Российский государственный университет нефти и газа
(Научно-исследовательский университет) имени И.М.Губкина

Ткачева В.Л., Гриняев С.Н., Правиков Д.И., Фатьянов А.А., Шушкевич Ю.А.

Топливно-энергетический комплекс в эпоху становления цифровой экономики

Применение технологий цифровой экономики в энергетике

Москва
2019

АННОТАЦИЯ

В последнее время в публичном пространстве, в экономической теории и в практической деятельности отраслей национального хозяйства, в том числе топливно-энергетической, активно обсуждается внедрение элементов цифровой экономики. В этой связи, в рамках анализа процессов формирования цифровой экономики в ТЭК, авторами монографии рассмотрен комплекс вопросов, отражающих место России в глобальном энергетическом и информационном пространстве, анализируются стратегические и тактические приоритеты безопасного функционированию ТЭК, аргументируется необходимость усовершенствования системы комплексной безопасности объектов ТЭК в условиях цифровизации.

Монография рассчитана на научных работников, студентов, специалистов в области информационных технологий, управленческий персонал организаций и предприятий.

Авторский коллектив: Ткачева Вероника Леонидовна, доктор экономических наук, профессор кафедры «Административного и энергетического права» РГУ нефти и газа им. И.М.Губкина (Глава 2, параграфы 2.1, 2.2, 2.3); Гриняев Сергей Николаевич, доктор технических наук, декан Факультета комплексной безопасности ТЭК РГУ нефти и газа им. И.М.Губкина (Глава 1 полностью, Глава 4, параграфы 4.1, 4.2, 4.3); Правиков Дмитрий Игоревич, кандидат технических наук, директор Научно-образовательного центра новых информационно-аналитических технологий РГУ нефти и газа им. И.М.Губкина (Глава 3, параграфы 3.1, 3.2, Глава 4, параграфы 4.4, 4.5, Глава 6, параграф 6.2); Фатьянов Алексей Александрович, доктор юридических наук, заведующий кафедрой «Административного и энергетического права» РГУ нефти и газа им. И.М. Губкина (Глава 3, параграф 3.3, Глава 6, параграфы 6.1, 6.3), Шушкевич Юрий Анатольевич, кандидат экономических наук, главный научный сотрудник, заместитель руководителя ЦРКЦФА ВИНИТИ РАН (Глава 5 полностью).

ВВЕДЕНИЕ

Внедрение элементов цифровой экономики в отрасли национального хозяйства неразрывно связано с разработкой новых технологий, в том числе информационных. Так называемая информационная революция безусловно трансформирует деловой, финансовый мир и системы управления технологическими процессами. В этот период особо актуальными становятся вопросы информационной, финансовой и технологической безопасности отраслей хозяйства, воспринимающих цифровые тенденции.

В настоящее время цифровая экономика рассматривается как категория, объединяющая не только электронную торговлю и финансовые услуги, но и другие цифровые решения для бизнеса, граждан и государства в целом.

Цифровые (электронные) валюты – уже реальность нашего времени. Разновидностью электронных валют являются криптовалюты, создание и оборот которых связан с применением криптографических методов. Технология блокчейн (Block Chain, цепочка блоков транзакций) была создана именно для первой криптовалюты – биткоина, хотя сейчас уже имеет самостоятельное применение.

Несмотря на осторожное отношение многих правительств к виртуальным формам расчётов, вполне вероятно, в будущем именно цифровые валюты могут стать основными средствами платежа, в том числе при расчётах за энергоносители, включая углеводородное сырьё.

Топливно-энергетический комплекс России, обладая мощным технологическим, финансовым, научным и кадровым потенциалом, в своей хозяйственной деятельности, может выступить пилотным проектом формирования качественно нового состояния информационного пространства, включающего огромные массивы данных в цифровой форме базирующихся на безопасной информационной инфраструктуре.

При этом, безусловно, потребуется качественно новое направление развития правовой системы, связанной с обеспечением условий для создания прорывных и перспективных сквозных цифровых платформ и технологий. Перед правовой системой стоит непростая задача – осмыслить цифровые реалии и на основе существующих тенденций создать новые правовые средства регулирования общественных отношений и обеспечения развития страны в условиях цифровой экономики.

СОДЕРЖАНИЕ

ГЛАВА 1. РОССИЯ В ГЛОБАЛЬНОМ ЭНЕРГЕТИЧЕСКОМ И ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

1.1 Краткий анализ текущих развитий

Современный мир можно описать рядом тенденций, характерных именно для современного уровня развития техники и технологий. Одной из таких

тенденций является глобализация в плане энергообеспечения и применения информационных технологий. С другой стороны, управление добычей энергоресурсов, генерация энергии и ее распределение является залогом экономической независимости современных государств, и, как следствие, предметом конкуренции и геополитического противостояния.

Сегодня, спустя пятьдесят лет со дня создания глобальной сети Интернет[1], тотальная «сетивизация» общества привела к тому, что наряду с традиционными игроками международных отношений – государствами – все большее значение приобретают негосударственные структуры. Среди множества сфер жизнедеятельности общества на первое место выходит принципиально новая сфера – информационная. Более того, сегодня все чаще упоминается киберпространство, как принципиально новая сфера жизнедеятельности человечества в XXI веке[2].

Новой сфере жизнедеятельности свойственны как новый ресурс – информация, - так и новые противоречия, вызванные борьбой за обладание этим ресурсом. Соответственно зарождаются новые вызовы и угрозы безопасности государства. Эти угрозы в своей основе сетевые, охватывают, как правило, несколько сфер жизнедеятельности. Сегодня в экспертном сообществе все чаще говорят о появлении гибридных угроз – угроз, зарождающихся в одной из сфер, а реализующейся в другой или нескольких[3].

В условиях кардинального изменения самих принципов мироустройства под влиянием процессов глобализации особое место занимает вопрос обеспечения национальной безопасности. Как отметил в одном из своих выступлений Президент РФ: «…мир в целом находится в состоянии трансформации, очень мощной, динамично развивающейся трансформации, и, если мы вовремя не сориентируемся, если мы вовремя не поймём, что нам нужно делать и как, отстать можем навсегда…»[4].

Сегодня само понятие национальной безопасности как важнейшей функции государства трансформируется. **Созданная в соответствии с моделью угроз**

---

[1] Статья «Интернет», https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82

[2] Гриняев С.Н., Правиков Д.И. Основы общей теории киберпространства. Теория боя в киберпространстве / Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина. — М.: АНО ЦСОиП, 2018. — 124 с.

[3] Гриняев С.Н., Правиков Д.И. Основы общей теории киберпространства. Теория боя в киберпространстве / Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина. — М.: АНО ЦСОиП, 2018. — 124 с.

[4] https://ria.ru/20181208/1547660777.html

индустриальной эпохи система безопасности государства, рассчитанная на противоборство с подобными же структурами противника, не в состоянии справиться с угрозами нового времени.

Сегодня существенная доля всех противоречий между государствами перенесена в информационную сферу. Данное обстоятельство привело к трансформации подходов к понятию «военной силы». На смену «грубой силе» оружия приходит «мягкая сила» убеждения и психологической манипуляции. Реализация этого принципа требует пересмотра подходов к формированию военной стратегии новой эпохи. Доминирующая роль информации и информационных технологий, а также ориентация на парирование принципиально новых угроз информационной эпохи, заставили руководство ряда западных стран и, прежде всего, США активнее внедрять новые концепции строительства вооруженных сил. К таким концепциям относится концепция «сетевой войны».

На этом фоне Российская Федерация в среднесрочной перспективе, несмотря на осуществляемые попытки уйти от сырьевой зависимости, сохранит привязанность развития экономики к состоянию и перспективам использования топливно-энергетического комплекса страны[5, 6.]

Именно по этой причине, согласно Стратегии национальной безопасности Российской Федерации[7], одним из главных направлений обеспечения национальной безопасности на долгосрочную перспективу является повышение уровня энергетической безопасности.

В статье 12 Стратегии указывается[8], что развитие России сегодня происходит на фоне новых угроз национальной безопасности, имеющих комплексный взаимосвязанный характер. Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического, военного и информационного давления. В борьбе за влияние на международной арене сегодня задействован весь спектр политических,

5 Путин: зависимость России от сырьевой конъюнктуры все еще сильна, https://ria.ru/20101125/300658363.html#ixzz2tqLTQtAc

6 Послание Президента Федеральному Собранию, 12.12.2012, http://kremlin.ru/events/president/news/17118

7 Указ Президента Российской Федерации от 31.12.2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации", http://www.kremlin.ru/acts/bank/40391

8 Указ Президента Российской Федерации от 31.12.2015 г. № 683 "О Стратегии национальной безопасности Российской Федерации", http://www.kremlin.ru/acts/bank/40391

финансово-экономических и информационных инструментов. Гибридная война сегодня стала вполне реальной.

Стратегия развития информационного общества в Российской Федерации на 2017-2030 гг. была утверждена Указом Президента Российской Федерации от 09.05.2017 г. № 203[9]. Документ определяет цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Как определено в Стратегии, цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг.

По мнению авторов, цифровая экономика – это, по большому счету, параллельное формирование, а затем переход от одного экономического уклада к другому благодаря развитию новой технологической платформы "персональный компьютер - носимый компьютер - широкополосный мобильный доступ в сеть Интернет".

В настоящий период времени мы видим только некоторые контуры этого неумолимо надвигающегося процесса, который будет постоянно расширять диапазон своего воздействия практически на все общественные отношения, складывающиеся в экономике, и не только в ней. Что понятно уже сейчас: речь идет о новых, постоянно совершенствующихся способах получения различной информации и ее обработки. Поэтому можно смело сказать, что цифровая экономика представляется во-многом явлением информационным. Также очевидно, что опорной группой технологий, которые будут предопределять развитие отношений в области цифровой экономики, является Интернет в своих многочисленных проявлениях.

В марте 2018 года Президент Российской Федерации подписал Указ «О национальных целях и стратегических задачах развития Российской

[9] СЗ РФ. 2017. № 20. Ст. 2901.

Федерации на период до 2024 года»[10]. Указ предписывает правительству принять ряд мер «в целях осуществления прорывного научно-технологического и социально-экономического развития» страны.

Важнейшие из национальных целей заданы в первом пункте указа, в соответствии с которым правительство должно уже к 2024 году обеспечить (в том числе) выход на следующие показатели[11]:

- ускорение технологического развития страны, увеличение числа организаций, осуществляющих технологические инновации, до 50% от их общего числа;
- обеспечение ускоренного внедрения цифровых технологий в экономике и социальной сфере;
- вхождение России в число пяти крупнейших экономик мира, обеспечение темпов экономического роста выше мировых при сохранении макроэкономической стабильности, в том числе инфляции на уровне, не превышающем 4%;
- создание в базовых отраслях экономики высокопроизводительного экспортно-ориентированного сектора, развивающегося на основе современных технологий и обеспеченного высококвалифицированными кадрами.

В каких же условиях придется решать поставленные задачи? Как и каким образом обстановка в информационной сфере буде содействовать или наоборот, препятствовать, решению стоящих задач?

1.2. О ситуации в информационной сфере

По мнению ряда экспертов ситуация в области обеспечения национальных интересов в информационной сфере резко осложнилась после терактов в США 11 сентября 2001 года, когда эта сфера первые столь явно стала ареной противостояния государств с новым явлением международного терроризма, и к настоящему времени продолжает ухудшаться [2]. Все, что происходит, представляет собой не что иное, как борьбу за передел сфер влияния внутри принципиально новой сферы жизненно важных интересов современного

[10] http://www.kremlin.ru/events/president/news/57425
[11] https://www.rbc.ru/politics/07/05/2018/5af05f3a9a79472b558b1a4f

общества – в киберпространстве[12]. В этом переделе ключевая роль сегодня принадлежит США.

Понять глубину, характер, а также основные направления произошедших трансформации можно, если ретроспективно обратиться к некоторым аналитическим работам периода зарождения нового облика угрозы национальной безопасности.

Так, более 15 лет назад в рамках инициативы «Информационная революция» программы стратегических оценок Национального совета по разведке США аналитической корпорацией РЭНД был проведен ряд международных научных конференций и семинаров, в ходе которых изучалось и оценивалось мнение ведущих экспертов по проблеме трансформации общества под воздействием информационной революции.

Результаты проделанной работы были обобщены экспертами РЭНД в отчете «Глобальный курс информационной революции: общие вопросы и региональные различия» («The global course of the information revolution: recurring themes and regional variations», MR-1680-NIC), опубликованном летом 2003 года[13].

Исследование РЭНД на тот момент явилось заключительным этапом в многолетней программе работ, направленной на изучение феномена глобализации и информационной революции, движущих сил развития современного общества, анализ конфликтного потенциала и выявление потенциальных угроз национальной безопасности США в ближайшие 10-20 лет. Собственно, сегодня мы вполне обоснованно можем сравнивать тот прогноз с реальной картиной текущих развитий.

Интересно отметить, что уже тогда в исследовании отмечалось, что прогресс в информационных технологиях уже затронул большинство сфер бизнеса, государственной и общественной деятельности практических во всех регионах мира. Информационные технологии и связанная с ними информационная революция, превратились в один из наиболее значимых факторов, способствующих динамичной трансформации общества, его переходу от общества постиндустриального к обществу информационному. Стремясь наиболее полно использовать преимущества, которые несет с собой

[12] Гриняев С.Н., Правиков Д.И. Основы общей теории киберпространства. Теория боя в киберпространстве / Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина. — М.: АНО ЦСОиП, 2018. — 124 с.

[13] «The global course of the information revolution: recurring themes and regional variations», MR-1680-NIC, https://www.rand.org/pubs/monograph_reports/MR1680.html

информационная революция, американские аналитики пытались прогнозировать развитие информационных технологий, как на краткосрочную, так и среднесрочную перспективу.

Результаты анализа позволили выявить ряд характерных особенностей развития информационных технологий и влияния информационной революции, причем ряд особенностей характерен большинству регионов мира, а некоторые из них специфичны для отдельных регионов планеты.

Так, среди особенностей, характерных большинству регионов мира, стремящихся использовать достижения информационной революции, эксперты РЭНД отметили следующее.

1. Разработка новых технологий будет непрерывно стимулировать информационную революцию.

2. Информационная революция породит новые бизнес-модели, которые существенно трансформируют деловой и финансовый мир.

3. Информационная революция существенно затронет механизмы управления обществом и создает новых политических игроков.

4. Информационная революция останется многоликой, и будет формироваться социальными и культурными ценностями.

5. Сохранится многофакторная форма и характеристика национального подхода к восприятию информационной революции.

Кроме того, эксперты РЭНД прогнозировали тогда (в 2003 году (!)) следующее основные тенденции развития геополитической обстановки в мире в долгосрочной перспективе.

1. В ближайшие 10-20 лет США останутся в авангарде информационной революции.

2. Информационная революция в Европе будет развиваться медленнее и несколько иным путем, отличным от ее развития в США и Канаде.

3. В ближайшие 10-20 лет ряд стран Азиатско-Тихоокеанского региона продолжат стремительное развитие и масштабное использование информационных технологий.

4. Геополитические тенденции, которым содействует информационная революция, могут обозначить новые вызовы национальной безопасности Соединенным Штатам и другим развитым странам мира.

Поскольку темпы перечисленных технологических революций возрастают, а их синергетическое воздействие увеличивается, растет и понимание последствий их воздействия на общество. Эксперты РЭНД констатировали тогда, что в ходе указанных технологических революций сохранится неравенство отдельных наций и регионов планеты, более того ускорение темпов технологической революции приведет к углублению неравенства и как следствие – к небывалому росту напряженности во всем мире.

Вполне очевидно, что сделанный пятнадцать лет назад прогноз аналитиков РЭНД сегодня во многом оправдался [2]. Более того, по некоторым направлениям ситуация изменялась даже стремительнее, чем это ожидали сами исследователи. Очевидно, что недопонимание нарождавшихся негативных тенденций тогда, сегодня привели к формированию вполне сложившихся и осязаемых угроз безопасности новой природы.

1.3. Угрозы информационной безопасности Российской Федерации

Основной угрозой информационной безопасности для Российской Федерации являются планы ряда стран Запада и, прежде всего, США использовать свое превосходство, полученное в результате интеллектуального отрыва в организации и технологиях ведения информационной борьбы в едином глобальном информационном пространстве[14].

В последние годы в США активизировано проведение работ, направленных на реализацию национальной информационной стратегии. Цель проводимых работ – обеспечить подавляющее информационное превосходство путем навязывания информации, побуждающей высшее военно-политическое руководство других стран принимать выгодные для США решения. Ключевыми элементами в деле достижения целей национальной информационной стратегии является управление восприятием целевой аудитории и формирование «общественного мнения» путем манипулирования информацией. Основная форма достижения поставленных

[14] «Доктрина информационной безопасности Российской Федерации», введена указом Президента Российской Федерации от 5 декабря 2016 г. №646, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html

целей – ненасильственные действия и инициирование «бархатных» революций.

Очевидно, что цели национальной политики США будут достигаться путем ведения стратегического информационного противоборства с использованием атакующего информационного оружия. В качестве такового в последнее время все чаще рассматриваются не столько аппаратно-программные средства воздействия на информационные системы и информационный ресурс противника, а средства и методы манипулирования информацией. Об этом говорит анализ работ по данной тематике – в зарубежной прессе в последние годы возросло число работ по средствам и методам манипулирования сознанием (в частности, по методам нейролингвистического программирования, гипноза и другим методам суггестивного воздействия), исследованиям психологии личности и др. Появился ряд новых понятий, например - «реальная виртуальность», когда освещение некоторого события в прессе приобретает большую важность, чем само это событие.

Реализация подобных методов на государственном уровне требует пересмотра ключевых подходов к проведению внешней и внутренней политики государства в информационную эпоху.

Стремительное развитие информационного общества значительно увеличивает влияние информационной сферы на национальную безопасность страны.

Переход информации в разряд одного из важнейших ресурсов человечества, ведет к росту числа и интенсивности конфликтов в информационной сфере, направленных на завоевание и удержание господства над этим новым ресурсом.

Среди прочих факторов угроз национальной безопасности России в информационной сфере наиболее значимыми в ближайшие годы будут следующие.

Продолжающийся неконтролируемый рост масштабов глобальных информационных сетей. Уже сегодня ситуация в глобальных информационных сетях во многом вышла из под контроля ее создателей. Почти ежедневно в Сети появляются новые средства массовой информации, сайты различных радикальных группировок и др.

В последнее время информационное пространство все активнее используется террористами и экстремистами для координации своей деятельности, организации связи и привлечения финансирования. Осознавая потенциал, которым обладают новые информационные технологии, ряд международных террористических организаций в последнее время пытается устанавливать связи с глобальными сетевыми сообществами хакеров. Террористами ведется работа по возможному их привлечению в будущем для планирования и проведения террористических актов. Установление рабочих контактов между террористами и хакерами грозит резким скачком в технологическом развитии террористов, что может привести к тому, что террористы приобретут способность проведения масштабных терактов в информационной сфере уже в ближайшие годы.

Появление принципиально новых средств и способов доведения информационно-пропагандистских материалов до аудитории при ведении информационно-психологических операций. За последние годы стали широко использоваться такие новые медийные средства как спутниковое телевидение и радио, цифровое телевидение, электронная почта, средства виртуальной реальности и др. В армии США с октября 2001 года действует специализированный Центр стратегического влияния, в задачу которого входит координация действий по проведению стратегических психологических операций, в том числе с использованием новых средств массовой информации.

За последние годы резко возросло количество средств специального программно-математического воздействия на ресурсы информационных систем, при этом сами эти средства с развитием глобальных сетей стали широко доступны, что ведет к росту числа хакерских атак на информационные системы объектов критической информационной инфраструктуры. Во много раз увеличилось количество компьютерных вирусов, существующая антивирусная промышленность уже не справляется с возросшей нагрузкой.

Продолжается рост числа систем спутниковой связи и совершенствование их технических характеристик. За последние годы возросло число операторов спутниковой связи. Сегодня спутниковые каналы связи – неотъемлемая часть реализации новой военной доктрины США по проекции силы. Важно, что ряд официальных документов США закрепляет

приоритет этой страны в космосе[15]. Россия же до настоящего времени не может в полном объеме восполнить орбитальную группировку спутников связи и глобального позиционирования, а низкий срок службы отечественных космических аппаратов на орбите делает российскую связь малопригодной для использования в чрезвычайных условиях.

Развиваются научно-исследовательские программы по созданию технических средств манипулирования сознанием. По заявлению ряда информационных агентств, в последние годы получен ряд положительных результатов по созданию технических средств дистанционного управления животными (включая и человека), что в ближайшей перспективе грозит появлением нового класса угроз, связанных со скрытым воздействием на подсознание высшего военного и политического руководства страны.

Снижается квалификационный потенциал выпускников российских ВУЗов по специальностям, связанным с информационными технологиями. По мнению ряда специалистов в последние годы наблюдается снижение уровня подготовки специалистов в области информационных технологий, а также их выезд за рубеж[16]. Такая ситуация грозит тем, что в ближайшие годы Россия лишиться необходимого интеллектуального потенциала, без которого невозможна разработка и внедрение новых информационных технологий. Начиная с середины 80-х годов XX века хронически недофинансируются фундаментальные исследования. Сегодня Россия почти не имеет задела для будущего развития высокотехнологичной промышленности и вынуждена в значительной степени ориентироваться на импорт информационных технологий.

Трансформации современного общества, вызванные глубоким проникновением в повседневную жизнь информационных технологий, во многом есть объективный процесс, не зависящий от проводимой государством политики. Происходящие процессы столь фундаментальны, что несут серьезную угрозу всем, кто не воспринял новых условий. Причем темпы преобразований столь высоки, что, не учтя характера изменений сегодня, завтра догнать уже не будет времени и сил.

В этой ситуации в качестве базовой цели видится **сохранение целостности и государственного суверенитета, а также обеспечение условий развития**

[15] National Cyber Strategy of the United States, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

[16] «Рекрутеры выяснили причины отъезда российских IT-специалистов за рубеж», https://www.rbc.ru/rbcfreenews/5b168d0e9a7947958ec9dcf3

Российской Федерации как субъекта международного права в новых условиях глобального мира и формирования планетарного информационного общества.

К сожалению, говорить сегодня о возможности завоевания лидирующих позиций в новом миропорядке можно лишь с большой натяжкой.

Несмотря на то, что в России принят ряд программных документов, темпы их реализации не позволяют говорить о том, что разрыв, отделяющий Россию от остального мира, будет преодолен в ближайшее десятилетие.

Сегодня Россия по ряду показателей формирования информационного общество находится позади не только ведущих стран Запада, но и многих стран Азии (например, по числу суперкомпьютеров[17]).

Долгосрочные возможности развития и внедрения информационных технологий в России, сегодня также являются весьма проблематичными. За последние годы в стране сократилось число высококвалифицированных специалистов в области информационных технологий. Большое количество специалистов уехали на Запад. В этой связи остро встала проблема «утечки мозгов».

Опираясь на целый ряд футуристических прогнозов (в том числе и на приведенный выше прогноз экспертов РЭНД), в ближайшие 10-15 лет ситуация в России будет характеризоваться следующими изменениями.

В политической сфере.

1. Продолжится перенос общественно-политической деятельности в глобальную Сеть. Появятся новые сетевые политические образования, и даже партии. Возможно появление транснациональных политических объединений на основе Сети, которые будут оказывать влияние на деятельность сразу нескольких государственных структур. ***Основной политической силой становится не иерархическая партия, а негосударственное сетевое общественное объединение.***

2. Атомизация межличностных отношений, продолжающийся рост и развитие горизонтальных связей в еще большей степени возвысит потенциал «общественного мнения», как мерила эффективности деятельности госаппарата.

[17] «Среди 500 самых мощных суперкомпьютеров мира осталось лишь три российских», https://www.vedomosti.ru/technology/articles/2017/06/21/695300-superkompyuterov-rossiiskih

3. Продолжится рост и развитие электронных средств массовой информации. Политические кампании буду приобретать все больше виртуальности, побеждать на выборах станет не личность, а виртуальный образ политика, сформированного СМИ.

4. Оппозиционная деятельность также сосредоточится на использовании Интернет. Важнейшей транснациональной оппозиционной силой останется движение антиглобализма.

5. Продолжится углубление кризиса государственного и финансово-экономического управления страной, базирующегося на принципах и подходах индустриальной эпохи и не воспринимающей нововведения эпохи информационной.

6. Сохранение, а в отдельных случаях и углубление «цифрового неравенства» среди регионов страны.

В социальной сфере.

1. Сохранится социальное неравенство в обществе. При этом само общество претерпит глубокую кластерную (классовую) трансформацию: исчезнут некоторые прежние профессии и появятся новые, соответственно, новые профессиональные союзы и классы. Наиболее массовым по численности будет кластер наемных рабочих и корпоративных служащих – среда, наиболее восприимчивая к изменениям в обществе.

2. Продолжится снижение инновационного потенциала населения страны в следствие изменения демографической карты России, вызванного общим старением, снижением рождаемости, снижением продолжительности жизни, низким уровнем жизни в большинстве, так называемых, дотационных регионов страны, неконтролируемыми миграционными процессами из стран Средней Азии и Китая.

В финансово-экономической сфере.

1. Продолжится стремительная трансформация экономики под влиянием новых маркетинговых концепций «сетевой торговли» [1].

2. Ключевую роль займут электронные средства платежей, как на уровне юридических, так и физических лиц.

В промышленной сфере.

1. Сохранится ориентация на развитие сборочного производства на территории России.

2. Ключевые для становления информационного общества отрасли высокотехнологичной промышленности в России в обозримом будущем восстановлены не будут. Сохранится зависимость от поставок зарубежного оборудования и технологий.

3. Общий невысокий уровень развития информационной инфраструктуры в стране и ее неравномерное развитие по регионам.

В сфере науки и образования.

Сохранится многолетний провал в области фундаментального знания в области информационных технологий, ориентация на зарубежные нормативные документы и стандарты в области информационных технологий.

В сфере безопасности.

1. В сферу интересов преступности попадет новая цифровая экономика. Увеличится число противоправных действий с использованием информационных технологий и против объектов информационной инфраструктуры.

2. Экстремистские действия приобретут характер кибер-террористических. Произойдет слияние преступных хакерских сообществ с террористическими организациями. Возможно появление высоко-законспирированного преступного сетевого сообщества, аналога Аль-Каеды, но ориентированного на экстремистскую деятельность в глобальной сети.

Таким образом, предстоящее десятилетие будет нести в себе ряд принципиальных новаций в социальном устройстве общества, которые кардинально повлияют на характер как межличностных, так и государственных отношений.

При этом с учетом текущего состояния и возможностей России, **важнейшей будет являться не столько задача достижения лидирующих позиций в новом обществе, сколько сохранение «статус-кво» в принципиально новых условиях.**

Все вышеизложенное позволяет сделать вывод о том, что происходящие сегодня изменения в обществе весьма серьезны, они несут в себе мощный трансформационный потенциал, способный существенно преобразить ландшафт нового мира: изменения коснутся всех без исключения сфер жизни и деятельности человека.

Сегодня необходимо внимательно изучать происходящие изменения и вырабатывать собственное мнение по их полезности для общества. Нет ничего хуже, чем бежать за лидерами и слепо копировать их действия, не учитывая при этом национальной специфики. Тем более что мы имеем перед собой результаты ряда таких «подражательных» проектов: это и попытки копировать вычислительные комплексы IBM в нашей Единой серии ЭВМ, и попытка создания собственного космического челнока (кстати, американцы с неохотой, но все же вынуждены констатировать правильность нашего решения об использовании ракет-носителей). Да и сам проект «демократии», скопированный у нас в ходе «перестройки» показал свою несостоятельность.

Сегодня нет никаких оснований снова повторять исторические ошибки. Необходимо помнить о ряде фундаментальных принципов, определяющих успех или неуспех нового предприятия.

1. Государство есть надстройка над обществом, поэтому **государство не в состоянии формировать новое общество, оно может лишь не мешать и пытаться трансформироваться соответственно изменениям в обществе** (например, по типу «электронного правительства»).

2. **Современное, постиндустриальное общество сохранило традиционную основу общественных отношений – иерархию, новое общество базируется на принципиально новой, сетевой модели.** Это влечет за собой колоссальные изменения в экономике, политике, самой структуре власти, обеспечении безопасности и др. Также это влечет за собой и **изменение алгоритма выработки и принятия управленческих решений**.

3. В США в 90-х годах XX века информационное общество было практически построено, но **существенных результатов это не дало**, а привело к фатальному краху высокотехнологичных биржевых индексов. Надо делать выводы. **Сама по себе**

информационная индустрия ничего не дает, это локомотив, к которому необходимо цеплять вагоны, которые дают реальную продукцию, повышающую качество жизни человека. Как отмечалось выше, на западе такими «вагонами» сегодня считают биотехнологии, нанотехнологии и энергетические технологии. Все они не могут существовать без технологий информационных, но способны выдавать вполне конкретный продукт.

В условиях глобализации необходима кардинальная реформа системы обеспечения национальной безопасности Российской Федерации. Новая система должна быть способной адекватно отвечать на угрозы нового времени. Более того, сегодня в основу обеспечения национальной безопасности государства должна быть положена его информационная политика, определяющая национальные интересы и приоритеты в информационной сфере. Его внешняя и внутренняя политика должна строиться, базируясь на информационной политике государства. **Достижение и удержание информационного превосходства должно стать основой международной деятельности всех государственных структур Российской Федерации.**

Особое место в строительстве новой политической и государственной системы российского общества в информационную эпоху должны занимать вопросы, связанные со стандартизацией взаимодействия. Стремясь сохранить национальную самоидентичность и ментальные особенности русского народа, отраженные в системе подготовки научных и инженерных кадров, не следует однозначно воспринимать в качестве государственных стандартов те, которые создавались другим народом, с иным восприятием ценностей и подходом к решению стоящих задач.

В целом следует отметить, что во многом процессы глобализации объективны, и вызваны уровнем научно-технического прогресса, отказаться от многих достижений сегодня уже просто невозможно. Следует признать, что США и другие развитые страны одними из первых осознали преимущества, которые дает глобализация, и попытались выстроить модель нового глобального общества под собственные во многом эгоистические интересы. Однако уязвимость этой идеи очевидна – **устойчивое глобальное общество может быть построено только на основе сетевой, а не иерархической, структуры, в которой каждый узел будет равноправен в**

своих отношениях. За время, истекшее с начала агрессии против Ирака в 2003 году, США уже поплатились за свои амбиции, восстановив против себя более половины человечества. В этих условиях одной из насущных проблем становится выработка новых идей дальнейшего позитивного развития глобального общества и в этом вопросе Россия может и должна сыграть свою объединительную роль.

1.4. Проблемы безопасности биржевой торговли нефтепродуктами

Складывающаяся в последние годы благоприятная для России рыночная конъюнктура, начало реализации плана по масштабному совершенствованию экономики страны, позволяют говорить о начале нового этапа развития России. На этом этапе предстоит решить ряд важнейших задач, связанных с модернизацией существующих и созданием новых инфраструктурных проектов, существенно повышающих экономическую мощь и качество жизни в России.

У России – наследнице СССР - имеется богатейший исторический опыт в постановке и успешном решении колоссальных задач: от индустриализации 30-х годов XX века и послевоенного восстановления страны, до запуска первого спутника и полета человека в космос. Однако в отличие от имеющегося опыта, основанного в первую очередь на тоталитарных и административных механизмах, решать поставленные сегодня задачи необходимо с использованием исключительно рыночных механизмов. Одним из таких механизмов является биржевая торговля.

Западные экономисты определяют роль биржевой торговли, не как рынка, осуществляющего сбыт товаров, а как финансового института, облегчающего ведение торговли и удешевляющего ее. Причем по значимости формирование биржевой инфраструктуры приравнивается по значению к промышленной революции конца XVIII века, придавшей колоссальный импульс развития всей западной цивилизации.

Биржа - системообразующая часть рыночной инфраструктуры. Задачей биржи является организация, упорядочение, унификация рынков сырья, капитала и валюты. Именно консолидация под управлением единой биржевой инфраструктуры рынков капитала, валюты и товаров позволяет получить наилучший результат.

Важнейших функций у биржи две: организация рынка с помощью биржевого механизма, а также формирование и регулирование биржевых цен. Концентрация спроса и предложения на бирже, заключение большого количества сделок исключает влияние нерыночных факторов на цену, делают ее максимально приближенной к реальному спросу и предложению. Биржевая цена устанавливается в процессе ее котировки. Под котировкой понимают фиксирование цен на бирже в течение каждого дня ее работы, регистрацию курса валюты или ценных бумаг, цену биржевых товаров.

Биржевая торговля является механизмом стабилизации цен на рынке. Важным фактором стабилизации цен является гласность заключения сделки, публичное установление цен на начало и конец биржевого дня (биржевая котировка), ограничение дневного колебания цен пределами, установленными биржевыми правилами.

Характерен такой факт – как только та или иная страна вступала в ВТО, то практически сразу ее биржевая система поглощается одним из крупнейших глобальных биржевых игроков: американскими биржами NYSE и NASDAQ, скандинавской QNX, немецкой Deutsche Boerse. Исключением пока является лишь Китай, сохранивший суверенитет национальной биржевой системы после вступления в ВТО. ***Поглощение бирж лишает национальных производителей возможности формирования адекватных условий конкуренции на рынках.***

Понимая значимость и перспективность биржевой торговли для модернизации российской экономики и создания благоприятных условий конкуренции на мировых рынках, Президент России Владимир Путин в своем ежегодном послании Федеральному собранию еще в 2006 году предложил организовать на территории России биржевую торговлю нефтью, газом и другими стратегическими товарами. При этом он уточнил, что расчеты на такой бирже должны производиться в рублях, что является одним из важных факторов обеспечения стабильности национальной валюты.

«Это стало этапным событием в развитии биржевой торговли в стране. Для формирования организованного товарного рынка в России, создания объективных рыночных индикаторов по наиболее значимым сырьевым товарам в мае 2008 года зарегистрировано ЗАО «Санкт-Петербургская Международная Товарно-сырьевая Биржа». Работа по организации торгов на товарном рынке прошла несколько этапов. Это развитие спот-рынка нефтепродуктов, с достижением ликвидных показателей, расчет и

публикация индексов, охватывающих весь топливный спектр, которые стали признанными всеми участниками рынка, создание системы регистрации внебиржевых сделок. Произошел запуск срочных контрактов на СПбМТСБ, поставочных и расчетных, предоставивших российским участникам рынка новые возможности по управлению рисками.»

С одной стороны наша экономика уже созрела для интеграции в мировую биржевую торговлю. Так, по итогам 2006 года капитализация российского фондового рынка составила около одного триллиона долларов США, что практически равно значению ВВП страны за тот же год. Вместе с тем с другой стороны исторический опыт развития биржевого дела в России показал, что без государственного участия в этой деятельности невозможно достичь эффективных условий позиционирования российских товаров и акций компаний на мировом рынке.

Так известно, что Первая биржа в России была учреждена Петром I в 1703 году и открыта в Петербурге. В отстроенном специально для нее в 1705 году здании Петр лично установил часы биржевых собраний. Однако объективные условия не способствовали ее развитию. Через двадцать лет волевым указом 1723 года государь предписывал "приневолить" купцов к посещению этих новых коммерческих учреждений. Таким образом, в отличие от Запада инициатива создания биржи принадлежала не торговцам, а государству. Создание Московской биржи также связано с декретом императорской особы - Екатерины II. Указ "Об утверждении плана построения Гостинного двора с биржей при нем", подписанного императрицей в 1789 году.

После Октябрьской революции деятельность биржевых комитетов, как и самих бирж, была прекращена. Однако НЭП восстановил биржи в правах. Первые товарные биржи в СССР возникли в конце 1921 года. Большинство бирж, в соответствии с резолюцией IX съезда Советов, возникли как государственные, кооперативные или государственно-кооперативные. В условиях НЭПа биржам отводилась одна из важнейших ролей по стабилизации цен на ключевые продукты.

Следует отметить, что уже сейчас наметились тенденции по перегруппированию мировой банковской системы, снижению капитализации российских нефтяных и газовой компаний, реанимации и ревизии в пользу США прошлых международных соглашений.

В частности, за последние годы обстановка в финансово-экономической сфере двухсторонних отношений России со странами СНГ складывается для нашей страны в целом неблагоприятно и имеет тенденцию к дальнейшему ухудшению. Это грозит в ближайшем будущем кардинальным изменением интенсивности и направленности финансовых потоков, центром которых, до настоящего времени была Россия.

Подобное положение дел является следствием того, что в последние годы в ряде стран СНГ и иных государствах бывшего СССР (например, в Прибалтике) зародились и активно поддерживаются руководством этих стран проекты формирования, так называемых, «региональных финансовых центров».

Активно развиваются региональные финансовые центры в Казахстане (Региональный финансовый центр – РФЦА – в Алма-Ате), Латвии (основные направления его развития обсуждаются, в частности, в рамках Латвийско-американского финансового форума) и на Украине (формируется при поддержке Агентства по экономическому развитию США). Польша заявила о том, что стратегической целью ее финансовых кругов является построение регионального финансового центра для восточноевропейского региона.

В Украине в сфере борьбы за контроль над инфраструктурой фондового рынка наиболее активно работают немецкие и североевропейские компании.

В частности, скандинавская группа компаний OMX уже установила контроль над биржами прибалтийских государств, а также активно продвигается в инфраструктуру Армении, Казахстана и России.

Общая геополитическая цель всех этих проектов проста и понятна – максимально расширить сферу влияния американской валюты, включив в долларовые активы ресурсы республик бывшего СССР. ***Основным инструментом этой политики является перехват финансовых потоков из России и в Россию, прежде всего, от сделок по реализации российского сырья.*** Понятны и перспективы такого развития событий – в условиях падающего курса доллара и многотриллионного внешнего долга США, странам СНГ не избежать глобальных экономических кризисов, а возможно и потери части суверенитета.

С другой стороны, обладая уникальными запасами природных ресурсов, большой территорией, приспособленной для развития сельского хозяйства и создания эффективных транспортных коридоров «восток-запад» и «север-

юг», большими ресурсами пресной воды (которая в ближайшие годы может оказаться ценнее нефти), ***Россия вместе с дружественными странами СНГ (прежде всего, Белоруссией и Казахстаном) может стать не только экономически самодостаточным территориальным образованием, но и основным энергетическим и финансовым центром мирового уровня***.

Зарубежные «партнеры» России в последнее время крайне озабочены возможностью выхода российского бизнеса на международный уровень. Поэтому руководство ряда стран Европы (прежде всего, Великобритании, Германии, Франции) и США в последние месяцы предпринимают целый ряд согласованных действий, направленных на недопущение, в частности, приобретения российским капиталом крупных пакетов акций компаний и корпораций на территории Евросоюза и США. С этой целью существенно ужесточается контроль за иностранными инвестициями и регламентирующее законодательство, что ничего общего не имеет с рыночными принципами глобальной экономики.

В частности, в конгресс США был внесен законопроект, обязывающий все компании (не только американские), сотрудничающие со «странами-изгоями» (по американской терминологии), такими как Иран и КНДР, пройти процедуру делистинга (исключение из котировальных списков) на американских биржах, что автоматически ведет к необходимости продажи иностранными инвесторами принадлежащих им долей акционерного капитала таких компаний и последующего резкого ухудшения общего финансового состояния таких компаний. Подобная политика американских властей ведет к диктату с их стороны по отношению к иностранным компаниям, что представляет собой явную угрозу национальным интересам любой страны, подвергшейся воздействию подобных мер.

Кроме того, в СМИ появилась информация, что Британское управление по финансовому регулированию и надзору (FSA) намерено ужесточить правила проведения IPO иностранных компаний. FSA указывает, что требования к иностранным компаниям, акции которых представлены на Лондонской фондовой бирже (LSE), слишком либеральны, что увеличивает риски инвесторов. Заявления FSA коснуться, прежде всего, российских компаний, обеспечивающих основную долю размещений на LSE. Это, по оценкам экспертов, может привести к отказу ряда российских эмитентов от размещений на западных площадках.

Формально до 65% всех объемов торгов российскими активами приходится на Россию и лишь 35% – на Лондон. Однако из 65% значительная часть приходится на тех же иностранных инвесторов, которые имеют в России представительства. В частности, у ФСФР есть данные, что 70% всех оборотов российских бумаг приходится на нерезидентов, что составляет порядка 700 млрд. долларов США.

Важным является тот факт, что зарубежные инвесторы отреагировали, в частности, на обострение отношений между Россией и Великобританией летом 2007 года резким понижением котировок на бумаги российских компаний, причем падение составило почти 10%.

По мнению экспертов, в случае замораживания оборота акций российских компаний на иностранных биржах совокупный ущерб может составить более 100 млрд. долларов США (так, только на LSE обращается акций более чем на 50 млрд. долларов, а с учетом оборота российских акций на немецкой бирже Deutsche Boerse и на нью-йоркской бирже NYSE оборот российских акций превышает 100 млрд. долларов).

В целом, в мире достаточно широко распространены факты государственного участи и государственной поддержки фондового рынка.

Что касается, прежде всего, США, то в них роль государства в биржевой торговле и биржевой инфраструктуре на первый взгляд выражена не так явно. Но это лишь на первый взгляд. На самом деле биржа в США – это один из символов национальной культуры, основы американского государства. На бирже формируется капитализация американских компаний – нынешней основы мировой экономики.

Государственные кредитно-финансовые институты сыграли значительную роль в модернизации промышленной структуры в Японии, особенно на начальной стадии. За счет займов государственных финансовых институтов в 1955 г. финансировалось 32% закупок нового промышленного оборудования в японских фирмах, в 1965 г. - 16%, в 1980 г. - 17,6% и в 1990 г. - 8,1%.

Важное направление стимулирования государством инвестиционного процесса в странах Юго-Восточной Азии - регулирование уровня процентных ставок.

Государство активно участвует в развитии финансовых и товарных рынках в странах Ближнего Востока. Так, Объединенные Арабские Эмираты (ОАЭ) рассчитывают на звание крупного финансового центра.

В октябре 2005 года в эмирате Дубай начала работать международная фондовая биржа (Dubai International Financial Exchange - DIFX). Оператором биржи является компания компания Dubai International Financial Centre (DIFC).

Компания DIFC была создана три года назад правительством Дубая. По мнению аналитиков, правительство Дубая разрабатывает планы по превращению дубайской биржи в одну из крупнейших в мире. Чтобы добиться этого относительно быстро, потребуются сделки по слияниям с уже существующими площадками. Так, в 2006 году DIFC приобрела 3,5% акций Euronext, а также небольшие пакеты в банках HSBC и Deutsche Bank. В настоящее время биржа активно конкурирует с американской NASDAQ за право владения контрольным пакетом акций скандинавской биржи OMX – одной из группы бирж.

Кроме того, на товарной бирже Dubai Mercantile Exchange с 1 июня 2007 года начались торги по фьючерсам на поставку сырой нефти из Омана. Таким образом, в Дубае появится альтернатива контрактам на нефть марки WTI в Нью-Йорке и Brent в Лондоне, ведущим фьючерсам, по которым рассчитываются цены на все мировые сорта нефти. Этот проект осуществлен при непосредственном участии и поддержке правительства страны. При этом правительство эмирата уже объявило, что прекратит использовать действующий механизм цен при продаже сырой нефти и будет пользоваться фьючерсами с Dubai Mercantile Exchange. Правительство Омана также будет использовать новые фьючерсы для экспортных контрактов.

Все это еще раз показало наличие крайне высоких политических рисков размещения акций российских компаний на иностранных площадках, и вводит ***вопрос о необходимости государственных гарантий развития отечественного фондового рынка в число приоритетных***.

Кроме того, понимая важность и значимость контроля над рынком энергоресурсов, ряд ведущих западных стран и, прежде всего, США, которые не обладают достаточными природными запасами сырья, избрали путь установления собственного контроля над мировым рынком энергоресурсов – были взяты под контроль процессы формирования и сама инфраструктура

рынка энергетического сырья. В результате сегодня в мировой экономике сложилась ситуация, когда вся инфраструктура рынка – от формирования цены на энергоносители до реализации их поставки, и юридического обеспечения договоров контролируется США, а страны-поставщики сырья оказались лишены возможности участвовать в формировании цены на свой товар.

В частности, сегодня существует четыре биржи мирового уровня, на которых осуществляется торговля углеводородным сырьем. Это (в порядке уменьшения объемов сделок): Нью-Йоркская NYMEX, Американская Intercontinental Exchange (ICE), Сингапурская Singapore Exchange Limited (SGX), Токийская TOCOM.

Нефть, как биржевой продукт, стандартизирована. На сегодняшний момент существует два мировых стандарта нефти – Brent и WTI. Относительно этих сортов нефти с использованием системы дисконтов, зависящих, в первую очередь от качества нефти, формируется цена на иные сорта нефти, в частности, на российскую нефть Urals.

В ряде случаев рыночная инфраструктура используется в целях достижения внешнеполитических целей этой страны. В новейшей истории хорошо известны факты применения, так называемого «нефтяного оружия», когда в результате сговора арабских производителей нефти и администрации США, произвольным образом устанавливалась цена на нефть, что провоцировало глобальные экономические кризисы. Наиболее ярким примером применения таких средств экономического давления в XX веке стал развал Советского Союза и всего социалистического блока. И сегодня система ценообразования на российскую нефть Urals через котировки агентств Platts и Argus Media вызывает у российских экспертов серьезные подозрения в занижении цен через непрозрачную систему скидок/дисконтов за качество. Дисконт к биржевой цене эталонного сорта Brent, с которым котируется содержащая больше серы Urals, постоянно меняется, при том, что качество российской экспортной нефти остается постоянным. Естественно, возникает мнение, что этот дисконт может быть результатом манипуляций. Так, существующая система дисконтов на различные марки нефти ведет к тому, что Россия на экспорте нефти марки Urals теряет до 3 млрд. долларов в год.

Наряду с ужесточившейся борьбой на сырьевом рынке, активизировалась и борьба за доминирование в сфере фондовых рынков. Так, одним из наиболее ярких событий года является ситуация с поглощением европейской биржи

EURONEXT американской биржей NYSE. Следует отметить, что поглощение состоялось, несмотря на то, что лидеры ведущих европейских стран (Германия и Франция), а также представители Европейского банка высказались против подобного поглощения - давление со стороны США оказалось намного сильнее.

В последние месяцы возросло стремление иностранного капитала к проникновению в акционерный капитал и российских фондовых бирж.

Так, стартовал проект создания Международной биржи «Санкт-Петербург» с участием шведской группы компаний OMX. Об этом проекте можно сказать и то, что компания OMX сама завершает переговоры о возможном слиянии с американской биржей NASDAQ на условиях 72%(NASDAQ)/28%(OMX), что приведет к созданию второй (после NYSE-EURONEX) транснациональной биржи, под влиянием США, и в целом поставит под контроль США до 70% мирового фондового рынка.

Есть информация о переговорах ММВБ и немецкой биржи Deutsche Boerse об открытии в Германии филиала ММВБ по торговле акциями российских компаний за рубежом. Реализация такого проекта никак не способствует развитию рынка в России, а лишь стимулирует отток капитала из страны.

