Вячеслав Волошин

Кибернетическая безопасность

Социальные и прикладные вопросы

Освита Украины
2020

«*Only amateurs attacks machines;*

professionals target people»

Bruce Schneier.

Вячеслав Волошин

Кибернетическая безопасность

Социальные и прикладные вопросы

Освита Украины
2020

УДК 004.056
В 686

Рекомендовано Ученым советом ГВУЗ
«Приазовский государственный технический университет»
(протокол № 6 от 24.12.2020)

Рецензенты:
Холькин А. М., профессор, доктор физико-математических наук (Мариуполь, ПГТУ).
Коваленко Г. Д., профессор, доктор физико-математических наук (Харьков, ХФТИ).
Рачев З., профессор, доктор *PhD* (София, Болгария, ХТМУ).

В 686 Волошин В. С. Кибернетическая безопасность. Социальные и прикладные вопросы – К. : ИД «Освита Украины», 2020. – 300 стр., 20 рис., 13 табл., 192 библ. назв.
ISBN 978-617-7993-02-4

Настоящая книга является одним из немногих источников, в котором изложено несколько иное видение актуальной области знаний, которая носит название кибернетическая безопасность. Автор, специалист по безопасности технических систем, на основании многочисленных собственных исследований и исследований других авторов сделал попытку некоторого переосмысления этой важной современной области знаний, приблизив ее к пользователю, к человеку, как потребителю огромного многообразия информационной продукции, что является естественным для любых человеко-машинных систем, которые составляют естественную природу любого инженерного прогресса, в том числе, в современных *IT*. Не умаляя огромных достижений в областях защиты программного компьютерного продукта, безопасности современных баз данных, защиты персональных данных в современном интернет-пространстве, сделана попытка расширить область притязаний этой науки за счет исследования других аспектов безопасности человека, как участника глобального информационного пространства, что может обогатить эту науку новыми системными результатами.

Книга рассчитана на специалистов в области кибербезопасности, научных работников и аспирантов в областях социальных наук, экономики, безопасности труда, может быть полезна студентам и школьникам старших классов, интересующимся современными подходами в различных областях информационных наук.

ISBN 978-617-7993-02-4
УДК 004.056

АВТОР

Волошин Вячеслав Степанович – доктор технических наук, профессор, заслуженный деятель науки и техники Украины, Почетный действительный член академии экономических наук, Международной кадровой академии, действительный член Нью-Йоркской академии наук, Почетный профессор Венского университета экономики, ректор Приазовского государственного технического университета. Область научных интересов – безопасность и аварийная диагностика технических систем, теория рисков, социальная экономика и экология урбосистем, поведение с промышленными отходами, водные экосистемы. Автор и соавтор двадцати одной монографии и учебников по направлениям научной деятельности.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Предшественницей области знаний, которую теперь называют кибернетической безопасностью, является безопасность информационная, которая сформировалась во второй половине XX века как совокупность знаний о защите и сохранении информации предприятий, компаний, банков, государственного сектора от использования в преступных или конкурентных целях. Она требовала приведения сотрудников, людей к единой дисциплине по отношению к конфиденциальной информации, избирательности и минимизации внешнего доступа к этой информации, контроля за соблюдением таких требований. Информационная безопасность, от локального способа защиты постепенно, с развитием коммуникативности в обществе, переходит в более конкретную область защиты программного продукта и информации от внешнего воздействия. Предполагается защита как от людей, например, хакеров, от вирусов, так и защита самих людей от влияния искаженной информации, поступающей от программ, попавших под вирусные атаки, от ее использования не по прямому назначению и др.

На определенном этапе развития информационной безопасности появляется потребность в кибернетической безопасности, с привлечением узких *IT*-специалистов, с целью защиты развивающегося информационного пространства и его составляющих от внешнего программно-технического воздействия, от деформации этого пространства. Это уже не просто защита информации, а защита всей системы формирования, восприятия, передачи, хранения информации вместе с ее носителями и другим техническим обеспечением, включая пользователей этой системы.

Кибернетическая безопасность, и как термин, и как наука, вошла в жизнь не только ученого мира, но и большинства жителей планеты одновременно с понятием глобального

информационного пространства и, самое главное, факта участия большей части (96 %) человечества в этом пространстве. Нечасто бывает так, что сразу же после рождения область научных и прикладных знаний становится актуальной для большей части общества, причем потребность в ней постоянно растет в той же пропорции, в которой растет цифровизация современного нам мира. В равной мере с необратимостью этих процессов, появилось понятие необратимости знаний в области кибернетической безопасности, сфера интересов которой постоянно расширяется, включая смежные области знаний – экономику, финансы, право, инженерию, искусство, психологию, медицину и многое другое. Трудно будет удивиться, если с течением времени в этой науке появятся совершенно не связанные пока с ней области знаний и деятельности, потому что цифровизация мира уже сегодня представляется как неизбежность, как необратимая данность современной эпохи развития. Этому имеются многие эмпирические доказательства.

