безопасности
D. Pravikov, A. Petukhov – Cybersecurity as a new fundamental research area in the field of information se curity.....19

П.Е. Мурзин – Основные подходы к разработке протокола консенсуса в распределенных реестрах
P. Murzin – The main approaches to developing a consensus protocol in distributed registries.....26

2. ЭКОНОМИЧЕСКИЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Ю.А. Шушкевич – Возможности использования криптовалют в интересах стабилизации и развития финансовых рынков и национальных денежных систем
Yu.A. Shushkevich – Opportunities of cryptocurrencies in favour of stabilizing and developing financial markets and national monetary systems.....37

3. ОБЩЕСТВЕННО-ПОЛИТИЧЕСКИЕ АСПЕКТЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

А.В. Домашев, А.Ю. Щербаков – Международный консенсус как развитие парадигмы консенсуса
A. Domashev, A. Shcherbakov – International consensus as developing of the consensus paradigm.....48

А.Ю. Щербаков – Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН как инструмент решения научно-методических проблем в сфере цифровой трансформации.....54

4. ФИЛОСОФСКИЕ ПРОБЛЕМЫ ЦИФРОВЫХ ТЕХНОЛОГИЙ

А.А. Рязанова, А.Ю.Щербаков – Искусственный интеллект как феномен имитации
A.Ryazanova, A.Shcherbakov – Artificial intelligence as a phenomenon of imitation.....56

О.О. Тихоненко – Семантика языка как источник откровения
O. Tihonenko – Semantics of language as a source of revelation.....62

5. ЛИТЕРАТУРА О ЦИФРОВЫХ ТЕХНОЛОГИЯХ

Егор Федоров – Цифра.....80

РЕДАКЦИОННОЕ ПРИМЕЧАНИЕ

Журнал «Вестник современных цифровых технологий», его редакционный совет и Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН поздравляет Сергея Владимировича Запечникова с 45-летием и желает ему крепкого здоровья и новых творческих успехов!

Сергей Владимирович — выдающийся российский ученый, ведущий российский специалист по криптографическим протоколам, обеспечению устойчивости распределенных вычислений, обеспечению безопасности доступа к базам данных и системам распределенного реестра, приложениям интеллектуального анализа данных и машинного обучения в кибербезопасности. Автор 165 научных и учебно-методических трудов.

Доктор технических наук (2011), доцент (2005), профессор Института интеллектуальных кибернетических систем Национального исследовательского ядерного университета «МИФИ».

Выпускник Московского государственного инженерно-физического института (технического университета) по специальности «Прикладная математика».

Лауреат премии Национального форума информационной безопасности «Инфофорум» в номинации «Преподаватель года» (2009), победитель конкурсов научных исследований в области информационной безопасности «ИнфоТеКС-Академия» (2012, 2014, 2018) победитель конкурса грантов благотворительного фонда В. Потанина для преподавателей государственных вузов России (2003, 2006). Награжден нагрудным знаком «Лучший молодой преподаватель НИЯУ МИФИ» за высокие достижения в научно-исследовательской деятельности (2015), отмечен Благодарственным письмом генерального директора ГК «Росатом» за многолетний добросовестный труд, значительные личные успехи в научно-исследовательской деятельности и большой вклад в развитие атомной отрасли (2018).

Первый номер нашего журнала открывается разделом «Фундаментальные проблемы цифровых технологий». В нем представлены работы как корифеев криптографической отрасли, так и молодых ученых-аспирантов, только начинающих свой путь в науке.

В первую очередь хотелось бы отметить фундаментальную работу Сергея Владимировича Запечникова «Криптографическая защита процессов обработки информации в недоверенной среде: достижения, проблемы, перспективы». В статье проанализированы известные методы и модели криптографической защиты процессов обработки информации. Среди них следует выделить основные компоненты стойких криптографических протоколов: доказательства с нулевым разглашением, безопасные многосторонние вычисления и схемы гомоморфного шифрования. Наиболее общей задачей криптографической защиты вычислительных процессов является задача безопасных многосторонних вычислений. Следует отметить, что появление столь сложных криптографических протоколов стало возможным благодаря значительному развитию теоретической базы – доказательных методов и моделей криптографии. Представляется, что это направление современной криптографии имеет большой потенциал роста. В недалеком будущем рассмотренные в статье криптографические протоколы имеют все основания стать основным инструментом для создания защищенных персонализированных информационных сервисов, способных предоставлять пользователям информационные и вычислительные услуги в соответствии с индивидуальными потребностями без раскрытия их персональных данных.

Теоретически значимой и также фундаментальной работой в области кибербезопасности стала статья «Кибербезопасность как новое фундаментальное направление в области информационной безопасности», написанная Дмитрием Правиковым и Алексеем Петуховым. В статье рассмотрен новый подход к научному обоснованию понятия «кибербезопасность». На основании анализа структуры абстрактной социотехнической системы введены виды обрабатываемой информации, а также предложено формальное описание кибербезопасности в виде произведения предикатов.

Весьма интересной является обзорная статья Петра Мурзина, аспиранта ВИНИТИ РАН «Основные

подходы к разработке протокола консенсуса в распределенных реестрах».

Раздел «Экономические проблемы цифровых технологий» представлен статьей Юрия Шушкевича «Возможности использования криптовалют в интересах стабилизации и развития финансовых рынков и национальных денежных систем». Статья открывает весьма интересную и дискуссионную тему влияния криптовалют на финансовые рынки и национальные денежные системы и анализирует причины специфики политики в отношении криптовалют в различных государствах. Показаны механизмы, посредством которых обращение криптовалют может нанести ущерб или, наоборот, создать конкурентные преимущества национальным финансовым рынкам. Делается обоснованный вывод о наличии у Российской Федерации фундаментальных предпосылок для использования национальной криптовалюты в интересах укрепления международного экономического сотрудничества и обеспечения национальных интересов в условиях односторонних санкционных ограничений со стороны США и ряда других стран. Приводятся основные характеристики и принципы работы проектируемой национальной криптовалюты, дается средне– и долгосрочный прогноз ее влияния на развитие в России финансового рынка и формирование условий для стабилизации и укрепления рубля с перспективой его превращения в полноценное средство международных расчетов и одну из мировых резервных валют.

Раздел «Общественно-политические аспекты цифровых технологий» составили статьи Алексея Домашева и Андрея Щербакова «Международный консенсус как развитие парадигмы консенсуса» и заметка Андрея Щербакова «Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН как инструмент решения научно-методических проблем в сфере цифровой трансформации», прозвучавшая в качестве доклада на Ученом Совете ВИНИТИ РАН.

Раздел «Философские проблемы цифровых технологий» открывает интересная статья Алины Рязановой и Андрея Щербакова «Искусственный интеллект как имитация», посвященная использованию субъектно-объектной модели для потенциально возможного синтеза систем искусственного интеллекта и преодолению диалектического тупика в развитии данной проблемы, и продолжает основополагающая статья Олега Тихоненко «Семантика языка как источник откровения».

Журнал завершает рассказ Егора Федорова «Цифра», посвященный возможному будущему цифровых технологий.

Редакция надеется на интерес ученых цифровой отрасли к журналу и приглашает к сотрудничеству авторов.

Криптографическая защита процессов обработки информации в недоверенной среде: достижения, проблемы, перспективы

S. Zapechnikov

Cryptographic Protection of Information Processing in an Untrusted Environment: Achievements, Challenges and New Perspectives

Abstract. *The article deals with the problems of cryptographic protection of data processing. This is a set of novel techniques allowing to process private information without disclosing it to persons engaged in processing. We review important building blocks for cryptographic protection of data processing, such as zero-knowledge proofs, secure multi-party computations and homomorphic encryption. Often, big data processing includes data mining and machine learning algorithms, so privacy-preserved machine learning is very important task. The concept of differential privacy is analyzed which is the basis for privacy-preserving machine learning and some other cryptographic schemes. It is noted that one of the main applications of such security tools is the creation of personalized information services, which opens up new opportunities for business and reduces the risks of unauthorized access to personal data.*

Keywords: *cryptographic protocols, zero-knowledge proofs, secure multi-party computations, homomorphic encryption, privacy-reserving machine learning, personalized information services.*

С.В. Запечников [1,2]

[1]доктор технических наук, доцент, Национальный исследовательский ядерный университет «МИФИ», профессор отделения интеллектуальных кибернетических систем офиса образовательных программ, SVZapechnikov@mephi.ru, раб. тел. +7(495)788-56-99;

[2]Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН, главный научный сотрудник

Аннотация. *В статье рассматриваются проблемы создания криптографических средств защиты процессов обработки данных, позволяющих обрабатывать конфиденциальную информацию без раскрытия её для лиц, осуществляющих обработку. Проводится обзор важнейших компонентов таких криптосхем: доказательств с нулевым разглашением, протоколов безопасных многосторонних вычислений, схем гомоморфного шифрования. Обработка больших массивов данных часто включает в себя алгоритмы интеллектуального анализа данных и машинного обучения, поэтому задача конфиденциального машинного обучения должна рассматриваться как одна из важнейших. В статье проводится анализ концепции дифференциальной приватности, которая служит основой протоколов конфиденциального машинного обучения и ряда других криптосхем. Отмечается, что одно из основных применений таких средств защиты – создание персонализированных информационных сервисов, которые открывают новые возможности для бизнеса и снижает риски несанкционированного доступа к персональным данным.*

Ключевые слова: *криптографические протоколы, доказательства с нулевым разглашением, безопасные многосторонние вычисления, гомоморфное шифрование, конфиденциальное машинное обучение, персонализированные информационные сервисы.*

ВВЕДЕНИЕ

Со времени появления первых средств вычислительной техники в течение нескольких десятилетий криптографические методы защиты информации использовались для обеспечения безопасности информации либо при её хранении, либо при передаче по каналам связи. Основными целями криптографической защиты при этом являлись конфиденциальность и аутентичность (целостность и подлинность) информации. Защищаемая информация предполагалась статичной. Так, получатель сообщения должен расшифровать и проверить аутентичность в точности такого же сообщения, какое было выслано ему отправителем. Аналогичные предположения делались и при хранении информации: после снятия криптографической защиты должен быть восстановлен в точности такой же информационный массив, какой был подвергнут преобразованию.

Разделение криптографии на симметричную и асимметричную ветви породило обширный инструментарий для решения этих задач. Так, основными средствами обеспечения конфиденциальности стали симметричные схемы шифрования с использованием блочных и поточных шифров, а также схемы открытого шифрования, а основными средствами обеспече-

ния аутентичности – коды аутентификации сообщений и схемы цифровой подписи. Такой подход вполне соответствовал архитектурам обработки данных, преобладавшим на ранних этапах развития вычислительной техники, когда обработкой данных занимался преимущественно сам владелец данных либо лица, которым он доверяет.

Однако в начале 2000-х гг. начинается активное развитие децентрализованных и распределенных технологий хранения и обработки данных: облачных хранилищ и центров обработки данных, файлообменных сетей, беспроводных сетей с динамической топологией, а в последние годы – систем распределенного реестра (блокчейн-технологий) и пр. Вокруг каждой из перечисленных технологий, как правило, вырастает целая «экосистема» связанных с ними методов и средств обработки информации, а также основанных на них информационных сервисов. Развитие таких технологий позволило обеспечить доступ большому числу клиентов с относительно маломощными устройствами (смартфонами, планшетами, портативными и бортовыми компьютерами, микропроцессорами) к большим пулам компьютерных ресурсов, способных как выполнять высокопроизводительные вычисления, так и хранить огромные объёмы данных. При значительной степени коллективизации средств обработки и хранения информации информационно-телекоммуникационная среда открывает для пользователей широкие возможности доступа к многочисленным информационным сервисам: электронной почте, мессенджерам, картографическим и геоинформационным системам, поисковым машинам, видеохостингам и многим другим услугам. Одновременно такая среда пользуется всё меньшим доверием пользователей, поскольку открывает широкие возможности для легитимного и негласного сбора персональных данных, применения различных средств глубокого анализа данных, характеризующих поведение пользователей, их предпочтения и другие аспекты деятельности.

Эти обстоятельства делают актуальными создание таких методов и средств криптографической защиты информации, которые позволяли бы защищать информационные потоки в динамике, т.е. собственно процессы обработки информации, преобразования данных и метаданных, выработки новых данных и знаний. Таким образом, происходит кардинальный сдвиг интересов в сфере обеспечения безопасности информации – возникает запрос на защиту не только собственно данных, но и вычислительных процессов, процессов алгоритмических преобразований данных.

Ещё несколько лет назад криптографическая защита процессов обработки информации была попросту невозможна из-за колоссальной вычислительной сложности соответствующих алгоритмов. Однако в конце 2010-х гг. ситуация в этой сфере начала коренным обарзом меняться, и сейчас мы стоим на пороге нового этапа развития криптографических методов и средств защиты информации. Настоящая статья посвящена анализу достижений, актуального состояния дел и перспектив криптографической защиты процессов обработки информации.

С этой целью в п. 1 статьи рассматриваются основные предпосылки, теоретические и прикладные аспекты криптографической защиты процессов обработки данных, пп. 2 – 4 посвящены отдельным, наиболее существенным инструментам защиты вычислительных процессов: доказательств с нулевым разглашением, безопасным многосторонним вычислениям, гомоморфному шифрованию. В п. 5 рассматриваются два класса задач, связанных с обеспечением безопасности персональных данных при реализации вычислительных процессов: совместная обработка данных небольшим количеством сторон и так называемая федеративная обработка данных. В п. 6 выделяются проблемы конфиденциального анализа данных и машинного обучения, включая центральную для этой области идею дифференциальной приватности. В заключительной части статьи содержатся выводы и прогнозы автора относительно перспектив развития рассматриваемых в статье технологий.

ОСНОВНЫЕ ПРЕДПОСЫЛКИ, ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ АСПЕКТЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПРОЦЕССОВ ОБРАБОТКИ ДАННЫХ

Научные исследования в области криптографической защиты процессов обработки данных берут свое начало с 1980-х гг. [1, 2], однако до конца 2010-х гг. практическое их внедрение было невозможно по двум причинам: ввиду высокой, «астрономической» сложности почти всех известных алгоритмов, а также по причине недостаточной производительности и объёма памяти абсолютного большинства вычислительных средств, используемых массовым потребителем.

Практическую потребность в криптографической защите процессов обработки данных можно оценить как весьма высокую. Любой активный пользователь информационных сервисов оставляет в открытой сети много персональных данных, которые необходимы либо для исполнения его запросов, либо обусловлены законодательными требованиями: фамилию, имя, отчество, паспортные данные, сведения о своем местоположении, о приобретаемых товарах, реквизиты своих банковских карт и пр. Таким образом, сам факт наличия персональных данных в сети создает потенциальную возможность для их сбора, анализа, использования как в позитивных, так и в негативных целях. Несмотря на то, что в большинстве развитых стран мира существуют законодательные требования по защите персональных данных, они не всегда способны предотвратить раскрытие персональных данных и злоупотребления с ними. Более того, пользователи чаще всего недостаточно внимательно знакомятся с политиками управления персональными данными, с которыми они соглашаются при пользовании информационными сервисами (или вообще не читают такие документы, автоматически ставя «галочки» в отведенном для этого месте). В результате складывается ситуация, когда пользователь по истечении некоторого времени не помнит, где и какие персональные данные он оставил, и они бесконтрольно хранятся у операторов информационных сервисов, а возможно, и обращаются в сети. В то же время персональные данные становятся все более ценным ресурсом. Радикальным решением этой проблемы могло бы стать широкое использование криптографических методов и средств защиты не только самих данных, но и процессов их обработки. При этом информация, предоставляемая владельцем, сможет находиться в зашифрованном виде в процессе всего цикла обработки, оставаясь нераскрытой для иных лиц, кроме её владельца. Лица, которым в нынешних условиях эта информация предоставляется для исполнения запросов пользователей, смогут получать лишь результаты её обработки в точности в том объёме, который необходим для выполнения ими своих функций. Таким образом, появляется возможность создания персонализированных информационных сервисов без доступа к персональным данным кого бы то ни было, кроме их владельца. Со временем использование такой схемы обработки данных может быть закреплено законодательно.

В настоящее время достигнут значительный прогресс в росте производительности криптографических схем, реализующих криптографическую защиту отдельных элементов процесса обработки данных. По оценкам экспертов, производительность реализованных решений за последние 30 лет выросла на несколько порядков величины [3, 4]. Рост производительности достигается как путем снижения вычислительной сложности вновь разрабатываемых алгоритмов, так и за счет роста производительности вычислительной техники, на которой они реализуются. В условиях роста производительности алгоритмов решающими факторами, определяющими практичность алгоритмов и протоколов, становятся пропускная способность каналов связи, возможности предварительного выполнения участниками части вычислений в автономном режиме, асимметрия в требованиях к вычислительным ресурсам.

Второй проблемой, препятствующей широкому распространению рассматриваемых средств, является высокая сложность их реализации, а в ряде случаев и достаточно высокие требования к квалификации самих пользовате-

лей. Успешная реализация требует тщательной оптимизации программного кода, грамотного выбора языков программирования, библиотек функций, аппаратной базы и учета множества других факторов. Очевидные требования к пользователям таких защищенных персонализированных информационных сервисов включают в себя требования к общей культуре информационной безопасности, включая понимание принципов работы средств защиты информации, умение безопасно обращаться с криптографическими ключами, распознавать попытки мошенничества с персональными данными, противостоять «социальной инженерии».

Анализ литературы показывает, что исследования проблем криптографической защиты процессов обработки информации идут сразу по многим направлениям. Условно можно выделить исследования, посвященные разработке отдельных криптографических схем и протоколов, решающих типичные задачи, связанные с неразглашением секретов, децентрализованными вычислениями, обработкой данных «под шифром», а также исследования, посвященные решению типовых задач, возникающих в сфере обработки и анализа данных. В следующих трех разделах статьи рассмотрим криптосхемы, которые, по мнению автора, являются важнейшими «строительными блоками» систем криптографической защиты процессов обработки данных.

ДОКАЗАТЕЛЬСТВА С НУЛЕВЫМ РАЗГЛАШЕНИЕМ

Доказательства с нулевым разглашением являются представителями обширного семейства криптографических протоколов, называемых вероятностными доказательствами, в которых одна из сторон с некоторой вероятностью убеждает другую сторону в справедливости некоторого утверждения. В последнее время к этой идее проявился большой практический интерес, и она была воплощена во многих средствах и системах защиты информации. В связи с этим далее остановимся на тех вероятностных доказательствах, которые имеют наибольшее практическое значение. Идея вероятностных доказательств и доказательств с нулевым разглашением впервые предложена в работе [5].

Интерактивная система доказательства (interactive proof system) – это протокол, включающий двух участников: *доказывающего (prover – P)* и *проверяющего (verifier – V).* Предварительно формулируется некоторое утверждение *S*, например, утверждение о том, что некоторый объект *w* обладает свойством *L*, или, в другой интерпретации, слово w принадлежит языку $L: w \in L$. В ходе выполнения протокола *P* и *V* обмениваются сообщениями. Каждый из них может генерировать случайные числа и использовать их в своих вычислениях. В конце протокола *V* должен вынести свое окончательное решение о том, является ли *S* истинным или ложным.

Цель *P* всегда заключается в том, чтобы убедить *V* в том, что *S* истинно, независимо от того, истинно ли оно на самом деле или нет. Таким образом, *P* может мошенничать в протоколе, так как *S* может быть ложно, т.е. он может быть активным противником. *V* должен проверять аргументы участника *P*. Цель участника *V* заключается в том, чтобы вынести решение, является ли *S* истинным или же ложным.

Как видим, интересы участников протокола *P* и *V* не совпадают. Однако участник *V* имеет полиномиально ограниченные вычислительные возможности, а именно время его работы ограничено некоторым полиномом от длины доказываемого утверждения: $t \le p(|w|)$. Это предположение является стандартным для моделирования вычислительных возможностей современных средств вычислительной техники. В силу этого он самостоятельно, без помощи *P*, не способен распознать истинность утверждения *S*.

Вычислительные возможности *P* теоретически никак не ограничиваются, что на практике соответствует ситуации, когда *P* владеет какой-то априорной информацией, которую трудно получить в ходе выполнения протокола, например, для этого пришлось бы решать вычислительно сложную задачу (хотя он может и обманывать, утверждая, что такая информация у него имеется).

Программа действий участника *V* должна

быть устроена таким образом, чтобы:

1) если *S* истинно, *P* смог бы убедить *V* признать это;

2) если *S* ложно, *P* не смог бы убедить *V* в противном, какие бы аргументы он ни выдвигал, т.е. вне зависимости от получаемых от *P* сообщений.

V может ошибаться, но ставится условие, чтобы вероятность принятия им неправильного решения была бы пренебрежимо мала.

Протокол между участниками *P* и *V* называется *интерактивным доказательством* для языка *L*, если *V* полиномиально ограничен, и выполнены следующие два условия:

1) для $\forall x \in L\ P\{(P, V)_{(x)} = 1\} = 1$ (т.е. вероятность принятия проверяющим доказательства истинного утверждения равна единице);

2) для $\forall x \in L$ и для $\forall P' \neq P$ (для любого другого участника, который действует не так, как честный участник) вероятность принятия проверяющим доказательства ложного утверждения исчезающе мала, т.е. $P\{(P', V)_{(x)} = 1\} = 1/2^{n^c}$, где *C=Const.*, *n* – число раундов протокола.

Условие 1 называется *полнотой* (completeness), условие 2 – *корректностью* (soundness) доказательства.

Пусть задана интерактивная система доказательства $\langle P, V, S \rangle$. В определении интерактивной системы доказательства ранее не предполагалось, что *V* может быть противником – предполагалась только возможность существования нечестного участника *P*. Но *V* тоже может оказаться противником, который хочет выведать у *P* какую-либо новую полезную информацию об утверждении *S*. В этом случае *P* может не хотеть, чтобы это случилось в результате выполнения протокола интерактивной системы доказательства $\langle P, V, S \rangle$. Таким образом приходим к идее доказательства с *нулевым разглашением* (zero-knowledge proof). Нулевое разглашение подразумевает, что в результате работы протокола интерактивной системы доказательства *V* не увеличит свои знания об утверждении *S*, или, другими словами, не сможет извлечь никакой информации о том, почему *S* истинно.

Практическую ценность для защиты процессов обработки информации имеет обобщение доказательств с нулевым разглашением для произвольных функций. В этих протоколах также два участника: *P – доказывающий* (prover), *V – проверяющий* (verifier).

Цель протокола – *P* должен доказать V, что он вычислил некоторую функцию $y = F(x)$, процесс вычисления был выполнен корректно, и пара значений (x, y) в самом деле связана функциональной зависимостью *F*, при этом *V* не должен повторять процесс вычисления функции *F*.

Можно указать по крайней мере три ситуации, при которых применение таких протоколов актуально:

1) *x* – очень большой массив данных (big data), который невозможно или нецелесообразно копировать проверяющему;

2) функция *F* – очень сложно вычислимая, и проверяющий не может или не хочет повторять эти вычисления;

3) *x* – конфиденциальная информация, и доказывающий не может разглашать её проверяющему.

Одним из наиболее эффективных способов реализации доказательств с нулевым разглашением для произвольных функций являются *компактные неинтерактивные доказательства знания с нулевым разглашением* – zk-SNARKs (zero-knowledge Succinct Non-interactive Arguments of Knowledge) [6, 7]. Они обладают следующими свойствами:

- *компактность:* размер доказательства растёт медленнее, чем размер вычисленных доказывающим данных (проверить доказательство гораздо проще, чем выполнить вычисление);

- *неинтерактивность:* протокол между *P* и *V* требует пересылки всего 1 сообщения, не считая предварительного этапа;

- *доказательство знания: P* всегда докажет *V* корректное утверждение, обман доказывающим проверяющего возможен лишь с пренебрежимо малой вероятностью;

- *нулевое разглашение:* в процессе выполнения доказательства проверяющий не увеличит свои знания о тех данных, которые являются секретом P и которые участвовали в вычислении функции *F*.

Конструирование и применение zk-SNARKs

включает в себя следующие этапы:

1. Описание функции F(·) на некотором языке программирования.

2. Компиляция исходного кода на языке программирования в арифметическую схему.

3. Задание канонического представления арифметической схемы, описывающего вычисление функции $y = F(x)$, с учетом ограничений, в специальном виде (так называемой R1CS-форме).

4. Переход к квадратичному полиномиальному представлению (QAP-форме) арифметической схемы, позволяющей свести доказательство к выборочной проверке точек полинома.

5. Собственно конструирование криптографического протокола доказательства с нулевым разглашением.

К наиболее очевидным практическим применениям протоколов zk-SNARKs относятся:

1. Обеспечение безопасности блокчейн-технологий, а именно:

- разграничение доступа и обеспечение конфиденциальности информации, хранимой в системах распределенного реестра;

- обеспечение конфиденциальности исполнения смарт-контрактов.

2. Реализация проверяемых вычислений (verifiable computations) в недоверенных средах, например, в облаках или на недоверенных аппаратных компонентах.

Привести здесь конкретные примеры протоколов не представляется возможным из-за ограниченного объема статьи.

Вместе с тем, реализация zk-SNARKs пока ещё сталкивается с множеством проблем. На текущий момент известно множество видов доказательств с нулевым разглашением, среди которых нет явного лидера: помимо zk-SNARKs, также известны zk-STARKs – zero-knowledge Scalable Transparent Arguments of Knowledge, Bulletproofs, Range proofs и др. – неоднозначным остается вопрос об эффективности их применения в разных прикладных задачах. Другой открытый вопрос – как повысить производительность протоколов и уменьшить размер доказательств? (Вычислительная сложность протоколов, оцениваемая как $O(n)$, где n – длина а ещё лучше $O(\log\log n)$ или ниже). Также нерешенным остается вопрос обеспечения стойкости протоколов к атакам нарушителя, обладающего квантовым компьютером.

Следует отметить, что в настоящее время прилагатся усилия по международной стандартизации протоколов доказательства с нулевым разглашением [8].

БЕЗОПАСНЫЕ МНОГОСТОРОННИЕ ВЫЧИСЛЕНИЯ

Задача безопасных многосторонних вычислений (secure multi-party computations) – одна из фундаментальных задач теории и практики конструирования криптографических протоколов. Постановка задачи и фундаментальные основы её решения известны из работ [1, 2], относящихся к середине 1980-х гг. Рассматривается множество из n участников криптосистемы. Каждый из участников обладает секретом x_i, $i = 1, n$. Цель выполнения протокола заключается в том, чтобы участники протокола своими совместными действиями без привлечения доверенной третьей стороны смогли вычислить некоторую функцию *F* от множества их секретов, не разгласив свои секрету друг другу либо кому-то из третьих лиц. Таким образом, протокол должен обладать следующими основными свойствами [9]:

- *корректностью:* каждый из участников должен получить значение $y=F(x_1,...,x_n)$;

- *конфиденциальностью:* никакие иные сведения, кроме значения *y*, не будут разглашены в процессе выполнения протокола.

В качестве желательного также зачастую выдвигается следующий набор дополнительных свойств:

- *независимость входных данных:* никто из участников не может выбрать входные данные таким образом, чтобы они полностью совпадали с входными данными другого участника;

- *честность получения результата:* либо все участники протокола должны получить результат, либо никто из участников не должен его получить.

Частный случай задачи безопасных многосторонних вычислений – безопасные дву-

сторонние вычисления – та же самая задача при $n=2$.

При конструировании протоколов безопасных многосторонних вычислений, таким образом, исходят из предположения о том, что для каждого из участников все остальные участники являются недоверенными, тем не менее, все они заинтересованы в совместном решении общей задачи. Цель конструирования протокола заключается в том, чтобы множество из n участников своими совместными действиями гарантировало бы такую же степень доверия внутри сообщества, как при использовании услуг доверенной третьей стороны: нотариуса, арбитра, третейского судьи и т.п.

При этом могут рассматриваться различные модели нарушителя: в частности, стандартными являются предположения о «пороговом» противнике, который может контролировать не более установленного порогового числа участников протокола, в то время как остальные участники являются честными, также противник может быть пассивным или активным, статическим или адаптивным.

Примером практического применения безопасных многосторонних вычислений может служить ситуация, когда необходимо оценить эффективность какого-либо определенного способа лечения пациентов, находящихся в разных клиниках. Скорее всего, при решении задачи необходимо будет использовать данные, относящиеся к медицинской тайне. Применение протокола безопасных многосторонних вычислений позволит всем клиникам совместно определить эффективность лечения, выраженную, например, в баллах, не передавая между клиниками сведения о пациентах и не раскрывая их персональные данные. К частным случаям безопасных многосторонних вычислений относятся также протоколы электронных аукционов, электронных выборов и многие другие протоколы.

В зависимости от предполагаемой модели нарушителя применяется несколько подходов к построению протоколов безопасных многосторонних вычислений. Для модели пассивного нарушителя классическими протоколами безопасных многосторонних вычислений считаются GC-схемы (garbled circuits) [1].

Это двусторонний протокол для булевых функций, но он служит «строительным блоком» для множества других протоколов, в том числе и многосторонних. Ещё одним широко известным протоколом является протокол Гольдрайха – Микали – Вигдерсона [2], который решает эту задачу для многостороннего случая и применим как к булевым функциям, так и к арифметическим схемам, выполняется за количество раундов, пропорциональное глубине схемы. Альтернативным подходом можно считать протокол Бен-Ора, Гольдвассера и Вигдерсона [10]. Существует множество других подходов, отличающихся ограничениями, налагаемыми на вычисляемую функцию, числом раундов, вычислительной сложностью, различными нюансами модели нарушителя.

Для модели активного нарушителя также известен целый ряд протоколов, основанных как на GC-схемах, так и на других подходах. Примером может служить протокол, предложенный в статье [11].

ГОМОМОРФНОЕ ШИФРОВАНИЕ

Гомоморфное шифрование – ещё одна важнейшая составляющая криптографической защиты вычислительных процессов. В основе концепции гомоморфного шифрования лежит модель аутсорсинговых вычислений, когда одна из сторон протокола обладает данными и желает получить результат вычисления некоторой функции от этих данных. Вторая сторона получает и хранит эти данные в зашифрованном виде, выполняет вычисления над зашифрованными данными и передает зашифрованные результаты владельцу данных, но сама при этом не приобретает никаких знаний ни об исходных данных, ни о промежуточных результатах вычислений, ни об окончательном результате вычислений. Владелец исходных данных, получив зашифрованный результат вычислений, может расшифровать его и получить окончательный ответ. Схемы гомоморфного шифрования позволяют в точности реализовать такую схему вычислений.

Выделяют два типа схем гомоморфного шифрования: частично гомоморфное и полно-

стью гомоморфное шифрование. Частично гомоморфные схемы позволяют реализовать описанную выше схему аутсорсинговых вычислений только в отношении какой-либо одной арифметической операции (обычно либо сложения, либо умножения). Однако практическое применение частично гомоморфных схем ограничено лишь теми задачами, которые могут быть сведены к вычислению функции, которая может быть выражена в терминах поддерживаемой операции.

Полностью гомоморфное шифрование обеспечивает искомые свойства для любой функции, представимой в виде арифметической схемы. Формально схема полностью гомоморфного шифрования определяется как совокупность четырех алгоритмов ***(Gen, Enc, Eval, Dec)*** [12]. Алгоритмы ***Gen, Enc, Dec*** соответствуют стандартной функциональности схем шифрования – это генерация ключа, зашифрование и расшифрование, а алгоритм ***Eval*** принимает на входе вектор шифртекстов и функцию ***f***, а выдает зашифрованный результат применения этой функции к вектору шифртекстов. При этом обеспечивается следующее свойство корректности:

$Dec_{sk}(Eval(f, Enk_{pk}(x_1),..., Enk_{pk}(x_n))) = f(x_1,...,x_n)$, где $(pk, sk) \leftarrow Gen(1^k)$, k – параметр безопасности (длина секретного ключа схемы).

Практическая значимость полностью гомоморфных схем шифрования определяется тем, что они позволяют реализовать модель вычислений «вслепую», т.е. сторона вычислительного процесса, которой доверена обработка данных, сможет выполнять любые вычислительные операции, никогда не видя обрабатываемые данные.

Многие известные схемы открытого шифрования обладают частично гомоморфными свойствами. Так, например, повсеместно применяемая криптосистема RSA гомоморфна по умножению, а схема шифрования Пайе (Paillier) [13] гомоморфна по сложению. Первая полностью гомоморфная схема шифрования была предложена Джентри в 2009 г. [14]. Она основана на математическом аппарате целочисленных решёток. В последующие годы было предложено ещё несколько полностью гомоморфных схем, широко известных сегодня, а также предпринимались многочисленные попытки их эффективной реализации [15 – 17]. Тем не менее, основной проблемой гомоморфного шифрования по-прежнему остается очень низкая производительность полностью гомоморфных схем в сравнении с протоколами безопасных многосторонних вычислений.

В настоящее время предпринимаются шаги по международной стандартизации схем гомоморфного шифрования [18].

Рассмотренные криптосхемы являются универсальными, в них не делается предположений о конкретном виде вычисляемых функций, за исключением предположений о том, в каком виде они представлены: в виде булевых функций или арифметических схем. Вместе с тем многочисленные частные практические задачи, в которых вид функции фиксирован и известен заранее, зачастую могут быть решены гораздо проще и эффективнее, без использования общих схем (хотя и подходы, основанные на общих схемах, в целом ряде случаев работают хорошо). Далее рассмотрим примеры решения наиболее существенных задач.

ДВА ТИПА ЗАДАЧ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ПРОЦЕССОВ ОБРАБОТКИ ИНФОРМАЦИИ

Среди задач, для которых актуальна криптографическая защита процессов обработки информации, выделяется пласт задач с относительно небольшим числом равноправных участников, обладающих примерно одинаковой или сравнимой вычислительной мощностью. При этом участники взаимодействия постоянно соединены каналами связи и доступны друг для друга.

Одна из таких задач – конфиденциальное вычисление пересечения множеств (PSI – private set intersection). У каждого из не доверяющих друг другу участников протокола есть некоторое множество объектов – требуется определить подмножество объектов, присутствующее во всех множествах, без разглашения каких-либо дополнительных сведений о каждом из множеств (его мощности, конкретного

состава объектов и т.п.). В качестве практического примера можно указать ситуацию, когда необходимо определить круг пациентов, лечившихся в нескольких клиниках, без разглашения каких-либо дополнительных сведений о пациентах каждой из клиник. Лучшие из известных протоколов, решающих эту задачу, предложены в работах [19] (для модели пассивного нарушителя) и [20] (для модели активного нарушителя). По сведениям, приведенным авторами этих работ, при мощности множеств на входе порядка 2^{20} объектов первый из протоколов решает задачу за время порядка 10 с, второй – за время порядка 10^4 с. Сходная задача конфиденциального агрегирования (суммирования) элементов множеств по общим атрибутам (private intersection-sum) рассматривается в работе [21].

Другая задача – конфиденциальное извлечение информации из БД (PIR – private information retrieval). Суть задачи состоит в том, что клиент должен извлечь запись из БД, хранящейся у недоверенного провайдера, по известному ему индексу, не разглашая свой запрос провайдеру. Неразглашение запроса подразумевает, что провайдер не сможет узнать не только индекс извлекаемой из БД записи, но и не по множеству запросов одного и того же клиента не сможет получить каких-либо сведений о частоте его доступа к той или иной ячейке, связать разные запросы в одну цепочку. Одна из лучших криптосхем, предложенная в работе [22] решает эту задачу примерно за 12 с при объеме БД 2^{22} записей и длине одной записи 288 байтов.

Задачу безопасных двусторонних вычислений также можно рассматривать как пример задачи совместной обработки данных небольшим количеством сторон и искать её решение не как частный случай безопасных многосторонних вычислений, а при помощи специально сконструированных двусторонних протоколов. Лучшие из известных решений предложены в работах [23] (для модели пассивного нарушителя) и [24] (для активного нарушителя). Стандартным показателем эффективности такого протокола считается время зашифрования блока при помощи алгоритма AES: для первого протокола оно равно менее 1 мс, для второго – менее 10 мс, а при взаимодействии через глобальную сеть – порядка 113 мс.

Второй тип задач носит название «федеративная обработка данных». Он возникает в ситуации, когда большое число маломощных устройств взаимодействует с одним центром обработки данных (ЦОД) и, таким образом, взаимодействие происходит, как правило, в клиент-серверной модели при значительном дисбалансе вычислительной мощности.

Наиболее разработанной среди задач такого типа является задача о безопасной агрегации данных. Имеется ряд устройств, с которых собирается статистика. Они взаимодействуют с одним или несколькими ЦОДами. Требуется построить такой протокол, чтобы ЦОДы могли собрать обобщенную статистику о каких-либо величинах, переданных с пользовательских устройств, без разглашения данных, собранных с каждого из устройств в отдельности. Конфиденциальность данных должна обеспечиваться как в аспекте невозможности раскрытия данных ЦОДами, так и пользователями – данных друг друга. Наиболее существенные работы, посвященные решению этой задачи, - статьи [25] и [26]. Как отмечено в этих работах, основным фактором, ограничивающим практическое применение этого типа протоколов, являются высокие требования к пропускной способности каналов связи. В частном случае, когда данные собираются в единственный ЦОД, возможно получение гораздо более эффективных решений.

КОНФИДЕНЦИАЛЬНЫЙ АНАЛИЗ ДАННЫХ И МАШИННОЕ ОБУЧЕНИЕ

Ожидается, что в наибольшей степени криптографические методы защиты процессов обработки информации будут востребованы в сфере интеллектуального анализа данных и машинного обучения. Поэтому в настоящее время разработке методов защиты, которые могли бы использоваться при обучении и применении моделей, уделяется очень большое внимание.