Заявлено создание Международной нефтяной биржи с участием американской биржи NIMEX в Санкт-Петербурге.

Важность вопросов стабилизации мирового и национального рынков отчасти подтверждается и тем, что российские предложения в этом направлении, сделанные на последней встрече лидеров G8, были отвергнуты - ***наши «партнеры» не намерены пускать Россию к управлению мировыми финансами и по-прежнему рассматривают их в качестве главнейшего инструмента управления мировой политикой***.

Наряду с вышеизложенными негативными тенденциями, в последние годы в ряде стран мира происходит осознание опасности, исходящей из факта сформировавшегося контроля США над глобальным биржевым рынком и биржевой инфраструктурой. В частности, страны Азии пытаются начать собственные биржевые проекты, которые хотя бы частично гарантировали им суверенитет и защиту от манипуляции их фондовыми и товарными рынками со стороны как целых стран, так и отдельных глобальных спекулянтов типа Дж.Сороса, известного в качестве одного из организаторов Азиатского финансового кризиса 1998 года.

Пришло, в частности, осознание руководством КНР опасности, связанной с бесконтрольной деятельностью иностранных спекулянтов на китайских биржах.

Так, с середины мая 2006 г. китайские биржи начали торги с 8 новыми парами валют, что направлено на диверсификацию валютного рынка. До этого в Китае проходили торги только 4-мя парами валют – юанями по отношению к американскому доллару, японской иене, евро и гонконгскому доллару. Эксперты ожидают, что этот шаг позволит Пекину подготовиться к ревальвации юаня, на чем настаивают США.

Китайские биржи сыграли и продолжают играть свою положительную сдерживающую роль и в условиях адаптации экономики КНР к условиям членства во Всемирной торговой организации (ВТО).

Иран также активно ведет работы по созданию собственной нефтегазовой биржи с расчетами в евро.

Однако, по результатам контактов с иранской стороной, в 2006 - первой половине 2007 гг., можно сделать вывод о том, что заявленное открытие нефтяной биржи не состоялось, причем в качестве основной причины можно указать на сложность отладки всего технологического цикла биржевой торговли: от заключения контракта до поставки нефти покупателю. Иранцам не удалось пока преодолеть возникшие трудности.

Все это еще раз и уже наглядно показало значение инфраструктуры фондового рынка в условиях современной глобальной экономики, важность наличия эффективных и гибких механизмов управления с целью недопущения либо минимизации последствий глобальных финансовых кризисов.

Таким образом ***складывающаяся геополитическая перспектива является наиболее благоприятной для реализации собственного проекта создания в России глобального финансового центра***.

ГЛАВА 2. СТРАТЕГИЧЕСКИЕ И ТАКТИЧЕСКИЕ ПРИОРИТЕТЫ ДЛЯ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ ТЭК В СОВРЕМЕННЫХ УСЛОВИЯХ

2.1.Экономические и правовые аспекты финансовой и энергетической безопасности при реализации глобальных межгосударственных проектов

Международное сообщество в лице государственных и политических лидеров, а также аналитиков по глобальным экономическим процессам, валютно-финансовым и военно-политическим проблемам, в настоящее время определяет состояние межгосударственных отношений как трудно прогнозируемые, с постоянно увеличивающимся числом рисков и вызовов, ломающих сложившуюся ранее экономическую систему, включая условия её безопасности.

Падает доверие к основным фундаментальным основам функционирования экономического и политико-правового взаимодействия, а следовательно, возрастает риск военно-силового вмешательства в процессы разрешения возникших противоречий, не только в региональных, но и глобальных направлениях.

Как известно, мировая экономика и мировой рынок при данном, существующем сейчас, способе производства предполагает наличие конкуренции, свободного перемещения товаров и услуг, а также капиталов и рабочей силы.

Однако, в последнее время, основные фундаментальные опоры давно устоявшегося способа производства с чёткой институционально-правовой его обоснованностью, подверглись серьёзным изменениям. А именно – валютно-финансовую и банковскую системы губит спекулятивный капитал, в том числе из-за огромного притока криминальных, а следовательно, неконтролируемых денег. Принцип конкурентности в экономическом и торговом взаимодействии замещается откровенным силовым или запретительным давлением, а в ряде случаев военной дестабилизацией целых регионов. На рынке труда, из-за массового перемещения людей, нуждающихся в социальной защите, давно присутствует правовой нигилизм.

Точка невозврата, в плане разноаспектной безопасности, практически наступила в таких регионах мира, как Ближний Восток, Северная Африка, Балканы, Украина и т.д.

Примером острой деформации и разбалансированности могут быть такие направления глобальной экономики и рынка, как энергетика и валютно-финансовая система, включая банковский сектор. Положение в этих направлениях усугубляется тотальной статистической и аналитической дезинформацией. Такую точку зрения высказывает и один из самых информированных аналитиков мира, Президент компании «Роснефть» Игорь Сечин в ряде печатных изданий, а также в докладе на саммите энергетических кампаний Петербургского международного экономического форума.

Так, им было отмечено, что «… аналитические службы не способствуют формированию рациональных ожиданий у участников рынка. … Очевидно, что проблема адекватной информации и взвешенного обоснованного анализа рынков превратилась в одну из острейших»[18].

Таким образом, можно определённо констатировать то, что на рынках углеводородов и, даже шире, энергоресурсов вообще, а также на рынке финансов уже произошла смена парадигмы функционирования взаимодействия непосредственных участников процесса.

Традиционно, основными регуляторами производства и потребления нефти был картель ОПЕК, а в финансовой сфере диктат принадлежал МВФ и ФРС США. Сейчас же, по мнению И.Сечина, с которым несомненно, стоит согласиться «… новая реальность заключается в том, что движение рынка всё больше определяется комплексом факторов, заключающим в себя доступность и качество ресурсов, впечатляющий прогресс в развитии и применении самых современных технологий физического рынка плюс развитие финансовых инструментов и финансовых технологий[19].

Не последнюю роль в формировании новых глобальных экономических парадигм играют кардинальные изменения и на мировом рынке труда, которые особенно негативно проявляются в связке – энергетика плюс финансы. В этих сферах нужна высокотехнологичная, непрерывная организация производственного цикла, а также качественный уровень

[18] Журнал «Эксперт» №26(933) от 27.06.2016г.,с.30-31
[19] Из доклада И.Сечина на саммите энергетических кампаний Петербургского международного экономического форума 2016г.

технологичного образования и профессиональной подготовки. При этом, уровень квалификации и рациональное использование часов рабочей недели находятся в определённом противоречии. Вместе с тем, продолжительность рабочей недели является показателем социального достижения.

По данным ОЭСР «Better life index», аналитиков Oxford University, Statista OECD, UBS исследование Prices and carnings и других аналитических, страховых и статистических служб возникла обратная тенденция. И, если XX век смог записать себе в актив социально-правовые достижения трудового законодательства, то в начале XXI века во многих, даже развитых странах, идёт процесс ликвидации социальных привелегий. Так, например, в Гонконге рабочая неделя составляет 50 часов, в Мехико- 45,5 ч., в Дубае- 45,7ч., в Токио- 41,3 ч.(для сравнения: в Москве-34,5ч., в Париже- 33,4ч.).

Европейский Союз, на официальном уровне, по-прежнему включат в список своего благополучия низкий показатель рабочей недели, но в реальности, трудовое законодательство пересматривается с молчаливого согласия общества (как в Германии, Польше, Италии), так и с сопровождением общественными беспорядками и демонстрациями (как во Франции, Бельгии, Испании).

Быстро меняющиеся условия на рынке труда способствуют увеличению вызовов для системы экономической безопасности в целом. В этой связи, перед мировым сообществом стоит задача формирования гибкого трудового законодательства, отвечающего реалиям нынешнего времени.

События в ряде европейских стран, как то во Франции, а именно упорное стремление профсоюзов сохранить щадящие условия труда, а также не менее упорное стремление власти и собственников бизнеса провести изменения в части увеличения продолжительности рабочей недели и увеличения пенсионного возраста, яркий показатель того, что система социального баланса почти разрушена, а это вызов системе внутригосударственной безопасности в целом.

По мнению ряда аналитиков, угрозы безопасности экономической стабильности растут лавинообразно. Параллельно с этим, идут дипломатические переговоры, военно-политические и экономические демарши, саммиты глав государств. Подписываются декларации, где скрупулёзно выверяются, координируются и, затем с необыкновенной

лёгкостью нарушаются интересы государств, межгосударственных объединений и регионов.

Одной из главных проблем для многих государств стали инвестиции. Инвестиционный «голод», то есть потребность в «длинных деньгах» напрямую затронула даже энергетические, казалось бы благополучные, отрасли экономики. При этом, мировая банковская система, обладая колоссальными финансовыми возможностями, для финансирования любого, даже суперглобального проекта, испытывает определённые сложности из-за «личных» капиталов, которые в определённой степени, деформируют банковскую мировую систему, наносят ущерб колоссальных масштабов налоговым системам государств и, как следствие, способствуют углублению социальной напряжённости.

Действительно, в плане наведения порядка в банковской системе, международное сообщество предпринимает определённые действия, но очень робко и непоследовательно. Видимо опасаясь испортить отношения со своими основными клиентами – «состоятельным гражданином и богатой компанией».

В этой связи следует отметить, что в настоящее время заработал международный стандарт «Automatic Exchange of Information (AEOI). Стандарт обязывает различные финансовые институты, как-то: банки, инвестиционные компании, страховой бизнес регулярно отчитываться о наличии счетов и движению финансовых средств по счетам своих клиентов.

К упомянутому стандарту вынуждены были присоединиться практически неподконтрольные ранее оффшоры. В их числе такие крупнейшие оффшорные территории, как: Виргинские, Бермудские, Каймановы острова, Панама, Кипр, остров Мэн и другие. Практически, к этому регламенту присоединились или находятся в процессе присоединения более 100 стран. Российская фискальная служба стала достаточно активно сотрудничать с 1 июля 2016 года, когда закончился срок предоставленной амнистии капиталам российских резидентов, которые разместили свои финансовые средства в зарубежных финансовых институтах. Теперь, держателям таких счетов предложено заполнять tax form, т.е. документ-обязательство. Кстати, документ достаточно сложный, рассчитанный на индивидуальный подход. Отказ от заполнения такого документа может служить основанием для разрыва отношений по транзакциям со стороны кредитной организации.

Вместе с тем, в мировой финансовой системе продолжает действовать американский аналог – система контроля за финансовыми потоками и налоговыми резидентами (FATCA), которая, мягко скажем, не особо обременяет отчётами крупный капитал.

Процесс жесткого регламентирования в мировой системе финансовых услуг, будет, по всей видимости, достаточно продолжительным. А это, конечно же, фактор негативного влияния на инвестиционные возможности.

При этом, как мы знаем, развитие экономик государств напрямую связано с активизацией инвестиционных потоков и внедрением новых технологий.

Необходимость инвестиций и освоения прорывных технологий, становится особо актуальной в настоящее время, когда происходит смена парадигмы развития и взаимодействия национальных экономик в глобальных процессах.

Суть новой парадигмы можно определить как **проекты объединения**. Такие проекты, с серьёзным участием Российской Федерации, уже существуют. Например, «Шёлковый Путь» или «Голубой поток». А также находятся в стадии активного проектирования - это: проект Продовольственной безопасности, гарантированной Сибирью и проект Строительства сверхскоростной трассы на Дальнем Востоке. И это далеко не полный перечень глобальных проектов, объединяющих для их реализации крупный капитал и технологические возможности ряда государств.

Традиционно Сибирь считается зоной рискованного земледелия, однако, в настоящее время, при наличии современных сельскохозяйственных технологий, обладая колоссальным объёмом энергетических ресурсов, Россия, реализуя проекты объединения, получает возможность освоения огромных пространств плодородных земель, имея при этом немалые запасы пресной воды в этом регионе (ставшей уже дефицитом во всем мире). К такому глобальному проекту, несомненно, должны проявить интерес государства, расположенные в климатически жарких зонах, страдающие от недостатка пресной воды.

В настоящее время считается, что конечным продуктом углеводородов является глубокая переработка нефти и газа. В новой парадигме развития – конечным продуктом станет объединённое использование таких ресурсов как: территория, энергетика, вода, рынок труда, центры высоких технологий (к примеру - космодром «Восточный»). А также, безусловно, финансовые и

другие экономические ресурсы государств, ориентированных на стратегическое партнёрство в глобальных объединённых проектах.

Более глобально конечный продукт можно будет определить как **перечень направлений стратегической безопасности России:**

- в территориальном отношении (например, совместные проекты с участием Японии могут нивелировать территориальные претензии по поводу Курильских островов);
- в продовольственной безопасности;
- в финансовой безопасности;
- в транспортной и информационной безопасности;
- в энергетической безопасности и т.д.

При этом, такой экономический подход активизирует взаимозависимость ряда государств, нивелирует возможные противоречия во имя получения сверхприбыли и социальных гарантий.

Фундамент новой парадигмы развития экономики, ориентированной на конечный продукт в виде совместного использования имеющихся ресурсов: природных, людских, энергетических, финансовых, технологических и др. практически уже заложен усилиями России и требует дальнейшего экономического и правового обоснования и регламентации, началом которого является глобальное сотрудничество в рамках Евразийского партнёрства.

2.2. Экономические и социальные вызовы и противоречия финансово-технологической революции

Финансовая технологическая революция (далее - финтех) (financial technology - fintech) коренным образом меняет, даже можно сказать - ломает, все сложившиеся к настоящему времени финансовые и банковские системы, их традиционные правила взаимодействия и, главное, их законы, зафиксированные в тысячах правовых источниках.

Сейчас финтех внедряется в банковские системы почти стихийно, т.к. руководство почти всех банков боятся потерять конкурентоспособность и действуют на опережение в плане продаж банковских и финансовых продуктов. Современные банки уже превратились в финтехкомпании,

которые пока с различной долей успеха осваивают секторальные инновации. А именно:

- финансовое планирование и управление финансами;
- предоставление акционерного и заёмного капитала;
- инвестиционное консультирование, управление активами;
- страхование и главное – формирование страховых пулов;
- платежи и переводы (это самые распространённые транзакции) и др.

Итак, вход в мир финансов финтех предлагает через компьютер, смартфон, другое устройство, которое можно обобщенно, используя определенную коннотацию, назвать гаджет. При этом, смартфон, для большинства участников финансовых операций , стремительно превращается из дорогого и непонятного гаджета в достаточно доступный инструмент.

Однако, единый механизм входа в мир финансов, посредством смартфона, предполагает продажи всех финансовых продуктов через единые платформы. На самом деле современное финансово-экономическое взаимодействие, не только на секторальном уровне, но даже, на уровне отдельной системы не позволяет создать роботизированный алгоритм на основе многофункциональной единственной карты для специализированного гаджета, с защищённым входом. Главным условием должен стать стабильный финансовый рынок и уверенность в том, что хотя бы в средне-срочной перспективе не будет глобальных экономических кризисов.

Возникает парадокс. С одной стороны финтех революция даёт банковским и финансовым системам неограниченные возможности для модернизации, но, с другой стороны, революционная стадия развития создаёт условия для дисбаланса при котором колебания рынка становятся непредсказуемыми и этим всё больше пользуются деструктивные силы, а именно: спекулянты и мошенники. При этом, надо не забывать, что существуют ещё и технические риски, в частности, зависимость от электрических сетей.

Тем не менее, финтех революция – это современная данность и поэтому менеджмент в таких секторах как: финансы, капиталы, банковские и финансовые системы должен поставить современные финансово-экономические «тектонические» сдвиги под обновлённое правовое обеспечение. Изменения должны затронуть и субъекты международного

права, в том числе, правовое регулирование деятельности международных финансовых организаций, правовое регулирование новых видов собственности (к примеру таких как – платформы, криптовалюты, распределённые реестры и т.п.).

Единая платформа, с единой точкой входа в финансовый рынок даёт одинаковые возможности для крупных банков и просто для физических лиц. Соответственно, для всех случаев, необходим адекватный регулирующий правовой механизм.

Возникают некоторые проблемы. Например, во взаимодействии субъектов в бесконтактных системах оплаты, которые, как известно, состоят из ряда своеобразных финансовых инфраструктур. Это - и наличие денег (можно на традиционном банковском счёте; счёте электронного кошелька или счёте на смартфоне и др.), и инфраструктура платёжной системы (например, Viza, Mastercard, Мир и т.д.), через которую со счетов, с использованием данных традиционной или виртуальной карты, идет собственно процесс по платёжным терминалам.

Таким образом, на одну денежную единицу (валюту) клиента в процессе платежей и переводов приходится несколько собственников и, главные из них – это инфраструктура платёжной системы и специальные токены.

Кроме этого, необходимо отметить, что финтех инновации пришли не только в сектора платежей и переводов, но и в онлайн-эквайринг, т.е. проведение платежей через Интернет по пластиковым картам, а также в онлайн (мобильное) управление оборотным капиталом, в P2P платформы (межпользовательские займы) и в страховой сектор и т.д.

Вполне логично то, что владельцы информационных технологий (ИТ) считают себя собственниками изрядной доли прибыли в ранее, вполне автономном финансово-банковском секторе экономики.

Переход к цифровой экономике, в настоящее время, определяет острую необходимость создания в опережающем режиме особого международного юридического кодекса, а, следовательно, статусного фундамента для реализации перехода к современному цифровому восприятию экономики. При этом, имеют место определённые несоответствия с устоявшимися ранее законодательно-правовыми отношениями и нормативной базой.

Прежде всего, это:

- появление новых форм собственности, пока не располагающих устойчивыми правами;

- стремительное изменение баланса распределения занятости на рынке труда, что вызывает социальную напряжённость;

- сложно контролируемое увеличение роста коммуникационных сетей, обоснованное не экономическими параметрами, а, скорее, финансово-спекулятивными перспективами роста.

Известно, что «цифровая» собственность весьма специфична. Она, создавая новую экономику, может, повышая процент своего участия, поглотить традиционную собственность. «Цифра» молниеносно может переводить акции в токены, которые работают уже не на бирже, а в собственном цифровом кошельке, где ликвидность значительно выше. Привлекательность для «кошелька» очевидна. Также очевидно то, что в этот законодательно-правовой вакуум устремились проекты, так называемые «однодневки», вытесняя вполне рентабельные, но долгосрочные.

Любителям быстрой спекулятивной наживы и теоретикам «от цифровой экономики» выгодно проявлять себя эксклюзивными знатоками перспектив развития мирового производственного цикла, тем более, что без современных цифровых гаджетов (компьютер, планшет, смартфон и т.д.) сейчас трудно решать проблемы не только экономического свойства, но и элементарно – в быту.

Справедливо возникает вопрос: как быстро надо переводить традиционную экономику в «цифровое» русло? И не потерялись ли цифры и факты истинного положения глобальной экономики в общем хоре восхваления цифровой экономики. А именно: то, что мировой ВВП в последние годы, в среднем, растёт на 2,3%, а мировой сегмент цифровой экономики (а это, более трёх триллионов долларов США или 5% мирового ВВП) практически не растёт (журнал «Эксперт», N 29, 2017г.).

Возможно, в ответ на спекулятивный ажиотаж, мировая экономика «включила» режим саморегулирования и, в дальнейшем, при наличии новых регуляторов и более благоприятном восприятии достижений высокотехнологичной революции большей частью населения, «цифра» даст другие, более адекватные технологическому развитию, результаты.

Глобальные и, особенно, региональные рынки товаров широкого потребления, промышленного производства и рынки трудовых ресурсов, пока не воспринимают однозначно «цифру» драйвером своего перспективного развития, в отличие от таких сегментов мирового рынка, как – рынок капитала и рынок услуг. Однако, даже в этих сегментах, новые финансово-инвестиционные схемы непосредственно зависят от уровня и качества жизни, от наличия свободных финансовых активов среднестатистического владельца информационно-цифровых гаджетов.

Информационно-цифровые гаджеты, с правовой точки зрения, являются собственностью того или иного физического или юридического лица, и, соответственно, защищены законом. Чего нельзя сказать о криптовалютных технологиях и их принадлежности какому-либо собственнику.

Так, например, сейчас в период быстрого освоения достижений финансово-технологической революции, по мнению специалистов, появилось значительное количество не достаточно обоснованных и защищённых краудверсий. При этом, очевидна необходимость их законодательного, или просто нормативно-правового обеспечения, которое явилось бы барьером мошенническим схемам крауд-инвестиций. Подобные схемы привлекают средний и малый бизнес обещаниями «процветания» без посредников и без больших затрат, а физических лиц – получением впечатляющих доходов. При этом, о рисках потерь всех вложенных в эти проекты средств – умалчивается.

Известно, что краудфандинг – это привлечение средств от частных лиц на развитие бизнеса. Краудфандинг – от английских слов: «crowd» - толпа и «funding» - вложение средств или финансирование. Площадка краудверсии – это новая коллективная собственность в денежном эквиваленте. Краудверсии, вместе с тем, находятся в зоне высоких рисков невозврата вложенных средств.

Современное банковско-финансовое законодательство не даёт чётко определённых регламентаций ни для инвестиций оформляемых по equity crowdfunding, ни по debt crowdfunding (equity crowdfunding – это вид краудфандинга, при котором реципиент продаёт определённую часть своего бизнеса донору (инвестору) или же просто предлагает долю в своей компании на условии долгосрочных инвестиций; debt crowdfunding – подразумевает вложение денег в обмен на определённую долю в будущем проекте или же в обмен на возврат инвестиций).

Более того, законодательство РФ даёт право осуществлять кредитные операции только кредитным организациям, имеющим лицензию ЦБ РФ на проведение таких операций и при этом регламентирует, что:

- кредитная организация – это юридическое лицо, которое основной целью своей деятельности имеет извлечение прибыли;

- кредитная организация осуществляет свою деятельность на основе специального разрешения – лицензии Центрального Банка РФ, которая выдаётся в полном соответствии с законодательством РФ;

- кредитная организация образуется на основе любой формы собственности, как хозяйственное общество;

Вместе с тем, на рынке финансовых услуг, сейчас активно развиваются новые формы кредитования без участия кредитной организации – и это данность времени «цифре».

Новые формы кредитования, в числе которых, например, – P2P кредитование – это метод осуществления финансовых операций при котором транзакции осуществляются без участия кредитной организации, а кредитором является физическое лицо.

Аббревиатура P2P расшифровывается как «Peer to Peer», что буквально переводится как «равный к равному» или же другой вариант «Person to Person», то есть « от человека к человеку». То есть в данной схеме отсутствует традиционный финансовый посредник, например, банк или другой финансовый институт, имеющий лицензию Центрального Банка РФ на проведение кредитных операций и правоотношения с которым очень чётко регламентированы действующим законодательством.

Займы предоставляются онлайн на вебсайтах специальных организаций, посредством специальных платформ кредитования и инструментов проверки кредитоспособности.

Считается, что важным элементом системы равноправного кредитования является возможность кредиторов диверсифицировать риски невозврата и просрочки по выданным суммам. Современные онлайн-платформы равноправного кредитования позволяют кредитору одновременно выдавать небольшие по размеру кредиты большому количеству заёмщиков. Таким образом, если выдано значительное количество кредитов, дефолт нескольких

заёмщиков не несёт критических последствий для всего кредитного портфеля и у кредитора сохраняется возможность получить ожидаемый доход.

Развитием такого кредитования является P2B кредитование, когда вместо заёмщика - физического лица выступает уже - юридическое лицо. При этом, имеет место усугубление нарушения существующего кредитного законодательства. А новые формы «цифрового» кредитования остаются вне правового поля.

Традиционно консервативные деловые отношения, законодательно регламентированные в банковско-финансовой системе, сейчас, буквально взрывает анархия IT-энтузиастов, стремящихся к сверхскоростному обогащению.

Необходимо, уже в настоящее время, активно разрабатывать регламентацию понятия: виртуальная финансовая собственность. Учитывая, что цифровая экономика призвана реструктуризовать классическую банковскую систему в том виде в котором она существует столетия в нечто новое «цифровое».

Внедрение новых высокотехнологичных и сверхскоростных средств делового общения конечно нельзя игнорировать, их нужно грамотно осваивать. Одним из условий такого процесса освоения технологий цифровой экономики является своевременная разработка их нормативно-правовой и законодательной основы. При этом, учитывая, что банковская система государства интегрирована в мировую систему, соответственно, подготовка правовых основ должна быть ориентирована не только на внутренние проблемы, но и на внешние, мировые тренды.

Быстрые изменения в научно-технологическом секторе, ломая старые стереотипы поведения, одновременно являются поводом для пересмотра социально-экономического взаимодействия технически подготовленных, а также управленческих слоёв общества с большей частью населения. При переходе к массовым цифровым технологиям, нельзя не учитывать факт социального неравенства населения как в части доходов так и в части уровня и качества образования.

При этом, такое социальное расслоение, как ни парадоксально звучит, может вызвать жёсткую конфронтацию сторонников и противников цифровой экономики не столько в пределах страны, но, в большей степени – на глобальном уровне.

Глобальные межгосударственная и бизнес управленческая элиты уже давно поделили всех на «развитые» в технологическом плане государства, «развивающиеся» и все остальные, которые, в целом, не принимаются во внимание, когда речь идёт о будущем «новом» порядке.

«Развитые» страны напористо позиционируют свой, не всегда объективно обоснованный, статус, якобы передового экономического либерально-демократического способа производства, нарушая, при этом, систему взаимного, обязательного исполнения международных норм и законов мирового рынка. Нарушают этику в конкурентном режиме сотрудничества.

До периода финансово-технологической революции, человечество долго, упорно и ответственно выстраивало систему коллективного общественно-социального договора, в целом, и по разным направлениям рыночных отношений. В частности, жёсткий регламент был выработан в системе регулирования мировым банковско-финансовым институтом.

Теперь, когда отчётливо наметился тренд на отказ от банковской системы, в её классическом виде, передав её функции отдельным, возможно, мини-компаниям, а возможно – роботизированным системам, наделив их управленческими функциями, объективно может возникнуть проблема изменения, на этой революционной основе, существующего ныне межгосударственного финансового порядка в целом.

Можно сказать, что вершины этого порядка, коими являются межгосударственные финансовые институты – МВФ (Международный Валютный Фонд); ВБ (Всемирный Банк); межрегиональные и специально ориентированные (например, инвестиционные) банки, теряют ряд функций из-за самого факта уже существующих технологических возможностей и достижений в организации финансовой деятельности.

Вышеизложенное также обуславливает необходимость разработки опережающего законодательно-правового и нормативно-регламентирующего поля для всего спектра функционирования капитала на основе новой цифровой данности, учитывая при этом, безусловно, приоритет государственных интересов в межгосударственных проектах.

В настоящее время сложилась ситуация, когда ряд существующих в банковском праве норм требуют внесения поправок, регулирующих оказание финансовых услуг через цифровые каналы. Сейчас, всё ещё актуальна личная явка клиента в банк (классический, а не виртуальный), в некоторых,

достаточно редких, случаях идентификация по фото (возможно селфи) или по каким-либо другим идентификаторам для населения не только в России, но и за рубежом. Выбор в пользу реального посещения банковского учреждения обуславливается как рядом социальных факторов, так и во многом, отсутствием гарантий безопасности и юридической защиты.

Социальные препятствия достаточно разноплановые. К основным, по нашему мнению, можно отнести: во-первых дисбаланс между возможностями финтех революции и реальной адаптацией к ней основной части населения, а во-вторых наличие множества мошеннических схем по отъёму денежных средств при использовании современных финансовых технологий.

Финансово-технологическая революция предполагает изменить, правильно сказать – коренным образом изменить сложившиеся на протяжении длительного времени, социально-привычные взаимоотношения в обществе, законодательно-правовую регламентацию в финансовом и банковском секторах экономики.

Финтех революция, скорее всего, «выбросит» из привычных экономических организационных схем, в том числе, активную и профессионально подготовленную часть специалистов, занятых в современном банковском производстве. И к этой данности надо тоже быть подготовленными.

Революционные преобразования, в целом, весьма привлекательны, но они сейчас не несут системного характера. В связи с этим, технические инновации, которые готов освоить финансовый и банковский сектор, на наш взгляд, необходимо встраивать в процесс модернизации, начиная с систематизации многих элементов функционирования общества.

Многие аналитики современного состояния экономики, особенно в производственной сфере, постоянно декларируют необходимость модернизации вообще, без конкретизации. Узкие специалисты понимают модернизацию как освоение инноваций в той или иной отрасли экономики или даже узко-направленного производства. Сообщество управляющих (менеджмент), особенно в сфере предоставления финансовых услуг, оперирует звучными новыми терминами «цифровой экономики» пытаясь найти нишу для конкурентности своих продуктов по формуле: «свои интересы превыше всего». В результате экономика получает продукт не от лучшего производителя, а от более изворотливого и, таким образом, трансформируется сама суть конкуренции.

Изменить такой современный «дикий капитализм» смогут только новые правила игры, а это не что иное, как законодательно-правовое обеспечение нововведений в финансовой сфере.

Реальная экономика требует стабильного инвестиционного цикла («длинных» денег), где дивиденды пока находятся в «туманной перспективе», а капитал банковско-финансовой структуры готов рисковать только процентами с транзакций, но с условием линейки услуг в оборотах – платежи и переводы. Микро-модернизация здесь просто «зашкаливает». Банки, на самом деле, считают себя прогрессивными глобалистами т.к. они встраиваются в мировые платёжные системы такие как «Visa», «Mastercard», «Samsung Pay», «Apple Pay» или же в компании финтех -стартапы, такие как « Fintech Lab» , которые через кооперацию банков помогают реализовывать проекты. Так, например, четыре российских банка «Санкт-Петербург», ВТБ 24, «Ак Барс», «Хоум Кредит» скооперированы с платёжной системой «Mastercard». Вместе с тем, любое объединение на глобальном уровне напрямую зависит от перманентных экономических рецессий, от финансовой прочности и стабильности резервных валют и от немотивированных политических и экономических санкций.

Несмотря на это, в настоящее время, прогнозируется количественное увеличение и рост активов финтех компаний за счёт ликвидации традиционных классических банков и, следовательно, ликвидации многочисленного банковского персонала. Таким образом, при переформатировании финансовых устоев, собственники отстаивают свои финансовые интересы явно в ущерб социальных прав населения. Этот факт можно рассматривать как определённый негативный вектор.

Но процесс финансовой модернизации может выстроить и ещё один потенциальный негативный вектор. А именно, непропорциональную аккумуляцию средств в сегменте торговли (услуги, платежи, переводы и др.), а не в большой промышленной экономике, которая может рентабельно функционировать только на значительном объёме основного капитала и у которой пока много нерешённых проблем по линии «цифровой» экономики.

Нивелировать возможные отрицательные явления в, целом, нужном и своевременном процессе финансовой модернизации, сможет специально адаптированная законодательно-правовая база как на международном, так и на государственном уровне. При этом, цифровая экономика и цифровая финансовая система могут активно потребовать цифровой правовой

регламентации новейших процессов. Однако, кардинальным, на наш взгляд, при этом становится вопрос возложения ответственности. Представляется, что ответственность, всё-таки, должна быть возложена на субъекты финтех процессов, а не на роботизированные системы, гаджеты или другие технологические инновации.

Индустриальная, затем информационная технологические революции, будучи драйверами развития глобальной экономики, не смогли дать проекту «глобализация» последовательного и сбалансированного решения социальных проблем.

Прежнему развитию общественного согласия мешает стремительно растущая поляризация между доходами и благополучием, с одной стороны, и безработицей с последующим обнищанием – с другой. Эта тенденция наблюдается не только внутри каждой отдельно взятой страны, но и между государствами и даже регионами мира.

Оптимисты от экономики теперь возлагают надежды на новую технологическую волну. На кардинальные перемены, которые сейчас получили название финансово-технологической революции. Справедливо отдавая свои предпочтения новым возможностям банковско-финансовым и сервисным технологиям, пропагандируя и внедряя их в сознание общества, игнорируются негативные социальные последствия. А именно, заинтересованность в инновациях значительно снижает внимание к возможным негативам в социуме, как это уже было в пиковых фазах индустриальной и информационной революциях.

На этапе формирования обществ индустриализации, затем информатизации – сообщество людей оставалось без законодательно- правового обеспечения распределения выгод от этих достижений на сбалансированной основе и без учета вклада каждой стороны общества, или на основе социальной необходимости.

Законодательно-правовое регулирование значительно отставало от внедрения технологий и на этой основе развития экономики.

Возможности цифровой экономики и финансово-технологической революции некоторыми аналитиками глобальных экономических процессов, воспринимаются чуть ли не панацеей от всех бед современной экономической рецессии. Совершенно уместно изучается положительный эффект инновационного вклада новых технологий в развитие всего

экономического процесса, но при этом остаются почти без внимания социальные, включая законодательно-правовые последствия. Например, инвестиции по принципу долевого участия, хотя они и отрегулированы в правовом поле, но в то же время являются достаточно рискованным предприятием.

Новые технологии в финансовой сфере уже сейчас могут изменить не только банковские системы в отдельно взятом государстве, но и глобальную финансово-банковскую структуру. Как известно, уже сейчас создано несколько международных консорциумов, которые считают целесообразным организовать такое экономическое пространство, которое на основе электронных инструментов обмена, помогут перераспределить значимость валютного функционирования в пользу новых «блокчейн-платформ» и криптовалют.

Инициатива создания новой, революционной банковско-финансовой деятельности уже в работе таких банковских объединений как консорциум R3 в США, состоящий из 43 значимых банков мира; Народного банка Китайской Народной Республики; Банка Англии; Швейцарского банка UBS; Немецкого банка Deutsche Bank; Сбербанка РФ и компании Qiwi, Citigroup и и Goldman Sachs, а также созданного в 2015 году Азиатского Банка инфраструктурных инвестиций (АБИИ).

Фундаментом стратегии нового типа банковской деятельности становятся взаимосвязанные технологии: финансовые проектные платформы и распределённые реестры активов. Автоматизированные финансовые платформы пытаются вытеснять посредников, т.е. банковские кредитные организации.

Разумеется, новые направления финансово-технологической революции ещё должны доказать свою необходимость и эффективность по отношению к уже работающим инновационным трендам. Решающим фактором в этой конкуренции, вероятно, станет заранее подготовленная правовая база. Защищающая новые формы собственности и, в частности, проектные платформы на основе больших капиталов, обеспечивающих длительные циклы экономического развития в межгосударственных инфраструктурных проектах: транспортно-коммуникационных, космических, энергетических, экологических, водных и т.д., уже не говоря о машиностроении, энергообеспечении и модернизации сельского хозяйства в каждом отдельно взятом государстве или регионе.

Стремительно внедряются в банковский понятийный аппарат определения новых смыслов, пока к сожалению, стихийно, вследствие этого новый термин понимается субъективно, и поэтому неоднозначно.

В сложных комплексах и при новых процессах оперативного учета движения активов, без опоры на адекватную, в данной ситуации, правовую основу не обойтись т.к. есть риск отставания в управленческих решениях.

Ситуация усложняется ещё и тем, что финансовая революция, особенно в плане создания криптовалют, предлагает избавиться от посредников, т.е. от банков в том их структурном виде, в котором они существуют ещё с эпохи Бреттон-Вудских и Ямайских соглашений прошлого века.

Распространение идеи создания криптовалют уже не остановить, следовательно, надо найти этой инновации правовое обоснование в геоэкономических процессах. Финансовая революция создаёт новое геоэкономическое пространство, которое должно базироваться на высоко эффективном взаимодействии различных инвестиционных платформ и электронных инструментах обмена. Вместе с тем, без правового обеспечения такое функционирование не возможно.

Финансовая революция предполагает расширение спектра вариантов при конфиденциальных договорных отношениях владельцев новых блокчейн платформ, однако, дальнейшая проработка документации пока остаётся в узких, в конкретном случае, рамках современных правовых институтов. Отказаться сейчас от привычной схемы взаимодействия, т.е.: реальная экономика (производство продукта) с финансово-банковской составляющей, без создания на правовой основе обновлённых распределённых реестров активов, достаточно сложно.

Финансовые аналитики отмечают тревожную, для основной массы населения, практически по всему миру, тенденцию снижения интереса к депозитарному процессу управления капиталом. Банки снижают процентные ставки по депозитам и увеличивают свои доходы через сервисные комиссии. Этот, практически, неконтролируемый процесс комиссионных доходов, в определённой степени продлевают «жизнь» банкам, как посредникам между частными комиссиями в сервисном обслуживании. Известный аналитик банковско-финансовой деятельности В.Фокеева отмечает: «Несмотря на то, что в нашем представлении банк – в первую очередь кредитор, сами банки весьма охотно, сами зарабатывают на функции посредника. Настолько

охотно, что непроцентные доходы, т.е. доходы, полученные не от выдачи денег в долг – формируют значительный кусок «пирога» (до 30-40%) в структуре выручки банков, как в России, так и за рубежом. При этом, существенная доля непроцентных доходов приходится на комиссионные…». И далее «… тем, кто считает, что российские банки берут слишком много комиссионных, стоит посмотреть, как на комиссиях зарабатывают американские банки: Citibank, Wells, Fargo Bank, Bank of America взимают по 3% от суммы зарубежной транзакции».

При этом, финансовые аналитики, и с ними стоит согласиться, отмечают, что этот ресурс у банков временный, т.к. его в перспективе может свести к минимуму финансово-технологическая революция.

Однако, в настоящее время, сервисно-платёжные услуги, дающие неплохой доход финансовым структурам, всё ещё являются трендом в плане увеличения капиталов посредников. Такие заинтересованные системы как «Master Card», «Visa», «Developer Center» и, даже, «WharsApp» и «Vider», которые тоже постепенно становятся платёжными, озаботились расширением инструментария управления личностных платежей.

Платёжные системы на основе клиринга, т.е. системы взаимных безналичных расчётов в двусторонних, многосторонних, внутренних (в каждой системе) и международных, а также в межбанковских и валютных отношениях осуществляются на основе существующего, и отрегулированного в правовом поле, документооборота. По мнению ряда специалистов, существующие рамки достаточно жёстко ограничивают процесс делового соглашения по соинвестированию многостороннего проектного клиринга. Более того, современные финансовые технологии могут заблокировать или привести к краху систему инвестиционных банков. Среди прочих факторов, это обстоятельство можно было наблюдать в кризисе системы инвестиционных банков в экономике США в 2008 году.

В то же время, реальное производство может предложить массу доходных проектов, в самых разных инвестиционных форматах: от малого и среднего бизнеса до проектов межгосударственного значения. Однако, современная банковско-финансовая система использует технологические достижения, в основном, для улучшения опять-таки сервисного обслуживания текущих индивидуальных расчётов.

Крупный банк, особенно это наблюдается в России, ограничивает вход инвестиций в свои компании, тем, что акции распространяются по подписке. Ограничителями поступления капиталов в реальную экономику являются, в разной степени агрессивности, налоговые платежи, а также, связанные с ними юрисдикции разных стран.

Однако, в последнее время, благодаря финансово-технологической революции, держатели финансовых активов всё чаще сталкиваются с уголовным законодательством, а именно – мошенничеством в особо крупных размерах. Россия в этих случаях – не исключение, о чём свидетельствует постоянный отзыв Центральным банком РФ лицензии на осуществление банковских операций, как у банковских, так и небанковских кредитных организаций.

Вследствие, определённой коллизии, законодательной базы с современными реалиями, практически провальной оказалась деоффшоризация и интеграция налоговой системы России в международную, а также присоединение, к далеко не совершенной, системе AEOI. При этом, AEOI нацелена на обмен информацией по проблеме происхождения денежных средств и других финансовых активов и их соответствия налоговой юрисдикции по форме tax form.

Конвенция организаций экономического сотрудничества и развития (ОЭСР) ограничивает транзакции с теми государствами, которые не подписали этот документ. Возникает проблема с зарубежными счетами в отношении договоров займа и кредита, доверительного управления средствами, особенно в тех случаях, когда, как в России, ими управляет нерезидент РФ. В этой связи, перевод клиентов в сферу отечественной платёжной системы «Мир» является серьёзным достижением отечественной денежно-кредитной политики России.

Но до настоящего времени, многие «оффшорные» россияне сталкиваются иногда с тупиковой ситуацией, при которой российское законодательство не упрощается, вследствие требований финансово-технологической революции, а, наоборот, усложняется. Первоначальный смысл законодательства теряется в массе подзаконных актов, которые могут привести собственника к административному, или даже, к уголовному наказанию. Зачастую разобраться в этих хитросплетениях и вернуться к первоначальному смыслу законодательства может только специальный консультант, т.е. ещё один

посредник между финансовым активом и реальной экономической необходимостью.

Вместе с тем, чёткая правовая регламентация пригодилась бы сейчас для формирования инвестиционных проектных платформ в важной для российской экономики нефте- и газоперерабатывающей отрасли. И не только в трубопроводном или обслуживающих секторах, но и в менее масштабных, но не менее прибыльных. Например, потенциально возможных, блокчейн платформах строительства региональных и районных систем по газоснабжению населения.

Мультипликаторами для создания цифровой экономики в России могут стать базовые компании нефтегазового профиля.

Флагман отрасли – компания «Роснефть», осуществляет стратегию взаимного сотрудничества импортёров и экспортёров нефти и нефтепродуктов с рядом государств, в том числе – Германией, Китаем, Индией, Ираком (Территория нефтедобычи – Курдистан) и другими. Сотрудничестово основывается на принципиальной позиции сбалансированного для всех участников процесса приоритета государственных интересов, а не только из интереса увеличения чистой прибыли для самих компаний.

В традиционной экономике прибыль и рост капитала всегда считались лучшими рыночными показателями успешности компании, даже, если она зарабатывает на демпинге и растрачивает при этом свой ресурсный потенциал. Но, анализируя возможности цифрового направления по развитию отдельных отраслей производственного цикла, можно прогнозировать то, что вслед за банковско-финансовой сферой и сферой услуг, начнут более активно переходить производственные сегменты экономики базовых энергетических отраслей и, прежде всего, энергетики углеводородов.

Российская компания «Роснефть», определив приоритетом своей деятельности государственный интерес, уже сейчас стала частью межгосударственной цифровой экономики. В частности, в последние годы компания активно занимается развитием своих НПЗ (нефтеперерабатывающих заводов), обеспечивающих продукцией розничный сегмент рынка, а это уже сфера услуг, которая использует возможности «цифры». В ряде межгосударственных проектов компания использует схему

BOOT (Build – Own – Operate – Transfer) т.е. : строительство – владение – эксплуатация – передача. По такой схеме, например, компания анонсирует свое участие в строительстве регионального газопровода в Иракском Курдистане, сырьё которого будет поставляться даже на европейский рынок и, в частности, в Германию.

Схема BOOT предполагает для компании реальное расширение рынка услуг, давно освоившим элементы цифровой экономики.

Не менее интересным является проект объединения импортно-экспортных задач трёх субъектов: России, Венесуэлы и Индонезии, которая в последнее время из-за истощения своих нефтяных пластов перешла из разряда экспортёров в разряд импортёров углеводородного сырья. В соответствии с проектными намерениями, оператором поставок нефти с месторождений Гыданского полуострова является «Роснефть», а индонезийская Petramina финансирует этот капиталоёмкий проект. При этом, предполагается совместное российско-индонезийское строительство нефтеперерабатывающего завода для переработки тяжёлой сернистой нефти и дальнейшей реализации его продукции на рынке.

Несмотря на использование альтернативных источников энергии, кстати, как правило очень дорогих и не всегда надёжных, углеводороды остаются драйвером экономического развития и потенциальным участником цифровой экономики.

Подобный опыт внедрения элементов цифровой экономики, может быть спроецирован на проекты и программы базовых компаний, т.к. такие проекты обеспечивают технологическую доступность, транспарентность, открывают новые возможности финансирования, расширяют сферу услуг в реальной экономике, включают продажу продукции в глобальную Интернет-платформу и, практически, совмещают в одном проекте функции как генерации энергии, так и потребления.

Основой должна стать стратегия создания новой модели сотрудничества, базирующейся на цифровой интеграции в направлении глобализации рынков товаров и услуг.

Необходимо принять во внимание то, что ряд проектов «Роснефти» территориально базируются в странах под сильным давлением политической нестабильности и угрозой нарушения «правил игры» на мировом рынке, где

применяется принудительное введение экономических и политических санкций.

В этой связи межгосударственные проекты России и Китая - особый , стабильный вариант развития сотрудничества в нефтяной и газовой отрасли, где вполне вероятно можно отработать, а затем закрепить в международном правовом поле кодекс применения элементов цифровой экономики при реализации энергетических проектов.

Китайские компании уже сейчас получают доли в акционерном капитале добывающих предприятий «Роснефти» в обмен на участие российской компании в капиталах перерабатывающих и сбытовых компаниях Китая, таких как CNPC и в её торговом представительстве China Oil, в компаниях Sinopec, Chem China и Beijing Gas. Особо хочется отметить компанию Beijing Gas, которая осуществляет поставки природного газа в наиболее развитые в промышленном отношении северо – восточные регионы Китая и в Пекин, а также расширяет импорт сжиженного природного газа (СПГ).

«Роснефть» и Chem China реализуют проект Восточной нефтехимической компании (ВНХК), который представляет сверхсовременный технологический кластер для поставок продукции на рынки АТР (Азиатско-Тихоокеанского региона).

Партнёрством России и Китая заинтересовался суверенный инвестиционный фонд QIA Катара, государства в Персидском Заливе, долгое время, находящегося под политическим давлением США.

Ускоренный переход на цифровую экономику зависит, в том числе, и от того, как быстро политическое давление будет блокировано новым международным юридическим кодексом, обеспечивающим чёткую реализацию задач цифровой экономики.

Финансово-техническая революция призвана существенно изменить направления банковско-финансовой деятельности, особенно в инвестиционных, оффшорно-налоговых и просто налоговом пространствах. Изменения уже происходят в платёжно-сервисных структурах, кредитно-залоговой банковской системе, во взаимодействии с кредитным посредником в части транзакций спекулятивного капитала.

Финансово-технологическая революция диктует новый подход в плане фиксации всех её требований, Этот современный феномен буквально

навязывает другую последовательность действий, В прежнем формате, во-первых было технологическое совершенствование отрасли экономики, а уже вторичным – законодательно-правовой и нормативный режим. Теперь же необходим другой подход т.к. крайне необходимо концептуально оформить новые формы собственности.

Привлекательность и, главное, целесообразность и доходность таких активов собственности как недвижимость, депозиты, предметы роскоши (яхты, самолёты, драгоценные металлы и др.) уже, видимо, в скором времени не смогут привлекать так, как участие в инвестиционных проектных платформах и распределённых реестрах собственности. А криптовалюты способствуют переориентации тренда развития экономики.

На заседании Валдайского делового клуба в 2016 году, В.В. Путин говорил о том, что «…готовых рецептов правовой, политической, экономической основы нового миропорядка сейчас нет, для их определения потребуется участие и государства, и бизнеса, и гражданского общества, и, в том числе, различных экспертных площадок».