Распознавание образов всегда было основным качеством человека, связывающим его с реальной действительностью и позволяющим не только узнавать мир, но изучать его, делать понятным для существования в нем.

То, что сегодня называется модным словом «диджитализация» или «цифровизация», «*dg*-», преследует наше общество уже на протяжении почти века. Дэвид Брукс в 2013 году даже придумал соответствующую религию – датаизм, в которой информационный поток, как конструкция Вселенной, представляется высшей ценностью для человека, чтобы лишний раз подчеркнуть значимость информации в современном обществе. Но эта оригинальность не отвечает на основные вопросы, касающиеся влияния глобального информационного пространства на человека, в частности, зачем это нужно человеку.

В середине XX века научная общественность была счастлива, когда с появлением первых электронных вычислительных машин (ЭВМ) можно было «оцифровать» и зашифровать арабские цифры при помощи двоичных кодов и задать их в виде некоторых сигналов, которые легко узнавались и моделировались различными приборами однонаправленного действия: аналоговыми гидравлическими и пневматическими логическими клапанами и дросселями, электронными двух-, трехэлектродными лампами, полупроводниковыми диодами, триодами, триггерами и др., давая возможность преобразовывать в электрические сигналы те же самые арабские цифры. Скорость вычислений двоичных сигналов, как электрических аналогов арабских цифр, логические действия над ними, которые обеспечивала булева алгебра, позволяли выполнять относительно несложные математические расчеты со скоростью сотен и тысяч операций в секунду. Это был прорыв в цифровизации, в развитии математического счета. Такой, что мы даже не заметили, как с появлением первых персональных компьютеров произошла цифровизация двоичными кодами лингвистических символов и букв любого алфавита. Постепенно мы превратили в «цифру» любую геометрическую фигуру, а затем плавно перешли к оцифровыванию фигур произвольной формы, сложности и цвета, получив, таким образом, возможность превращать в «цифру» любой визуальный образ или фотографию. Скорости обработки такой информации постоянно росли, и мы уже не удивлялись появлению цифровых фотоаппаратов, камер, межкомпьютерных сетей, интернета, оцифрованных, опять-таки, двоичным кодом книг и журналов, и, в конечном счете, оцифрованного глобального информационного пространства, как объекта не только хранения и передачи оцифрованной документальной информации, но и оцифрованной человеческой речи и сложного фигурного образа. Мы стали свидетелями и участниками тотального вхождения в мир цифровых

сигналов, которые сегодня могут становиться аналогами не только арабской цифре или букве алфавита, но и при помощи «интернета вещей» и смарт-чипов в блокчейн технологиях – аналогом любого документа, любого материального предмета, отражая его физические и другие свойства.

Без сомнения, это цифровая революция. По своему влиянию на человека она равнозначна многим другим революциям: когнитивной (начало – около 70 тыс. лет назад), аграрной (начало – около 12 тыс. лет назад), научной (500 лет назад). Причем эта революция еще не окончена, и сроков ее стабилизации не видится в обозримом будущем. По форме воздействия на человека этот процесс имел аналоги в прошлом. Они связаны с «маркировкой» информации, как в прошлом, так и в настоящем, и в будущем. Как и прежде, подобная революция требует от человека приобретения новых социальных свойств, без которых она не состоится или войдет в конфликт с обществом.

Примерно 70 тысяч лет назад стала зарождаться первоначальная человеческая культура, в основании которой было распознавание мира, его образов, явлений природы, причем, все это имело сугубо утилитарную цель: приспособить человека к этим природным явлениям. А затем – приспособить природные явления под человека, пока эта культура не стала частью жизни любого человека. И продолжается сейчас.

История позволяет нам судить о том, что подобные отображения революций в области познания были характерны и для других периодов жизни человека.

Это были последовательные способы социального активирования – вначале процессов: созерцания, размышления, сравнивания, общения, а затем действий: собирательства, охоты, земледелия, выращивания животных, производства, торговли, исследования.

Базовым в распознавании мира была «маркировка» его предметной основы в соответствии с представлениями, кото-

рые давали человеку его органы чувств, прежде всего, зрение, слух, осязание, обоняние, языковая семантика. Человек не просто распознавал мир. Он его «метил» названиями рек, гор, долин, деревьев, животных и т. д. Эта серьезная информационная деятельность приносила свои плоды, делая мир рельефным, узнаваемым для человека при помощи эмпирических форм «маркировки», языковых знаний, при помощи таких инструментов, как гортань, легкие, звукоизображение, при помощи такого «программного продукта», как семантическое присвоение и удержание информации в памяти человека. Подобная «информационная революция» длилась тысячелетиями.