Рассматривается ситуация, когда обучающая выборка может содержать данные ограниченного распространения, в частности, персональные данные. Владельцы этих данных могут

быть заинтересованы в том, чтобы их данные использовались для обучения какой-либо модели, но не хотят терять контроль над ними. Владелец модели также может не желать, чтобы параметры модели стали известны другим лицам, в том числе тем, кто предоставляет данные для обучения модели. Тем не менее, и владельцы данных, и владелец модели заинтересованы в обучении и последующем использовании модели. Реализовать этот сценарий при условии сохранения конфиденциальности данных каждой из сторон возможно при помощи протоколов конфиденциального машинного обучения.

Центральной идеей в разработке защитных механизмов для конфиденциального машинного обучения (privacy-preserving machine learning) является шумовой подход. Суть шумового подхода заключается в добавлении шума к входным (выходным) данным при интеллектуальном анализе данных либо при обучении каких-либо моделей. К шумовым подходам относятся, в частности, *дифференциальная приватность* (differential privacy) и *локальная дифференциальная приватность* (local differential privacy). Согласно [27], базовая модель дифференциальной приватности формулируется следующим образом. Пусть имеется база данных ***(БД) X***, в которую вводятся конфиденциальные данные $x_1, x_2,...,x_n$ о некотором множестве n пользователей. К этой БД могут делать запросы $q_1, q_2,...,q_k$ уполномоченные на то пользователи, среди которых могут быть и злоумышленники, пытающиеся анализировать данные, как легитимными, так и нелегитимными способами и использовать в своих интеерсах результаты анализа (аналитики, коммерческие компании и даже правительственные учреждения). Пусть на запросы $q_1, q_2,...,q_k$ ими получены от оператора БД ответы $a_1, a_2,...,a_k$.

К ответам предъявляется требование:

$a_1, a_2,...,a_k$ должны быть как можно ближе к значениям функции $q_1(X), q_2(X),...,q_k(X)$, которые мы считаем истинными ответами. В то же время точные ответы на большое количество запросов с богатой семантикой могут разгласить довольно много информации о $x_1, x_2,...,x_n$. Основная идея дифференциальной приватности состоит в том, чтобы давать такие ответы на запросы, чтобы из них невозможно было выделить факт присутствия или отсутствия в БД сведений о каком-либо одном конкретном лице. Таким образом, если есть две БД X и X', отличающиеся записью только об одном лице: $x_1,...,x_i,...,x_n$ и $x_1,...,x_i',...,x_n$, обработка запросов осуществляется вероятностным алгоритмом $A(\cdot)$, то распределения вероятностей ансамблей случайных величин $A(X)$ и $A(X')$ должны быть близки между собой. В связи с этим вводится следующее определение.

Алгоритм A называется (ε,δ) -дифференциально приватным, если для любых соседних наборов данных X и X' любых множеств S выполнено условие:

$$Pr[A(X) \in S] \le e^{\varepsilon} \cdot Pr[A(X') \in S]+\delta, \quad (1)$$

где ε - как правило, малая дробная величина: $0 < \varepsilon < 1$, а δ асимптотически стремится к нулю при увеличении длины наборов данных. При $\delta = 0$ получаем *чистую дифференциальную приватность* (pure differential privacy). Заметим, что при перемене местами X и X' в формуле (1) она остаётся справедливой, так как неравенство должно выполняться для любых двух соседних наборов данных. Определение подразумевает, что условие (1) должно выполняться вне зависимости от любых других дополнительных данных, известных нарушителю.

Теория дифференциальной приватности доказывает, что при точных ответах алгоритма $A(\cdot)$ на поставляемые ему запросы достижение дифференциальной приватности невозможно – требуется рандомизация. Для нечисловых признаков должно использоваться показательное распределение, а для числовых – распределения Лапласа либо Гаусса [27]. Распределение Лапласа позволяет обеспечить чистую дифференциальную приватность.

Указанные общетеоретические принципы далее должны быть применены к каждому из методов машинного обучения в отдельности, что может в каждом случае порождать сложные самостоятельные задачи. Наибольшие успехи сейчас достигнуты в отношении машинного обучения, основанного на оптимизации методом градиентного спуска, в частности, нейронных сетей [28], линейной регрессии [29], байесов-

ских методов [30]. Открытым пока остается вопрос обеспечения дифференциальной приватности для композиций алгоритмов машинного обучения, в частности, бэггинга и бустинга.

Как продемонстрировано в [31, 32], методы обеспечения конфиденциальности, основанные на дифференциальной приватности, могут быть применены к протоколам безопасных многосторонних вычислений.

Основной недостаток всех методов обеспечения конфиденциальности, основанных на шумовом подходе, – в том, что они заведомо снижают точность обрабатываемых данных. Дифференциальная приватность лучше подходит для обучения моделей, сохраняя конфиденциальность данных, в то время как локальная дифференциальная приватность хорошо себя проявляет при сборе данных, без ущерба их конфиденциальности, и анализе их распределений. Тем не менее, идея дифференциальной приватности остается пока лучшим из известных способов обеспечения конфиденциальности информации в задачах анализа данных и машинного обучения.

ЗАКЛЮЧЕНИЕ

В статье проанализированы известные методы и модели криптографической защиты процессов обработки информации. Среди них следует выделить основные компоненты стойких криптографических протоколов: доказательства с нулевым разглашением, безопасные многосторонние вычисления и схемы гомоморфного шифрования. Наиболее общей задачей криптографической защиты вычислительных процессов является задача безопасных многосторонних вычислений. Следует отметить, что появление столь сложных криптографических протоколов стало возможным благодаря значительному развитию теоретической базы – доказательных методов и моделей криптографии.

Криптографические методы защиты процессов обработки информации активно развиваются. За последние несколько лет в этой области достигнут очень существенный прогресс, что позволило на несколько порядков увеличить быстродействие протокола для всех сторон, снизить требования к пропускной способности каналов связи. Тем не менее, эти требования во многих случаях остаются ещё довольно высокими. Вместе с тем, во многих частных случаях протокол решения конкретной задачи может быть построен значительно более эффективно. Одна из важнейших задач, которая позволит реализовать бизнес-процессы с применением механизмов криптографической защиты процессов обработки информации, – конфиденциальное машинное обучение, которое позволит обучать алгоритмы без раскрытия своих конфиденциальных данных (или интеллектуальной собственности) участниками процесса обучения моделей.

Представляется, что это направление современной криптографии имеет большой потенциал роста. В недалеком будущем рассмотренные в статье криптографические протоколы имеют все основания стать основным инструментом для создания защищенных персонализированных информационных сервисов, способных предоставлять пользователям информационные и вычислительные услуги в соответствии с индивидуальными потребностями без раскрытия их персональных данных. А появление таких сервисов способно дать толчок реализации новых бизнес-процессов и развитию новых сфер деловой деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Yao, C. How to generate and exchange secrets / C. Yao // Proc. of 27th Annual Symposium on Foundations of Computer Science, 1986. Pp. 162–167.

2. Goldreich O. How to play any mental game / O. Goldreich, S. Micali, A. Wigderson // Proceeding STOC ‘87 Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing. Pp. 218–229.

3. Raykova M. Advanced cryptography on the way to practice / M. Raykova // Real World Cryptography

2019, Switzerland, Zurich, 2019. URL: https://rwc.iacr.org/2019/slides/RWC-Raykova.pdf (дата обращения: 29.09.2019)

4. Halevi, S. Advanced cryptography: Promise and challenges / S. Halevi // Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. P. 647. URL: https://shaih.github.io/pubs/Advanced-Cryptorgaphy.pdf (дата обращения: 29.09.2019)

5. Goldwasser, O. The knowledge complexity of interactive proof systems / O. Goldwasser, S. Micali, C. Rackoff // SIAM Journal on Computing, 18 (1), 1989. Pp. 186–208

6. Ben-Sasson, E. Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture / E Ben-Sasson, A. Chiesa, E. Tromer et al. // IACR eprint Archive. 2013. 37 pp. URL: https://eprint.iacr.org/2013/879.pdf (дата обращения: 04.10.2019)

7. Reitweissner, K. zkSNARKs in a nutshell / K. Reitweissner. URL: http://chriseth.github.io/notes/articles/zksnarks/zksnarks.pdf (дата обращения: 29.09.2019)

8. Zero knowledge proof standardization: An open industry / academic initiative. 2019. URL: https://zkproof.org/index.html (дата обращения: 04.10.2019)

9. Damgard, I. Secure distributed systems / I. Damgard, J. B. Nielsen, C. Orlandi // Electronic book, 2018. 332 pp. URL: https://blackboard.au.dk/webapps/blackboard/content/listContent.jsp?course_id=_116846_1&content_id=_1801036_1&mode=reset (дата обращения: 04.10.2019)

10. Ben-Or, M. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract) / M. Ben-Or, S. Goldwasser, A.Wigderson // Proc. of 20th Annual ACM Symposium on Theory of Computing. ACM Press. 1988. Pp. 1–10.

11. Mohassel, P. Fast and Secure Three-party Computation: The Garbled Circuit Approach / P. Mohassel, M. Rosulek, and Y. Zhang // Proc. of ACM CCS 15: 22nd Conference on Computer and Communications Security. Ed. by I. Ray, N. Li, and C. Kruegel. ACM Press. 2015. Pp. 591–602.

12. Armknecht, F. A guide to fully homomorphic encryption / F. Armknecht, C. Boyd, C. Carr et al. 2017. 35 pp. URL: https://pdfs.semanticscholar.org/ e6bc/da98a3385f1a287175a152fe6aa636a97c17.pdf (дата обращения: 04.10.2019)

13. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes" / P. Paillier // Advances in Cryptology – EUROCRYPT'99. Ed. by J. Stern. Vol. 1592. Lecture Notes in Computer Science. Springer, Heidelberg. 1999. Pp. 223–238.

14. Gentry C. A fully homomorphic encryption scheme. Ph.D. theses / C. Gentry // Stanford university. 2009. 209 pp. URL: https://crypto.stanford.edu/craig/craig-thesis.pdf (дата обращения: 29.09.2019)

15. Halevi, S. Bootstrapping for HElib / S. Halevi, V. Shoup // Cryptology ePrint Archive. 2014. 38 pp. URL: https://eprint.iacr.org/2014/873 (дата обращения: 04.10.2019)

16. Chillotti, I. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds / I. Chillotti, N. Gama, M. Georgieva et al. // Advances in Cryptology – ASIACRYPT 2016, Part I. ed. by J. H. Cheon and T. Takagi. Vol. 10031. Lecture Notes in Computer Science. Springer, Heidelberg. 2016. Pp. 3–33.

17. Chillotti, I. Faster packed homomorphic operations and efficient circuit bootstrapping for TFHE / I. Chillotti, N. Gama, M. Georgieva et al. // Advances in Cryptology – ASIACRYPT 2017, Part I. Ed. by T. Takagi and T. Peyrin. Vol. 10624. Lecture Notes in Computer Science. Springer, Heidelberg. 2017. Pp. 377–408.

18. Homomorphic Encryption Standardization: an Open Industry / Government / Academic Consortium to Advance Secure Computation. 2019. URL: https://homomorphicencryption.org (дата обращения: 04.10.2019)

19. Kolesnikov V. Efficient Batched Oblivious PRF with Applications to Private Set Intersection / V. Kolesnikov, R. Kumaresan, M. Rosulek, N. Trieu // Proc. Of 23rd ACM Conference on computer and communications security (CCS 2016). 19 pp. URL: https://eprint.iacr.org/2016/799.pdf (дата обращения: 29.09.2019)

20. Rindal P. Malicious-Secure Private Set Intersection via Dual Execution / P. Rindal, M. Rosulek // Proc. Of 24th ACM Conference on computer and communications security (CCS 2017). 27 pp. URL: https://eprint.iacr.org/2017/769.pdf (дата обращения: 29.09.2019)

21. Ion M. Private Intersection-Sum Protocol with Applications to Attributing Aggregate Ad Conversions / M. Ion, B. Kreuter, E. Nergiz // IACR eprint Archive. 2017. 14 pp. URL: https://eprint.iacr.org/2017/738.pdf (дата обращения: 29.09.2019)

22. Angel S. PIR with compressed queries and amortized query processing / S. Angel, Chen H,. Laine K., Setty S. // IACR eprint Archive. 2017. 18 pp. URL: https://eprint.iacr.org/2017/1142.pdf (дата обращения: 29.09.2019)

23. Gueron, S. Fast garbling of circuits under standard assumptions / S. Gueron, Y. Lindell, A. Nof, B. Pinkas // Proc. of ACM conference on computer and communications security (CCS), ACM Press, 2015. Pp. 567–578.

24. Wang, X. Global-scale secure multiparty computation / X. Wang, S. Ranellucci, J. Katz // IACR eprint Archive. 2017. 35 pp. URL: https://eprint.iacr.org/2017/189.pdf (дата обращения: 04.10.2019)

25. Bonawitz, K. Practical secure aggregation for federated learning on user-held data / K. Bonawitz, V. Ivanov, B. Kreuter et al. // 30th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain. 2016. 5 pp. URL: https://arxiv.org/pdf/1611.04482.pdf (дата обращения: 04.10.2019)

26. Corrigan-Gibbs, H. Prio: Private, robust, and scalable computation of aggregate statistics / H. Corrigan-Gibbs, D. Boneh // Proceedings of NSDI 2017 conference. 30 pp. URL: https://arxiv.org/pdf/1703.06255.pdf (дата обращения: 04.10.2019)

27. Dwork C. The algorithmic foundations for differential privacy / C. Dwork, A. Roth // Foundations and Trends in Theoretical Computer Science. Vol. 9, Nos. 3–4 (2014). Pp. 211–407. URL: https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf (дата обращения: 29.09.2019)

28. Abadi M. Deep learning with differential privacy / M. Abadi, A. Chu, I. Goodfellow etc. // Proc. Of 23rd ACM Conference on computer and communications security (CCS 2016). URL: https://arxiv.org/pdf/1607.00133.pdf (дата обращения: 29.09.2019)

29. Gascon, A. Privacy-Preserving Distributed Linear Regression on High-Dimensional Data / A. Gascón, P. Schoppmann, B. Balle, et al. // Proceedings on Privacy Enhancing Technologies ; 2017 (4):345–364, URL: https://eprint.iacr.org/2016/892.pdf (дата обращения: 04.10.2019)

30. Dimitrakakis C. Differential privacy for Bayesian inference through posterior sampling / C. Dimitrakakis, B. Nelson, Z. Zhang etc. // Journal of machine learning research, 18 (2017). Pp. 1 – 39. URL: http://www.jmlr.org/papers/volume18/15-257/15-257.pdf (дата обращения: 29.09.2019)

31. Cheu A. Distributed differential privacy via shuffling / A. Cheu, A. Smith, J. Ullman etc. // Advances in Cryptography – Eurocrypt'19, LNCS 11476. Springer, 2019. URL: https://www.springerprofessional.de/en/distributed-differential-privacy-via-shuffling/16720230 (дата обращения: 29.09.2019)

32. Bittau A. PROCHLO: Strong privacy for analytics in the crowd / A. Bittau, U. Erlingsson, P. Maniatis etc. // Proc. Of SOSP'17, Shanghai, China. Pp. 1-19. URL: https://static.googleusercontent.com/media/research.google.com/ru//pubs/archive/46411.pdf (дата обращения: 29.09.2019)

Кибербезопасность как новое фундаментальное направление в области информационной безопасности

D.Pravikov, A.Petukhov

Cybersecurity as a new fundamental research area in the field of information security

Abstract. *The article considers an approach to the scientific substantiation of the concept of cybersecurity. Based on the analysis of the structure of an ideal social system, types of processed information are introduced, it is shown that the existing traditional approaches to ensuring information security are associated with only one of its types. The proposed approach is correlated and built into the existing system of approaches to ensuring information security. The definition of cybersecurity is formulated. A formal description of cybersecurity as a product of predicates is proposed.*

Keywords: *cybersecurity, security of the protected object, integrated security system, social and technical system.*

Д.И.Правиков [1]
А.В.Петухов [2]
[1] *НОЦ НИАТ РГУ нефти и газа (НИУ) им. И.М.Губкина*
Email: dip@gubkin.pro
[2] *Kaspersky Industrial CyberSecurity Russia*
Email: Alexey.Petukhov@kaspersky.com

Аннотация. *В статье рассмотрен подход к научному обоснованию понятия кибербезопасность. На основании анализа структуры абстрактной социотехнической системы введены виды обрабатываемой информации, показано, что существующие традиционные подходы к обеспечению информационной безопасности связаны только с одним из ее видов. Предлагаемый подход соотнесен и встроен в существующую систему подходов к обеспечению информационной безопасности. Сформулировано определение кибербезопасности. Предложено формальное описание кибербезопасности в виде произведения предикатов.*

Ключевые слова: *кибербезопасность, безопасность защищаемого объекта, комплексная система безопасности, социотехническая система.*

ВВЕДЕНИЕ

Современная научная мысль в последние несколько лет в различных работах зафиксировала появление нового ноумена – киберпространства. Его определение, основные свойства, вызовы и угрозы описаны в целом ряде работ, в частности [1,2]. При этом, как было показано в [1], человечество подошло к «кромке хаоса»: в связи с активным развитием технологий появились системы, устройства, приборы и т.п., обобщенно называемые киберфизическими системами, которыми человек не может управлять непосредственно и вынужден передавать эту функцию автоматическим (не автоматизированным!) системам управления, результаты деятельности которых напрямую не подконтрольны операторам. Говоря другими словами, непосредственное управление оборудованием осуществляет, условно говоря, искусственный интеллект, решения которого по различным причинам могут быть небезопасными. С учетом внедрения подобных систем в различные сферы человеческой деятельности, в том числе объекты критической инфраструктуры, возникла необходимость обеспечения надежности и безопасности их функционирования.

Интересно отметить, что сходные идеи о небезопасности систем автоматического управления, очевидно опирающиеся на мнение ведущих экспертов, высказывают западные политики. Такое мнение, в частности, выразил генеральный секретарь НАТО Йенс Столтенберг во время выступления в Центре стратегических исследований при университете Виктории в Новой Зеландии. «Последний общий вызов, о котором я упомяну, это кибер[технологии]… технологии, такие как искусственный интеллект или квантовые вычисления или автономное оружие, в сочетании с кибер[технологиями], которые уже существуют некоторое время, теперь меняют природу конфликта так же принципиально, как промышленная революция изменила природу конфликта до Первой мировой войны.[1]»

В настоящее время аналитики задумываются о войнах будущего, отводя в них существенную роль киберпространству как пространству боевых действий[2]. Но возникает естественный вопрос, достаточно ли

[1] https://www.nato.int/cps/en/natohq/opinions_168242.htm?selectedLocale=en
[2] https://www.kommersant.ru/doc/4073388?from=main_3

существующих подходов к обеспечению информационной безопасности, для того, чтобы суметь адекватно противостоять грядущим вызовам?

Текущее состояние информационной безопасности как научного и технического направления деятельности характеризуется целыми рядом сформировавшихся противоречий.

1. Качественное и количественное расширение областей применения систем автоматизированного управления, в рамках которого уже невозможно поддерживать уровень соответствия требованиям по безопасности, ориентированными на системы высоких классов защищенности и квалифицированный персонал.

2. Появление массовых систем автоматического управления при обеспечении функциональной и промышленной безопасности, увеличение зависимости общества и государства от их безопасной и надежной работы.

3. Исчерпание потенциала теоретического обоснования информационной безопасности вычислительных систем, основанного на их замкнутости. Противоречие между традиционным субъектно-объектным подходом при обеспечении информационной безопасности и фактической разомкнутостью систем управления киберфизических систем.

4. Выявление отдельных неявных противоречий в нормативной базе, регламентирующей вопросы обеспечения информационной и комплексной безопасности.

Прокомментируем п. 3 более подробно. Несмотря на существующую нормативную базу, решения по защите информации, накопленный практический опыт, фактическую защищенность ряда объектов и т.п., можно утверждать, что в настоящее время используемые фундаментальные подходы исчерпали свой потенциал развития. Это связано с тем, что современные системы автоматического управления технологическими процессами и сложными устройствами удаленного обслуживаются сервисными службами, которые, как правило, подключаются к ним с правами, превышающими права доступа рядовых пользователей. С точки зрения обеспечения непрерывности технологического процесса отказаться от такого режима нецелесообразно, при этом его использование нежелательно с точки зрения безопасности.

Если рассматривать с точки зрения фундаментальных подходов к обеспечению информационной безопасности, то исторически их можно разделить на следующие этапы (это личные наблюдения автора с учетом анализа зарубежной нормативной базы, опыта ведущих предприятий типа Сбербанка и т.д.).

1. Концепция защищенного периметра (из того времени идут подходы с рубежами защиты, тот же defence-in-depth).

Данное направление плавно развивалось и на его основе была разработана:

2. Концепция парирования конечного множества угроз (задаваемых моделью угроз и моделью нарушителя).

Со временем стало понятно, что данная концепция недостаточно динамично реагирует на выявление нового вида угроз. Поэтому ближе к настоящему времени была сформулирована

3. Концепция управления рисками.

Несмотря на достаточную распространенность подход не идеальный. По личному мнению авторов, ограничения связаны с тем, что в настоящее время информатизация затрагивает практически все основные процессы современного предприятия. В результате возникают сложные цепочки типа: «пожарная безопасность влияет на состояние вычислительной среды, безопасность вычислительной среды влияет на промышленную и, как следствие, экологическую безопасность» и просчитать риски в отдельных ситуациях становится затруднительно. Более того, режим реального времени работы многих функциональных систем и систем их защиты практически отсекает человека от принятия тактических решений, а значит и управления рисками.

При этом следует заметить, что риск-ориентированный подход еще не исчерпал себя и как существенный элемент общей системы защиты информации может использоваться в дальнейшем. Вместе с тем, уже на текущем этапе необходимо понять, что может прийти ему на смену.

Рассуждая об информационной безопасности многие исследователи в качестве отправной точки выбирают информацию как объект исследования.

Продуктивность данного подхода привела к появлению многих теорий, среди которых можно выделить субъектно-объектный подход, на котором строится целое семейство моделей разграничения доступа, начиная от моделей Харрисона-Руззо-Ульмана и заканчивая ДП-моделями [3]. Вместе с тем, углубленный анализ позволяет прийти к выводу, что информация в данном случае рассматривается как статический объект, изменение которого возможно только в результате воздействия субъекта компьютерной системы. Говоря другими словами, информация представляет собой некий актив, у которого выделяются свойства хранения, модификации и использования (чтения). При этом модификация и использование происходит в результате воздействия активных сущностей, называемых субъектами.

Современные подходы, особенно подтвержденные практикой создания и использования автоматизированных систем управления технологическими процессами (АСУ ТП), показывают, что информация рассматривается как существенный элемент управления. При этом, с учетом режима реального масштаба времени, такую информацию принципиально нельзя рассматривать как объект или контейнер (см. [3]), имеющий в момент хранения свойство неизменности. Для иллюстрации данного тезиса представьте датчик, который десять раз в секунду генерирует данные о мгновенной скорости потока жидкости в трубопроводе. Как следствие, различными исследователями для указанных областей применения были сформулированы другие подходы к обеспечению информационной безопасности, изложенные, например, в [4]. Суть их заключается в том, что свойства информационной безопасности оцениваются через качество управления управляемой системы. Необходимо отметить, что изменение подходов к обеспечению информационной безопасности в первую очередь киберфизических систем отмечается и другими исследователями, достаточно упомянуть фундаментальную работу [5].

Возникающее противоречие между пониманием и моделью информации, а также подходами к обеспечению ее безопасности возможно разрешить если рассматривать не выделенную вычислительную систему, а в целом процесс организации некоей функциональной деятельности в рамках социотехнической системы. Развернутое определение социотехнической системы приведено, в частности, в [6]. Для настоящего исследования существенным будет то, что социотехнические системы состоят из технической и социальной подсистем.

Определим, что социотехническая система управляет технологическим процессом. В ходе данного управления используется информация в различных видах, а именно:

- собственная модель социотехнической системы;
- информационные активы бизнес-процесса;
- модель и параметры технологического процесса;
- параметры безопасности технологического процесса.

Указанные виды представлены на рис. 1.

Рисунок 1. Виды информации при управлении технологическим процессом

Представляется целесообразным разделить всю информацию, обрабатываемую в социотехнической системе на четыре категории:

1. Собственную модель социотехнической системы.
2. Информационные активы бизнес-процесса.

3. Модель и параметры технологического процесса.
4. Параметры безопасности технологического процесса.

Значение собственной модели социотехнической системы достаточно подробно описаны в [1]. Более того, в дальнейших рассуждениях она затрагиваться не будет, достаточно сказать, что по своим свойствам она близка к информационным активам. С учетом вышеизложенного информационные активы бизнес-процесса можно описать в виде пассивных сущностей субъектно-объектной модели, по отношению к которым применимы такие канонические свойства информационной безопасности, как конфиденциальность, целостность и доступность, а значит для них применимы уже наработанные подходы к обеспечению информационной безопасности.

В этом случае формируемый подход может быть вписан в существующую систему подходов в соответствии со схемой, представленной на рис. 2.

Рисунок 2. Схема концептуальных подходов к обеспечению информационной безопасности

Модель и параметры технологического процесса, а также параметры безопасности технологического процесса будем рассматривать в виде «динамической» информации, связанной с технологическим процессом. Безопасность именно этой информации в дальнейшем будем рассматривать как кибербезопасность.

Данный подход целесообразно сопоставить с подходом, описанном в документе, озаглавленном “Defence-in-depth: cybersecurity in the natural gas & oil industry”, который был подготовлен в 2018 г. Координационным советом подсектора по нефти и природному газу совместно с Советом по природному газу США. В качестве политической оценки отмечено, что «компании, занимающиеся добычей природного газа и нефти признают, что их активы являются объектами растущего числа все более изощренных кибератак, совершаемых различными злоумышленниками».

Обращает на себя внимание то, что в общем случае, применительно к информационной безопасности авторы документа отмечают защиту информационных технологий, интеллектуальной собственности и персональных данных. При этом в рамках указанного документа отдельно выделено рассмотрение АСУ ТП и защита технологического процесса в части мониторинга с использованием средств вычислительной техники, а также систем управления физическим доступом. Как следствие, *цели атак условно делятся на два направления: кража интеллектуальной собственности и компрометация АСУ ТП.*

Таким образом, предлагаемый подход, основанный на разделении категорий защищаемой информации и, соответственно, подходов к обеспечению ее безопасности, не противоречит складывающейся мировой практике. Более того, он позволяет разрешить неявное терминологическое противоречие, связанное с существованием двух терминов – «информационная безопасности» и «кибербезопасность». С учетом того, что понятие «информационная безопасность» закреплено в документах стратегического планирования Российской Федерации, в частности в Доктрине информационной безопасности, будем считать данный термин родовым. Кибербезопасность определим как производный термин, связанный с обеспечением информационной безопасности данных при обеспечении управления и безопасности технологического процесса.

Кибербезопасность – безопасность защищаемого объекта, системы которого функционируют в условиях деструктивных информационных воздействий.

Данное определение опирается на понятие «безопасность защищаемого объекта», определение которого приведено в действующем ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования:

Безопасность защищаемого объекта - состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей; имуществу физических или юридических лиц; государственному или муниципальному имуществу; техническому состоянию, инфраструктуре жизнеобеспечения; внешнему виду, интерьеру(ам), ландшафтной архитектуре; окружающей природной среде.

В формируемой системе определений существенным являются следующие аспекты:

1. В ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели приведено следующее определение: Кибербезопасность (киберзащита)- действия, необходимые для предотвращения неавторизованного использования, отказа в обслуживании, преобразования, рассекречивания, потери прибыли, или повреждения критических систем или информационных объектов. Принципиальным отличием предлагаемого автором совместно с рядом экспертов, определения является то, что оно определяет не действия, а состояние защищаемого объекта.

2. Определение безопасности защищаемого объекта уже существует и зафиксировано в соответствующем стандарте. Таким образом, предлагаемое определение кибербезопасности оказывается вписанным в существующую систему определений. Вместе с тем, в случае необходимости данное определение может быть скорректировано.

3. Не определяется характер воздействий (информационное или иное). Как показывает практика, воздействие на систему безопасности может носить настолько разнообразный характер, что классифицировать их в отдельных случаях не представляется возможным. Более того, в определение заложен заранее неопределенный характер воздействия.

4. Не выделяется какой-либо аспект безопасности защищаемого объекта. Указанное обстоятельство приводит к тому, что кибербезопасность является существенной частью общей системы обеспечения комплексной безопасности защищаемого объекта.

Комплексная система безопасности - система безопасности, одновременно выполняющая несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей.

Для более точного определения представим кибербезопасность как следствие обеспечения ряда видов безопасности, представленных на рис. 3.

Рисунок 3. Схема формирования кибербезопасности

Рассмотрим определение кибербезопасности с точки зрения дефляционных теорий истины. Не вдаваясь в подробности указанной философской теории отметим, что в рамках этой теории истина понимается как «логическое» свойство, а не как свойство в обычном смысле.

В этом случае определение кибербезопасности можно рассматривать как некий предикат, вычисляемый относительно свойств управляемого объекта и свойств его управления.

Обозначим предикат «кибербезопасность» через *Cs*. Тогда истинность утверждения о наличия свойства кибербезопасности будем определять через предикат свойств качества

и безопасности его управления *Ctl* и предикат свойства безопасности защищаемого объекта *Obj*.

$$Cs = Ctl \cdot Obj.$$

Рассмотрим подходы к формализации свойств качества и безопасности управления, которые были описаны в [4]: система является защищённой, если под воздействием факторов, влияющих на информацию, передаточная функция *AC* меняется таким образом, что качество управления объектом управления остаётся в заданных пределах. При этом под передаточной функцией *W* подразумевается зависимость сигнала *S(t)*, подаваемого на вход объекта управления, от структуры управляющего информационного трафика *I(t)*, поступающего на вход *AC*. Деструктивное воздействие информационной атаки *x(t)* приводит к изменению как управляющего трафика $I'(t)=I(t) \oplus x(t)$, так и самой управляющей функции $W'=W \circ x(t)$, в результате чего на объект поступает искажённый сигнал управления:

$$S'(t)=W'(I'(t)). \quad (1)$$

Система считается защищённой, если для всех возможных $x:S \rightarrow S'$ качество управления объектом управления остаётся приемлемым. В этом случае, используя подходы теории автоматического управления, можно говорить о том, что киберфизическая система, находящаяся в условиях деструктивного воздействия, должна обладать робастной устойчивостью и робастным качеством. В частности, для оценки качества переходных процессов можно применить три формализованных показателя качества управления – коэффициент перерегулирования σ, первое максимальное отклонение x_M и длительность $t_П$.

Тогда, если вернуться к введенному определению кибербезопасности, формализация понятия «управления в условиях деструктивных воздействий» может быть описано следующим образом.

В любой момент времени, независимо от условий воздействия на управляемый объект и систему управления, должно быть обеспечено условие:

$$Ctl(\sigma, x_M, t_П) = \{\sigma < \sigma^{max}, x_M < x_M^{max}, t_П < t_П^{max}\}.$$

В более общем случае предикат качества управления может зависеть от другого набора характеристик качества управления, например устойчивости, что не влияет на общность рассуждений.

Предикат безопасности защищаемого объекта *Obj* также можно представить как произведение предикатов, описывающих свойства безопасности, приведенные на рисунке 3.

$$Obj = Obj^{inf} \cdot Obj^{fun} \cdot Obj^{phy} \cdot Obj^{cic},$$

где

Obj^{inf} - предикат свойства информационной безопасности информационных активов;

Obj^{fun} - предикат свойства функциональной безопасности системы управления социотехнической системой;

Obj^{phy} - предикат свойства физической безопасности;

Obj^{cic} - предикат свойства безопасности систем промышленной безопасности (защита средств обеспечения защиты).

Предикат свойства информационной безопасности определим, в первом приближении, как превышение оценки величины предотвращенного ущерба $\overline{W}$ над допустимым уровнем ущерба $W_{доп}$.

$$Obj^{inf} = (\overline{W} > W_{доп}).$$

Методика расчета $\overline{W}$ приведена в [8] и основывается на оценке вероятности проявления угрозы из заданного перечня угроз и вероятности ее устранения, что фактически является риск-менеджментом и связывает с ним понятие кибербезопасности.

Для определения предиката свойства функциональной безопасности будем рассматривать управляемый объект как набор контролируемых параметров в сфере функциональной безопасности:

$$p_i \in P.$$

Тогда функциональная безопасность будет рассматриваться как удержание контролируемых параметров в заданных пределах:

$$Obj^{fun} = \{\forall p_i : p_i^{min} \le p_i \le p_i^{max}\}.$$

Предикат определения свойств физической безопасности определим как отсутствие сигналов, свидетельствующих о проникновении через рубежи защиты.

$$Obj^{phy} = \{\forall t > 0 \nexists s_i(t): s_i(t) \in S^{dan}\},$$

где S^{dan} – множество сигналов, расцениваемое как сигналы проникновения через рубеж физической защиты.

Предикат свойства безопасности систем промышленной безопасности можно определить по аналогии с предикатом свойства физической защиты – за рассматриваемый период времени при периодическом тестировании системы защиты отсутствуют сигналы, расцениваемые как недопустимые.

$$Obj^{cic}=\{\forall t > 0 \nexists s_j(t): s_j(t) \in S^{'dan}\}.$$

ВЫВОДЫ

Предложенный подход к определению кибербезопасности оценивается как перспективный, т.к. он учитывает:

- информационную безопасность всех категорий информации, обрабатываемых в социотехнических системах;
- подходы к обеспечению безопасности управления социотехнической системой в условиях воздействий неизвестной природы;
- ранее разработанные подходы к обеспечению и описанию информационной безопасности социотехнических систем.

Представляется целесообразным развить предложенный подход в дальнейших работах.

СПИСОК ЛИТЕРАТУРЫ

1. Гриняев С.Н., Правиков Д.И. Основы общей теории киберпространства. Теория боя в киберпространстве. – М.:АНО ЦСОиП, 2018. – 124 с.

2. Кардава Н.В. Киберпространство как новая политическая реальность: вызовы и ответы. // История и современность. – 2018.- № 2. – стр. 152 – 166.

3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2011. – 320 с.

4. Гарбук С.В., Правиков Д.И., Полянский А.В., Самарин И.В. Обеспечение информационной безопасности АСУ ТП с использованием метода предиктивной защиты. // Вопросы кибербезопасности. – 2019.- № 3(31) – стр. 63 – 71.

5. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации. // Вопросы кибербезопасности. – 2018.- № 2(26) – стр. 2 – 15.

6. Гриняев С.Н., Гришенин Р.Н., Правиков Д.И. Перспективные модели информационного управления социотехническими системами. // Современная наука: актуальные проблемы теории и практики: серия «Естественные и технические науки». – 2019.- № 3/2. – стр. 31 – 38.

7. Ламберов Л.Д. Дефляционные теории истины: проблема обобщенного определения. // Вестник НГУ. Серия: Философия. 2011. Т.9. Вып. 3. С. 13–19.

8. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ООО «ТИД «ДС», 2001.

Основные подходы к разработке протокола консенсуса в распределенных реестрах

P. Murzin

The main approaches to developing a consensus protocol in distributed registries

Abstract. *This paper provides a brief overview of existing consensus protocols in distributed ledgers. The issues of decentralization, confidentiality and anonymity are considered. The classification of blockchains and existing solutions to the problems of network scalability are given. An approach to the development of a fast and scalable private blockchain is proposed.*

Keywords: *distributed ledgers, consensus, decentralization, scaling, anonymity, completeness models.*

П.Е.Мурзин [1]
[1]АО «Концерн ГРАНИТ»
Email: murzin.p@granit-concern.ru

Аннотация. *В статье представлен краткий обзор существующих протоколов консенсуса в распределенных реестрах. Рассмотрены вопросы децентрализации, конфиденциальности и анонимности. Приведена классификация блокчейнов и существующие пути решения проблем масштабируемости сети. Предложен подход к разработке быстрого и масштабируемого приватного блокчейна.*

Ключевые слова: *распределенные реестры, консенсус, децентрализация, анонимность, масштабирование, модели завершенности.*

ВВЕДЕНИЕ

В последнее время в российской и зарубежной научной литературе все большее и большее внимание уделяется вопросам разработки распределенных реестров, блокчейнов, распределенных приложений (DApps). Бум технологии распределенных реестров начался с 2008 года, когда Сатоши Накамото опубликовал bitcoin whitepaper. В данной работе была решена проблема византийских генералов, или каким образом при условии абсолютного недоверия равноправные узлы в сети могут достигать консенсуса, а также решена проблема двойной траты [1].

При этом важно понимать, что bitcoin не был первым блокчейном. Уже на протяжении десятилетий математики и инженеры разрабатывают распределенные сети и протоколы консенсуса, но только с появлением проекта биткоина эта технология сделала значительный рывок вперед. Этот шаг сделал возможным создание приложений абсолютно нового типа. Сатоши Накамото удалось создать систему, которая способна функционировать при полном отсутствии доверия между участниками. Все взаимодействия основаны на строгой математике, никакого человеческого фактора – и именно в этом была революционность идеи, а не только в использовании peer-to-peer сети.