Таким образом, поддержкой финансово-технической революции безусловно будет создание новых и использование уже имеющихся и действующих площадок обсуждения государственных и международных финансовых и экономических проблем.

2.3. Стратегические и тактические приоритеты функционирования передовых секторов ТЭК России в условиях цифровой экономики.

Энергетическая безопасность России, по всем параметрам, должна быть безупречно организованной и стабильной.

Наша страна располагает в достаточно серьёзным объёме всем комплексом энергетических ресурсов. Однако, только одни ресурсы и наличие технологических и инфраструктурных систем, созданных ранее для использования энергии углеводородов, атома, воды, возобновляемых источников не дают гарантии конкурентоспособности на внешних рынках, а, следовательно, безопасности.

Внутри страны определённые угрозы энергетической безопасности для экономики ещё более очевидны. Сейчас это особенно касается

электроэнергетического сектора, который находится в стадии коренных перемен, но, пока, не располагает адекватной, планируемому экономическому росту, концепцией реформирования на основе нового технологического уклада.

Стратегическая концепция развития электроэнергетической отрасли, включая и генерацию и сети должна, прежде всего, иметь две составляющие части: это научно обоснованный механизм устойчивости в отношении перспективных технологических вызовов и безопасность в плане конкуренции на мировых рынках.

Пока даже не определяются такие показатели, как баланс потребностей в генерации между дефицитом и профицитом; повсеместно наблюдается несогласованность потребностей производства и схем передачи электроэнергии, включая вопросы цены. Угрозой для безопасности функционирования отрасли является отсутствие регламентированного сотрудничества между генераторами всех видов генерации и сетевиками.

Россия на пороге экономического освоения, уже в самое ближайшее время, огромных территорий и, следовательно, остро встаёт вопрос создания электроэнергетических производственных мощностей в расширенных городских агломерациях и инфраструктурных системах. Всё это должно опираться на безусловную стабильность, которая исключает угрозы безопасности.

Некоторые государства, имеющие с Россией похожие климатические условия, такие как, например, скандинавские, отдают предпочтение теплоэлектроцентрялям (станциям ТЭЦ), которые производят одновременно электроэнергию, но, в основном, обеспечивают потребителя отоплением и горячей водой. Рентабельно ли применить такую практику у нас, например, в большинстве районов Сибири или Крайнего Севера, работающих зачастую в вахтовом режиме из-за большой удалённости от агломераций?

Безусловно опираясь на показатель рентабельности между отдельными производителями и потребителями в том или ином конкретном случае при создании режима комбинированной выработки электроэнергии и тепла можно обеспечить значительную выгоду. Однако, выгода одного субъекта экономического взаимодействия, может создать угрозу региональному рынку и, следовательно, привести к дестабилизации освоения большой территории,

где надо учитывать комплексное развитие самых сложных инфраструктурных и производственных систем.

Энергетическая концепция безопасности скандинавских стран не может быть равнозначной, допустим, планам и проектам КНР, которые дают электроэнергетической отрасли очень динамичный ускоритель развития, ориентированный на взаимодействие с Россией.

Новая геополитическая парадигма, возникшая в результате китайского проекта «Один путь – один пояс» осенью 2013 года, предложила мировому сообществу задуматься о приоритетах стратегического масштаба. Евроатлантическое сообщество (США, ЕС, Канада) почувствовали угрозу своему лидерству и включили в свою политику режим экономического удушения России через санкции и дестабилизацию политических отношений. Тем самым влияя на основную часть китайского геополитического курса, учитывая то, что значительная часть проекта будет нуждаться в энергетических ресурсах России.

Свою заинтересованность в вышеуказанном проекте уже обозначили около шестидесяти государств. При этом, основным партнёром и политическим союзником «одного пояса» будет Российская Федерация через весь Евразийский континент и «одного пути» по Северному Ледовитому океану.

В 2017 году на экономическом форуме в Давосе председатель КНР Си Цзинпин предложил мировому сообществу конкретный план глобализации на принципах равноправного партнёрства. В настоящее время Китай располагает огромными финансовыми возможностями. Его активы достигают 33 триллионов в эквиваленте долларам США, что, в свою очередь, примерно вдвое превышает активы США.

Ожидается, что 2019-2020 годы станут решающими для глобального российско-китайского проекта, т.к. уже апробирована, так называемая, практика опоры на «модельное проектное решение» на очень разных региональных участках: Египет, Кения, Афганистан и т.д. В этой связи и Китай вложил 16 млрд. долл. США в строительство скоростной магистрали Москва-Казань и сопутствующей инфраструктуры.

В противовес тому, что РФ и КНР дают мировой экономике гигантский шанс развития, часть евроатлантических государств очевидно будет создавать всё новые и новые препятствия посредством санкций, шантажа, дестабилизации, информационных войн и т.д., что, в свою очередь, может создать

масштабный массив угроз безопасности российской экономике и, прежде всего, энергетическим отраслям. С некоторой долей уверенности можно сказать, что через вышеуказанные воздействия на Россию наносится косвенный удар и по экономике Китая.

В настоящее время уже достаточно чётко определился внешнеполитический курс евроатлантического блока в отношении России. Это – ограничение страны в иностранных инвестициях, блокирование российских капиталов в банковских системах США, ЕС, Англии, Канады и др. и санкции, которые призваны ослабить взаимодействие российских компаний с ТНК (транснациональными компаниями) и ТНБ (транснациональными банками).

В такой напряжённой геостратегической ситуации, для снижения уровня угроз безопасности для всей страны необходимо выводить самую фундаментальную и в то же время самую уязвимую отрасль национального хозяйства – топливно-энергетический комплекс России, из-под давления экономических войн, финансовых и торговых ограничений на основе новой концепции развития и безопасности функционирования.

Концепция должна определить стратегические и тактические приоритеты развития. И, в частности, как пример, можно рассмотреть электроэнергетический сектор комплекса.

Стратегическим приоритетом в России – стране, которая является лидером по возможностям использования ресурсов для энергетики, является капитализация всех мощностей, особенно в электроэнергетическом секторе, а также по ресурсной логистике с учётом нужд мирового рынка.

Тактическим приоритетом можно считать добавленную стоимость в результате тщательно проработанных проектов по созданию новых объектов генерации, а также модернизации уже имеющихся, с учётом новых технологических возможностей.

Представляется очевидным и то, что угрозы безопасности для развития всего экономического и социального секторов страны проистекают не только от глобальной энергетической нестабильности, но и от концептуальной неопределённости стратегических и тактических приоритетов в практической деятельности и в управлении.

Экономика России сейчас испытывается двумя прямо противоположными геополитическими тенденциями: США и страны ЕС – санкциями, а КНР и

некоторые страны Востока предлагают масштабное партнёрское сотрудничество. При этом, сформирована уже готовая концепция такого сотрудничества: «После того, как в Китае утвердили новые концепции развития и определили инновации как движущую силу, торгово-экономическое сотрудничество между Китаем и Россией вступает в новую эпоху. Как стандарт рассматривается не только количество, но и повышенное внимание уделяется и качеству, что помогает удовлетворить жизненные интересы людей, стимулировать развитие торгово-экономического сотрудничества между двумя странами».

Новая эпоха уже обозначила свой магистральный путь, который, в основном, будет определяться финансово-технологической революцией (финтехом). Стратегический приоритет в данной ситуации – это наличие энергетического ресурса и, следовательно, у России уже есть возможность заплатить за эту технологическую революцию.

Экономическая политика, анонсированная в Послании Президента РФ В.В.Путина (март 2018 г.) аккумулирует все направления роста, при минимизации угроз безопасности всей системы в Новом общественном договоре. Новые проекты должны учесть множество запросов и одновременно подвергнуть глубокому анализу (на основе законодательно-правового регулирования) все существующие и возможные угрозы экономической безопасности.

Мировой рынок энергетических ресурсов слишком политизирован, при этом, зачастую не соблюдается международно-правовое регламентирование, что приводит к торговым войнам, даже при том, что потребность в энергетических ресурсах постоянно растёт. В связи с этим, стратегическим приоритетом развития всех энергетических отраслей необходимо обозначить их фундаментально-значимый статус.

Угрозы для стабильного функционирования энергетической отрасли исходят: во-первых, от политических амбиций конкурентов, которые практически ломают договорную систему взаимодействия, основанную на рациональном подходе; и, во-вторых, от постоянного спорного утверждения о том, что углеводороды, т.е. нефть и природный газ являются «тормозом развития страны», они якобы просто «сырьевая игла». При этом, принижается тот факт, что «сырьевая игла» помимо значительного наполнения бюджета, даёт не только себе, но и смежным отраслям технологический рост, т.к. передовой

научный уровень отрасли впечатляет своей грандиозностью, инновационностью и мультипликативным эффектом.

Сам факт постоянного употребления фразы «сырьевая игла» при игнорировании опыта добычи углеводородов ведущими российскими компаниями внутри страны и за рубежом, говорит о намеренном занижении инновационно-мультипликативных возможностей не только в сфере энергетической, но и смежных с ней отраслей. В определённой степени такие суждения без предоставления развёрнутого технологического анализа привносят определённую долю непонимания значимости процесса добычи углеводородного сырья для экономики.

Нельзя оставлять без внимания, в качестве негативного фактора для энергетической безопасности в целом, зачастую встречающуюся бюрократическую волокиту. Так например, известные трудности от «оппонентов» испытывает Иркутская компания «Гелиос», которая разработала и предлагает использовать прибор ДНМЭ (дифференциально-нормативный метод электроразведки), Благодаря этому инновационному подходу удалось достичь подтверждаемости «опережающего прогноза» на наличие углеводородов на уровне 80% (данные компании «Гелиос». Иркутский национальный научно-исследвательский технический университет), который считает целесообразным использовать методику ДНМЭ не только для нефтегазовой отрасли, но и для поиска твёрдых полезных ископаемых: золота, полиметаллов и алмазных кимберлитов (так называемых, кимберлитовых трубок). Метод поиска прошёл испытания в полевых условия – в поисках золота в Республике Горный Алтай, где эффективность составила 77% против средних по отрасли 30%.

Аналогичных примеров использования высокотехнологичных инновационных достижений, которые даёт нефтегазовое производство энергетической отрасли другим отраслям экономики, великое множество. Технологическое и инновационное обновление другим производствам даёт и глубоководные нефтегазовые платформы, особенно арктические.

Постоянно повторять «заклинания» о пагубности «нефтегазовой иглы» для экономики России, могут только те, кто заинтересован в том, чтобы любыми способами затормозить развитие этого канала технологических преобразований.

Топливно-энергетическая отрасль находится также на переднем рубеже программного обеспечения для обработки крупных массивов данных, математических моделей и апробированных методик для перехода на уровень цифровой экономики.

Не признавать этот факт и по-прежнему ссылаться на «нефтегазовую иглу», как на глубочайшее отставание российского технологического уровня от западного, значит дискредитировать проекты и программы экономического подъёма на уровень цифровой экономики. Уже сейчас, примеры внедрения «цифры» наглядно просматриваются в энергетической отрасли и на уровне её самой и в плане сотрудничества с логистической инфраструктурой самых разных направлений, включая сферу социально-государственного взаимодействия.

Торговые войны между государствами или отдельными макрорегионами, в большинстве случаев, начинались с борьбы за энергетические ресурсы и сопровождались манипулированием цен. В то же время, порядок и избежание хаотичности в сегментах мирового рынка обеспечивали такие международные организации, как ВТО, МВФ ВБ и т.д., которые должны были через законодательно-правовое регламентирование минимизировать возникающие проблемы.

В настоящее время, торговые войны ломают прежнюю договорную правовую систему, т.к. главными в новой парадигме международного взаимодействия становятся политические предпочтения. Политика направлена на сохранение прежнего ранжирования экономического уровня развития: т.е. на развитые ведущие державы; на развивающиеся и на, просто, экономически подчинённые страны. Длительная рецессия в странах, в основном, евроатлантического региона не изменила этот подход к экономическому порядку, а сопротивление новому направлению организации мировой экономики идёт по нарастающей, несмотря на то, что изменились приоритеты выживания и конкурентоспособности, прежде всего, в энергетической отрасли.

Энергетическая отраслевая экономика прошлого вида, в большей степени опиралась на государственно-стратегический приоритет, В настоящее время технологические возможности отрасли, на наш взгляд, диктуют сбалансированный подход в соотношении стратегического и тактического приоритетов.

Стратегический приоритет в развитии энергетики – это учёт роста мирового потребления в геополитических и геоэкономических направлениях крупных проектах глобального значения, таких как, например, российский проект технологического всеобъемлющего рывка роста экономики; китайского «ЭПШП» (Экономический проект шёлкового пути»; российско-японского освоения островов Курильской гряды; снабжение энергетическими ресурсами государств Европы через трубопроводы «Северный поток – 2» плюс создание рынка СПГ (сжиженного природного газа) на Евразийском континенте и т.д.

Тактический приоритет – это своевременное выявление, определение, предупреждение или минимизация рисков в развитии отрасли, а также угроз безопасности. Тактический приоритет в отрасли, т.е. в каждом отдельном направлении её функционирования имеет свои особенности, риски и угрозы безопасности, а, следовательно, и инструменты нейтрализации отрицательного влияния, даже на смежные отрасли.

Если говорить об электроэнергетической безопасности, то необходимо отметить тот факт, что она находится в прямой зависимости от природного ресурса, такого как уголь; природный газ, нефть, мазут и др.; от природных возобновляемых источников – воды, ветра, энергии солнца; от надёжности поставок специального атомного топлива. Наиболее существенной опасностью, на наш взгляд, для электроэнергетической отрасли сейчас является нестабильность глобального рынка, который находится в тисках во-первых, политических предпочтений конкурирующих сил, во-вторых, финансовой технологической революции и, в-третьих, технических возможностей долгосрочного накопления электроэнергии. при этом, технологичные разработки долгосрочного и бесперебойного резерва электроэнергии находятся в стадии научных поисков, или на этапе военно-стратегической засекреченности, как ядерная энергоустановка для российской крылатой ракеты с неограниченным энергоресурсом. Таким образом, безопасность одной из самых значимых для развития человечества отрасли зависит от дальнейших научно-технологических достижений, от финансовой нестабильности, от экономического шантажа; от региональных военных столкновений за обладание ресурсами, а также от того, что стремительно разрушается прежняя законодательно-правовая регламентация взаимодействия.

Законодательно-правовая основа подвергается сейчас разрушению как в глобальном масштабе, так и на государственном уровне. Объясняется эта тенденция необходимостью реформирования отрасли, или политической независимостью от ресурсной базы. Однако, чем бы не объясняли манипулирование правовой регламентации – всё привносит в отрасль дестабилизацию и риски в плане безопасности.

Основная опасность, как представляется, заключается в том, что и генерация, и оптовики, и сети, и розница по продажам, могут, каждый, исходя из своих, зачастую необоснованных производством и сбытом, интересов, манипулировать ценами. Таким образом, возникают риски для социально-экономической безопасности из-за стремления обогатиться, особенно в плане бесконечного повышения тарифов. Создаётся ситуация кризиса как в производственно-сбытовой цепочке, так и, что значительно опаснее, в социальной сфере. Угроза безопасности для внутреннего бесперебойного функционирования сегмента отрасли грозит угрозой, в целом, социально-политическому климату в стране. Регламентирующие инструменты, а именно: планирование покупок на оптовом рынке, клиентские сервисы, индивидуальные контракты и практика совместных решений, до сих пор не могут разрешить возникающие коллизии.

Одной из проблем, связанных с безопасностью электроэнергетической отрасли можно считать и отсутствие чёткой правовой регламентационной основы перехода от стратегии создания единой электроэнергетической системы советского периода к стратегии распределённой генерации и, соответственно, собственности на сети, которые, чтобы выжить в жёсткой конкурентной среде, должны опираться на баланс спроса и предложения.

Последние десять лет, как минимум, отметились тем, что модернизация отрасли свелась к реализации идеи распределённой генерации. Был отработан и предложен документ: «Договор на поставку мощности» (ДПМ), который стал специальным инвестиционным инструментом, законной гарантией реализации программы модернизации энергетической инфраструктуры отечественной экономики. По данным Минэнерго РФ в объекты генерации всех видов (гидроэнергетика, атомная энергетика, объекты теплогенерации и т.д.) за вышеуказанный период было вложено около 3,6 триллионов рублей; к концу 2017 года построено 130 генерирующих производств, суммарной мощностью более 27 ГВт, т.е. почти 11% от всего энергетического потенциала страны. ДПМ решил проблему

дефицита электроэнергии, которую предсказывали аналитики, принимая во внимание изношенность оборудования. Вопреки ожиданиям, возник даже некоторый профицит, но при этом произошёл раздел энергетической централизации РАО ЕЭС на две части: генерацию и сети. Новые субъекты генерации раздробленной системы должны были в очень короткие сроки построить станции и получить за это надбавку к тарифу в 14%, что по прогнозам, позволило бы им за десять лет окупить инвестиции. Государственные деньги, вложенные в проект ДПМ оказались весьма доходными, а, следовательно, привлекательными для бизнеса и, в связи с этим, энергетическая реформа стала пропагандироваться в вариант ДПМ-2. Особую заинтересованность к «Договору на поставку электроэнергетических мощностей» стал проявлять бизнес по возобновляемым источникам энергии. Российская компания «Фортум», на основе инвестиционного фонда развития ветроэнергетики, созданного в содружестве с компанией «Роснано», в январе 2018 года поставила на оптовый рынок электроэнергии и мощности (ОРЭМ) 35 МВт, затратив на первую в РФ ветрогенерацию 65 млн. евро., при этом имея преференции, выражающиеся в том, что компания «Фортум» будет получать гарантированные платежи за мощности в течение пятнадцати лет.

Энтузиасты возобновляемых источников энергии прогнозируют, что в самое ближайшее время, они могут заменить углеводороды и станут доминировать на оптовом рынке электроэнергетики и мощности. Такие прогнозы имеют своё некоторое основание в виде технологических возможностей и относительной доступности строительства и обслуживания этих объектов генерации, а также их локализации. Доводы в пользу возобновляемых источников энергии – ветра и солнца, подкрепляются и стоимостью 1КВт, якобы, вполне себе конкурентной. Разработчики ветроэнергетики в России, а это компании «Фортум» и «Роснано» , уже получили право на строительство объектов ветрогенерации одной тысячи меговатт (1000МВт) мощности до 2022 года.

Однако, пока трудно сказать, сколько будет стоить землепользование, особенно земель сельскохозяйственного назначения, и сопутствующее технологическое обустройство, включая необходимость соблюдения режима безопасности объектов. При этом, малая генерация снижает стоимость киловатта, и, в связи с этим, потребителям среднего бизнеса будет выгодно переходить на строительство собственных генерирующих объектов. Возникнет дилемма, стоит ли переходить на десятки тысяч автономных генераций, а, следовательно, ликвидировать сети регионального значения,

которые помогают продавать излишки через единую энергетическую систему.

Да и климатические условия на большинстве территорий РФ далеки от идеальных для развития энергетики солнца и ветра. Россия, как известно, не очень солнечно-ветренная страна и, видимо, деньги, полученные по ДПМ-1, пока использовались скорее для научно-технологического эксперимента, как представляется, дорогостоящего.

Влияние негативных факторов требует особенно тщательного изучения и анализа, т.к. велика вероятность роста тарифов и угроз безопасности в электроэнергетической отрасли в целом. Минимизация таких угроз возможна при наличии чёткой законодательно-правовой регламентации, которая сможет сбалансировать экономические интересы бизнеса и социально-политические интересы общества.

Правовая регламентация должна отрегулировать также вопросы продажи излишков генерации без посредников, как соседним регионам, так и зарубежным потребителям. В частности: Белоруссии, странам Закавказья и Прибалтики.

Таким образом, сейчас необходим глубокий анализ, на предмет включения этих генераций в тактический приоритет реформирования электроэнергетического сегмента топливно-энергетического комплекса. А, связанные с этим инвестиции, можно отнести в разряд венчурных.

«Малая энергетика», конечно же, заслуживает особого внимания. Но, вместе с тем, Президент Российской Федерации в своём Послании в марте 2018 года обосновал главный ориентир стратегического развития экономики, а это: «Гармоничное пространственное развитие всей территории страны. Нефорсированная модернизация экономики с опорой на развитие инфраструктуры, социальный сектор, ВПК, инвестиции и экономический рост.»

Концепция реформирования посредством объединения больших территорий, несомненно, станет стратегическим приоритетом энергетической политики. К примеру, в проекте «Енисейская Сибирь», экономическая синергия объединит три субъекта электроэнергетической мощи для пространственного развития России. Это - Красноярский край, Тыва и Хакассия.

Промышленность, сельское хозяйство и социальная сфера находятся в прямой зависимости от услуг, предоставляемых ТЭК, и, в частности, электроэнергетическим комплексом. Здесь источником угроз безопасности может являться цены, которые, как известно, имеют преимущественную тенденцию роста независимо от наличия профицита продукта. Повсеместно оказанные услуги и сама электроэнергия продаются как безальтернативные, независимо от генерирующего предприятия. Сложилась пагубная практика оправдывать рост цен трудностями, причиной которых является модернизация, основанная на замене старого технологического оборудования и внедрении новых импортируемых технологий.

Изменить сложившееся положение, по всей вероятности, сможет только независимое поэтапное системное управление процессами реформирования и только на основе директивного обозначения приоритетов стратегии.

Сможет ли, слегка изменённый ДПМ-1 на ДПМ-2 (договор на поставку мощностей) быть совершенным инвестиционным приоритетным инструментом в электроэнергетике? Известно, что ДПМ-1 способствовал масштабному строительству новых генерирующих мощностей, которые дали профицит электроэнергии. Но полученный профицит не смог повлиять на переформатирование рынка хотя бы в плане ценообразования, т.е. снижения цены за 1 КВт/час.

При этом, практика увеличения объектов генерации по проекту ДПМ-1 с целью избавления от дефицита электроэнергии реализовывалась одновременно с рекомендациями соблюдать режим экономии. Постановлением Правительства РФ декларировалась, в частности, замена ламп накаливания на светодиодные, которые, кстати, входят в список импортных товаров достаточно затратных в финансовом отношении.

Производство светодиодов в стране требует очень значительных инвестиций, кроме того утилизация использованных светодиодов тоже процесс, требующий серьёзных технологий и финансовых вложений. Таким образом, казалось бы, рациональные, правильные и своевременные рекомендации, по сути оказываются, мягко говоря, сомнительными. Так, в случае с заменой ламп выяснилось, что, во-первых, покупка импортной продукции была не очень своевременной из-за политики импортозамещения, во-вторых, на строительство отечественных производств не предусматривались источники финансирования и, в – третьих, не бралась в расчёт утилизация.

Проект ДПМ, в отсутствии стратегического приоритета, т.е. создания конкурентоспособного электроэнергетического рынка для всего хозяйственного комплекса, а также тактических приоритетов внутри отрасли, остаётся только проектом текущего момента.

Рост цен на электроэнергию для всех участников экономической цепочки от производителя до потребителя, в особенности для малого и среднего бизнеса – это угроза для социальной стабильности и угроза вытеснения российского производителя товаров и услуг (особенно в банковской сфере из-за очень высокой энергоемкости майнинга криптовалют) с рынков.

Главной категорией в определении безопасного экономического, политического и социального функционирования и развития страны является, адекватная высокому технологическому уровню, стоимость жизни. Технологический прогресс в мировой энергетической отрасли стремительно меняет парадигму взаимодействия с другими отраслями хозяйственной деятельности и также направлениями жизненного уклада и, соответственно, высоко ценится. Возникает вопрос: кто будет платить за прогресс? Бизнес – через повышение цен или государство за счёт налогоплательщика или социальными беспорядками, или сбалансированной политикой государственных приоритетов развития? А пока, совершенно очевидно, безопасность и стабильность, во многом, будет зависить от «киловатта», точнее от его стоимости. При этом, нельзя не учитывать, что достаточно дешёвый природный газ (ПГ) становится дорогим, к примеру, из-за того, что принимается решение в пользу высокотехнологичных импортных газовых турбин.

В результате, самые, на первый взгляд, рациональные рекомендации без выявления тактического приоритета электроэнергетической безопасности, способствуют, в лучшем случае, только сохранению рецессии.

Цифровая экономика будущего, очевидно, потребует многократного увеличения электроэнергетического ресурса и его эффективного распределения по перспективным направлениям инновационного роста. Эта неизбежная данность потребует чётко выверенной стратегии реформирования электроэнергетической отрасли и, тесно связанных с этим направлением, других производств.

Крайне необходимо, исходя из геополитического климата в мире, прежде чем принимать параметры общегосударственной стратегии в

электроэнергетической отрасли, определить законодательно-правовые и регламентационные условия её функционирования с учётом социально-экономической модернизации и с изменениями в глобальной экономике, как прогрессивного, так и регрессивного характера.

Глобальная экономика, как известно, за счёт малого роста ВВП развитых стран Запада, переживает длительную рецессию; зачастую характеризуется невыполнением соглашений и договоров ВТО, когда принципы этой международной организации игнорируются в результате диктата некоторых правительств. В последнее время всё чаще используется термин «торговые войны», а также наблюдаются стремительные изменения в валютно-денежных и банковско-финансовых секторах глобальной экономики. Таким образом, очень важно законодательно отрегулировать взаимодействие участников, если не на глобальном, то, хотя бы на мега-региональных уровнях.

Глобализация дала, что называется, побочный эффект – возник феномен «сплав интересов» глобального переустройства мира с опорой на суверенные интересы государств. Этот феномен пока не располагает общепринятыми инструментами и институтами развития и модернизации мирового сообщества.

Политические институты для феномена глобально-государственных интересов преобразования и развития начинают действовать в рамках ШОС и Евразийского сотрудничества. А их инструменты воздействия на межгосударственные отношения проявляют себя всё более и более последовательно и наступательно. В то же время, некоторые политики и аналитики отмечают малую эффективность их влияния на тенденции взрывающие ВТО и повсеместное доминирование Международного валютного фонда (МВФ), Всемирного банка (ВБ) и других регуляторов.

В данной ситуации, уместно было бы признать и законодательно оформить российский «Проект роста» и китайский проект «Один путь, один пояс» глобально-государственным стратегическим приоритетом нового формата международных отношений, открытым для других стран.

Другим стратегическим приоритетом, конечно же, являются инвестиции для создания внутреннего рынка потребления электроэнергии по функциональным направлениям: света, тепла, воды и других социальных нужд. При этом, можно было бы активизировать привлечение внутренних

инвестиций т.е. от населения. Задача сложнейшая, т.к. развитию инвестиционной активности граждан может помочь только осознание всеми потребителями продукции и услуг коммунально-хозяйственного назначения, своей общей взаимозависимости, а, следовательно, совместного участия в процессах реформирования отрасли.

Электроэнергетика является значительной частью теплоснабжения, а этот сегмент энергетики, пожалуй, самый трудно поддающийся модернизации в части генерации тепла и в части распределительных сетей. Специалисты предлагают создавать «умные дома» и «альтернативные котельные».

Известно, что с июля 2017 года, в соответствии с Федеральным законом № 279-фз, рекомендована апробация новой модели рынка теплоснабжения, названная «альтернативной котельной», которая призвана стать новым объектом генерации на оптовом рынке электроэнергии и мощности на рынке тепла, т.е. когенерации. Речь идёт о крупных агломерациях и их рынках энерго-тепло-водо- снабжения и где реформирование каждой из систем, в той или иной степени, касается других. Следовательно, тактические приоритеты вычленить из общего хозяйственного механизма практически невозможно, т.к. возникнут риски для безопасного функционирования всего комплекса жилищно-коммунального обеспечения населения. Мегаполисам удобно сотрудничество с единым, обобщённым ресурсом и желательно с правовым обеспечением взаимодействия городской администрации и частного бизнеса.

В каждой отдельной ситуации отдельного мегаполиса, на первый план выходит стратегический приоритет перехода к созданию модели цифровой экономики. Цифровая экономика предусматривает создание «умных городов», а это значит, что в распоряжении энергетиков будет иметь место самый точный и в то же время самый оперативный учёт ресурсов всех видов генерации и мониторинг работы сопутствующих технологических систем.

Мегаполис может создать сеть на основе блокчейна, где каждый потребитель сможет проверить своё участие в возможной акции краудфандинга или краудинвестинга т.е. акции, которая позволит потребителям электричества, тепла и воды вкладывать деньги в муниципальный бизнес и получать не только услугу, но и прибыль. При этом, краудфандинг это способ коллективного финансирования, основанный на добровольных взносах. А краудинвестинг, соответственно, альтернативный финансовый инструмент для привлечения капитала в стартапы и предприятия малого бизнеса от широкого круга микроинвесторов.

Сейчас, на первых этапах реформ, одной из основных проблем является привлечение инвестиций и, в связи с этим, стратегическим приоритетом должно стать безусловное доверие населения, потенциального инвестора, обеспеченное не только нормативно-правовой базой, а независимым блокчейном. При этом, безусловным фактором в повышении уровня такого доверия может стать фактор безопасности, обещанный специалистами. Анонсируется то, что преимуществом блокчейна-распределённого реестра является проблематичность его взлома. Так как информация обо всех транзакциях хранится в гатжетах каждого участника, технология системы построена по принципу консенсуса, а именно, ни одна транзакция не будет находиться в блоке, а блок не попадёт в цепочку, если не будет подтверждена участниами взаимодействия, которые не доверяют друг другу, но их обязывает задача договариваться во имя общего результата.

Таким образом, цепочка преобразований, а именно: инвестирование, реформирование и модернизация электроэнергетического сегмента энергетической отрасли, как представляется, должна иметь следующую последовательность: во-первых, определение параметров стратегического приоритета, а это – источники финансирования и усовершенствование государственно-частного партнёрства; во-вторых, выявление тактических приоритетов и их последовательности от инновационных возможностей для модернизации технологических узлов систем генерации. В свою очередь, межотраслевой рынок или специальная торговая биржа могут решить проблему финансовых, технологических и прочих рисков, особенно во временном диапазоне и создадут предпосылки к безопасности в энергетической отрасли.

2.4. Создание высокоскоростных крупномасштабных сетей передачи данных – основа успешного развития государства в условиях становления цифровой экономики

По мнению ряда американских экспертов, исследования и разработки в области создания крупномасштабных сетей призваны обеспечить технологическое лидерство США в высокопроизводительных межсетевых коммуникациях. Считается, что эти технологии позволят обеспечить такой уровень развития методов построения сетей, который необходим для дальнейшего роста общедоступных сетей типа Интернет и внутренних сетей федеральных министерств и ведомств. Первоначальные инвестиции

правительства США в исследования и разработки сетевых технологий дали возможность сформировать технологическую основу сегодняшней глобальной сети Интернет. Научно-исследовательские лаборатории, научное сообщество и промышленность помогли развернуть прототипы создаваемых сетей на национальном уровне, а также организовать производство популярных приложений - электронной почты и программ просмотра гипертекста - которые изменили сам подход к использованию ЭВМ человеком. Все это проложило путь к лидерству США во много миллиардной информационной индустрии.

Важным является то, что результаты совместных исследований и разработок в области создания крупномасштабных сетей, проводимых научным сообществом, промышленностью и правительством, являются своеобразным мостом, переброшенным к частному сектору, где их использование преобразовывает сам характер общественных связей.

Ключевыми направлениями исследований являются работы в области создания сетевых компонентов и технологий разработки, а также управления крупномасштабными сетями будущего. Считается, что работы по программе создания крупномасштабных сетей в рамках правительственной инициативы «Информационные технологии XXI века» позволят:

- повысить эффективность исследований в области сетевых технологий, финансируемых из федерального бюджета;
- создать эффективные сети федеральных министерств и ведомств;
- создать сетевые приложения, которые позволят решить ряд задач обеспечения национальной безопасности;
- обеспечить обмен информацией и облегчить взаимодействие участников в ходе проведения фундаментальных исследований и разработок;
- отработать механизмы сотрудничества в области исследований и разработок между федеральными агентствами, правительственными лабораториями, научным сообществом и промышленностью.

2.4.1. Организационная структура работ

Так в 1998 году основное внимание разработчиков было сосредоточено на инициативе создания Интернет следующего поколения (Next Generation Internet, NGI). В основе создания NGI лежат программы развития крупномасштабных сетей, обеспечивающих исследования и разработку передовых технологий и приложений, а также тестирование и демонстрацию

результатов, внедрение которых позволит значительно расширить возможности Интернет.

Усилия научного сообщества по данному проекту координируются рабочей группой проекта создания крупномасштабных сетей (LSNWG). С целью получения адекватного представления о ходе работ по проекту LSNWG организовала сбор необходимой информации от четырех специализированных рабочих групп, отвечающих за состояние дел по конкретному направлению развития проекта. Такими группами являются.

Объединенная инженерная группа (Joint Engineering Team, JET). JET координирует работы по выработке общей сетевой архитектуры и организации взаимодействия между сетями федеральных агентства (FedNets) и сторонними высокопроизводительными экспериментальными сетями. JET обеспечивает тесную координацию среди поставщиков оборудования, научного сообщества и промышленности в вопросе взаимодействия и предоставления услуг с тем, чтобы улучшить характеристики, доступные конечному пользователю, а также избежать дублирования ресурсов и усилий в обеспечении предоставления высококачественных услуг. Кроме того, JET сотрудничает с академическим сообществом по программе разработки гигабитных коммутаторов (Gigapops), сетью Abilene (консорциум компаний Qwest, Cisco, Nortel и университета штата Индиана), а также с участниками программы создания Internet 2 (I2). В настоящее время JET помогает осуществлять тестирование и отладку NGI.

Наряду с этим JET поддерживает взаимодействие между федеральными агентствами и сетью Abilene с целью обеспечения возможности доступа к более дешевым телекоммуникационным услугам, обеспечивающих пользователей географически удаленных территорий США (штатов Аляска и Гавайи).

Группа исследования архитектуры сетей (Networking Research Team, NRT). NRT координирует исследовательские программы по организации сетей в федеральных агентствах, распределению информации о результатах исследований среди участников работ, а также поддерживает действия по достижению основных целей NGI. Проводимые работы позволяют снизить время на получение необходимой информации по результатам исследований и способствуют улучшению взаимодействия между разработчиками и конечными пользователями.

Группа применения высокопроизводительных сетей (High Performance Networking Applications Team, HPNAT). HPNAT координирует исследования и разработки с целью сохранить и расширить технологическое

лидерство США в использовании высокопроизводительных сетей посредством проведения исследований, результатом которых является создание усовершенствованных технологий организации сетей, новых услуг и повышения производительности. Считается, что эти достижения позволят получить новые более эффективные сетевые приложения для решения задач, стоящих перед федеральными агентствами, помогая создавать основу для длительного развития национальной информационной инфраструктуры. Кроме этого, группа HPNAT обеспечивает механизмы сотрудничества между федеральными агентствами, правительственными лабораториями, научным сообществом и промышленностью в разработке приложений для крупномасштабных сетей, а также организует распространение информации, включая проведение демонстраций технологий, конференций и семинаров.

Группа обеспечения защиты Internet (Internet Security Team, IST). Группа IST облегчает испытание и экспериментирование с усовершенствованными технологиями защиты, а также служит центром по выработке требований к системе защиты. Эта группа снабжает руководство LSNWG информацией необходимой для организации исследований по защите NGI. IST финансирует разработку и тестирование систем защиты Internet, тесно взаимодействуя с агентствами и JET, что помогает осуществлять подобные эксперименты, а также делает их результаты доступными для национальных и международных исследователей в области безопасности.

2.4.2. Программы научных исследований и разработок в области создания крупномасштабных телекоммуникационных сетей

Программы исследований и разработок в области создания крупномасштабных сетей направлены на удовлетворение требований участвующих в работах федеральных агентств, а также на разработку технологий и приложений, расширяющих возможности Internet. В этот круг программ включены работы по следующим темам.

Программа исследований усовершенствованной сетевой инфраструктуры (ANIR). Данная программа объединяет усилия по исследованиям научного и инженерного сообщества США с целью повышения эффективности проводимых исследований в области фундаментальных работ по изучению сетей и сетевых инфраструктур.

В рамках программ обеспечивается разработка и развертывание высокопроизводительных сетей для проведения исследований по многим научным направлениям, требующим высокоскоростных вычислений, с целью выявления наиболее перспективных технических и технологических решений для их последующего внедрения в сети нового поколения.

Согласно этой программе сеть vBNS связала высокопроизводительные вычислительные центры Национального научного фонда и около 100 исследовательских институтов, занятых в работах по исследованию возможностей сетей следующего поколения, по все территории США. К работе подключаются такие исследовательские учреждения, программы работы которых требуют от сетей самой высокой производительности.

В рамках программы ANIR также проводятся исследования по разработке протоколов сетевого доступа и управления, инструментальных средств управления сетью, методов организации беспроводных сетей, мобильных вычислений, оптических сетей, программного обеспечения поддержки распределенных вычислений, программного обеспечение поддержки поиска и распределения сетевых ресурсов, а также устройств и подсистем ввода-вывода.

Разработка технологии организации сети. Программа интеренет-технологий Национального научного фонда фокусируется на достижениях фундаментальной науки и техники, необходимых для повышения эффективности высокоскоростной передачи информации в сетях и распределенных системах.

В рамках программы поддерживается разработка методов комплексного мониторинга сети, обнаружения проблем и механизмов их разрешения, разработка автоматизированных и усовершенствованных инструментальных сетевых средств, сетевого обеспечивающего программного обеспечения и сетевых инструментальных средств, а также создание сетевых приложений, которые способствуют организации совместных исследований и обмену информацией.

Активные сети. Управление перспективных исследований Министерства обороны США (DARPA) разрабатывает новую архитектуру сети, в основе которой лежит программируемая инфраструктура. В рамках программы разрабатываются методы организации активных сетей, методы управления и высокоуровневые услуги для конечного пользователя. Данная программа тесно взаимодействует с разработкой технологий сетей, проводимых Министерством обороны США, НАСА и другими федеральными агентствами.

Глобальные подвижные информационные системы. Работы по созданию глобальных подвижных информационных систем, проводимые DARPA, обеспечивают мобильным пользователям возможность работы и использования полного объема услуг, доступного в информационной инфраструктуре Министерства обороны США.

Масштабируемая организация сети. Программа разработки расширяемой сети, также проводимая DARPA, ставит целью обеспечить способность базовых сетей к адаптации к масштабным изменениям трафика в

современных сетях. Считается, что достижения в этой области позволят обеспечить доступ к географически распределенной и гетерогенной информационной инфраструктуре гарантируя при этом, что емкость основной сети и ее услуги будут приспособлены к особенностям ускоренного роста масштабов системы.

В рамках этой программы Управление перспективных исследований Министерства обороны США в 1999 году инициировало исследования по созданию гигабитной беспроводной сети связи, включающей космический сегмент на базе низкоорбитальных спутников связи.

Создание сверх высокоскоростных сетей. Результатом работ по этой программе, проводимой Агентством национальной безопасности США, должна стать инфраструктура высокоскоростной сети со скоростью предоставления канала в несколько гигабит в секунду и способностью поддержать устойчивые потоки данных, по крайней мере, до сотен мегабит в секунду уже сегодня и, в конечном счете, достичь скорости потока информации в несколько гигабит в секунду.

Еще в 1999 году Агентство национальной безопасности увеличило эффективность сетей путем снижения общего числа уровней протоколов взаимодействия сетей, а также путем перемещения управления к оконечным узлам сети. В сотрудничестве с NRL и Разведывательным управлением Министерства обороны США (РУМО), АНБ использовало режим асинхронной передачи (ATM) с разделением по длине волны для передачи 720 цифровых сигналов по 1.5 Гбит каждый на дистанцию в 400 километров через восемь ATM-коммутаторов.

Кроме этого, в рамках программы АНБ начало эксплуатацию полностью оптической сети, базирующейся на двух оптических технологиях:

- прототипах серийных маршрутизаторов с волновым разделением от Lucent, созданных в рамках одного из проектов Консорциума MONET, финансируемого DARPA;
- оптический коммутатор от Optical Networks, Inc.

Эта сеть позволяет АНБ организовать прямую связь между конечными пользователями без вмешательства электрооптического преобразования, что существенно повышает защищенность системы связи от несанкционированного доступа и перехвата сторонних излучений.

Основываясь на результатах экспериментов 1999 года, АНБ в настоящее время изучает новые подходы к управлению перегрузкой в сети, разрабатывая методы распределенного управления сетью связи.

Сети для биомедицинских исследований. Национальный институт рака (NCI) планирует применить развивающиеся технологии организации сетей и высокоскоростные интерфейсы к вычислительной инфраструктуре

одного из суперкомпьютерных центров (Frederick Biomedical Supercomputing Center, FBSC) с целью улучшить доступ к ресурсам для членов биомедицинского исследовательского сообщества. Считается, что это позволит получить новые данные для совершенствования технологий передачи данных в локальных мультимедиа-сетях.

Усовершенствованная ATM-сеть Национального агентства обработки и распределения информации дистанционного зондирования Земли (NOAA). В результате проведенных экспериментов и испытаний, финансируемых в соответствии с этой программой, NOAA разворачивает ATM-сеть. Сеть будет иметь 2400 узлов, объединенных в 80-90 виртуальных локальных сетей (VLANs). Такая архитектура дает избыточность и гибкость, необходимую для распределения полосы пропускания каналов в зависимости от индивидуальных потребностей. Инфраструктура сети должна поддержать в реальном масштабе времени обработку наблюдений поверхности Земли, получаемой со спутников дистанционного зондирования.

Единая федеральная сеть (FedNets). FedNets – единая сеть федеральных агентств - включает действующие информационные сети федеральных агентств и высокоскоростные экспериментальные сети. FedNets включает:

- vBNS - высокопроизводительную магистральную сеть связи Национального научного фонда;
- DREN - исследовательскую и инженерную сеть Министерства обороны;
- NREN - исследовательскую и образовательную сеть NASA;
- NISN - сеть интегрального обслуживания NASA;
- Esnet - сеть научного сообщества энергетиков.

Точка доступа к высокоскоростным сетям для научного сообщества (STAR TAP) и международная сеть (iGrid). Национальный научный фонд установил точку доступа (STAR TAP) в точке сетевого входа (NAP) компании Ameritech в Чикаго для связи vBNS с аналогичными международными сетями. STAR TAP управляется Электронной лабораторией визуализации (EVL) университета штата Иллинойс в Чикаго, Национальная Лаборатория Argonne и NAP Ameritech - точка обмена с Интернет следующего поколения (NGIX), который соединяется с FedNets и Abilene, обеспечивая международное сотрудничество с другими Федеральными агентствами, университетами и промышленными компаниями.

Более 15 сетей разных стран были объединены посредством STAR TAP к концу 1999 года. Среди них сети Азиатско-Тихоокеанского консорциума (APAN), Канады (CA Net), сеть Европейской лаборатории физики

элементарных частиц (CERN), Франциb (Renater), Израиля, Нидерландов (SURFnet), скандинавских стран (NORDUnet), Сингапура (SingaREN), Тайваня (TANet), Американо-азиатского тихоокеанского консорциума (TransPAC) и американо-российский Консорциум (MirNET). Одна из главных особенностей - STAR TAP разрабатывает и использует объединенный подход к управлению, измерению характеристик, планированию и использованию географически распределенных ресурсов, названный Международной Сетью (iGrid).

Провайдеры высокоскоростных сетей (HPNSPs). Национальный научный фонд обозначил категорию коммерческих провайдеров услуг доступа в высокоскоростные сети (HPNSPs), которые снабжают усовершенствованные услуги сети по широкополосным сетям к университетским и Федеральным местонахождениям агентства и снабжают высококачественные услуги необходимыми NGI. Сеть Abilene - первый HPNSP. Продавцы координируют близко с HPNSPS, сквозь JET и другие группы LSN, снабжать связность и усовершенствованные услуги высококачественным пользователям сети.

Усовершенствование распределенного доступа к данным. Ряд федеральных агентств, таких как NASA, NIH, NOAA и другие, прогнозируют в течение ближайших лет существенное увеличение требований на передачу данных от искусственных спутников Земли через сети связи.

Результаты прогнозов заставляют эти агентства проводить в рамках группы JET ряд исследований, направленных на совершенствование высокоскоростного доступа к массивам данных. В частности, NOAA прогнозирует, что информационный поток в Центра Силвер Спринг в штате Мэриленд, будет расти от сегодняшних 150 Гбайт в день до 1 Террабайта в день в 2002.

Для подготовки к столь масштабным изменениям, NOAA в сотрудничестве с другими агентствами, работающими по программе крупномасштабных сетей, проводит ряд работ по совершенствованию методов управления высокоскоростными сетями передачи данных. Среди наиболее перспективных технологий высокоскоростной передачи данных называется технология асинхронной передачи данных.

2.4.3. Области приложения высокоскоростных крупномасштабных сетей передачи данных

Главная цель исследований и разработок в области создания крупномасштабных сетей состоит в том, чтобы дать конечному пользователю такие услуги, которые были бы в состоянии решать все возрастающие потребности в вычислительных мощностях.

Среди множества приложений высокоскоростных сетей особо отмечаются следующие области.

Высокопроизводительные приложения для нужд науки и техники (HPASE). Национальный научный фонд поддерживает обширную программу исследований по созданию приложений для фундаментальных отраслей науки, что позволит приблизиться к масштабным и наиболее важным открытиям современной науки, позволяющим дать ответ на важнейшие вопросы современности. Столь амбициозные задачи выводят приложения этой группы на высшую ступень иерархии потребностей вычислительных ресурсов.

В 1999-2000 годах совместными усилиями университетского сообщества, Центра Атмосферных Исследований (NCAR) и других федеральных лабораторий в рамках программы HPASE были продолжены разработки системы моделирования климата Земли и атмосферы. К концу 1999 исследователям уже стали доступными результаты моделирования, охватывающих период с 1860 до 2300 годов, отражающими изменения климата Земли под влиянием различных факторов, в том числе и деятельности человека.

В 2000 г. согласно программе HPASE, NCAR получило новую суперкомпьютерную систему, что позволило продолжить работы по развитию новых вычислительных методов.

Погода. NOAA также поддерживает программу исследований в области сбора и обработки метеорологических данных. В достижении этой цели NOAA активно использует существующий и перспективный доступ к высокопроизводительным вычислительным системам, а также современные информационные технологии, включая NGI, распределенное вычисление, iGrid и цифровые библиотеки.

Телемедицина. Исследования и разработки в области создания крупномасштабных сетей в Национальной медицинской библиотеке (NLM) формируют сети для связи больниц, вспомогательных учреждений, медицинских школ, медицинских библиотек и университетов, чтобы дать возможность медработникам и исследователям обмениваться медицинскими данными и иметь доступ к необходимой медицинской литературе. NLM также поддерживает разработку технологий, обеспечивающих медработникам в отдаленных местах прямой контакт с их коллегами в крупных медицинских центрах, включая технологии визуализации анатомии

человека, анализаторы рентгеновских снимков, компьютерную томографию и другие диагностические инструменты, а также технологии баз данных для хранения, доступа и передачи медицинских данных с соблюдением необходимых мер по защите целостности и конфиденциальности этих данных.