Следует отметить в сравнении, что прачеловек был более приспособлен к природе потому, что его естественная «маркировка» предметов, основанная на эмпирических природных механизмах обратной связи, которые давали ему зрение, слух и т. д., предоставляли ему больше конкретной информации о возможностях природы удовлетворять его инстинкты и требования, чем это имеется даже сейчас, в век научного прогресса. Человек был ближе к естественной природе, чем сейчас. Тем не менее, цифровая аналогия предметного мира, являющаяся новой ступенью в познании мира, станет важнейшим этапом в понимании процессов развития самого человечества.

Вместе с новым способом визуализации предметного мира и формированием современного глобального информационного пространства, мы получили и определенный порядок вещей, до сих пор не существовавший, в частности, проблемы экономического, политического, социального порядка. Они существуют, но прогресс не отменить, и поэтому эти проблемы подлежат своему разрешению.

Следует понимать, что именно формирование глобального информационного пространства стало одной из важнейших причин появления в законодательствах многих стран

законов, защищающих персональные данные своих граждан. Пока эти законы, как правило, малоэффективны. По причине молодости и бурного развития платформ для размещения таких данных в информационном пространстве, которое, по сути, является централизованным, дающим возможности не только для накопления индивидуальных данных о многих жителях многих стран в таких «накопителях», как *Facebook* (1,5 млрд пользователей), *Twitter* (1,3 млрд), *Instagram* (1 млрд), *YouTube* (1 млрд) и др., но и для использования в некорректных целях. Концентрация персональных данных, включающих, кроме паспортных данных, особенности профессиональной деятельности индивида, его психофизические портреты, медицинские данные, круг знакомств, специфику характера, связи и многое другое, что, при умелом использовании, может быть использовано против этого индивида, представляет для него существенную опасность. Мы уже понимаем, что за бесплатное участие в различных социальных сетях, конференциях, презентациях мы расплачиваемся именно своими персональными данными в виде огромной базы для тех людей, которые составляют абсолютную часть человечества. Эти данные являются важным коммерческим капиталом для их централизованного держателя и могут быть проданы, переданы, заимствованы для любых целей и для любого пользователя, в том числе, и для преступных целей.

Вместе с появлением таких баз данных, а также с тем, что цифровизация материального мира, в первую очередь, коснулась финансовых сфер, появился новый специфический вид преступности – кибернетическая преступность. Следом за ней появилась защитная функция общества против такого криминала – кибернетическая безопасность. В государственных структурах служб безопасности, внутренних дел, органов надзора стали появляться соответствующие подразделения по борьбе с этим явлением. Основным ориентиром, в

этом случае, для кибернетической безопасности стала безопасность программного и компьютерного оборудования, защита против хакерских атак, взломов программного продукта, несанкционированная интеграция в социальные сети, нарушение целостности и правильности их работы. Примеров борьбы органов кибербезопасности с правонарушениями, которые уже принимают системный характер, огромное количество. Ими заполнен интернет, бумажные и электронные средства массовой информации. Кибербезопасность превратилась в отдельную отрасль науки и образования, которая развивается с переменным успехом, потому что все, что создается в области хакерства, тут же находит отражение в средствах защиты, и наоборот, любое новое средство защиты от взломов, хакерских атак и наказания за эти действия, постепенно преодолевается новыми преступными средствами. При этом совершенствуется действующее законодательство.

К сожалению, сформировавшаяся область знаний – кибернетическая безопасность, пока весьма равнодушна к основному объекту безопасности, человеку. И отдельные компьютеры, и компьютерные сети, и интернет, и облачные технологии вкупе с блокчейн технологиями не могут существовать без участия в них человека. По существу, это обычные, давно изученные системы типа «человек-машина» или человеко-машинные системы. Рассматривая безопасность таких систем в классическом понимании, мы должны в равной степени обеспечивать и безопасность машины от поломок, и их защиту от субъективности самого человека, и защиту человека от аварий, травм, в том числе, психологических, юридических, экономических. Последнему кибернетическая безопасность, как область знаний, почти не уделяет внимания, концентрируя внимание на защите от преступлений хакеров, взломщиков программных продуктов, похитителей оцифрованных финансовых и других материальных ценностей.

Мы хотим показать, что сегодня этого уже недостаточно. Глобальное информационное пространство стало неотъемлемой частью современного мира. Каждую секунду на планете 12 человек становятся жертвами киберпреступлений. В конечном результате страдают от кибернетических преступлений именно люди. Это требует защиты человека, его прав, здоровья и жизни, в особенности, в современный нам переходный период. Он характерен тем, что мы имеем дело пока с весьма специфической продукцией, в определенной мере полуфабрикатного свойства, имеющей свои изъяны, недостатки разработчиков, приводящие не только к потерям денег, активов, но и к психологическим, физическим потерям для пользователей, количество которых постоянно растет, в сопоставимом размере ко всему населению планеты. Это вопросы, при всей актуальности работ в области безопасности собственно глобального информационного пространства вместе с его машинным и программным обеспечением, должны подниматься, иметь свои эффективные способы решения в системном изложении с другими вопросами современной кибернетической безопасности.