Одной из предпосылок к созданию биткоина послужил мировой финансовый кризис 2008 года, который резко подорвал доверие к банкам и существующей финансовой системе. Люди начали поиски новых инструментов обмена ценностями. Нынешнюю денежную систему критикуют за возможность бесконтрольно печатать деньги. Есть даже мнение, что существующая хищническая денежно-кредитная система является наибольшей угрозой человеческой свободе, миру и гармонии с окружающей средой, и должна быть упразднена и заменена уже проверенными временем инструментами или чем-то принципиально новым. Энтузиасты по всему миру анализируют возможные пути создания новой валютной системы.[2]

В то же время применение распределенных реестров не ограничивается исключительно финансовыми инструментами. В них можно хранить и другие активы. Деньги — одно из благ, которые ценятся человеком. В реестре можно учитывать не только деньги, но и документы, например, свидетельство о рождении и смерти, брачные договоры, права на собственность, дипломы о высшем образовании и научные звания, финансовые счета, медицинские процедуры, страховые случаи, результаты голосования, происхождение продуктов питания — все, что может быть представлено в цифровом формате. Отличие от печатных версий

этих документов состоит в том, что эти данные нельзя подменить или подделать (по крайней мере сделать это достаточно сложно). Таким образом, технология дает возможность обмениваться ценностями.

В процессе проектирования протоколов распределенных реестров разработчики сталкиваются со многими проблемами. Это и вопросы приватности, масштабирования сети и ее безопасности, децентрализации, а также увеличение пропускной способности системы, уменьшение энергопотребления и другие. В то же время на сегодняшний день не существует протокола, который мог бы адекватно отвечать современным требованиям. Этот факт побуждает исследователей и разработчиков экспериментировать и подробнее изучать механизмы работы распределенных реестров.

О ДЕЦЕНТРАЛИЗАЦИИ, КОНФИДЕНЦИАЛЬНОСТИ И АНОНИМНОСТИ В РАСПРЕДЕЛЕННЫХ РЕЕСТРАХ

Основой технологии распределенного реестра *(Distributed Ledger Technology, или DLT)* является протокол консенсуса. Под протоколом консенсуса понимается механизм или набор правил, с помощью которых сеть приходит к согласию, а именно каким образом узлы согласовывают валидацию транзакций. Роль консенсусных алгоритмов заключается в достижении уровня надежности сети, построенной на серии узлов (устройств, соединённых с другими устройствами как часть компьютерной сети). Это означает, что, если совершена транзакция, то алгоритм начнет работать - обмениваться данными по сети, чтобы проверить, может ли данное действие иметь место. Тот же процесс также применяется для создания новых узлов данных в блокчейне или при синхронизации сетевого оборудования, чтобы обеспечить согласованность всего консенсуса. При проектировании таких протоколов особое внимание уделяется вопросам децентрализации и анонимности.

Под децентрализацией понимается тот факт, что сеть абсолютно однородна и не контролируется какой-либо одной сущностью. При этом децентрализация рассматривается с разных аспектов: с точки зрения эмиссии (майнинга), верификации транзакций, хранения данных, разработки и модификации самого протокола.

Виталик Бутерин, создатель Ethereum, выделяет три типа децентрализации, применимых к программным продуктам: архитектурная, политическая, логическая [3]. Архитектурная децентрализация фактически отвечает на вопрос: из скольких физических машин состоит система, сколько компьютеров могут отказать в обслуживании одновременно, чтобы система продолжила корректно функционировать. Политическая – сколько сущностей реально контролируют систему. Логическая: является ли система монолитом или нет? Иными словами, если разделить систему на части, продолжат ли эти части функционировать независимо. Говоря о блокчейне, мы понимаем, что он архитектурно и политически децентрализован (т.е. никто его не контролирует и отсутствует единая точка отказа), но логически централизован (т.е. всегда существует лишь единственное состояние реестра и фактически система функционирует как единый компьютер).

Определим теоретические условия, в которых функционирует децентрализованный протокол консенсуса. Как уже отмечалось ранее, в системе отсутствует центральная доверенная сторона. Сеть состоит из равноправных или практически равноправных узлов. Если злоумышленник пытается провести атаку на узел, сеть продолжает нормально функционировать, пока честные участники системы составляют большинство всех работающих узлов. При этом честные узлы не знают, какие узлы были атакованы злоумышленниками. Более того, узлы могут выходить из строя и функционировать каким-либо произвольным образом, в том числе быть скоординированными злоумышленниками для проведения атаки против сети.

Также предполагается, что некоторые процессы и системы могут быть недоступны, а сообщения потеряны сетью или доставлены со значительной задержкой. Алгоритм консенсуса должен быть отказоустойчивым и работать для достижения заранее определенного консенсуса (одобрения от большинства машин в сети). Именно в таких условиях децентрализованный

консенсус должен продолжать нормально функционировать и все честные узлы должны приходить к одному и тому же журналу транзакций и получать одинаковый список блоков.

Таким образом, каждый честный узел приходит в одно и то же состояние в условиях сбоев части узлов или скоординированной работы злоумышленных узлов. Также накладывается следующее ограничение – протокол должен быть формализован, т.е. никакого дополнительного участия со стороны человека или иной сущности быть не должно, и только следуя четкому алгоритму, все честные узлы должны приходить к одному и тому же решению.

Однако следует понимать, что абсолютная децентрализация едва ли возможна [4,5]. И связано это прежде всего с тем, что у каждой системы есть «автор», который имеет больше знаний о ней и возможностях по ее доработке и изменению. Существуют и риски в централизации управления, например культ личности. Хотя по мнению Виталика Бутерина криптовалюты никем не контролируются, но его вес в мире криптовалют настолько велик, что большинство членов сообщества Ethereum согласились на возврат украденных средств The DAO, взлом которой был проведен в июне 2016 (таким образом образовался хардфорк Ethereum Classic), хотя это и нарушало одно из ключевых свойств блокчейна – неизменность. Также существуют риски централизации сервисов. Т.к. обработка всего блокчейна требует достаточно большой вычислительной мощности, обычные пользователи, которые хотят провести транзакцию, предпочитают использовать централизованные сервисы. Например, пользователи bitcoin доверяют blockchain.info, пользователи Ethereum – myetherwallet.com. Существуют и риски централизации майнинга, которые будут рассмотрены далее.

Одной из проблем, которую пытаются решить разработчики сегодня – это масштабируемость сети и увеличения ее пропускной способности. Современная оценка скорости транзакций биткоина – 5-7 транзакций в секунду, у Ethereum — 15-30. Причем эта оценка распространяется на всю сеть, поскольку каждый узел реплицирует (или полностью реплицирует в случае полной ноды) другие узлы. Добавление нового узла повышает устойчивость системы, но никоим образом не увеличивает скорость её работы или максимальный объём хранения данных. То есть, изменение данных (каждое изменение данных в блокчейне — это транзакция) является абсолютно минимизирующим фактором. Большая сеть медленнее синхронизируется, и одним из подходов для решения этой проблемы является применение «более централизованного» решения. Многие протоколы консенсуса предлагают использовать новые сущности в распределенных реестрах: «мастер-узлы», «свидетели», «федерации», «делегаты». Количество этих доверенных узлов может быть разным, но, используя этот метод для решения проблем масштабируемости, разработчики также разрушают децентрализованную природу блокчейна.

Таким образом, при проектировании распределенных реестров мы должны всегда отдавать отчет, что такие системы – это всегда компромисс между скоростью работы системы и степенью их децентрализации.

В целом, если рассматривать существующие алгоритмы консенсуса, то наиболее децентрализованным (и самым медленным) является используемый в Bitcoin консенсус Накамото (PoW). Все процессы максимально децентрализованы: эмиссия (майнинг), верификация транзакций, хранение данных. Даже разработка протокола и его модификация в настоящее время при использовании организационных мер децентрализована. Хотя и существует мнение о возможности проведения атаки 51% (теоретически это значение еще может быть снижено, см. раздел 2), т.к. всего 5 майнинг-пулов владеют большей частью хешрейта [6], но для оценки вероятности данного события необходимо представлять, как работает и что из себя представляет майнинг-пул. По факту пул – это множество узлов, которые объединяя свои мощности, получают больший хешрейт, а следовательно и большую вероятность стать создателем следующего блока. Далее прибыль в виде вознаграждения за добытый блок, а также комиссий за транзакции, включенных в него, делится среди участников пула. Для осуще-

ствления вышеуказанной атаки, майнинг-пулам первоначально необходимо прийти к согласию. Также важно понимать, что внутри майнинг- пула могут существовать свои правила и регламенты, и чисто технически, если члены пула не согласны с его политикой, они могут перейти «на работу» в другой пул, что может вызвать перераспределение мощностей в системе в любой момент времени. Поэтому хотя эта атака и выглядит пугающей, но в силу необходимости соглашения между пулами, а также между всеми членами пула не всегда тривиальна.

Помимо децентрализации, активно рассматриваются вопросы анонимности и приватности. Однако следует принимать во внимание тот факт, что на самом деле существующие криптовалюты псевдоанонимны. Например, в блокчейне биткоина каждая транзакция должна быть зарегистрирована публично (это сделано в целях безопасности сети). При этом все пользователи могут видеть денежный поток от адреса к адресу. Конечно, пользователи не могут идентифицировать эту информацию, потому как номер транзакции – это случайное число, а биткоин-адрес – это последовательность от 26 до 35 символов, полученных двойным хеширование открытого ключа сначала по алгоритму SHA256, а затем RIPEMD160, с дальнейшим прикреплением контрольной суммы. Однако анонимность заканчивается, когда пользователь обращается в криптообменник для вывода средств. Если далее он оплачивает покупку в интернете, то существует вероятность, что злоумышленник, увидев две транзакции, сможет сопоставить данные и доказать, что их произвел один человек. В целом, процесс деанонимизации проблематичен, т.к. существуют дополнительные серверы-миксеры (их услуги могут стоить дополнительных средств), которые могут подменять адреса или смешивать монеты. В некоторых случаях анонимность может служить частью схемы по отмыванию денег или иных криминальных схем. Существуют ряд сервисов вроде Chainalisys или Elliptic, задачей которых является расследование финансовых преступлений в блокчейн-технологиях.

Конфиденциальность в полной мере не обеспечивается. Но в некоторых проектах этому уделяется большее внимание. Например, в Dash используется механизм миксирования CoinJoin, в Monero используется кольцевая подпись (Ring Signature), которая по сути представляет собой электронную подпись, позволяющую одному из участников группы (называемой кольцом) выполнить подписание некоторого сообщения от имени всей группы, при этом не будет доподлинно известно, кто из участников группы выполнил подписание.

В проекте Zcash используется высокотехнологичная форма верификации с нулевым разглашением [7]. Доказательство «нулевого разглашения» позволяет одной стороне (доказывающему) доказать другой стороне (проверяющему), что утверждение верно, не раскрывая информацию, не касающуюся достоверности утверждения. Например, если существует хеш в виде случайных цифр, доказывающий может убедить проверяющего в том, что число с этим значением хеша действительно существует, не раскрывая его значения. Более того, существуют проекты по интеграции этого механизма в Ethereum [8].

Таким образом, говоря о децентрализации, анонимности и конфиденциальности, исследователи и разработчики распределенных реестров делают множество допущений, при которых их система действительно является таковой.

О СУЩЕСТВУЮЩИХ ПРОТОКОЛАХ КОНСЕНСУСА

Прежде чем перейти к рассмотрению различных протоколов консенсуса, необходимо провести классификацию распределенных реестров, т.к. выбор протокола консенсуса в целом зависит от типа используемого распределенного реестра. Распределенные реестры классифицируются по возможности участия в работе сети (публичный, консорциум, приватный), а также по возможности верификации транзакций (permissionless – инклюзивный, permissioned – эксклюзивный). Публичный блокчейн представляет собой открытую сеть, где любой участник может загрузить протокол, прочитать, написать к нему дополнение

принять участие в работе сети. В консорциум-блокчейне консенсус контролируется заранее определенным набором узлов, при этом права чтения могут быть публичны или ограничены для участников. В приватном блокчейне у каждого участника свой уровень доступа. У участника должно быть разрешение на запись, чтение, проверку блоков [9].

Permissionless от permissioned отличается тем, что в permissionless-модели новые транзакции могут быть зарегистрированы любыми участниками, в то время как в permissioned-блокчейнах вносить изменения в реестр может строго ограниченное число лиц. В зависимости от модели реестра могут применяться различные протоколы консенсуса.

Рассмотрим основные протоколы распределенных реестров - PoW (доказательство работы) и PoS (доказательство владения доли).

В PoW количество майнеров неизвестно, они анонимны (или псевдоанонимны) и не имеют репутации. Для того, чтобы добавить новый блок, участник должен доказать, что он выполнил определенную работу. Если быть точным, он решает очень сложную задачу по нахождению хэша (hash), который соответствует определенным правилам. Первый, кому посчастливилось найти правильную комбинацию, получает возможность добавить блок в цепочку. Консенсус достигнут, если стороны, контролирующие большинство хешрейта находятся в согласии. PoW используется в Bitcoin, Monero, Litecoin, Ethereum (в ближайшее время возможен переход на PoS). Преимуществом PoW является то, что он работает в среде, где участники могут не доверять друг другу. Однако это стоит огромных затрат вычислительных ресурсов (по некоторым сведениям, сеть биткоин потребляет 32 ТВтч в год, что примерно равно количеству электроэнергии, используемой Данией). Более того, скорость транзакций остается невысокой (процесс искусственно замедлен в целях безопасности). Еще одна проблема связана с тем, что большинство майнеров присоединяются к сети с целью заработать биткоины, а не для поддержания справедливости. После того как будут выпущены последние биткоины (это произойдет в 2140 году, т.к. эмиссия ограничена 21 миллионом монет), майнеры будут зарабатывать только на комиссиях от транзакций, включенных в блок. Если мотивация майнеров снизится, это может существенным образом повлиять на безопасность сети.

Техническая особенность PoS — отсутствие сложных и ненужных вычислений. Вместо того, чтобы конкурировать с другими, участники сети дают в залог свои криптоактивы, и ждут, чтобы их выбрали для создания нового блока. На практике этот алгоритм еще хорош, потому что мотивация участников сети кардинально отличается от PoW, т.к. участники заинтересованы в безопасности, ведь они сами владеют монетами системы. PoS опирается на вероятностную модель выбора валидаторов, где вероятность того, что валидатор сгенерирует блок, прямо пропорциональна количеству монет, внесенных им в качестве залога для безопасности сети. Если со стороны валидатора было замечено какое-либо нарушение (заверение неправильных или конфликтующих блоков), то залог может быть изъят. Консенсус достигается, если владельцы большинства монет согласовали состояние базы данных. PoS используется в Peercoin, Tezos, NXT, BitShares (DPoS). Алгоритм выбирает одного валидатора, основываясь на принадлежащей ему доле. Поэтому если участник владеет долей в 5%, то и проверять будет 5% транзакций. Идея состоит в том, что чем выше доля валидатора, лежащей в основе криптовалюты, тем меньше у него интерес к манипуляциям процессом валидации. Однако скептики указывают на тот факт, что валидаторы с крупными долями будут выбираться чаще и, стало быть, будут получать ещё больше токенов: богатые становятся богаче.

PoW и PoS отличаются моделями безопасностями, т.к. в PoS-протоколах система по факту основана на репутации. Валидаторы (минтеры/форджеры) могут терять ставки, если добавленные в блок транзакции оказались не валидными.

В PoW в целях безопасности искусственно замедлен процесс выпуска блоков (в биткоине в среднем 600 секунд). В консенсусе Накамото можно видеть, что часть блоков, генерируемых честными пользователями, все равно отбрасы-

вается (т.н. Orphaned blocks). Т.е. большая часть сети решила не продолжать на них цепочку. Если таких блоков немного, то это некритично. Но если их становится больше, когда сеть не успевает синхронизироваться, то получится, что часть вычислительных мощностей потрачена впустую. Поэтому злоумышленнику требуется даже менее 50% хешрейта для успешного проведения double-spending атаки, если в сети действительно большие задержки с доставкой сообщений. Подробные математические модели по теме были представлены в работе [10]. Именно поэтому в протоколах такого типа имеется значительное время генерации между блоками, что безусловно уменьшает пропускную способность сети. Но сделано это именно для того, чтобы сеть успевала синхронизироваться и вероятность появления таких блоков была мала.

Кроме искусственного замедления генерации блоков, PoW имеет стойкость еще засчет сложности выполнения работы (по сути узлы пытаются найти прообраз хеш-функции в соответствии с текущим уровнем параметра difficulty, который пересчитывается каждые 2016 блоков). Отсюда как следствие, в PoW колоссальные затраты электроэнергии.

По сравнению с PoW, PoS обеспечивает существенно большую пропускную способность системы (которая в принципе ограничена только задержками в синхронизации p2p-сети). PoS не требует избыточных затрат электроэнергии. При этом в PoS более сложный подход при разработке. В PoS атака 51% не имеет смысла. Для валидации транзакций достаточно иметь полную ноду и некоторое количество монет.

Тем не менее, PoS более централизован, чем PoW, т.к. чтобы запустить PoS-сеть, монеты уже должны находиться у участников. Здесь встает вопрос о том, кто и каким образом будет изначально распределять эти монеты между участниками (может быть ICO, премайн или другие механизмы распределения).

Первый PoS был имплементирован в PeerCoin, который является форком Bitcoin. При этом в Peercoin первые блоки генерировались с PoW, а далее на определенной высоте блок чейна добавилась возможность добавления PoS- блоков. Интересным моментом протокола Peercoin является тот факт, что вероятность формирования корректного PoS-блока пропорциональна не только количеству монет валидатора, но и их возрасту (CoinAge), т.е. положению транзакции в истории блокчейна [11]. PoS используется и в других блокчейн-сетях – NXT (протокол был имплементирован с нуля), BitShares (модификация PoS – DPoS), Cardano (PoS- протокол Ouroboros). Проект Ethereum планирует переход на PoS. В данный момент разрабатывается Casper. Casper – это совокупность двух исследовательских проектов: Casper FFG (Friendly Finality Gadget разрабатывает Виталик Бутерин) и Casper CBC (Friendly GHOST – correct by construction разрабатывает Влад Замфир) [12]. Casper FFG – это гибридный PoW/PoS механизм консенсуса. Он спроектирован таким образом, что PoS протокол работает поверх обычного Ethash PoW протокола. Таким образом, блоки продолжают генерироваться с помощью PoW, но каждый 50-ый блок дополнительно верифицируется PoS. Протокол Casper необходим Ethereum для масштабирования, энергоэффективности, а также для последующего перехода к PoS.

Рассмотрим одну из модификаций PoS – DPoS (делегированное доказательство доли). Одной из особенностей DPoS является распределение ролей. Существуют пользователи, комитет, валидаторы. При этом члены комитета и валидаторы не анонимны и имеют репутацию. Участники делегируют производство новых блоков небольшому и фиксированному числу избранных валидаторов. Голосование пользователей за создателя следующего блока проходит на основе PoS (чем больше монет у пользователя, тем весомее его голос). Держатели монет могут проголосовать за кандидатов в любое время. Это определяет высокую устойчивость сети: если большинство исполнителей терпят неудачу, сообщество сразу же проголосует за их замену. После того как пользователи проголосовали за валидаторов, происходит их сортировка. Из отсортированного списка валидаторов выбираются первые N валидаторов. Далее с использованием механизма Shuffle

каждому валидатору выделяется временное окно, в которое он может сгенерировать свой блок.

Преимущество DPoS состоит в том, что при такой схеме большая часть монет участвует в консенсусе, а также соблюдена строгая очередность валидаторов для создания блоков. Иногда применяется механизм Proxy Voting, при котором пользователь может делегировать право голоса узлу, которому он доверяет, чтобы тот смог голосовать за других представителей сообщества от его имени. DPoS используется в EOS и BitShares. DPoS позволяет создавать блоки на высокой скорости и обрабатывать большее количество транзакций в секунду, чем PoS.

Однако пропускную способность можно еще увеличить, если спроектировать протокол «еще более централизованным» образом. Например, протокол BFT хорошо подходит для разработки корпоративных блокчейнов. В этом случае участники знают друг о друге несколько больше данных, либо вообще участники известны с самого старта сети. Скорость может увеличиться до 10 раз, что отлично подходит для корпоративных решений. BFT представляет новый класс протоколов, в которых не требуются токены для голосования. Кроме того, данный тип протокола решает проблему задержек в коммуникации и сбоев в системе. Система будет работать, даже если нода переходит в оффлайн.

Как и DPoS для PoS, существует модификация BFT – DBFT (делегированная модель), использующая предопределенных валидаторов. Такая модель позволяет значительно увеличить пропускную способность. Например, пропускная способность блокчейна NEO составляет около 10 тысяч транзакций в секунду (но там используется объединенный протокол PoSDBFT).

Существует и более простая модификация BFT – PBFT, который является отличным решением для быстрого и масштабируемого приватного блокчейна. Его отличие от предыдущего варианта заключается в том, что он часто работает в приватной среде с известными участниками. Когда валидатор получает сообщение, он должен принять решение — верить ему или нет. Для этого он выполняет свои проверки и после опрашивает все остальные узлы по очереди, действительна ли транзакция по их мнению. Если ⅔ участников проголосовали за эту транзакцию, узел её принимает и передает своё решение в сеть для других валидаторов. Таким образом, консенсус достигается на основе подтверждения, которое будет представлено всеми валидаторами.

PBFT эффективен в системах с низкой задержкой, но очень чувствителен к количеству валидаторов и пропускной способности, так как одно сообщение генерирует множество других запросов и проверок. Он хорошо подходит для частной среды, где не требуется большая нагрузка, но есть потребность в большом количестве транзакций. PBFT гарантирует окончательность решений о транзакциях в сети, так как оно было принято абсолютным большинством в каждый момент времени. Такой протокол используется в Hyperledger [13].

Еще одним семейством протоколов является FBA (федеративное византийское соглашение). В отличие от протоколов семейства BFT этот протокол не требует разрешения или заранее известного набора участников. Транзакции валидируются фиксированным количеством участников, которые выбираются из числа тех, кто находится онлайн. Ликвидность сети обеспечиваются специальными шлюзами и мейкерами. FBA используется в Ripple и в его форке Stellar.

Рассматривая протоколы консенсуса, нельзя не упомянуть о моделях завершенности (finality) рассмотренных протоколов. Под завершенностью понимается подтверждение или гарантия того, что все правильно сформированные блоки не будут отменены, после того как попадут в блокчейн [14]. В семействах протоколов FBA и BFT завершенность немедленная, т.е. блоки, однажды попав в блокчейн, ни при каких обстоятельствах уже не будут отменены. В PoW и PoS завершенность носит вероятностный характер. Это значит, что вероятность того, что транзакция не будет отменена, увеличивается, если блок, содержащий эту транзакцию, «погружается все глубже» в блокчейн. Именно поэтому пользователям биткоина рекомендуется подождать, пока после блока, содержащего

транзакцию пользователя, не появится еще хотя бы 6 блоков (что занимает около часа), чтобы обеспечить очень низкую вероятность отмены этой транзакции. Тем не менее, эта вероятность ненулевая и чисто теоретически возможно создание форка с более длинной цепочкой блоков. В таком случае транзакции из блоков на параллельной цепочке будут отменены.

На первый взгляд может показаться, что немедленная завершенность гораздо более желательна для пользователей, чем вероятностная. Но существуют случаи, в которых использование вероятностной модели гораздо предпочтительнее. Здесь можно применить теорему CAP [15]. Теорема CAP гласит, что в случае раздела распределенная система может сохранять только либо согласованность данных, либо доступность. Система сохранения согласованности данных скорее остановит, чем пропустит неточные транзакции. Система сохранения доступности продолжит работу, даже если она позволяет проводить неточные транзакции. Системы, обеспечивающие согласованность данных, являются примером немедленной завершенности, а системы, обеспечивающие доступность,- вероятностную завершенность.

При осуществлении платежей пользователи часто предпочитают доступность, которую обеспечивают вероятностные окончательные цепочки (именно поэтому многие протоколы на основе DAG, в которых в первую очередь акцент сделан на доступность, а не согласованность, фокусируются на поддержке платежей). Однако многие блокчейн-платформы предлагают больше, чем просто платежи, например, децентрализованные приложения со смарт-контрактами.

Для различных DApps могут потребоваться разные модели завершенности. Для одних требуется доступность, и таким образом транзакции всегда были бы в состоянии преодолеть некоторые неточности, поэтому такие приложения имели бы вероятностную завершенность. А для других приложений, для которых важна согласованность данных, использовалась бы немедленная завершенность. Завершенность существенно влияет на UX приложений.

Помимо рассмотренных протоколов существуют и так называемые протоколы-«неблокчейны», имеющие отличную от последовательности блоков структуру. Создание таких протоколов – это по сути еще один подход к решению задачи масштабирования. Дело в том, что блокчейн имеет синхронную природу. Блокчейны не могут быть параллельными. Конечно, можно изменить размер блока (форк биткоина Bitcoin Cash пошел именно этим путем, увеличив размер блока с 1 Мб до 8 Мб) или их частоту генерации, или менять узлы, участвующие в валидации, по какому-либо алгоритму, но в конечном итоге вся история событий блокчейна ложится в строгую линейную последовательность.

В качестве альтернативы была предложена технология DAG (направленный ациклический граф). Она является асинхронной, что дает конкурентное преимущество при обработке одновременных событий. Протокол в таких системах позволяет участникам для добавления одного блока транзакций подтвердить несколько предыдущих. Т.е. сеть придерживается принципа: чем больше новых транзакций, тем быстрее валидируются старые. Но необходимо учитывать, что сверхвысокие скорости доступны только для большой сети, т.к. DAG будет более медленным в меньших масштабах. Такой протокол используется в проектах IOTA и ByteBall.

Еще одним протоколом-«неблокчейном» является Hedera HashGraph. Ключевым отличием от предыдущего варианта является использование механизма протокола «gossipaboutgossip» [16]. Узлы связываются случайным числом с использованием этого протокола и соглашаются на консенсус после определенного раунда коммуникации. Узел получает набор транзакций с меткой времени, о которых «знает» другой узел. Для работы такого алгоритма все участники в сети должны быть известными. В результате синхронизации каждый узел хранит всю информацию и историю получения этой информации всеми узлами сети. Как только узел видит в своей истории, что конкретное сообщение уже было получено и проверено большинством, то он считает его валидным. Однако в этой технологии существуют опреде-

лённые ограничения. Во-первых, существует мало доказательств практической реализации технологии в крупных масштабах, особенно по сравнению с рабочими блокчейн-проектами. Во-вторых, технология HashGraph запатентована, а приобретение лицензии стоит средств. И как следствие - отсутствие сильного сообщества (как например те, что связаны с проектами с открытым исходным кодом), которое могло бы проверить надежность протокола, его уязвимость перед атаками злоумышленников и проблемы совместимости.

Сегодня разработчиками рассматриваются и другие средства увеличения масштабируемости сети. Помимо упомянутых (таких как увеличение размера блока, повышение частоты их генерации, увеличение степени централизации сети, использование Casper в Ethereum, SegWit в Bitcoin) рассматриваются и другие подходы. Это и использование шардинга, при котором блокчейн разбивается на несколько частей – цепочек блоков, это и концепция «блокчейн как арбитр», при котором вычисления проводятся без участия блокчейна, а в блокчейне происходит только валидация. Также внимание разработчиков приковано к имплементации оффчейн-транзакций и state channels (подход, при котором транзакции собираются в группы, а далее уже группа добавляется в блокчейн).

О РАЗРАБОТКЕ ПРОТОКОЛА

В работе [17] была сформулирована концепция создания доверенного защищенного распределенного реестра. Также были определены требования к архитектуре системы и принцип нулевого разглашения информации о ней, а именно определена необходимость того, что для внешнего наблюдателя имена отправителя и получателя либо должны быть неизвестными, либо меняться при каждой транзакции. Было выявлено, что для надежного функционирования системы, необходимо обеспечить несколько следующих механизмов. Во-первых, пользователь должен иметь свой приватный идентификатор, который вырабатывается при помощи ДСЧ с гарантированными статистическими свойствами и известен только ему. Этот приватный идентификатор хранится исключительно у пользователя на отчуждаемом носителе и не передается по сети (для защиты от НСД). Во-вторых, пользователь должен обладать некоторым псевдонимом (т.н. сетевым именем), который создается на основе его приватного элемента. При этом исключается возможность выявления связей между сетевым именем и цифровыми данными пользователя со стороны внешнего наблюдателя. В качестве некоторой аналогии для сетевого имени можно привести адрес в биткоине, но там для формирования адреса используется двойное хеширование открытого ключа, а затем перевод в систему счисления по основанию 58. В то же время сетевое имя должно быть проверяемым, т.е. уполномоченный орган должен иметь возможность убедится в соответствии сетевого имени и данных пользователя.

Стоит отметить, что в системе присутствует доверенная сторона – оператор. Он знает имена пользователей, т.к. должен взаимодействовать с ними, передавать информацию и пр. В общем случае он обеспечивает обработку информации пользователей с использованием криптографических процедур, использующих сетевой ключ, который был сформирован на основе сетевого имени пользователя и закрыт паролем и который не известен другим пользователям системы. Также должен быть реализован безопасный транспорт для передачи информации от пользователя к оператору распределенного реестра и произведен контроль целостности и аутентичности информации, помещаемой в реестр. Факт помещения информации в реестр должен фиксироваться в квитанциях, заверенных оператором. Участники могут формировать запросы на выдачу информации из реестра. При этом должна быть реализована система разграничения доступа к ней. Кроме того, для механизма обеспечения “нулевых знаний” о структуре системы, ее участниках и транзакциях необходимо реализовать процедуру изменения имен отправителя и получателя, а также других данных транзакции, зависящей от сетевого ключа пользователя.

Для обеспечения большей децентрализации системы, предполагается использовать

нескольких операторов распределенного реестра. В этой системе все участники известны операторам. При этом операторы не анонимны, а данные пользователей им известны. Поэтому для быстрого и масштабируемого приватного блокчейна будет разработан механизм консенсуса, основанный на протоколе BFT с немедленной моделью завершенности.

Предполагается спроектировать протокол таким образом, при котором операторы будет организованы в специальную структуру, т.н. виртуальное дерево, для распараллеливания верификации блоков честными операторами. Если вдруг нечестный оператор мешает верификации, то корни всех поддеревьев, которые смогли достичь соглашения, выполняют BFT-консенсус для завершения раунда. При этом используется меньшее количество сообщений, чем в случае участия всех операторов. Далее необходимо перестроить дерево таким образом, чтобы в нем находились только надежные узлы. Таким образом можно ограничить влияние недобросовестных операторов.

Эта стратегия организации позволяет честному и надежному кворуму операторов быстро распределять необходимое количество блоков распределенным образом, что позволяет алгоритму масштабироваться до большого количества операторов, если это будет необходимо.

Для подписания транзакций можно использовать механизм мультиподписи. Например, сначала пользователь полуподписывает транзакцию, а далее отсылает запрос оператору на ее доподписание и уведомляет оператора через второй фактор аутентификации (смс, email, физическое посещение и другие каналы передачи данных). Сервис удостоверяется в валидности пользователя и доподписывает транзакцию. Преимущество такого подхода заключается в безопасности и удобстве использования. Оператор не сможет украсть данные пользователя, т.к. не сможет получить к ним доступ без его разрешения. При этом пользователь может иметь защищенный доступ из любого места.

Также можно увеличить скорость поиска транзакций в реестре. В настоящее время реестр представляет собой совокупность индексного и информационного файлов. Индексный файл используется для быстрого поиска в реестре. Внедрив механизм кеширования, например, как в bitcore, можно сделать поиск еще более быстродействующим.

ЗАКЛЮЧЕНИЕ

Резюмируя, можно сказать, что сегодня существует множество различных протоколов консенсуса. И каждый из них имеет достоинства и недостатки. Протоколы консенсуса являются неотъемлемой частью распределенных систем. Протоколы консенсуса разрабатываются в зависимости от типа распределенного реестра. Proof-of-Work стал первым и самым надежным протоколом консенсуса для публичных блокчейнов, таких как Bitcoin и Ethereum. Proof-of-Stake не требует сложных вычислений. Вместо этого, он поощряет пользователей закладывать собственные средства для выполнения эквивалентного количества проверок транзакций и предполагает, что все будут действовать рационально. BFT является упрощением концепции PoS, которая делает её намного быстрее. Однако BFT протоколы практичны только в небольшой и приватной среде. PBFT — это проверенное решение для приватных распределённых систем. DBFT улучшает BFT, позволяя участникам сети делегировать ответственность на валидаторов. Этот протокол, в отличие от PBFT, может быть использован в публичной среде. Очень быстрый, но более централизованный. Хотя вышеупомянутые варианты BFT являются блокчейнами, требующими разрешения, чтобы быть допущенным к сети, FBA является открытым для участия и часто не требует разрешения. Также были рассмотрены и другие протоколы-«неблокчейны».

Тем не менее, на сегодняшний день существует множество вызовов для разработчиков распределенных реестров. Абсолютные децентрализация, анонимность, конфиденциальность требуют значительных ресурсов сети и потому едва ли достижимы. Перед сообществом стоят нерешенные задачи масштабируемости, увеличения пропускной способности сети, снижения степени централизации серви-

сов, хранения данных, обратной совместимости реестров.

СПИСОК ЛИТЕРАТУРЫ

1. S. Nakamoto, “Bitcoin Whitepaper”, URL: https://bitcoin.org/bitcoin.pdf- (Дата обращения: 17.07.2019).

2. Топливно-энергетический комплекс в эпоху становления цифровой экономики / Ткачева В.Л., Гриняев С.Н., Правиков Д.И., Фатьянов А.А., Шушкевич Ю.А. – РГУ нефти и газа им. И.М. Губкина – 2019.

3. V. Buterin, “The meaning of decentralization”, https://medium.com/@VitalikButerin/the-meaning-of-decentralization- a0c92b76a274 – (Дата обращения: 17.07.2019).

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

5. Блог компании Waves, URL: https://habr.com/ru/company/waves/blog/404051/- (Дата обращения: 20.07.2019).

6. Ameer Rosic, Hypothetical attacks on cryptocurrencies, URL: https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies- (Дата обращения: 20.07.2019)

7. Zcash company blog, zk-SNARKS, URL: https://z.cash/technology/zksnarks- (Дата обращения: 21.07.2019)

8. Gautam Botrel, “How Zcash can fill Ethereum’s Privacy Gap”, URL:https://media.consensys.net/how-the-zcash-protocol-can-fill-ethereums-privacy-gap-4fb8e58cd429 - (Дата обращения: 21.07.2019)

9. Vitalik Buterin, Ethereum blog, https://blog.ethereum.org/2015/08/07/on- public-and-private-blockchains- (Дата обращения: 21.07.2019)

10. Bitfury Group, Proof of Stake versus Proof of Work Whitepaper, Version 1.0- 2015, https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf

11. Sunny King, Scott Nadal , PPCoin: Peer-to-Peer Crypto-Currency with Proof- of-Stake, 2012, https://peercoin.net/whitepapers/peercoin-paper.pdf

12. Introducing the “Minimal CBC Casper” Family of Consensus Protocols / Vlad Zamfir, Nate Rush, Aditya Asgaonkar, Georgios Piliouras – 2018. URL: https://github.com/cbc-casper/cbc-casper-paper/blob/master/cbc-casper-paper- draft.pdf

13. An Introduction to HyperLedger. URL: https://www.hyperledger.org/wp- content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf- (Дата обращения: 22.07.2019).

14. Alexis Gauba, Finality in Blockchain Consensus, https://medium.com/mechanism-labs/finality-in-blockchain-consensus- d1f83c120a9a- (Дата обращения: 22.07.2019).

15. Википедия, URL: https://ru.wikipedia.org/wiki/Теорема _CAP- (Дата обращения: 23.07.2019).

16. Dr. Leemon Baird, Mance Harmon, and Paul Madsen. Hedera: A Public Hashgraph Network & Governing Council V.1.5 – 2019. URL: https://www.hedera.com/hh-whitepaper-v1.5-190219.pdf

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

18. Онлайн-лекции по блокчейн-технологиям, dlt-academy.com

Возможности использования криптовалют в интересах стабилизации и развития финансовых рынков и национальных денежных систем

Yu. A. Shushkevich

Opportunities of cryptocurrencies in favour of stabilizing and developing financial markets and national monetary systems

Abstract. *The article focuses on impact which cryptocurrencies provide on financial markets and national monetary systems and reveals the causes of variations in policies regarding cryptocurrencies in different states. The mechanisms through which cryptocurrencies circulation can cause damage or, conversely, create competitive advantages for national financial markets, are shown. A proven conclusion is made that the Russian Federation fundamentaly benefits from significant and long-term prerequisites of using national cryptocurrency in the interests of support international trade and ensuring national interests under unilateral sanctions and restrictions by the United States and other western countries. Basic characteristics and operating principles of possible Russian national cryptocurrency are given, as well medium– and long-term forecast of its impact on development of financial market and formation background for strengthening Russian ruble with the prospect of its becoming a full-fledged mean of international transactions and reserve currency in global scale.*

Keywords: *cryptocurrency, Bitcoin, Ethereum, Tether, Libra, Stock market, Debt market, Foreign exchange market, Monetary system, Fiat currencies, China, USA, Switzerland, National Russian Cryptocurrency, Sanctions, Global reserve currency.*

***Ю.А.Шушкевич*[1]**

[1]кандидат экономических наук,
заместитель начальника по экономике и инновациям,
Центр развития криптовалют
и цифровых финансовых активов ВИНИТИ РАН
Email: Yuri_Shushkevich@mail.ru

Аннотация. *В статье рассматриваются вопросы влияния криптовалют на финансовые рынки и национальные денежные системы и анализируются причины специфики политики по отношению к криптовалютам в различных государствах. Показаны механизмы, посредством которых обращение криптовалют может нанести ущерб или, наоборот, создать конкурентные преимущества национальным финансовым рынкам. Делается обоснованный вывод о наличии у Российской Федерации фундаментальных предпосылок для использования национальной криптовалюты в интересах укрепления международного экономического сотрудничества и обеспечения национальных интересов в условиях односторонних санкционных ограничений со стороны США и ряда других стран. Приводятся основные характеристики и принципы работы проектируемой национальной криптовалюты, дается средне– и долгосрочный прогноз ее влияния на развитие в России финансового рынка и формирование условий для стабилизации и укрепления рубля с перспективой его превращения в полноценное средство международных расчетов и одну из мировых резервных валют.*

Ключевые слова: *криптовалюта, биткойн, эфириум, Tether, Libra, фондовый рынок, долговой рынок, валютный рынок, денежная система, фиатные валюты, Китай, США, Швейцария, национальная российская криптовалюта, санкции, мировая резервная валюта.*

ВВЕДЕНИЕ

Криптовалюта — это цифровая валюта, эмиссия, обращение и контроль за которой осуществляются с использованием криптографических методов. За последнее десятилетие криптовалюты из старапов отдельных энтузиастов превратились в объемный и развитый сегмент глобального финансового рынка с общей капитализацией более 0.3 трлн. долларов США, в том числе биткойна (BTC) — более 180 млрд. долларов США [1], [2].