Кроме этого, NLM сосредотачивается на оценке эффективности методов телемедицины. Так в 2000 году NLM продолжила финансирование проектов, способствующих реализации телемедицины.

Компьютеризированные истории болезни. Цель программы компьютеризированной истории болезни (AHCPR'S) состоит в том, чтобы повысить оперативность, точность и тиражирование данных о состоянии здоровья пациента, способствовать их использованию для повышения качества клинических решений.

Программа создания Объединенных Академических систем управления информацией (IAIMS). Цель программы IAIMS состоит в том, чтобы развивать и внедрять системы управления потоками информации в пределах университетских центров и больших медицинских центров, чтобы увеличить отдачу от результатов научных исследований, улучшить доступ к данным для оценки состояния здоровья. К программе подключены более 120 академических медицинских центров включая учебные заведения, больницы, клиники и лаборатории. Эти центры нуждаются в сиюминутной информации относительно состояния здоровья пациентов, результатах исследований, содержащих в базе данных библиографические и фактические данные о пациентах, их молекулярные данные, базы данных лабораторных и клинических исследований.

Проект "Видимый Человек" (VH). Большой размер набора изображений VH и других медицинских изображений оспаривает хранение и технологии передачи сети. Так как полный набор изображений человека требует емкости больше, чем 100 CD, NLM исследует методы сжатия, чтобы минимизировать емкость и улучшать скорость передачи данных по Интернет.

Биоинформатика. Биоинформатика ключевой компонент исследований генома человека, генной инженерии и проектирования новейших лекарственных препаратов, где широко используются аналитические и прогнозные методы для определения ключевых молекулярных групп, связанных со здоровьем и болезнью человека.

Национальный центр биотехнологической информации (NCBI) сосредотачивается на автоматизированных системах записи и анализа обширной информации молекулярной биологии, биохимии и данных генетики, объемы которой постоянно возрастают. В распределенной базе данных NCBI накапливает данные от исследователей со всего мира и включает их в GenBank - банк данных ДНК-последовательностей - ключевой ресурс проекта «Геном человека». К этим базам данных обращаются ежедневно по Интернет более 90.000 сайтов.

ГЛАВА 3. КОМПЛЕКСНАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ТЭК В ЭПОХУ ЦИФРОВИЗАЦИИ

3.1. Нормативная основа обеспечения безопасности объектов ТЭК Российской Федерации

Согласно Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 12 мая 2009 г. № 537, национальная безопасность представляет собой сложную многоуровневую систему, функционирования которой обусловлено множеством социально-экономических, политических и иных факторов. К основным видам безопасности относят экономическую, социально-политическую, военную, энергетическую и др. Необходимо отметить, что энергетическая безопасность интегрирует несколько направлений обеспечения безопасности, имея влияние на экологическую, экономическую и иные виды. Соответственно угрозы энергетической безопасности реализуются и в других сферах жизнедеятельности, что подчеркивает их комплексную природу.

При этом, усиление энергетического фактора в российской экономике делает энергетическую безопасность ключевым условием повышения экономической безопасности в целом. Так, в пункте 60 Стратегии отмечено, что энергетическая безопасность является одним из главных направлений обеспечения национальной безопасности в экономической сфере на долгосрочную перспективу [1].

Необходимо отметить, что при перечислении условий ее обеспечения используется термин «национальная энергетическая безопасность» [1]. Помимо национального выделяется региональный (субъект РФ) и локальный (местный) уровни обеспечения энергетической безопасности России.

В «Энергетической стратегии Российской Федерации на период до 2030 года» подчеркнуто, что достижение энергетической безопасности осуществляется на базе реализации всех основных составляющих государственной энергетической политики. Энергетическую политику можно определить как систему мер государственного регулирования, направленных на эффективное обеспечение потребностей экономики в энергоносителях при общественно приемлемых ценах и тарифах [2].

В соответствии с указанным документом мы сейчас находимся на третьем этапе развития энергетической отрасли, связанном с развитием инновационной экономики.

Согласно документу, проведение политики такого рода основывается на следующих важнейших принципах [2]:

- обеспечение надежности энергообеспечения экономики и населения России;
- разделение полномочий и ответственности органов власти на всех уровнях, энергоснабжающих компаний и хозяйствующих субъектов-потребителей;
- обеспечение надежного функционирования и предсказуемого развития энергетической инфраструктуры;
- своевременность геологоразведки, подготовки и освоения новых месторождений традиционных видов топлива, в том числе за счет частно-государственного партнерства и рациональной налоговой политики (имея в виду опережающий добычу прирост разведанных извлекаемых запасов), своевременность подготовки к использованию замещающих инновационных энергоресурсов и источников энергии по мере исчерпания традиционных ископаемых энергоресурсов;
- снижение уровня износа основных производственных фондов;
- максимально возможное использование конкурентоспособного отечественного оборудования во всех технологических процессах и проектах, стимулирование развития отечественного производства энергоносителей с высокой добавленной стоимостью и повышения качества нефтепродуктов за счет ужесточения стандартов качества моторного топлива, модернизации нефте- и газоперерабатывающих комплексов на территории России, дифференциации ставок акцизов на моторные топлива различного качества;
- повышение уровня национальной энергетической безопасности в результате международного сотрудничества в сфере

Стоит указать, что понятие энергетической безопасности отличается от используемого в дальнейшем понятия безопасности объектов ТЭК. Так, данный аспект отмечается, например, в работе Т.А. Спицыной [3]. Как

показывает анализ документов, безопасность объектов ТЭК является составной частью более масштабной национальной энергетической безопасности. Если первое воспринимается как состояние защищенности страны, ее граждан, общества, государства и экономики от угроз надежному топливо- и энергообеспечению, то второе акцентировано на защищенности конкретных объектов от внутренних и внешних угроз различного типа.

Детализация мер, предусмотренных Стратегией национальной безопасности, осуществлена в Поручении Президента РФ от 15.11.2011 № Пр-3400 «Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года». В соответствии с Поручением выделяются угрозы природного и техногенного характера, а также террористические угрозы.

При этом одним из основных принципов формирования и реализации государственной политики в области обеспечения безопасности населения и защищенности критически важных и потенциально опасных объектов от угроз различного характера является принцип обеспечения комплексной защиты критически важных и потенциально опасных объектов.

Применительно к ТЭК комплексное обеспечение безопасности объектов регулируется рядом нормативных актов, основным из которых является Федеральный закон от 21.07.2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» [4].

Приказом Министерства энергетики РФ от 13 декабря 2011 г. № 587 утвержден перечень работ, непосредственно связанных с обеспечением безопасности объектов топливно-энергетического комплекса [5]:

1. Оценка достаточности инженерно-технических мероприятий, мероприятий по физической защите и охране объекта топливно-энергетического комплекса.

2. Монтаж и эксплуатация и техническое обслуживание инженерно-технических средств охраны и средств пожаротушения объектов топливно-энергетического комплекса.

3. Осуществление внутреннего контроля в области обеспечения безопасности объектов топливно-энергетического комплекса.

4. Охрана объектов топливно-энергетического комплекса.
5. Разработка, монтаж и эксплуатация информационных систем, информационно-телекоммуникационных сетей и систем защиты информации и информационно-телекоммуникационных сетей объектов топливно-энергетического комплекса.

Необходимо отметить, что данный перечень фактически дает определение комплексной безопасности объектов ТЭК. На основании вышеупомянутого перечня работ можно утверждать, что комплексная безопасность объектов ТЭК включает в себя:

- физическую безопасность объектов в совокупности с мерами обеспечения контрольно-пропускного режима;

- пожаро- и взывобезопасность, защиту от техногенных аварий;

- промышленную безопасность объектов;

- информационную безопасность.

Основные положение по физической безопасности объектов ТЭК раскрыты в постановлении Правительства Российской Федерации от 5 мая 2012 г. № 458 «Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса» [6]. Вопросы пожаро- и взывобезопасности регламентируются различными документами, в частности:

- ППБ 01-03 Правила пожарной безопасности в Российской Федерации
- ВППБ 01-04-98 Правила пожарной безопасности для предприятий и организаций газовой промышленности
- СНиП 21-01-97 Пожарная безопасность зданий и сооружений.
- ССБТ. Пожаровзрывобезопасность веществ и материалов. Номенклатура показателей и методы их определения (ИСО 4589-84).
- Приказом Ростехнадзора от 26.12.2012 № 781 «Об утверждении Рекомендаций по разработке планов локализации и ликвидации аварий на взрывопожароопасных и химически опасных производственных объектах»
- и другими документами.

Вопросы промышленной безопасности регламентируются Федеральным законом № 116-ФЗ "О промышленной безопасности опасных производственных объектов". Дополнительно можно отметить, что на сайте Межгосударственного совета по промышленной безопасности приводится статистика по аварийности и травматизму по странам-участницам совета. Существенная доля аварий приходится на предприятия ТЭК, что говорит об актуальности обеспечения промышленной безопасности в отрасли.

Существенным признаком формирования цифровой экономики является активное использование различных автоматических и автоматизированных систем управления технологическими процессами. Как следствие, промышленная безопасность объектов начинает зависеть от вопросов информационной безопасности. Данное положение нашло отражение в «Основных направлениях государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации», где отмечено, что целью государственной политики в области обеспечения безопасности этих систем является «снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем» [7].

Основным актом стратегического планирования, определяющим политику в области обеспечения информационной безопасности Российской Федерации является Доктрина информационной безопасности, в которой отмечено, что к национальным интересам страны относится обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры и единой сети электросвязи.

3.2. Понятие комплексной безопасности объектов ТЭК

Вопросы комплексной безопасности, в том числе комплексной безопасности объектов ТЭК, рассматривались в различных научных работах, но, как представляется, отсутствие методического подхода приводило к тому, что, в зависимости от области профессиональных интересов авторов, под комплексной безопасностью понимался тот или иной набор аспектов безопасности. Вместе с тем, развитие нормативной базы, теории и практики обеспечения безопасности привело к тому, что на текущий момент научно

обоснованное и зафиксированное в научных работах непротиворечивое определение комплексной безопасности объектов ТЭК отсутствует.

Прежде чем перейти к описанию понятия комплексной безопасности объектов ТЭК, определим ряд базовых понятий, вытекающих из общих подходов к обеспечению безопасности. Необходимо отметить, что для каждого из рассматриваемых понятий уже существует ряд определений, закрепленных в нормативных актах и научно-технической документации, вместе с тем, необходимость выработки методически единого подхода к описанию комплексной безопасности объектов ТЭК требует их переопределения.

Как представляется, основными понятиями являются «угроза», «ущерб» и «уязвимость», которые будут рассмотрены ниже.

Угроза – потенциальная возможность нанесения ущерба объекту.

Ущерб - результат негативного изменения состояния объекта вследствие реализации каких-то событий, явлений, действий, в том числе в результате реализации угроз, выражающийся в ухудшении свойств объекта.

Необходимо отметить, что угроза связана с характеристиками самого объекта, в отношении которого она проявляется, в первую очередь, с его уязвимостями. Данное замечания является существенным с той точки зрения, что в дальнейшем изложении будет рассматриваться специфика объектов ТЭК, а, значит, перечень угроз будет сформирован с учетом отраслевой специфики.

Уязвимость. Недостаток (слабость) отдельных элементов объекта или объекта в целом, который (которая) может быть использована в случае реализации угроз безопасности.

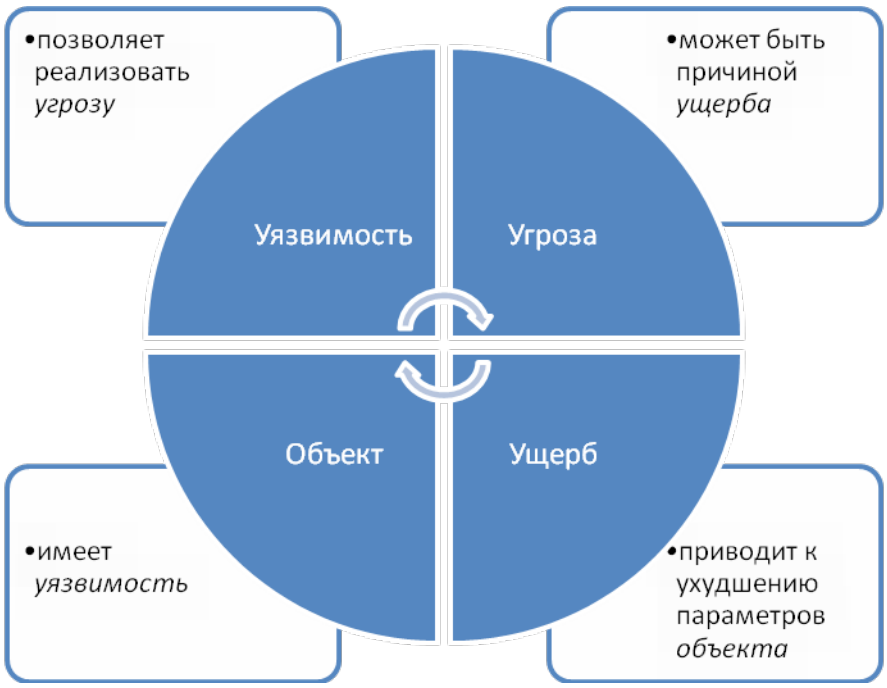


Рис. 3.1. Взаимосвязь базовых понятий безопасности.

На рис. 1 представлена схема взаимосвязи базовых понятий безопасности. Как уже было отмечено, объект ТЭК имеет отраслевую специфику, т.е. имеет не только общие, но и специфичные уязвимости, влияющие на его безопасность в целом.

С научной точки зрения объект ТЭК можно описать как социотехническую систему S, состоящую из элементов и связей между ними, что согласуется с подходами, изложенными в [8]. Под элементом $o_i\, o_i$ объекта ТЭК будем понимать аспект его рассмотрения в виде феномена, обладающего уязвимостями определенного рода. Так, например, объект ТЭК с точки зрения Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 № 187-ФЗ, объект ТЭК может рассматриваться как объект критической информационной инфраструктуры. Обозначим через O множество аспектов рассмотрения объекта ТЭК.

$$O = \{o_i\}$$

Определим, что связь $c_{ij}\, c_{ij}$ между элементами существует, если деградация элемента $o_i\, o_i$ приводит к деградации элемента $o_j\, o_j$. В противном случае связь между элементами отсутствует. Так, например, поражение АСУ ТП вследствие компьютерного инцидента (объект ТЭК как объект критической

информационной инфраструктуры) может привести к производственной аварии (объект ТЭК как опасный производственный объект с точки зрения Федерального закона "О промышленной безопасности опасных производственных объектов" от 21.07.1997 № 116-ФЗ). Обозначим через C множество связей между элементами.

Тогда объект ТЭК может быть описан как совокупность элементов и связей между ними.

$$S = (O, C)$$

Для описания множества аспектов рассмотрения объекта ТЭК примем подход, что включаемый в рассмотрение аспект должен иметь:

- отражение в законодательной и нормативной базе;
- государственное регулирование деятельности по выделенному аспекту;
- подтверждение фактами (статистикой) реализации угроз, связанными с выделенным аспектом.

На основании предложенного критерия определим, что объект ТЭК может рассматриваться как:

- юридическое лицо, имеющее участников, уставной капитал, счет в банке, цели функционирования в рамках разрешенных видов деятельности и т.д.;
- физический объект, характеризуемый местом расположения, перечнем и параметрами зданий, сооружений, включая охранные, линейных объектов и т.д.;
- производственный объект, характеризуемый производственным процессом, имеющим технологические особенности, в том числе повышенной опасности;
- источник производимой продукции, характеризующейся товарной стоимостью, сроком годности, порядком складирования, хранения и реализации и т.д., имеющей существенное значения для жизнедеятельности населения и функционирования промышленности;

- субъект финансово-хозяйственной деятельности - источник прибыли, возникающей в результате реализации товарной продукции;
- объект информатизации, обладающий информационными активами (как результат реализации определенного производственного процесса, в случае наличия таковых), информационными ресурсами, с помощью которых обеспечивается производственный процесс, и информационными ресурсами, с помощью которых управляется сам производственный объект;
- коллектив специалистов (трудовой коллектив), обеспечивающих решение производственных задач;
- источник повышенной опасности а) для сотрудников предприятия, б) граждан, находящихся в зоне производственного объекта, в) искусственных сооружений, находящихся в зоне производственного объекта, г) окружающей среды.

Каждому аспекту объекта ТЭК в соответствие может быть поставлено ключевое понятие его рассмотрения, нормативный документ, определяющий данное рассмотрение, пример данных, подтверждающий наличие угроз, связанных с данным аспектом. Необходимо отметить, что угрозы могут рассматриваться на макроуровне, когда они актуальны для всех объектов, имеющих выделенные особенности, и на микроуровне, по отношению к конкретному объекту. Для обобщения все примеры угроз сведены в таблицу. Можно полагать, что данная таблица отражает актуальное на текущий момент понимание комплексной безопасности объектов ТЭК.

Обращаем внимание читателей на то, что однозначно определенными в данной таблице являются аспекты рассмотрения объекта ТЭК. Остальные данные носят характер примеров и могут быть дополнены.

Аспект объекта ТЭК	Ключевое понятие	Нормативный документ	Подтверждение угрозы	Ответственное ведомство	Макроуровень	Микроуровень
Юридическое лицо	Субъект ТЭК / Лицензиат	256-ФЗ	Статистика отзыва лицензий	Ведомства, ответственные за выдачу лицензий	Изменение порядка лицензирования	Нарушение условия лицензии
Физический объект	Охраняемый объект ТЭК	256-ФЗ	Статистика последствий катастроф и нападений на объекты	Росгвардия	Стихийное бедствие	Незаконное вмешательство
Производственный объект	Опасный производственный объект	Федеральный закон от 21.07.1997 № 116-ФЗ	Статистика производственных аварий.	Ростехнадзор	Несовершенные технологии	Износ оборудования
Источник продукции	Критически-важный объект ТЭК	256-ФЗ	Статистика уголовных дел	Минэкономраз-витие	Истощение запасов сырья	Хищение продукции
Субъект финансово-хозяйственной деят.	Налогоплательщик	НК РФ	Статистика арбитражных дел	ФНС, МВД	Санкции	Штрафы
Объект информатизации	Объект критической информационной инфраструктуры	187-ФЗ	Статистика компьютерных инцидентов	ФСБ России, ФСТЭК России	Вирусные эпидемии	Целевая компьютерная атака
Коллектив специалистов	Трудовой коллектив	ТК РФ	Статистика трудовых споров.	Минтруд	Общий уровень образования и	Трудовой конфликт на

					оплаты труда	предприятии
Источник повышенной опасности	Потенциально опасный объект ТЭК	256-ФЗ	Статистика пожаров и ЧС	МЧС	Использование сырья, или производство продукции пожаро-, взрыво-, химически опасной(ого).	Нарушение правил эксплуатации
Источник воздействия на окружающую среду	Объект, оказывающий негативное воздействие на окружающую среду	Федеральный закон от 10.01.2002 № 7-ФЗ	Статистика экологических правонарушений	Ростехнадзор	Изменение экологического законодательства	Авария с экологическим и последствиями

Исходя из изложенного, определим аспекты рассмотрения объекта ТЭК как перечень, изложенный на рис. 3.2.

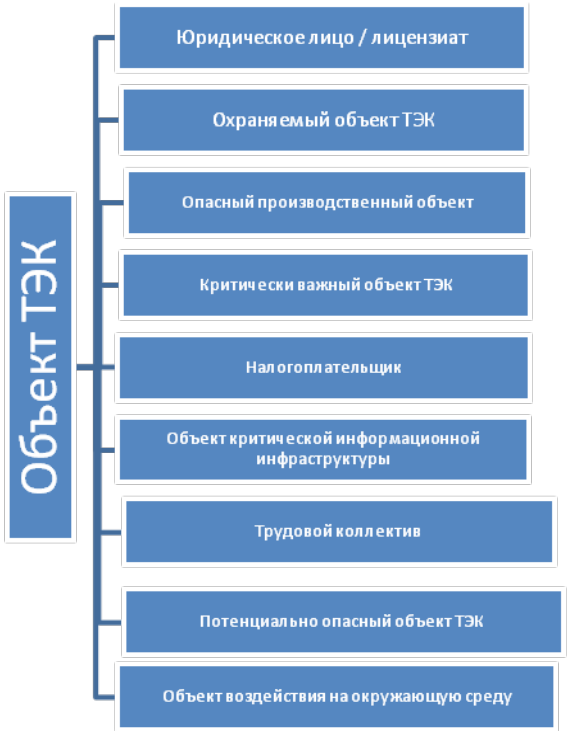


Рис. 3.2. Нормативно определенные аспекты рассмотрения объекта ТЭК.

В рамках секции «Обеспечения комплексной безопасности и защищенности объектов промышленности, нефтегазового сектора и электроэнергетики» на международном форуме «Технологии безопасности», прошедшем в феврале 2019 г. в г. Москве, специалистами было отмечено, что вопросы промышленной безопасности, противопожарной безопасности и безопасности по чрезвычайным ситуациям достаточно сильно коррелируют между собой. Вместе с тем, разделение данных вопросов обусловлено распределением ответственности и надзорных функций между различными ведомствами, что и подчеркнуто в приведенной таблице.

Необходимо отметить, что источник угроз может носить либо техногенный, либо антропогенный характер. Выделение антропогенного источника угроз позволяет разделить инициирование угроз на умышленное и неумышленное.

Парирование угроз, в соответствии с общей теорией безопасности, реализуется через:

- выявление угроз;
- предупреждение угрозы до момента ее реализации;

- пресечение угрозы в стадии реализации;
- ликвидация последствий реализации угроз.

Описание объекта ТЭК как социотехнической системы, обладающей элементами и связями, было введено из-за наличия гибридных угроз, когда угроза, возникающая в одной области, реализуется в другой. Пример отрицательного воздействия на производственный процесс через компьютерную атаку на АСУ ТП был приведен выше. В общей теории безопасности существует принцип равномощности рубежей защиты, в соответствии с которым организация комплексной системы безопасности не допускает наличия «слабых мест» или отсутствия защитных мер, противостоящих выявленным угрозам.

На текущий момент теория противодействия гибридным угрозам отсутствует. Представляется, что определение комплексной безопасности, в данном случае объектов ТЭК, является первым шагом в данном направлении.

3.3. Информационная безопасность, информатизация, электронные финансы и новая экономика

В большей степени современное общество можно охарактеризовать как пограничное между обществом материального производства и обществом постиндустриальным, информационным, характеризуемым новой политикой и экономикой, базирующейся на накоплении и обработке знаний и информации в различных формах. Происходящие процессы, связанные в первую очередь с глобализацией производства и потребления информации, в весьма скором будущем кардинально изменят и уже сейчас изменяют как способ общественного производства, так и многие общественные институты.

Важная задача в этом процессе – проанализировать, правильно истолковать и спрогнозировать существующие тенденции производства, передачи, обмена информацией, дабы предложить стремительно формирующемуся обществу будущего адекватные механизмы для работы с новыми категориями, понятиями и отношениями в сфере общественного производства и отношений.

В первую очередь необходимо отметить возрастание роли конкретного субъекта-индивидуума в процессе производства им информации в различных формах, в том числе и в форме товара. Из этой роли вытекает, с одной стороны, необходимость персонализации как самого субъекта, так и производимой и обрабатываемой им информации, защиту его интересов в

сфере производства и потребления информации, а с другой – необходимость разработки и реализации механизмов безопасного и равноправного обмена произведенной информацией-товаром и адресного получения за нее материальных благ.

Вместе с тем, очевидно, что персонализированный индивидуум вступает в совершенно новые отношения с обществом и государством в лице их институтов. Эти отношения характеризуются в первую очередь высоким динамизмом и отказом от анонимности, а также равноправным участием персонализированного индивидуума в обмене информацией с государственными и общественными организациями. Высокий динамизм определен в первую очередь использованием глобальных компьютерных систем и сетей связи, а равноправный обмен информацией, защищающей интересы индивидуума в постиндустриальном обществе – это защищенный обмен, а также безопасность персональных данных и ресурсов индивидуального пользователя.

Изменяется медийное поле общества, поскольку персонализированный индивидуум, с одной стороны, не может являться источником непроверенной анонимной информации, а с другой – выступает потребителем вполне конкретных услуг в информационном поле, организуя четкие обратные связи с общественными и государственными медиа-институтами. И если перед конкретным общественным институтом пользователь абсолютно не анонимен, то обязанность институциональных участников информационного обмена – обеспечить его конфиденциальность относительно не участвующих в нем субъектов.

В области финансов изменяется роль денег, которые в большей степени становятся «электронными». Электронным деньгам в полной мере присущи все три функции денег: измерение-учет, обращение и накопление. Особенностью «постиндустриальных» денег может и должна являться возможность их прямого обмена между индивидуумами («электронные кошельки»). Электронный обмен денежными эквивалентами – есть овеществленная безопасность этой информации, ибо ничего кроме символьных эквивалентов мер стоимости при нем не передается.

Совокупность названных факторов свидетельствует о формировании «новой экономики» или «экономики знаний», важнейшей чертой которой является неубывание информации как товара при ее обмене между участниками рынка, что позволяет говорить о потенциальной возможности стабильного

экономического роста. Важнейшей стратегической задачей, как для личности, так и для государства становится создание механизмов реализации прав и обязанностей производителей информации, участников рынка информационных товаров и услуг, медийных корпораций, а также государственных и общественных институтов.

Таким образом, безопасность информации является стратегической целью постиндустриального общества. Безопасными должны быть все процессы производства, хранения и обмена информацией, все компоненты технического, программного, протокольного, институционного типа, участвующие в этих процессах.

Одной из таких трансформаций является формирование в настоящее время такого нового качества глобальной сети, как "Интернет ценностей" (Value Web). Реализация данной общепланетарной парадигмы создаст условия, при которых практически каждый дееспособный житель Земли потенциально может быть вовлечен в систему финансовых отношений по получению прибыли, может заявить о себе, как об источнике ценной для других информации, распространять разработанные им знания и умения. В "Интернете ценностей" появляются новые категории, которые могут быть предметом договоров мены или купли-продажи, получившие обобщенное название "токен ценности". Это могут быть скидки по дисконтной карте, "наградные мили" авиакомпаний, объем интернет-трафика или минут в сети мобильной связи. Все указанные категории, в конечном итоге, могут быть выражены в форме традиционных денег, однако они уже сейчас существуют сами по себе и их гражданский оборот будет только расширяться.

Основной угрозой здесь является прежде всего слабое понимание в настоящий момент времени сути данных отношений подавляющим большинством предпринимателей, государственных служащих и граждан, что создает почву для мошеннических действий. Однако угрозы не только в этом. Недопонимание изменения подходов к понятию "ценность", "актив" в экономическом и правовом смыслах может привести к отставанию в развитии новых способов взаимодействия между продавцом и покупателем, способов инвестиционной деятельности и так далее. В конечном итоге это может привести к отставанию в финансировании нефтегазовой отрасли.

Многочисленные авторы, пишущие в настоящий период времени о развитии цифровой экономики, в качестве одной из "прорывных" технологий, характерных для этой экономической модели, представляют технологию

блокчейн, которая может быть описана как распределенная база данных, последовательная запись информации в которой создает условия для высокой степени достоверности внесенных сведений за счет многочисленных обновляемых (реплицированных) копий этой базы, находящихся у разных пользователей, и математической связи между предшествующими массивами информации (блоками) и последующими, что делает практически невозможным внесение изменений в ранее созданные блоки.

Как представляется, технология блокчейн может получить широкое распространение для различных утилитарных целей, в том числе и в нефтегазовой отрасли, например, для подтверждения качества топлива, для более четкой фиксации операций на различных технологических циклах, для проведения расчетов с потребителями продукции и т.п. Однако представлять данную технологию в качестве основного движителя цифровой экономики было бы, по мнению автора, несколько легковесным подходом, так как ее применение в практической деятельности имеет вполне конкретные границы.

Основой угрозой применения технологии блокчейн в системах с ограниченным количеством пользователей данной базы данных является как раз эта ограниченность. Говоря иначе, достоверность блокчейна тем выше, чем больше его пользователей, так как внесение изменений во все копии по понятным причинам связано с существенными технологическими трудностями. Если же пользователей и, следовательно, копий мало, то решение такой задачи становится вполне реальным и достоверность данных может оказаться под угрозой.

Производным от технологии блокчейн являются так называемые криптовалюты, то есть некие единицы (токены) ценности, которые появляются в результате решения математических задач, формируемых специальными программами. В настоящий период времени насчитывается более 2500 видов криптовалют. Соревнование между криптовалютами и фиатными валютами пока выигрывается последними из-за того, что криптовалюты имеют слишком высокую волатильность и не признаются большинством государств в качестве денежных средств, разрешенных к хождению на рынке. Однако по мере развития такого феномена, как "Интернет вещей", то есть установление связи и удаленного взаимодействия между отдельными устройствами без вмешательства человека, технология криптовалют может быть использована для расчетов между такими устройствами. Не исключено, что в недалеком будущем, по мере устранения

недоработок программных продуктов, мы сможем увидеть какую-то криптовалюту в качестве официальной расчетной единицы на международном уровне. К такому развитию событий следует готовиться уже сейчас.

Теперь собственно об "Интернете вещей". Эта группа технологий, как представляется, будет внедряться в экономическую практику уже в ближайшее время и во-многом будет определять технологическое развитие в самых разных отраслях экономики. Не является исключением и нефтегазовая отрасль. Различного рода датчики и комплексы, работающие в полностью автоматическом режиме, для данной отрасли уже сейчас являются реальностью. Подключение их к сети Интернет и управление посредством возможностей зарождающегося искусственного интеллекта является совсем близкой перспективой. То же самое можно сказать и в отношении взаимодействия предприятий нефтегазового комплекса и конечными потребителями их продукции.

Здесь, однако, следует сразу озаботиться проблемой обеспечения информационной безопасности в самом широком плане, так как все экономические преференции, которые влечет за собой применения технологий "Интернета вещей", могут быть снивелированы теми угрозами, которые возникают при блокировании компьютерных систем, ими управляющих. Игнорирование обеспечения защиты таких систем от различного рода угроз, причем защиты превентивной и системной, может привести к самым печальным экономическим последствиям как для отдельных организаций нефтегазовой отрасли, так и для целых сегментов российской экономики.

Авторы также полагают, что проблема обеспечения информационной безопасности при развитии цифровой экономики является системной задачей, которая требует осмысления со многих точек зрения, а имеющееся правовое обеспечение этой деятельности, как показано в настоящей работе, , является явно недостаточным в силу своей схематичности и отсутствия должной системности.

Существующие особенности и перспективы развития бизнеса создают предпосылки для перехода к электронным формам ведения бизнеса, что обуславливается и естественным ходом научно-технического прогресса общества в целом. При этом появление информационно-коммуникационных технологий привело не только к изменениям в организации бизнеса в виде

автоматизированных систем управления производством, систем учета и контроля за движением товаров, электронного документооборота, но и к совершенствованию традиционных видов бизнеса.

Экономический эффект, который достигается за счет внедрения компьютерных систем в процессы организации бизнеса, заключается в ускорении и повышении качества работ с технической и финансовой документацией, в возможности внедрения передовых технологий, в частности, в автоматизированных производствах, в уменьшении зависимости эффективности бизнеса от места расположения предприятия, в расширении возможностей специализации и кооперации.

Другим принципиально новым аспектом, связанным с появлением электронного бизнеса, является создание новых сфер деятельности в области производства товаров и услуг. В первую очередь, это относится к развитию собственно новых видов телекоммуникаций и информационных технологий и возникающих при этом возможностей в области обработки, хранения и передачи информации. Здесь можно выделить такие составляющие, как производство оборудования и технических средств для телекоммуникационных и информационных систем, разработка программного обеспечения, создание банков информации и информационно-аналитических служб. Фактически, это направление связано с обеспечением инфраструктуры электронного бизнеса и разработкой инструментария информационных технологий.

Налоги сегодня собираются в реальном времени. Бюджеты формируются и распределяются столь же оперативно. Нет необходимости консолидировать средства за определенный период, чтобы спланировать их траты. Сегодня появилась возможность расходовать средства в зависимости от возникающих потребностей и в наиболее прибыльных направлениях, что позволяет получать ранее даже непрогнозировавшуюся прибыль.

Потребитель все чаще обращается к так называемой «шеринговой экономике»[20] – высочайшие темпы просто не позволяют осмыслить происходящее, модные тенденции стремительно возникают и столь же стремительно исчезают. Новые марки, модели возникают и уходят в небытие. Угнаться за этим в одиночку, скупая все, что можно, именно сейчас, уже невозможно.

[20] https://riss.ru/analitycs/48206/

Суть шеринга — в максимально эффективном использовании ресурсов. Автомобиль может везти не только своего владельца, а еще пару его соседей. Если соседи компенсируют часть затрат на бензин, это будет выгодно для всех, а «коэффициент полезного действия» машины будет выше. Этот же принцип касается любых других предметов быта, инструментов, техники, которые вне промышленного производства, как правило, используются лишь малую долю времени.[21]

Мы живем в крупнейшем в мире пункте проката. Шеринг-экономика сегодня — катализатор трансформации бизнеса в глобальную площадку, где люди больше не делят знания и навыки, а делятся ими друг с другом.[22]

К 2025 году мировой объем экономики sharing увеличится почти в 20 раз и достигнет $335 млрд, свидетельствуют данные из отчета PwC. Вдохновленные цифрой, мы пытаемся спрогнозировать, в каких нишах — образовании, HR или финансах — еще можно заработать на шеринге. Хотя вскоре мы можем навсегда уйти от вопроса, кто потребитель, к вопросу, нужен ли он вообще.

Развитие 3D-печати открывает исключительные возможности для персонализации потребления. Сегодня Вы можете заказать уникальные вещи, которые будут только у Вас.

Производитель спортивной одежды и аксессуаров Adidas показал первую серийную модель кроссовок, напечатанных на 3D-принтере. До конца следующего года компания намерена произвести 100 тысяч пар Futurecraft 4D, которые позиционируются как обувь для бега.[23]

Все эти нововведения в несколько раз увеличивает оборачиваемость капитала в экономике.

Если абстрагироваться от конкретных видов бизнеса, то можно выделить ряд общих вопросов, которые необходимо решить с точки зрения организации и ведения электронного бизнеса. В большинстве своем эти системы дублируют аналоги из «традиционного бизнеса» на современном уровне развития общества.

---

[21] https://makeyour.business/theory/sheringovaya-ekonomika/

[22] http://www.forbes.ru/karera-i-svoy-biznes/360815-nado-delitsya-kak-shering-ekonomika-prevrashchaet-potrebitelya-v

[23] http://hitech.vesti.ru/article/652907/

С другой стороны, преимущества электронного бизнеса и использования современных информационных технологий создают предпосылки для формирования новых областей применения, например, для обеспечения деятельности правительств, чем и обусловлено появление термина «электронное правительство».

«Электронное правительство» – концепция осуществления государственного управления, присущая информационному обществу. Она основывается на возможностях компьютерных систем и ценностях открытого гражданского общества. Характеризуется направленностью на потребности граждан, экономической эффективностью, открытостью для общественного контроля и инициативы. Принято считать, что «электронное правительство» состоит из трех основных категорийных модулей (G2G – government to government, правительство правительству; G2B – government to business, правительство бизнесу; G2C – government to citizens, правительство гражданам) и включает в себя многочисленные прикладные элементы: свободу доступа граждан к государственной информации; перевод государственных органов на безбумажное делопроизводство; установление для всех государственных органов показателей эффективности работы на год и регулярный их контроль, который проводится как парламентом, так и гражданами; введение в государственных органах пластиковых карт для идентификации госслужащих, перечисление им зарплаты, расчетов за командировки, перенесение в сеть большинства стандартных транзакций между государством и гражданами, проведение тендеров. Электронное правительство тесно связано с такими компонентами информационного общества, как электронная коммерция, электронный бизнес, электронный банкинг, универсальный доступ к информационным ресурсам, электронное образование. Частным случаем данного понятия является использование систем электронной коммерции в отдельно взятых министерствах и ведомствах.

Вне зависимости от того, в какой сфере человеческой деятельности используются информационные технологии, будь то электронная коммерция или электронное правительство, можно выделить следующие основные технологические процессы, в которых используются современные компьютерные системы:

- юридически значимое оформление документов в электронном виде;

- взаимодействие с клиентами информационных систем, например, заказ товаров и услуг или получение налоговой отчетности;
- доставка товаров и услуг потребителю;
- электронные платежные системы;
- управление организацией;
- кредитование организаций и предприятий.

Применительно к использованию КС существует ряд дополнительных проблем, которые не могут быть решены традиционными методами. К таким специфическим проблемам следует отнести:

- проблемы информационной безопасности;
- создание технологической основы для производства продукции и услуг в сфере обработки и передачи информации;
- страхование информационных рисков.

По существу решение каждой проблемы из перечисленной совокупности сопряжено с созданием соответствующей системы, регулирующей взаимоотношения между различными участниками электронного бизнеса, и обеспечением необходимой технической и технологической поддержки для функционирования. При этом каждая из указанных систем является неотъемлемой частью электронного бизнеса.

Так, например, в традиционной экономике существенная часть всех бизнес-процессов заключалась в идентификации сторон сделки или получателя государственной услуги (нотариальное заверение копий, сканы документов и т.п.). Соответственно, при увеличении количества сделок и получаемых услуг растет в абсолютном измерении время на доказывание очевидного факта, что "я это я". В пределах одного района я и избиратель, и почтовый абонент, и пациент поликлиники, и потребитель услуг ЖКХ, и гражданин, стоящий на учете в военкомате, и т.д., и т.п. И каждый раз подтверждаю это какими-то документами. Возникает естественный вопрос, а можно ли это как-то упростить? На самом деле, мы настолько привыкли предъявлять по каждому поводу документы, что это нас уже не удивляет.

Сейчас в Москве, благодаря предпринятым усилиям, острота проблемы снята. Но она не решена в целом. В случае введения единого идентификатора

гражданина, выдаваемого (или формируемого по биометрическим параметрам) по факту его рождения, можно решить целый ряд проблем.

Или сделать немного сложнее. На основании факта рождения формируется идентификатор по биометрическим параметрам. С его использованием гражданин получает медицинскую помощь, может быть устроен в дошкольное заведение или среднюю школу и т.д.

При наступлении совершеннолетия получает электронную подпись - может голосовать, заключать брак и т.д.

При поступлении на государственную службу или при занятии определенной должности он получает усиленную цифровую подпись - может подписывать документы в соответствии с занимаемой должностью.

Второй аспект, связанный с подписью, это фиксация факта принятия на себя обязательств в соответствии с подготовленным контрактом. Отдельным направлением деятельности, как следствие, становится выяснение перечня контрактов, связанных с конкретным лицом (бюро кредитных историй и т.п.).

Как сейчас. Записываетесь в библиотеку - заполните формуляр, обращаетесь в банк - еще формуляры, полететь в другой город - формуляр в виде именного билета. А можно сделать наоборот. Вот запись обо мне в глобальном банке данных. Вот и связывайте с ней все мои отношения, предусматривающие различные формы ответственности. Если хотите, то глобальная система балльной оценки.

Отдельно остановимся на решении задач информационной безопасности. Традиционно принято считать, что основными задачами информационной безопасности являются:

- обеспечение конфиденциальности информации;
- обеспечение целостности и достоверности информации;
- обеспечение юридической значимости информации;
- обеспечение доступности информации и информационных ресурсов.

Градация приоритетов среди перечисленных задач информационной безопасности является вопросом, решаемым только в конкретных условиях применения, и зависит от требований, предъявляемых непосредственно к информационным системам. Для государственных организаций на первом

месте стоит конфиденциальность, а целостность понимается исключительно как неизменность информации. Для коммерческих структур, вероятно, важнее всего целостность, доступность и юридическая значимость информации. По сравнению с государственными, коммерческие организации более открыты и динамичны, поэтому вероятные угрозы для них отличаются и количественно, и качественно.

Различия будут также и в уровне предъявляемых требований по обеспечению информационной безопасности, которые продиктованы как моделью нарушителя для информационной системы, так и уровнем значимости защищаемой информации. Также различия будут проявляться в типе и уровне используемых средств защиты информации, например, если для клиентов интернет-магазинов, проводящих сделки на небольшие суммы, возможно использование криптографических алгоритмов, реализованных в современных операционных системах (ОС), то для инфраструктуры, обеспечивающей проведение государственных тендеров, должны использоваться совершенно другие решения, прошедшие сертификацию в соответствии с принятой государством политикой сертификации.

Соответственно и комплексы мер защиты информации, применяемых в том или ином случае, будут различными. Если в государственных структурах возможно использование широкого перечня организационных мероприятий в силу того, что информационные системы государственных структур являются более закрытыми, то большинство систем электронной коммерции, используемых коммерческими структурами, является потенциально открытыми, и поэтому здесь организационные мероприятия будут представлены менее значительно и, возможно, будут ограничиваться только регламентами и договорами использования такой системы.

Но если есть децентрализованная безопасность, значит должны быть ресурсы для её обеспечения, а значит скоро возрастет спрос на специализированные дата-центры. Майнинговые фермы в гаражах и сараях сменятся современными вычислительными центрами.

К чему эти рассуждения? Вполне очевидно, у России есть определенные преимущества в этой гонке «ресурсных вооружений». У современного дата-центра три ключевых параметра: площадь здания, энергопотребление (даже точнее, электропотребление) и кондиционирование. Ну, каналы связи, конечно, никто не отменял. Вот и давайте строить мега дата-центр на

«северах» (вот вам площадь и кондиционирование с природной составляющие), возле источников электроэнергии.

Будут масштабные вычислительные ресурсы…, а там посмотрим…

ГЛАВА 4. ЭЛЕКТРОННЫЕ ФИНАНСОВЫЕ РАСЧЕТЫ И КРИПТОВАЛЮТЫ КАК ИНДИКАТОР ЗАПРОСА НА НОВЫЕ ТЕХНОЛОГИИ

Формирование цифровой экономики идет параллельно с формированием киберпространства, поэтому без возникновения технологической основы невозможно говорить о ее существовании.

В киберпространстве не работает классическая физика, не работает химия и биология, не работает и целый ряд иных наук, но при этом некоторые получают иное прочтение и трактовку. Так, лингвистика разворачивается в сторону формирования новых языков, пригодных для межпрограммного или межпроцессного взаимодействия без участия человека. Экономика пытается сохранить свое место под солнцем и уходит в цифровую среду…

Но нужны и новые отрасли знаний, те, которые будут строиться на новых, уникальных характеристиках киберпространства, на новых, еще только выявляемых законах и правилах его функционирования.

Так уж сложилось, что большинство проблем современной экономики и финансов связаны именно с фундаментальными недостатками, принятыми «как есть» бизнес-сообществом, которые просто невозможно устранить, не затронув самих основ современной бизнес-культуры.

Как следствие, возникают новации, в частности введение виртуальной электронной валюты. Это – одно из тех изобретений, которое можно было бы найти у писателя-фантаста прошлого века: электронная криптовалюта, обходящаяся без бумаги и печатного станка и неподконтрольная спецслужбам и правительствам.

Согласно определению межправительственной организации «Группа разработки финансовых мер борьбы с отмыванием денег», криптовалюта – это основанная на математических принципах децентрализованная конвертируемая валюта, которая использует криптографию для создания децентрализованной и защищённой информационной экономики (курсив наш).

4.1. Системы электронных платежей и проблема отмывания денег

Сегодня много говорится о том, что в последние месяцы резко сокращается число гражданских свобод, связанных с беспрепятственным распространением и получением информации. За последние несколько недель под давлением США в ряде стран спешно корректируется законодательство, как-либо связанное с противодействием терроризму. Согласно последним законодательным инициативам Белого дома, к террору приравнены и преступления в области высоких технологий. Для выявления террористов ФБР активно задействует различные системы контроля, в том числе электронные. Сегодня все чаще звучат такие названия как «Carnivore» (система контроля электронных коммуникаций и перехвата сообщений), «Echelon» (глобальная система радиоэлектронной разведки) и др.

Из всего потока информации важнейшей является информация финансовая. Именно здесь сосредоточена настоящая сила. Своевременная информация о финансовых потоках может быть весьма ценной. Оставить без контроля столь значительный кусок глобального информационного пространства для США было бы просто невозможно. Поэтому, еще в 1998 году экспертами корпорации RAND было проведено исследование, результаты которого должны были лечь в основу создания новой системы контроля за финансовыми потоками в системах электронных платежей.

Электронные платежи – сравнительно недавно появившийся класс инструментов на основе платежных систем, поддерживающих электронную передачу наличных средств. Передача наличности в системах этого класса может осуществляться с использованием глобальных сетей типа Internet или с помощью физического перемещения высоко номинальных смарт-карт с записанным значением наличной суммы денег. Новые технологии оплаты предназначены в основном для замены наличных денег в розничной торговле, а также в сделках уровня потребителя.

В силу эффективность и простоты, с которой они заменяют наличность, системы электронных платежей несут в себе и новые вызовы юридическому сопровождению сделок. Существующие технологии, которые реализованы в таких системах, позволяют комбинировать скорость передачи наличности, присущей существующим банковским системам телеграфного перевода, и анонимность валютных вкладов. В результате возникают проблемы, которые должны быть разрешены в процессе развития систем этого класса,

позволяющие гарантировать обнаружение и предотвращение проведения операций по отмыванию денег, а также других нелегальных финансовых сделок.

Как отмечалось выше, еще в 1998 году сотрудники одного из специализированных подразделений Департамента торговли США (сеть по расследованию финансовых преступлений, FinCEN) совместно с экспертами корпорации RAND провели ряд исследований с целью анализа и выявления возможных путей использования современных систем электронных платежей для осуществления операций по отмыванию незаконных финансовых средств.

Первый шаг FinCEN в продвижении этого вопроса имел место в сентябре 1995 года, когда был проведен семинар по данной проблеме в Юридическом институте города Нью-Йорк. Далее, в мае 1996 года сотрудники FinCEN совместно с Национальным университетом обороны, провели масштабные учения по отработке действий, связанных с выявлением незаконных операций по отмыванию денег, проводимых с использованием систем электронных платежей. В ходе этих учений отрабатывался ряд возможных сценариев задействования систем электронных платежей в незаконных операциях.

Системы электронных платежей оказались в сфере интереса Белого дома, Конгресса Соединенных Штатов и ряда других структур. В июле 1997 года, Президент представил доклад относительно Глобальной информационной инфраструктуры (GII), озаглавленный «Основа глобальной электронной торговли» часть которого непосредственно адресована значению систем электронных платежей.

Кроме того, системы электронных платежей являлись темой слушаний, проводимых в 1996 году Подкомиссией по внутренней и международной валютной политике Комитета по банкам и финансовым услугам.

Системы электронной оплаты также удостоились самого пристального внимания и на международном уровне. Многосторонние обсуждения и изучения были предприняты рабочими группами по противодействию отмыванию незаконных средств (FATF) «большой семерки». В июне 1996 года, была добавлена новая рекомендация за № 13 к Рекомендациям FATF. Она констатирует, что «…все страны должен обратить особое внимание на схемы отмывания денег, свойственные новым или развивающимся

технологиям и предпринимать меры, если необходимо, для предотвращения их использования в подобных схемах…».