I

Предмет исследования

Когда появляется новая область знаний, к ней приковано внимание науки, в особенности смежных направлений.

Постепенно новая область знаний сама формируется в новое научное направление, со временем становясь полноценной частью мировой науки.

Кибернетическая безопасность формировалась как область знаний о защите, прежде всего, компьютеров от искусственных программ-вирусов, которые блокировали работу компьютерного оборудования, препятствовали решению определенных технических и расчетных задач, для которых была предназначена эта техника и ее программное обеспечение. Постепенно, с появлением сетевых ресурсов, развития компьютерных коммуникаций кибербезопаснсть приняла на себя роль защиты от хакерских проникновений (*hacker* – взломщик), намеренных взломов систем компьютерной безопасности, которые не только препятствовали работе компьютеров, но и влияли на коммуникации, вмешивались в компьютерное обеспечение работы предприятий, банков, учреждений, даже государственных и военных институций. Постепенно, защита от проникновения в сети стала превращаться в экономическую, а со временем и в социальную проблему. В ней, кроме компьютера, его софта стал появляться еще один объект воздействия – человек. Общество стало нести потери в областях, связанных не только с чисто компьютерным оборудованием, но и в смежных областях.

С появлением понятия глобального информационного пространства (ГИП) появилось и понятие всеобъемлющей опасности и нового способа преступлений, и нового способа

жизни, нового подхода к образованию, ко многим областям жизни, которые в их традиционном понимании были совершенно изменены. С приходом ГИП человек получил новое понимание собственного эго, которое теперь неразрывно связано с информацией, с оцифрованием всего и всякого, и возможностями для сопоставления ранее несопоставимых вещей, предметов, понятий, всего, что составляет сегодня искусственную окружающую среду для этого современного человека.

1.1 Понятие глобального информационного пространства, его свойства, признаки и качества

Современный мир тонет в океане информации. Это уже не аллегория. Это действительность. Потому, что в этой фразе есть предмет, есть реальное действие, есть полученный результат. Сегодня оцифровано или находится в процессе оцифровывания почти все, с чем связан человек: мысли, выражения, предметы искусства, старинные рукописи и современные книги, знания и деньги, чертежи и технологии, договоры и нотариальные акты, другие материальные предметы. Оцифровывается ложь, обман, хитрость, даже преступления. Для этого создан интернет, социальные сети, облачные технологии, блокчейн технологии, смарт-чипы и многое другое, что позволяет эту информацию систематизировать, делать доступной, пользоваться ей так, как это только возможно. Создано глобальное информационное пространство (ГИП), в котором человек, как социальное звено, является организованной частицей, источником информации, ее транспортером, потребителем, критиком и убийцей в одном лице.

Следует отметить, что истории известны факты, когда глобальные (даже конструктивные) процессы приводили к

глобальным, не только позитивным, но и внесистемным отрицательным результатам. Самым типичным примером могут являться крупные, например, мировые войны.

Историки причисляют к таковым, в частности, монгольские войны XIII–XIV веков, которые по своим масштабам завоеваний и освоения территорий до сих пор являются непревзойденными. Даже наполеоновские войны XIX века или македонские завоевания, даже две мировые войны XX века, по масштабам не могут сравниться с монгольскими войнами в пропорциональной глобальности. В частности, монгольские войны приносили людям не только гибель и оккупацию территорий более, чем 30 современных государств общей площадью примерно 12 млн км^2 и с современным населением в 3 млрд человек [1]. Такие качества, как веротерпимость, стремление заработать не только на дани, но и на развитии торговли, открытие совершенно новых торговых путей между огромными регионами мира: Азией, Европой, Ближним и Средним Востоком, Северной Африкой, способствовали развитию глобалистических процессов уже в средние века. Чем это не пример глобальной коммуникативности, развития глобальных информационных потоков?

Через территории монгольских улусов и их вассальных государств старыми традиционными и новыми торговыми путями с достаточно высокой для того времени скоростью перемещалось в год более 20 млн тонн самых различных грузов. Впечатляет их номенклатура, число наименований, превышающее 60 тысяч. Каждый вид товара имел собственные данные:

– название товара;

– цена товара, суммарные денежные цифры от торговли этим товаром, налоги, взятки и подношения;

– количество и показатели качества товара;

– принадлежность товара;

– источник изготовления;

– пункт назначения и др.

По самым общим оценочным подсчетам для товаров из 60 тыс. наименований, общей массой в 20 млн тонн суммарный объем информации, которая за год кочевала по империи могла достигать $(16 \div 58) \cdot 10^3$ ГБ в год. Мы имеем дело с очень высоким по мощности, и не очень плотным информационным потоком глобального значения для средних веков. Следует признать, что этот глобальный информационный поток был неосознанным, малоуправляемым, в некоторой степени, стихийным, формировался в основном как спонтанный. Но он был...