С точки зрения количественного масштаба финансовых рынков, суммарная капитализация которых поддается лишь приблизительной оценке, составляющей только по группе 10 развитых стран, включая Россию, 52 трлн. долларов США для фондового рынка и 68 трлн. долларов США для долгового рынка [3], доля криптовалют по их суммарной капитализации не превышает 0.25%. Еще меньше окажется доля криптовалют в масштабе расширенного глобального финансового рынка, включающего рынок деривативов, объем которого на сегодняшний день оценивается в интервале от 300 до 600 трлн. долларов США [4], [5]. Казалось бы, что криптовалюты были и остаются незначительным по значению финансовым активом, интересным только небольшим группам субъектов финансового рынка.

Однако ситуация выглядит совершенно по-другому, если сопоставить капитализацию криптовалют с денежной массой фиатных валют (денежный агрегат М1). Так, по состоянию на середину 2019 года отношению к денежной массе долларов США капитализация криптовалют составляет 7.8%, по отношению к валютам еврозоны 3.1%, по отношению к российскому рублю — 93% [6]). А поскольку все сегменты финансовых рынков привязаны к фиатным валютам, в которых номинируется их оборот и фиксируется прибыль, то здесь криптовалюты начинают играть очень важную и чувствительную роль.

Не случайно поэтому наиболее жесткие запреты на использование криптовалют, зачастую караемые тюремным заключением, введены в странах со слабыми, неустойчивыми национальными валютами, такими как Непал, Боливия, Бангладеш, Алжир, Вьетнам, Индонезия, Таиланд и др. Страны с сильными валютами и устойчивой финансово-кредитной системой в тех или иных формах допускают свободный оборот криптовалют, постепенно и весьма осторожно разрабатывая нормативные акты для его регулирования,— это, прежде всего, США, Канада, Германия, Великобритания, Израиль и др. Наименьшим числом ограничений по операциям с криптовалютами характеризуются такие страны, как Швейцария, Япония и Сингапур — можно утверждать, что в этих странах криптовалюты практически легализованы.

Основной причиной для беспокойства национальных финансовых властей по отношению к криптовалютам является такое их свойство, как *трансграничность*. Так, во Вьетнаме и Непале официально обнародованной причиной максимально жесткого запрета криптовалют является опасение, что финансово неграмотное население, в расчете на курсовой рост вкладывая в криптовалюты личные средства и даже специально взятые кредиты, будет способствовать «сбросу» национальной валюты на обменном рынке с неизбежным снижением ее курса.

Анонимность криптовалют выступает второй причиной вводимых против них ограничений, хотя «анонимность блокчейна» — в значительной степени миф, поскольку при наличии соответствующих технических и программных возможностей отслеживание транзакций в блокчейне с определением имен и адресов конечных устройств — вполне решаемая задача. Другое дело, что ее решение возможно при высоком уровне подготовке соответствующих государственных служб, которым страны «третьего мира» не могут похвастать.

Следующей причиной настороженного отношения к криптовалютам является *децентрализация размещения и обращения*, создающая известные неудобства и потенциальные риски для национальных денежных регуляторов. Так, даже в США сделалась очевидной резкая оппозиция Федеральной Резервной Системы к планам компании FaceBook по запуску криптовалюты Libra — к проекту, активно поддержанному многими американскими банками и финансовыми операторами Visa, MasterCard, PayPal и др. [7].

Наконец, беспокойство взывает *необратимость платежей*, осуществляемых посредством криптовалют. Малозначимая у частных пользователей невозможность отозвать совершенный с помощью криптовалюты платеж для крупных корпораций и государственных структур — при ошибках персонала или в случаях мошеннических действий — становится фактором опасности и необратимого ущерба.

Отсюда можно сделать общий вывод — появление криптовалют и их становление в качестве полноценного платежного средства стало реальным вызовом для финансовых систем стран мирового сообщества. Реакция на этот вызов неоднозначна и зависит во многом от уровня экономического развития государств и устойчивости их политических систем. Однако тот факт, что несмотря на многочисленные проблемы и потенциальные угрозы криптовалютный сектор продолжает развиваться, свидетельствует о наличии у него мощного позитивного потенциала.

ВОЗМОЖНОСТЬ И НАПРАВЛЕНИЯ ПОДДЕРЖКИ НАЦИОНАЛЬНЫХ ФИАТНЫХ ВАЛЮТ С ПОМОЩЬЮ КРИПТОВАЛЮТЫ

Принципиальная возможность положительного влияния криптовалют на национальные

системы традиционных фиатных валют длительное время не признавалась в силу факта прямой конкуренции «токена с фиатом», а также из-за отсутствия при криптовалютном обороте обременений по государственным налогам и резервированию. Также отмечалось, что криптовалютный оборот способен привносить возмущения на денежный (межбанковский валютный) рынок, нарушать платежный баланс государств и провоцировать неточности в системе национальных счетов.

Однако, как показала практика, для финансовых систем стран с развитой экономикой и устоявшимися потоками экспортно-импортных операций появление криптовалют прошло практически незамеченным. Понятно, что перевод расчетов по межстрановым потокам товаров и иных материальных ценностей, которые легко учитываются таможенными службами, из «фиата» в криптовалюту с целью сокрытия доходов и ухода от таможенных платежей — в массовом масштабе невозможен. А оплчиваемые криптовалютой внешнеторговые операции по услугам для стран с развитой экономикой практически безопасны, поскольку итоговое (конечное) использование доходов от последних осуществляется, как правило, в исходных юрисдикциях. Можно допустить, что оплаченный криптовалютой доход от неких услуг, оказанных в США, будет в конечном итоге потреблен в Великобритании или Швейцарии,— однако в силу интегрированности западных рынков практически наверняка аналогичный по объему доход, полученный в Швейцарии и Великобритании, окажется потребленным в американской юрисдикции.

Также для развитых стран практически полностью исключены потери, связанные с уходом крупных налогоплательщиков в «криптовалютную тень». Для стабильно работающих компаний такой уход немедленно окажется в фокусе внимания фискальных органов, а аналогичные действия со стороны субъектов с разовыми и случайными доходами в таких странах не могут считаться критичными. В условиях несущественности перечисленных выше рисков основным преимуществом, которое оборот криптовалют способен принести денежным рынкам, становится приток иностранных фиатных валют в процессе покупки той или иной популярной криптовалюты, а также в процессе майнинга (если таковой предусмотрен). Так, до 2017 года центром притяжения зарубежных фиатных валют был материковый Китай, где осуществлялось до 80% мирового майнинга биткойна, и биткойнами оплачивалось до 30-40% стоимости так называемого «серого», то есть проходящего таможенный контроль по максимально заниженным ценам, экспорта китайских товаров в страны Юго-Восточной и Средней Азии, а также в Россию [8]. Оборот китайских резидентов по криптовалютным операциям только с Россией в 2017-2018 гг достигал 4.5-5.0 млрд. долларов США [9], а в целом он оценивается в 50-70 млрд. долларов США ежегодно. Операции с биткойнами объективно усиливали трансграничный спрос на юани и доллары Гонконга (ставшего основной площадкой для обмена биткойнов на «фиат» после запрета конвертации криптовалют в КНР в 2013 году), что объективно способствовало укреплению указанных китайских фиатных валют [10]. В постиндустриальной экономике крепкая национальная валюта считается одним из условий привлекательности страны для притяжения каптала, способствуя переводу в ее юрисдикцию финансовых активов из других стран,— однако для экономики Китая, опирающейся на индустриальную модель, более важным оказалось поддерживать курс юаня на минимально допустимом уровне. Следование данной политике послужило одной из причин жестких мер, предпринятых правительством КНР против операций с биткойнами на протяжении 2013-2017 гг, что в итоге привело к обвальному снижению курса биткойна в 2018 году. Однако независимый китайский бизнес быстро нашел замену, перейдя на использование стабильной (в отличие от биткойна жёстко привязанной к доллару США) криптовалюты Tether (USDT), эмитируемой одноименной компанией из Гонконга [11]. Поскольку конверсионные операции компания Tether проводит вне юрисдикции КНР, в основном на Тайване и в США, то китайские владельцы криптовалюты USDT вполне уверены в ее стабильности на длительную перспективу.

Немаловажно отметить, что в начале 2019 года китайские пользователи биткойна нашли альтернативные пути конвертации BTC в фиатный юань или доллар, благодаря чему курс BTC вырос практически в два раза [12]

Таким образом, своеобразный и отчасти парадоксальный опыт Китая по борьбе с криптовалютами во имя недопущения укрепления китайского юаня подтверждает наличие значительного влияния показателей денежного спроса и предложения на состояние национального финансового рынка. В условиях валютного рынка России с ежедневным средним объемов торгов 20.4 млрд. долларов США (по состоянию на июль 2019 года) [13], когда изменение теоретического предложения валюты со стороны экспортеров углеводородного сырья, составляющего от 480 до 520 млн. долларов США в день, из-за 3%-го изменения мировых цен (на 15 млн. долларов США) приводит к изменению курса в паре «доллар-рубль» в среднем на 1.5% [14], наличие положительного сальдо по операциям с криптовалютами в размере порядка тех же 15 млн. долларов США в день способно, по нашей оценке, укрепить рубль с условных 65 до 64 рублей за доллар. Если же это сальдо в длительной перспективе окажется устойчивым и начнет фиксироваться и учитываться участниками межбанковских валютных торгов, то его влияние на укрепление рубля может оказаться еще более существенным.

Описанные выше механизмы поддержки национальных валют с помощью криптовалюты работоспособны и эффективны при наличии следующих факторов:

— криптовалюта расходуется или конвертируется, в основном, в рамках национальной юрисдикции;

— курс национальной валюты формируется посредством валютного рынка, а не через параметры рынка долгового (как в случае с первоклассными резервными валютами: долларом США, евро, британским фунтом и швейцарским франком).

Оба эти фактора применимы в России, поэтому имеется возможность путем либерализации механизмов обмена криптовалют на рубли значительно повысить показатели использования криптовалют в отечественной юрисдикции. В условиях, когда в значительной части стран мира операции с криптовалютами в той или иной степени ограничены, Россия имеет возможность стать «операционным хабом», получая выгоды от дополнительного притока на свой рынок иностранных валют и оказывая соответствующие финансовые услуги.

Примечательно, что для стран с первоклассными резервными валютами «криптовалютный приток» несет больше проблем, нежели выгод, поскольку чувствительность параметров долгового рынка к избытку предложения «фиата» в условиях сверхнизких долговых ставок, характерных для этих стран, значительно выше, нежели чувствительность валют типа рубля к избытку предложения на рынке валютном. Именно по этой причине главный регулятор США — Федеральная Резервная Система — вступает категорически против запуска криптовалюты Libra, эмиссию которой планирует осуществить компания Facebkook. Поскольку Libra проектируется как привязанный к американскому доллару «стэйблкойн» и гарантированно сможет заменить часть долларов в обращении, «избыток» долларов неизбежно начнет вредить планам регулятора по повышению базовой процентной ставки, что ограничит в США приток капитала и поставит под вопрос исполнение дефицитного госбюджета.

По нашим оценкам, если капитализация Libra достигнет 200 млн. долларов США (аналогично биткойну), то есть 5% от капитализации доллара США (агрегат M1 по состоянию на 13.07.2019 составлял в США 3.79 млрд. USD), то это приведет к снижению доходности по краткосрочным (годовым) облигациям США на 0.5-0.6%, по долгосрочным (10-летним) на 0.3-0.4%, то есть примерно на одну четверть — одну треть от сложившихся котировок. Понятно, что такая угроза категорически не устраивает финансовые власти США даже несмотря на то, что они располагают механизмами изъятия с рынка «излишней ликвидности».

Аналогичными соображения руководствуются и финансовые власти других стран с

«первоклассными» валютами, из-за чего ни о каких масштабных проектах, связанных с крипто-валютами, на сегодняшний день там не слышно.

Однако ни в коем случае нельзя считать, что потенциальная выгода от криптовалют в подобных условиях будет доставаться «бедным» странам. Неэффективная экономика, слабый или недиверсифицированный внешнеторговый оборот, закредитованность и неразвитость финансового рынка в странах с низким уровнем развития никоим образом не могут быть отменены или хотя бы исправлены «с помощью» криптовалют. Убедительный тому пример — история с неудачной эмиссией государственной криптовалюты Венесуэлы Petro (PTR), предпринятой в 2017 году. Несмотря на законодательное закрепление привязки (обеспечения) Petro нефтяными запасами венесуэльской провинции Атапирире и адекватное программное обеспечение на базе блокчейна Etherium, внешний спрос на новую криптовалюту не проявился, а внутренний спрос оказался слабее самых неблагоприятных прогнозов. Первое и по сути единственное размещение Petro было оплачено неустановленными лицами, за которыми ряд аналитиков предполагает российские и китайские компании, ведущие бизнес с нефтяной отраслью Венесуэлы. Криптовалюта Petro используется внутри страны для уплаты налогов и ограниченно — для расчетов за услуги. Обращение и конвертация Petro за пределами Венесуэлы отсутствуют [15].

Принято считать, что основной причиной неудачи Petro являются санкции США, введенные против данной криптовалюты и запрещающие гражданам и компаниям США осуществлять с ней какие-либо операции [16]. Однако не меньше оснований полагать, что причина состоит в неустойчивости политической ситуации в данной стране и сильнейшем экономическом кризисе, которые ставят под сомнение как возможность реализовать нефтяное обеспечение Petro, так и сохранить в длительной перспективе гарантии, выданные в отношении нее нынешним политическим руководством Венесуэлы.

ОБЕСПЕЧЕНИЕ СТАБИЛЬНОСТИ НАЦИОНАЛЬНЫХ ФИНАНСОВЫХ СИСТЕМ В УСЛОВИЯХ ТОРГОВЫХ ОГРАНИЧЕНИЙ И ПОЛИТИЧЕСКИХ САНКЦИЙ ПОСРЕДСТВОМ КРИПТОВАЛЮТНЫХ ТЕХНОЛОГИЙ

Анализ негативного опыта венесуэльской криптовалюты Petro показывает, что «криптовалютные инициативы» в странах с проблемной экономикой и неустойчивой политической системой не имеют заметных перспектив. А наличие противодействия, вплоть до прямых санкций, со стороны Соединенных Штатов, гарантирует подобным проектам откровенную неудачу.

В то же время нельзя не видеть, что в мировой экономике действует большое число интересантов, находящихся под давлением и ограничениями со стороны США и потому заинтересованных в существовании возможностей обеспечивать свои торговые и финансовые интересы вне сферы, где существуют или могут быть введены рестрикции. В настоящее время под теми или иными санкционными ограничениями со стороны США находятся следующие страны (или значительные по влиянию группы экономических субъектов в соответствующих странах): Беларусь, Бирма, Кот-д'Ивуар, Куба, Демократическая Республика Конго, Иран, Ливан, Ливия, Северная Корея, Сомали, Судан, Южный Судан, Сирия, Йемен, Зимбабве, Китай, Россия. Помимо экономических ограничений против государств, с начала 2000-х годов США практикуют точечные санкции против отдельных финансовых институтов, в том числе на территории стран, с которыми США находятся в политическом союзе: среди них французский банк BNP Paribas (2014, штраф 8.97 млрд. USD за «нарушение режима санкций в отношении Судана, Ирана и Кубы[1]»), германский Deutsche Bank AG (2016-2017, штраф до 14 млрд. USD за «манипулировании ценами на ипотечные бумаги в период до кризиса 2008 года», британ-

[1]Речь идет не о международных санкциях, вводимых резолюциями Совета Безопасности ООН, а об односторонних санкциях, объявленных правительством США

ский банк HSBC (2012, штраф 1.92 млрд. USD за операции с Кубой), британский банк Standard Chartered (2012, штраф 667 млн. USD за транзакции с Суданом, Бирмой и т.д.), швейцарский банк Credit Suisse (2012, 2018, штрафы около 3 млрд. USD за операции с Ираном и «за помощь гражданам США в уклонении от налогов»), британский банк Lloyds TSB Bank (2012, штраф 350 млн. USD за операции с Суданом и Ираном), британский банк Barclays (2016, штраф 298 млн. USD за предоставлении корреспондентских услуг для банков на Кубе, в Иране, Ливии, Судане и Бирме) и др. Начиная с 2011 года финансовые власти США активно преследует банки Швейцарии «за содействие в уклонении от налогов» собственных граждан, в 2013 году в результате этих действий прекратил существование старейший в Швейцарии банк Wegelin & Co, ведущий свою историю с 1466 года. Всего за период 2009-2019 гг Министерство финансов США, Министерство торговли США и Министерство юстиции США оштрафовало 191 компанию и десять физических лиц за нарушение своих санкционных режимов (здесь и далее представлены оценки Российского совета по международным делам) — всего 201 случай [17]. Наконец, под фактическими финансовыми санкциями находятся ненатурализованные граждане США (т.е. люди, формально считающиеся американскими гражданами в силу места рождения, но на территории США не проживающие), все доходы которых свыше минимума в 97 тыс. USD подлежат декларированию и налогообложению американскими властями [18]. Так, в 2014 году фискальные органы США предъявили претензии по неуплате налога на прирост капитала и подоходного налога на сумму в несколько миллионов долларов мэру Лондона Б.Джонсону, основанием для чего послужил факт рождения известного британского политика в Нью-Йорке [19].

В условиях, когда в мире сложился значительный по масштабу кластер государств, экономических субъектов и частных лиц, объективно заинтересованных вести дела гарантированно вне юрисдикции Соединенных Штатов, объективно формируется потребность в финансовых механизмах, способных обеспечивать расчеты и накопление не только без использования замыкающихся на банки США корреспондентских счетов в долларах США, но и вне финансовых институтов, на которые могут быть обращены претензии и так называемые «вторичные санкции».

Определенную роль в этой миссии приняли на себя наиболее капитализированные криптовалюты — биткойн и эфириум (Etherium). Однако в силу объективной нестабильности курсов использование указанных криптовалют в целях накопления затруднено, а в расчетах — сопряжено с риском значительных издержек.

Не решают проблемы и так называемые “стэйблкойны» — уже упоминавшийся Tether, а также BitUSD, BaseCoin, смарткойн Dai и ряд других. Операторы всех выведенных на рынок «стэйблкойнов» используют для конвертации и обеспечения своих продуктов долларовые счета и расположены в уязвимых для претензий США юрисдикциях. Также для ряда операторов, не подлежащих обязательному аудиту, под вопросом оказываются размеры заявленных резервов и финансовая состоятельность [20]. В то же время относительный успех «стэйблкойна» Tether, за относительно короткий срок достигшего капитализации более 4 млрд. долларов США [21], говорит о высокой востребованности такого рода инструментов.

Глобальная потребность в криптовалюте стабильного класса в полной мере может быть обеспечена новой криптовалютой, централизованный выпуск и биржевое обслуживание которой в части конвертации в фиатные валюты будет обеспечиваться с территории Российской Федерации.

Предпосылки для успешной реализации проекта подобного рода следующие:

- стабильно работающая экономика со значительными доходами от экспорта, диверсифицированными по странам и товарным группам;
- в достаточной степени устойчивая национальная фиатная валюта — российский рубль — через операции с которым могут осуществляться конвертационные операции, полностью изолированные от «долларовой зоны»;
- возможность быстрой мобилизации на внутреннем финансовом рынке денежных

ресурсов на кратко- и среднесрочной основах для использования в конверсионных операциях и операциях по стабилизации новой криптовалюты;

• возможность надежного и малозаметного для внешнего контроля размещения фиатных активов, находящихся в распоряжении оператора криптовалюты, в различных сегментах финансового рынка России (валютном, долговом, фондовом и т.д.);

• достигнутый долгосрочный консенсус политических и экономических элит в части укрепления основ суверенного, независимого развития Российской Федерации

• политическая поддержка, пусть даже в ряде случаев неявная, со стороны государств, недовольных политическим и экономическим диктатом США;

• наличие в стране одной из лучших мировых школ криптографии и защиты информации;

• наличие развитой аппаратной и сетевой инфраструктуры.

Спрос на подобную новую криптовалюту объективно будет формироваться за счет следующих групп интересантов:

• российские компании и финансовые институты, находящиеся под адресными или секторальными санкциями США, или опасающиеся применения таковых;

• компании и физические лица из стран, находящихся под санкциями США, заинтересованные в сбережении и накоплении средств

• компании и физические лица из широкого круга стран, опасающиеся необоснованных штрафов и налоговых требований со стороны США;

• участники торгового оборота с государствами под санкциями США, исключающего возможность расчетов в американских долларах или с использованием банков, опасающихся вторичных санкций США;

• граждане России и других стран, заинтересованные в диверсификации доступных платежных инструментов в криптовалюте.

Таким образом, речь должна идти о создании ***свободно конвертируемой национальной криптовалюты с механизмом управляемой эмиссии и искусственно поддерживаемым курсовым паритетом к доллару США.***

Требование привязки новой криптовалюты к доллару не предполагает какой-либо прямой или косвенной зависимости от валюты США и нацелено исключительно на использование при работе с ней наиболее широко распространенной и привычной шкалы цен, поскольку международная торговля подавляющим большинством биржевых товаров (commodities) номинируется в настоящее время в американских долларах. Поскольку одним из условий организации эмиссии и обращения криптовалюты должно стать отсутствие «соприкосновений» с долларовой системой как таковой, во избежание ненужных подозрений можно привязать новую криптовалюту к швейцарскому франку, чей курс на протяжении многих лет поддерживается в практическом паритете к американскому доллару.

Категорически неприемлем подход, предполагающий свободное курсообразование новой криптовалюты — хотя в случае успеха, подобного биткойну, он способен принести эмиссионному центру значительную дополнительную прибыль. Международная торговля исторически тяготеет к валютам максимально стабильным, отсюда привязка новой криптовалюты к стабильному «фиату» — важнейшее техническое условие ее функциональности.

Официально поддерживаемая система конвертации между новой криптовалютой и фиатным сектором должна будет осуществляться либо через рублевый рынок, либо через первоначальную («шлюзовую») конвертацию посредством других криптовалют. Это позволит компании-оператору новой криптовалюты и ее официальным партнерам избегать контактов с «токсичными» зонами обращения доллара США и других западных валют. Со временем начнут возникать независимые узлы конвертации (независимые криптобиржи и т.п.), в том числе оперирующие с «токсичными» западными валютами напрямую,— формированию таковых не следует препятствовать, сохраняя при этом должное юридическое дистанцирование.

В качестве аналогов валюты подобного рода можно, с определенными оговорками, привести золотой рубль, применявшийся в СССР

в 1920-е годы, либо так называемый «евродоллар» — расчетную квазивалюту, использовавшуюся банками стран Западной Европы для кредитования торговли с Советским Союзом в конце 1960-х — начале 1970-х гг в условиях установленных Соединенными Штатами ограничений советским банкам на открытие и ведение долларовых корсчетов.

Создание и запуск подобного рода российской криптовалюты в условиях развитых цифровых технологий и наличия в финансовой системе страны достаточных объемов ликвидности в долларах США и евро не представляют системных сложностей и займут непродолжительный срок. Новая криптовалюта сможет использоваться для предоставления депозитарных и расчетных услуг широкому кругу международных субъектов без задействования корреспондентских счетов, открытых в финансовых институтах США и других стран Запада. Первыми бенефецирами новой криптовалюты станут российские структуры, включенные в санкционные списки США, компании стран, находящихся под аналогичными западными рестрикциями, а также компании и банки третьих стран, таких как КНР, Индия, Бразилия, ЮАР и т.д., опасающиеся вторичных санкций США.

В дальнейшем сфера использования новой криптовалюты сможет быть существенно расширена — как по географии, так и в части инвестиционных инструментов. В частности, у нее имеются все основания заместить финансовые институты Швейцарии, Люксембурга и Сингапура в части обеспечения банковской тайны. Как известно, после вступления в силу в 2013 году Федерального закона Швейцарии о международной помощи в налоговых вопросах, оказалось упраздненным различие между понятиями практически непреследуемого «уклонения от уплаты налогов» *(Steuerhinterziehung)* и «налогового обмана» *(Steuerbetrug)* — различие, на котором на протяжении многих лет базировалось исполнение знаменитой «швейцарской банковской тайны» [22]. Аналогичные новации, разрешающие предоставление третьим странам, прежде всего США, информации о любом владельце депозита на основании лишь формального подозрения последнего в «налоговом обмане», введены в Люксембурге, Сингапуре и в значительной части оффшорных юрисдикций, что практически устраняет там понятие банковской тайны.

В сложившихся условиях новая российская криптовалюта, опираясь на экономический потенциал Российской Федерации и её независимую внешнюю политику, подкрепленную дееспособной системой национальной обороны и возможностями для эффективной защиты интересов отечественного бизнеса на международной арене, в полной мере способна на глобальном уровне заместить деградирующие системы сбережений и расчетов, базирующиеся на фиатных валютах стран «западного блока». Соответствующая ниша финансовых услуг на сегодняшний день практически пуста, ее неспособны заполнить ни традиционные криптовалюты (биткойн и аналогичные — по причине сильной курсовой волатильности, Tether и другие “стэйблкойны» — из-за сильной и многоканальной привязке к фиатному долларовому обороту, проектируемая Libra — в силу американской юрисдикции), ни альтернативные доллару США и евро фиатные валюты стран БРИКС, ни традиционные активы, такие как золото, товарные фьючерсы и т.д. С учетом факторов, изложенных в начале настоящего раздела, криптовалюта с необходимыми параметрами может быть создана только в России и Китае. Однако сохраняющаяся высочайшая степень привязанности китайской экономики и финансовой системы к западным рынкам и платежным механизмам делает подобную инициативу со стороны Китая в обозримой перспективе маловероятной.

В отличие от фиатного российского рубля, для которого в силу большого числа факторов характерна заметная волатильность, новая российская криптовалюта должна будет обладать высокой курсовой устойчивостью. Для этого в механизм выпуска и обращения новой криптовалюты с самого начала встраивается ***механизм управляемой эмиссии***, обеспечивающей паритет курса криптовалюты с долларом США (швейцарским франком или иной анкерной фиатной валютой) с диапазоном суточных отклонений не более 0.25%—0.50%.

Паритет должен обеспечиваться автоматическим круглосуточным контролем за курсом с механизмом выброса на обменный рынок фиатной валюты, находящейся в ликвидных резервах, и противоположным ему механизмом вывода излишков криптовалюты в ликвидный резерв. Для этого у финансового института, отвечающего за эмиссию криптовалюты, должен иметься ***критический запас фиатной ликвидности*** (первоначально — в эквиваленте 3-5 млрд. рублей, по мере расширения оборота — до нескольких десятков миллиардов рублей).

Нетрудно видеть, что если все средства в фиатной валюте, выручаемые при продаже криптовалюты, будет находиться в ликвидном резерве, то у оператора всегда будет иметься гарантированная возможность обеспечить для эмитированного объема криптовалюты обратный выкуп. Если данный ликвидный резерв будет еще в достаточной степени диверсифицирован с целью устранения курсовых рисков, то обратный выкуп сможет быть обеспечен по широкой корзине фиатных валют. Если же оператор сможет привлечь дополнительную ликвидность, то он, по сути дела, обеспечит себе инвестиционный рейтинг и со временем сумеет функционировать в качестве полноценного банка, специализирующегося на обслуживании специфического актива в виде криптовалюты.

Привлечение ликвидности за счет продажи криптовалюты целесообразно мотивировать через получение владельцами счетов в новой криптовалюте процентного дохода по средневзвешенному остатку средств с уровнем на 1.0-1.5% выше ставки доходности по долларовым вложениям соответствующего уровня риска и сроков (в случае депозитных счетов). Учитывая тот факт, что выплата процентного дохода будет осуществляться в зоне доходных ставок инструментов, связанных с фиатными валютами стран западного блока, для которых сегодня характерен крайне низкий уровень, вплоть до отрицательной доходности, бюджет криптовалютного оператора для формирования процентного дохода сравнительно легко может быть сформирован из доходов от транзакционных и конвертационных комиссий, а также за счет краткосрочного размещения резервов на межбанковском рынке. Как известно, в настоящее время на межбанковском рынке России заметна нехватка инструментов кредитования на срок более 1-2 дней, а ставка по последним (в долларах США) составляет на середину лета 2019 г 3.4% годовых [23].

С целью снижения риска недружественных действий финансовых институтов стран западного блока по отношению к новой криптовалюте, особенно на первых этапах ее функционирования,— например, её скоординированной продажи с целью обрушения курса,— в первые годы желательно поддерживать определенный уровень размещения криптовалюты на счетах заведомо дружественных держателей — например, госбанков и госкорпораций РФ.

Другим механизмом для снижения волатильности и блокирования спекулятивных атак может стать раздельное ведение счетов для оперативных (торговых) расчетов и счетов депозитных (инвестиционных). Для последних имеется смысл отказаться от полной анонимности в терминах классического блокчейнаи использовать технологии защищенного реестра: оператор криптовалюты, осуществляющий работу по гарантированию устойчивости ее курса, будет готов предоставлять долгосрочные гарантии в виде покрытия выплат другими валютами или золотом только при наличии специального соглашения, в рамках которого личность инвестора должна быть раскрыта. В этой связи необходимо разработать криптомеханизм, гарантирующий хранение соответствующих данных на территории России с многоуровневой защитой.

На сегодняшний день в мире сформировались оптимальные условия для запуска новой российской криптовалюты, обладающей, как было показано, потенциально мощными и действующими продолжительное время факторами конкурентоспособности. При этом в России имеются как необходимые цифровые технологии, так и внутренние источники для формирования стартового капитала проекта.

При создании и в процессе организации работы компании-оператора новой российской криптовалюты должны быть на максимально возможном уровне обеспечены возможности

для справедливого арбитража, а также механизмы выполнения признаваемых Российской Федерацией рекомендаций FATF по борьбе с отмыванием денег, финансированием международного терроризма и т.д.

Оптимальный объем эмиссии первого этапа создания новой российской криптовалюты, при котором ее устойчивость определяется наличием инерции со стороны большого числа держателей расчетных счетов и инвесторов, оценивается в эквиваленте до 50 млрд. долларов США. Очевидно, что при обращении к новому инструменту со стороны хотя бы части крупных отечественных экспортеров, включая Газпром, Роснефть и Росвооружение, — это вполне реальная цифра.

В среднесрочной перспективе, по мере упрочения международного статуса новой российской криптовалюты с доведением среднего объема эмиссии до эквивалента 100-150 млрд. долларов США, новая российская криптовалюта укрепится в первой пятерке мировых криптовалют. С точки зрения внутреннего финансового рынка, при достижении новой криптовалютой вышеназванного уровня капитализации, эквивалентного 50% денежной базы РФ в широком определении, сформируются условия для формирования у российского рубля фундаментальных основ свободной конвертируемости. Достаточно привести в качестве примера спрос на фиатные рубли, поддерживаемый деятельностью оператора криптовалюты, в качестве эффективного противовеса попыткам финансовых спекулянтов «сыграть» на длительное понижение его курса.

Со временем это сделает фиатный рубль менее зависимым от конвертаций в рамках экспортно-импортных операций и повысит егоинвестиционную оценку с позиций внутренних и зарубежных инвесторов, что позволит приступить к снижению ключевой ставки в России до уровня ведущих свободно конвертируемых валют.

В долгосрочной перспективе, предполагающей, что новая российская криптовалюта для какой-то части государств, корпораций и частных лиц заменит доллар США либо в качестве безопасной альтернативы внешнеторговых операций и накопления, либо в качестве инструмента диверсификации, показатель ее капитализации сможет увеличиться до эквивалента 500 млрд. долларов США и выше. Подобный объем превысит, очевидно, величину денежной базы РФ, что будет означать полномасштабный выход рубля из обеспечения преимущественно внутристранового обращения в систему международных расчетов.

Таким образом, проектируемая российская криптовалюта, востребованная в силу сложившегося баланса геополитических отношений и опирающаяся в своем генезисе на отечественную финансовую систему и российский рубль, сыграет положительную роль в обеспечении стабильности национальной денежной системы и сможет способствовать последовательному укреплению фиатного рубля с перспективой превращения его в полноценную валюту международных расчетов и одну из мировых резервных валют. При этом роль и значение проектируемой криптовалюты будут сохраняться по меньшей мере до тех пор, пока мировые отношения не станут свободными от односторонних санкций и ограничений, нарушающих международное право.

СПИСОК ЛИТЕРАТУРЫ

1. Капитализация криптовалют. URL: https://tehnoobzor.com/cryptolife/bitcoin/2531-kapitalizaciya-bitkoina-na-segodnya.html

2. Графики рыночной капитализации криптовалют». URL: https://ru.tradingview.com/markets/cryptocurrencies/global-charts

3. М.В.Петров Мировая финансовая система: долгий путь к многополярности/ Финансовый журнал, №2, 2018

4. Т.К.Блохина Рынок деривативов: мировые тренды и перспективы развития / Вестник РУДН, серия «Экономика», №1, 2015
5. Ю.А.Гроссман Системные риски и подходы к международному регулированию финансовых рынков, Глобальные рынки и финансовый инжиниринг. — 2016. — Т. 3. — № 2. — С. 95–114.
6. Денежная масса M1 по странам. Статистические данные. URL: https://take-profit.org/statistics/money-supply-m1/
7. Е.Делюкин. Что известно о криптовалюте Libra. URL: https://vc.ru/finance/71909-chto-izvestno-o-kriptovalyute-facebook-libra-i-zachem-ona-nuzhna-marku-cukerbergu
8. Вещевой рынок и биткоины: как китайцы выводят прибыль из России // Новые Известия, 15.03.2018
9. ICO Форум: Кто и как покупает криптовалюту в Москве. URL: https://icoforum.net/threads/kto-i-kak-pokupaet-kriptovaljutu-v-moskve-sberkoin-kitajcy-s-sadovoda-xomjachki-investory-i-t-d.131/
10. К.Хилл "Задушить биткойн: как в Китае борются с криптовалютой» // Форбс, 21.01.2014 11. Anna Baydakova: Millions in Crypto Is Crossing the Russia-China Border Daily. There, Tether Is King.URL: https://www.coindesk.com/tether-usdt-russia-china-importers
12. Д.Носова, И.Чумаченко «Китайская криптограмота: как стать мировым лидером блокчейна, запрещая криптовалюты» // Форбс, 07.06.2019
13. Пресс-релиз ММВБ от 02.08.2019 . URL: https://www.moex.com/n24546/?nt=106
14. Курс рубля до конца года — факторы поддержки и риски// Бюллетень ФИНАМ от 16.07.2019. URL:https://www.finam.ru/analysis/forecasts/kurs-rublya-do-konca-goda-faktory-podderzhki-i-riski-20190716-184731/
15. Технический обзор криптовалюты Petro. URL: https://crypta.guru/kriptovalyuty/kriptovalyuta-petro
16. USA Federal Register Vol. 83, No. 55 Wednesday, March 21, 2018
17. И.Тимофеев, Специальный доклад Международного дискуссионного клуба «Валдай» для Петербургского международного экономического форума. Июнь 2019. URL: http://ru.valdaiclub.com/files/27298
18. USA Internal Revenue Service // Foreign Earned Income Exclusion. URL: https://www.irs.gov/individuals/international-taxpayers/foreign-earned-income-exclusion
19. Чиновники США и мэр Лондона обвиняют друг друга в неуплате налогов // РИДУС, 21 ноября 2014. URL: https://www.ridus.ru/news/172441.html
20. Д.Токарев Stable Coins — самые стабильные криптовалюты // BitCryptoNews — 25.06.2018. URL: https://bitcryptonews.ru/blogs/cryptocurrency/stable-coins-samyie-stabilnyie-kriptovalyutyi
21. Теханализ криптовалют по рыночной капитализаци// CoinMarketCap . URL: https://coinmarketcap.com/ru/
22. Соотношение национальных и международных норм о противодействии злоупотреблению правом в законодательстве и судебной практике Швейцари // Налоговед, 03.03.2013. URL: https://e.nalogoved.ru/article.aspx?aid=308545
23. ЦБ РФ, Показатели ставок межбанковского рынка с 01.08.2000. URL: https://www.cbr.ru/hd_base/mkr/mkr_base/

Международный консенсус как развитие парадигмы консенсуса

A. Domashev, A. Shcherbakov

International consensus as developing of the consensus paradigm

Abstract. *The article is devoted to the most important problem of distributed registries - the legitimacy of the consensus procedure. Based on a review of the history of the development of distributed registries and a comparative analysis of various projects using the blockchain, the situation is illustrated and substantiated that in order to create completely legitimate procedures for international interaction in the field of distributed storage and processing of data, it is necessary to move to the paradigm of international consensus when the subjects of the consensual procedure become subjects of international law or their authorized organization.*

The article considers not only the technical aspects of building and operating blockchain platforms, but also one of the fundamental moments in the implementation of such projects - what is the subject of consensus in various practical implementations and how does this affect the technical characteristics of the target platforms? And also - what should be the subject of consensus for the target platform to have real value from the point of view of international law?