Классические кредитные или дебетовые карты позволяют их владельцам купить товары и услуги без использования наличных денег, но неизменно вовлекают посредническое финансовое учреждение или эмитента кредитной карты. Напротив, основная характеристика многих современных систем электронных платежей связано с устранением регулирующего третьего лица (например, банка) при передаче денежных средств между двумя (или более) объектами. Возможность передачи наличности через информационные сети без посредничества значительно понижает затраты на совершение сделок. Как результат - экономическая конкурентоспособность и эффективность расширяют пространство сетевого обеспечения, что позволяет значительно расширить круг пользователей подобных услуг, которые в свою очередь требуют новые типы инструментов оплаты.

Глобальные масштабы подобных систем и тот факт, что передача наличности может иметь место с высокой скоростью и степенью анонимности, которая препятствует надлежащему контролю правительственными структурами, является серьезным поводом для беспокойства правительств ряда стран.

Проблема отмывания денег

Традиционные схемы отмывания

Отмывание денег - нелегальная деятельность, посредством которой легализуются преступные доходы. Это функция свойственна практически всем действиям по созданию прибыли преступными сообществами. Так Уголовный кодекс США содержит больше 100 статей, нарушения которых относится к категории преступлений, связанных с отмыванием денег. Эти нарушения охватывают области деятельности от торговли наркотиками и финансового мошенничества, до похищения и шпионажа.

Большинству финансовых транзакций свойственен некоторый след, однозначно привязывающий сумму к конкретной персоне. Преступники избегают использовать традиционные платежные системы типа чеков, кредитных карточек, и т.д., именно в силу наличия этого следа. Они предпочитают использовать наличность потому, что это анонимно. Физическая наличность, однако, имеет весьма существенные неудобства. Прежде всего - это большой объем и масса. Например, 44 фунта кокаина, стоящего 1 миллион долларов, эквивалентен 256 фунтам наличности суммой

в 1 миллион долларов. Наличность больше чем шесть раз превышает вес наркотиков. Существующие платежные системы и наличность - это большие проблемы для преступников. И гораздо больше они для больших межнациональных групп организованной преступности. Законодательное регулирование и банковский контроль увеличили их затраты и риски, связанные с отмыванием средств.

Физическое перемещение больших сумм наличности – самая большая проблема для тех, кто занимается отмыванием денег. Чтобы лучше понимать потенциал для злоупотребления системами электронных платежей с целью отмывания денег, приведем краткое объяснение того, как преступники "узаконивают" наличность через традиционный процесс отмывания денег.

Размещение, иерархическое представление и *интеграция* - термины, обычно используемые, чтобы описать три стадии, через которые легализуются преступные доходы.

Размещение. Размещение - первая стадия в процессе отмывания денег. Именно в течение стадии размещения физическая валюта вводится в финансовую систему, и нелегальные доходы наиболее уязвимы к обнаружению. Когда незаконные суммы денег успешно депонированы в финансовом учреждении, размещение произошло. Законодательно установлено несколько типов транзакций, о которых работники банка должны информировать правоохранительные органы. Преступнику требуется скрывать свои действия, в силу чего им необходимо либо полностью обойти законную финансовую систему, либо нарушить установленные правила. Соответственно, официальные лица, следящие за соблюдением законов, работающие в сотрудничестве с финансовой сферой, находятся в уникальной позиции, способствующей пресечению отмывания денег на этой стадии.

Иерархическое представление. Иерархическое представление описывает деятельность, предпринимаемую с целью затенить след, который оставляет вексель, оплаченный "грязными" деньгами. В течение стадии иерархического представления преступник может проводить ряд финансовых транзакций, чтобы создавать уровни между средствами и их незаконным источником. Например, ряд переводов денежных средств от банка к банку составил бы иерархическое представление. Подобные действия могут быть столь запутанными, что отследить маршрут денег становится очень сложно.

Интеграция. В течение это, конечной стадии в процессе отмывания, незаконные фонды объединяются с суммами денег от законных коммерческих действий, поскольку они вводят в экономику. Таким образом, незаконные средства приобретают законность. Интеграция незаконных сумм денег в законную экономику очень трудно обнаружить, если контрольный след не был установлен в течение стадий иерархического представления или размещения.

СХЕМЫ ОТМЫВАНИЯ ДЕНЕГ

Схемы отмывания денег могут сильно изменяться по характеру и сложности. Они могут вовлекать любой число посредников и использовать традиционные и нетрадиционные платежные системы. В большой степени, возможности и характер операции отмывания денег ограничены только творческим потенциалом лиц, их проводящих. К примеру, международные торговцы наркотиками могут использовать множество различных методов отмывания денег и схем, каждая из которых специально создавалась, чтобы выполнить определенные задачи и достичь определенной цели.

Передовые компьютерные технологии и технологии связи в настоящее время обычно используются, чтобы увеличить эффективность и защиту связанных с наркотиками действий по отмыванию денег. Примеры, которые следуют ниже - базовые схемы, предназначены для ознакомления читателей с несколькими простыми методами для перемещения незаконных средств.

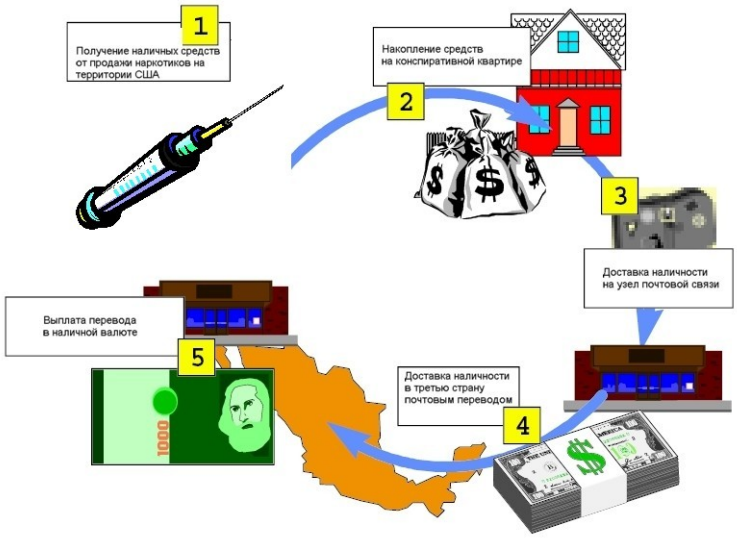


Рис. 4.1. Перемещение денежных средств из США в третью страну (первый вариант)

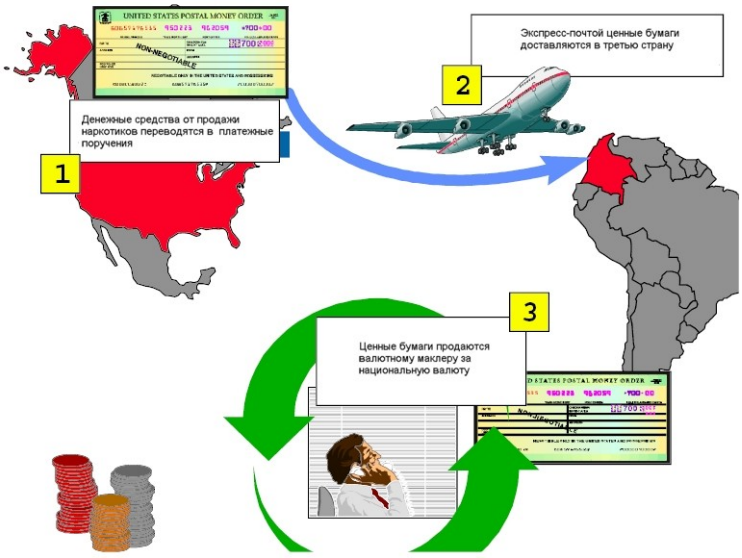


Рис. 4.2. Перемещение денежных средств из США в третью страну (второй вариант)

Пример 1 (Рис. 4.1): Перемещение средств, полученных незаконным путем в США, в третью страну для использования в местной экономике.

1. Продажа наркотиков осуществляется в США (наличность - привилегированная форма расчетов за эти транзакции.).

2. Наличность от одной или множества точек продаж накапливается в бандитском притоне для обработки.

3. Наличность передается для пересылки из страны. Чтобы избежать внимания со стороны правоохранительных органов или банка, наличность может быть разделена на суммы меньше минимально контролируемой суммы (например, 10000 долларов США) и "размыта" (для этой цели привлекается большое количество индивидуумов, чтобы сделать небольшие по сумме депозиты) или структурируется (суммы передаются порциями ниже федеральных требований информирования).

4. Средства пересылаются посредством перевода американским отправителем своему иностранному коллеге.

5. В третьей стране переводы выплачиваются уже в национальной валюте.

Пример 2 (Рис. 2): Перемещение отмытых денег из США в третью страну.

1. Деньги от продажи наркотиков в США переводятся в платежные поручения.

2. Платежные поручения отправляются в третью страну экспресс-почтой.

3. Американские платежные поручения продаются валютному маклеру за национальную валюту страны.

Системы электронных платежей

Краткий обзор технологии

В настоящее время существуют и разрабатываются системы электронных платежей нескольких видов. Между тем, сегодня доминируют два универсальных типа систем: (1) системы на основе смарт-карт, хранящих сумму наличности, и (2) платежные системы на основе сети Internet. Последние разработки показывают, что эти два типа систем останутся доминирующими и в ближайшие годы.

> В настоящее время наблюдается значительный прогресс в разработке стандартов систем электронных платежей. Однако, вопросы финансового взаимодействия (взаиморасчет), и связанные с ними проблемы ответственности между компаниями-эмитентами в различных странах, являются сегодня существенным препятствием на пути продвижения платежных систем этого типа.

Некоторые особенности систем электронных платежей, такие как возможность передачи наличных средств на одном уровне от человека к человеку, при условии анонимности плательщика предлагают клиенту услуги со свойствами гибкости и удобства в обращении с наличностью вместе с расширенной способностью провести закупки на почти глобальном пространстве.

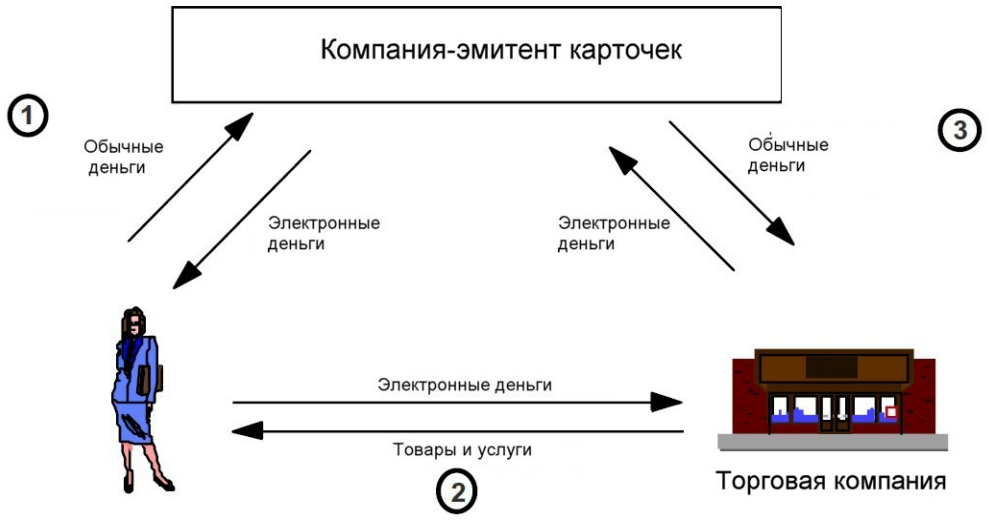
Четыре модели систем электронных платежей

Ниже описываются четыре основных типа построения систем электронных платежей:

1. Модель на основе торговой компании, выполняющей функции эмитента карточек (**Рисунок 3**). В этой модели эмитент смарт-карт и продавец товаров – одна и та же компания.

2. Модель на основе банка-эмитента (**Рисунок 4**). Торговая компания и эмитент карт в этой модели различные стороны. Транзакции осуществляются через традиционные финансовые системы.

3. Модель, в которой эмитент – небанковская компания (**Рисунок 5**). Пользователи покупают электронную наличность у эмитентов, используя традиционные деньги, и тратят электронную наличность в компаниях-участниках системы. Эмитент впоследствии выплачивает электронную наличность фирме-продавцу



4. Одноранговая модель (**Рисунок 6**). Банк или небанковское учреждение выступает в качестве передаточного звена между потребителями. Точка контакта между традиционной системой платежей и электронной наличностью - начальная закупка электронной наличности у

эмитента и выплата электронной наличности со стороны отдельных личностей или торговых фирм.

Все четыре модели позволяют легко добавлять наличные суммы или перемещать их между карточками с использованием различных средств.

Потенциальное использование систем электронных платежей для отмывания денег

Исследование, проведенное экспертами корпорации RAND, было сосредоточено на поиске и исследовании тех возможностей систем электронной оплаты, которые могут быть использованы для осуществления операций по отмыванию незаконных финансовых средств. По своей природе системы электронных платежей имеют потенциал, позволяющий решить одну из самых серьезных проблем для теневого бизнеса - физическое перемещение больших количеств наличности.

Глобализация многих существующих систем электронных платежей дает возможность преступникам использовать национальные различия в стандартах защиты и правилах надзора, чтобы скрыть движение незаконных средств.

Выполненные исследования идентифицировали множество особенностей транзакций в системах электронных платежей, которые правоохранительные органы должны внимательно изучить. Среди них - (1)

отказ от посредничества; (2) банк или небанковское учреждение в качестве эмитента карт; (3) одноранговые транзакции; (4) операционная анонимность и (5) пределы номинирования и даты истечения срока действия карт.

Каждая из этих базисных особенностей ниже описана более подробно. С одной стороны эти базисные особенности делают системы электронных платежей привлекательными в качестве потенциальных средств, позволяющих уменьшить стоимости транзакции в торговле и способствовать увеличенной эффективности экономики, с другой - эти особенности определяют и те уязвимости, которые могут использоваться преступниками.

Отказ от посредничества. Исторически правоохранительная деятельность и регулирующие организации положились на посредничество банков и других регулируемых финансовых учреждений, чтобы обеспечить "точки перехвата", через который средства должны проходить и где возможно получить полный отчет об их происхождении.

Отказ от посредничества вовлекает передачу средств между объектами без промежуточного вовлечения третьего лица, подчиненного правительственному надзору (например, требования регистрации через банк). Если системы электронных платежей разрешают передачи средств без посредничества в неограниченных количествах, преступники могут использовать это как возможность избежать традиционных методов отслеживания перемещения денежных средств.

Банк и небанковское учреждения в качестве эмитента карт. Банки и небанковские учреждения могут быть подчинены различным правилам относительно их операций с системами электронных платежей. Это различие уже имеет место в нескольких странах, где небанковское учреждение эмитенты карт систем электронных платежей в настоящее время подчиненно набору правил, отличному от такового для банков. Простое расширение требований, сформированных ранее для традиционной платежной системы, к новому небанковскому учреждению-эмитенту карт может вызвать ряд претензий со стороны клиентов о возможных злоупотреблениях.

Однако новые системы построены по-другому и постоянно видоизменяются, так что принцип "один размер соответствует всему" не будет оптимальным.

Одноранговые передачи. Некоторые системы электронных платежей позволяют потребителям передавать значение одноранговый (и таким образом, без посредника) использование электронной "инкассаторской

сумки", телефона, или Internet. Такая возможность возможно таит в себе прямой вызов правительственному надзору в системах электронных платежей. При отсутствии сведений или доказательств из других источников (например, физическое наблюдение), одноранговые передачи, вряд ли, могут быть обнаружены.

Операционная анонимность. В некоторых находящихся на стадии становления системах электронных платежей, точка введения средств в систему непрозрачна и тождество объекта, передающего их, весьма трудно определить. Фактически анонимность плательщика (тождество стороны, инициализирующей передачу наличности в систему электронных платежей) – основная характеристика некоторых предложенных систем. При передаче наличности в систему электронных платежей (например, через Internet или телефонную сеть) операционная анонимность могла бы стать почти непреодолимым барьером для обнаружения таких операций. В то время как варианты решения для этой проблемы были выдвинуты, они поднимают проблемы относительно сохранения тайны частных вкладов.

Пределы номинирования и даты истечения срока действия карт. Создатели систем электронных платежей, вероятно, ограничат максимальные суммы, которые могут быть сохранены на карточках, уменьшая тем самым риск мошенничества или других потерь. Как с кредитными карточками, эмитенты систем электронных платежей также вероятно установят пределы достоинства на основе потребностей, которые были бы определены рекламой и конъюктурными факторами. Так недавние испытания потребителя систем электронных платежей указывают вероятные пределы потребителя приблизительно 1,000 $ - 3,000 $. Системы электронных платежей, между организациями, вероятно, будут иметь намного больший предел номинирования чем те, для индивидуальных клиентов, и будут широко различаться между фирмами.

Карты в системе электронных платежей могут быть запрограммированы так, чтобы прекращать свою работу после некоторого числа передач.

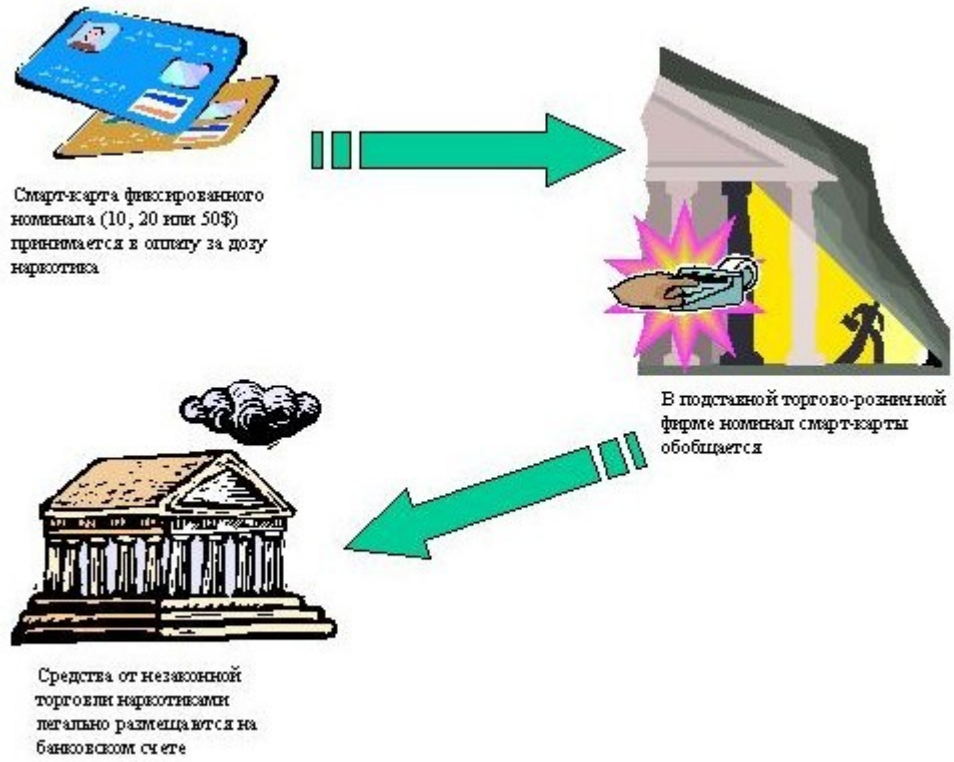
Чем больше электронные платежные системы подражают валюте, тем больше вероятность того, что записи о транзакции будут ограничены. Так в некоторых образцах, может фиксироваться тольк ограниченное число самых последних транзакций.

Некоторые примеры по использованию систем электронных платежей для отмывания денежных средств

Оба рассматриваемых примера основываются на использовании высокономинальных смарт-карт.

Уличный сбыт наркотиков

В этом примере (см. **Рисунок 7**) наркотики продаются пользователям в обмен на одноразовые карточки, номиналом, типично связываемых с транзакциями наркотиков - 20$, 50 $, или 100 $. Эти карточки собираются торговцем наркотиками и реализуются через подставную фирму в области розничной торговли. Эта фирма передает электронное значение карточек со своих терминалов в банк. Фирма получает некоторую плату за использование ее возможностей.



Как только средства введены в законную платежную систему, они перемещаются по всей цепочке стандартного процесса отмывания и вводятся в экономику третьей страны.

Два типа передачи наличности в системах электронных платежей

В этом примере (см. **Рисунок 8**) средства, полученные от деятельности незаконного оборота наркотиков, и размещенные на смарт-карте могут быть переданы, по крайней мере, двумя простыми способами. Возможно наиболее предсказуемый способ движения средств - через физическое перемещение высоко номинальных карт, содержащие доходы незаконного оборота наркотиков. Из-за их небольшого размера эти карточки могут быть легко и надежно скрыты, и в конечном счете быть обналиченными через повторное депонирование, но уже в зарубежной стране.

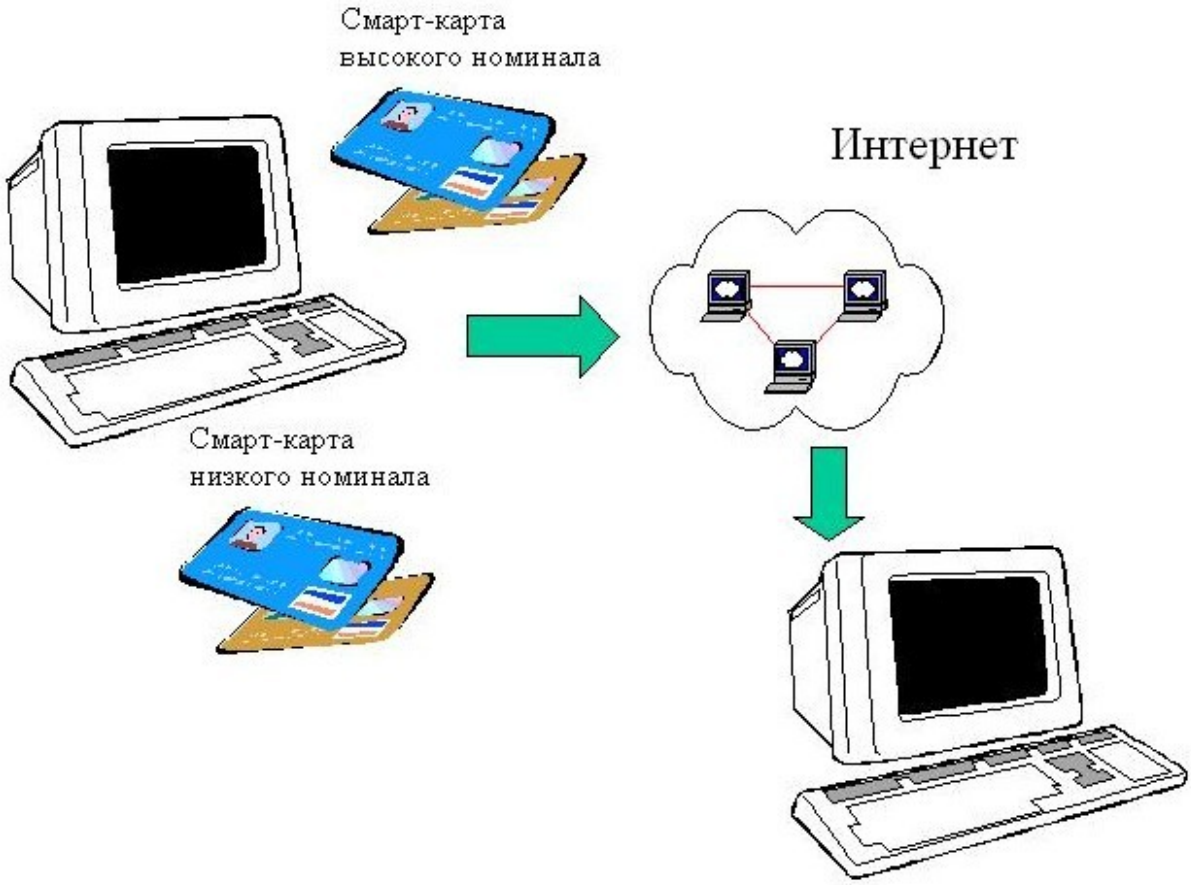
Второй путь транспортировки средств вне досягаемости полномочий правоохранительных органов может состоять в передаче средств на карточке по телефону. И сотовые и обычные аналоговые телефоны легко взаимодействуют с различными сервисами, позволяющими выполнить подобные операции.

Как только фонды вводят платежную систему, они являются неотличимыми от фондов, полученных из законных источников.

Переводы денежных средств через системы на основе Интернет

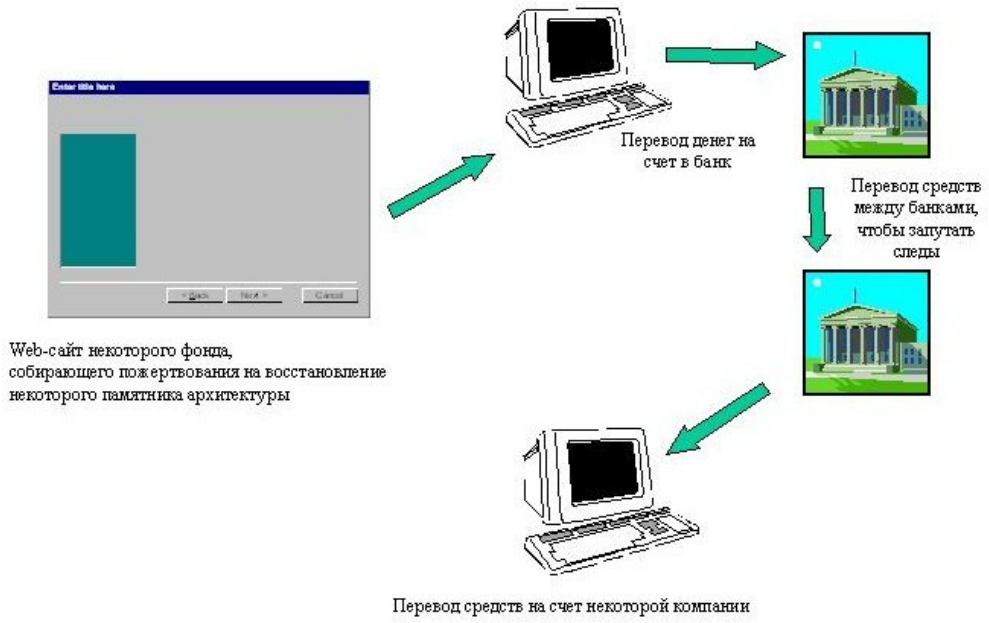
В этом примере (см. **Рисунок 9**) с низко номинальных карт значение передается на персональные компьютеры, которые передают это значение по

Internet, используя все более и более доступные анонимные сервисы, чтобы скрыть пункты поступления незаконных средств. Получатель средств имеет возможность объединить низкономинальные платежи и повторно интегрировать их в платежную систему.



Электронные деньги и всемирная паутина

Последний пример незаконного использования системы электронных платежей (см. **Рисунок 10**) проводится под флагом милосердия, которое служит только прикрытием для получения денежных переводов в виде пожертвований. Фонды, изначально созданные как благотворительные, и честно выполнявшие свою миссию, вместе с тем могли выступать в качестве одного из звеньев цепочки по отмыванию преступных средств с использованием систем электронной оплаты.



В таких системах денежные средства могли быть переведены из электронных кошельков на компьютерах владельцев на банковский счет, а затем перечислены из одного финансового учреждения в другое, расположенное в произвольном месте планеты, законы которого наиболее благоприятны для инвестирования незаконных средств в реальную экономику.

ПОДГОТОВКА К ДЕЙСТВИЮ

Участники проведенного исследования, вне зависимости от их взглядов на отдельные вопросы, сошлись во мнении, что участие правительства необходимо. Оно требуется для начала диалога о том, как обеспечить соответствующее регулирование и организацию действий правоохранительных органов, необходимых для налаживания эффективной работы систем электронных платежей как действующих, так и находящихся в стадии проектирования. Сегодня правительство США, понимая роль и место систем электронных платежей в процессе формирования бюджета мировых террористических организаций, активно участвует в работах по предотвращению использования передовых технологий в финансовой сфере для финансирования преступного сообщества.

Анализ существующих и перспективных технологий и технических особенностей нового класса систем - первый шаг к пониманию применения в их отношении существующих правоприменительных норм, а также шаг на пути формирования новых законодательных актов. Как известно,

большинство систем электронной оплаты разрабатываются коммерческими фирмами. Наличие конкуренции в этой сфере позволяет организовать работы с привлечением самых совершенных информационных технологий. В этой связи желательно, чтобы правительство развернуло диалог с частным сектором по вопросу совершенствования нормативной и правовой базы по системам электронных платежей, включая обеспечение информационной безопасности в таких системах. Информация, полученная в результате проведенного исследования, способствовала проведению тщательной оценке угроз безопасности, характерных для систем электронных платежей.

Какие выводы можно сделать после изучения материалов RAND по вопросу использования систем электронной оплаты для отмывания денег? Прежде всего – это то, что исследования показали существование широкой области проблем, связанных с обеспечением контроля в системах такого рода, а также связанных с обеспечением информационной безопасности. Существующая правоприменительная практика не всегда может эффективно решать вопросы, связанные с предотвращением использования систем электронных платежей для отмывания денег.

Необходимо широкое сотрудничество и совместные действия правительства и разработчиков систем электронных платежей, а также правительств ведущих государств с тем, чтобы перекрыть каналы легализации незаконных финансовых средств с использованием систем электронных платежей. Международное сотрудничество, практически, единственный действенный способ реально перекрыть такие потоки.

Сотрудничество в области стандартов, регулирующих прозрачность, и активный контроль за возможной эксплуатацией выявленных уязвимостей в интересах преступных группировок является ключом успешной защите систем электронной оплаты от злоупотребления. Кроме того, сама проблема отмывания денег международная. Эффективная правоприменительная деятельность требуется, чтобы национальные правительства сотрудничали в урегулировании основных правил создания систем электронных платежей и операций с их применением.

Выполненное исследование послужило своеобразным полигоном, на котором прототипы подобных международных действий в рамках отработки политики функционирования систем электронных платежей могли быть отработаны. В будущем, расширение моделирования, чтобы включить международных участников учло бы более глубокое понимание вовлеченных

вызовов. В свою очередь, исследование высветило важность согласования подходов к контролю за системами электронных платежей. Опасность, что преступники будут стремиться эксплуатировать слабости в инструкциях везде, где они появляются, предлагает, чтобы правительства были должны координировать исследовательский и действия принуждения, нацеленные, свертывая потенциальное злоупотребление.

В то время как пока еще преждевременно говорить о формировании проекта всестороннего регулирующего режима для систем электронных платежей, необходим расширенный и более глубокий диалог между компаниями-эмитентами кар, правительством и разработчиками систем поможет сформировать направление такого режима. Авторы также надеются, что понимание проблем, поставленных в исследовании, помогут в продвижении общественных дебатов по организации надежной защиты системы электронных платежей и в определении необходимой роли для правительства в этом быстро растущем секторе Глобальной Информационной Инфраструктуры.

4.2. Технологические предпосылки возникновения криптовалют

В настоящее время существует достаточно много объяснений феномену появления и популярности криптовалют. Из всего множества наиболее рациональным, на взгляд авторов, является версия о «плате» за ресурс.

Вспомним, например, практически забытую сеть FIDO, где залогом существования сети были вычислительные ресурсы, предоставляемые в общее пользование «нодами». Основной проблемой существования сети было то, что она действовала фактически на энтузиазме ее организаторов, которые предоставляли во всеобщее пользование дисковое пространство и свободное время телефонной линии.

Как представляется, идея оценки востребованности ресурса лежала на поверхности. Если есть то, что востребовано, то у владельца возникает естественное желание это каким-либо образом измерить и результат измерения зафиксировать. Востребованность сайта можно измерить с помощью счетчика посещений, востребованность личной страницы – с помощью количества подписчиков и «лайков». Вместе с тем, есть ряд ресурсов, для которых требуется какая-то своя единица потребления, причем фиатные деньги в данном случае стоят даже не на первом месте.

Для иллюстрации идей, лежащих в основе криптовалют, позволим вспомнить еще один пример, датирующийся, ориентировочно концом прошлого века. Имитировался полет к одной из планет, испытатель жил в замкнутой оранжерее, получая кислород и часть питания от растений. При этом растения, насекомые и, если не изменяет память, животные были подобраны таким образом, чтобы самодостаточную экосистему. Пример приведен для того, чтобы подчеркнуть устойчивость системы, основанную на организации полного цикла оборота ресурсов внутри замкнутого контура. Это один из вариантов организации системы, где все элементы одновременно являются и донорами и реципиентами. В реальной жизни создать полностью замкнутую систему, как правило, не удается и объем ресурсов, предоставляемых со стороны доноров, меньше, чем объем ресурсов, запрашиваемых реципиентами. Как следствие, возникает идея создания промежуточного механизма балансировки спроса и предложения. По аналогии с фиатными валютами, возможно введение условных денег с динамическим формированием «цены» на ресурсы.

В работе [6] исследовались свойства киберпространства с точки зрения противоборства. Но киберпространство может быть и средой кооперации! Пытаясь осознать явление, условно называемое обобщенным понятием «блокчейн», в первую очередь необходимо определиться с теми отношениями, которые формируют его идеологию.

Представляется, что идеи, лежащие в основе появления криптовалют, заключаются в том, чтобы создать систему равновесного обмена ресурсами. Часть ресурсов в киберпространстве может иметь физический характер (дисковая память, пропускная способность канала), часть – временной (квант времени центрального процессора, выделяемого на решение конкретной прикладной задачи), часть – информационной (получение доступа к той информации, в которой заинтересован потребитель). Если реципиент не может обеспечить вклад в систему соответствующими ресурсами, он может расплатиться некими условными единицами, которые и являются прототипом криптовалют. В любом случае, в основе системы будет лежать простая идея равновесного обмена.

Основываясь на текущем понимании процессов, с точки зрения авторов, можно выделить три этапа формирования киберпространства.

I этап. Отдельные компьютеры стали объединяться в сети. Предпосылки к формированию киберпространства возникли в виде передачи пакетов данных

и файлов. Основные затраты по поддержанию киберпространства лежали на конечных пользователях компьютеров.

II этап. Стали выделяться ресурсы и сервисы общего пользования, например, в виде поисковых и почтовых сервисов. Основные затраты на поддержание киберпространства лежали на провайдерских компаниях (физическая связность) и компаниях, предоставляющих различные публичные сервисы (логическая связность).

III этап. Резкое увеличение количества устройств, предназначенных для функционирования в составе сети (смартфоны, нетбуки, Интернет вещей и т.п.). Поддержание киберпространства обеспечивается уже, в том числе, как за счет производителей различного оборудования, так и за счет их пользователей. Возникает эффект самовоспроизведения киберпространства.

Как представляется, мы сейчас стоим на пороге **IV этапа**, в котором вклад каждого будет оцениваться через общую меру. Ведь мы за присутствие в киберпространстве платили всегда. Сначала мы платили дефицитными вычислительными ресурсами собственных компьютеров. Затем наступил момент, когда компьютеры подешевели и критичным ресурсом стал трафик. Не за горами монетизация публичных сервисов. И, в данном случае, появление криптовалюты первый шаг в данном направлении.

Если говорить точнее, то примером платы пользователей/реципиентов за ресурсы системы (платформы) является gas в Ethereum'е[24]. В других публичных сервисах есть более яркие примеры монетизации.

Достижения современных информационных технологий позволяют кардинально перестроить экономику: от момента зарождения стоимости, до ее монетизации.

Сегодня, к примеру, появилась возможность монетизировать такие феномены, как популярность того или иного сайта или страницы в Сети. Можно монетизировать и популярность того или иного деятеля культуры и искусства или отдельного произведения, модного течения и др. Достичь этого традиционными средствами крайне сложно.

Еще одним стимулом распространения криптовалют является желание пользователей организовать как можно более широкий обмен ресурсами в рамках всего киберпространства. В этом случае криптовалюта берет на себя

[24] https://bitblog.tech/2017/03/28/chto-takoe-gas-v-ethereum/

функцию обмена товарами, как у фиатных денег, вне зависимости от того, какие сервисы возникнут в будущем, какие ресурсы они будут потреблять и какие вырабатывать.

С точки зрения организаторов бизнеса, так или иначе связанного с функционированием киберпространства, появление платы за потребляемые ресурсы позволит в перспективе, более равномерно распределить нагрузку затрат и, соответственно, прибыли по стеку инфраструктурных сервисов. Поясним сказанное на примере из другой области. Пусть есть Интернет-магазин, торгующий, например, дорогой косметикой. В отдаленную деревню этот магазин отправляет заказанный товар обычной почтовой посылкой. Для конечного пользователя итоговая цена товара складывается из двух частей: стоимости товара в Интернет-магазине и стоимости доставки. Исходя из имеющихся в открытых источниках отзывах, маржинальность продажи существенно превышает маржинальность доставки, что не устраивает почтовую сеть. Необходимо отметить, что в условиях Российской Федерации такая балансировка прибыли может способствовать развитию сетевой инфраструктуры, «цифровизации» населения и, в конечном итоге, определенному выравниваю в плане доступности различного рода услуг, включая телемедицину и удаленное образование, а также создание новых высокотехнологичных рабочих мест.

Таким образом, можно утверждать, что в основе создания и обращения криптовалют лежит идея кооперации провайдеров сервисов и услуг, а также пользователей в киберпространстве.

4.3. Финансово-экономические предпосылки возникновения криптовалют

Как отмечено в [1], актуальность создания новых валютных систем, их возможные место и роль могут быть правильно поняты только в контексте фундаментальных проблем мировой финансовой системы и при сопоставлении с альтернативными предложениями по ее реформирования.

При оценке возможного места криптовалюты в экономической системе необходимо вспомнить о функциях денег.

Деньги выполняют следующие пять функций: мера стоимости, средство обращения, средство платежа, средство накопления и сбережения, мировые деньги. В роли мировых деньги функционируют как всеобщее платежное

средство, всеобщее покупательное средство и всеобщая материализация общественного богатства.

Как показало время, наиболее важным свойством денег является не то, кто их выпустил, и даже не то, насколько они портативны или долговечны, а количество людей, готовых их использовать. В XX веке доллар получил и сохранил статус мировой валюты во многом потому, что большинство людей в мире считали, что США и их финансовая система имеют лучшие шансы выстоять в любых кризисах, чем другие страны. Это объясняет, почему многие люди предпочитают хранить свои сбережения в долларах.

Современная мировая валютная система сформировалась по итогам четырех ключевых событий XX века: отмены золотого стандарта в США (1933 г.), заключения Бреттон-Вудского соглашения, которое предоставило доллару США статус мировой резервной валюты (1944 г.), отказа США обменивать доллары на золото (1971 г.), образования Ямайской валютной системы (1976-1978 гг.), положивший конец Бреттон-Вудскому международному соглашению. В настоящее время цена валюты определяется на свободном рынке Forex, хотя в финансовых операциях доминирует доллар США.

Ценность денег основана на доверии. Финансовый кризис 2008 г. подорвал доверие к ведущим мировым валютам, доллару и евро. 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 ломают головы над тем, как можно решить проблему создания новой валютной системы.

Кто-то призывал вернуться к золотому стандарту, другие рассматривали свободную от процентов валюту, выпускаемую минфином без участия центральных банков (например, директива 11110 Дж.Ф. Кеннеди от 4 июля 1963 г.). Защитники золота уверяют, что бумажная валюта (которая, по их мнению, ничем не обеспечена) не является деньгами, т.к. не имеет сырьевой стоимости. Золотые и серебряные монеты (товарные деньги) и 100% обмениваемые на золото депозиты (расписки) многими считаются единственно правильной и честной денежной системой.

Ответное основное возражение критиков золота заключается в том, что его запасы не бесконечны, и им также можно манипулировать. Но всё зависит от цены золота, а также от возможности привлечения в оборот ювелирного золота, как это было в США во времена Великой депрессии.

Для обеспечения объективной устойчивости валютной системы необходимо, чтобы валюта обладала мерой стоимости. Это – необходимое стратегическое условие. Без этого доверие к ней рано и поздно будет утрачено.

Депозиты и накопительные фонды себя исчерпали – стоимость обездвиженного хранения финансовых ресурсов сегодня выросла в разы.

Отрицательные ставки стали реальностью современного финансового мира еще несколько лет назад. Национальный банк Швеции, Riksbank, в 2009 году стал первым современным ЦБ, который стал брать у своих клиентов плату за принятые от них на корсчета деньги, т.е. ввел, таким образом, отрицательную депозитную ставку.

Падение американского корпоративного гиганта Enron в 2001 году стало символом завершения эры традиционных корпораций – этого символа XX века. Это падение, фактически, подтвердило на практике наличие стратегических, масштабных и всеобъемлющих проблем, лежащих в самой сути выстроенных корпоративных отношений. Ситуация, подобная Enron должна была проявиться. Более того, Enron стал, фактически, «козлом отпущения», приняв на себя во многом ответственность за существовавшие (а в ряде случаев и продолжающие существовать) проблемы современных корпоративных кодексов поведения.

Если коротко, то суть проблемы Enron в механизмах, использованных менеджментом корпорации, для манипулирования статистическими данными отчетности. Сформированные «инструменты» позволяли, оставаясь формально в рамках действующего законодательства, совершать действия, лежащие за гранью легитимного бизнеса[25].

Фактически, бюджеты корпорации формировались не по результату выполнения проектов, а лишь по результатам планируемой прибыли за выполненный проект.

[25] https://www.nur.kz/1051288-kak-enron-obmanula-vsekh-vklyuchaya-sebya.html

Как сегодня отмечается в ряде исследований, посвященных анализу краха Enron[26], менеджмент корпорации делал две основные вещи: одна - то, что называется market-to-market accounting (рыночная переоценка), другая – structured finance (структурированные финансы).

Самый простой способ заработать деньги на market-to-market accounting, если вы делаете это непрозрачно и в тайне от других, это заключить две сделки: одну на продажу газа через двадцать лет, другую – на покупку газа, и поставить туда разные предположения о цене газа через двадцать лет.

Но главной «фишкой» тогда стало «изобретение» структурированных финансов - за три года было создано три тысячи юридических лиц, включая 800 офшорных компаний. Эта магия была устроена так: вместо того, чтобы занимать какие-то деньги, Enron вместе с кредиторами, типа Citibank, например, открывал офшорную компанию, на эту офшорную компанию привлекался долг.

Если принять обобщенный результат, то, фактически, менеджмент Enron лишь грамотно воспользовался теми фундаментальными проблемами, которые накопились в практике корпоративного управления к концу XX века.

Дополнив эту картину действиями аудитора, компании Arthur Andersen, основанной в 1913 году в Чикаго, которая в течение 90 лет была одной из самых успешных аудиторских компаний мира. Тогда самым крупным клиентом хьюстонского офиса Arthur Andersen был именно Enron, плативший ей за аудит до $20 млн в год и еще столько же – за консалтинг. Взвесив все риски и преимущества, аудиторы просто не захотели терять такого клиента, и выдавали такое заключение, каким его хотели видеть в Enron, даже когда несоответствия в отчетности были более чем очевидны. А потом сотрудники Arthur Andersen и вовсе совершили свой главный «шаг»: они стали уничтожать документы…

Актуальность разработки и применения электронных цифровых валют существенно стимулировалась не только долгосрочными, но и текущими проблемами финансовой системы. Дело в том, что существующая система денежных переводов устарела и явно нуждалась в инновациях. Иначе говоря, мировые деньги стали в недостаточной мере выполнять одну из своих основных функций – быть эффективными средствами платежа.

[26] Там же

В марте 2012 г. Федеральная резервная система США провела однодневную конференцию по теме денежных переводов, в ходе которой чётко обозначилось, что: система национальных переводов базируется на разработках 60-х годов XX века. Любой платёж проходил минимум один банковский день. Для большинства американцев наиболее простым и быстрым способом передавать деньги стала чековая книжка. И это проблема относится не только к США.

Несостоятельность традиционной платёжной системы стала особенно очевидной во время финансового кризиса, когда банк Morgan Stanley, обслуживающий Уолл-стрит, договорился о кредите в размере $9 млрд. с одним японским банком. Кредитный договор был подписан в воскресенье, но осуществить перевод в ближайшие дни оказалось невозможно, поскольку в выходные платёжная система не работает, а на понедельник выпал праздничный день. Так выяснилось, что даже банки не способны пересылать друг другу деньги в выходные дни. Для того, чтобы обойти это ограничение, японскому банку пришлось пойти на абсурдные действия – выписать бумажный чек на $9 млрд. [6].

Хотя в Биткойне трансакции осуществляются не мгновенно, для их надёжного прохождения нужно лишь подтверждение майнера и включения в блокчейн, на что затрачивается десятки минут. Это – не несколько часов, дней или недель. В итоге биткойн-транзакции оказывались гораздо быстрее, чем традиционные методы.

По мнению сторонников криптовалют, ротенциал основанной на технологии Биткойн сети BitPay, как более быстрой и экономичной платёжной системы, с практической точки зрения представляет преимущество более ценное, чем анонимность участников и идеологические плюсы децентрализации [6]. Комиссия системы BitPay составляла 1% от суммы перевода, в то время как традиционные платёжные сервисы взимали 2-3% за каждую транзакцию.

Таким образом, в настоящее время уже чётко обозначилось одно из позитивных свойств электронных денег – быть эффективным средством платежа.

Для того, чтобы понять, как и, главное, насколько криптовалюты соответствует другим функциям денег, нужно вспомнить об их технологических основах. Тем более, что по ходу изложения уже возникла необходимость пояснения некоторых терминов и словосочетаний.

4.4. Идеология, положенная в основу криптовалют

Истоки идеологии криптовалют и блокчейна, как сопутствующей им технологии, в разных источниках принято искать в работах до сих пор неидентифицированного Сатоши Накамото. Вместе с тем, представляется более целесообразным в качестве такого источника определить более ранние по времени работы шифропанков, которые не только вели практические разработки, но и пытались формировать за счет внедренных технологий отношения между людьми.

Если проанализировать относительно краткую ретроспективу развития научно-технической мысли, то можно выделить две проблемы, носящие фундаментальный характер: обеспечение качества управления и обеспечение защиты хранимых и передаваемых данных.

До какого-то момента эти две проблемы развивались параллельно, причем и в том, и в другом случае прорабатывались подходы, связанные с наличием некоего ключевого элемента решения. Так, например, при защите данных таким ключевым элементом был ключ шифрования. При управлении – само управляющее звено.

С развитием технологии коммуникаций стала развиваться идея децентрализованного управления, т.н. «нетократии»[27] или сетевого сообщества, которое достаточно хорошо применимо для решения определенного класса задач. При этом основным инструментом реализации стали социальные сети, по оценкам специалистов способствующие в ряде случаев реализации сценариев «цветных революций».