Мы отдаем себе отчет в том, что глобальные войны имели свои собственные информационные потоки, и XX век был далеко не исключением. Это информация об объемах и качестве вооружений, своих и противников, о тактических планах, многочисленных стратегических операциях и др. Эти потоки максимально уплотнялись, их объемы росли лавинообразно.

Вторая мировая война и предшествовавшие ей глобальные мировые экономические кризисы, социальные и политические катастрофы первой половины XX века сразу во многих странах Европы, Северной и Южной Америк, Дальнем и Ближнем Востоке привели к появлению запредельного по критичности «спускового крючка» в виде ядерного оружия. Глобальное ядерное военное противостояние стало основанием для появления новой глобальной мировой политики, политической биполярности, холодной войны, зарождающегося глобального терроризма, как альтернативы системе «спускового крючка».

Вывод, который следует из этих рассуждений, может быть очень простым. Глобальные процессы в краткосрочных целях и в ближних перспективах приводят к некоторым позитивным результатам. Но исторический опыт подсказывает, что отдаленные негативные последствия таких процессов существуют, они слабо прогнозируемы, и по результатам мо-

гут быть самыми непредсказуемыми. Такой исторический экскурс весьма интересен. Он может давать некоторое понимание методов, по которым развиваются глобальные процессы в нашем обществе, и, в первом приближении, подсказывать пути, по которым происходят негативные последствия, включая вопросы безопасности человека и общества. Но то, что они сопровождают глобалистику и несут в себе определенные опасности, сомнений пока нет.

Глобальное информационное пространство – это всемирно признанный термин, определяющий состояния современного, практически равноправного и доступного, информационного обеспечения для всего человечества. Понятие ГИП тесно связано с интернетом, который и является основой для такого обеспечения.

Перечислим некоторые общепризнанные признаки интернета.

Интернет – это сложная саморазвивающаяся система типа «человек-машина», состоящая из взаимосвязанных многофункциональных компьютерных сетевых подсистем и их элементов для хранения, обработки и передачи информации на основе стека протоколов типа *TCP*/*IP*, замкнутых при помощи систем обратных связей на человека, пользователя этих систем. В литературе можно встретить легко узнаваемые термины: Всемирная сеть, Глобальная сеть.

Интернет структурно включает: технические, программные, информационные, энергетические ресурсы, компьютерные технологии, операторов и пользователей сети. Следует подчеркнуть, что интернет может существовать только в том случае, если в нем присутствует человек.

Несколько специфично понятие «машины» в этой системе. Обычно под этой частью человеко-машинной системы понимается некоторое техническое сооружение, техническая система. В интернете под «машиной» следует понимать не

только *Hard*, но и всю совокупность информации, которой насыщена среда интернет.

Для интернета существует собственная среда, которую своеобразно называют киберпространством. Подчеркивая мировое значение, для этого пространства придуман термин глобальное информационное пространство или ГИП. Пользователи интернета также располагаются в нем. Часть этого пространства иногда называют виртуальным из-за активного оперирования в нем не самими вещами, а их компьютерными образами, которые в воображении пользователя наделяются теми же качествами, что и реальные прототипы.

Главные цели интернета заключаются в обеспечении коммуникаций для пользователя, создания для него объемного информационного поля, сокращении временных затрат на его обслуживание, обеспечении упрощенного доступа к информации и к другим пользователям.

Субъекты интернета: пользователи, операторы и посредники, это вторая часть системы «человек-машина» применительно к интернету. Но все они, так или иначе, относятся к категории пользователей. Уточняются только их индивидуальные функции. Ни операторы, ни посредники не смогут выполнять свои системные (в отличие от простых пользователей) функции, если они не зарегистрируются в качестве пользователей сети интернет.

Операторы создают и управляют техническим, программным и фактологическим обеспечением работы интернета. Операторы наполняют интернет содержательной частью, для ее распространения среди пользователей. Отдельно следует различать операторов сети интернет. Их задача – довести разработанный контент до пользователя, правильно ориентировать его в объемах этого контента.

Пользователи принимают участие в развитии сети интернет, являются неотъемлемой составляющей сети в качестве ячеек для коммуникаций. Пользователи используют ре-

сурсы интернета для решения своих индивидуальных и коллективных задач. Посредники – это специалисты по оказанию услуг в сети по оптимальной работе, поиску нужной информации. Посредник – это такой же пользователь, только системный.

Основным системным качеством интернета является расширение возможностей для проявления творчества человека. Развитие сети интернет осуществляется по принципу равного доступа всех участников к созданным достояниям в области информации. При этом, если контент не эффективен, он просто не используется, по-своему загрязняя среду интернета.