Keywords: *blockchain, distributed registry, international consensus, distributed storage, cryptocurrency, trusted international platform, Distributed Ledger Technology (DLT), consensus, cross-border retail payments, Central Banks Digital Currencies (CBDC).*

Алексей Домашев[1],
Андрей Щербаков,
д.т.н., проф., главный научный сотрудник РАН,
начальник Центра развития криптовалют
и цифровых финансовых активов (ЦРКЦФА)[2]
[1]Центр развития криптовалют и цифровых
финансовых активов ВИНИТИ
e-mail: a.domashev@c3da.org
[2]Центр развития криптовалют
и цифровых финансовых активов ВИНИТИ
e-mail: a.shcherbakov@c3da.org, x509@ras.ru

Аннотация. *Статья посвящена важнейшей проблеме распределенных реестров - легитимности процедуры консенсуса. На основе рассмотрения истории развития распределенных реестров и сравнительного анализа различных проектов, использующих блокчейн, проиллюстрировано и обосновано положение о том, что для создания полностью легитимных процедур международного взаимодействия в поле распределенного хранения и обработки данных необходимо перейти к парадигме международного консенсуса, когда субъектами консенсуальной процедуры становятся субъекты международного права или уполномоченные ими органы.*

В статье рассмотрены не только технические аспекты построения и эксплуатации блокчейн-платформ, но и один из принципиальных моментов реализации таких проектов - что является субъектом консенсуса в различных практических реализациях и как это влияет на технические характеристики целевых платформ? А также - что должно быть субъектом консенсуса, чтобы целевая платформа обладала реальным значением с точки зрения международного права?

Ключевые слова: *распределенный реестр, международный консенсус, распределенное хранение, криптовалюта, доверенная международная платформа, трансграничные розничные платежи, цифровые валюты центральных банков.*

ВВЕДЕНИЕ

Понятие блокчейн впервые стало широко известно благодаря криптовалюте Bitcoin [1]. Блокчейн может быть определен как неизменяемый (immutable) реестр для записи транзакций, поддерживаемый в рамках распределенной сети, участники которой в различной степени не доверяют друг другу. Каждый участник сети поддерживают свою собственную копию реестра. С целью валидации транзакций все участники сети поддерживают соответствующий протокол консенсуса. Валидные транзакции объединяются в блоки, которые связываются друг с другом посредством цепочки хеш-функций. Такой процесс упорядочивает транзакции и поддерживает сетевой распределенный реестр в согласованном состоянии (consistency).

Классифицировать блокчейн-платформы можно по различным признакам. Для нас принципиальным является управление доступом для участников сети. В инклюзивных (permissionless) блокчейн-платформах любой может стать участником сети и для этого не нужно проходить процесс идентификации. Инклюзивными блокчейн-платформами

являются в первую очередь сети большинства криптовалют, которые используют протокол консенсуса, базирующийся на концепциях «proof of work» (PoW) или «proof of stake» (PoS) и опираются на финансовое стимулирование участников консенсуса.

В противоположность этому участники сетей эксклюзивных (permissioned) блокчейн-платформ проходят обязательную процедуру идентификации. Эксклюзивные блокчейн-платформы предоставляют возможность организовывать взаимодействие в группах, где участники не полностью доверяют друг другу. Такие блокчейн-платформы подходят для организации межкорпоративного взаимодействия, где все участники бизнес процессов хорошо известны. Благодаря тому, что в эксклюзивных блокчейн-платформах все участники идентифицируются, сети, построенные по данному принципу, могут использовать различные практические реализации Византийского (Practical Byzantine Fault Tolerance- pBFT) консенсуса. В качестве примеров эксклюзивных блокчейн-платформ можно привести решения на основе открытого проекта Hyperledger Fabric [2] [3] или проект криптовалюты Libra [4], реализуемый группой компаний во главе с Facebook [5][1].

Большинство как инклюзивных так и эксклюзивных блокчейн-платформ имеет возможность выполнять произвольную логику транзакции в форме смарт-контрактов (smart-contract) или чейнкода (chaincode). Термин смарт-контракт получил распространение благодаря его использованию в блокчейн-платформе криптовалюты Ethereum [6], в то время как термин чейнкод используется в платформах, построенных на основе проекта Hyperledger Fabric. Функции смарт-контрактов представляют собой доверенные распределенные приложения, безопасность которых базируется на функциональности блокчейн-платформы и консенсусе среди участников сети.

СУБЪЕКТЫ КОНСЕНСУСА

Кто же является субъектами консенсуса в существующих и будущих блокчейн-платформах? Этот вопрос обозначен как целевой для данной статьи. Давайте сформулируем его более точно. Какими субъектами права являются участники консенсуса в существующих вариантах блокчейн-платформ и какие субъекты права до настоящего времени не становились участниками консенсуса? Ответ на первую часть вопроса нам кажется очевидным: в настоящее время участниками консенсусов являются физические и юридические лица[2].

Концепция инклюзивных блокчейн-платформ, таких например, как две самых распространенных криптовалюты Bitcoin [1] и Ethereum [6], постулирует, что любое физическое лицо может стать участником консенсуса, никто не может ограничить его в этом праве. Для этого нужно владеть определенными техническими возможностями, позволяющими производить вычисления хеш-функций с необходимым для реального участия в консенсусе PoW хешрейтом (hashrate). Юридическое лицо тоже может стать таким участником, но в условиях отсутствия идентификации это не имеет никакого правового значения и в данном случае речь идет по сути о физическом лице (или группе лиц), которое владеет секретным ключом подписи.

На практике состав участников консенсуса и Bitcoin и Ethereum существенно отличается от теоретических концепций. На примере развития сети Bitcoin можно увидеть, что физические лица были реальными субъектами консенсуса только в самом начале функционирования сети. В настоящее время для того, чтобы достичь приемлемой вероятности вычисления целевого значения хеш-функции за разумный период времени, необходима концентрация в одном кластере огромных вычислительных мощностей. Если проанализировать данные сети Bitcoin за последний год [7], то можно увидеть, что четыре самых мощных пула ответственны за вычисление более 50% блоков, а семь пулов – за более чем 76% блоков.

Если же взглянуть еще немного глубже, то мы увидим, что двумя первыми пулами

[1] На момент выхода статьи группа компаний, участвующих в проекте, может претерпеть изменения. Компания PayPal уже объявила о выходе из Libra Foundation [20]. Другие участники финансового блока компаний также пересматривают свое участие в проекте [19].

[2] Авторы хотели бы предупредить, что не являются специалистами в области юриспруденции, а здесь и далее рассуждают на эти темы как разумные технические специалисты.

BTC.com и AntPool владеет одна и та же китайская компания Bitmain Technology [8]. Таким образом, за более, чем 30% вычисленных блоков за последний год ответственно только одно юридическое лицо. В целом же по разным оценкам до 80 % майнинговых мощностей сети Bitcoin приходится на КНР. Правда, отношение китайских властей к этому пока сугубо отрицательное и, что будет происходить с майнерами из Поднебесной, не ясно.

В противоположность инклюзивным сетям концепция эксклюзивных блокчейн платформ, как уже говорилось, предполагает строгое регулирование доступа участников консенсуса. На практике очевидно, что каждое конкретное решение на основе такой платформы определяет участников консенсуса, исходя из конкретной бизнес-логики проекта.

В подобных межкорпоративных платформах субъектами консенсуса выступают сами корпорации, общественные или правительственные организации, участвующие в проекте. В принципе ничего в концепции эксклюзивных блокчейн-платформ не противоречит тому, чтобы участником консенсуса стало физическое лицо, прошедшее соответствующую идентификацию, но в большинстве случаев участниками консенсуса являются юридические лица.

СУБЪЕКТЫ МЕЖДУНАРОДНОГО ПРАВА

Так что же такое «международный консенсус»- термин, который мы вынесли в заголовок статьи?

О реальной значимости и перспективах использования технологии блокчейна до сих пор идут споры, есть как горячие сторонники так и не менее пылкие противники. Даже само понятие блокчейн до настоящего времени однозначно не определено. Например, многие апологеты криптовалютных платформ считают, что только такие инклюзивные блокчейн-платформы могут считаться настоящим блокчейном.

Многие специалисты, в том числе авторы данной статьи, сходятся во мнении, что именно как основа для международных проектов комплексная идеология блокчейн способна быть не просто удобным инструментом для бизнес процессов, но реализовать абсолютно новую концепцию международной доверенной платформы распределенных приложений.

Эта мысль не нова, но давайте посмотрим текущее положение дел и оценим, являются ли существующие и проектируемые международные платформы распределенных приложений реально доверенными?

Первым практическим примером такой платформы можно считать сеть криптовалюты Ethereum, поскольку сценарии, реализуемые в транзакции Bitcoin, нельзя классифицировать как приложения. Как и в случае с платформой Bitcoin, первоначальная концепция, что субъектами консенсуса может стать любое физическое лицо выродилась в то, что субъектами консенсуса является узкий круг огромных майнинговых пулов. Данные за последний год [9] показывают, что четыре крупнейших пула ответственны за вычисление более 70% блоков в блокчейн-платформе Ethereum.

Одним из последних резонансных примеров эксклюзивной блокчейн-платформы, которая обладает возможностью исполнение распределенных приложений, является платформа криптовалюты Libra [4][3]. Как уже отмечалось, Libra в настоящее время разрабатывается группой компаний во главе с Facebook [5]. Правда в настоящее время консенсус тоже получается довольно однобоким. Из 28 официальных участников проекта 21 является американскими компаниями.

Мы привели примеры этих двух международных платформ распределенных приложений, чтобы подчеркнуть очевидную мысль. Для того чтобы платформа распределенных приложений была реально международной и доверенной субъектами консенсуса, в этой платформе не могут быть четыре или десять майнинговых пулов, часто не являющихся даже юридическими лицами или группой из 28 или 100 частных компаний, большинство из которых являются акционерными обществами и выражают финансовые интересы своих акционеров. Ни группа правовых субъектов, сформировавшихся в результате экономической конкуренции, ни группа,

[3] Более точный термин для Libra- это стейблкоин (stablecoin) — общее название криптовалют, которые привязаны к запасам реальных активов (валют, драгоценных металлов или других товаров), которые участники вносят в общий фонд.

сформировавшаяся в результате корпоративных переговоров, не может быть реальной основой доверенной международной платформы.

Группа, которая может стать основой такой платформы не должна формироваться, эта группа уже есть. Она уже сформировалась в результате нескольких тысяч лет развития цивилизации. Для того чтобы идентифицировать эту группу, мы должны переместиться в правовом поле от физических и юридических лиц к субъектам международного права. Мы имеем в виду прежде всего государства.

Таким образом, переходя к государствам или их уполномоченным органам, мы имеем 193 субъекта консенсуса и вряд ли кто-либо сможет утверждать, что эта группа сформирована не по объективному принципу[4].

По нашему мнению именно государства должны взять на себя ответственность за реализацию международной платформы распределенных приложений. Построение информационной инфраструктуры, обеспечение выделенных скоростных каналов передачи данных между узлами консенсуса, обеспечение безопасности хранения данных блокчейн-платформы должно быть зоной ответственности государственных структур. Построенная по таким принципам сеть изначально будет иметь доверие и поддержку со стороны исполнительных, законодательных органов и центральных банков государств участников.

МЕЖДУНАРОДНЫЙ КОНСЕНСУС В СФЕРЕ ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Один из проектов, который, по нашему мнению, является серьезным кандидатом на реализацию в рамках международного консенсуса, является модернизация платформы трансграничных розничных платежей (cross-border retail payments).

В настоящее время международные финансовые институты исследуют различные подходы к решению этого вопроса. Для подробного ознакомления с текущим положением дел по этой теме мы рекомендуем нашим читателям обратиться к отчету Банка Международных Расчетов [10][5].

По сути речь идет о модернизации бэкенда современной системы трансграничных розничных платежей, ядром которого является сеть передачи электронных сообщений SWIFT. Платформа на основе технологии распределенного реестра является идеальным кандидатом на построение подобной современной системы передачи сообщений. Очевидно, что с технологической точки зрения эту задачу компания SWIFT абсолютно компетентна решить самостоятельно и, что совершенно не удивительно, она это делает [11].

Но здесь идет речь о новой парадигме построения платформ распределенного реестра. Именно в подобных системообразующих проектах применимы выводы о необходимости государственным институтам стать субъектами консенсуса. Модернизация системы трансграничных розничных платежей на основе принципов международного консенсуса позволит реализовать решение, которое будет обладать не только новыми техническим характеристиками, но и станет абсолютно устойчивой к попыткам, если можно так выразится, «политического» воздействия.

И если в вопросе новой платформы трансграничных розничных платежей мы говорим о модернизации существующей системы на основе новых принципов, то в проекте выпуска цифровых валют центральных банков (Central Banks Digital Currencies – CBDC) речь идет о реализации абсолютно новой концепции выпуска и обращения национальных валют. Для подробного ознакомления с текущим положением дел по этой теме мы также рекомендуем нашим читателям обратиться к отчету Банка Международных Расчетов [12].

В данном случае CBDC не является единственным проектом. В настоящее время целый ряд центральных банков, в том числе и ЦБ РФ [13], рассматривают возможность эмиссии и обращении национальных валют в цифровом

[4] Как известно, Ватикан является особым субъектом международного права. Надо полагать, что участие Святого Престола могло бы предать такому консенсусу особый вес.

[5] Здесь и далее при обсуждении различных финансовых проектов мы ссылаемся на отчеты Банка Международных Расчетов (Bank of International Settlements (BIS)) — международной финансовой организации, в функции которой входит содействие сотрудничеству между центральными банками, кроме этого BIS является центром экономических и денежно-кредитных исследований и уделяет большое внимание исследованию перспектив использования технологий распределенного реестра в финансовых операциях.

виде. Формы эмиссии и обращение такой валюты внутри стран могут быть разнообразными, в том числе с использованием блокчейн-платформ. Для международного обращения цифровых валют, очевидно, необходима общая доверенная международная платформа, и платформа международного консенсуса как нельзя лучше подходит на эту роль.[6]

ПИЛОТНЫЙ ПРОЕКТ ДЛЯ ПОРТАЛОВ ОТКРЫТЫХ ДАННЫХ

Будем реалистами, проекты реализации международной платежной системы и цифровых валют центральных банков крайне амбициозны и сложны. Поэтому в качестве «пилотного» проекта для реализации на платформе международного консенсуса необходимо выбрать что-либо менее «политически нагруженное», но при этом то, что может иметь реальное практическое значение. В качестве такой темы можно предложить проект международного электронного нотариата и в качестве первых клиентов этого проекта порталы открытых данных Европы и России: EU Open Data Portal [14] и Портал открытых данных [15].

Для порталов открытых данных, таких как EU Open Data Portal [14] или Портал открытых данных [15], в рамках международного консенсуса предлагается реализовать проект электронного нотариата, реализующего функциональность подтверждения подлинности, проставления временных меток и возможно другого полезного функционала.

Подобные проекты на основе блокчейн-платформ в глобальном масштабе реализуются сейчас с использованием функциональности сетей Bitcoin, Ethereum и ряда других криптовалют. Таким проектом является, например, Stampery [16][7]. В данном и других подобных проектах целевая функциональность подтверждения подлинности реализуется путем размещения значения хеш-функции документа или значения групповой хеш-функции многих документов в транзакции соответствующей криптовалютной сети [18].

Реализация проектов электронного нотариата на основе криптовалютных сетей выявила ряд серьезных технических проблем, связанных с базовыми принципами их функционирования. Эти проблемы и пути их частичного решения хорошо изложены в [18]. Основная техническая проблема - это очевидно большое время прохождение транзакции.

На поверхности лежит и главная юридическая проблема. Это отсутствие признанного юридического статуса этих сетей и, как следствие, отсутствие этого статуса у проектов, реализованных на их основе. Реализация проекта электронного нотариата на основе международного консенсуса даст такому проекту необходимое юридическое признание.

ЗАКЛЮЧЕНИЕ

Авторы вполне отдают себе отчет в масштабности и сложности реализации изложенной ими концепции международного консенсуса.

Если детализировать наше видение эволюции проекта международного консенсуса, то можно предположить, что первично это может быть пилотный проект, включающий Россию, страны ШОС и ряд европейских стран.

При этом необходимо заключение соответствующих межправительственных соглашений и определение статуса и полномочий участника консенсуса внутри страны. Целесообразно, чтобы это была независимая техническая организация, аналогичная по функционалу комитетам по стандартизации, обеспечивающая функционирование соответствующих аппаратных и программных платформ. В дальнейшем, на основе регламентаций более частного характера (например, о передаче таможенной или финансовой информации), согласованных таможнями или банками государств-участников, можно расширять функционал консенсуса.

Помимо организационно-правовых аспектов платформы, участникам предстоит решить и большое количество технических проблем.

[6] Недавно Августин Карстенс (Augustín Carstens), генеральный менеджер Банка Международных Расчетов, в интервью газете «Financial Times» [21] сказал по поводу выпуска центральными банками CBDC: «И возможно, что это произойдет быстрее, чем мы думали, есть рынок и нам необходимо иметь возможность выпуска цифровых валют центральных банков» (Перевод авторов). Интересно, что эти слова были сказаны вскоре после того как Facebook публично заявил о планах выпуска криптовалюты Libra.

[7] Stampery достиг достаточно серьезного уровня практического внедрения. Достаточно отметить, что представители компании Microsoft создали Add-In для Microsoft Outlook, позволяющий вызывать через REST API Node.js сервера Stampery, расположенный в Microsoft Azure [17].

Детальные характеристики предлагаемой сети могут быть определены только в результате практической работы. Учитывая, что участниками данного консенсуса будут государства, решения для многих, на первый взгляд, технических вопросов потребует определенно неординарных решений. Результат, по нашему мнению, может быть очень многообещающим, как в финансово-техническом, так и в политическом аспекте.

СПИСОК ЛИТЕРАТУРЫ

1. Bitcoin Project. [В Интернете] https://bitcoin.org.
2. The Linux Foundation. Hyperledger Fabric. [В Интернете] https://www.hyperledger.org/projects/fabric.
3. —. Hyperledger Fabric- Industries. [В Интернете] https://www.hyperledger.org/resources/industries.
4. Libra Association. [В Интернете] https://libra.org.
5. —. Founding Members. [В Интернете] https://libra.org/en-US/association/#founding_members.
6. Ethereum Foundation. [В Интернете] https://ethereum.org.
7. Bitmain Technology. Pool Distribution. btc.com. [В Интернете] https://btc.com/stats/pool?pool_mode=year.
8. —. [В Интернете] https://www.bitmain.com/.
9. —. Mining Insights. Ethereum Explorer. [В Интернете] https://eth.btc.com/miningstats.
10. Bank for International Settlements. Cross-border retail payments. [В Интернете] 2018 г. https://www.bis.org/cpmi/publ/d173.htm. ISBN 978-92-9259-134-2.
11. SWIFT. Distributed Ledger Technology (DLT). [В Интернете] https://www.swift.com/your-needs/industry-themes/distributed-ledger-technology-dlt_#topic-tabs-menu.
12. Bank for International Settlements. Central bank digital currencies. [В Интернете] 2018 г. https://www.bis.org/cpmi/publ/d174.htm. ISBN 978-92-9259-143-4.
13. Российская газета. Куда переведут наличные- Банк России задумался о создании цифровой валюты. Интернет-портал «Российской газеты». [В Интернете] 16 Июнь 2019 г. https://rg.ru/2019/06/16/bank-rossii-zadumalsia-o-sozdanii-cifrovoj-valiuty.html.
14. Publications Office of the EU. EU Open Data Portal. [В Интернете] https://data.europa.eu/euodp/en/home.
15. Минэкономразвития России. Портал открытых данных Российской Федерации. [В Интернете] https://data.gov.ru/.
16. Stampery. [В Интернете] https://stampery.com/.
17. Компания «Microsoft». Stampery Blockchain Add-in for Microsoft Office. Developer Blog. [В Интернете] https://www.microsoft.com/developerblog/2017/04/10/stampery-blockchain-add-microsoft-office/.
18. de Pedro Crespo, Adán Sánchez и Cuende García, Luis Ivan. Stampery BlockchainTimestamping Architecture (BTA). Stampery. [В Интернете] https://s3.amazonaws.com/stampery-cdn/docs/Stampery-BTA-v6-whitepaper.pdf.
19. Andriotis, AnnaMaria и Rudegeair, Peter. Visa, Mastercard, Others Reconsider Involvement in Facebook's Libra Network. The Wall Street Journal. [В Интернете] 2 Октябрь 2019 г. https://www.wsj.com/articles/visa-mastercard-others-reconsider-involvement-in-facebook-s-libra-network-11569967023.
20. Rudegeair, Peter. PayPal Drops Out of Facebook's Libra Payments Network. The Wall Street Journal. [В Интернете] 4 Октябрь 2019 г. https://www.wsj.com/articles/paypal-drops-out-of-facebooks-libra-payments-network-11570218306.
21. Jones, Claire. Central bank plans to create digital currencies receive backing. Financial Times. [В Интернете] 30 Июнь 2019 г. https://www.ft.com/content/428a0b20-99b0-11e9-9573-ee5cbb98ed36.

Центр развития криптовалют и цифровых финансовых активов ВИНИТИ РАН как инструмент решения научно-методических проблем в сфере цифровой трансформации

А.Ю. Щербаков,
д.т.н., проф., главный научный сотрудник РАН,
начальник Центра развития криптовалют
и цифровых финансовых активов (ЦРКЦФА)[1]
[1]*Центр развития криптовалют и цифровых*
финансовых активов ВИНИТИ
E-mail: a.shcherbakov@c3da.org

Министерство науки РФ и Российская Академия наук большое внимание уделяют фундаментальным исследованиям в области современных глобальных стратегий и технологий. В связи с этим в рамках Всероссийского института научной и технической информации (ВИНИТИ) РАН в апреле 2018 г. был создан Центр развития криптовалют и цифровых финансовых активов (ЦРКЦФА).

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.

За более, чем год работы в рамках Центра был собран коллектив ведущих российских ученых и практиков, занимающихся решением актуальных теоретических и практических проблем цифровой экономики, осуществлением, организацией и координированием научных работ, в том числе и с международным участием. В настоящее время в ЦРКЦФА работают два доктора и два кандидата наук. Ведется работа и в области подготовки научных кадров и поддержки молодых ученых – к работе привлечен один аспирант, тема диссертации соответствует основным направлениям исследований Центра.

Основная миссия и задача Центра- создание благоприятной научно-образовательной и научно-информационной среды в области цифровой экономики и цифровой трансформации общества, 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 соответствии с перечнем стратегических направлений, определенных в программе «Цифровая экономика Российской Федерации» (большие данные, распределенные реестры, искусственный интеллект, квантовые технологии).

Стратегическими партнерами Центра являются Российская ассоциация криптоиндустрии и блокчейна (РАКИБ), Российский государственный университет нефти и газа имени И. М. Губкина, Сберегательный банк РФ, группа компаний «Инфовотч». В международной научной кооперации Центр является партнером ассоциации разработчиков блокчейна HyperLedger.

С участием Центра в течение года выполнен целый ряд важных практических проектов, в частности, разработан первый доверенный российский распределенный реестр «Купол» (в настоящее время согласовано техническое задание на сертификацию в ФСБ РФ), разработана платформа защищенных токенов нового поколения (находится на регистрации в Минкомсвязи РФ), представлена архитектура национального цифрового актива.

Центр сопровождает процесс сертификации платформы «Мастерчейн» в кооперации со специалистами Сбербанка РФ. ЦРКЦФА опубликовал более 10 уникальных работ в области распределенных реестров и цифровых активов, получивших международное признание.

Для реализации задач и миссии ЦРКЦФА создан Координационный совет, включающий авторитетных руководителей заинтересованных ведомств и организаций. Желание принять участие в работе Координационного совета высказали члены Совета Федерации и Государственной Думы РФ, заместитель председателя Сбербанка, руководители государственной финансовой корпорации Внешэкономбанк, ответственные руководители Росгвардии, МЧС и Министерства обороны РФ.

Министерством науки утверждено и финансируется Государственное задание, в соответствии с которыми ЦРКЦФА выполняет научно-изыскательские работы 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: 0003-2019-007, данные работы включены также и в план работ ВИНИТИ РАН.

Говоря о стратегических перспективах работы Центра, необходимо заметить, что сейчас полным ходом идет процесс «цифровой трансформации» российской экономики, формирования доверенной и корректной цифровой среды разработки и применения цифровых национальных технологий. Сегодня в этой области остро ощущается «давление» иностранных цифровых и криптовалютных технологий, в том числе технологии оборота токенов, цифровых активов, технологии распределенного хранения данных, включая распределенные реестры (блокчейн). Кроме того, регистрируются активные попытки создания на базе технологий распределенного реестра и разного рода криптовалют реальных систем, обеспечивающих решение широкого спектра задач. Вместе с тем, как показал ряд исследований, несмотря на заявленные качества, реализованные системы не обладают свойствами информационной безопасности и доверенности.

Неразумное копирование западных технологий, особенно в условиях создания «цифровой экономики», может иметь весьма пагубное влияние на технологическую безопасность и независимость России, в том числе на устойчивость российского бизнеса как на национальном уровне, так и на международной арене.

В связи с этим необходимо создание технологической платформы для цифровой трансформации, определенной государственным заданием и отвечающей следующим фундаментальным требованиям:

- доверенность (универсальная открытая структура и открытый программный код);
- национальная криптографическая локализация (использование национальных стандартов и готовность к получению соответствующих сертификатов у регуляторов);
- универсальность (возможность использования как в технологии цифровых активов, так и в работе с товарами и продукцией, а также для обеспечения государственного заказа и закупок).

Активное изучение технологий распределенного реестра отечественными специалистами привели к появлению собственных наработок. После обсуждения заделов естественным образом были объединены усилия академической и вузовской науки, поддержанные ведущими технологическими компаниями. Текущая работа ЦРКЦФА является результатом не только теоретических проработок, но и их прототипирования и практической реализации, что, в случае соответствующей научной и финансовой поддержки, создает возможность реализации оригинальных отечественных информационных технологий, способных положительно повлиять на развитие цифровой экономики в Российской Федерации.

Искусственный интеллект как феномен имитации

A.Ryazanova, A.Shcherbakov

Artificial intelligence as a phenomenon of imitation

Abstract. *Based on the analysis of the concepts of mind and intelligence in their philosophical and historical evolution, the thesis that modern artificial intelligence projects are an attempt to imitate human thinking procedures, moreover, on an imitation basis, in particular on neural networks, is illustrated. Using the subject-object model of a computer system, which can be extrapolated to the processes of cognition and modeling of processes and architectures of both intelligent and intelligent systems, an approach is proposed to overcome the dialectic impasse in artificial intelligence projects - a transition to a more general model of thinking that is not related to anthropic principles, and focused on the flow of information and their analysis, as well as on the implementation of the procedure for generating new subjects, as a creative component of artificial intelligence.*

Keywords: *artificial intelligence, artificial mind, subject-object model, information flows, imitation of thought processes.*

А.А. Рязанова*[1]*,
***А.Ю.Щербаков*[2]**
[1]Заместитель начальника Центра
по международной деятельности,
Email: a.ryazanova@c3da.org
[2]Начальник Центра,
Центр развития криптовалют и цифровых
финансовых активов ВИНИТИ РАН
E-mail: a.shcherbakov@c3da.org

«Искусственный интеллект – это бестелесный и безличный дух, живущий в построенной человеком среде, - код, свободно копирующий и переписывающий свои секвенции и большую часть времени не сосредоточенный нигде конкретно. Это ничто и одновременно нечто, опирающееся на волну и поток, перемещающееся со скоростью света сквозь схлопывающееся в точку пространство…» (В. Пелевин, «iPhuck-10»)

Аннотация. *На основе анализа понятий разума и интеллекта в их философско-исторической эволюции проиллюстрирован тезис о том, что современные проекты искусственного интеллекта являются попыткой имитации человеческих процедур мышления, причем на имитационной базе, в частности на нейросетях. С использованием субъектно-объектной модели компьютерной системы, которая может быть экстраполирована и на процессы познания и моделирование процессов и архитектур как интеллектуальных, так и разумных систем, предложен подход преодоления диалектического тупика в проектах искусственного интеллекта - переход к более общей модели мышления, не связанной с антропными принципами, а ориентированной на потоки информации и их анализ, а также на реализацию процедуры порождения новых субъектов, как креативной компоненте искусственного интеллекта.*

Ключевые слова: *искусственный интеллект, искусственный разум, субъектно-объектная модель, потоки информации, имитация мыслительных процессов.*

ВВЕДЕНИЕ. МИССИЯ СТАТЬИ

Рассуждая о проблеме искусственного интеллекта, мы в первую очередь подсознательно исходим из парадигмы антропоморфного интеллекта, который неразрывно связан с человеком и его биологической сущностью. Экстраполируя, мы можем представить себе интеллект и разум внешний относительно человека, но не можем наделить его конкретными свойствами. В этом, например, заключается принципиальный недостаток программ поиска внеземного разума, в котором мы ищем строго подобных себе, в частности, предполагая наивно, что «настоящий разум» обязательно будет давать о себе знать во внешний мир, т.е. вести некую «презентативную» деятельность. Также в дискурсе о проблеме технические специалисты практически никогда не разделяют понятий разум и интеллект.

Задача данной статьи — провести обзор понятий разума и интеллекта, связанных с антропоморфными сущностями, проиллюстрировать положение о том, что современная теория и практика создания искусственного интеллекта есть имитация человеческих подходов к мышлению, что противоречит диалектике развития как проблемы искусственного интеллекта в частности, так и логике развития науки и техники.

Немного забегая вперед, отметим, что первый закон диалектики, описывающий переход количественных изменений в качественные, в случае рассматриваемой нами проблемы дает надежду на становление нового восприятия проблемы искусственного интеллекта, как

нового качества, вырастающего из количественных изменений в творимом человеком процессе обработки и анализа данных.

РАЗУМ И ИНТЕЛЛЕКТ КАК ИСТОРИКО-ФИЛОСОФСКИЕ КАТЕГОРИИ

Разум в европейской философии понимается не только как всеобщий порядок вещей, называемый так же объективным разумом, но и как способность человека постигать этот порядок (в т.ч. способность анализа, обобщения, абстрагирования), в которой проявляется высшая степень мыслительной деятельности [1].

В античной философии понятие разума описывается тремя терминами- Логос, или вербально-логический разум (разум рассуждения и аргументации), Нус – разум осознания и постижения истины и Фронесис – разум, в более широком понимании, практической мудрости и умения принимать верные решения, которому Аристотель в своем сочинении «Этика Никомаха» противопоставил термин «София» как разум теоретической мудрости.

Большинство ученых, в их числе Дж.Локк и Г.В. Лейбниц, видели в разуме способность воспринимать вечные и необходимые истины. В отличие от рассудка (способности рассуждать и понимать предметы и явления), разум дан человеку, способному делать умозаключения, что невозможно без понимания взаимосвязей между предметами и явлениями. При этом сначала появляются ощущения, связанные с предметами и явлениями, и затем разум постепенно усваивает их и сохраняет в памяти, присваивая им определенные имена, которые он впоследствии абстрагирует. Таким образом, разум, наделенный абстрактными идеями и понятиями, начинает использовать их в качестве материала для рассуждения, выявления взаимосвязей между предметами и явлениями, для умозаключения. Эти процессы происходят посредством соединения простых идей в сложные, сопоставления как простых, так и сложных идей для выявления отношений и обособления идеи от всех других идей, то есть абстрагирования. Чем больше такого материала дается разуму, тем заметнее становится его работа и сила мышления [2].

В соответствии с учением Г.В.Лейбница разум человека оперирует понятиями, не существующими в окружающем мире и, следовательно, не отражаемыми с помощью ощущений [3], что в корне отличает его от учения Дж.Локка.

По мнению И.Канта, разум дает общие принципы и направляет рассудок в познавательной деятельности. В своей фундаментальной работе «Критика чистого разума» (1781г.), посвященной исследованию познавательных возможностей разума, Кант доводит до читателя мысль, что «вещь в себе» для разума человека есть его представления и понятия о ней, то есть она дана разуму как феномен, однако сама по себе она непознаваема [4].

В соответствии с философией Гегеля «сущность является, а явление существенно», следовательно, опровергается принцип непознаваемости сущности разумом, при этом разум является абсолютным явлением, или мировым духом, а индивиды (народы) достигают его цели и вносят свой вклад в его самопознание, являясь его инструментом. Разум не противопоставляется интеллекту, или рассудку, а включает его как меньшую категорию, в рамках которой берет начало мыслительный процесс [5].

До наступления Нового времени в восприятии разума присутствовала целостность, однако в 20в. под влиянием, в частности, философии постмодернизма - конструктивизма и эпистемологического релятивизма - произошли существенные изменения в восприятии разума. Появился «исторический», «научный», «диалектический», «технический» разум, сам термин «разум» стал заменяться понятием «рациональность». Наличие таких принципов философии постмодернизма, как иллюзорность реального мира, неоднозначность и непознаваемость истины, вариабельность внешнего мира (свойство, в соответствии с которым мы конструируем внешний мир сами) позволяет воспринимать разум не только как субъект познания и восприятия, но и в гораздо большей степени как субъект формирования реальности.

В отличие от разума как способности не только рассуждать и аргументировать, но и постигать и осознавать истину, выявлять общие

закономерности и взаимосвязи, интеллект или ум (а также рассудок) в большей степени является качеством психики, заключающимся в способности приспосабливаться к новым ситуациям, способности к обучению и запоминанию на основе опыта, пониманию и применению абстрактных категорий.

Интеллект (intellectus — разумение, понимание, постижение) — определяется как некая совокупность умственных способностей индивидуума, обладающая свойством устойчивой структуры, как мыслительные способности человека, включая, но не ограничиваясь способностью индивидуума действовать, руководствуясь здравым смыслом, а также приспосабливаться к меняющимся условиям. В настоящее время большинство психологов придерживаются данной точки зрения, однако по-прежнему не существует единого определения этого термина.

Интеллект и умственное развитие играют важнейшую роль в социальном и психологическом развитии индивидуума. От их уровня зависит поведение человека и взаимоотношения его с окружающим миром, его социальное положение. Интеллект является ключевым качеством целостного личностного развития, определяет личностную систему ценностей.

Как видно из приведенных выше определений, интеллект является в большей мере личностной и социальной, т.е. субъективной категорией, в то время как разум способен охватить надмирные сущности и оперировать объективными категориями, несмотря на то, что он неотделим от интеллекта и чувственности. Интеллект направлен на использование накопленного опыта, что существенно ограничивает пространство вариантов решения проблемы. Напротив, разум, будучи способным анализировать опыт и, руководствуясь некой картиной истины, не являющейся результатом практического опыта, может выявлять новые закономерности.

Возможно, именно по причине большого охвата разума, исследования интеллекта, начиная со второй половины двадцатого века, сместились на изучение креативного начала (мышления). Д.П. Гилфорд (the nature of Human Intelligence, 1967) обобщил результаты множества исследований и создал расширенную концепцию интеллекта [6]. Он выделил два типа мышления: конвергентное, необходимое для нахождения единственно точного решения, и дивергентное, порождающее множество оригинальных решений проблемы, кажущейся простой и однозначной.

При этом индивидуум обладает тем большим творческим потенциалом, чем выше у него коэффициент интеллекта. В результатах своих исследований Гилфорд подверг сомнению истинность концепции g (общего, генерального) фактора интеллекта, так как во многих исследованиях обнаруживались интеллектуальные факторы, независимые друг от друга, из чего следует, что решающим фактором для выполнения какой-либо деятельности является не интеллект вообще, а определенные интеллектуальные качества и способности. Факторно-аналитические исследования Дж.Гилфорда показали ложность убеждения, что при работе с разной информацией включается одна и та же способность.

Согласно общепринятой картине мира и взглядам современников информация разделялась на вербальную и невербальную. Гилфорд ввел третью категорию содержания (примененную им в тестовых заданиях, которые состояли из чисел и символов) - символическую. Все три категории– образная, символическая и семантическая – связаны с интеллектуальными способностями, однако их не объединяют более никакие факторы. Четвертая категория (тип содержания) по Гилфорду – поведенческая (связанная с пониманием чувств и мотиваций других людей).

Дж. Гилфорд выделял пять типов интеллектуальных операций (базовых интеллектуальных процессов) – познание, память, конвергентное продуцирование, дивергентное продуцирование, оценивание. Как операция, познание является основой для всех остальных. В цепочке познание – запоминание – продуцирование – оценивание чем дальше операция, тем более она зависима от других, предыдущих операций.

Гилфорд был последователем Л.Л. Терстоуна, модель интеллекта которого основывалась на идее об интеллектуальном акте как результате взамодействия множества

отдельных факторов, не имеющем общей основы. Терстоун стал автором метода факторного анализа [7], выделив такие факторы, как словесное понимание, числовой фактор (скорость и точность вычислений), ассоциативная память, скорость восприятия и др.

Ч. Спирмен в ходе своих исследований обнаружил взаимосвязь результатов психологических тестов и пришел к выводу, что в основе интеллектуального акта лежит как фактор, определяющий данную конкретную деятельность (S-фактор), так и общий фактор (или общая способность, G-фактор), отражающий общую умственную энергию, которой наделен индивидуум (двухфакторная теория интеллекта) [8].

Спирмен предложил метод факторного анализа матриц интеркорелляций, позволяющий найти независимый латентный генеральный фактор, влияющий на результат интеллектуального акта.

Согласно результатам исследований Спирмена генеральный фактор играет решающую роль при решении сложных математических задач, но не влияет на сенсомоторные действия. Также из данных научных результатов следует, что корреляции результатов выполнения группой людей интеллектуальных тестов должны быть положительными.