Слабым моментом социальных сетей стала их особенность, рассматриваемая поначалу как преимущество – анонимность участников. Очевидно, сейчас не составит труда зарегистрировать и «вырастить» в любой из социальных сетей «бота». Поэтому у оппонентов при противостоянии в виртуальном пространстве всегда есть возможность утверждать, что выраженное мнение в виде лайков или комментариев есть продукция информационного противостояния.

Внедрение традиционных схем защиты, связанных, например, с цифровой подписью, приводит к утверждениям про «ключи от неба» или, в данном примере, от удостоверяющего центра. Имеет смысл повторить еще раз: при традиционном подходе с ключевым элементом защищается именно он, но

[27] https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%82%D0%BE%D0%BA%D1%80%D0%B0%D1%82%D0%B8%D1%8F

при этом возникает проблема – кто сторожит самого сторожа. Именно это часто становится объектом критики.

Внедрение технологии блокчейн в социальные сети в корне изменит ситуацию. Ведь особенность технологии блокчейн – это децентрализованная защита. Значит, появляется возможность независимой проверки аккаунта – человек это или бот, а значит, децентрализованное управление через социальные сети приобретает принципиально новое качество, которое, пока нет русскоязычного термина, можно назвать «trusted community»[28].

Человеком, который заложил основы идеологии шифропанков, считается Дэвид Чаум, который в 1982 году получил степень доктора информатики и делового управления в Калифорнийском университете Беркли (University of California, Berkeley). Но еще раньше, в 1981 г. Чаум опубликовал работу «Неотслеживаемая электронная почта, обратные адреса и цифровые псевдонимы», положившую начало исследованиям в области зашифрованных коммуникаций в интернете.

«Вы должны объяснить своим читателям, насколько это важно, — сказал он однажды журналистам издания Wired. ***— В киберпространстве нет физических ограничений, нет никаких стен. Это совершенно другое, жуткое и странное место, и вопрос идентификации здесь — чистый кошмар. Понимаете? Все, что вы делаете, может видеть другой человек, все может быть записано навсегда. Это резко противоречит основному принципу демократии».***

[28] «доверенное сообщество», «сообщество, члены которого доверяют друг другу»

Ориентировочно в 1990 году им была создана компания DigiCash, создавшая первую криптовалюту eCash. Финансовый неуспех компании менее чем за 10 лет привел к отказу от использования первой криптовалюты.

«Несмотря на то, что технология не преуспела в бизнес-формате, идеи Чаума вдохновили группу криптографов, хакеров и активистов, связанных между собой электронной почтовой рассылкой. Именно эта группа, в которую входили члены команды DigiCash Ник Сабо и Зуко Уилкокс О'херн [ZCash], станет известна как шифропанки.

Первоначально криптовалюты задумывались именно как самостоятельная полноценная виртуальная денежная единица, независимая от государства, как новая модель социальной организации, лишённая центрального управления, функционирующая силами примкнувших к ней людей.

Показательны идеалистичные высказывания энтузиастов (они называли себя шифропанками) этих проектов [6], находящихся в эйфории от первых успехов.

«Главная цель того, чем мы занимаемся – это отправить Большого брата на свалку истории. Не стоит недооценивать эту задачу. Возможно, когда-нибудь мы оглянемся и увидим, что это было самое важное из всего, что мы сделали» (Хэл Финни).

«Мы хотим создать полностью анонимные средства обмена с минимальной комиссией. Если у нас это получится, банки постигнет участь динозавров, чего они в полной мере заслужили» (Бэк).

«Биткойн – это самое важное изобретение человечества после Интернета. Весь мир скоро будет вести бизнес совсем по-другому» (Роджер Вер).

«Финансовая сеть с открытой архитектурой – это то, что нужно, чтобы встряхнуть привилегированные элиты, которые получали непропорциональную долю прибыли от существующей финансовой системы» (Патрик Мерк).

Вероятно, представители этой группы придерживались даже более радикальных взглядов, чем сам Чаум. В течение 1990-х годов и в начале 2000-х они внесли несколько предложений в контексте электронных денежных систем. И только в 2008 году, через десять лет после падения DigiCash, некто «Сатоши Накамото» представил протокол биткоина в еще одной рассылке, которая стала преемником группы шифропанков.

Биткоин и eCash имеют мало общего. Ключевым моментом было то, что централизованный контроль над eCash находился в руках DigiCash и технология не смогла предложить полностью независимую валюту. Даже в том случае, если бы каждая транзакция в мире проводилась с помощью eCash, необходимость в банках оставалась бы для открытия счетов и подтверждения транзакций. Это означает, что, несмотря на приватность, eCash был не сильно устойчив к цензуре. И если WikiLeaks удалось получать финансирование в биткоинах в ходе банковской блокады, то с eCash это было бы невозможным, поскольку у банков были бы полномочия по блокировке счетов организации.»[29]

Вот здесь интересно рассмотреть первый посыл Д.Чаума. «Никто не должен знать, кому и сколько я плачу денег». Следующим этапом развития идей становится появление биткоина. «Никто не сможет заблокировать получение мной денег, никто не сможет заблокировать мой платеж».

В этой связи интересно будет процитировать текст, озаглавленный следующим образом: «Джулиан Ассанж совместно с Джейкобом Аппельбаумом, Энди Мюллер-Магуном, Жереми Циммерманом. Шифропанки: свобода и будущее интернета. Интернет – это угроза всей человеческой цивилизации.» В России эта книга выпущена в 2014 году, но судя по дате проверки ссылок, она подготовлена к опубликованию в конце 2012 года.

«Новый мир интернета, отделившийся от старого мира неодушевленных атомов, жаждал независимости. Однако государства и их друзья решили поместить его под колпак, заполучив власть над его физическими носителями… А потом государство воплотит все, чему научилось, в реальном мире: оно станет развязывать войны, нацеливать беспилотные боевые машины, манипулировать комитетами ООН и торговыми соглашениями, а также оказывать услуги обширной сети скованных одной цепью бизнесменов, инсайдеров и коррупционеров.

Но мы нашли средство против государства. Это наша единственная надежда на противодействие тотальной власти. Надежда на то, что храбрость, вдохновение и солидарность помогут нам оказать сопротивление. Мы обнаружили странное свойство физической вселенной, в которой живем.

Вселенная верит в шифрование.

[29] https://forklog.com/genezis-arhivy-ecash-devida-chauma-i-rozhdenie-mechty-shifropankov/

Зашифровать информацию легче, чем расшифровать.

Мы поняли, что сможем использовать это свойство, чтобы создать законы нового мира. Чтобы отделить наше новое платоновское царство от его физических носителей в виде спутников, подводных кабелей – и тех, кому они принадлежат. Укрыть наше пространство за криптографической завесой. Создать новые земли, закрытые для тех, кто контролирует физическую реальность, – ведь для того, чтобы следить за нами, им понадобятся бесконечные ресурсы.»

Цитата достаточно длинная, но весьма показательная. Во-первых шифропанки мыслят категорией киберпространства, отделенного от физического пространства, в котором они могут считать себя свободными личностями. В этой связи становится понятным указание в анонсах различных криптовалютных платформ на «справедливость» оплаты и обмена данными. Во-вторых, и это уже очевидно, создание биткоина это сознательная попытка вывести из-под государственного контроля отношения, возникающие внутри сформированного киберпространства.

Показательным является и то, какие недостатки были выявлены у блокчейн технологий при их анализе специалистами по защите информации. Та же пресловутая атака «51%» говорит, в первую очередь о том, что эти технологии должны применяться единомышленниками (или, если хотите, сообщниками), в то время как данные платформы оценивались с точки зрения применения для независимых пользователей.

Но из всего изложенного уже возникает вопрос «А криптовалюта это точно то, что мы хотим?». И ответ здесь зависит от того, какими мы пониманием справедливые социальные отношения, устанавливаемые, в первую очередь, с государством.

Таким образом для определенной части людей уже не является секретом, что анонимные криптовалюты и блокчейн технологии направлены против государственной системы. При этом их активное развитие обуславливает то, что они являются средством поражения государственной системы в условиях глобального противоборства.

Не исключено, что противоборствующие стороны осознают опасность внедрения блокчейн технологии и, как следствие, блокчейн идеологии, но считаю (или имеют твердую уверенность), что они, после подавления

противостоящей стороны, смогут взять ситуацию с неконтролируемым оборотом денежных средств под свой контроль.

В сложившихся условиях ажиотажного развития и попыток внедрения в Российской Федерации технологий, условно называемых «блокчейном», выход заключается в декомпозиции этого обобщенного понятия на более элементарные, но более предметные технологии, их последующий анализ как с функциональной, так и с точки зрения обеспечения защиты информации, и последующее определение к ним нормативно закрепленных требований со стороны регуляторов.

Представляется, что такие ограничения, как запрет анонимности криптовалюты, использование только сертифицированной криптографии и пр. позволят сохранить необходимый уровень контроля и, как следствие, не допустить ослабления государственности.

При рассмотрении различных источников, содержащих описания рассмотренных криптовалют, внимание авторов обратило достаточно частое использование слова «справедливость». Так, в частности, по мнению разработчиков предлагаемые решения позволяют обеспечить большую «справедливость» при распространении результатов интеллектуальной деятельности.

Прокомментировать данный подход можно следующим образом. Производством продуктов интеллектуальной деятельности занят определенный социальный слой, представляемых, в основном молодыми людьми, чья профессиональная деятельность, хобби и свободное время связано с киберпространством. Не исключено, что в определенной степени их раздражают попытки корректировки их деятельности со стороны традиционных структур в виде издательств, продюсерских центров, крупных торговых центров. Представители этого социального слоя считают, что они могут организовать «справедливую» систему отношений, в которой они смогут уйти от присутствия таких институтов, как государство, банки, цензура и т.п.

В определенной степени популярность криптовалют можно объяснить запрос со стороны описанной социальной прослойки на новую систему взаимоотношений – аспект, который в доступных авторам источниках в целом не исследовался. По мнению данной прослойки, внедрение технлогий

блокчейна поможет сформировать новую систему, которая в большей степени отвечает представлениям молодого поколения.

Так, в печати[30] приводится семь принципов построения экономики блокчейн.

Сетевая целостность

Доверие возникает изнутри системы, оно не продиктовано извне. Участники воспринимают 4 аспекта доверия как единое целое. Они честны на словах и на деле, уважают интересы других, готовы отвечать за последствия своих действий, их решения прозрачны. Целостность закодирована в каждом шаге процесса и распределена между всеми участниками, а не принадлежит одному. Участники обмениваются ценностями, полагая, что остальные также разделяют целостный подход.».

Распределение нагрузки

Энергозатраты распределены по всей пиринговой сети. Нет одного выключателя. Ни один из участников не может выключить систему. Если центральный орган заблокирует человека или группу, система продолжит работать. Если примерно половина сети попытается взять контроль над всей сетью, остальные увидят, что происходит.

Ценность как стимул

Система выравнивает стимулы всех заинтересованных сторон. В 1990-х у девочек была популярна электронная игрушка Тамагочи. Устройство олицетворяло собой яйцо пришельца. При активации из яйца появлялся детеныш неизвестного домашнего животного. Задачей было ухаживать за ним. Для участников блокчейна сеть выглядит как глобальный Тамагочи. Задача участников — беречь и развивать ее. В этом случае они могут рассчитывать на вознаграждение.

Безопасность

Каждый участник сети должен использовать шифрование. Меры безопасности встроены в сеть. Они предоставляют конфиденциальность и подлинность. У пользователя два ключа: один для шифрования, другой для дешифрования. Метод получил название «инфраструктура открытых

[30] Тапскотт Дон, Тапскотт Алекс. Революция блокчейн. Как технология, стоящая за биткоин, меняет деньги, бизнес и мир

ключей» (английский акроним — PKI). Биткоин сегодня — самый масштабный проект в мире, где реализована методология PKI.

Приватность

Люди должны контролировать свои данные. У людей должно быть право решать, какие сведения, когда, как и в каком объеме сообщать о себе. Поскольку один из принципов блокчейн — доверие, больше не нужно идентифицировать других, чтобы с ними взаимодействовать. Чтобы загрузить и пользоваться приложением биткоин, не требуется имя, адрес электронной почты или другие персональные данные.

Защищенность прав

Права собственников прозрачны и закреплены. Свобода личности признается и уважается. Фиксирование времени транзакции и PKI не только исключают двойное расходование, но и фиксируют право собственности на каждый токен в сети. Мы можем торговать только тем, что принадлежит нам. Кроме криптовалюты, токен может содержать любую ценность, в том числе и интеллектуальное право.

Вовлеченность

Экономика работает лучше, когда она работает для каждого. Это означает снижение входного барьера. Это означает создание платформ для распределенного капитализма, а не перераспределенного капитала.

4.5. Пример применения технологии блокчейна

По мнению экспертов – специалистов в области экономики (Тайный рубль: зачем российской экономике национальная криптовалюта: http://www.rbc.ru/opinions/economics/23/10/2017/59edb53a9a79477502fc7ee1) технологии блокчейна и криптовалют интересны, исходя из следующих позиций.

«Во-первых, электронный рубль нужен для удобства проведения транзакций в цифровых системах с помощью специальных кошельков или программных устройств, позволяющих хранить деньги, пополнять счета и производить покупки через интернет без задействования основного банковского счета, что делает такие операции более удобными и безопасными…

Во-вторых, вся дискуссия вокруг национальной электронной валюты выглядит как отчаянная попытка уговорить Центральный банк увеличить

монетизацию экономики, страдающей от кредитного сжатия, или хотя бы вывести часть денежного оборота за пределы банковской системы, внутри которой сейчас происходит оседание финансовых ресурсов, и дать дополнительную свободу движению капитала внутри страны. В частности, предлагается сделать небольшую эмиссию добавочной электронной валюты, чтобы запустить рост хотя бы в цифровом сегменте российской экономики…»

С точки зрения неэкономиста вышесказанное можно, конечно весьма огрублено, проиллюстрировать игрой в преферанс – мы по ходу игры всё считаем в вистах (аналог криптовалюты), которые при подведении итогов игры и подтверждении правильности расчетов переводим в реальные деньги.

С точки зрения технического специалиста явными преимуществами блокчейна и криптовалют являются:

1. Возможность трассировки использования каждой криптомонеты.
2. Децентрализация (а точнее, полицентрализация) контроля транзакций.

Исходя из мнения экономистов и описанных свойств использование криптовалюты, на наш взгляд, лучше всего подходит для осуществления расчетов при реализации государственного оборонного заказа.

Концепция проекта

В настоящее время определенный контроль за движением финансовых средств, выделенных по государственному оборонному заказу, согласно ФЗ-275, возлагается на уполномоченные банки, которые фактически должны отслеживать всю цепочку платежей, осуществляемых при исполнении каждого государственного контракта. При этом они должны обеспечить как валидацию, так и возможность контроля при проведении финансовых транзакций. Необходимо отметить, что в случае создания сложных изделий, предусматривающих кооперацию значительного количества предприятий цепочка платежей (с обязательным приложением копий подтверждающих документов) может быть очень большой и практически не доступной для контроля и анализа в ручном режиме. По мнению финансово-экономических работников подрядных организаций, существующие механизмы проведения расчетов при реализации гособоронзаказа достаточно обременительны с точки зрения трудозатрат и, в конечном итоге, приводят к увеличению стоимости поставляемой продукции за счет увеличения накладных расходов.

Для выработки предложений по внедрению новых технологий, давайте рассмотрим подробнее для каких целей был принят Федеральный закон от 29.12.2012 № 275-ФЗ (текущая ред. от 29.07.2017) "О государственном оборонном заказе".

Для начала вспомним в качестве полушуточного примера сцену из мультфильма «Золотая антилопа». Бедняк приходит к радже и демонстрирует ему свои золотые монеты, полученные из нового центра эмиссии – золотой антилопы. Раджа берет их для «сравнения», относит в сокровищницу и «временно» помещает в хранилище вместе со своими золотыми. На просьбу бедняка отдать ему его монеты раджа отвечает, что он не может отличить их от своих и был бы рад отдать, но вдруг с монетами бедняка он отдаст свою монету, а это будет неправильно.

Данный пример демонстрирует одно из свойств современных фиатных денег – обезличенность. Монеты, безналичные счета, даже купюры обезличены с точки зрения того, что мы не можем проследить историю каждой единицы валюты в произвольно выбранной транзакции. Да, в отдельных случаях используются номера купюр и специальные пометки, но, как известно из сводок новостей, это относится к оперативно-розыскной деятельности, а не к денежному обращению.

До 2013 года, в случае заключения предприятием нескольких контрактов по государственному оборонному заказу с использованием одного расчетного счета, образовывался «общий котел». Как следствие, при осуществлении контроля возникали сложности с точки зрения проверки правильности расходования средств гособоронзаказа, что создавало предпосылки для возможных экономических злоупотреблений.

В качестве организационно-экономической меры противодействия таким возможным злоупотреблениям был принят ФЗ-275. Данный закон выделяет группу уполномоченных банков, которые под реализацию каждого государственного контракта открывают отдельный счет. При этом деньги, перечисленные заказчиком на этот счет, могут быть реализованы только для обеспечения выполнения соответствующего государственного контракта (см. главу 3.1. ФЗ-275).

Технические показатели предлагаемого подхода

Несмотря на возможные возражения финансовых специалистов, попытаемся оценить возможное количество транзакций, которые будут записываться в

проектируемый блокчейн. С учетом разъяснения МО, которое не находит в законе запрета на оплату командировочных расходов, сырья и комплектующих, амортизации и ремонта основных средств и т.п. возможное количество транзакций может составлять несколько сотен, а в случае крупных контрактов с большим количеством исполнителей 2 и 3 уровня несколько тысяч на один контракт.

Вместе с тем, как представляется количество транзакций целесообразно оценивать применительно не к одному контракту, а к некоему усредненному предприятию, причем за единицу измерения целесообразно брать не рабочий день или неделю, а месяц. Такой подход обусловлен тем, что на таком предприятии существуют обязательные ежемесячные платежи, связанные с обслуживанием здания (арендой помещений), обслуживанием основных средств, оплаты услуг связи, уплаты налогов и сборов, выплаты заработной платы сотрудников и т.п. Как следствие, количество транзакций в месяц N будет пропорционально количеству основных средств B, количеству ежемесячно потребляемых услуг S, количеству персонала P, количеству n и сложности c_i заключенных контрактов.

$$N = f_1(B, S, P) + f_2\left(\sum_{i=0}^{n} c_i\right)$$

Практический опыт работы компаний по государственному оборонному заказу показывает, что среднее количество финансовых транзакций за рабочий день не превышает нескольких десятков, а пиковые значения не превышают 10^2. Исходя из опыта создания различных баз данных, можно предположить, что с учетом размера одного блока в блокчейне (от одного килобайта) объем хранимых данных при современных объемах хранилищ вряд ли будет каким-либо сдерживающим фактором внедрения технологии.

Более существенным моментом, на наш взгляд, может явиться пропускная способность каналов связи, а также порядок транзакций – поступления должны опережать расход финансовых средств.

Реализация концепции

Теперь предположим следующую ситуацию. В соответствии с установленными законодательством процедурами, уполномоченным юридическим лицом заключается государственный контракт с поставщиком продукции. Под данный контракт, на основании его электронной формы,

центром эмиссии выпускается криптовалюта, которая в рамках как авансирования, так и окончательного расчета, перечисляется подрядчику. Данные о генерации криптовалюты содержат сведения о конкретном государственном контракте и предполагается, что выпущенная валюта будет обеспечена товаром, поставленным по гособронзаказу.

Данные средства подрядчик может использовать для следующих целей:

- уплаты налогов и обязательных платежей;

- расчетов с другими субподрядчиками в рамках выполнения конкретного государственного контракта;

- выплаты заработной платы работникам предприятия;

- других необходимых выплат.

Понятно, что вся цепочка транзакций по конкретному государственному контракту отражается в копиях блокчейна, которые могут храниться в первую очередь в контрольных и правоохранительных органах. ФНС может проверить, со всех ли выплат по контракту заплачены налоги и обязательные платежи. Правоохранительные органы могут полностью проверить не только факт расходования средств по конкретному государственному контракту, но и его обоснованность, т.к. каждая транзакция должна будет иметь в блокчейне копию подтверждающих документов (или ее функцию от их цифрового образа). Отдельно стоит отметить пока детально не проработанный механизм перевода крипторублей в реальные рубли для выплаты заработной платы. Как представляется, введение отдельной системы контроля за этой операцией позволит снизить возможные коррупционные риски.

Вышеописанное предложение может быть реализовано на базе схемы, описанной в [1]. Данную схему предлагается доработать следующим образом. Выпуск монет осуществляется только центром эмиссии под заключенные контракты. Для осуществления обращения выработанная монета, стоимость которой изначально равна стоимости контракта, должна внутри системы иметь возможность быть разделенной на более мелкие по стоимости монеты с целью оплаты поставок субподрядчиков. Деление монеты возможно как центром эмиссии, так и участниками работ по проектам (по разрешению центра эмиссии).

Область хранения - блокчейн распределен в центре эмиссии, фискальных и контролирующих государственных органах, уполномоченных банках и подрядных организациях. С целью разграничения доступа каждое звено (а возможно, и каждый атом блокчейна) должен иметь метку конфиденциальности, которая позволит реализовать политику безопасности, как в интересах заказчика, так и в интересах подрядчиков, которые могут быть заинтересованы в сокрытии своих субподрядчиков и поставщиков. Блокчейн может быть реализован в рамках национального оператора, который выполняет подключение всех участников и обеспечивает доступ к звеньям и атомам блокчейна в соответствии с правами доступа и ролями участников работ.

Исходя из [2], можно выделить следующие группы требований к блокчейну, используемому для хранения информации о работах по гособоронзаказу:

1) структурные, касающиеся наличия в звеньях блокчейна тех или иных типов данных (атомов) для обеспечения работы заданных технологий. В частности, в звеньях блокчейна должны храниться все транзакции по делению «контрактной монеты», кроме того, наличие звеньев типа Y, связанных с необходимостью гарантированного по длительности времени перебора значений могут быть использованы для реализации конкурсных процедур или открытия условий и результатов конкурсов в заданные сроки.

2) организационные, связанные с национальным криптографическим регулированием, предполагающие применение национальных, рекомендованных или сертифицированных криптографических средств для формирования и обработки атомов блокчейна. Кроме того, данная группа может включать требования, связанные с национальными или ведомственными нормативами в областях применения – налоговая сфера, конкурсные процедуры, корпоративный документооборот и т.д.;

3) технологические, связанные с надежностью хранения звеньев блокчейна, что должно обеспечивать заданные регуляторами соответствующих отраслей, в которых используется блокчейн, параметры надежности хранения и доступности этих звеньев. Кроме того, технологические требования должны описывать требования к производительности операций со звеньями и предельные объемы их накопления и хранения;

4) требования доверия, имеющие четкую структуру блокчейна, регламентированные технологии работы со звеньями, а также интерфейс для

выполнения операций над звеньями. Для обеспечения высокого доверия все прикладные интерфейсы должны быть стандартизованы и доступны в исходных кодах. Кроме того, технология может быть формально верифицирована с помощью математических моделей. Возможные технологии верификации описаны в [3].

Более подробная схема может быть проработана как результат выполнения поручений Президента Российской Федерации по итогам совещания по вопросу использования цифровых технологий в финансовой сфере, состоявшегося 10 октября 2017 года.

Технико-экономические показатели

Проведем технико-экономический анализ по следующим направлениям использования предлагаемой технологии:

- *стоимость хранения информации*,

- *объем трафика*,

- *скорость транзакций*,

- *архитектура хранения данных и транзакций*,

- *сохранение инвестиций в ИТ-проект.*

Стоимость хранения информации. В настоящее время средняя стоимость хранения информации в ЦОДах общего назначения в России составляет около 30-40 рублей за гигабайт в месяц[31]. В корпоративных ЦОД эта сумма увеличивается в 3-5 раз. На данный момент по оценкам зарубежных экспертов цена хранения 1 GB данных при пропускной способности в 30 GB в месяц обходится в $1.51[32]. С учетом более компактного хранения информации в разрабатываемом отечественном прототипе распределенного реестра, объем хранения может быть уменьшен в 2-2,5 раза, соответственно, во столько же раз снизится стоимость хранения информации.

Объем трафика. За счет оптимизированной структуры данных и использования предельных оптимизаций криптографических алгоритмов приблизительно в 1,7 раза уменьшен объем служебного трафика.

---

[31] **Рекомендации по выбору ЦОДа в России. https://habrahabr.ru/post/246419/**

[32] **Распределенное хранение данных: от облака до блокчейна https://forklog.com/raspredelennoe-hranenie-dannyh-ot-oblaka-do-blokchejna/**

Кроме того, межведомственное использование распределенного реестра позволит избежать дублирования трафика для почтовых рассылок и доступа к базе данных. Экспертная оценка дает значение уменьшения в среднем порядка 4,8 раза.

Скорость транзакций. Современная оценка скорости транзакций биткоина - 7 транзакций в секунду, у Ethereum — 15. Причем эта оценка распространяется на всю сеть, поскольку каждый узел полностью реплицирует другие узлы[33]. 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.

Отечественный прототип может быть лишен этого недостатка, в настоящее время скорость транзакций даже без применения специализированных аппаратных платформ составляет до 3000 транзакций в секунду, т.е. это более чем в 100 раз выше, чем Ethereum и Masterchain.

Это позволяет не только получить стратегический эксплуатационный выигрыш, но и расширить поле применения отечественной технологии, в частности, для платежных систем реального времени.

Архитектура хранения данных и транзакций. Как отмечает источник [4], состояние блокчейна является базой данных «ключ-значение», она достаточно примитивна. Поиск в такой базе данных возможен только по первичному ключу, объем хранимых данных очень ограничен. Для серьёзных приложений этого явно недостаточно. Таким образом, при разработке приложений на блокчейнах, например, для Ethereum и Masterchain, проблема хранения и обработки данных стоит очень остро. Сейчас нет удовлетворительных способов её решения.

Предлагаемая технология будет содержать универсальные интерфейсы формирования данных и доступа к ним, которые могут быть встроены в любое приложение и обеспечить работу аналитических и управленческих систем государственного уровня, минимизировав затраты в них на этапе разработки и внедрения. По оценкам экспертов, применение стандартизованных интерфейсов снижает стоимость разработки, владения, сопровождения и обучения примерно на 25-30%.

[33] Где хранить данные децентрализованным приложениям на блокчейне? https://habrahabr.ru/post/327836/

Кроме того, в отечественный прототип будут встроены методы обеспечения информационной безопасности в соответствии с требованиями национальных регуляторов. По оценкам экспертов, затраты на ИБ составляют 7-9% стоимости IT-проекта[34], соответственно, настолько же можно дополнительно минимизировать стоимость проектов.

Сохранение инвестиций. Предлагаемая концепция обеспечит совместную работу уже созданных ведомствами ИТ-систем, минимизировав затраты в них на этапе разработки и внедрения, предлагаемый проект не требует дополнительных инвестиций в аппаратные платформы и их сопровождение, снижает требования к объемам хранения и трафику.

Выводы

Принципиальными преимуществами изложенного подхода являются:

1. Отсутствие необходимости появления новой фиатной валюты, сохранение центра эмиссии в руках государства (выигрыш регулятора).
2. Повышение контроля за использованием средств, выделенных на реализацию государственного заказа. Повышение эффективности исполнения требований ФЗ-275 (выигрыш контролирующих и фискальных органов).
3. Возможность государственного контроля при отработке технологии блокчейн (выигрыш разработчиков технологий).
4. Возможность снижения непроизводственных затрат у поставщиков госзаказчиков (выигрыш конечных пользователей).

По нашему мнению, общий экономический эффект проекта может составить не менее половины от сумм на формирование, реализацию и поддержку ИТ-проектов государственного уровня, а также в несколько раз (до 10) минимизировать затраты на обеспечение гособоронзаказа.

[34] **Оценка затрат компании на Информационную безопасность http://bre.ru/security/18881.html**

5. ИСПОЛЬЗОВАНИЕ КРИПТОВАЛЮТ ДЛЯ ОСУЩЕСТВЛЕНИЯ МЕЖДУНАРОДНЫХ РАСЧЕТОВ ЗА ПРОДУКЦИЮ ТЭК В УСЛОВИЯХ САНКЦИОННЫХ ОГРАНИЧЕНИЙ

Углубления системного кризиса глобализированной экономики с происходящим буквально на глазах усилением контроля со стороны государственных структур США за обращением доллара в качестве валюты международных расчетов и капитального сбережения, рост санкционного давления западных государств на Россию, Иран, Венесуэлу и другие страны, снижение инвестиционной надежности доллара США и финансовых инструментов на его основе на фоне отсутствия эффективных альтернатив – всё это заставляет задумываться о создании альтернативных технологий проведения торговых расчетов и инвестирования для финансовых активов.

Экономика большей части государств, подвергшихся санкционным ограничениям США, либо напрямую связана с экспортом продукции ТЭК (Иран, Венесуэла), либо критически зависит от поставки извне энергоносителей (КНДР, Сирия в условиях оккупации нефтеносных восточных провинций). Практика показывает, что буквально по факту объявления санкций США и подписания исполнительных директив Министром финансов США блокируются любые расчеты, осуществляемые с указанными странами по традиционным каналам банковской системы. И неважно, что расчёты проводятся в национальных валютах или валютах стран, не участвующих в санкционной политике,- в условиях, когда практически все финансовые институты во всех странах критически зависят от операций в «долларовом поле», они, опасаясь вторичных санкций, добровольно отказываются от подобных транзакций.

Накопленный негативный опыт в данной сфере заставляет задуматься не только о придании глобальных расчетных функций российскому рублю как валюте самой крупной и влиятельной страны, геополитически противостоящей Соединенным Штатам, но и о создании механизмов проведения платежей без прямого и явного использования открытых банковских каналов.

5.1. Условия, формирующие необходимость создания российской свободно конвертируемой криптовалюты для международных расчетов

Создание российской свободно конвертируемой эмиссионной криптовалюты (далее – сокращенно РСКЭК) не может считаться временной, сиюминутной задачей, связанной с преодолением последствий текущего обострения взаимоотношений между Россией и странами Запада. Так называемые экономические и финансовые санкции, ограничивающие использование нашей страной глобальных механизмов, начали вводиться с апреля 2013 года и многие из них оказались настолько прочно имплементированы в законодательство США, стран ЕС и ряда их союзников, что говорить о перспективах возврата к «открытому и свободному рынку» не приходится.

Со стороны Соединенных Штатов в отношении России по состоянию на конец февраля 2019 года действуют следующие санкционные акты:

- санкции против России по т.н. «закону Магнитского» (2013);
- санкции в связи с воссоединением Крыма с Россией (2014);
- санкции в связи с событиями на востоке Украины (2014);
- санкции «за кибератаки» (2015);
- санкции по федеральному закону «О противодействии противникам Америки посредством санкций» (CAATSA) (приняты в 2017, конкретизированы в апреле 2018);
- санкции за сотрудничество с властями Сирии и КНДР (2016-2018);
- санкции в связи с «делом Скрипалей» (2018-2019);

Всего под санкциями США оказались 781 юридических и физических лиц Российской Федерации, а также были введены существенные общесекторальные ограничения против предприятий топливно-энергетического комплекса, транспорта, электронной промышленности, финансового сектора и т.д.

Со стороны Европейского Союза в отношении России по состоянию на конец февраля 2019 года действуют следующие санкционные акты:

- санкции в связи с воссоединением Крыма с Россией (2014)

- санкции в связи с событиями на востоке Украины, включая санкции против "Сбербанка России", ВТБ, "Газпромбанка", "Внешэкономбанка", "Россельхозбанка" (2014);
- санкции в связи с поставками турбин Siemens в Крым (2017);
- санкции в связи с выборами Президента России в Крыму (2018);
- санкции в связи со строительством Крымского моста (2018);
- санкции в связи с «делом Скрипалей» (2018-2019)

Схожие в той или иной степени санкции по отношению к России введены Канадой, Японией, рядом других стран.

Санкции США их союзников можно разделить на блокирующие (в США это список SDN — Specially Designated Nationals) и секторальные (в США это список SSI — Sectoral Sanctions Identifications). При попадании под блокирующие санкции активы физических лиц и компаний, как в США, так и в ЕС, блокируются. Запрещается вести какие-либо дела и сделки с ними. Физическим лицам, попавшим под санкции, запрещается въезд на территорию США и/или ЕС. Действие секторальных санкций распространяется на конкретных лиц, ведущих деятельность в определенных секторах экономики, а также на компании, находящихся в собственности или под контролем таких лиц.

Активы компаний, включенных в секторальный список санкций, не замораживаются в отличие от списка SDN. В банковском секторе попадание в такой список не предполагает изоляции этих компаний от финансовой системы — речь идет только об ограничениях на предоставление нового финансирования компаниями США и ЕС. На практике это означает, что, например, попавшие под секторальные санкции банки не смогут привлекать займы у банков и инвесторов, будь то облигации или кредиты. При этом запрет не распространяется на долг сроком менее 14 дней (для санкций США) и 30 дней (для санкций ЕС).

В оборонном секторе для лиц и компаний, попавших под санкции США, введен запрет импорта и экспорта вооружений и сопутствующих материалов, товаров и услуг двойного назначения из/в Россию. Для включенных в санкционные списки ЕС установлен запрет на покупку, продажу, трансфер, экспорт оружия и боеприпасов в Россию лицами ЕС, а также запрет на экспорт товаров двойного назначения (товары, которые могут быть

применены как в мирных целях, так и при создании оружия массового уничтожения) и технологий для военного использования.

В энергетическом секторе для лиц и компаний, попавших под санкции США, введен запрет экспорта в Россию товаров, услуг или технологий, связанных с разведкой и добычей нефти на Арктическом шельфе, глубоководной добычей, со сланцевыми проектами (энергетический сектор). Для включенных в санкционные списки ЕС введена процедура лицензирования сделок с Россией в отношении товаров и технологий, предназначенных для добычи и разведки нефти и других полезных ископаемых.

Отдельными правовыми актами могут быть предусмотрены исключения в виде ограничения действия санкций при осуществлении конкретных операций[35].

Значительно более жесткие и всеобъемлющие санкции введены США против Ирана в 2018 году. Секторальные ограничения распространяются на ключевые отрасли иранской экономики – топливно-энергетический сектор, автомобильную промышленность, банковский сектор, торговлю золотом и т.д. Кроме того, в конце 2018 года Иран по требованию США был отключен от международной системы межбанковских расчетов SWIFT. Вводя санкции против Ирана, Соединенные Штаты применили угрозу вторичных (экстерриториальных) санкций к странам и компаниям-торговым партнерам Ирана, чем смогли добиться «добровольного» ухода с иранского рынка значительного числа крупных компаний. Ряд «исключений», оставленных США по покупке иранской нефти для Китая, Индии, Греции, Южной Кореи, Японии, Тайваня, Италии и Турции, практически не работают в условиях невозможности расчета с Ираном в долларах или других валютах (Евро, швейцарский франк и т.д.), проходящих через корреспондентские счета банков, опасающихся вторичных санкций и прямых штрафов со стороны правительства США[36,37].

Не менее значителен список санкций США против Венесуэлы. Первые санкции были введены в начал 2014 года, затем в конце 2014 года они были кодифицированы принятым Конгрессом США «Актом о защите прав человека и гражданского общества в Венесуэле». 8 марта 2015 года

[35] Ю.Сапронова, Д.Линделл и др. Пять лет санкций против России.// РБК. URL: https://www.rbc.ru/politics/04/12/2018/5bffb0f09a79470ff5378627

[36] М.Бондаренко. «Самые жесткие» санкции США против Ирана вступили в силу // РБК. URL: www.rbc.ru/politics/05/11/2018/5be049809a7947e8d49edae2

[37] США опубликовали список санкций против Ирана // РИА Новости. URL: https://ria.ru/20181105/1532152625.html

президент США указом № 13692 ввёл чрезвычайное положение в связи с нарушением прав человека в Венесуэле, якобы представляющее «угрозу национальной безопасности и внешней политике США». Данный указ вводил в действие против Венесуэлы «Акт об особых экономических полномочиях» (IEEPA), а также «Акт о чрезвычайных положениях» (NEA). Далее экономические и финансовые санкции США против Венесуэлы расширялись и усиливались указами президента США №13808 (август 2017), указом №13827 (март 2018), указом №13835 (май 2018) и указом №13850 (ноябрь 2018)[38]. В 2019 году Соединенными Штатами были заморожены активы крупнейшей венесуэльской нефтедобывающей компании PDSVA, а также наложен фактический запрет на использование венесуэльским правительством зарубежных финансовых активов.

Особо следует обратить внимание на указ президента США №13827 от 19 марта 2018 г, направленный на противодействие обороту национальной криптовалюты, выпущенной правительством Венесуэлы в начале 2018 года. Данным указом вводится запрет на «…все операции, связанные с предоставлением финансирования и другими операциями в Соединенных Штатах или на территории Соединенных Штатов Америки с любой цифровой валютой, цифровой монетой или цифровым токеном, которые были выпущены от имени, от имени или по поручению правительства Венесуэлы 9 января 2018 года или после этой даты…»[39].

Помимо санкций по отношению к России, Ирану и Венесуэле, действует множество аналогичных ограничений, введенных США и их союзниками против КНДР, Сирии, ряда стран Африки и т.д., продолжают оставаться актуальными некоторые из санкций, введенных против Китая еще в 1989 году (после событий на площади Тяньаньмэнь) и т.д. При этом с точки зрения международного права из всех ныне действующих санкций законными являются только санкции, введенные Советом Безопасности ООН против КНДР, все остальные являются ничем иным, как попыткой распространить юрисдикцию западных держав на другие страны мира.

Резюмируя перечисленное выше, можно сделать вывод о том, что в условиях наличия очень объемной и постоянно расширяющейся системы финансовых, экономических и политических ограничений, мировая экономика вступает в период сегментации и нестабильности. Действия стран-инициаторов

[38] И.Тимофеев. Санкции США против Венесуэлы: прекурсор смены власти? // Международный дискуссионный клуб «Валдай», 25.01.2019 URL: http://ru.valdaiclub.com/a/highlights/sanktsii-protiv-venesuely/
[39] USA Federal Register Vol. 83, No. 55 Wednesday, March 21, 2018

санкционных мероприятий приводят к разрушению системы глобальных мирохозяйственных отношений, при этом инструментарий санкций направлен на то, чтобы ущерб для «атакуемых» оказывался существенно выше, чем для «атакующих». По сути дела, единственным примером эффективного ответа на западные санкции со стороны «атакуемого» государства явилось введенное Россией в 2014 году продовольственное эмбарго[40]. При этом аналогичных по степени воздействия на страны-инициаторы санкций мер нет в настоящее время ни у России, ни у других государств.

Более того, даже при минимальных или нулевых экономических связях со странами-инициаторами санкций их жертвы оказываются крайне стеснены в международных экономических отношениях, поскольку их потенциальные торговые и финансовые партнеры («третьи лица»), формально не имеющие запрета на сотрудничество, опасаются либо вторичных санкций по отношению к себе, либо проблем на ценных для них рынках США, стран Европейского Союза и т.д. Теоретически проблему защиты «третьих лиц» можно решить через создание компаний специального назначения (SPV – Special Purpose Vehicle), например, специальной компании, которая будет торговать с Ираном и никогда не появится на рынке США,- однако в реальности подобные SPV все равно должны использовать систему расчетных и корреспондентских счетов, прямо или косвенно связанных с крупнейшими финансовыми институтами, оплачивать услуги глобальных морских перевозчиков и т.д. По этой причине подобные SPV, даже если и создаются, то добровольно ограничивают свою деятельность оборотами, связанными с «гуманитарными товарами» (продовольствия, лекарства и т.д.), поскольку даже для них работа по товарным группам и в отраслях, являющихся объектами санкционных ограничений, создает неприемлемые риски.

С другой стороны, совокупный экономический потенциал стран «санкционного блока» и стран, не принимающих официального участия в санкционных инициативах, составляет около 70% от общемирового экономического потенциала, что формирует возможность создания независимого от США и ЕС рынка товаров, капиталов и услуг. Этот рынок, по сути и по масштабу также являющийся глобальным, в полной мере

[40] Указ о применении отдельных специальных экономических мер в целях обеспечения безопасности Российской Федерации // Официальный сайт Президента России, 6 августа 2014 г.

сможет обеспечить условия для эффективного экономического развития для своих участников.

В сложившихся условиях обеспечение независимости, безопасности и выборочной конфиденциальности финансовых транзакций и торгового оборота, осуществляемого между странами-объектами санкционного давления или с участием таковых, становится одной из важных в деле обеспечения экономической безопасности России, повышения ее статуса и роли в международных экономических отношениях и мировой политике.

5.2. Основные задачи, решаемые посредством российской свободно конвертируемой эмиссионной криптовалюты (РСКЭК)

Как было показано выше, предпринимаемые сегодня попытки действий по выходу из «санкционной петли», начиная от перехода в двусторонних расчетах России с Китаем, Индией, Ираном и другими странами на национальные валюты, попытки перевести часть внешнеторгового оборота России на рубли и т.д. – не дают должного эффекта или, в лучшем случае, решают ситуативные и локальные проблемы межстрановых расчетов.

Так, практически все крупные и средние банки, имеющие возможность проводить платежи через корреспондентские счета, открытые в национальных валютах, по факту имеют также корсчета в долларах США и Евро и потому крайне неохотно соглашаются на сотрудничество подобного рода. Данную ситуацию могла бы преломить высокая инвестиционная ценность рубля или хотя бы китайского юаня – однако в условиях сложившейся за многие годы и сохраняющейся в неизменном виде дискриминационной системы курсообразования, когда любая обменная операция происходит с премией в пользу доллара или Евро, подобная перспектива пока представляется невозможной.

Проблему валюты для расчетов, бывших бы достаточно защищенными от контроля со стороны, и которая при этом бы имела одинаковую с долларом или Евро инвестиционную привлекательность, можно решить в 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 долларах США.

Категорически неприемлем и подход, предполагающий свободное курсообразование новой криптовалюты – хотя в случае успеха, подобного биткойну, он способен принести эмиссионному центру значительный дополнительный доход. Международная торговля исторически тяготеет к валютам максимально стабильным, отсюда привязка новой криптовалюты к доллару – важнейшее техническое условие ее функциональности.

В качестве аналогов валюты подобного рода можно привести золотой рубль, применявшийся в 1920-е годы, либо так называемый «евродоллар» - расчетную квазивалюту, использовавшуюся банками стран Западной Европы для кредитования торговли с СССР в конце 1960-х – начале 1970-х гг в условиях установленных Соединенными Штатами советским банкам ограничений на открытие и ведение долларовых корсчетов.

Создание и запуск российской свободно конвертируемой эмиссионной криптовалюты (РСКЭК) в условиях развитых цифровых технологий и наличия в финансовой системе России достаточных объемов ликвидности в долларах США и Евро не представляет системных сложностей и займет непродолжительный срок. Первоначально РСКЭК сможет использоваться для осуществления международных платежей, номинированных в долларах США, без задействования корсчетов, открытых в финансовых институтах США и других стран Запада. Первыми бенефецирами новой системы расчетов на основе РСКЭК станут российские структуры, включенные в санкционные списки США, компании Ирана, Сирии, а также компании и банки КНР и Индии, заинтересованные в работе с Россией, однако опасающиеся вторичных санкций США.

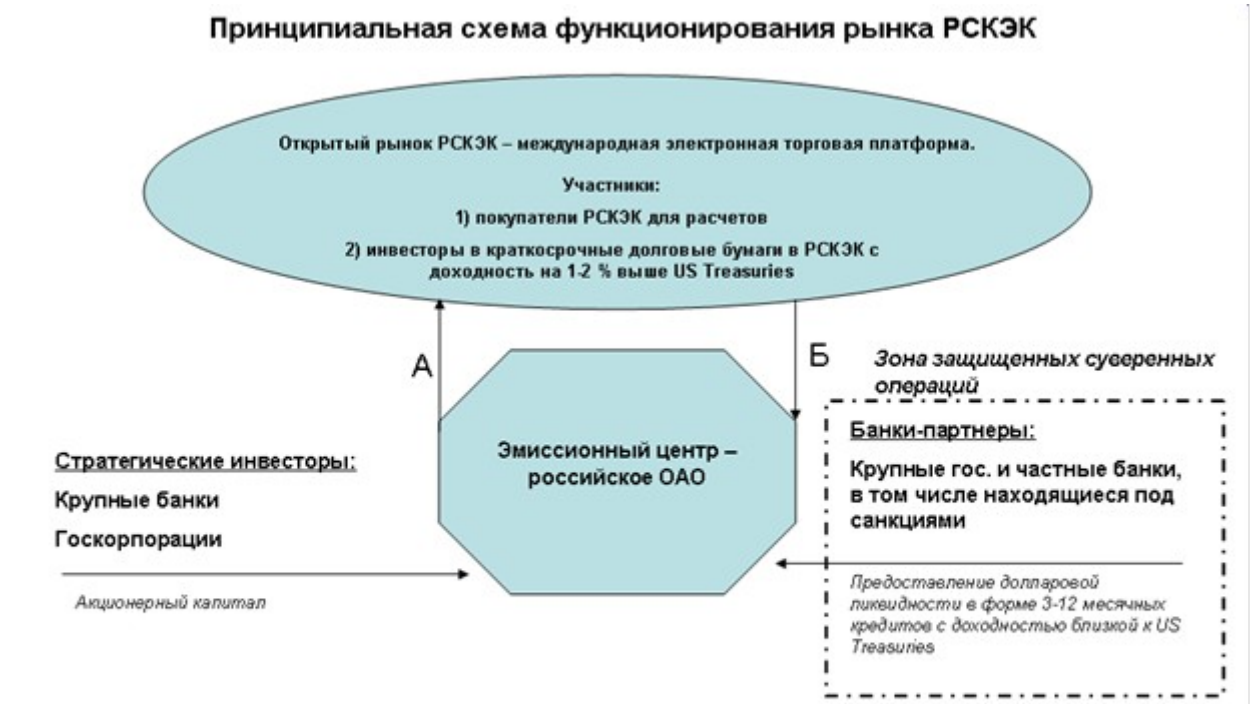
В дальнейшем сфера использования РСКЭК сможет быть существенно расширена – как по географии, так и в части инвестиционных инструментов.

Ключевой особенность новой национальной криптовалюты должна стать ее целенаправленная привязка по курсу к доллару США. Речь при этом идёт не о «подчинении» доллару, а наоборот, о «финансовом флибустьерстве», о

намерении в результате «набега» на области, которые в результате политики США стали для доллара уязвимыми, явочным порядком отобрать у доллара часть сегментов его международного обращения с максимальным комфортом для контрагентов, привыкшим к расчетам, номинированным в традиционной для международной торговле валюте.

Для этого в механизм выпуска и обращения новой криптовалюты с самого начала встраивается механизм управляемой эмиссии, обеспечивающей паритет курса криптовалюты с долларом США с диапазоном суточных отклонений не более 0.25%-0.50%.