Пользователи могут создавать объединения или комитеты по конкретным вопросам, приглашая других пользователей войти в их состав или пользоваться их продукцией. Одной из таких организаций является общественный *Internet Society* (*ISOC*) [2]. Работу по общественному регулированию киберпространства пытаются взять на себя ряд таких же общественных организаций пользователей, как технические комитеты и комиссии *ISOC*: *IETF* (*Internet Engineering Task Force*), *IAB* (*Internet Architecture Board*), *IRTF* (*Internet Research Task Force*), *IANA* (*Internet Assigned Numbers Authority*), *CERT* (*Internet Computer Emergency Responce Team*), *RIPE* (*Reseaux IP Europeens*), *InterNIC*, информационный центр *MERIT* и другие [3].

Глобальное информационное пространство имеет свое узнаваемое лицо, качества, свойства, обладает собственными правами и обязанностями по отношению к обществу, к себе, к окружающей природной среде. Оно реально и неуловимо, систематизировано и бессистемно, размеры его поражают, несмотря на то, что оно создано человеком. Мы учимся его применять. Мы учимся защищаться от него. Мы создаем целые области новых наук – информационную логику, массовые коммуникации, криптографию, кибернетическую безо-

пасность и др. Для современного общества ГИП, наравне с материальными, трудовыми и энергетическими ресурсами, выступает в качестве важнейшего ресурса социально-экономического развития. Совершается методологическое оформление концепции нового общества на основе глобальной информатизации всех сторон его существования.

Можно сказать, что после изобретения музыки, глобальное информационное пространство стало вторым порождением человека, таким, которого не знала Природа. Это ГИП. Искусственное образование, которому суждено перевернуть этот мир. И от человека зависит – этот переворот будет системным, направленным на созидание, или он подомнет под себя всю планету, превратив ее в безжизненную пустыню, потому что по силе воздействия на все, что имеется на планете, ГИП можно смело сравнивать с совокупным ядерным потенциалом всех государств мира. Это не преувеличение. Поскольку современное общество, погрузившись в океан информации, постепенно передает в его распоряжение то, что никогда не отдавало природе: способность, вне человека, мыслить и делать выводы, способность ограничивать свои же потребности возможностями самой природы. Сегодня мы на том пути, когда глобальное информационное пространство сумеет стать на путь искусственного разума, который имеет все возможности обособиться от разума человеческого в принятии решений и, через те же материальные предметы, влиять на состояние планеты, на своего «родителя» – человека. Можно бесконечно спорить о перспективах искусственного интеллекта, роботов и их способностях к воспроизводству, но в любом случае, если не произойдет что-либо экстранеординарное, мы придем к реальности искусственного разума: либо в виде помощника и послушного проводника мыслей человека, либо в виде самостоятельного субъекта в принятии решений, которые будут влиять на все общество, сделают его независимым от воли людей.

Это может быть похожим на текст из фантастического произведения, но, по крайней мере, вектор на такое развитие человечества дает нам изучение феномена, порожденного человеком, его мыслью – глобального информационного пространства.

Постепенно становится данностью, еще несколько лет назад считавшаяся абстракцией, теория датаизма, согласно которой мир следует рассматривать не как цепочки причинно-следственных зависимостей, а как потоки данных, которые постоянно концентрируются для последующей обработки. И сущность, и ценность любого явления и любого объекта, включая биологические системы, определяется их вкладом в обработку данных. Это фактическое поклонение новому божеству, название которому «*Big Data*» и которое требует от общества расплаты в виде трех «*V*» – *volume*, *velocity*, *variety* (объемы, скорость, многообразие) [4, 6, 7]. Теория датаизма подробно описана в известной книге Юваля Ноя Харари [3], на которую теперь ссылаются все ее поклонники, хотя контент автора здесь в немалой степени критичен.

Некоторые исследователи и сторонники датаизма с нетерпением придают информации статус мировой центральной нервной системы, для которой даже человек, как и всякая другая вещь, есть не что иное как алгоритмизированный сборщик и переработчик данных, как природная составляющая глобального Интернета Всех Вещей, ради которого и устроена наша вселенная.

Мы обратим внимание только на один момент этой теории, который близок по смыслу к содержанию нашей работы. Имеется в виду системное оцифрование мира, так называемая цифровизация, появление *dg*-общества. Оно, в действительности, способно подтолкнуть нас не только к понятию алгоритмизации машинных действий, но и к алгоритмизации биологических субъектов, как равноправных «обработчиков данных» в системе «человек-машина». Отсюда со-

всем недалеко до искажений таких общепринятых понятий, как знания, постижение истины, опыт, мудрость, в пользу того, что называется искусственным интеллектом. Эта реальность, которая идет за нами по пятам. И тотальное оцифрование, алгоритмизация биологических систем, которые сами по себе, согласно тем же рассуждениям Ю. Харари, приводят к существенной централизации, в противопоставлении с традиционной системой распределенной обработки данных (блокчейн, например), дает повод считать эти действия в глобальном информационном пространстве далеко не самыми убедительными для общества, которое, по мнению идеологов датаизма, также является одной из таких «систем для обработки данных».