Соотношение интеллекта и разума, а именно, является ли интеллект источником творческого потенциала, являлось на протяжении двадцатого века предметом множества исследований, среди которых можно выделить и исследования Льюиса Мэдисона Термена, позволившие сделать вывод о том, что креативность является одной из составляющих общего развития интеллекта. Однако, те же исследования показали, что уровень креативности не находится в прямой зависимости от уровня интеллекта.

Таким образом, если рассуждать о поступательном движении и последовательном развитии, то нет необходимости создавать отдельно модели искусственного разума, поскольку различные категории искусственного интеллекта могут отвечать как за накопление опыта, так и за креативное его осмысление (обработку).

ИСКУССТВЕННЫЙ РАЗУМ И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ

Когда мы говорим о создании антропоморфного интеллекта, мы прежде всего должны четко разделять понятия «искусственный разум» и «искусственный интеллект». В понятие «искусственный разум» мы вкладываем не только фактор создания человеком сущности, имеющей способность к логическим построениям, но и имеющей самосознание и собственную волю.

Обратим внимание, что в информатике и системном анализе существует «субъекто-объектная модель системы в целом и в частности компьютерной системы [9]. В СО-модели выделяются активные компоненты (сущности) системы – субъекты и пассивные – объекты. Активные сущности производят операции над пассивными, а появляются (рождаются) они из пассивных сущностей под действием других активных компонент. Таким образом, математически СО-модель состоит из двух отображений – поток – это изменение объекта под воздействием субъекта и порождение субъекта – появление нового субъекта из объекта под воздействием субъекта. Данная модель обладает, таким образом, некоторой полнотой и описывает широкий круг явлений. В частности, в компьютерной системе объектами являются файлы, а субъектами – программы.

В свете описанной субъектно-объектной модели мы рассматриваем познание человеком мира как поток информации из окружающей его действительности - объекта познания к человеку – субъекту познания. На самом деле мы говорим о потоке между внешними объектами и ассоциированными с «мозгом-вычислителем» объектами, в которых локализована его память. Отображение «поток» в рамках СО-модели- перенос информации от объекта к объекту под действием субъекта, т.е. познание – перенос информации из внешнего мира внутри субъекта-человека. В случае обратно направленного потока – преобразования действительности – человек инициирует поток информации вовне. Но мы не напрямую трансформируем реальность, а косвенно, создавая машины, инструменты, книги, вычислительные системы.

Компьютерная система содержит в смысле субъектов – исполняемые модули (программы) и именно возможность моделировать как человека, так и компьютерную систему СО-моделью позволяет нам создать общее видение проблемы и перейти к неспекулятивной модели искусственного интеллекта. Неспекулятивность модели состоит в том, что мы должны отказаться рассматривать понятия «поток» и «порождение» для интеллекта человека и для компьютерной системы подобным образом.

Подсознательно именно мыслительные процессы, как процессы преобразования информации в рамках потоков информации, так и порождение новых алгоритмов обработки информации (порождение субъекта) человек на протяжении длительного времени пытается экстраполировать на искусственно создаваемые антропоморфные сущности, используя при этом инструментарий из разных областей – химии, биологии, а в настоящее время и информационные технологии. Однако ни одна из созданных человеком сущностей, во-первых, не обладала всем набором качеств, свойственных человеку, а во-вторых не воспроизводила себя, являясь по сути тупиковой ветвью. Есть достаточно примеров созданных человеком сущностей (мы не имеем документальных свидетельств о попытках создания ИИ, но по косвенным данным СССР занимался созданием ИИ на биологической и химической основе). Кроме того, широко известна легенда об искусственном «интеллектуальном» существе Големе, остатки которого находятся в Праге.

Несмотря некоторые эпизодические успехи история попыток создания человеком себе подобного интеллекта на антропоморфной основе показывает, что наделить искусственно создаваемые сущности сознанием и волей человек, не являясь демиургом, не имеет возможности (даже сознание человека, согласно некоторым исследованиям прошлого века, существует ограниченный период времени). Человек, созданный по образу и подобию божьему, может создавать, однако он не может создавать сущности того же порядка, то есть себе подобных.

Поэтому, если раньше ИИ исходил из андроидной модели, то есть даже внешний облик искусственного существа должен был соответствовать человеку (впервые термин «робот» предложен чешским писателем Карелом Чапеком в начале 20-го века в отношении живых людей, создаваемых на специальной фабрике), то теперь мнение об ИИ стало более реалистичным и практичным.

ПРЕОДОЛЕНИЕ ДИАЛЕКТИЧЕСКОГО ТУПИКА. ВЫВОДЫ.

По причине невозможности создать искусственный разум и интуитивного осознания человеком своего предопределенного места и роли в «запрограммированной» демиургом реальности, человек обращается к информационным технологиям как средству создания искусственного интеллекта, наделенного свойствами помощника. Компьютерная система является в некотором смысле моделью окружающего мира, в которой действуют в качестве субъектов исполняемые модули (программы), которыми управляют пользователи. Субъекты, как мы отметили, инициируют потоки информации между объектами.

В целом человека также можно рассматривать как вычислительную систему (то есть, компьютерная система является, кроме того, и моделью человека) с аппаратной частью – телом и мозгом с нейронной системой, операционной системой – совокупностью рефлексов (дыхание, сердцебиение) и «прикладными программами» - навыками, умениями, знаниями и способами познания и изменения окружающего мира. Аналог операционной системы тем более впечатляющ, поскольку у всех людей одинаково функционирует рефлекторная деятельность, т.е. операционная система «физиология человека» установлена на всех людей. В создаваемых компьютерных системах человек бессознательно воспроизводит процесс своего зачатия и рождения.

Из желания прямого копирования возникает желание и соблазн имитировать работу мозга путем моделирования нейронных структур, работающих как электронные модули и объединенные в нейросети. Однако мы видим, что такие подходы нисколько не приближают нас как к созданию искусственного

интеллекта, так и к пониманию его сущности.

Мы полагаем, что взгляд на искусственный интеллект в рамках СО-модели позволит совершить конструктивный прорыв в этом направлении. Ведь идею моделировать полет взмахами крыльев и движение – переставлением ног в технике оказались невозможными, самолет и колесо – примеры других, неимитационных подходов к созданию конструктивных сущностей.

СО-модель не только онтологична (описывает существование КС и человека), но и гносеологична, поскольку описывает процессы познания мира и его преобразования.

Таким образом, предлагается «разрешить» искусственному интеллекту по-другому преобразовывать информацию и порождать новые сущности для обработки информации (реализации потоков), не связанные жестко с человеческой, антропоморфной логикой, в этом путь преодоления диалектического тупика, основа создания действующих проектов искусственного интеллекта, творческого, немитационного порядка.

СПИСОК ЛИТЕРАТУРЫ

1. Лебедев А.В. и др. РАЗУМ //Большая российская энциклопедия. Том 28. Москва, 2015, стр. 178-180

2. Дж. Локк . Опыт о человеческом разумении. Сочинения в 3-х т. Под ред. И.С.Нарского. – М. : Мысль, 1985. – 623 с.

3. G.W. Leibniz: Neue Abhandlungen über den menschlichen Verstand. Leipzig, 1904, S. 3. Entstanden 1701-1704.

4. I. Kant. Kritik der reinen Vernunft

5. Encyklopädie der philosophischen Wissenschaften im Grundrisse // Heidelberg, 1817 г.

6. Guilford, J.P. The nature of human intelligence. New York, NY, US: McGraw-Hill, 1967.

7. Thurstone, L. L., & Thurstone, T. G. (1941). Factorial Studies of Intelligence. Psychometric Monographs, 2, 94. (1941)

8. C. Spearman. General intelligence, objectively determined and measured //American Journal of Psychology.1904)15, 201-293.

9. Девянин П.Н., Михальский О.О., Правиков Д.И., Щербаков А.Ю. Теоретические основы компьютерной безопасности // Издательство Радио И Связь, 2000, 192 стр.

Семантика языка как источник откровения

O. Tihonenko

Semantics of language as a source of revelation

Abstract. *A semantic and system-analytical approach to the analysis of the sacred texts is applied. The article starts 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 first four 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*

О.О. Тихоненко

к.филос.н., руководитель НКО «Библейская Истина»

fzr@bk.ru, oleglanin.com

Редакционная ремарка. *Олег Олегович Тихоненко, один из оригинальных философов-исследователей и современных богословов, применяет семантический подход к анализу и изучению Священных текстов. Данная статья – начало 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 начинает цикл исследований по смыслу букв первичного языка, на котором были записаны тексты Библии. Автор на примере первых четырех букв алфавита показывает, что каждая из букв связана с предыдущей и следующей множеством семантических, богословских и исторических смыслов и содержаний.*

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

ВВЕДЕНИЕ

Мы изучим буквы, узнаем, что означает та или иная буква, каково ее числовое значение, и какое отношение она имеет к нам.

Это первоначальный палеоиврит в формате пиктограмм, первоначальная форма изображения современных букв иврита. Это было четыре тысяч лет назад. Эти буквы начертаны на камнях и других предметах, найденных в израильской земле. Все это для того, чтобы представить краткий обзор того, как эти буквы выглядели.

Алеф (א), Бет (ב), Гимель (ג), Далет (ד), Хей (ה), Вав (ו), Заин (ז), Хет (ח), Тет (ט), Йуд (י), Каф (כ,ך), Ламед (ל), Мем (מ, ם), Нун (נ, ן), Самех (ס), Аин (ע), Пей (פ, ף), Цади (צ, ץ), Куф (ק), Реш (ר), Шин (ש), Тав (ת).

Это современный иврит. Я могу вам сказать, что когда я начал рассматривать и изучать иврит, это изменило мою жизнь. Это буквально изменило мое отношение к Писаниям. Это изменило способ моего изучения. Теперь я испытываю гораздо больше уважения к своим предшественникам, и к тем, кто хотя бы даже преподает иврит.

ЗАЧЕМ ИЗУЧАТЬ ИВРИТ?

Первое: Если вы женились на иностранке, сколько пройдет времени, прежде чем вы совершенно устанете общаться с ней через посредника? Примерно пять минут? Если вы хотите отправиться с ней на свидание, вам приходится брать с собой переводчика, как вы понятия не имеете, о чем она говорит. На самом деле именно так мы и поступали в течение

двух тысяч лет со Словом БОЖЬИМ. У нас есть прекрасный, удивительный СУПРУГ, который хочет общаться с нами, а нам приходится обращаться к посреднику, чтобы понять ЕГО.

Считаете ли вы возможным, что при переводе что-либо будет утрачено? Кто-нибудь видел, как проходят заседания в ООН или другой международной организации? У каждого в ушах маленькие наушники, не так ли? У каждого! Когда выступающий говорит на иностранном языке, не задумывались ли вы почему, когда он что-то говорит: «Бла-бла-бла-бла-бла», а перевод длится две минуты! Как перевод может длиться две минуты, тогда как он лишь сказал: «Бла-бла-бла»? Большинство политиков все равно только это и говорят, но в любом случае. А иногда происходит наоборот. Бывает, кто-то выдаст очень длинное предложение, а переводчик скажет: «Встретимся через месяц». Как такое вообще может быть? Считаете ли вы возможным, что при переводе что-то может быть утрачено? Безусловно!

Итак, я сделаю некоторые заявления, которые, возможно, окажутся спорными. Нельзя взять Библию и читать ее, как газету! Нельзя взять Библию и читать ее, как некое произведение Стивена Спилберга. Это нельзя сравнить с просмотром кинофильма, это не пассивное занятие. Библия существует не для того, чтобы ее «читали»! От Бытия до Откровения вы не найдете ни одного раза, когда бы ТВОРЕЦ повелел вам «читать» ЕГО Слово. ОН говорит: «Изучай!». Газету вы не изучаете. Книгу вы не изучаете. Вы изучаете ЕГО Слово. Потому что когда вы изучаете ЕГО Слово, ЕГО буквы, вы изучаете ЕГО! Это все равно, что сесть напротив своей невесты, это все равно, что сидеть напротив своего жениха перед вступлением в брак, пристально смотреть ему в глаза и внимать каждому слову, которое он произносит. Мы так не поступаем, потому что всех нас учили «читать» Библию. И удивительно то, что БОГ так велик и так изобретателен, и так исполнен милости и благодати, что ОН на самом деле позволяет нам что-то извлекать из Библии, даже когда мы читаем ее, как газету. Но она не предназначена для того, чтобы вы, братья и сестры, читали ее в качестве «снотворного» перед сном. Она не для того, чтобы вы сказали: «У меня молитвенное уединение». ОН хочет вас знать, а вы не сможете познать ЕГО в полной мере. Возможно, это кому-то покажется спорным, но смиритесь с этим. Вы не сможете близко познать БОГА Живого так, как ОН это задумал - не общаясь с НИМ на ЕГО языке. Вы не сможете узнать, что ОН действительно имеет в виду в СВОЕМ Слове, если не будете знать ЕГО Слово! Вы можете читать его на русском языке, но уверяю вас, что вы никогда не сможете познать ТВОРЦА так глубоко и на том уровне, что ОН изначально планировал, пока не станете общаться с НИМ лицом к лицу, зная ЕГО слова, - именно так, как ОН их и записал.

Кто-то из вас спросит: «Олег, не хочешь ли ты сказать, что Библию нельзя понять без понимания иврита?». Нет. Вы не сможете познать всей глубины того, что ОН пытается сказать, не зная того, что сказано в языке оригинала, так же, как вы не сможете иметь всей глубины близких отношений. Да, у вас могут быть близкие отношения с вашей женой, если у вас есть переводчик. Да, вы можете понимать, что она говорит, но лишь до некоторой степени. Однако в каждом языке есть определенные слова, которые нельзя перевести. И что тогда будет делать переводчик? Видели ли вы такого переводчика, который, когда тот или иной человек говорит, делает паузы? Почему он делает паузы? Перевод должен идти из него сплошным потоком. Один мой знакомый является профессиональным переводчиком с английского языка. И несколько раз было так, что ему удавалось одновременно и слушать и переводить. Он может непрерывно говорить перевод, слушая при этом одним ухом оригинал. Но часто ему приходится останавливаться. Почему? Потому что его мозг «дает сбой», ведь то, что он только что услышал на английском языке, не имеет соответствующего слова в русском языке. И тогда переводчик добавит еще одно слово, как можно более подходящее по смыслу, с тем, чтобы слушателю было понятно. При этом переводчик знает, что слушатель ни в коем случае не сможет полностью понять то, что этот человек только что сказал.

Итак, я надеюсь, что мне удастся «соблазнить» вас, побудить некоторых из вас к изучению этого прекрасного языка. Потому что когда вы увидите текст на ЕГО языке таким, каким он был написан, и постигнете его глубину, то уже не сможете жить, как прежде.

Второе: Иврит является основным языком Библии и всех апостолов. В то время, в первом веке, люди говорили на арамейском языке, иврит использовался как духовный язык, а древнегреческий, как деловой язык, язык Рима. Но именно иврит является языком Библии.

Третье: Вы не сможете в полной мере понять то, что ОН пытается сказать, если не будете говорить на ЕГО языке.

Давайте поговорим о некоторых случаях игры слов, прежде чем непосредственно приступить к изучению нескольких букв.

Бытие 2:19 - *Господь Бог образовал из земли (это древнееврейское слово «адама») всех животных полевых и всех птиц небесных, и привел к человеку (Адаму), чтобы видеть, как он назовет их, и чтобы, как наречет человек (Адам) всякую душу живую, так и было имя ей.*

Сразу стало ясно, что если бы я не вставил в русский перевод это ивритское слово, то вы бы не увидели никакой связи, не так ли? Вы бы видели только «землю» и «Адама». Где между ними фонетическая связь? Ее нет! Но в оригинале на иврите мы видим нечто очень интригующее. Вам даже не нужно быть очень умным. Даже если вы пятилетний ребенок, умеющий говорить и читать на иврите, вы сразу же заметите связь между этими двумя словами в девятнадцатом стихе второй главы. Вы увидите, что «**земля**» и «**Адам**» происходят от одного и того же коренного слова: «Адам» и «**адама**». Адам был образован из земли. Здесь есть связь. Итак, мы выявили более глубокую связь, потому что видим похожее коренное слово. Одно слово произошло от другого.

«АДАМА»

א ד מ ה

Давайте разберем слово «АДАМА» и увидим в точности, что у нас есть. Прежде всего, если взять буквы «АЛЕФ» и «ДАЛЕТ» ד א, то получим «АД», что означает «ПАР». Итак, это слова, которые можно найти только лишь в слове «АДАМА» («ЗЕМЛЯ»).

Здесь также есть «ДАЛЕТ» и «МЕМ» מ ד, что значит «КРОВЬ».

И еще есть א ד מ «АДАМ», что значит «ЧЕЛОВЕК».

Итак, внутри слова «АДАМА» есть слово «ПАР» (которое связано со словом «ДУХ» или «ВЕТЕР»), слово «КРОВЬ» и слово «ЧЕЛОВЕК». Сложив все это, получаем «ЧЕЛОВЕК, НАПОЛНЕННЫЙ КРОВЬЮ, ИМЕЮЩИЙ ПАР ИЛИ ДУХ БОГА, И ПРОИЗОШЕДШИЙ ОТ ЗЕМЛИ». Все это в одном слове.

«АВ» - «ОТЕЦ»

א ב

Это слово «АВ». Это древнееврейское слово, означающее «ОТЕЦ». «ОТЕЦ» - это «АВ». Буква «БЕТ» также может произноситься как «АБА» в зависимости от того, есть ли в середине буквы «БЕТ» маленькая точечка. Итак, справа вы видите букву «АЛЕФ», а слева - букву «БЕТ». Это две первые буквы алфавита, о которых мы поговорим, и это слово «ОТЕЦ». Слово «ОТЕЦ» - чрезвычайно абстрактное. «Я пришелец с планеты Икс!». Но что такое «ОТЕЦ»? Слово «ОТЕЦ» не значит ничего. Оно греческое, абстрактное. Вы никак не сможете узнать, что значит «ОТЕЦ», если только вам это кто-то не объяснит или у вас есть отец. Вы не сможете это узнать, всего лишь видя слово «ОТЕЦ».

Давайте выясним, что это слово действительно означало на иврите, когда его читали три тысячи лет тому назад.

Это первоначальные пиктограммы двух первых букв. Одна из них, та, что справа, похожа на голову быка. Та, что слева, это буква «БЕТ». Та, что справа,- «АЛЕФ». Та, что слева, буква «БЕТ», похожа на дом или палатку. Именно такими и были их первоначальные значения.

Первая буква - это «СИЛА». «АЛЕФ» значит «СИЛА» или «ЛИДЕР», а «БЕТ» - это «ДОМ» или «ПАЛАТКА». На самом деле ОТЕЦ - ЭТО ОПОРНЫЙ ШЕСТ ДЛЯ ПАЛАТКИ ИЛИ ФУНДАМЕНТ. Ведь в чем крепость дома? В ФУНДАМЕНТЕ.

В чем крепость палатки? Что придает крепости вашей палатке? Когда вы только вытащили свою палатку, она ничего собой не представляет. Это всего лишь кусок ткани. Палаткой, в которой можно жить, она становится лишь тогда, когда ее держит шест. Этот шест и есть «АВ» или, как мы говорим, «АВВА» по-арамейски, «ОТЕЦ». ОТЕЦ - это тот, кто является основой, опорным шестом для палатки, который поддерживает палатку.

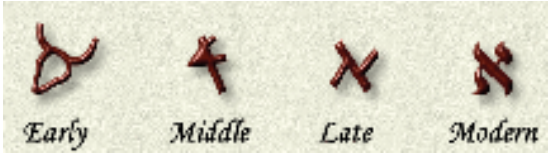
Когда знающие иврит люди читают это слово, они понимают: СИЛА ДОМА- вот что значит «ОТЕЦ». У слова «ОТЕЦ» может быть миллион значений. Сегодня отцом считают того, кто произвел на свет ребенка. Но на языке Библии «ОТЕЦ»- это «СИЛА ДОМА».

Если вы знакомы с Библией, вы понимаете, о каком именно доме идет речь. Потому что во всей Библии есть лишь один дом, а это именно - Храм. Мы установили связь между «СИЛОЙ» или «ЛИДЕРОМ» ДОМА и «ЛИДЕРОМ» ХРАМА. А теперь тот, кто мыслит, как иври, подумает: «Что находится в Храме?» НАСТАВЛЕНИЯ. И все это взаимосвязано. Видите, как это работает? Это прекрасный язык, потому что когда вы его знаете и можете распознавать образы, которые он рисует, ваши мысли разлетаются в миллионе направлений, потому что таких связей - бесконечное множество. Сегодня «ОТЕЦ» это тот, кто говорит, что «У меня есть сын», значит вы отец. Но в библейские времена было не так. ОТЕЦ - это лидер в доме БОЖЬЕМ. Сегодня мы являемся храмом ДУХА СВЯТОГО, и мы служим нашему ОТЦУ, который обитает в Доме.

1. БУКВА «АЛЕФ»

א 

Буква «АЛЕФ». Справа, она показана в форме пиктограммы.



Пиктограмма **Ктав Иври** **Ктав Ашурит** **Книжный Шрифт**

Такова морфология слова, как оно трансформировалось из формата пиктограммы, появившегося четыре тысячи лет назад, в «Ктав Иври» - шрифт, появившийся три тысячи лет назад, который является палеоеврейским письмом. «Иври» означает «еврейский».

В раннем варианте письма эта буква, означающая быка или силу, была в форме посоха. И эта форма использовалась с тысячного года до нашей эры и до самого прихода МЕССИИ, а после вавилонского плена, когда они вернулись, этот шрифт пришел в упадок, и получил распространение «Ктав Ашурит». Поэтому, к тому времени, как по этой земле стал ходить ИИСУС, ОН уже видел и читал «Ктав Ашурит». Сегодня в современном иврите есть такой книжный шрифт, очень похожий на него. Сегодня мы видим шрифт, буквы которого очень похожи на те, которые мог бы писать и читать ИИСУС в свитках, если только ОН не черпал сведения из еще более древних источников. Может быть, это был и «Ктав Иври» - палеоеврейский шрифт. Итак, это был лишь краткий экскурс в историю.

«АЛЕФ»

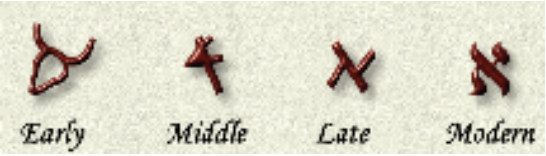
א ל פ

«АЛЕФ». Когда вы произносите название буквы «АЛЕФ», это не просто буква. Когда вы произносите ее название, оно состоит из букв «АЛЕФ»(א), «ЛАМЕД»(ל) и «ПЕЙ»(פ).

«ПЕЙ» может также произноситься как «ЭФ». Я не собираюсь подробно рассматривать эти буквы, однако я хотел вам это показать, потому что вместе они означают «СИЛА», «ЛАМЕД» - это «ПОСОХ» или «НАСТАВЛЕНИЯ», а «ПЕЙ» - это «УСТА».

В действительности «АЛЕФ» означает «СИЛА НАСТАВЛЕНИЯ СЛОВОМ (устами или словом)». И мы знаем, что на иврите «НАСТАВЛЕНИЯ» или «ИНСТРУКЦИИ» - это «ТОРА». Поэтому на самом деле это можно прочесть так: «СИЛА ТОРЫ - ЭТО СЛОВО». Первая буква во Вселенной означает «СИЛА ТОРЫ - ЭТО СЛОВО». И именно от слова произошла вся Вселенная. Она обязательно должна быть связана со словом посредством первой буквы.

МОРФОЛОГИЯ



«АЛЕФ» преобразовалась в древнегреческую букву «АЛЬФА». А затем в латинскую букву «А». Именно от нее произошла английская буква «ЭЙ». «АЛЬФА» в древнегреческом языке, латинская буква «А», а позже - английская буква «ЭЙ» и русская буква «А». Все три буквы: латинская, английская и греческая - все они произошли от этой буквы. Ей соответствует звук «А» или «ЭЙ». Букве «АЛЕФ» соответствует звук «А» или «ЭЙ», и ее числовое значение - «ОДИН».

Если вы еще не знаете, то каждой букве алфавита соответствует то или иное число, а также изображение. У каждой буквы есть значение и число. И это начинается с числа «ОДИН». «АЛЕФ» - это «ОДИН», «БЕТ» - это два и так далее, пока вы не дойдете до буквы «ЙУД», которая означает «ДЕСЯТЬ», а затем идет переход к числам «ДВАДЦАТЬ», «ТРИДЦАТЬ», «СОРОК», «ПЯТЬДЕСЯТ».

Слово «АЛЕФ», в сумме имеет числовое значение «сто одиннадцать». Это нечто первое, начало. В сумме будет сто одиннадцать. Если сложить «АЛЕФ», «ЛАМЕД» и «ПЕЙ», то получится сто одиннадцать.

ЗНАЧЕНИЕ ЧИСЛА «ОДИН»

Это для того, чтобы вы знали числовое значение в библейской терминологии.

- Это число БОГА. Это число ЯХВЕ. Потому что ОН «ЭХАД». ОН ЕДИН. Так сказано в Шма.

- Это число означает единство, неразделимость. «АЛЕФ» невозможно разделить. Это самая первая буква, ее невозможно разделить. Она всегда будет одна.

- Это начало. Число «ОДИН» значит «НАЧАЛО». Число «ВОСЕМЬ» - это «НОВЫЕ НАЧИНАНИЯ», а «ОДИН» - «НАЧАЛО». Вполне логично: это начало чисел.

- Оно уникально. Число один уникально. Оно ни с чем не связано, поэтому оно уникально. Оно само по себе.

- И это также «завершенность». Оно совершенно. Нет ничего другого. Будь вы единственным человеком на планете Земля, вы были бы совершенным. Вас не с кем было бы сравнивать! Будь вы большой или маленький, будь вы с лысиной или шевелюрой, все это не имело бы значения, будь вы единственным человеком на планете Земля. Вы были бы завершены, совершенны и уникальны.

א 

Значение буквы «АЛЕФ» - это «БЫК», «СИЛА», «ВЛАСТЬ», «ЛИДЕР». Поэтому, когда вы видите «АЛЕФ» в своей Библии, то вы видите силу или власть, или лидера.

Бытие 1:1 - *В начале сотворил Бог небо и землю.*

Бытие 1:1 - «*Берешит бара Элохим ЭТ хашамаим веет хаарец»*, так это звучит на иврите. А теперь я хочу показать вам нечто невероятное. Вы этого не сможете увидеть в русском и английском переводе. «*В начале сотворил Бог небо и землю*». ОН сотворил небо и землю. Но на иврите сказано не так, а гораздо конкретнее, и мудрецы вот уже несколько тысяч лет пытаются разгадать эту тайну. В древнем оригинале прямо перед фразой «*небо и землю*» стоит одно слово из двух букв, которое невозможно перевести. И оно не переведено ни в одном переводе, потому что оно непереводимое. Там сказано: «*В начале сотворил Бог «ЭТ»*». Слово «ЭТ» на иврите является непереводимым, и оно означает «ПРЯМОЕ ДОПОЛНЕНИЕ СЛЕДУЕТ». Другими словами, когда вы сталкиваетесь со словом «ЭТ» в тексте на иврите, то оно вам указывает: «ОБРАТИ ВНИМАНИЕ НА СЛЕДУЮЩЕЕ СЛОВО, ОНО ГЛАВНОЕ». Следующая фраза или следующее слово - это то, на что я хочу обратить внимание, это прямое дополнение в предложении. Именно этим и является слово «ЭТ». Но смотрите, что оно означает на иврите. Слово «ЭТ» состоит из букв «АЛЕФ» и «ТАВ».

א ת

Итак, «в начале сотворил Бог...» Слово «сотворил» на иврите может означать «ПРОИЗВЕЛ НА СВЕТ» или «ЯВИЛ», так же, как вы «производите на свет» ребенка. Сотворил, произвел

на свет, явил то, что было сокрыто. Плод находится во чреве в течение девяти месяцев, и вы понятия не имеете, что там такое. Вы никогда этого не видели. В древности не было оборудования, при помощи которого можно было заглянуть вовнутрь и увидеть, как он выглядит. Сегодня прогресс зашел настолько далеко, что детям даже незачем показываться - мы уже и так точно знаем, как они выглядят. Можно даже сделать их цветные фотографии. Вы уже знаете, есть ли у них волосы, есть ли у них пухлые щечки или они худенькие, - это так удивительно! А в то время вы ничего этого не знали. Это было полностью сокрыто до тех пор, пока ребенок не появится на свет. В начале БОГ «произвел на свет» «АЛЕФ» и «ТАВ». Это первая буква и последняя буква алфавита. В НАЧАЛЕ ОН СОТВОРИЛ АЛФАВИТ! ОН СОТВОРИЛ ВСЕ, ЧТОБЫ СОТВОРИТЬ ВСЕ. Позвольте еще раз это сказать. В НАЧАЛЕ ОН «ПРОИЗВЕЛ НА СВЕТ» СВОИ СЛОВА. Ведь прежде чем что-либо сотворить, вы должны иметь слова. А прежде чем иметь слова, вы должны иметь буквы. ОН сотворил алфавит.

Давайте посмотрим, связано ли это как-нибудь с тем, что вам, наверное, знакомо.

Откровение 1:8 - *Я есмь Альфа и Омега, начало и конец, говорит Господь, Который есть и был и грядет, Вседержитель.*

Здесь сказано: «*Я есмь Альфа и Омега*». Это греческие буквы. Неужели вы действительно считаете, что наш ГОСПОДЬ в этот момент установления Тысячелетнего Царства, после того как ОН создал иврит, который сотворил всю Вселенную, предстал бы перед Вселенной и сказал: «*Я есмь Альфа и Омега*»? То есть - «*Я есмь греческий алфавит*». ОН же не Зевс, ОН не греческий бог. ОН еврейский БОГ. ОН Элохим. ОН бы не сказал: «*Я есмь Альфа и Омега*». Я даже не могу это выговорить. ОН бы сказал: «*Я есмь Алеф и Тав!*» «*Я есмь всё, что сотворил Мой Отец. Я есмь этот язык. Я есмь все эти слова. Я есмь Слово*».

Исаия 44:6 - *Так говорит Господь, Царь Израиля, и Искупитель его, Господь Савваоф: Я первый и Я последний, и кроме Меня нет Бога.*

Это говорит ГОСПОДЬ. Если вы сомневаетесь, среди тысяч людей есть некоторые сомневающиеся в божественности САМОГО ИИСУСА. У нас большая проблема, если ОН не божественен. Я не хочу углубляться в богословские тонкости, но прямо здесь, в Книге Исаия, ГОСПОДЬ говорит, что ОН является ЦАРЕМ Израиля (ИИСУС назван ЦАРЕМ Израиля), и ОН является ИСКУПИТЕЛЕМ. ГОСПОДЬ САВАОФ - Воин, Могущественный ЦАРЬ.

«*Я первый и Я последний, и кроме Меня нет Бога*». ИИСУС в **Откровении 1:8** говорит: «*Я первый и последний*». У вас проблемы, если вы полагаете, что ИИСУС - всего лишь человек. Если ОН всего лишь пророк, то ОН не может делать такие же заявления, что и ГОСПОДЬ, о том, что ОН первый и последний, самое начало и самый конец.

«В НАЧАЛЕ»

В каком месте Библии также сказано «в начале»? В Евангелии от Иоанна. Не думаете ли вы, что Иоанн, самый «еврейский» из всех апостолов, думал о чем-либо конкретном, когда он это писал? Этот человек вырос с тем, что они называли Писанием, Танахом, а мы называем Ветхим Заветом, и который начинается со слов «В НАЧАЛЕ». Когда Иоанн приступил к написанию своего послания, эта мысль была у него в голове. Он не сам это придумал. Это уже было у него в уме, когда он сказал: «В начале», он что-то с чем-то связывает. Посмотрим, что именно.

Иоанна 1:1 - *В начале было Слово, и Слово было у Бога, и Слово было Бог.*

В начале БОГ произвел на свет «АЛЕФ» ***(א)*** и «ТАВ» ***(ת)***. Я верю, что когда Иоанн сказал: «*В начале было Слово, и Слово было у Бога, и Слово стало...*», а затем в четырнадцатом стихе он говорит: «*И Слово стало плотию*». Иоанн знает, что в **Бытии 1:1** сказано: «*В начале Бог сотворил (или произвел на свет) «АЛЕФ» и «ТАВ»*», а также то, что в Книге Исаия и в Книге Откровение и БОГ, и Десница БОЖЬЯ заявляют, что они являются «АЛЕФ» и «ТАВ». Видите связь? Это слово неспроста находится в **Бытии 1:1**. Как у Исаии, так и в Откровении сказано, ИИСУС и БОГ (Рука и Тело, если хотите) заявляют, что ОНИ являются «АЛЕФ» и «ТАВ», а на иврите это означает «ВЛАСТЬ ИЛИ СИЛА ЛИДЕРА ЗАВЕТА». Потому что пиктограмма буквы «ТАВ» представляет собой крест или метку и

означает «ЗАВЕТ».

Итак, в начале БОГ сотворил Лидера Завета, Лидера и силу Завета. Поэтому, когда ИИСУС говорит: «*Я есмь «АЛЕФ» и «ТАВ*», ОН имеет в виду «*Я - Лидер Завета! Я - Сила Завета!*». Проблема лишь в том, что мы не знаем, о каком Завете ОН говорит, потому что мы не читаем начало Книги, где и находится этот Завет. Когда мы говорим «Новый Завет», мы должны выяснить, что это такое, что значит иметь Новый Завет. Значит ли это, что весь Ветхий Завет отброшен в сторону? Если да, то нам нужно избавиться от всех Десяти Заповедей. Не имеет значения то, что, как говорят, девять из них есть и в Новом Завете. Мы должны избавиться от них всех! Потому что невозможно избавиться от того или иного завета, но оставить какую-либо его часть. Или можно? Когда вы подписываете договор с клиентом или партнером, стоит изменить в договоре лишь одно слово, и весь договор признается недействительным. Спросите любого юриста. Я мог бы переписать весь договор слово в слово, но изменить лишь график получения комиссионных, и тогда это был бы совсем другой договор. Можно ли сказать, что я избавился от всего, что было в нем? Нет! Я изменил лишь что-то одно. Что изменилось в Новом Завете? Первосвященство. Изменилось первосвященство, и потому это Новый Завет.

א

ו י

Буква «АЛЕФ» состоит из двух букв: «ЙУД» и расположенной по диагонали буквы «ВАВ». Справа вы видите буковку, похожую на палочку - она называется «ВАВ». А буква рядом слева похожа на апостроф - это «ЙУД». Когда ИИСУС сказал: «*Ни одна йота или ни одна черта*», ОН на самом деле бы сказал: «*Ни один йуд или ни один дагеш*». Один йуд. Вот о чем ОН говорит - всего лишь об одной малюсенькой буковке алфавита! О маленьком апострофе. Буква «АЛЕФ» имеет огромное значение. Ведь какая первая буква в вашей Библии? ? «БЕТ», «БЕРЕШИТ», «В начале». Можно было бы подумать, что раз БОГ такой умный, то ОН мог бы начать с первой буквы. В этом было бы что-то особенное - «АЛЕФ». Однако буква «АЛЕФ», братья и сестры, передает гласный звук. Она непроизносимая и она означает «сила и власть лидера», и посмотрите, каким будет значение, когда вы соедините вместе эти три буквы. Ведь на самом деле это «ВЫСШАЯ ВЛАСТЬ», потому что «ЙУД» - это десница власти. Это высшая власть, отделенная от низшей власти (то есть от нас) при помощи гвоздя. Ведь буква «ВАВ» в пиктографическом письме - это «ГВОЗДЬ», «ТО, ЧТО СОЕДИНЯЕТ».

Итак, БОГ отделен от нас, но в то же время мы соединены гвоздем ИИСУСА. Удивительно, как это все совпадает. Итак, «АЛЕФ» - это скрытая буква. Вот эта буква - делаем вдох ртом. Это и есть буква «АЛЕФ». «АЛЕФ» - это вдох. «БЕТ». «БАРУХ» «БЕРЕШИТ». Вселенная была сотворена. «АЛЕФ» - это вдох. Это непроизносимая буква силы, которая разделяет и готова соединить. Вот что такое «АЛЕФ». Это «СИЛА ЛИДЕРА». А кто является лидером, как мы выяснили? ОТЕЦ.

СЛОВА С БУКВОЙ «АЛЕФ»

Давайте поговорим о некоторых словах с буквой «АЛЕФ», которые вам, возможно, знакомы.

«ЭЛОХИМ» אלהים - это БОГ.

«АВ» אב - это «ОТЕЦ».

«ЭХАД» אחד - означает «ОДИН».

«АХАВА» - это «ЛЮБОВЬ».

На самом деле «ЭЛОХИМ» означает «множественное число, величественный Судья». Это Судья. Вот что подразумевается, когда вы видите слово «ЭЛОХИМ».

«ОР» - «СВЕТ».

«ЭМЕТ» - «ИСТИНА».

«АХА» - «ГЛАЗ».

«АВРАКА» - «Я БЛАГОСЛОВЛЮ».