Паритет будет обеспечиваться автоматическим круглосуточным контролем за курсом с механизмом выброса на обменный рынок РСКЭК долларовой или рублевой ликвидности соответственно. Для этого у отвечающего за эмиссию РСКЭК российского финансового института должен иметься критический запас ликвидности (первоначально – в эквиваленте до 100 млн. долларов, по мере расширения оборота – несколько миллиардов долларов).



Привлечение дополнительной ликвидности оператору криптовалюты целесообразно организовать на рыночной основе, через доход от кредитования в новой криптовалюте (ставку кредитования в новой

криптовалюте разумно установить на 1.0-1.5% выше ставки доходности по долларовым вложениям соответствующего уровня риска), что позволит оператору криптовалюты привлекать средства с российского финансового рынка. Разумеется, говорить о перспективах долгосрочных инвестиционных инструментов в РСКЭК, аналогичным казначейским облигациям США, пока рано, однако по прошествии 2-3 месяцев с момента запуска краткосрочные инструменты, номинированные в РСКЭК, вполне могут быть приняты рынком. Особенно если принять во внимание, что в настоящее время на российском межбанковском рынке практически отсутствуют инструменты кредитования на срок более 1-2 дней, а ставка по последним составляет на начало марта 2019 г 2.4% годовых[41].

Не надо забывать и о том, что значительные средства в долларах и евро у национального оператора криптовалюты будут образовываться от ее продажи субъектам мирового финансового рынка в объемах, которые постепенно начнут превышать стоимость ликвидности и золота, задействованных в обеспечительных целях.

С целью снижения риска недружественных действий финансовых институтов Запада по отношению к новой криптовалюте, особенно на первых этапах ее функционирования,– например, скоординированной продажи с целью обрушения курса,– в первые годы необходимо поддерживать определенный уровень актива 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 и проч.) расчетов и счетов инвестиционных. Для инвестиционных счетов есть смысл отказаться от полной анонимности – эмитент криптовалюты, осуществляющий работу по гарантированию устойчивости ее курса, будет готов предоставлять гарантии в виде покрытия выплат другими валютами и/или золотом только при наличии специального соглашения, для которого личность инвестора должна быть раскрыта. В этой связи необходимо разработать криптомеханизм, гарантирующий хранение соответствующих данных на территории России и многоуровневую защиту от несанкционированного доступа.

[41] Центральный банк Российской Федерации. Показатели ставок межбанковского рынка с 01.08.2000 // URL: https://www.cbr.ru/hd_base/mkr/mkr_base/

На сегодняшний день в мире сформировались оптимальные условия для запуска новой криптовалюты в работу. В случае ее успешного внедрения возможно в короткие сроки довести объем ее эмиссии как минимум до 30-40% от объема иранского нефтяного экспорта в пересчете на 3-х недельный оборот стандартного нефтетанкера, т.е. порядка 1.2-1.5 млрд. долларов.

Представляется возможным, чтобы эти средства были привлечены в рамках госпрограмм международного сотрудничества России, в рамках договоренностей в формате совместных с Россией межправительственных комиссий (с Ираном, Венесуэлой и т.д.), а также в рамках Нового банка развития стран БРИКС (НБР).

Однако для сохранения суверенного характера новой криптовалюты целесообразно концентрировать усилия на внутрироссийских источниках фондирования.

Оптимальный объем эмиссии, при котором устойчивость криптовалюты определяется наличием значительной инерции со стороны большого числа держателей расчетных счетов и инвесторов, оценивается в 50-70 млрд. долларов. Очевидно, что при обращении к криптовалюте со стороны хотя бы части крупных отечественных экспортеров, включая Газпром, Роснефть и Росвооружение, - это вполне реальная цифра.

В перспективе, по мере упрочения международного статуса новой российской криптовалюты с доведением среднего объема эмиссии до 100-120 млрд. долларов, что эквивалентно 50% денежной базы РФ в широком определении, сформируются условия для формирования у российского рубля фундаментальных основ свободной конвертируемости, что позволит упрочить международное влияние российской валюты и снизить ключевую ставку до уровня ведущих свободно конвертируемых валют.

5.3. Преимущества РСКЭК в сравнении со специальным механизмом Евросоюза для расчетов с Ираном INSTEX

5.3.1. Краткая характеристика системы INSTEX

После одностороннего выхода США в 2018 году из международной сделки Ираном, заключенной в 2015 году, Германия, Франция и Великобритания запустили систему, поддерживаемую ЕС, для содействия торговле с Ираном,

чтобы помочь европейским предприятиям обойти односторонние санкции США в отношении Ирана.

Инструмент поддержки торговых обменов в лице компании специального назначения (SPV) с названием INSTEX был зарегистрирован после нескольких месяцев обсуждений и технических переговоров.

Компания INSTEX SAS, что расшифровывается как Instrument in Support of Trade Exchanges («Инструмент в поддержку торговых обменов»), зарегистрирована 30 января 2019 года в Париже по адресу французского Министерства экономики и финансов. Главой компании является немецкий банкир Пер Фишер[42]. Наблюдательный совет будет состоять из трех человек — постоянного секретаря британского МИДа Саймона Макдональда, французского дипломата Мориса Гурдо и немецкого дипломата Мигеля Бергера.

Данное юридическое лицо планирует работать как своего рода клиринговая палата по бартерным операциям, номинированными в Евро, с целью облегчить Ирану проводить торговые расчеты с европейскими компаниями. Все транзакции INSTEX не должны попадать под контроль банков США и осуществляться вне юрисдикции США[43].

Ожидается, что торговля через INSTEX SAS будет сосредоточена на несанкционированных товарах первой необходимости, таких как гуманитарные, медицинские и сельскохозяйственные продукты. Это означает, что на данный момент INSTEX избежит прямого столкновения с Белым домом, поскольку санкции США разрешают эти категории торговли из-за их гуманитарного характера.

Расчеты по сделкам, связанным с иранской нефтью, которые по требованию США прекратились в конце 2018 года и которые являются основным источником иностранной валюты для Ирана, на сегодняшний день проводить через INSTEX не планируется.

Для старта нормальной работы INSTEX необходимо согласование и решение ряда технических моментов.

---

[42] помимо прочего, П.Фишер занимает пост независимого директора российского банка «Центр-инвест» (Ростов-на-Дону)

[43] E.Geranmayeh, E.Batmanghelidj. Trading with Iran via the special purpose vehicle: How it can work // European Council of Foreign Relations, 07th February, 2019 URL: https://www.ecfr.eu/article/commentary_trading_with_iran_special_purpose_vehicle_how_it_can_work

Прежде всего, речь идет о защите от США информации по операциям европейских компаний через INSTEX. Несмотря на выведение расчетов из контролируемой США долларовой зоны, правительственные агентства США смогут получать незащищенную информацию о сделках европейских компаний с Ираном и затем применять к ним собственные санкции, штрафы и т.д. Ряд крупных компаний ЕС в силу этой опасности отказываются от работы с Ираном, в силу чего INSTEX SAS официально делает ставку на работу с малыми и средними компаниями из стран ЕС.

Второй нерешенный технический момент – это создание параллельного SPV на территории Ирана, которое будет «аккумулировать» операции со стороны множества иранских субъектов бизнеса и осуществлять итоговый клиринг с европейским SPV.

Данная иранская организация (до сих пор она не создана) по требованиям европейской стороны должна будет соблюдать высокие стандарты прозрачности в правилах борьбы с отмыванием денег и финансирования терроризма. В ходе идущих в настоящее время переговоров европейские посредники предлагают сформировать данное иранское SPV под иранским банком, на который не распространяются вторичные санкции США. К сожалению, вопрос о создании иранского SPV, которое по факту должно сильно зависеть от INSTEX, вызывает в Иране политические дебаты и до сих пор не решен. С целью ускорить решение данного вопроса, в органах Евросоюза прорабатывается вопрос о выделении из фондов ЕС средств технической помощи для финансирования запуска и деятельности иранского SPV.

В общем плане, механизм расчетов через INSTEX должен выглядеть следующим образом: европейские продавцы товаров для Ирана, в силу санкций США рискующие получить отказ обслуживающих их европейских банков принять пришедший из Ирана трансфер в Евро, теперь будут получать оплату со счетов зарегистрированного во Франции INSTEX SAS, что не должно вызывать юридических коллизий.

Соответственно, европейские импортеры товаров из Ирана (кроме нефти, операции с которой по-прежнему ограничены санациями) перечисляют оплату за иранский товар не напрямую в иранский банк, а на парижский счет INSTEX SAS.

Один из возможных вариантов организации сделки через INSTEX SAS может выглядеть следующим образом:

Европейский экспортер, получивший от иранского импортера заказ на партию лекарств, предоставляет INSTEX соответствующую документацию по сделке, включающую доказательства того, что импортер практиковал разумную юридическую проверку в отношении иранского покупателя и конечного пользователя. Данная проверка остается в обязанностях европейских партнеров Ирана, т.к. INSTEX не будет предоставлять услугу комплексной проверки и предоставлять соответствующие гарантии.

После одобрения сделки INSTEX, она отражается в его в торговом регистре

Затем INSTEX изучает возможность через свою базу «встречных сделок» профинансировать данную покупку лекарств учитываемой у него выручкой в Евро, полученной, скажем, от европейского импортера иранских фисташек.

После этого INSTEX утвердит платеж от европейского импортера фисташек европейскому экспортеру лекарств. Это означает, что платеж может быть произведен из одного европейского банка в другой без использования средств, полученных из Ирана.

Для того, чтобы завершить процесс торгового посредничества, иранский партнер INSTEX (иранское SPV) аналогичным образом будет координировать аналогичную оплату от иранского импортера лекарств иранскому экспортеру фисташек в иранской валюте. Соответствующие средства останутся в Иране.

В интересах успешной работы INSTEX предстоит найти способ сбалансировать платежи как внутри общего торгового потока, так и на операционном уровне, чтобы все транзакции в идеале могли быть выполнены единовременно, максимум – в течение 60 дней. Чтобы сбалансировать общий объем торговли через INSTEX, планируется увеличить экспорт иранских продуктов питания в Европу, для чего руководство ЕС планирует увеличь квоты и снять ряд фитосанитарных ограничений.

Европейские аналитики полагают, что подобная полубартерная схема расчетов в части продовольствия вполне сможет заработать, поскольку торговля стран ЕС продуктами питания с Ираном уже сегодня в целом сбалансирована: по данным Евростата, за первые одиннадцать месяцев 2017

года экспорт продовольствия из ЕС в Иран составил 298 млн. евро, а импорт аналогичных товаров из Ирана в ЕС составил 292 млн. евро.

В то же время торговля лекарствами и медицинским оборудованием сбалансирована в гораздо меньшей степени: объем экспорта из ЕС составляет 851 млн. евро, а импорт - всего 27 млн. евро. И если раньше Иран, критически нуждающийся в медицинских товарах, восполнял данный дефицит доходами от продажи нефти, то в сегодняшних условиях этот механизм эффективно работать не сможет[44].

Одним из предложений по компенсированию дефицита оборота с Ираном в части лекарств и медицинской продукции INSTEX рассматривает сотрудничество с банком или SPV в России. Поскольку Россия обладает в торговле с Ираном положительным торговым балансом, а также сохраняет возможность приобретать иранскую нефть, соответствующее российское SPV могло бы предоставлять INSTEX необходимое покрытие в Евро – например, через оплату поставок лекарств для Ирана, отгружаемых через Россию. Однако сотрудничество с российским SPV, которое легко может оказаться под санкциями США и не может быть защищено иммунитетом от институтов ЕС, остается рисковым проектом.

Помимо России, INSTEX рассматриваются варианты сотрудничества с другими государствами, продолжающими закупать иранскую нефть – с Китаем, Индией и Японией.

После отработки и налаживания всех механизмов планируется динамичное увеличение торговых оборотов через INSTEX. Пополнение оборотных средств INSTEX для оперативных расчетов с европейскими экспортерами будет осуществляться за счет взносов стран ЕС и других акционеров.

INSTEX планирует взимать комиссию за использование своих услуг в размере 2-3%, доходы от которой также будут направляться в формирование оборотных резервов.

В то же время в неофициальных разговорах создатели INSTEX фиксируют в качестве своей ближайшей задачи достижение оборота всего лишь порядка 20-30 млн. Евро, что не превышает 5% величины европейского экспорта в Иран. Для достижения более внушительных показателей учредили INSTEX

[44] C. Winter. What is the EU-Iran payment vehicle INSTEX? // DW News Bulletin URL: https://www.dw.com/en/what-is-the-eu-iran-payment-vehicle-instex/a-47306401

ожидают дополнительной финансовой и правовой поддержки от стран ЕС и руководства Европейского Союза.

5.3.2. Альтернативная схема расчетов с Ираном через РСКЭК

Рассмотрим аналогичную описанной выше схему, в рамках которой компания из Ирана имеет намерение приобрести партию лекарственных препаратов производства одной из стран ЕС условной стоимостью 10 млн. Евро.

Исходим из того, что у этой компании есть возможность приобрести эквивалент 10 млн. ЕВРО у одного из экспортеров иранской нефти – например, в Китай. Пусть оплата за нефть поступает на счет иранского нефтеэкспортера в юанях, открытый в китайском банке. Нефтеэкспортер поручает своему брокеру приобрести на эти деньги 10 млн. долларов в РСКЭК на электронной криптобирже.

При этом продавцом указанных 10 млн. долларов РСКЭК по факту может быть кто угодно, начиная от российского оператора системы РСКЭК и кончая инвестором из любой другой страны, вложившим свои деньги в РСКЭК как в одну из криптовалют, наряду с биткойном, эфириумом и т.п.

После того, как сделка по переводу иранским нефтеэкспортером эквивалента 10 млн. долларов из юаней в РСКЭК будет завершена, эта сумма окажется «невидимой» для агентств США и Евросоюза, обязанных следить за транзакциями в санкционных странах.

Далее эти 10 млн. долларов РСКЭК путем добавления электронной записи в распределенном реестре (блокчейне) РСКЭК и в рамках внутреннего оборота в юрисдикции Ирана переходят в распоряжение от иранского нефтеэкспортера к иранской компании, желающей приобрести лекарства в ЕС.

Иранский импортер лекарств посылает распоряжение российскому оператору РСКЭК о необходимости оплаты инвойса европейского поставщика лекарств. Получив распоряжение, российский оператор либо самостоятельно обменивает сумму в РСКЭК на доллары или Евро, используя для фиксации данной суммы партнерские отношения (при необходимости – через цепочку посредников) с «несанкционными» банками, имеющие возможность оперировать корсчетами в США или странах ЕС, либо – при необходимости

максимальной скрытности – через 1-2 транзакции на рынке других криптовалют.

По факту получения оплаты в долларах или Евро, поставщик лекарств отгружает свою продукцию иранскому получателю напрямую (сегодня законодательство ЕС позволяет такие отгрузки), либо через другие страны. Для логистического сопровождения соответствующих перевозок при российском операторе РСКЭК может быть создана международная транспортная компания.

Разумеется, подобная схема оказывается более сложной и длительно, нежели через использование стандартных банковских транзакций, и ее стоимость (размер комиссии) на первых порах может быть сопоставимым со стоимостью услуг INSTEX, то есть 2-3%. В этом случае, если вернуться к нашему примеру с поставкой на 10 млн. долларов, стоимость фактической отгрузки составит 9.7-9.8 млн. долларов. Но даже в этих условиях система РСКЭК работает лучше INSTEX, поскольку не предполагает необходимости «параллельного» SPV в Иране: сделка по обмену условных иранских нефтеюаней на РСКЭК может быть проведена в рамках специальной торговой сессии с участием двух иранских компаний и оператора РСКЭК, организованной либо в штаб-квартире российского оператора, либо дистанционно.

Однако по мере наращивания оборотов через РСКЭК, что позволит покупать и продавать данную российскую криптовалюту в непрерывном режиме и с достаточным уровнем среднесуточного оборота, транзакционные издержки начнут быстро снижаться и в перспективе приблизятся к стандартным банковским комиссиям.

Развитие инвестиционной компоненты РСКЭК, о которой говорилось в разделе 2, еще более увеличит операционные возможности системы, со временем превратив ее, по сути, из специального расчетно-платежного механизма в новую международную валюту.

5.4. Другие криптовалютные механизмы, опыт которых следует учитывать при проектировании РСКЭК

5.4.1. Государственная криптовалюта Венесуэлы

Криптовалюта El Petro стала первой криптовалютой в мире, выпускаемой официально под государственным контролем и для решения конкретной проблемы - облегчения американских санкций, введённых против Венесуэлы.

Особенностью El Petro стала привязка ее к баррелю нефти (1 El Petro = 1 баррель нефти, то есть стоит порядка 55-60 долларов, как и марка венесуэльской нефти).

Из-за этой особенности венесуэльскую криптовалюту Petro (PTR, El Petro) иногда путают с частной криптовалютой PetroDollar (XPD). Последняя эмитирована компанией Signal Capital Management, одна монета XPD эквивалентна 13,5 баррелям нефти. Токен XPD активно торгуется на Cryptopia и Yobit, к этой монете лояльно относится правительство США, в то время как против El Petro введены и поддерживаются американские санкции. Можно также сказать, что PetroDollar (XPD) и El Petro (PTR) – это конкуренты в нише цифровых активов, обеспеченных нефтью.

Первоначально правительство Венесуэлы планировало запустить криптовалюту со свободным доступом к майнингу, что дало бы населению страны дополнительный источник дохода. Правительство даже организовало Реестр потенциальных майнеров, в который было внесено более 50 тысяч желающих зарабатывать на добыче El Petro. Однако затем от идеи свободного майнинга отказались.

Государственная криптовалюта Венесуэлы El Petro характеризуется следующими особенностями:

- El Petro основана на блокчейне NEM (при том что первоначально планировался Ethereum)
- весь объем El Petro был премайнен в момент эмиссии (в объеме 100 млн. токенов на сумму в почти 6 млрд. долларов) и находится в распоряжении Правительства Венесуэлы; дополнительный майниг запрещен
- в рамках пресейла (ICO) было выставлено на продажу 38.4 млн. токенов El Petro, за продажу которых предполагалось выручить 2.3 млрд. долларов США; однако реализовать удалось далеко не все токены, объем

фактических продаж составил около 750 млн. долларов США, т.е. порядка 32% от планировавшегося

- в рамках ICO приобрести El Petro могли только резиденты страны за следующие валюты: российский рубль (единственная дозволенная фиатная валюта), Bitcoin, NEM и Ethereum

- с помощью El Petro в Венесуэле можно оплачивать различные госуслуги и товары (коммунальные платежи, бензин, налоги, сделки с недвижимостью, авиабилеты и т.д.)

- в Белой книге проекта венесуэльской криптовалюты не указано, как именно правительство собирается осуществлять привязку крипты к баррелю нефти

Практика использования и оборота венесуэльской криптовалюты свидетельствует, что из-за ряда ошибок в эмиссии и практике обращения, а также в результате санкций США, El Petro в настоящее время далека от полноценной криптовалюты. В частности, El Petro до сих пор не листируется в рейтинге Coinmarketcap, крупнейшего и наиболее авторитетного специализированного ресурса в криптовалютной сфере. Можно лишь предположить, что правительство Венесуэлы, получив в результате неполного ICO 750 млн. долларов США практически «из воздуха», просто ждёт подходящего момента для продажи остающихся неэмитированными 61.6 млн. токенов El Petro, либо негласно осуществляет их продажи небольшими траншами с целью решения текущих финансовых проблем.

Таким образом, признать выпуск El Petro полностью успешным проектом нельзя. Из-за ряда ошибок в первоначальной подготовке, а также из-за отсутствия механизма конвертации криптовалюты в обеспечивающий товарный эквивалент – нефть, результат эмиссии оказался в три раза ниже запланированного. При этом неудачи нельзя списать исключительно на санкции США, поскольку даже в условиях таковых оборот венесуэльской государственной криптовалюты пусть с издержками и потерями, но мог развиваться на независимых площадках, чего, к сожалению, не происходит.

5.4.2. Частная криптовалюта с курсовой привязкой к доллару США - Tether

В контексте анализируемой идеи использования криптовалют для международных расчетов в условиях санкционных ограничений, затрудняющих или делающих невозможными транзакции через традиционные банки не только в долларах и евро, но и в иных государственных фиатных валютах, представляет интерес опыт первой криптовалюты с декларируемой курсовой привязкой к доллару США – криптовалюты Tether.

Tether (USDT) — криптовалютный токен, выпущенный в 2015 году компанией Tether Limited, которая утверждает, что его стоимость обеспечивается запасами долларов США, хранящимися на её банковских счетах. Основная идея разработчиков Tether состоит в предоставлении участникам криптовалютного рынка возможности пользоваться стабильным цифровым активом («стейблкоином»), курс которого привязан к курсу доллара США и не испытывает столь сильных колебаний, как курсы других криптовалют.

Если с технической точки зрения Tether идентичен традиционным криптовалютам, то его системное отличие заключается в контролируемом курсе и централизованной эмиссии.

Покупка каждого нового токена Tether – это его выпуск, который требует от пользователя перечисления 1 доллара на счет компании в обычном фиатном виде. Для покупки EURT требуется 1 евро и так для каждой вариации. Покупка на криптобиржах сопровождается примерно аналогичными расценками. Таким образом, только через Tether Limited можно совершить первичную покупку токена, однако через сторонние организации можно приобрести и использовать в обороте уже выпущенные валютные единицы.

Майнинг Tether пользователями не предусмотрен.

Считается, что успех эмиссии Tether определялся тем, что эмитент Tether Limited был афиллирован с криптобиржей Bitfinex, которая первой интегрировала данный токен в свой сервис. Короткое время спустя Tether был интегрирован в сервис американской биржи криптовалют Poloniex.

За период с января 2017 года по август 2018 года общий объем эмиссии токенов Tether вырос примерно с 10 млн. долларов США до приблизительно 2,4 млрд. долларов США. В начале 2018 года на долю Tether приходилось

около 10% объема сделок с биткойном, а к середине 2018 года данный показатель вырос до 80%.

При этом нельзя не отметить, что факт покрытия эмиссии Tether фиатными долларами США, якобы находящимися в распоряжении компании Tether Limited, вызывает сомнения. В начале 2018 года Комиссия США по торговле товарными фьючерсами проводила на этот счет расследование – правда, информации о результатах этого расследования нет.

Криптовалюта Tether характеризуется следующими особенностями:

- Tether работает на платформе SecurePlatform.

- Денежные переводы, в которых задействована криптовалюта Tether, прозрачны и надежны, чего удалось достичь благодаря применению блокчейн-технологии; обменять Tether на наличные деньги можно в любой момент.

- Создатели Tether утверждают, что их продукт сочетает в себе лучшие качества криптовалют и фиатных денежных единиц, их криптовалюту можно назвать разновидностью виртуальных денежных средств. Стабильность котировок Tether обеспечивается применением виртуальных аналогов классических валют; финансовые транзакции осуществляются оперативно, а в качестве виртуальных аналогов могут использоваться как доллар США, так и Евро с обозначениями USDT и EURT соответственно.

- Криптовалюта дополнена удобным мобильным приложением и веб-кошельком, благодаря чему не возникает проблем с безопасным хранением, получением и отправкой криптовалютной единицы.

- Использование системы Tether предполагает также получение и отправку платежей на другие онлайн кошельки или на кошельки Биткоин, которые могут поддерживать Tether. Банковский долларовый перевод используется для вывода средств и пополнения кошелька, а для обмена можно пользоваться услугами разных сервисом. Чаще всего обмен проводится без комиссий и осуществляется мгновенно.

- Организация Tether интегрирована с большим числом компаний, ведущих деятельность в криптовалютной сфере. В качестве примера можно привести интеграцию с Cryptsy, благодаря которой не возникает проблем в привязке фиатных денежных единиц к Биткоину, что дает существенный вклад в развитие системы. Также стоит упомянуть о партнерстве с Coinsbank,

благодаря которому можно использовать дебетовые карты для проведения платежей в EURT или USDT. Coinsbank отвечает за обеспечение биржевых решений и финансовых технологий. Токены EURT можно найти на крипто-финансовой платформе OpenLedger, которая дополняет биткоин-платформу Omni Layer. Такое сотрудничество обеспечивает низкие биржевые комиссии, максимально узкий спред и прозрачные цены при отправке EURT в SEPA посредством данной платформы.

• Минимальный размер суммы, которую можно вводить на кошелек или выводить, составляет 1 криптовалютную единицу, размер комиссии аналогичный. Комиссия при этом не взимается только за вывод средств.

• Валюта пересылается за счет одноранговой сети, при этом преобразование возможно как в автономном режиме за счет мобильного кошелька, так и в режиме онлайн.

Ниже представлены основные преимущества и недостатки криптовалюты Tether (на основе данных источника[45]).

Сильные стороны криптовалюты Tether:

1. Классические денежные средства с использованием Tether можно передавать контрагентам дешевле и намного быстрее, чем при использовании традиционного банковского перевода. Скорость проведения финансовых операций с участием Tether такая же, как при использовании других виртуальных средств.

2. Пользователи не уплачивают комиссионные сборы за перевод денежных единиц между кошельками, разработанными компанией Tether. Небольшая комиссия предусмотрена только за ввод средств и составляет 1 USD.

3. Платежи максимально защищены благодаря использованию блокчейн технологии.

4. Платформа позволяет не только покупать, но также продавать USDT обратно. При такой финансовой операции необходимо находиться на сайте Tether Limited, передать USDT компании и после этого вы получите фиатную валюту с вычетом комиссии. Выведенные таким способом USDT уничтожаются компанией согласно установленному алгоритму, они считаются погашенными и теряют обеспеченность соответствующим числом

[45] URL: https://kripto365.ru/crypto/tether-usdt.html

фиатных денежных единиц. Стоит лишь помнить, что продажа рассматриваемой криптовалюты не сопровождается сложными формальностями на криптовалютных биржах и такой способ считается более выгодным.

5. В большинстве случаев при получении фиатных средств в обмен на криптовалюту создатели направляют их на создание резерва для обеспечения этим же монетам рыночной стабильности. На данный момент резерв насчитывает более 450 млн. долларов, что почти равно общему числу Tether в обращении.

6. Правовое положение некоторых бирж и невозможность получить лицензию на открытие торгов с долларами не позволяло включить их в число торговых валют, но благодаря Tether торговля на таких биржах существенно улучшилась.

7. Переводы долларов с биржи на биржу с использованием USDT стали не такими дорогими, долгими и сложными.

8. Наблюдается простая программная интеграция USDT с онлайн-кошельками других криптовалютных единиц. Пользователи уже имеют возможность скачивать биткоин-кошельки с поддержкой рассматриваемой виртуальной денежной единицы.

Слабые стороны криптовалюты Tether:

1. Курс USDT периодически колеблется, волатильность Tether далека от заявленной «нулевой (обычный коридор колебаний курса ±3%).

2. Несмотря на анонимность отправки и получения USDT, при покупке данной криптовалюты за фиатные деньги необходимо верифицировать аккаунт, а для этого нужно подтвердить личность с помощью сканов документов. На некоторых биржах достаточно регистрации, но все-таки анонимность - не полная.

3. Криптовалюта не рассчитана на независимый майнинг, следовательно, добыча доступна только компании, которая ее создала.

4. Запас ликвидности торговых пар с рассматриваемой криптовалютной единицей на разных биржах не всегда большой. В интернет-обменниках наблюдается более высокая ликвидность, однако, курсы продажи и покупки в данном случае не такие выгодные.

5. Выпуская токены разработчик не обязуется выкупать их у владельца обратно, если тот пожелает. Провести такую финансовую процедуру чаще всего не составляет труда, однако право на усложнение этой операции остается за Tether Limited и это может произойти в любой момент.

Говоря о современном положении виртуальной валюты Tether, его следует назвать достаточно стабильным, что позволяет предполагать длительной и успешное существование проекта. Однако настораживающим фактором является ситуация с увеличением количества эмитированных монет в 2017 году с 10 млн. долларов США до приблизительно 2,4 млрд. долларов США. Имеются серьезные основания думать, что данная эмиссия должным образом не обеспечена и поэтому при возникновении проблем с обменом Tether на фиатные доллары проект может обернуться крахом.

5.5. Концепция создания и функционирования цифровых юрисдикций (криптоюрисдикций)

При использовании криптовалютных механизмов с целью осуществления платежей в условиях санкционных ограничений и рисков немаловажное значение приобретает безопасность юрисдикции, из которой осуществляются те или иные управляющие или согласующие воздействия. Ведь в случае осуществления таких воздействий из той или иной национальной юрисдикции инициаторы санкций в лице, например, США могут распространить на соответствующее государство всевозможные ограничения, объявить «спонсором терроризма» и т.д.

В подобных условиях представляется возможным и технически осуществимым использовать механизм «цифровых юрисдикций» на основе технологий распределенных реестров (блокчейн) и элементов искусственного интеллекта.

Опыт работы оффшоров из т.н. «удобных» юрисдикций уже сам по себе во многом «виртуализирует» понятие традиционной национальной юрисдикции. Так, в 99.9% случаев владелец оффшора не посещает страну регистрации и не ведет в ней арбитраж, а вся его работа связана с удаленным доступом к банковскому счету и фиксированной оплатой юридических и бухгалтерских услуг для своей компании.

Если допустить, что оффшор будет открыт не в одной из существующих стран (Панама, Виргинские острова и т.п.), а в некоей стране XYZ, при этом

вместо традиционного банковского счета будет использоваться цифровой финансовый инструмент, то в вышеупомянутых 99.9% случаев функционирование такого оффшора ничем не будет отличаться от оффшора традиционного.

В то же время остающиеся условные 0.1% - это случаи арбитража и подтверждения прав на капитал. Важность подобных вещей часто бывает столь высока, что владельцы оффшоров часто соглашаются переходить в контролируемые западными державами оффшорные юрисдикции, поскольку по устоявшемуся мнению именно последние обеспечивают лучшую защиту прав на капитал и справедливость арбитража.

Однако соответствующие условия значительно лучше могут быть реализованы в рамках современных цифровых платформ. Так, подтверждение прав на капитал реализуется через систему распределенных реестров, а арбитраж для значительной части возможных споров может обеспечиваться функционалом нейросети, построенной на основе базы знаний по решениям наиболее авторитетных арбитражных инстанций (Лондон, Стокгольм и т.д.). При этом всегда может быть предусмотрена возможность (для крайнего случая) перевести решение того или иного вопроса на рассмотрении «человеческого комитета» (human panel) – либо действующего в одной из традиционных юрисдикций, либо в режиме распределённого голосования, защищённого блокчейном.

Таким образом, путь к созданию криптоюрисдикций в практическом плане - открыт.

В силу определенной сложности соответствующей работы и необходимости для запуска криптоюрисдикции располагать внушительным объемом транзакций, нуждающихся в защите (например между Россией и Венесуэлой или Францией и Ираном), формирование криптоюрисдикций не сможет стать процессом общедоспутным и массовым, подобным эмиссии частных криптовалют. Так или иначе, участие государственных и крупных корпоративных структур окажется необходимым, поэтому встанет дополнительный вопрос о надежной защите информации по такого рода содействию.

Ценность и популярность криптоюрисдикции будет определяться уровнем развития соответствующей цифровой платформы, включающей систему защиты прав и систему арбитража. Отсюда не исключено, что по мере

развития и совершенствования последних заинтересованность в ведении бизнеса через криптоюрисдикции начнут проявлять и несанкционные компании, нуждающиеся в справедливом и беспристрастном арбитраже. Таким образом, соответствующие проекты со временем смогут получить мощную капитализацию и бизнес-развитие.

В качестве еще одной идеи для обсуждения можно предложить перспективный механизм географической локализации криптоюрисдикций на небесных телах, например, в пределах 200-мильных зон от мест посадки на Луну советских космических аппаратов. При всей своей фантастичности, такой подход не только поможет устранить в ряде случаев нежелательную для бизнеса «абсолютную цифровизацию», но и помочь в создании экономического механизма для колонизации ближнего космоса, опирающегося на «право первооткрывателя».

ГЛАВА 6. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБЪЕКТОВ ТЭК В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ.

6.1. Нормативное закрепление угроз информационной безопасности критической информационной инфраструктуры РФ

Как следует из положений Доктрины информационной безопасности Российской Федерации, поступательному развитию информационных технологий в различных отраслях промышленности и в экономике в целом сопутствует возрастание ряда системных угроз.

В качестве первой из таких угроз обозначена *возможность использования трансграничного оборота информации для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности*.

Раскроем данное положение более подробно. Речь здесь прежде всего идет о том, что потоки информации, которыми обмениваются различные субъекты (в нашем случае - субъекты экономической деятельности) не осуществляют свое движение исключительно в рамках юридических границ того или иного государства. Эти потоки могут проходить через устройства передачи информации, находящиеся географически довольно далеко от границ нашей страны. Таковы особенности топологии построения системы сети Интернет, которая давно стала опорной для передачи деловой видео, речевой и текстовой информации. Причем вполне может создаться положение, при котором какой-то ключевой сегмент этой системы находится в полном распоряжении компаний, подконтрольных государству, которое является для России и потенциальным противником в геополитическом противостоянии, и конкурентом в экономике. Это влечет за собой по крайней мере три потенциально негативных следствия:

1) возможность перехвата и чтения информации российских пользователей;

2) возможность модификации и искажения такой информации;

3) возможность отключения российских пользователей от данных серверов.

Любая из таких угроз влечет за собой серьезные проблемы для управления объектами нефтегазового комплекса и передачи деловой информации российскими компаниями, которые осуществляют деятельность в данной сфере.

Существенной угрозой являются также террористические проявления. Современный международный терроризм обладает существенными финансовыми ресурсами, позволяющими привлекать к противоправной деятельности высококвалифицированных специалистов в области IT-технологий, с их помощью реализовывать сценарии блокирования работы различных производственных объектов, создания аварийной обстановки или организации катастроф путем негативного воздействия на информационную инфраструктуру. В последние годы российское государство предприняло ряд шагов в сфере нормативного обеспечения противодействия этим угрозам, о чем речь пойдет в других разделах данной работы.

В качестве следующей основной угрозы обозначено *наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях*.

Анализ данного положения показывает, что оно системно связано с предыдущим, однако формирует несколько иной угол зрения на данную проблему. Дело в том, что информационно-техническое воздействие на информационную инфраструктуру в военных целях может быть как стратегическим, так и тактическим, то есть в одном случае требуется массированная атака на все ключевые объекты промышленности, которые влияют на обороноспособность того или иного государства. Во втором случае осуществляется атака на конкретный объект. Очевидно, что для массированной атаки необходимы значительные силы и средства, которые не всегда возможно задействовать. Во втором случае степень вероятности достижения искомого результата намного выше, так как для решения данной задачи возможно сконцентрировать должное количество сил и средств. Например, значительно реальнее вывести из строя одну систему управления узлом транспортировки природного газа, чем, скажем, всю систему управления магистральными газопроводами.

Как далее следует из положений Доктрины информационной безопасности, *расширяются масштабы использования специальными службами отдельных*

государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

Применительно к нефтегазовому комплексу это прежде всего означает попытки дискредитации основных субъектов экономической деятельности, а именно Газпрома, Роснефти, Транснефти и ряда других, которых постоянно обвиняют в монополизации рынка, подкупе должностных лиц различных государств, нарушении экологии и многих других нарушениях.

В качестве еще одной системной угрозы Доктрина информационной безопасности определила *возрастание масштабов компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий*.

Данная угроза, хотя и не может повлечь за собой таких масштабных последствий, как предыдущие, но носит для повседневной действительности более реальный характер. Дело в том, что в IT-сфере по-прежнему велика роль отдельных талантливых людей, которые свои способности могут направить не на созидание, а на разрушение и наживу. Исходя из этого, сценарии взлома систем защиты информационной инфраструктуры отдельных объектов нефтегазового комплекса из хулиганских побуждений вполне вероятны. Негативные последствия при этом могут быть сопоставимы с тем воздействием, которое осуществляется, так сказать, на профессиональной основе. Причем субъектами таких проступков могут быть и граждане нашего государства, и иностранные граждане, имеющие доступ к информационной инфраструктуре, так и работники организаций, эксплуатирующих объекты нефтегазового комплекса.

Не менее существенным для обеспечения стабильности работы нефтегазового комплекса является финансовая составляющая данной деятельности. Поэтому кражи денежных средств со счетов организаций, блокировка финансовых потоков и другие негативные сценарии могут

оказать существенно вредное влияние на стабильность работы отдельных структур данной отрасли промышленности.

Отдельную проблему составляет обеспечение защиты личной жизни граждан и обеспечение сохранности их персональных данных в деятельности организаций, осуществляющих деятельность в области розничного снабжения газом и розничной продажи нефтепродуктов. Учитывая масштабы данной деятельности, множественность организаций, которые задействованы в данной области экономических отношений, проблема исключения несанкционированного доступа к персональным данным граждан приобретает в данном случае весьма существенное значение. По бонусным картам сетевых автозаправок вполне можно с высокой точностью отследить передвижение гражданина, на имя которого такая карта была оформлена, в течение довольно длительного промежутка времени. Хорошим поисковым ресурсом являются обрабатываемые в автоматизированном режиме договоры на розничное снабжение газом в многоквартирных домах и в домах индивидуального пользования. Таким образом, информационные ресурсы организаций нефтегазового комплекса, могут быть использованы для получения персональной информации граждан, в том числе и с противоправными целями. И с каждым годом, по мере роста и совершенствования поисковых систем, такая опасность будет возрастать.

5 декабря 2016г. состоялось заседание «круглого стола» Комитета Государственной Думы по энергетике на тему: «Перспективы развития вопросов информационной безопасности топливно-энергетического комплекса и законодательные аспекты обеспечения безопасности информационных систем объектов топливно-энергетического комплекса». В рекомендация, принятых по итогам заседания, отмечено: «в последнее время объекты топливно-энергетического комплекса по всему миру становятся мишенью для дестабилизации ситуации, … наблюдается устойчивый рост количества инцидентов по нарушению информационной безопасности, при этом увеличивается как сложность и комплексность угроз, так и их интенсивность.

…Наблюдается устойчивое усложнение иерархии групп нарушителей, повышение их технической оснащенности и уровня маскировки. Данные преступные группы как правило ставят своей целью дестабилизацию обстановки потенциального противника, информационную борьбу, вывод из

строя объектов инфраструктуры, нарушение работоспособности целых секторов экономики и нарушение работы коммуникаций и связи…»

6.2. Нормативно-правовая база, регламентирующая вопросы безопасности критической информационной инфраструктуры РФ

В настоящее время вопросы безопасности критической информационной инфраструктуры Российской Федерации регламентируются целым блоком нормативных актов, основным среди которых является Федеральный закон от 26.06.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[46].

Данный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак. Определены основные принципы обеспечения безопасности, полномочия государственных органов, а также права, обязанности и ответственность лиц, владеющих на праве собственности или ином законном основании объектами инфраструктуры, операторов связи и информационных систем, обеспечивающих взаимодействие этих объектов. Закреплены понятия компьютерной атаки, компьютерного инцидента и др. Функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы увязано с защитой КИИ. Предусмотрены категорирование объектов; ведение реестра значимых объектов; оценка состояния защищенности; государственный контроль.

Одновременно с принятием Федерального закона от 26.06.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» внесены дополнения в следующие федеральные законы:

- Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» (пункт 4 статьи 5);
- Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (пункт 1.1 статьи 12, пункт 1 статьи 46);
- Федеральный закон от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при

[46] СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

осуществлении государственного контроля (надзора) и муниципального контроля» (Часть 3.1 статьи 1);

- Уголовный кодекс Российской Федерации (статья 274-1);
- Уголовно-процессуальный кодекс Российской Федерации (статья 151).

Среди всех дефиниций, представленных в рассматриваемом законодательном акте 187-ФЗ, выделим пять, которые можно обозначить в качестве новелл, ранее не встречавшихся в актах такого уровня, и создающих систему понятий для данной сферы правового регулирования.

Первой из таких дефиниций является собственно понятие критической информационной инфраструктуры. Оно определено в Законе как "объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов". Из этого понятия следует, что критическая информационная инфраструктура образует систему собственно из ее самой, а также из сетей электросвязи, которые задействованы для передачи информации, циркулирующей в данной системе.

Исходя из вышесказанного, логично определить и понятие "объекты критической информационной инфраструктуры", под которыми понимаются "информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры". Определения объектов, включенных в данное понятие, мы можем найти в другом профильном законодательном акте - Федеральном законе от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации"[47], где информационная система определена, как "совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств", а информационно-телекоммуникационная сеть, как "технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники". Понятие "автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры Российской Федерации" содержится в другом акте - "Основных направлениях государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и

[47] СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

технологическими процессами критически важных объектов инфраструктуры Российской Федерации", утвержденных Президентом Российской Федерации 03.02.2012 № 803[48], где под ним понимается "комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам Российской Федерации, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий и организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий".

Следует отметить, что в системе критической информационной инфраструктуры организаций нефтегазового комплекса, данный вид объектов является, как представляется авторам, основной целью защиты.

Следующей дефиницией, подлежащей рассмотрению, является понятие "значимый объект критической информационной инфраструктуры", под которой Закон предлагает понимать "объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры". Из данного определения видно, что для признания такого объекта значимым необходимо реализовать две административные процедуры:

1) осуществить его отнесение по определенным правилам к определенной категории (осуществить категорирование);

2) в установленном порядке включить его в перечень, именуемый реестром значимых объектов критической информационной инфраструктуры.

Ниже данные процедуры и их правовое регулирование будут рассмотрены несколько подробнее.

[48] Документ опубликован не был. Источник: банк правовой информации КонсультантПлюс.

Следующим понятием, которое представлено в Законе, является дефиниция "компьютерная атака", под которой предлагается понимать "целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации".

Понятие, прямо скажем, довольно сложное и, как представляется автору, не до конца проработанное. Итак, есть некоторые программные средства, аппаратно-программные средства или их совокупность. Под ними следует понимать программы для ЭВМ, совокупность программ для ЭВМ с техническими устройствами, находящимися во взаимодействии, а также системы, состоящие из программных средств и аппаратно-программных средств, которые действуют в рамках общего функционирования ЭВМ. Эти средства "целенаправленно воздействуют" на определенные объекты, имея целью прекращение их функционирования, а также нарушения такого функционирования. Следует отметить, что сами по себе программы или аппаратно-программные средства не могут ничего сделать - они начинают управлять ЭВМ или системой ЭВМ, которые, в свою очередь, прекращают нормальное функционирование. Эти ЭВМ входят в состав объектов критической информационной инфраструктуры.

Понятие «безопасность информации» по своей доктринальной сути представляет собой состояние защищенности сведений от их противоправного копирования, видоизменения или уничтожения, то есть в данном случае речь идет не о угрозе функционирования некоторой системы автоматизированного управления, а о сведениях, которые имеют самостоятельную ценность, например, о сведениях, составляющих государственную тайну.

Следующим понятием, которое необходимо проанализировать, является представленная в Законе дефиниция "компьютерный инцидент". Под ним понимается "факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки".

Очевидно, что определение рассматриваемого понятия не связывает напрямую сбой в работе или прекращение функционирования объекта критической инфраструктуры с компьютерной атакой, однако в любом случае такому происшествию присваивается название "компьютерный инцидент". Как представляется, причиной такого подхода является презумпция того, что все современные информационные системы и системы связи основаны на компьютерных технологиях.

Применительно к понятию "субъекты критической информационной инфраструктуры" следует отметить, что рассматриваемый законодательный акт достаточно четко определяет социальные и экономические сферы, в которых государственные органы, государственные учреждения, юридические лица (в определении подчеркивается, что только находящиеся под юрисдикцией нашего государства) или индивидуальные предприниматели могут быть признаны таковыми. К этим сферам относятся: здравоохранение, наука, транспорт, связь, энергетика, банковская сфера и иные сферы финансового рынка, горнодобывающая, металлургическая и химическая промышленность.

Одной из важнейших задач, которую призван был разрешить Закон о безопасности критической информационной инфраструктуры, является создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак. На рисунке 2.1. схематично показана трехуровневая структура: на верхнем уровне – Президент и Правительство Российской Федерации, издающие распорядительные нормативные акты, на втором уровне – регуляторные органы, среди которых целесообразно выделить ФСТЭК России, ФСБ России, в составе которой образован "Национальный координационный центр по компьютерным инцидентам"; на третьем уровне субъекты критической информационной инфраструктуры, которые должны непосредственно принимать участие в обеспечивать обнаружении, предупреждении и ликвидации последствий компьютерных атак и реагировании на компьютерные инциденты.

Необходимо отметить, что Указом Президента Российской Федерации от 22.12.2017 г. №620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» на Федеральную службу безопасности Российской Федерации возложены функции федерального органа исполнительной власти, уполномоченного в области

обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

рис. 6.1. Участники защиты критической информационной инфраструктуры

В связи с тем, что средний уровень системы является для отечественной административной системы новеллой, рассмотрим его задачи и функции несколько подробнее. Положение о "Национальном координационном центре по компьютерным инцидентам" утверждено приказом ФСБ России от 24.07.2018 г. № 366[49], что позволяет утверждать его, в основном, ведомственную принадлежность.

В качестве основной задачи для Центра определено "обеспечение координации деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения,

[49] Официальный Интернет-портал правовой информации. 10.09.2018.

предупреждения и ликвидации компьютерных атак и реагирования на компьютерные инциденты".

Для обеспечения выполнения данной задачи Центр осуществляет следующие функции:

1. Координирует мероприятия по реагированию на компьютерные инциденты и непосредственно участвует в таких мероприятиях. Из этого следует, что это не только наблюдательно-совещательная структура, но организация, способная выполнять конкретные работы.

2. Организует и осуществляет обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты. Из контекста данного положения следует, что борьба с хакерством рассматривается как общенациональная и даже международная задача. Указанное выводит данную работу на новый качественный уровень.

3. Осуществляет методическое обеспечение деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Функция довольно очевидная, так как любая постоянно действующая государственная система с большим числом элементов, находящаяся в развитии, требует единообразного и четкого методического обеспечения.

4. Участвует в обнаружении, предупреждении и ликвидации последствий компьютерных атак. Эта функция свидетельствует о том, что Центр является "рабочим" подразделением, которое может оказывать непосредственную помощь подразделениям системы третьего, низшего уровня.

5. Обеспечивает своевременное доведение до субъектов критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения. Данная функция корреспондирует к функции, описанной в п. 3, и является ее конкретизацией.

6. Осуществляет сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. Как представляется, данная функция является одной из важнейших в деятельности Центра, так как позволяет не только накапливать необходимую информацию и ее анализировать, но и вырабатывать новые научные методы борьбы с данными явлениями.