Не следует торопиться. Датаизм, от которого, как от любого другого знания, уже не уйдешь, имеет свои достоинства и недостатки. Но при всей своей фантастичности, он еще раз подчеркивает социальность такого явления, как глобальное информационное пространство, и его социальную роль для общества.

Итак, наш предмет изучения постепенно стал социальным явлением. ГИП незаметно перешел границы инженерного изобретения и, за счет своей глобальности, стал преимущественным фактором, оказывающим влияние на все без исключения стороны человеческой жизни. ГИП является стабилизирующим моментом в истории человечества, систематизируя накопленные знания и делая их абсолютно доступными для любого человека, позволяя рассчитывать на синергетические возможности таких знаний в большей степени, чем это было при жизни великих Архимеда, Ньютона, Резерфорда, Эйнштейна, не имевших доступа к таким массивам знаний. ГИП, при его относительно легкой управляемости и саморазвитии, представляет собой идеальный инструмент для науки, образования, бизнеса, финансовых и управленческих систем, независимо от их принадлежности и размеров.

ГИП показывает правила игры и для малых производств и компаний, и для целых государств, и даже для окружающей природной среды – океанов, лесов, ледников, пустынь, озонового слоя и иже с ними.

Но он же является явным дестабилизатором, по крайне мере, на современном этапе его развития, в мире несовершенного права, отсутствия цензуры, слабо развитой (отстающей, по меркам перспектив) инженерии, изощренной преступности, легко вписавшихся в этот феномен. ГИП пытается противопоставить себя даже тому, что до сих пор в цивилизованном мире считалось незыблемым – свободе человека, его индивидуальности, праву на собственное мышление, отделенное и сохраняемое от мышления других индивидов, от так называемого «коллективного разума». При всей формальной индивидуализации нашего общества, ГИП показывает вектор на восстановление стадных качеств человека, правда на более высокой социальной ступеньке, на очередном витке исторической спирали. Юваль Ной Харари дал бы этому феномену более характерное наименование – очередной революции, по своему влиянию на общество сходной с прошлыми революциями, давшими человеку способности мыслить, не зависеть от природы, развивать не только себя, но и подчинять себе эту же природу. Это последовательные когнитивная, аграрная, научная революции [5]. В этом ряду глобальное информационное пространство представляется как порождение таких же глобальных изменений в обществе, посредством которых оно имеет все возможности, в некотором временном интервале, превратиться в нечто, не поддающееся нынешнему разуму, ставящее человека высоко над самой Природой. Поскольку систематизированный разум является не менее ударной силой, чем огонь, земледелие, пар, углеводороды, субъективная мысль и эмпирические знания, постигаемые интуицией, опытом, экспериментом, наблюдениями за самой природой. Глобальное информационное про-

странство вводит общество в мир синергизма в большей степени, чем второе начало термодинамики, общая теория относительности и другие законы физики и химии, полученные как результат эмпиризма.

Таким образом, создав глобальное информационное пространство, человек получил не только удобный инструмент для знаний. Он получил способ воздействовать на природу, как это было и при научной революции. Человек получил способности воздействовать на равного себе, на самого себя, независимо от его же воли или желаний. Потому, справедливо говорить о том, что с появлением ГИП, интернета, технологий, подобных блокчейну, общество стоит в начале очень длинного и очень короткого пути: либо к самосовершенству, либо к саморазрушению.

Поражает неизбежность этого пути, даже его фатализм, как области знаний, которые, один раз появившись, уже не исчезнут, будучи обреченными на развитие в силу любознательности человека, помноженной на огромные возможности, которые ему же дает продукт его любознательности необычайного масштаба и культуры – глобальное информационное пространство.

Как и любое явление, ГИП имеет свое обозначение, свои качества и свойства, делающие его тем, что оно есть на самом деле. Трудно перечислить каждое из них. Именно этому, в определенной мере, посвящена эта книга.

Итак. Глобальное информационное пространство – это совокупность информационных ресурсов и информационной инфраструктуры, позволяющей на основе единых принципов и по общим правилам обеспечивать безопасное информационное взаимодействие государств, организаций и граждан при их равнодоступности к открытым информационным ресурсам, а также максимально полное удовлетворение их информационных потребностей при сохранении баланса национальных и международных интересов [8].

В произвольной форме, с учетом перспектив дальнейшего развития, глобальное информационное пространство – это все обо всем. С технических позиций, это совокупность средств и способов принятия, обработки, накопления, хранения и обмена информацией между техническими средствами и человеком. Перед нами – человеко-машинная система. Предмет ГИП – это, безусловно, цифровая информация. Субъектами ГИП являются человек и компьютер, сеть и гаджеты. Формируется и социальное обозначение ГИП. Его можно сформулировать следующим образом: совокупность знаний и информационных ресурсов, принадлежащих обществу, и, в равной мере, распределенных и доступных каждому его члену посредством цифровых технологий и электронных средств пользования. В литературе можно найти иные описания этого понятия [9, 10, 11, 12], суть которых меняется в зависимости от терминов, которыми называются те или иные характерные качества или свойства предмета описания – ГИП.