«ЭМУНА» - значит «ВЕРА». В русском языке «ВЕРА» - это неопределенное понятие, очень

похожее на греческое. «ЭМУНА»- это глубочайшая уверенность в том, что БОГ является причиной всего. Другими словами, да будет воля ЕГО. Потому что если вы праведны, то, согласно Писанию, ваш каждый шаг предопределен, хорошее или плохое - не имеет значения. Вы вышли на улицу, и вас сбила машина, и тогда это «ЭМУНА». Значит, ОН знал, что вы туда выйдете, и ОН не помешал машине врезаться в вас. Следовательно, такова ЕГО воля. Есть что-то, что в процессе должно быть благословлено. «ЭМУНА»- это единственное слово в алфавите, которое приносит «ШАЛОМ». «ШАЛОМ» - «МИР». В вашей жизни не может быть мира, если у вас нет веры. Поэтому Иаков говорит: «Покажи мне веру твою без дел твоих, а я покажу тебе веру мою из дел моих». Ведь о чем мы думаем, когда говорим «ШАЛОМ»? Иметь «ШАЛОМ» значит сидеть сложа руки и отдыхать, держать стакан с газированной водой и смотреть футбол или хоккей. Вот это «ШАЛОМ»! Вот это МИР! «ШАЛОМ», согласно Писанию, значит делать то, что вам говорит делать ТВОРЕЦ, зная, что все, что происходит в результате, идет от НЕГО. Остальное не имеет значения. Когда вы идете на работу, вы работаете для НЕГО. Когда вы отдаете приношения, вы отдаете ЕМУ. Все, что вы делаете: говорите со своей женой или благословляете своих детей, это «ЭМУНА», и все это потому, что результаты не принадлежат вам.

«АДОНАЙ» значит «ГОСПОДЬ».

«АДОНАЙ»

א ד נ י

«АЛЕФ», «ДАЛЕТ», «НУН», «ЙУД».

«СИЛА ЛИДЕРА, КОТОРЫЙ ОТКРЫВАЕТ ДВЕРЬ, НЕСУЩУЮ ЖИЗНЬ И СИЛУ». Вот что означает это слово.

2. «БЕТ»

ב ב

Обе эти буквы изображают «БЕТ». Одна из них относится к палеоеврейскому пиктографическому письму, а вторая - к современному ивриту.

Пиктограмма Ктав Иври Ктав Ашурит Книжный Шрифт

Морфология буквы «БЕТ» выглядит следующим образом. Ее числовое значение- «ДВА». И вы видите, как она преобразовывалась. Ей соответствует звук «Б», и от нее произошло русское слово, которое означает «ОБА». Что именно вы говорите, говоря «ОБА»? «ДВА». Не так ли? «*Они оба. Этот и этот*». Слово «ОБА» произошло от буквы «БЕТ», второй буквы алфавита. Вы не поверите, насколько тесно наша жизнь связана с ивритом. Если забрать из нее иврит, то у нас не останется языка. Многих языков мира. Более того, всех.

Эта буква передает два разных звука, когда встречается в вашей Библии. Она произносится либо как «БА», если в ней есть «ДАГЕШ» - маленькая точка, либо как «ВА», если у нее в центре нет этой точки.

ב בּ

Поэтому при чтении нам следует обращать внимание, есть ли у этой буквы точка. Если же точки вообще не ставятся в том или ином шрифте, тогда нам нужно достаточно хорошо знать язык, чтобы определять контекст.

בּ י ת

«БЕТ» пишется по буквам так: «БЕТ», «ЙУД», «ТАВ». «БЕТ»- это «ДОМ». «ЙУД»- это «СИЛА». «ТАВ» - это «ЗАВЕТ». Вместе это «ДОМ СИЛЫ ЗАВЕТА». ДОМ БОЖИЙ - ЭТО СИЛА ЗАВЕТА.

«АВ» בּ א – это «ОТЕЦ».

«БЕН» בּ ן – это «СЫН».

«БЕН»: «БЕТ», «НУН». «НУН» здесь выглядит иначе. Конечная «НУН» больше похожа на посох. Она больше похожа на посох. И вот что необыкновенно: если вы соедините ивритские слова «АВ» и «БЕН» («ОТЕЦ» и «СЫН»), то получите «АБЕН», что означает «КАМЕНЬ», «ОСНОВАНИЕ» или «СКАЛА».

בּ א ן

Что сказал ИИСУС? «*Я есмь камень, который отвергли строители*». Как ОН это сказал на иврите? ОН сказал: «*Я есмь «абен». Я есмь! Я есмь, прежде нежели был Авраам*». Все это взаимосвязано. «*«КАМЕНЬ» означает то, что власть ОТЦА заложена в МЕНЯ, СЫНА, и это образует краеугольный камень, о который вы преткнетесь, потому что вы не сможете это принять - то, что Я исшел от ОТЦА*».

Ее значение. Она означает «палатка», «дом», «план этажа», «семья» или «обитать». Все эти понятия связаны с домом. Это может быть палатка, как у древних израильтян, дом, план этажа (сама эта буква немного похожа на план этажа) или глагол «обитать». И они могут «обитать» благодаря руке, которая указывает на дом.

Ее числовое значение - «ДВА», что означает «РАЗДЕЛЕННЫЙ» или «ПОКАЗЫВАЮЩИЙ РАЗНИЦУ», или это может означать «СВИДЕТЕЛЬСТВО», «*где двое или трое собраны во имя Мое*». Нельзя было выдвигать обвинение на пресвитера или старейшину в какой бы то ни было общине в мире, в какой бы то ни было исторический период с тех пор, как была дана Тора, если нет двух свидетелей. Другими словами, если пресвитер в чем-то поступил неправильно, но вы не можете это доказать или привести свидетеля, то вы никак не можете его наказать. Это должно быть доказано свидетелем. У вас должен быть «БЕТ». У вас должен быть свидетель. Два свидетеля, чтобы показать разницу, чтобы привести свидетельство. Тора говорит, что свидетельство не может «состояться», если нет, по крайней мере, двух свидетелей.

«*Один плюс один равно два*». Особенно в том, что касается бракосочетаний, невозможно иметь дом с одним человеком. Дом - это один плюс один равно «БЕТ». Именно тогда у вас получается дом. Когда мы говорим «ДОМ», то представляем себе стены, крышу, ковер и, конечно же, телевизор!

Но на иврите «ДОМ» значит «ОДИН ПЛЮС ОДИН», двое людей составляют дом. Вам достаточно лишь иметь навес. Вам достаточно лишь иметь одну «сукку», одну маленькую палатку, которую поддерживает ОТЕЦ, как шест, основание, камень- и у вас есть дом.

Буква «БЕТ» связана с Исходом. Это вторая книга Библии. Буква «АЛЕФ» связана с Бытием. Это первая книга Библии и первая буква. Удивительно, что вся Книга Исход посвящена строительству Дома. Более пятнадцати глав Книги Исход посвящены проектированию и строительству Дома БОЖЬЕГО, и она заканчивается тем, что СЛАВА наполняет Храм.

Вот уже две тысячи лет мы строим дома так, как нам заблагорассудится. «*Я хочу построить свой дом здесь*», «*Я построю свой дом здесь*», я говорю в пророческом смысле, образно, о вероучениях, доктринах. «*Я буду верить в это!», «Я сделаю так!*», «*Я построю свой дом!*». Но ОТЕЦ говорит: «*Вы напрасно трудитесь, если дом не построю Я. Если Я не построю «БЕТ», вы трудитесь напрасно*».

Что БОГ делает в эти последние дни? ОН сносит дома для того, чтобы мы отстроили их заново на камне, чтобы мы отстроили их заново на ЕГО Доме, с тем, чтобы через пятьдесят глав мы закончили планировать и строить такой дом, который ОН хочет, чтобы мы имели, и при этом мы совершали Библейские поступки по-библейски, и мы хранили Шаббат, и мы начали есть то, что ОН нам говорит есть, и перестали есть то, что ОН вам говорит не есть, и отмечать дни, которые, как ОН говорит, важны для НЕГО, как для наших жен важны годовщины свадьбы. Когда мы начнем делать все это, а также многое другое, что угодно нашему ОТЦУ, тогда придет слава! До тех пор пока мы не очистим Дом, Слава не придет.

Мы хотим быть наполнены ЕГО Славой. Вот некоторые связанные с этим места Писания.

1-е Коринфянам 3:9 - *Ибо мы соработники у Бога, а вы Божия нива, Божие строение.*

10 - *Я, по данной мне от Бога благодати, как мудрый строитель, положил основание (камень), а другой строит на нем; но каждый смотри, как строит.*

11 - *Ибо никто не может положить другого основания, кроме положенного, которое есть Иисус Христос.*

Это и есть ваш камень.

1-е Коринфянам 6:19 - *Не знаете ли, что тела ваши суть храм живущего в вас Святого Духа, Которого имеете вы от Бога, и вы не свои?*

Некоторые слова с буквой «БЕТ»:

«БЕЙТ»- значит «ДОМ».

«БЕН»- значит «СЫН».

«БАНАХ»- значит «СТРОИТЬ».

«БАРАК» - значит «БЛАГОСЛОВЛЯТЬ» или «ПРЕКЛОНЯТЬ КОЛЕНИ».

«БОКАР» - значит «ПЕРВЫЙ СВЕТ», «РАССВЕТ» или «ПЕРВАЯ СТРАЖА».

«БОКЕР»- значит «УТРО».

«БОКЕР ТОВ»- значит «ДОБРОЕ УТРО».

«БЕЙН» - значит «МЕЖДУ» или «РАЗЛИЧАТЬ».

«БАДАЛ»- значит «БЫТЬ РАЗДЕЛЕННЫМ».

«БАКА» - значит «РАСЩЕПЛЯТЬ» или «РАЗЛАМЫВАТЬ».

«АЛЕФ» и «БЕТ»

א  «АЛЕФ»- значит «ЛИДЕР или «СИЛА».

ב  «БЕТ»- значит «ДОМ», «ПАЛАТКА» или «СЕМЬЯ» или глагол «ОБИТАТЬ».

А все вместе получается «СИЛА ДОМА СЕМЬИ - ЭТО ОТЕЦ». Вот кому мы должны молиться - нашему ОТЦУ, который является силой или лидером нашего дома. Мы - храм ДУХА СВЯТОГО.

3. «ГИМЕЛЬ»

По мере нашего рассмотрения алфавита, вы увидите, что каждая буква не является автономной. Она связана с предыдущей буквой, и она связана со следующей буквой. Они действуют в тандеме, словно привязанные канатами к причалу. Все корабли «привязаны». Бывает, вы видите корабль посреди океана или в бухте, и кажется, что он сам по себе стоит на одном месте, но вы не знаете, что от него до самого дна протянут канат с якорем, которым он и закреплен ко дну. Якорь обладает таким же «автономным правом», что и корабль, а корабль - тем же, что и якорь. Они оба работают в тандеме, они действуют сообща. Я хочу донести до вас мысль о том, что дом, разделившийся сам в себе, не имеет никакого «АЛЕФА», а это означает, что он не привязан к своему ТВОРЦУ. Это непроизносимая буква, которая находится там, но она сокрыта.

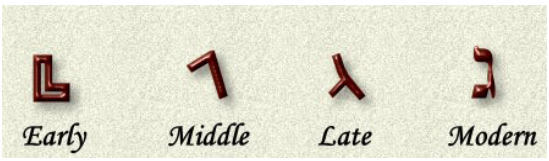
Сила дома зависит от ДУХА, который является дыханием, духом БОЖЬИМ, сокрытым в доме. Когда вы станете следовать за ОТЦОМ, начиная с «АЛЕФА», следовать за силой ЛИДЕРА, который должен идти первым, - именно тогда вы войдете в свой дом, а затем обязательно последует и единство. Если муж будет следовать за силой ЛИДЕРА, то дом никогда не разделится сам в себе. Но как только муж нарушит Слово БОЖЬЕ, когда муж нарушит «Инструкцию» ОТЦА, силу ЛИДЕРА, тогда дом сразу же разделится сам в себе, а иногда он даже не знает об этом в течение многих месяцев, пока те семена не начнут всходить и на поле не вырастут плевелы.

«ГИМЕЛЬ»

Это третья буква алфавита. Давайте узнаем, что она означает, потому что по мере того, как вы будете изучать эти буквы и духовную подоплеку этих букв, в вас пробудится острая жажда по отношению не только к ЕГО языку. Ведь я могу вас уверить: это не русский язык. В Тысячелетнем Царстве ОН будет говорить не по-русски и не по-английски, не по-испански и не по-французски. Знаете, почему это будет именно тысяча лет? Потому что нам, наверное, именно столько понадобится лет, чтобы выучить иврит. ОН хочет, чтобы мы выучили ЕГО язык, братья и сестры.

ג

Это оригинальное написание буквы «ГИМЕЛЬ». Современная прописная печатная буква «ГИМЕЛЬ».



Пиктограмма **Ктав Иври** **Ктав Ашурит** **Книжный Шрифт**

А это- таблица буквы «ГИМЕЛЬ», нечто вроде эволюции буквы «ГИМЕЛЬ». Ее значение в гематрии- ТРИ. Гематрия означает лишь то, что к каждой букве привязано то или иное число.

А каждое число означает ту или иную букву. Итак, значение этой буквы в гематрии - три. И вы видите, что ее пиктограмма чем-то напоминает ногу или латинскую букву L. Затем вы видите шрифт «ктав иври», существовавший около трех тысяч лет назад. Затем вы переходите к шрифту «ктав ашурит» - это тот шрифт, который видел наш ГОСПОДЬ ИИСУС. Когда ОН читал свитки, именно это ОН читал. А затем и современный книжный шрифт. Именно о нем мы и будем говорить.

Буква «ГИМЕЛЬ» означает «ВЕРБЛЮД». Если внимательно присмотреться, то можно почти различить образ верблюда в самой букве - с ногами и шеей.

Что же собой представляет верблюд? Для нас, современных людей, это некое странное, но интересное животное. Однако сегодня для нас оно мало что значит. Потому что мы ездим на машинах, водим внедорожники, летаем на самолетах и пользуемся всеми остальными видами транспорта. Но в Древнем Египте верблюд был средством передвижения богачей. Будь вы тогда бедняком, на ком бы вы ездили? На осле. Именно поэтому Мария и Иосиф приехали на осле, а не на верблюде. Ездили ли на ослах цари? Нет. Цари передвигались на верблюдах. Перенеситесь во времени в Древний Израиль, в древние времена - две-три тысячи лет тому назад - это было очень, очень важное животное. Верблюд - очень быстрое животное. Оно может очень быстро бежать, когда ему это нужно. И это было идеальное животное для передвижения по Древнему Израилю и пескам пустыни. Вы поймете, как это важно, по мере нашего продвижения.

ВЕРБЛЮД означает «ВСТАТЬ». Верблюды - встают. Пиктограмма буквы «ГИМЕЛЬ» может означать «ВСТАВАТЬ», «ПОДНИМАТЬ». Она может означать «ГОРДОСТЬ». Гордость возносится, не так ли? Она заставляет вас превозноситься, когда делать этого не следует. Или оно может означать «ПРЕСЛЕДОВАТЬ». Кроме того, оно может означать «ЩЕДРЫЙ БОГАЧ».

Слова, которые начинаются с буквы «ГИМЕЛЬ»

ג נ

«ГЭН» или «ГАН» - значит «САД». Это значит «ВОЗНОСИТЬ ЖИЗНЬ». Справа вы видите «ГИМЕЛЬ», а слева - букву «НУН». Буква «НУН» означает «ЖИЗНЬ».

Что значит «САД»? «ВОЗНОСИТЬ ЖИЗНЬ». Разве это не логично? Ведь именно это и делают сады. Вы сеете в саду семя, вы поливаете его «ДУХОМ», и восходит жизнь. В Эдемском саду находился сад жизни.

ג א ה

Слово «ГАА» состоит из букв «ГИМЕЛЬ», «АЛЕФ» и «ХЭЙ». Это слово переводится как «ГОРДОСТЬ».

Что оно означает? «ВОЗНОСИТЬ ГОЛОВУ ИЛИ ЛИДЕРА НАД ЧЕМ-ЛИБО» или «ОТКРЫВАТЬ». «ВОЗНОСИТЬ ГОЛОВУ, КОТОРАЯ ОТКРЫЛАСЬ». Вот что такое гордость. Гордость возносит голову над всеми остальными. Вот что такое гордость - слово «ГАА».

Слово «ГОЛГОФА» - место, которое было вознесено, где МЕССИЯ отдал СВОЮ жизнь. ОН был самым богатым Человеком на земле, ОН был самым богатым Человеком во Вселенной. И ОН также был самым щедрым Человеком, потому что ОН связан с буквой «ГИМЕЛЬ».

«ГИМЕЛЬ» - это третья буква алфавита, но именно поэтому слово «ГОЛГОФА» начинается с буквы «ГИМЕЛЬ», а не с какой-либо другой буквы. Это место даяния. Лобное место, не было скалой, похожей на череп. Это было местом, где подсчитывали людей во время переписи населения.

Слово «ГЕЙ» - ивритское и означает «ГОРДЫЙ». Вы больше никогда не будете воспринимать его по-прежнему.

Слово «ГАВА» - значит «ВЕЛИЧИЕ», «ГОРДОСТЬ» или «ВОССТАВАТЬ». Оно связано с чем-то царским. «НАГРАДА» или «ВОЗНАГРАЖДЕНИЕ».

Слово «ГАМАЛ» значит «БЛАГОДЕТЕЛЬ», «ТОТ, КТО ПРЕПОДНОСИТ ДАРЫ ЛЮДЯМ».

Буква «ГИМЕЛЬ» связана со щедростью. Она связана с тем, кто сидит на верблюде лишь

с одной целью - раздавать и преподносить дары. Кто сел на верблюда, чтобы принести дары самому могущественному Человеку во Вселенной? ВОЛХВЫ. Они привели верблюдов. Зачем? Вы видите пророческое значение: верблюды связаны с богатыми людьми, которые приносят дары и преподносят людям «ГОРДОВИТОСТЬ».

Число буквы «ГИМЕЛЬ»- «ТРИ». Число «ТРИ» является одним из самых интересных во всей числовой «атмосфере». Число «ТРИ» обозначает нечто КРЕПКОЕ, ПОДЛИННОЕ, СУЩЕСТВЕННОЕ, ПОЛНОЕ и ЦЕЛЬНОЕ. ЦЕЛОСТНОСТЬ - вот что значит число «ТРИ».

Наиболее крепкое строение, известное человеку, это пирамида, треугольник. Потому что когда на него обрушиваются ветры, бури и дожди, то они врезаются друг в друга. Вот почему брак состоит не из двух людей, а трех. У вас есть фундамент, то есть «АЛЕФ», и у вас есть «БЕЙТ» и «ГИМЕЛЬ», которые действуют сообща. Если не будет фундамента, то они просто упадут в одну линию. Но когда есть фундамент, и концы соединены с фундаментом, со скрытым основанием, то есть землей, тогда две эти линии - муж и жена, «БЕЙТ» и «ГИМЕЛЬ» - действуют вместе против друг друга. Поэтому когда муж и жена действуют сообща, то, по сути, они работают друг против друга, каким бы странным это ни показалось. Поэтому, мужья, когда вам кажется, что ваша жена против вас, то она в действительности укрепляет вас, если только вы к ней прислушиваетесь. То же самое и с мужьями по отношению к женам.

У БОГА три характерных признака: ВСЕВЕДЕНИЕ, ВЕЗДЕСУЩНОСТЬ и ВСЕМОГУЩЕСТВО.

ВРЕМЯ состоит из трех великих разделов: ПРОШЛОЕ, НАСТОЯЩЕЕ и БУДУЩЕЕ. Все это связано с буквой «ГИМЕЛЬ».

В ГРАММАТИКЕ есть три лица, которые выражают и охватывают все виды человеческих взаимоотношений. Первое лицо, второе лицо и третье лицо.

Это одно из наших четырех совершенных чисел.

«ТРИ» означает «БОЖЕСТВЕННОЕ СОВЕРШЕНСТВО».

«СЕМЬ» означает «ДУХОВНОЕ СОВЕРШЕНСТВО».

«ДЕСЯТЬ» означает «ПОРЯДКОВОЕ СОВЕРШЕНСТВО», совершенное число.

«ДВЕНАДЦАТЬ» означает «ПРАВИТЕЛЬСТВЕННОЕ СОВЕРШЕНСТВО». А начинается все это с числа «ТРИ».

«ТРИ» - это «БОЖЕСТВЕННОЕ СОВЕРШЕНСТВО».

Есть три части у Ааронова благословения.

1. «*Да благословит тебя Господь и сохранит тебя*»- это связано с буквой «АЛЕФ».

2. «*Да озарит Господь лицо Свое для тебя и помилует тебя*»- это «ДОМ», буква «БЕЙТ». ОТЕЦ озаряет СВОЙ Дом.

3. «*Да обратит Господь лицо Свое к тебе и даст тебе мир*». Эта фраза Ааронова благословения связана с двумя определениями буквы «ГИМЕЛЬ», а именно: «ВОЗНОСИТЬ» и «ДАВАТЬ».

Вот в чем вся суть Ааронова благословения: ВОЗНОСИТЬ ЕГО ЛИЦО, ОБРАЩАЯ ЕГО К НАШИМ ЛИЦАМ, С ТЕМ, ЧТОБЫ ОН МОГ ДАТЬ НАМ ШАЛОМ. Буква «ГИМЕЛЬ»- дает.

Авраам приготовил три меры еды для своих гостей-ангелов.

В третий день творения земля вознеслась над водой. Здесь намек на нечто иное, что затем должно было вознестись над землей на третий день. Это наш ГОСПОДЬ ИИСУС, который «ВОЗНЕССЯ» из гроба на третий день. Это тоже связано с буквой «ГИМЕЛЬ». Потому что как только тот верблюд поднимается, ЦАРЬ садится на него. Вот почему это не могло произойти на второй день. И вот почему это не могло быть на четвертый день. МЕССИЯ должен был воскреснуть на третий день, потому что это связано с буквой «ГИМЕЛЬ»- именно тогда ЦАРЬ возносится, чтобы что-то кому-то дать.

ИИСУС воскресил из мертвых троих людей. Все это связано!

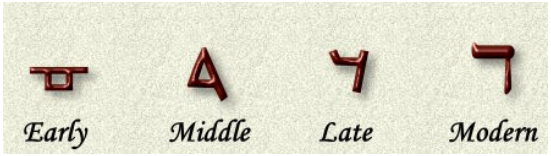
Существует три великих Праздника паломничества - Праздник опресноков, Суккот и Шавуот.

При даровании Торы на горе Синай Израиль трижды сказал: «*Все, что сказал БОГ, сделаем*». Это было еще до того, как они это услышали. «Слушай, Моисей. Все, что Он сказал тебе на горе, мы сделаем!». После того как они ска-

зали: «*Все, что Он сказал, мы сделаем*», БОГ сказал: «*Вот если бы они всегда такими оставались! У них такое хорошее отношение сейчас! Вот если бы они всегда были такими!*». Так сказано во второй версии Перевода короля Иакова. У БОГА есть чувство юмора. А также это доказывает, что ОН ВСЕВЕДУЩИЙ. Потому что ОН уже видел, как часто они будут все портить, и ОН говорит: «*Вот если бы они сохранили нынешнее отношение*». Многие из вас, как и я, отказываемся делать что-либо до тех пор, пока все не увидим, не поймем, не проанализируем, не докажем и не поместим это на рекламном щите. Мы не верим ЕМУ. На самом деле у нас сегодня нет веры. Мы говорим, что мы верим в ИИСУСА, мы верим в БОГА-ТВОРЦА Авраама, Исаака и Иакова, но хотим ли мы в действительности поступать так, как ОН нам говорит? Даже если мы не знаем, что это такое. Именно такая вера нужна для того, чтобы угодить ОТЦУ. Потому что когда ОН говорит: «*Я хочу, чтобы они были здесь*», то именно так должно быть. Словно появляется огромный красный флаг с надписью: «Так угодно ОТЦУ». ВЕРА- это то, что угодно ОТЦУ. Вера может быть только у тех, кто не совсем уверен в том, что делает, но все равно делает!

4. «ДАЛЕТ»

Эта буква интересна тем, что она неполноценна в своем значении. Эта четвертая буква в алфавите, так что она связана с числом «четыре».



Пиктограмма **Ктав Иври** **Ктав Ашурит** **Книжный Шрифт**

Вы видите пиктограмму этой буквы. Это линия с ящиком под ней. Это ворота. Вот что означает это изображение. Это ворота. Это палатка. Да, она не похожа на палатку, однако это изображение. Это ворота. Это палатка. Да, она не похожа на палатку, однако это изображение их палатки.

Второе написание- «Ктав Иври», следующий этап эволюции этой буквы. Вы видите нечто похожее на треугольник. Теперь она уже несколько походит на палатку, «сукка» на иврите.

Число «ЧЕТЫРЕ» означает «ЗЕМЛЯ» или «ТВОРЕНИЕ», «СТАБИЛЬНОСТЬ». Вот что такое «ЧЕТЫРЕ». Имя БОЖЬЕ (ЯХВЕ) состоит из четырех букв. Нет ничего более стабильного, чем эти четыре буквы: «ЙОД-ХЭЙ-ВАВ-ХЭЙ».

Существует четыре уровня библейского толкования. ПШАТ - это буквальное значение Писания. РЕМЕЗ - это аллюзия. Когда есть намек на что-то другое, то это называется Ремез - это более глубокий уровень, чем Пшат. ДРАШ- это аллегория. СОД - это глубочайшее значение Писания, которое только существует. Это некая тайная часть Писания. Чтобы ее увидеть, необходимо по-настоящему углубиться в Писание, и ДУХ СВЯТОЙ должен открыть вам это глубокое значение.

Если выделить первую букву каждого из этих слов: «П», «Р», «Д», «С», то получится «ПАРАДИЗ», то есть «РАЙ». Когда вы будете понимать Писание на всех четырех уровнях, а не просто тратить свое время в сфере буквального понимания Писания, тогда вы войдете в «ПАРАДИЗ», то есть совершенное присутствие ВСЕМОГУЩЕГО, в которое никто из нас не войдет, пока ОН не придет, потому что мы видим смутно сквозь стекло, а когда ОН придет, мы увидим полноту, и тогда мы войдем в парадиз. Тогда мы поймем каждое значение Писаний и испытаем «**моменты просветления**» в вопросах, мучивших нас тысячи лет. Представьте себе, как вы скажете: «Я смотрел на это место Писания миллион раз, но никогда не видел эти три другие уровня!».

Четыре времени года: ВЕСНА, ЛЕТО, ОСЕНЬ, ЗИМА. Мы видим силу числа «ЧЕТЫРЕ», и как оно связано с землей. Это нечто крепкое, имеющее твердое основание.

Четыре направления: СЕВЕР, ЮГ, ЗАПАД, ВОСТОК. Могло бы быть множество других направлений, но существует четыре основных направления, которые ОН избрал. Четыре стихии: ВОЗДУХ, ОГОНЬ, ЗЕМЛЯ и ВОДА.

Почему их четыре, а не пять или десять, или двенадцать? Потому что все это связано с буквой «ДАЛЕТ». Число «ЧЕТЫРЕ» обозначает КОРЕНЬ ДЕРЕВА, ИДУЩИЙ ОТ ЗЕМЛИ. Деревянное дерево. Это корень, который связан с землей, и он выходит из земли. Здесь существует связь. Потому что корень идет вниз. Задумайтесь об этом. Он идет только вниз. Нам это кажется логичным, потому что мы с детства об этом знаем. Но если бы вы оказались на какой-то другой планете, если такая планета существует, и увидели бы там перевернутое дерево, то вам бы показалось это более логичным, потому что корням дерева так легче принимать дождь. Почему же ОН сделал так, что корни уходят в землю? Все это имеет духовное значение, потому что вода, в которой нуждается дерево, скрыта в земле. Земля связана с буквой «ДАЛЕТ», которая является дверью, ведущей на небо и дающей жизнь. Без буквы «ДАЛЕТ», без этой «ДВЕРИ», без связи с основанием, которым является ДУХ, находящийся под землей - это подземная ключевая вода - именно ее и ищет дерево. Что в Писании символизирует дерево? Людей. Люди - это деревья. Братья и сестры, если ваши корни не будут углубляться в поисках скрытой воды, пресной воды, то вы не сможете расти. БОГ ищет - крепкие деревья, у которых есть стержневой корень, ушедший глубоко в землю. В этом случае враг, когда он придет, несмотря на всю свою силу, не сможет свалить такое дерево. Мы не должны быть углубленными на сантиметр и расширенными на километр. Вопрос не в том, сколько человек мы приведем на Небеса. Ведь все равно это не вы приводите их на Небеса! ОН никогда не говорил Петру: «*Иди и обращай в веру весь мир*». ОН сказал: «*Идите и научите*». Само слово «УЧЕНИК» является стержневым корнем, уходящим глубоко в землю, изучающим то, что говорит раввин.

Четвертая книга в Ветхом Завете - Числа. Она связана с буквой «ДАЛЕТ». Четвертая книга Библии охватывает тридцать восемь лет скитаний израильтян по пустыне. Для сравнения: в предыдущей книге (Левит) - один год, а еще в предыдущей (Исход) - один месяц. Вы видите: в одной книге - месяц, в другой - год, а затем доходите до Второзакония, где описано, как в течение тридцати восьми лет израильтяне шли через то место, на котором должны были жить, но они шли через него. С точки зрения БОГА, сверху вниз. Когда мы говорим «**шли через**», то, что возникает у нас в воображении? Мы переходим от одного места к другому. Вы переходите из одной комнаты в другую. Переходя из одной комнаты в другую, что вы делаете? Вы проходите через дверь. Вам приходится проходить через дверной проем. С точки зрения БОГА они проходят сквозь дверь. ОН открыл дверь при Исходе, после десятой казни, и ОН позволил СВОЕМУ народу выйти через эту дверь, но решение было за ними: выйти им немедленно и пойти к своему наследию или не идти через ту дверь. Они решили не идти. Поэтому они оставались в переходном, подвешенном состоянии в течение сорока лет.

Они испытали смирение и нищету, чтобы им подготовиться к Земле обетованной. Когда израильтяне вышли из Египта, они вышли богачами. В материальном плане они разграбили египтян. Они вышли, оседлали верблюдов и стали богатыми. Но проблема была в том, что они не воздали той жизнью, которую им дал БОГ, и поэтому все то золото обесценилось, случилось так, что за золото они не могли получить мяса. И если вы, братья и сестры, не считаете, что это слово предназначено для последних дней, то вы крайне обмануты и наивны. Не думайте, что ваше золото спасет вас в последние дни. Еда - вот что было важным для них в последние дни. Вышли они богачами, а в конце превратились в нищих. Почему? Почему БОГ водил их в течение сорока лет? Чтобы их сломить, чтобы их смирить, чтобы уничтожить их гордыню, потому что богатый человек, который сидит на верблюде, но никому ничего не дает, становится порочным под действием гордыни. Знали ли вы, что у врага тоже есть свой язык и в нем ДВАДЦАТЬ ДВЕ буквы. Потому что каждую букву алфавита можно так извратить, что она приобретет совершенно иное духовное направление. Хотите ли вы, чтобы в вашей жизни действовала сила ВСЕМОГУЩЕГО? Тогда следуйте положительному примеру из Сада. Следуйте языку БОЖЬЕМУ. Но у врага есть язык, который кажется точно таким! Он так хорошо

звучит! Он вызывает те же чувства. Однако он ведет в совершенно ином направлении. И этот же верблюд может вас убить. Он может породить «ГОРДОСТЬ ЖИТЕЙСКУЮ», которая в какой-то момент подкосит ноги этого верблюда, и тот рухнет на землю.

Итак, они смирились и обнищали, чтобы подготовиться к Земле обетованной откровения. Такой же путь должны пройти и мы. Мы переходим к значению буквы «ДАЛЕТ».

Иезекииль 41:23 - *В храме и во святилище по две ДВЕРИ.*

Речь идет о Храме. В Храме есть две двери, ведущие в святилище.

24- *И ДВЕРИ сии о двух ДОСКАХ, обе ДОСКИ подвижные, две у одной ДВЕРИ и две ДОСКИ у ДРУГОЙ.*

На иврите, каждое слово, которое я выделил, это слово «ДАЛЕТ». На самом деле здесь сказано, что «*в Храме и во святилище находятся две буквы «ДАЛЕТ». Две буквы «ДАЛЕТ» сии о двух буквах «ДАЛЕТ», обе буквы «ДАЛЕТ» подвижные, две у одной буквы «ДАЛЕТ» и две буквы «ДАЛЕТ» у другой буквы «ДАЛЕТ»*».

Что это значит, что такое доска? Например, у стола. У некоторых из вас есть обеденный стол, и вы знаете, что такое откидная доска. Здесь тот же принцип. Это по-прежнему стол, но у него есть другая секция. Подобным образом есть и две секции у дверей. Одна секция с одной стороны и другая- с другой. Их там по две, а всего - четыре. Четыре части на две двери, которые находятся у дверного проема в Храме. Слово «ДАЛЕТ» означает «ОБНИЩАЛЫЙ». Оно означает «ОТКРЫТАЯ ДВЕРЬ». Эта дверь всегда открыта. Именно поэтому у слова «ДАЛЕТ» всегда две стороны. Ей недостает третьей стороны. Потому что его духовное послание- это «ДВЕРЬ ОТКРЫТА». Дверь всегда открыта. ОН оставляет свет включенным.

ד ל ה

«ДАЛА» - от этого слова происходит название буквы «ДАЛЕТ». В его основе лежит слово «ДАЛА», которое означает «ОБНИЩАЛЫЙ». Его буквальное значение- «ВИСЕТЬ» или «СВИСАТЬ», как, например, занавес, или «ОСЛАБЛЯТЬ». Именно от него произошло имя Далила. Что сделала Далила? Она «ОСЛАБИЛА» Самсона. Ее имя произошло от слова «ДАЛА».

ד ל ה

«ДАЛЕТ», «ЛАМЕД», «ХЭ». «ДАЛЕТ» - это «ДВЕРЬ» или «СМИРЕННЫЙ ЧЕЛОВЕК В НУЖДЕ».

Буква «ЛАМЕД» означает «ЖЕЗЛ НАСТАВЛЕНИЯ, КОТОРЫЙ ПОДГОНЯЕТ ЖИВОТНЫХ, ДАЕТ ИМ УКАЗАНИЯ, ЗАДАЕТ ИМ ВЕРНОЕ НАПРАВЛЕНИЕ», «Тора».

Буква «ХЭ», которая значит «ОТКРЫВАТЬ» или «НАВЕРХ».

Итак, у вас есть «ДВЕРЬ, ВЕДУЩАЯ НАВЕРХ» или «СМИРЕННЫЙ ЧЕЛОВЕК, У КОТОРОГО ЕСТЬ ТОРА, НЕСУЩАЯ ОТКРОВЕНИЕ». Поэтому, братья и сестры, следующий стих так важен. Думаю, теперь вы поймете его гораздо лучше, чем понимали раньше.

2-е Коринфянам 8:9- *Ибо вы знаете благодать Господа нашего Иисуса Христа, что Он, будучи богат, обнищал (стал «ДАЛЕТ») ради вас, дабы вы обогатились Его нищетою.*

Видите, как будет на иврите? Иври читает это и думает: «Вот это да!» Он только что придал гораздо большее значение двум буквам, связанным друг с другом. В алфавите взаимосвязаны все буквы, расположенные рядом. Какова предыдущая буква? «ГИМЕЛЬ». Что означает «ГИМЕЛЬ»? «БОГАЧ», «ЩЕДРЫЙ БОГАЧ». ОН был богат. ОН сидел на верблюде. ОН был богатым и щедрым человеком. Но ради НЕГО САМОГО ОН стал «ДВЕРЬЮ». Именно поэтому сказано:

Иоанна 14:6 - *Я есмь путь и истина и жизнь; никто не приходит к Отцу, как только через Меня.*

Откровение 3:20 - *Се, стою у двери и стучу.*

15 - *О, если бы ты был холоден, или горяч!*

16 - *Но, как ты тепл, то извергну тебя из уст Моих.*

ОН говорит о дверном проеме. ОН приглашает вас войти и вечерять с НИМ. ОН хочет, чтобы вы либо остались снаружи, либо вошли внутрь. Но поскольку вы решили стоять на пороге, ОН извергнет вас из СВОЕГО дома. В Завете Порога говорится, что стоять на пороге- значит осквернять кровь, которая течет по желобку, сделан-

ному в пороге. Не смейте стоять на крови. Вы должны переступить через кровь. Если вы на чем-нибудь стоите, то в восточной культуре ступня считается самой омерзительной частью тела. Вы никогда не должны ставить ноги, скрестив их - это будет считаться оскорблением и выпадом в адрес человека, стоящего рядом с вами. Именно поэтому в восточных культурах в наше время снимают туфли и бросают в наших президентов. Потому что это означает оскорбление.

ИИСУС обнищал. ОН стал нуждающимся, обедневшим, нищим человеком. Вот почему в Писании сказано, что вы должны смириться. Вы должны поклониться БОГАЧУ, который находится перед вами, потому что если вы не поклонитесь этому БОГАЧУ и не смиритесь перед ТЕМ, КТО предлагает СЕБЯ в жертву за вас, то не сможете перейти к следующей букве, которая означает «ОТКРОВЕНИЕ»! Вы не сможете пройти дальше.

Это духовное путешествие, друзья мои. Этот алфавит- самое мощное явление, о котором вы пока еще не знаете. Потому что когда вы его понимаете, он учит вас жить. Прежде всего, мы должны следовать за силой ЛИДЕРА. Затем у нас должен быть ДОМ, не разделившийся сам в себе. Потому что ОН является ЛИДЕРОМ дома. И ЛИДЕР дома - щедрый, ОН дает нищему. Это создает открытую дверь и приносит откровение.

Буква «ДАЛЕТ» - это дверь смирения, покаяния, самоотверженности и самоотречения. Вот что значит «ДАЛЕТ» - это обнищалая душа в нужде.