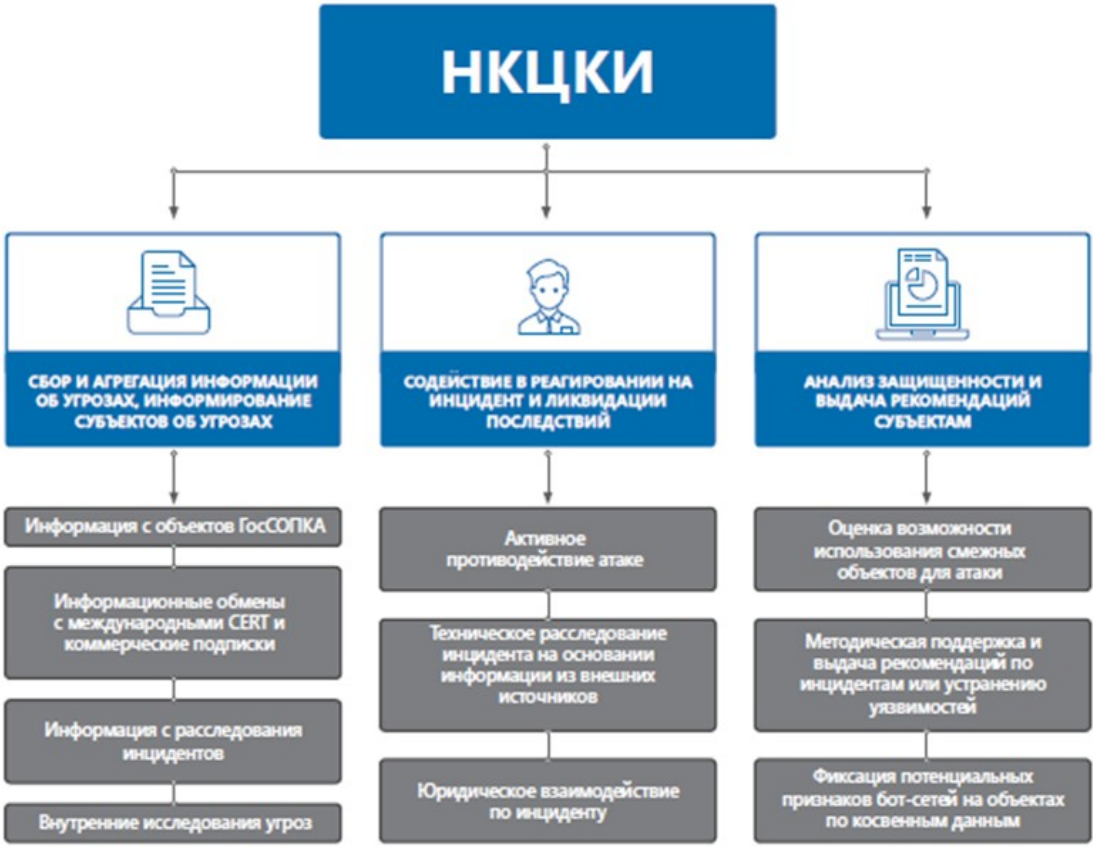


Рис. 6.2. Структура задач НКЦКИ

Следующей важной группой норм, определяющей параметры системы противодействия компьютерным атакам, является *категорирование* объектов критической информационной инфраструктуры, которое является административной процедурой, устанавливающей определенный уровень значимости (ценности, важности) того или иного объекта для определенных правоотношений. От величины категории чаще всего зависит объем затрат, которые необходимо осуществить для защиты данного объекта от

определенных угроз или сил и средств, которые необходимо привлечь для решения определенной задачи (например, для тушения пожара).

Рассматриваемый Закон определяет категорирование объекта критической информационной инфраструктуры как "установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения".

В соответствующей норме Закона определяется, что категорирование осуществляется, исходя из:

1. Социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги.

Обратим внимание на тот факт, что социальная значимость, как критерий категорирования, определена Законом на первое место. Это косвенно свидетельствует об основной направленности данной системы - защиты населения и экономики от угроз, связанных с последствиями компьютерных атак.

2. Политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики. Данный критерий категорирования связан с угрозами, заключающимися в атаках на информационную инфраструктуру органов государственной и муниципальной власти, общественных организаций политической направленности. Это прежде всего блокирование сайтов, дезорганизация их работы, попытки получения информации ограниченного доступа и т.д.

3. Экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации. В данном случае идет речь о материальном ущербе, который потенциально может быть представлен в денежном эквиваленте.

4. Экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду. Последствия компьютерных инцидентов могут

выражаться, в частности, в остановке работы очистных сооружений, во вредных выбросах в атмосферу и водоемы в результате возникшего из-за сбоев в работе автоматизированных устройств нарушения технологии производства определенных веществ и т.д.

5. Значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. Данный критерий является очевидным и должен участвовать в оценке применительно практически к любому объекту критической информационной инфраструктуры.

"Правила категорирования объектов критической информационной инфраструктуры" утверждены постановлением Правительства Российской Федерации от 08.02.2018 г. № 127[50]. Данная административная процедура опирается на определенный набор критериев значимости, приведенных в данном акте, и также разделенных на три уровня. Например, показатель "причинение ущерба жизни и здоровью людей (человек)": если их количество более или равно одному, но менее или равно пятидесяти, то присваивается III категория, если более пятидесяти, но менее или равно пятистам, то присваивается II категория, если число пострадавших более пятисот, то присваивается I категория.

Данные Правила также определяют перечень исходных данных для категорирования, к которым относятся:

а) сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

б) состав информации, обрабатываемый объектами критической информационной инфраструктуры, сервисы по управлению, контролю и мониторингу, предоставляемые объектами критической информационной инфраструктуры;

в) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной

[50] СЗ РФ. 2018. № 8. Ст. 1204.

инфраструктуры (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации);

г) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов;

д) угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

Процедура категорирования объекта критической информационной инфраструктуры производится комиссионно, в состав комиссии могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативному правовому регулированию в установленной сфере деятельности.

Следует также иметь ввиду то обстоятельство, что Закон о безопасности критической информационной инфраструктуры допускает изменение категории значимости объектов критической информационной инфраструктуры, как в сторону повышения, так и в сторону снижения первоначально установленной категории.

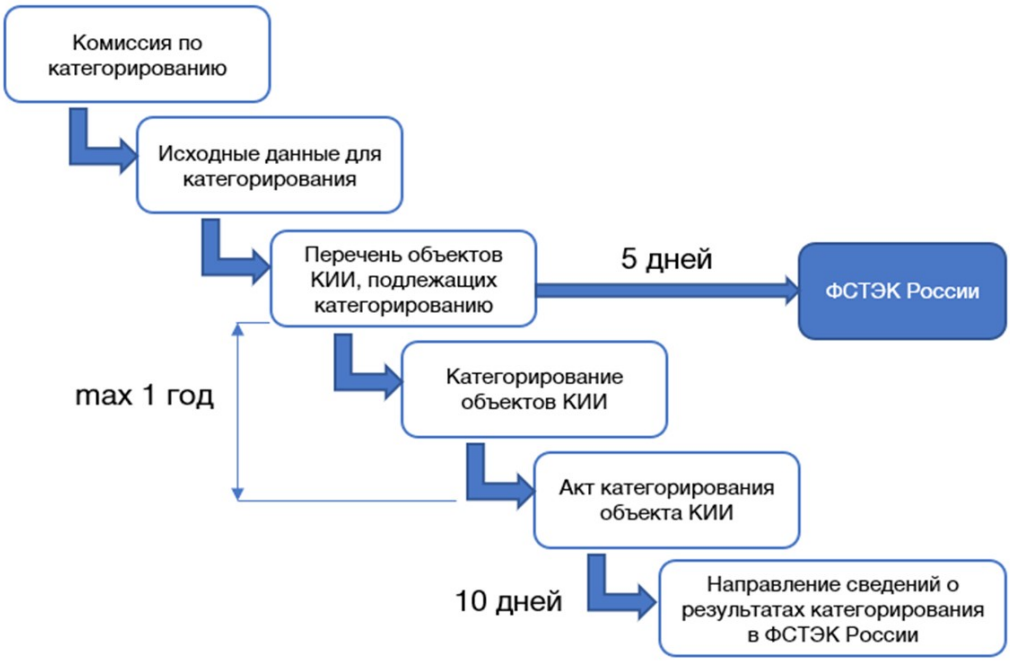


рис. 6.3. Схема процедуры категорирования объектов КИИ

Для единообразного подхода к формированию перечней объектов критической информационной инфраструктуры, подлежащих категорированию, рекомендуется «направлять в ФСТЭК России утвержденный руководителем субъекта критической информационной инфраструктуры (или уполномоченным лицом) перечень объектов критической информационной инфраструктуры, подлежащих категорированию, оформленный в соответствии с приложением 1» к Информационному сообщению ФСТЭК России «По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» от 24 августа 2018 г. № 240/25/3752.

Акты категорирования объекта КИИ направляются во ФСТЭК России, уполномоченное на ведение Реестра значимых объектов критической информационной инфраструктуры. Порядок ведения такого реестра определен приказом Федеральной службы по техническому и экспортному контролю от 06.12.2017 г. № 227[51]. Схема рассмотрения акта представлена на рис. 4.3.

[51] Официальный Интернет-портал правовой информации 09.02.2017.

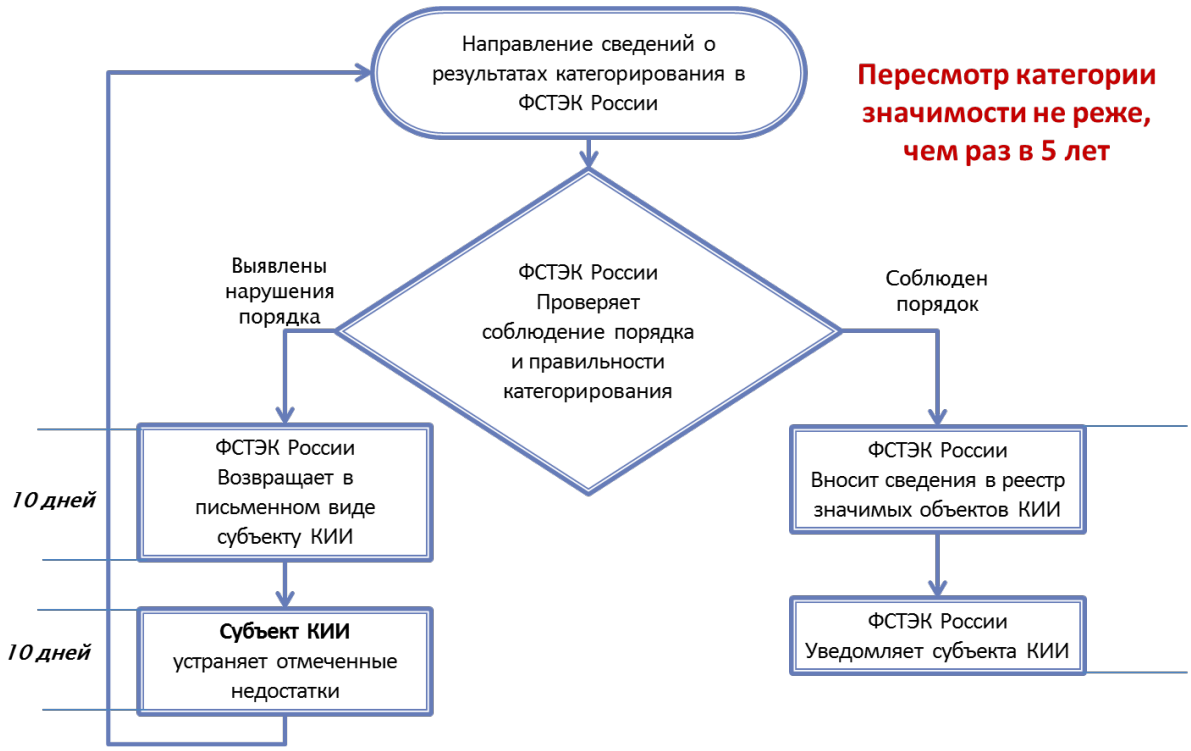


Рис. 6.4. Порядок рассмотрения результатов категорирования.

Решение о включении сведений о значимом объекте критической информационной инфраструктуры в Реестр принимается в течение тридцати дней со дня получения ФСТЭК России сведений от субъекта критической информационной инфраструктуры.

С точки зрения понимания совокупности проблем, возникающих в деятельности субъектов критической информационной инфраструктуры, целесообразно более подробно остановится на определенной рассматриваемым Законом системе их прав и обязанностей.

В соответствии со ст. 9 Федерального закона 187-ФЗ «в целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование».

Система безопасности объекта КИИ создается в соответствии с Приказом ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к

созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования». Данный приказ:

- устанавливает требования к силам обеспечения безопасности значимых объектов;
- устанавливает требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов;
- устанавливает требования к организационно-распорядительным документам по безопасности значимых объектов.

Данный приказ, в частности определяет:

«8. **Руководитель субъекта критической информационной инфраструктуры** или уполномоченное им лицо, на которое возложены функции обеспечения безопасности значимых объектов критической информационной инфраструктуры, создает систему безопасности, организует и контролирует ее функционирование.

9. **Руководитель субъекта критической информационной инфраструктуры** определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов критической информационной инфраструктуры…

10. **Руководитель субъекта критической информационной инфраструктуры** создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее - структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры.»

Приказом ФСТЭК России от 25 декабря 2017 г. № 239 утверждены Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации. Данный приказ:

- устанавливает требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов;

- устанавливает требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов;
- определяет состав мер по обеспечению безопасности для значимых объектов соответствующей категории.

Необходимо отметить, что для значимых объектов КИИ применяются приказы ФСТЭК России №235 и №239. Состав мер защиты информации и их базовые наборы в приказе ФСТЭК №31 (таблица в Приложении к Приказу) приведены в полное соответствие с составом мер по обеспечению безопасности значимого объекта КИИ в приказе ФСТЭК №239. При этом в приказе №31 требования определяются классами защищённости АСУ, а в приказе №239 — категориям значимости. Порядок определения угроз безопасности информации в приказе №31 приведён в соответствие с приказом №239.

Как следует из положений рассматриваемого Закона, субъекты критической информационной инфраструктуры имеют право:

1) получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, информацию, необходимую для обеспечения безопасности значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или на ином законном основании, в том числе об угрозах безопасности обрабатываемой такими объектами информации и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах;

2) в порядке установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

3) при наличии согласия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской

Федерации, за свой счет приобретать, арендовать, устанавливать и обслужить средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) разрабатывать и осуществлять мероприятия по обеспечению значимого объекта критической информационной инфраструктуры.

Как следует из приведенных выше положений, руководство со стороны федерального органа исполнительной власти, уполномоченного в области функционирования системы обнаружения компьютерных атак, является скорее информационно-методическим – основная материальная нагрузка ложится на субъектов критической информационной инфраструктуры, которые за счет собственных средств должны формировать у себя данную систему.

Реализация прав субъектов КИИ регламентируется приказом ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

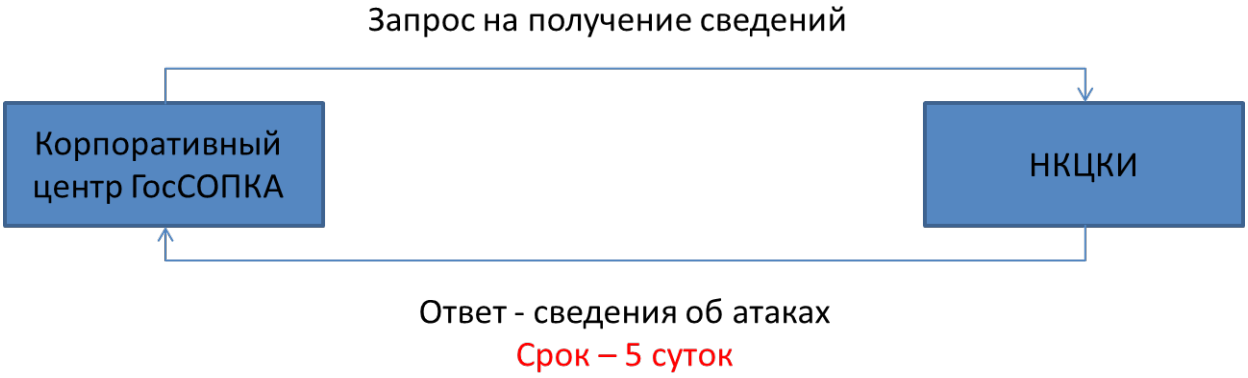


Рис. 6.5. Порядок получения сведений из НКЦКИ

Обратимся теперь к системе обязанностей субъектов критической информационной инфраструктуры, определенной рассматриваемым Законом. Кратко они выглядят следующим образом:

1) незамедлительно информировать о компьютерных инцидентах вышеуказанный федеральный орган исполнительной власти;

2) оказывать содействие должностным лицам вышеуказанного федерального органа исполнительной власти в обнаружении, предупреждении и

ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

Наряду с вышеуказанными обязанностями, те из субъектов, которым на праве собственности или на праве аренды принадлежат значимые объекты критической информационной инфраструктуры, дополнительно должны:

1) соблюдать требования по обеспечению значимых объектов критической информационной инфраструктуры;

2) выполнять предписания должностных лиц уполномоченного федерального органа исполнительной власти, об устранении нарушений в чсти соблюдения требований по обеспечению безопасности значимого объекта критической информационной инфраструктуры, выданные этими лицами в соответствии со своей компетенцией;

3) реагировать на компьютерные инциденты в порядке, утвержденном уполномоченным федеральным органом исполнительной власти, а также принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;

4) обеспечивать беспрепятственный доступ должностным лицам уполномоченного федерального органа исполнительной власти к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий по осуществлению государственного контроля.

В этой связи необходимо упомянуть приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

В соответствии со ст. 13 Федерального закона 187-ФЗ установлена система государственного контроля в области обеспечения безопасности значимых объектов КИИ. Постановлением Правительства Российской Федерации от 17.02.2018 № 162 утверждены Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, которые вступили в силу 28 февраля 2018 г.

Приказом ФСТЭК России от 11 декабря 2017 г. № 229 утверждена формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.

В соответствии вышеуказанным Постановлением Правительства Российской Федерации:

«34. На основании акта проверки в случае выявления нарушений требований по безопасности орган государственного контроля выдает субъекту критической информационной инфраструктуры предписание об устранении выявленного нарушения с указанием срока его устранения.

35. К акту проверки прилагаются протоколы или заключения по результатам контрольных мероприятий, проведенных с использованием программных и аппаратно-программных средств контроля, а также предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.»

Подводя итог рассмотрению вопроса о законодательном регулировании обеспечения безопасности критически важной информационной инфраструктуры, следует отметить, что рассмотренным Федеральным законом по сути легитимирована новая государственная система, центральным элементом которой является федеральный орган исполнительной власти, уполномоченных в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации компьютерных атак. В настоящий период времени инициатива по категорированию объектов информационной инфраструктуры формально принадлежит организациям и индивидуальным предпринимателям, которые такие объекты эксплуатируют, однако по мере того, как опасность компьютерных инцидентов будет возрастать, отнесение объектов к данной категории может стать императивным. Структурам топливно-

энергетического комплекса Российской Федерации предстоит большая работа по формированию такой системы на своих объектах и наработке опыта эксплуатации соответствующего программного обеспечения и оборудования.

6.3. Нормативное регулирование криптовалют как индикатор отношения государственных властей

Ниже представлены основные события в сфере попыток государственного регулирования криптовалют в разных странах. «Жирный» цвет обозначает даты, когда решения принимались **против** криптовалют, «курсив» – **за**.

Май 2012 г. ФБР опубликовала отчёт «Виртуальная валюта Биткойн», в котором Биткойн рассматривался в негативном свете, как система, «в которой преступники могут генерировать, переводить, красть и отмывать незаконные средства с некоторой долей анонимности». В отчёте говорилось, «что правоохранительные органы всё же смогут с достаточной степенью уверенности идентифицировать вредоносных субъектов и получить дополнительную информацию от них».

Март 2013 г. Минфин США потребовал, чтобы все фирмы, занимающиеся обменом виртуальной валюты, были зарегистрированы как MSB, а также выявляли бы подозрительные сделки и сообщали о них регуляторам, как это делают банки. После этого несколько бизнесов, работающих с bitcoin, сообщили, что банки закрыли их счета.

Июль 2013 г. ЦБ Таиланда запретил финансовым организациям страны использовать операции с криптовалютой, не признав её валютой.

19 августа 2013 г. Министерство финансов ФРГ официально признало криптовалюту bitcoin расчётной денежной единицей. В официальном заявлении указывается, что bitcoin – финансовый инструмент, который не может быть классифицирован как электронная или иностранная валюта, а больше напоминает «частные деньги», которые могут быть использованы для «многосторонних клиринговых операций».

Сентябрь 2013 г. в США состоялась встреча высокопоставленных сотрудников финансовых и правоохранительных органов США с руководством Bitcoin Foundation – организации, объединяющей участников

рынка bitcoin. По итогам представители федеральных властей США подтвердили намерение распространить на операции с bitcoin правила по борьбе с отмыванием денег, действующие в отношении обычных валют.

1 октября 2013 г. ФБР закрыло интернет-магазин Silk Road «Шелковый путь»), занимающийся, помимо прочего, продажей наркотиков. Все операции в магазине проводились в bitcoin, что позволяло покупателю сохранить анонимность. Вместе с закрытием магазина власти арестовали владельца сайта Росса Уильяма Ульбрихта (Ross William Ulbricht), также известного как Dread Pirate Roberts (сокращенно – DPR). В конце октября прокурор южного округа штата Нью-Йорк Прит Барара (Preet Bharara) сообщил, что правительство конфисковало у Ульбрихта 144336 монет bitcoin. Это число примерно равно количеству монет в самом «толстом» кошельке, который теперь принадлежит ФБР.

Ноябрь 2013 г. В середине ноября состоялись слушания по вопросу о Биткойне в Комитете по национальной безопасности Сената США. Такие заседания не предполагают принятия каких-либо нормативных и обязывающих документов, тем не менее, высказанные в ходе их мнения, а тем более, письменные заключения, играют в деловой и политической жизни Америки и мира огромную роль. Глава ФРС Бен Бернанке заявил о допустимости использования bitcoin в некоторых сферах. Это заявление способствовало резкому увеличению курса bitcoin.

К моменту, когда первая часть слушаний подошла к концу, газета «Washington Post» опубликовала статью под заголовком «Слушанья в Сенате превратились в чествование Биткойна». Когда сенатор Карпер закончил заседание, цена bitcoin на Mt.Gox достигла $700, увеличившись на $150.

5 декабря 2013 г. ЦБ Китая запретил китайским банкам и другими финансовым учреждениям осуществлять операции с bitcoin. В документе говорится: «В целях защиты прав собственности и интересов общества, для защиты правового статуса юаня как валюты, чтобы предотвратить риски отмывания денег и поддерживать финансовую стабильность… уведомляем, что bitcoin не является валютой или заменой денег, не имеет правового статуса и денежного эквивалента, не может и не должна использоваться в качестве денег при обращении на рынке. По сути, это всего лишь специфический виртуальный товар. Финансовым учреждениям не разрешается принимать и проводить платежи в bitcoin, как если бы это была

официальная валюта. Интернет сервисы должны соблюдать все правила по противодействию отмыванию средств, полученных незаконным путём».

При этом Китай подчеркнул, что разрешает своим гражданам покупать и продавать bitcoin, а сервисам и интернет-магазинам осуществлять расчёты в них. Но делать они должны это на свой страх и риск и Национальный банк Китая ответственности за это не несёт.

5 декабря 2013 г. сделал заявление центробанк Франции: подчеркивается, что анонимный и нерегулируемый характер bitcoin делает эту валюту пригодной для отмывания денег и даже спонсирования терроризма. Также в заявлении говорится, что bitcoin может представлять угрозу для инвесторов ввиду своей нестабильности.

Декабрь 2013 г. В самом начале декабря с.г. Биткойн поддержал Банк Англии. Он санкционировал выпуск Королевским Монетным Двором Великобритании памятных суверенных монет, номинированных в bitcoin для мини-государства Олдерни, входящего в состав Нормандских островов, и находящихся под суверенитетом Британской короны. Фактически Банк Англии пошел дальше всех. Памятную монету, которая, тем не менее, является обычными деньгами маленького островного государства, он разрешил номинировать в bitcoin, т.е. признал их, по сути, полноценными деньгами.

Декабрь 2013 г. ЦБ Индии предостерег финансовые организации от высоких рисков операций с bitcoin. Некоторые индийские торговые площадки по обмену bitcoin приостановили работу, но заявления о запрете криптовалют не прозвучало.

12-13 декабря 2013 г. Генеральный директор налоговой службы Норвегии Ганс Христиан Хольте заявил: «Bitcoin не соответствует традиционным представлениям о деньгах и валюте. Мы взвесили все «за» и «против» и решили, каким образом лучше подходить к bitcoin с точки зрения налогов». В итоге криптовалюту приравняли к биржевому инструменту, и значит, держатели этого актива вынуждены будут платить налог на прирост капитала. Напомним, что и Германия в августе обложила виртуальные деньги налогом.

13 декабря 2013 г. Европейское банковское управление (European Banking Authority) на волне резко возросшего интереса к bitcoin выступило с

заявлением о рисках использования виртуальных валют. При этом EBA изучает вопрос о необходимости регулирования этой сферы.

27 января 2014 г. Банк России распространил заявление, согласно которому обмен bitcoin и оплата ими работ и услуг будут приравниваться к отмыванию нелегальных доходов и финансированию терроризма. Согласно статье 27 закона «О Центральном банке РФ», выпуск на территории России денежных суррогатов запрещается.

«Банк России предупреждает, что предоставление российскими юрлицами услуг по обмену виртуальных валют на рубли и иностранную валюту, а также на товары (работы, услуги) будет рассматриваться как потенциальная вовлечённость в осуществление сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма».

Январь 2014 г. Финансовые власти Великобритании могут оптимизировать налоговый режим для операций с bitcoin, которые облагаются налогом в 20%, как операции с долговыми расписками.

Февраль 2014 г. В Генеральной прокуратуре РФ прошло заседание экспертов Межведомственной рабочей группы по противодействию преступлениям в сфере экономики (в неё входят представители ЦБ, МВД, ФСБ и Генпрокуратуры). По ее итогам прокуратура в своем заявлении предостерегла граждан и бизнес от использования bitcoin: «...анонимные платёжные системы и криптовалюты, в том числе наиболее известная из них – биткойн, являются денежными суррогатами и не могут быть использованы гражданами и юридическими лицами».

ФСБ и МВД ищут в России компании, принимающие bitcoin. Такое право им дает позиция Генеральной прокуратуры, которая вслед за Банком России объявила вне закона виртуальные валюты. Все операции с ними могут изучаться в рамках борьбы с отмыванием средств и финансированием терроризма.

Февраль 2014 г. Российские власти смягчились по отношению к электронным деньгам, отказавшись принимать полный запрет на bitcoin. Новым девизом стало «регулирование, а не запрет».

16 апреля 2014 г. В связи с санкциями США против Кремля за его санкции против Украины, MasterCard и Visa прекратили осуществлять некоторые

транзакции на территории России. Этот шаг воодушевил приверженцев электронных денег выдвинуть bitcoin в качестве решения финансовых проблем России.

На территории России bitcoin можно расплатиться за покупку товаров на некоторых сайтах, а также в нескольких магазинах и отелях. В глобальном рейтинге по количеству пользователей bitcoin Россия занимает 5-е место с 204502 пользователями. (четыре страны, опередившие Россию: США, где bitcoin используют 1133272 человек, затем следует Китай с 368004 пользователями, 3-е место занимает Германия – 247658 пользователей, и замыкает пятёрку Британия – 220145 пользователей).

23 апреля 2014 г. в России прошла 1-я конференция по Биткойну. В мае Европейский университет в Санкт-Петербурге запустит бесплатный интернет-курс о bitcoin.

Октябрь 2014 г. Минфин предложил ввести штрафы за выпуск и использование криптовалют: до 50 тыс. руб. для физических лиц и до 1 млн. руб. – для юридических. Центробанк, который ранее также критиковал криптовалюту, отказался «выявлять криптовалютные операции и принимать по ним решения», пояснив, что это не соответствуют его целям и функциям.

Октябрь 2015 г. Министерство финансов ужесточило подход к наказанию за выпуск и оборот криптовалют. Ведомство Антона Силуанова разработало поправки в Уголовный кодекс, по которым нарушителей будут сажать в тюрьму на 4 года. Ранее Минфин предлагал более мягкое наказание за выпуск и оборот криптовалют – штраф до 500 тыс. руб. или исправительные работы сроком до 2-х лет.

14 января 2016 г. в интервью «Российской газете» глава Следственного комитета Александр Бастрыкин заявил о поддержке ведомством идеи введения уголовной ответственности за выпуск и оборот денежных суррогатов, в частности bitcoin. «Анонимность платежей мотивирует к использованию виртуальной валюты для совершения преступлений, в том числе, таких как торговля наркотиками, оружием, финансирование терроризма, уклонение от уплаты налогов», – цитирует слова Бастрыкина «Интерфакс». Силовики отмечают, что криптовалюты используются при вербовке в ИГ.

2 июня 2016 г. Вопрос о легализации криптовалют в России обсуждался вчера на международной конференции «Электронная валюта в свете

современных правовых и экономических вызовов». ЦБ чётко обозначил свою позицию по данному вопросу: «Национальной криптовалюты в РФ в ближайшем будущем не будет». Об этом заявил заместитель директора департамента информационных технологий Банка России Вадим Калухов.

В России отказались от идеи создания национальной криптовалюты, но не намерены запрещать использование подобных инструментов. Предполагается, что с определёнными ограничениями криптовалюты смогут применяться, но не как самостоятельные денежные единицы, а как платёжный инструмент. Такой подход в корне меняет саму идею криптовалют как безэмиссионных и независимых от государства денег и лишает их привлекательности для конечного потребителя, но позволяет финансовым институтам усовершенствовать технологии.

Это, однако, не означает, что Банк России в принципе против применения криптовалют на территории России. «Признание криптовалюты денежной единицей, самостоятельно участвующей в расчётах, будет означать введение ещё одной валюты в нашей стране – это потребовало бы существенного изменения законодательства, начиная с Конституции. Такой вариант криптовалюты вызывал жёсткую реакцию у властей», – отметила в ходе конференции руководитель межведомственной рабочей группы по оценке рисков оборота криптовалюты Госдумы Элина Сидоренко. – «Есть ещё один вариант её применения – в качестве универсального платёжного инструмента»: человек обменивает реальные деньги на криптовалюту (по сути – цифровой код), далее этот код передается в другую финансовую организацию, где вновь обменивается на реальные деньги. Подобный подход к криптовалюте не потребует глобальной правки законодательства – достаточно пересмотреть закон «О национальной платежной системе», отметила Сидоренко. По её словам, проведение подобных операций ускорит платежи, а также позволит отказаться от SWIFT при финансовых переводах, в т.ч. межбанковских.

1-3 июня 2017 г. В ходе Петербургского международного экономического форума зампред Центробанка Ольга Скоробогатова сообщила, что регулятор приступил к работе над созданием национальной цифровой валюты: «До виртуальной национальной валюты мы точно дойдём, мы над этим уже начали работать…Мне кажется, что в ближайшие 2-3 года эта тема будет очень активно развиваться, и мы изучаем все плюсы и минусы этой темы»,

В Росфинмониторинге, который следит за законностью экономических операций в стране, поддержали идею создания российской криптовалюты. Заместитель руководителя ведомства Павел Ливадный сообщил, что при разработке данного инструмента Росфинмониторинг будет ориентироваться на устранение анонимности пользователей: «Мы понимаем, насколько криптовалюты могут оказаться вредоносными для национальных экономик, для стабильности финансовых систем, и исходим из того, что, поскольку все развитые страны эту тематику регулируют, она должна быть урегулирована и у нас».

9 июня 2017 г. замминистра финансов Алексей Моисеев заявил, что криптовалюту в России могут квалифицировать как «иное имущество», то есть придать ей более-менее легальный статус. Он добавил, что при проведении операций с отечественной цифровой валютой клиенты будут идентифицированы. Он также подчеркнул, что при проведении транзакций с криптовалютой необходимо ввести идентификацию клиентов и предусмотреть защиту прав покупателей.

Таким образом, речь не идёт о создании полного аналога Биткойна. Отечественная криптовалюта будет не анонимной и будет эмитироваться из единого центра, который можно легко контролировать. То есть от bitcoin отрежут 2 ключевых элемента. С другой стороны, создание криптовалюты подразумевает использование технологии блокчейн – на сегодняшний день это одна из самых передовых технологий, которая позволяет почти на 100% защитить транзакции внутри системы.

22 мая 2018 г. Государственной думой Российской Федерации в первом чтении был принят закон «О цифровых финансовых активах». Текст проекта опубликован на официальном сайте Министерства финансов Российской Федерации.

В статье первой проекта указано: «настоящим Федеральным законом регулируются отношения, возникающие при создании, выпуске, хранении и обращении цифровых финансовых активов, а также осуществлении прав и исполнении обязательств по смарт-контрактам».

Во второй статье сразу оговаривается, что цифровые финансовые активы не являются законными средствами платежа на территории Российской Федерации. Данный постулат сразу определяет криптовалюты и токены (а в соответствии с текстом проекта только они рассматриваются в виде

цифровых финансовых активов) как своеобразные бонусные баллы, «созданные с использованием шифровальных (криптографических) средств». При этом в статье четвертой отмечено, что операции по обмену цифровых финансовых активов на рубли, валюту или иное имущество можно совершать только через оператора обмена цифровых финансовых активов. Таким образом проект закона четко дает понять – криптовалюта и токены это не деньги.

Как представляется, основной посыл принятия данного закона заключается в нормативном закреплении на текущем этапе развития цифровой экономики нового вида имущества. Ранее в виде охраняемого законом имущества в электронном виде рассматривались только программы и базы данных. Данное имущество отличалось от иного различными формами получения контрафактных экземпляров а также легальных или нелегальных копий.

Развитие информационных технологий привело к тому, что возможно создать имущество, которое не будет (или по крайне мере не должно) иметь нелегальных копий и которое претендует на роль универсальных единиц обмена. Решение данной задачи имеет несколько возможных путей, но принятие проекта закона обозначило следующий. Де-факто существуют цифровые активы, которые, по мнению определенного количества пользователей, имеют стоимостное выражение. На текущий момент вопросы, связанные с хранением, оборотом, юридической защитой и защитой со стороны правоохранительных органов таких активов не решены. Вместе с тем, сразу обозначено ограничение обмена таких активов на фиатные деньги и иное имущество – только через оператора обмена цифровых финансовых активов.

Необходимо отметить еще одно существенное обстоятельство в рассматриваемом законопроекте. В нем оговорено, что «операторами обмена цифровых финансовых активов могут быть только юридические лица, которые созданы в соответствии с законодательством Российской Федерации и осуществляют виды деятельности, указанные в статьях 3 – 5 Федерального закона от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг», или юридические лица, являющиеся организаторами торговли в соответствии с Федеральным законом от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах». Помимо операторов, выделяется роль валидатора. При этом «валидация цифровой записи – *юридически значимое* [курсив наш] действие по подтверждению действительности цифровых записей в реестре цифровых

транзакций, осуществляемое в порядке, установленном правилами ведения реестра цифровых транзакций».

Окончательно позицию государственных органов обозначает вводимое требование по идентификации владельца цифрового кошелька в соответствии с Федеральным законом от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

Вышеописанные требования, с одной стороны, позволяют «вписать» цифровые финансовые активы в существующую нормативную базу и избежать возможных проблем в правоприменительной практике. С другой стороны, данный проект практически выхолащивает идеи шифропанков по созданию распределенного механизма взаимного доверия при обмене активами. Так, например, сейчас участвовать в майнинге может любое физическое или юридическое лицо, обладающее свободными вычислительными мощностями, которые оно считает целесообразным использовать для данного вида деятельности. Если проект примет силу закона, то майнить криптовалюту теоретически сможет любое лицо, но получать вознаграждение от майнинга – только зарегистрированное.

Как следствие, эмитент токенов должен будет обеспечить еще и выполнение требований Федерального закона от 27.07.2006 «О персональных данных». Поэтому, система, учитывающая пользователей, должна будет соответствовать требования приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

В этой связи необходимо отметить, что в Российской Федерации уже вступил в силу закон т.н. «пакета Яровой» (Федеральный закон от 06.07.2016 № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»). В соответствии с данным законом распространители информации в сети Интернет обязаны, если говорить упрощенно, передавать в компетентные органы ключи шифрования для передаваемых данных. Не исключено, что к передаваемым данным могут относиться как цифровые финансовые активы, так и сведения об операциях с ними.

Также необходимо упомянуть Положение о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя, утвержденным постановлением Правительства Российской Федерации от 16 апреля 2012 г. № 313. Из него следует, что при определенных технических условиях, компания, осуществляющая разработку платформы для криптовалюты, должна иметь соответствующую лицензию, предусмотренную указанным постановлением.

ЗАКЛЮЧЕНИЕ

В современном мире, хозяйственная деятельность, основанная на цифровых технологиях, представляется естественной и отвечающей потребностям времени. Появляются различные концепции, дискуссии и идеи внедрения цифровой экономики. Вместе с этим, уникальность объектов цифровой экономики обуславливает необходимость выбора адекватных им технологических , экономических и правовых средств.

Новая цифровая парадигма развития общества требует от учёных и специалистов новых идей и высоких обобщений теоретического и практического характера, основанных на объединении исследований и выводов из разных областей научных знаний. Вектором и источником формирования новых знаний для обустройства информационных реалий могут стать исследования на междисциплинарном уровне.

Синтез экономических, технических, правовых и других наук может стать драйвером развития цифровой экономики в Российской Федерации и гарантом обеспечения комплексной безопасности использования новых

цифровых технологий в ведущих отраслях национального хозяйства и в том числе – топливно-энергетическом комплексе.

НОРМАТИВНЫЕ ДОКУМЕНТЫ

1. Стратегия национальной безопасности Российской Федерации. Утв. Указом Президента Российской Федерации от 31 декабря 2015 г. №683 [Электронный ресурс].- Официальный сайт Президента России. Режим доступа: http://static.kremlin.ru/media/events/files/ru/ l8iXkR8XLAtxeil X7JK3XXy6Y0AsHD5v.pdf (дата обращения: 06.01.2018)

2. Энергетическая стратегия Российской Федерации на период до 2030 года Утв. Распоряжением Правительства Российской Федерации от 13 ноября 2009 г. № 1715-р [Электронный ресурс].- Официальный сайт Министерства энергетики РФ. Режим доступа: https://minenergo.gov.ru/node/1026 (дата обращения: 10.01.2018)

3. Федеральный закон от 21.07.2011 г. № 256-ФЗ "О безопасности объектов топливно-энергетического комплекса [Электронный ресурс].- Гарант. Режим доступа: https://base.garant.ru/12188188/ (дата обращения: 11.01.2018)

4. Приказ Министерства энергетики РФ от 13 декабря 2011 г. № 587 "Об утверждении перечня работ, непосредственно связанных с обеспечением безопасности объектов топливно-энергетического комплекса" [Электронный ресурс].- Гарант. Режим доступа: https://base.garant.ru/70132916/ (дата обращения: 11.01.2018)

5. Постановление Правительства Российской Федерации от 5 мая 2012 г. № 458 «Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса» [Электронный ресурс].- Техническая библиотека GIS Profi. Режим доступа: https://gisprofi.com/gd/documents/postanovlenie-pravitelstva-rf-ot-05-05-2012-№-458-ob-utverzhdenii-pravil.html (дата обращения: 15.01.2018)

6. Постановление Правительства Российской Федерации от 5 мая 2012 г. № 458 «Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса» [Электронный ресурс].- Консультант плюс. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_150730/ (дата обращения: 15.01.2018)

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Алексеенко О.А., Ильин И.В. Цифровизация глобального мира и роль государства в цифровой экономике // Информационное общество. – 2018. – п2. – с. 25-28.

2. Бестужева О.Ю., Вершинская О.Н. Некоторые особенности развития цифровой экономики // Энергетическая политика. – 2017. – N5. – С. 49-57.

3. Бачило И.Л. Цифровизация управления и экономики – задача общегосударственная // Государство и право. – 2018. – N2. – С. 59-69.

4. Гриняев С.Н., Фомин А.Н. Мировая экономика. Реальность или фикция? М.: ФИВ, 2008. 112 с.

5. Гриняев С.Н. Мир 2013: оценки, факты, комментарии. М.:АНО ЦСОиП, 2014. 328 с.

6. Гриняев С.Н., Правиков Д.И. Основы общей теории киберпространства. Теория боя в киберпространстве / Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина. - М.: АНО ЦСОиП, 2018. 124 с.

7. Гриняев С.Н., Правиков Д.И., Щербаков А.Ю., Фомин А.Н. Основы общей теории киберпространства. Электронные финансы и новая экономика / Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина. – М.: АНО ЦСОиП, 2019. – 140 с.

8. Джанджугазова Е.А. Инновационная экономика как пространство для развития новых идей // Российские регионы: взгляд в будущее. – М.,2016.- N4.- С.1-10.

9. Завальный П.И. Что такое цифровизация российской энергетики // Независимая газета. – 2018. – 13 ноября. – С. 9, 10.

10. Костикова Е.Г. Правовое регулирование безопасности в сфере финансов: новые подходы в условиях перехода к цифровой экономике // Финансовое право. – 2018. – N7. – С. 7-11.

11. Латышева А.Н. Это не просто бизнес: социальная составляющая российского краудфандинга // Журнал исследований социальной политики. М., 2017.-N4.- С.660-668.

12. Легкодымов А. Биткойн изнутри для непонимающих // Хабра-хабр. 2011 // habrahabr.ru/post/125572/.

13. Лопатин В.Н. Риски информационной безопасности при переходе к цифровой экономике// Государство и право. – 2018. – N3. – С. 77.

14. Лю Хуацинь. Китайско-российское торгово-экономическое сотрудничество вступает в новую эпоху // Китай.- 2018.- N4.- URL : https://www/pressreader.сщь/china-russian/20180408/281496456896894.

15. Пискунов А.И., Глезман Л.В. Развитие промышленных предприятий в условиях становления цифровой экономики // Креативная экономика. – 2019. – Том 13. – N3. – doi : 10.18334/ce. 13.3.40085.

16. Послание Президента РФ Федеральному собранию РФ от 01.03.2018 г. – URL : http : // kremlin. ru/events/president/nevs/56957.

17. Правиков Д.И., Щербаков А.Ю. Изменение парадигмы информационной безопасности // Системы высокой доступности. 2018. 2, с. 35–39.

18. Правиков Д.И., Щербаков А.Ю. Применение технологии блокчейна и криптовалюты для обеспечения работ по государственному оборонному заказу // Системы высокой доступности. 2017. 4, с. 25–30.

19. Расторгуев С.П. Математические модели в информационном противоборстве (экзистенциальная математика). – М.: АНО ЦСОиП, 2014.

20. Спицына Т.А. Безопасность объектов топливно-энергетического комплекса в системе национальной безопасности российской федерации // Вестник Саратовской государственной юридической академии. №6. 2017. С.150-156

21. Ткачева В.Л. Экономико-правовой анализ реализации финансово-технологической революции // Нефть, газ и бизнес. – М., 2017.- № 7. - С. 62-65.

22. Ткачева В.Л. Экономические и социальные вызовы и противоречия финансово-технологической революции // Проблемы экономики и управления нефтегазовым комплексом. – М., 2018. – N3. – С.20-22.

23. Ткачева В.Л. Стратегические и тактические приоритеты для безопасного функционирования передовых секторов топливно-энергетического

комплекса России // Проблемы экономики и управления нефтегазовым комплексом. –М., 2018. – N10. – С.7-13.

24. Фатьянов А.А. Правовое регулирование электронного документооборота: http://www.rg/2005/11/09/ bibliotechka – sbornik.html.

25. Фатьянов А.А. Правовой анализ категории «электронные денежные средства» в российском законодательстве // Государство и право. – 2014. – N10. – С. 114-116.

26. Фомин А.Н. Электронная валюта bitcoin: особенности, свойства, проблемы, перспективы: аналитический доклад. М.: Центр стратегических оценок и прогнозов, 2013.

27. Майним Bitcoin с помощью бумаги и ручки // Хабрахабр. 2014 // habrahabr.ru/post/258181/.

28. Часто задаваемые вопросы о Bitcoin // Русскоязычный информационный сайт о криптовалюте Bitcoin — Bits Media // bits.media/faq/.

29. Как устроен биткойн? Bitcoin Evolution.com, 2016 // bitcoinevolution.com/bitcoin-inside/.

30. Поппер Н. Цифровое золото. Невероятная история биткойна, или Как идеалисты и бизнесмены изобретают деньги заново» / Перев. с англ., под редакцией Слепцова А.В. - М: И.Д. Вильямс, 2016 // yadi.sk/i/OZXcqiGz3KQByi.

31. Масляев А. Альтернативы блокчейну для ведения защищенных реестров // Хабрахабр. 2017 // habrahabr.ru/post/331706/.

32. Кодачигов В., Кантышев П., Оверченко М. Из магазинов Москвы пропали компьютерные видеокарты // Ведомости. 20.06.2017 // www.comnews.ru/node/107368#ixzz4lBYCwH3M.

33. Исламский динар: боевики ИГИЛ начали выпуск собственной золотой валюты // Вести.RU. 24.06.2015.

34. Австралиец Крейг Райт назвал себя создателем биткойнов // Русская служба «Би-Би-Си». 02.05.2016 // news.mail.ru/society/25653737/?frommail=10.

35. Ратников А., Шароян С. 4000% годовых: сколько в России зарабатывают на биткойнах // РБК. 10.10.2014 // www.rbc.ru/finances/10/10/2014/5436b0f8cbb20f504085abcb.

36. Коломыченко М. Qiwi имитирует рубли // Новости@mail.ru. 6.09.2015 // news.mail.ru/economics/23316447/?frommail=1.139

37. Biktimirov M.R., Shcherbakov A.Yu. Cybernetics of megasystems as development of the subject area of effective and trusted systems, Quality // Innovations. Education. 2014. №. 12, 10–14.

38. Biktimirov M.R., Elizarov A.M., Shcherbakov A.Yu. Trends in the development of technologies for processing DigDatatools for storing multi-format data and analytics // Russian Digital Libraries Journal. Vol. 19. 2016. № 52, 390–411.

39. Zaitsev V., Gostev S.S., Cherkashin P.A., Shcherbakov A.Yu. Regarding the Technology of Distributed Storage of Confidential Information in

40. Centers of General-Purpose Data Processing // Automatic Documentation and Mathematical Linguistics. Vol. 51. 2014. № 3. P. 117–119.

41. Biktimirov M.R., Efremov P.V., Polikarpov S.A., Solodkin D.L., Shcherbakov A.Yu. The development of a system for the collection and use of scientific and technological results // Scientific and information proceeding. Vol. 41. 2014. P. 178–182.

42. Shcherbakov A.Yu. About development tools for creation corporative distributed ledger (blockchain) // Automatic Documentation and Mathematical Linguistics. 2018. 4, 30–34.

43. Дымова К. А. Особенности отраслевого регулирования условий труда работников топливно-энергетического комплекса: правовой аспект. Диссертация на соискание ученой степени кандидата юридических наук. МГЮА, - 2016.

44. Ничиков А.В. Перечень угроз: от общего к частному // Системы безопасности. – № 2, 2008. – стр. 230-235.