Откровение 3:16 - *Но, как ты тепл, а не горяч и не холоден, то извергну тебя из уст Моих.*

17 - *Ибо ты говоришь: «я богат, разбогател и ни в чем не имею нужды «; а не знаешь, что ты несчастен, и жалок, и нищ, и слеп, и наг.*

18 - *Советую тебе купить у Меня золото, огнем очищенное, чтобы тебе обогатиться, и белую одежду, чтобы одеться и чтобы не видна была срамота наготы твоей, и глазною мазью помажь глаза твои, чтобы видеть.*

19 - *Кого Я люблю, тех обличаю и наказываю. Итак будь ревностен и покайся.*

20 - *Се, стою у двери и стучу: если кто услышит голос Мой и отворит дверь, войду к нему, и буду вечерять с ним, и он со Мною.*

«ДАЛЕТ» - это та дверь, если сегодня вам необходим прорыв в вашей жизни. Много раз мы слышали учения и проповеди по всему миру, в большинстве из которых, как нам кажется, говорится о процветании. Те, кто говорят о процветании, в каком-то смысле правы, но в целом они извратили это понятие. Я говорил вам, что враг использует тот же язык, но извращает его. Видите ли, в том, чему учат некоторые из тех учителей процветания, есть духовная истина. Потому что они учат, что если вы будете давать, то станете процветать. Что ж, это неправда. Но здесь четко обозначена духовная истина, что ЕСЛИ ВЫ БУДЕТЕ ДАВАТЬ ПРАВИЛЬНО, ТО ПРИДЕТ ПРОЦВЕТАНИЕ.

Но, возможно, оно окажется не тем, что вы думаете. Потому что когда вы даете, что значит «ГИМЕЛЬ» (и в этом они правы), то щедрый человек дает (о чем они действительно должны вас учить с точки зрения иврим), и это создает открытую дверь для БОГА, с тем чтобы ОН мог действовать в вашей жизни. Потому что когда вы даете ОТЦУ так, как ОН просит вас давать, то это открывает дверь. К чему бы ОН ни хотел привести вас через эту дверь, что бы ни находилось на той стороне, то и есть процветание! Процветание определяется не тем, в насколько большом доме вы живете, какой костюм вы носите, в какой машине вы ездите. Процветание определяется тем, сколько вы даете. И все, что ОТЕЦ вам дает, это и есть ваше процветание. У даяния может быть миллион разных проявлений. Братья и сестры, мы не сможем принять в свою жизнь ПРОРЫВ и ОТКРОВЕНИЕ, пока не научимся быть по-настоящему ЩЕДРЫМИ и давать как богачи, которыми мы уже являемся.

Вы не хотите узнать, что на сердце у ОТЦА. Это приходит только во время поклонения, братья и сестры. Именно поэтому ангелы поют: «*Осанна в вышних*» двадцать четыре часа в сутки, и их не интересует, чему ОН может их научить. Их интересует поклонение ЕМУ, потому что ОН достоин. . В Книге Откровение вы не

увидите занятий по изучению Торы. Вы видите, как мужчины, женщины и ангелы поклоняются своему ТВОРЦУ всем, что у них есть.

Если в Христианстве есть хоть одна правильная вещь во время воскресных служб в церквях, то это их умение поклоняться. Они не спешат узнать то, что знает ОТЕЦ, но они познают ЕГО сердце, они хотят узнать, каково сидеть в присутствии Всемогущего БОГА. Потому что **чудеса происходят не благодаря тому, сколько вы всего знаете. Чудеса происходят в зависимости от того, сколько у вас веры.**

Пока вы не отдадите ОТЦУ то, что принадлежит ЕМУ по праву, - не только своими приношениями, но и всей своей жизнью, - у вас никогда не будет открытой двери. Некоторые из вас вообще никогда не слышали голоса БОГА Живого. Ни разу! Пытались ли вы когда-нибудь? Отдаете ли вы ЕМУ то, что по праву принадлежит ЕМУ? Ведь лишь когда вы отдаете ЕМУ свою жизнь, ОН открывает дверь с Небес и изливает СВОЙ голос и все, что ему сопутствует.

ОН хочет, чтобы вы знали, что ОН ждет вас на обед каждую неделю. Отдавайте ЕМУ то, что принадлежит ЕМУ по праву. Знали ли вы, что ИИСУС рассказывал притчу о брачном пире? И в определенное время дверь на пир закрылась. Помните десять дев? Пять из них отправились домой, потому что у них кончилось масло, и дверь затворилась. Когда зазвучит труба, братья и сестры, вам никак нельзя смотреть телевизор. ОН назначает встречу. Вы должны быть на этой встрече. Второго шанса не представится, и дверь - «ДАЛЕТ» - закрывается. Когда же дверь закроется, когда «ДАЛЕТ» закроется, не будет никакого откровения.

СЛОВА, СОДЕРЖАЩИЕ БУКВУ «ДАЛЕТ»

«ДАМУТ» - значит «ФОРМА» или «ПОДОБИЕ», или «ТИП». Оно связано с буквой «ДАЛЕТ» - «ОТКРЫТОЙ ДВЕРЬЮ».

«ДААТ» - значит «ЗНАНИЕ». Одно из десяти основополагающих характерных свойств БОГА - это «ДААТ». И это скрыто.

«ДАА» - значит «ЗНАТЬ». Посмотрите на это: знание, откровение приходит. Потому что есть открытая дверь.

«ДАМА» - «СЛЕЗИТЬСЯ» или «ПЛАКАТЬ».

«ДАММАМ» - значит «МОЛЧАЛИВЫЙ» или «ТИХИЙ». Только когда вы храните молчание и тишину, обычно во время хвалы и поклонения. Есть время для того, чтобы танцевать, и есть время для того, чтобы хранить тишину и молчание, чтобы что-то услышать. Если вы - «танцор», если у вас это выражается таким образом, вам не всегда следует танцевать. Убедитесь в том, что вы танцуете именно для НЕГО, а не просто потому, что вам нравится танцевать. **Если вы действительно исполнены ДУХОМ и водимы ЕГО ДУХОМ, то иногда вам следует сидеть и слушать, потому что ОН говорит**. Бывает, ЦАРЬ хочет, чтобы вы танцевали перед НИМ. А иногда ЦАРЬ хочет, чтобы вы присели и поклонились перед НИМ. Я призываю вас спрашивать у ЦАРЯ: «Что ТЫ хочешь, чтобы я сделал?» Будьте открыты, ведь ОН - ЦАРЬ.

«ДАЛА» - «ВЕШАТЬ», «ВИСЕТЬ», «ВИСЯЧИЙ». От него происходит слово «ДАЛЕТ», «ОТКРЫТАЯ ДВЕРЬ, КОТОРАЯ ВИСИТ».

Быть «ДАЛ» - «БЕДНЫМ», «СЛАБЫМ», «БЕССИЛЬНЫМ». Когда вы бессильны и слабы, тогда что сказано в Писании? ОН возносит вас, и вы становитесь сильным.

ד נ

«ДАН» - «ДАЛЕТ», «НУН». «ДВЕРЬ ЖИЗНИ» - это слово «ДАН», «СУДЬЯ». Судья может объявить жизнь или он объявляет смерть. То же самое слово. Вот почему слово «ДАН» часто неправильно понимают в Писаниях. Дело в том, что колено Дановo - это единственное колено, которое не упоминается в Книге Откровение. Это колено от БОГА, название которого означает «ДВЕРЬ ЖИЗНИ»! У колена Данова есть символ - Весы. Потому что они могут склоняться в ту или иную сторону. Некоторые из характерных особенностей слова «ДАН» могут склоняться в любую сторону. Это может быть сила жизни либо сила смерти.

ד מ

«ДАМ» - означает «КРОВЬ», «ДАЛЕТ», «МЕМ» - «ДВЕРЬ ХАОСА». Знали ли вы, что «ДВЕРЬ ВОДЫ», дверь, которая приносит воду, вода все смывает и порождает жизнь, что является следующей буквой после «МЕМ».

א ד מ ה

«АДАМА» - означает «ПОЧВА» или «ГРУНТ». Внутри слова «АДАМА» заключено слово «ДАМ», которое означает «КРОВЬ» - слово, которое мы рассмотрели выше. «ДАЛЕТ», «МЕМ» - прямо посередине «АЛЕФ», «ДАЛЕТ», «МЕМ», «ХЭ». «АДАМА» - означает «СИЛА ЛИДЕРА, КОТОРЫЙ ОТКРЫВАЕТ ДВЕРЬ, НЕСУЩУЮ ВОДУ, КОТОРАЯ ПРИНОСИТ ОТКРОВЕНИЕ». А также означает «КРАСНЫЙ». Кроме того, здесь есть слово «АДАМ». «АДАМ» - это «АЛЕФ», «ДАЛЕТ», «МЕМ». Все это происходит от почвы.

א ב
ג ד

Эти первые четыре буквы алфавита. Они рассказывают нам о духовном путешествии. Ваше путешествие начинается с понимания силы Лидера, «АЛЕФ», того, кто имеет рога жертвенника. Для вас это должно нечто означать. Почему они должны были прикасаться к рогам жертвенника? Потому что у рогов жертвенника они просили о милости, потому что им как иврим было известно, что рога жертвенника связаны с первой буквой алфавита, то есть «АЛЕФ», которая означает «СИЛА ИЛИ ВЛАСТЬ ЛИДЕРА, КОТОРЫЙ ИМЕЕТ ПРАВО ВАС ПОГУБИТЬ ИЛИ ПОМИЛОВАТЬ». Мы следуем за силой ЛИДЕРА. ОН является домом. «Дом, разделившийся сам в себе, не устоит». Поэтому брачный договор действует в единстве от «АЛЕФ», и от этого «АЛЕФ» мы имеем «СИЛУ ЛИДЕРА ДОМА» - это богач, который гордится тем, что он дает щедро обнищалым беднякам, чтобы могла появиться открытая дверь.

Вселенная создана из этих двадцати двух букв. Ваша жизнь создана из этих двадцати двух букв. Ваша ДНК связана с алфавитом. Каждая частичка ДНК связана с той или иной буквой. Одна часть ДНК соответствует одной букве алфавита. Разве вас не шокирует то, что в молекуле ДНК точно такое же количество частей, сколько букв в алфавите? Потому что ваша жизнь построена из ЕГО языка. Вот почему древние говорили: «*Если Он умолкнет, Вселенная погибнет*». Ведь единственным, что держит ее в целости, является частота, с которой звучит ЕГО голос, - даже сейчас. Именно поэтому ОН никогда не перестает говорить.

В завершение: ДЕРЖИТЕСЬ КРЕПЧЕ СИЛЫ ЛИДЕРА ВАШЕГО ДОМА.

«Цифра»

Егор Федоров,
Республика Беларусь,
писатель, сценарист, драматург

В приемной главврача Психиатрической клинической больницы им. В.А. Гиляровского было темно, неуютно и даже как-то мрачно. Табличка на двери «главного» выцвела и на ней скорее угадывалась, чем читалась простая русская фамилия – «Иванов». Инициалы угадать было много сложнее, но по силуэтам предположить можно было букву «Г» и букву «А»

- Тикоцкий, пройдите,- пригласила следующего в очереди секретарь после того, как из кабинета главврача вышел посетитель.

Мужчина, которого сейчас вызвали, внешне, казалось, был спокоен. Но по тому, как он поднялся со своего места, по тому, как пошел к кабинету главврача, чувствовался какой–то нерв, какая-то внутренняя разбалансированность посетителя.

Иванов Г. А. сидел за столом своего кабинета и что-то писал. Он ненадолго оторвал взгляд от своих записей, коротко кивнул вошедшему на стул напротив себя и продолжил заполнять какой-то бланк.

- Добрый день,- поздоровался главврач.

- Здравствуйте,- через паузу сказал посетитель. Он тяжело сел на стул, который ему предложили. Тикоцкий вообще был массивным человеком, но сейчас на стул он сел именно тяжело, как-то всем телом, сразу всей его тяжестью, как будто бы на стул хотел перенести весь вес проблемы, с которой вошел сегодня в этот кабинет.

- Слушаю вас,- сказал главврач располагающе, он продолжал писать.- Что привело?

Те первые предложения, что Тикоцкий должен был сказать в ответ на этот вопрос, он даже репетировал дома перед зеркалом. Но что-то мешало этому крупному мужчине начать. Он ещё некоторое время собирался с мыслями и, наконец, произнёс:

- В 2023 году гугл запустит три спутника, которые обеспечат бесплатный интернет всем людям планеты.

Тикоцкий сказал это и снова замолчал. Это была часть его плана - посмотреть, пощупать, понять - можно ли вообще заводить весь этот разговор, который он замыслил, с человеком, который сейчас сидел напротив него.

- Любопытно,- ответил Иванов Г.А. вроде бы достаточно искренне.

После этого ответа, Тикоцкому очевидно стало легче.

Он поправил движением руки ворот рубашки и продолжил.

- К 2037 году 97 процентов населения Земли будет иметь доступ с интернет. Не останется практически ни одного уголка планеты, не обеспеченного этим видом связи.

Посетитель опять замолчал в ожидании реакции главврача.

- Точность прогноза, конечно, спорная,- сказал тот, продолжая делать записи в своём бланке.- Но вполне допускаю.

Тикоцкий хотел что-то возразить, но вовремя одумался. Сейчас обязательно нужно было не сбиться. Сейчас обязательно нужно было сказать главное. То, ради чего он пришел сегодня в этот кабинет. Поэтому он не стал спорить с врачом, а продолжил:

- В 2046 году будет придуман новый вид наркотика- цифровой. Доступ к нему будет осуществляться через сеть интернет. С течением времени наркотик будет улучшаться, модифицироваться, изменяться и «дописываться». И приблизительно через 15 лет станет почти таким же мощным в плане «прихода», как героин. Но в отличии от героина этот наркотик будет совершенно бесплатным. И совершенно безвредным.

Здесь Тикоцкий снова остановился. Ещё дома, в репетициях своей речи он понял, что именно в этом месте обязательно нужна пауза. Врач поправил очки, оторвался от своей бумаги и посмотрел на посетителя. Кажется, он ожидал продолжения.

- В итоге это приведет к катастрофе,- закончил свою отрепетированную речь Тикоцкий.- Человеческая цивилизация погибнет.

Главный врач Психиатрической клинической больницы им. В.А. Гиляровского вернулся к своему документу, дописал его, перечитал в этом документе последний абзац, отложил ручку и стал рыться в ящичках стола в поисках печати.

- Очень интересные сведения,- сказал главврач. –Но есть сразу несколько слабых мест. Если хотите, можем их обсудить.

Вообще то, Тикоцкий продумывал возможные варианты реакции главврача на это своё выступление. Но такой реакции не ожидал совсем. Сейчас, кажется, Тикоцкий был несколько обрадован.

- Конечно, Глеб Алексеевич, если имеете, что сказать по этому поводу...- Тикоцкий слабо улыбнулся.

Главврач нашел, наконец, в столе печать, подышал на неё, потом прижал к бумаге и сказал:

- Бесценно, когда посетитель знает моё имя отчество,- он улыбнулся Тикоцкому.- Сразу располагает. А вас, простите, как величать?

- Александр Николаевич,- ответил Тикоцкий.

- Очень приятно,- сказал главврач.- Так вот, Александр Николаевич. Отчего же этот ваш наркотик, который, как вы утверждаете, появится в недалеком будущем... как вы его назвали, простите?

Тикоцкий знал наверняка, что название наркотика пока вслух не произносил, но спорить опять не стал.

- «Цифра»,- сказал он.- Этот наркотик назовут «Цифра».

- Да, «Цифра»,- сказал Глеб Алексеевич.- Так вот, Саша, любой наркотик , должен вас заверить- никак не может быть бесплатным. Тем более такой, который, как вы утверждаете, почти сравняется с героином по ...ммммм... воздействию.

- Может,- тихо, но очень уверенно сказал Тикоцкий.- То есть сначала, когда наркотик только появится, он конечно же, будет стоить денег. И денег немалых. Я могу вам даже сказать, что группа... эм.. ученых, которая этот наркотик изобрела, успела сколотить на «Цифре» огромное состояние. Это даже привело к некоторому бардаку на рынках ценных бумаг... Сами понимаете, когда на бирже появляется крупный игрок и начинает вести себя неадекватно и борзо, ничего хорошего это не предвещает.

Тикоцкий остановился, глянул на главврача, увидел в его глазах недопонимание и решил немного пояснить:

- Ну хакеры, в сущности, наркотик изобрели хакеры, понимаете? Что они могут смыслить в экономике? Они наняли себе, конечно, консультантов... Но это как если бы, знаете ли, астрономы явились на бал в честь замужества герцогини. И герцогине неловко, и астрономы не знают, что делать.

Главврач с любопытством посмотрел на Тикоцкого. Этот громоздкий человек на первый взгляд производил о себе совершенно неверное впечатление. Иванову сразу показалось, что к нему на прием явился то ли охранник в супермаркете. То ли водитель дальнобойщик. Но стиль изложения этого мужчины подсказывал Глебу Алексеевичу, что нет, перед ним был скорее представитель интеллектуального труда.

- Ну я и говорю, что наркотик обязательно должен быть платным,- вернул разговор в предыдущее русло врач.

- Сначала,- ещё раз настоял на своём Тикоцкий.

- А что же случилось потом?- спросил Иванов.

Тикоцкий ухмыльнулся.

- Да что случается со всем контентом интернете? Случается то, что любой продукт рано или поздно в интернете становится бесплатным. Почему вы считаете, что электронные наркотики не могут быть бесплатными?

- Ну,- замялся врач.- Тут невредно было бы понимать механизм действия наркотика, чтобы вообще о чем –то говорить...

- Достаточно понимать, что это просто контент,- сказал Тикоцкий.- Это просто набор нолей и единиц, понимаете? Виртуальное пространство. Это не мак, который нужно хотя бы вырастить, потом собрать, потом сварить и переработать, а затем под страхом смертной казни перевезти через границу...

- Знающего человека видно издалека,- решился на шутку Иванов.

- Нет, никогда не имел дела,- ответил Тикоцкий. - Только из литературы, так, что-то очень поверхностное.

Главврач поднялся со своего места и стал ходить по кабинету.

- Ну, допустим, - в каком-то воодушевлении сказал он. Воодушевление это было вполне понятным- сейчас перед Ивановым Г. А. сидел интересный персонаж, с какой-то пусть и больной, но все же интересной историей. Глеб Алексеевич всегда охотно принимал такие вызовы. Жаль, вызовы пациенты бросали главврачу крайне редко.

- Допустим, этот наркотик, эта ваша «Цифра», в итоге станет бесплатной. Как всё в интернете,-снова улыбнулся Иванов. – Бесплатной и доступной.

Глеб Алексеевич прошелся по комнате взад и вперед.

- Я допускаю даже то, - продолжил он, - что действительно часть нашего с вами человечества вымрет от этого. Ничего человеку так не мило, как, мнэм… с вашего позволения будем использовать простые определения?

- Да, конечно,- не возражал посетитель.

- Так вот. Ничто более человеку так не мило, как «вырубать кайфы». Тут все верно, особенно если они будут бесплатными, особенно если они будут доступными. Да, я готов согласиться, что некоторая часть населения так и, простите, подохнет за своими компьютерами или... как там ваш наркотик нужно будет вводить, посредством чего?

- Смартфон,- ответил Тикоцкий.

- Ещё лучше, ещё удобнее, - сказал Иванов. - Не нужен даже мощный компьютер, можно кайфовать везде. Ну и скажем, под кайфом начисто, к примеру, забыть о приеме пищи. И даже умереть можно от голода- вы ведь утверждаете, что это почти героин?

- Да,- сказал Саша.- Утверждаю.

- Пусть! - Глеб Александрович в азарте сунул руки в карманы своего халата и оттопырил карманы перпендикулярно телу. Он делал так всегда, когда о чем-то интенсивно думал. Через несколько секунд Иванов продолжил.

- В конце концов, был прекрасный эксперимент с крысой, которой дали педальку с электродом, который вел прямо в центр удовольствий…. Умерла крыса. В общем, пусть! Пусть, разлюбезный Александр Николаевич! Тут уговорили.

Главврач озорно посмотрел на Тикоцкого, немного помолчал, чтобы Александр Николаевич смог оценить все его великодушие. Затем продолжил:

- Но, но, но, Александр Николаевич,- сказал главврач,- . Никогда. Вы слышите, никогда такая судьба не постигнет всю популяцию! Никогда не замрет всё человечество мухами в янтаре, которые только и делают, что «вырубают кайфы». Помилуйте, Саша, это чушь. Семь. Нет! Я даже дам десять процентов тех, кто погибнет от того, что появился бесплатный и безвредный цифровой героин. И это,- Иванов достал руку из своего оттопыренного кармана и поднял указательный палец, - это я даю ещё крайне много, широко даю, Александр Николаевич. От души даю. Вы меня понимаете?

- Понимаю, - ответил Тикоцкий. Он немного помедлил, потом сказал. – Но я и не говорил вам, Глеб Алексеевич, что человечество вымрет непосредственно оттого, что будет принимать без оглядки «Цифру». Случилось кое-что гораздо хуже.

Главврач склонил голову на бок и на секунду задумался, просчитывая варианты. Вариантов рождалось большое количество, но все они были какие-то неправдоподобные, поэтому Глеб Алексеевич быстро сдался.

- И что же, позвольте осведомиться, случилось?- спросил он.

- Когда «Цифра» стала бесплатной, - сказал Тикоцкий,- охват этим наркотиком популяции людей составил 90-95 процентов. В 2073 году у каждого был уже смартфон. У каждого в этом смартфоне был интернет. Понимаете, да?

- Ну, что же здесь непонятного, - улыбнулся главврач.- Дальше?

- А дальше, вот что. Начиная приблизительно с 2082 года стали рождаться дети, которые не выживали без «Цифры».

- Физически не выживали? - переспросил Глеб Алексеевич.

- Да, - ответил посетитель. - Не выживали именно физически. Врачи достаточно

долгое время не могли разобраться с тем, что вообще происходит. Сами понимаете, какая в это время уже была медицина- смертность младенцев около нулевая. Но выяснили. Исследования, анализ, эксперименты. И в конце концов стали спасать таких младенцев тем, что начинали давать им дозу «Цифры» прямо с рождения.

- Гм,- Глеб Алексеевич прошелся ещё раз по комнате, затем сел на своё место за столом.- Ну… Ну давайте допустим, что такое тоже могло быть. Вмешательство в работу мозга… причем долговременное, причем совсем не ясно, какой там задействован механизм…

Главврач откинулся на спинку стула, закинул руки за голову.

- Пусть. Этот поворот чисто теоретически тоже возможен. Но всё равно не понимаю- что было дальше? – Иванов разогнулся в своём кресле.- Году, эдак, в 2091?

- В 2091 году, Глеб Алексеевич, это явление превратилось уже в пандемию. А в 2107 году на Земле прекратили рождаться нормальные люди. В паре родителей, один из которых хотя бы раз пробовал «Цифру», уже не могло родиться ребенка, который не был бы «подсажен» на цифру с рождения.

- Погодите, погодите,- Иванов закрыл глаза и что-то сосчитал в уме- Ну даже если события развивались так, как вы говорите. Ну должно же было человечество забить в набат чуть ранее? Должна была остаться хотя бы узкая полоска людей, которые родились ещё нормальными, но не успели, так сказать влиться в ряды потребителей. Да обязательно должна была быть такая полоска, Александр Николаевич! От рождения до начала потребления должно быть расстояние ну хотя бы в 10-15 лет.

- Все правильно, Глеб Алексеевич. Человечество спохватилось. И сделало это даже гораздо раньше, чем вы думаете. Начиная где-то с середины века уже стали появляться общины, которые практически изолировали себя от внешнего мира и которые отказались от употребления любых цифровых технологий. Таких общин появились сначала десятки. А в конце концов и сотни. В некоторых из таких общин даже велась интенсивная научная работа с тем, чтобы как-то нейтрализовать воздействие «Цифры» на человека. Сделать человека невосприимчивым к наркотику, понимаете?

- Понимаю. Но я несколько о другом,- сказал Иванов.- Я о тех, кто родился, не успел потребить эту вашу «Цифру» и потом мог дать нормальное потомство. Насколько я понимаю здесь речь должна идти о миллионах людей!

- Никаких миллионов не было, Глеб Алексеевич,- сказал Тикоцкий.- Вы посмотрите на то, что делается уже сейчас. Смартфоны бездумно дают детям уже лет с трех. Неужели вы думаете, в будущем ситуация изменится?

- Гм,- снова сказал главврач. – В будущем ситуация, я думаю, не изменится.

- Да,- сказал Тикоцкий.- Так вот в будущем уже лет в восемь дети или умели обходить любой «родительский контроль» для того, чтобы получить доступ к «Цифре». Или с ними «Цифрой» делились одноклассники в школе, во дворе, в чатах, в сообществах. Не было никакой полоски, Глеб Алексеевич. Смылась.

- Ну…- врач задумался.- Ну… а эти общины. Что происходило с ними? Вы же говорите, что… эээ… человеческая цивилизация погибла?

- Почти погибла, Глеб Алексеевич,- ответил Тикоцкий.- Иначе зачем бы я к вам тогда сюда пришел.

Главврач хотел было действительно уточнить, зачем же к нему пришел Александр Николаевич, но возможности такой не представилось. Тикоцкий заговорил дальше быстро- было понятно, что он знает предмет, о котором говорит.

- Основная проблема всех изолированных общин,- сказал Тикоцкий,- была такой, что в них точно также рождались дети, которым уже была совершенно необходима с рождения «Цифра». И это были не единичные случаи. Это было много детей, совсем не малый процент в составе общины.

- Это происходило потому, что кто-то из тех, кто входил в общину, уже пробовал «Цифру»?- догадался Иванов.

- Да,- ответил Тикоцкий.- Что делать с такими детьми? Что делать с такими людьми? По уму- изгонять всей семьей из общины, чистить общину, делать её ряды совершенно хрусталь-

ными. Но, во-первых, в такой общине все или родственники, или уж во всяком случае друзья.

А во-вторых- такие меры привели бы к уполовиниванию любой такой общины. А может быть и вовсе к исчезновению.

- Значит, не выжили и общины? - спросил Иванов.

- Выжили, но не все,- ответил Тикоцкий.- Выжили те, кто хоть как-то сопротивлялся. Выжили те общины, в которых искали противодействие «Цифре»- но это уже немного другой вопрос, его мы касаться пока не будем. Я могу сказать, что таких общин на всей Земле выжило всего две.

- Любопытно,- сказал Иванов. Он снова встал, оттопырил карманы медицинского халата и заходил по комнате. - Любопытно. Но разлюбезный Александр Николаевич, всё равно я не понимаю, отчего вдруг должен всенепременно наступить закат человечества? Даже если допустить, что все произойдёт именно так, как вы излагаете… Ну будут теперь люди получать … мнээээ… «Цифру» с рождения… Что поменяется?

- А вы попробуйте подумать сами, Глеб Алексеевич,- предложил Тикоцкий.

- Ну, - карманы халата снова взлетели перпендикулярно телу. Врач прошелся несколько раз по кабинету, потом, наконец, предположил.- Сложно делать такие совсем уж умозрительные построения. Но я могу попробовать… Допустим, если ребенок с самого рождения уходит в мир, который будет нереальным, мир иллюзий… Он будет путать наш мир и тот? Не будет понимать, что тот мир иллюзорен?

- Бинго, Глеб Алексеевич,- сказал Тикоцкий.- Вы, Глеб Алексеевич- голова.

- Благодарю вас,- без тени смущения сказал врач.

- И как вы считаете,- спросил посетитель.-Какой из этих двух миров будет им милее?

Иванов постучал ручкой по столу в небольшом размышлении.

- Ну тут –то все ясно,- главврач положил ручку на стол и улыбнулся. - Сначала шах, потом мат. Пора ронять короля.

- Все верно, Глеб Алексеевич,- Тикоцкий наклонился ближе к врачу.- Эти поколения совершенно не понимали, зачем нужно трудиться, если погружение в другой, более прекрасный мир, происходит путем нажатия нескольких кнопок. И самое главное, Глеб- эти поколения совершенно перестали понимать, для чего нужно размножаться. Они воспринимали потомство как колоссальный труд. Выносить, родить, взращивать. Зачем? Зачем столько времени уделять миру, в котором так неуютно?

Глеб Алексеевич покачал головой.

- Да уж…- сказал он. - Рассказали вы мне страшилку.

Врач снова поднялся и пошел к окну, занавесить перед уходом штору.

- Так что же, кирдык, говорите, человечеству через лет сто, Александр Николаевич? - спросил Иванов.

Тикоцкий внутренне поморщился от шутейного поведения главврача и ничего не ответил.

- Давайте,- снова тогда взял слово главврач,- тогда прольём немного света на два немаловажных вопроса.

- Да, конечно,- с готовностью ответил Тикоцкий.

- Итак,- главврач снова уселся за стол.- Откуда, прежде всего, вам в таких подробностях известно будущее Земли и землян? И второе- почему именно ко мне вы с этим пришли?

Александр Николаевич взялся поправлять ворот своей рубахи. Он о чем то напряженно думал.

- Начать, наверное, следует со второго вопроса,- после паузы сказал он. - Как вы думаете, куда бы меня отвезли, если бы я пришел с этими сведениями… ну, скажем, в ФСБ?

Иванов улыбнулся.

- Я думаю, что таки к нам.

- Снова бинго, Глеб Алексеевич,- сказал Тикоцкий. – В нашем же случае я пришел к вам по записи, на прием, как психически нормальный, здоровый гражданин.

- Ну,- Иванов покачал головой и снова улыбнулся,- вас ведь никто не обследовал.

- И вы знаете, мне повезло с вами, - не обратил внимания на эти слова Тикоцкий. - Мне на удивление с вами повезло. Вы позволили мне рассказать эту историю. Мало того, вы были ею увлечены. - Не обольщайтесь, Александр Нико-

лаевич, - сказал главврач. - Рутинные вопросы, знаете ли, дело утомительное. А тут целая угроза человечеству. Куда как интереснее. Но должен вас предупредить. То, что я вас внимательно слушал и даже с вами спорил, вовсе не означает, что я вам верю и считаю то, что вы тут излагали каким-то документальным прогнозом на обозримое столетие.

- Это не важно,- тихо сказал Тикоцкий.

- Да? Ну, а что тогда важно?- спросил Иванов. - Для чего –то же вы мне все это рассказали?

- Для чего-то рассказал,- так же тихо ответил странный посетитель. – Понимаете… Есть такой слух, что о некоторых сумасшедших вы докладываете в ФСБ.

- Это про каких же?- главврач оставался невозмутим.

- Ну… К примеру, если будет похоже, что сумасшедший выбалтывает гостайну,- сказал Тикоцкий. – Или, если рассказывает о каких-то криминальных случаях.

- Интересно,- Глеб Алексеевич сложил руки на груди.

- Так вот, я бы хотел, чтобы вы обо мне доложили, Глеб Алексеевич. Как главврач, - Тикоцкий смотрел прямо на Иванова.- Обставить это можно даже так, как если бы я уже был вашим клиентом. Я согласен на госпитализацию. Скажем, я вижу и запоминаю некие галлюциногенные сны с информацией от человека из будущего. Ну или что-то в этом роде. Дадите мне галоперидолу.

Врач рассмеялся. Вышло несколько неуместно и врач смущенно оборвал себя.

- Зачем это вам, Александр Николаевич?- спросил он, снял очки и стал их протирать.

- Мне это затем,- ровно и размеренно ответил посетитель,- что сейчас ещё не поздно все изменить. Я знаю наверняка, что группа хакеров, которая придумала «Цифру» работала в России. И сейчас ещё не поздно спасти человечество.

От этих слов- самых, пожалуй, главных слов из всего того, что сказал за этот вечер Тикоцкий, у него на лбу выступили капли пота.

Главврач клинической больницы имени Гиляровского перестал улыбаться, одел очки и посмотрел на посетителя долгим взглядом.- Вы вот что, Александр Николаевич,- участливо сказал врач. Он поднялся с места, обошел стол и подошел к Тикоцкому. Приобнял его. – Вы, голубчик не представляете, в какое дело ходите ввязаться с этой вашей… То есть с нашей, госпитализацией. Вы, видимо не понимаете, что за этим вполне может, к примеру, последовать увольнение с работы… Вы, простите, в госструктуре работаете?

- В гос,- подтвердил Тикоцкий.

- Тогда почти наверняка- увольнение с работы. Совсем наверняка- лишение прав управление транспортным средством, вы управляете транспортным средством?

- Да,- ответил несколько побледневший Тикоцкий.

- Затем- постановка на учет в психоневралогический диспансер. Ну, а после нашего лечения- дообследования раз в три месяца в течении двух лет. Александр Николаевич,- Иванов сделал паузу.- Мой вам совет- не надо. Я же вижу, что передо мной здравомыслящий человек.

Тикоцкий ничего не ответил.

- Тем более, хочу вас уверить, Саша,- продолжал между тем главврач,- что докладываем «туда» мы действительно совсем уж в редких случаях. Ваш случай- совсем не такой, поверьте мне на слово. Его «там» не будут даже и рассматривать. Вы поезжайте домой, подумайте ещё раз обо всем хорошенько. Через меня прошла масса пациентов и я почти не сомневаюсь, что вы психически нормальный человек. Не ввязывайтесь вы во все это, Александр Николаевич.

Тикоцкий сглотнул. Затем встал. Затем пошел к выходу. И по его уверенным шагам к двери стало понятно- не было никакой решимости у Александра Николаевича во всем этом мероприятии. Ровным счетом никакой.

- Всего доброго,- сказал Тикоцкий спиной, затем открыл дверь и вышел.

***

Новый, 2020 год главврач клинической больницы им. В.А. Гиляровского Иванов Г. А. встречал в компании сокурсников.

Получилось это вот как - Женя Гасперский бросил в вайбер гениальную идею-снова собраться курсом на Новый Год и встретить его всем вместе. Дети у всех уже были взрослыми и сами разъехались на Новый Год кто куда, так что идея встретила бурное одобрение среди сокурсников.

Кто-то, конечно же, приехать не смог, но вообще получилось шумно и весело. Все друг друга не видели уже черт знает сколько лет и ресторан спустя час уже гудел от восторженных воспоминаний когда-то близких, когда-то друзей.

К двум часам ночи Глеб Алексеевич приличнo уже набрался и чуть не подрался с Денисом Соколовским, с которым имел счеты ещё с института. Соколовский постоянно к месту и не к месту поднимал еврейский вопрос - поднял он его и сегодня. Дело уже пахло жаренным, когда Глеб Алексеевич вспомнил вдруг, сколько им уже сейчас всем лет и рассмеялся. Рассмеялся следом за ним и Денис, сейчас уже седой и солидный заместитель отдела криптографии в Математическом институте Академии Наук. Вообще-то все они учились на четвертом факультете Высшей школы КГБ, из него вышли весьма видные программисты и ведущие мировые специалисты в сфере информационной безопасности. Глеба Алексеевича же «ушли» с последнего курса института - произошел с ним один «несмываемый» случай.

После этого Иванов выучился- как и его отец- на врача, и сделал карьеру в больнице Гиляровского. Сейчас он был не очень в теме цифровых технологий вообще и информационной безопасности в частности. Именно поэтому Глеб Алексеевич к трём часам ночи уже скучал, слушая разговоры своих старых друзей. Женя Гасперский видел, как грустит бывший сокурсник и предложил тост за медицину.

Глеб Алексеевич с радостью тост поддержал, выпил и решил, что раз уж тост за медицину, то нужно взять слово за общим столом. Но тогда, когда слово это ему предоставили, оказалось, что Иванов совсем не представляет, о чем говорить. Внезапно на ум пришел тот странный посетитель, что рассказывал о цифровом наркотике будущего. Вкратце главврач изложил суть того, что помнил из рассказа этого посетителя. И в конце своего пересказа шутливо обратился с вопросом к сокурсникам - что думает об этом цвет нации, отвечающий за безопасность страны?

За столом после этого вопроса повисла загадочная тишина.

- И что? - спросил Гасперский, в задумчивости ковыряя вилкой свой салат.- Он приходил к тебе ещё раз?

Гаспепрский, отщипнул совсем немного салата и отправил вилку с салатом в рот.

- Нет,- ответил Иванов.- Больше этого человека я никогда не видел.

- А адрес,- спросил Соколовский.- Ну или хотя бы фамилия, у тебя какие-то данные о нём есть?

- Нет, - ответил Глеб Алексеевич. Он уже несколько пожалел о том, что затеял рассказывать историю про этого посетителя. Иванов стал вспоминать всё, что знал о нём. - Александр Николаевич его, что ли, звали?

- Зря не позвонил,- сказал Женя Гасперский. - Ну хотя бы вот мне. Цифровой наркотик... Это уж по крайней мере интересно. И да. Откуда он всё это знает, ты выяснил?

- Нет,- ответил Иванов.- Он же ушёл.

- Ну, положим, это не он ушел, а это ты его надоумил уйти, - сказал Соколовский.- А ведь что-то в его словах есть, что-то знаешь... очень любопытное.

Тут главврач вспомнил о книге регистраций.

- Так это,- сказал он.- Я думаю, он регистрировался под своей фамилией. Всё же у нас фиксируется. Я завтра могу вам скинуть его данные. Только надо вспомнить, какого числа это было... А, помню, это была последняя пятница сентября, да-да-да, совершенно точно, последняя пятница.

Гасперский после этих слов распрямился, улыбнулся Глебу Алексеевичу, подмигнул и сказал.

- Вот и славно. Кинь мне эти данные завтра в мыло, пожалуйста.

- Не вопрос,- пожал плечами главный врач психиатрической больницы имени Гиляровского.

Женя же Гасперский поднялся, пошел к окну

и посмотрел в темноту новогодней ночи загородного ресторана.

- Ну что?- спросил Гасперский.- Время взрывать салют?