Представим некоторые основополагающие свойства глобального информационного пространства, которые помогут нам ближе подойти к сути рассматриваемого вопроса. Перечислением их является:

– масштабность явления глобального информационного пространства, отсутствие зависимости от границ и территорий;

– унифицированность всего, что является оцифрованным в ГИП;

– универсальность инструментов, обеспечивающих существование ГИП (компьютеры, гаджеты, телекоммуникационная техника, смарт-системы), обеспеченность инженерными решениями на самом высоком уровне;

– проявление универсализма для пользователя в самых различных областях человеческого существования (интернет,

информационные, объединенные сотовые и др. социальные сети различной архитектуры и топологии);

– распространение на любые области человеческой деятельности (блокчейн технологии, облачные технологии и др.);

– социальная привлекательность для человека;

– обладание потребностью для большого количества людей;

– наличие виртуального пространства, как следствие ГИП;

– способности к саморазвитию (в пределе).

Свойства и качества, которыми обладает ГИП, во многом пересекаются со свойствами интернета, потому что интернет является главным системообразующим фактором для появления ГИП. Посредством возможностей интернета происходит оцифровывание огромных объемов информации, осуществляется распределенный доступ к информационным ресурсам. Глобальный эффект этого инженерного явления связан со способностями этой всемирной паутины к социальной диффузии, то есть – всепроникновению в любые области пространства и человеческой деятельности, независимо от границ, вероисповедания, национальностей и других социальных аспектов нашего общества. Например, если к 2000 году в странах третьего мира проживало 26 % всех интернет-пользователей в мире, то сейчас их уже около 60 %: мусульман, христиан, буддистов, конфуцианцев, индусов, китайцев, арабов, мужчин, женщин, детей и стариков, с самым различным социальным статусом, доходом. Несмотря на такие социальные различия, «цифровой разрыв» в сфере интернета сократился почти на порядок [13]. К 2020 году число пользователей интернета достигло 4,39 млрд человек, или 57 % населения планеты [14].

Незаметно техногенный век на планетарном уровне превращается в век «информогенный», особым признаком

которого стала цифровая информация, постепенно унифицирующая весь вещественный мир. Современный социум уже вполне способен рассматривать формирование особой электронной социальности, в частности, становление так называемых телегородов, *dg*-таунов и *dg*-государств [15], как соизмеримости информационного пространства и территории проживания людей.

Важным объективным свойством интернета является формирование у пользователя качества интернет-зависимости (*Internet addiction disorder*, *IAD*). Это качество далеко не всегда носит негативный оттенок. При этом пользователь сталкивается с появлением виртуального пространства, термин которого впервые появился в работах ученых Массачусетского технологического института для обозначения трехмерных компьютерных моделей, еще в 70-е годы прошлого столетия.

Интернет-зависимость может принимать формы подмены в сознании пользователя реальных вещей на виртуальные (так называемое социальное явление или феномен культуры). Это способствует психологической локализации пользователя, его предпочтениям мира виртуального миру реальному и является одним из негативных форм влияния интернета на человека, в основе которого – психологическое удовольствие, реакция человеческой психики. Интернет-зависимость, или аддиктивность, при которой пользователь отдает предпочтение интернет-ресурсам перед любыми другими информационными ресурсами, носит значительно меньший характер негативности. Позитив может быть связан только с таким пользователем, который рационально использует интернет-ресурсы в составе других информационных ресурсов. Например, в Австралии впервые в мире усилиями компании *eBay* и сети супермаркетов *Myer* создан супермаркет виртуальной реальности. Для участия в покупках пользова-

телям нужно только наличие очков виртуальной реальности в 3-*D* моделях. Выбираются товары только взглядом [16].

Как порождение интернета, глобальное информационное пространство, в качестве виртуального, представляемого, отраженного в сознании человека, все чаще рассматривается некоторыми исследователями как отображение специфической социальности этого явления [17].

В интернете расстояние и границы теряют свой смысл. Отдельные области виртуального пространства объединяются в единое целое благодаря цифровым технологиям. Формируется интегрированный на информационном уровне виртуальный мир, в котором комфортно располагается все больше людей, предпочитая его реальному миру с его социальными проблемами. Он уже сейчас имеет свои закономерности и правила, своих обитателей и почитателей, свою специфическую этику и мораль. Он далеко не всегда похож на реальный мир. Это скромно называется интернет-аддикцией, навязчивым *Web*-серфингом, виртуальным коннектом, без рассмотрения этого явления, как альтернативного пространства, куда человек уходит добровольно, часто прерывая свои социальные связи и разрушая отношения из реального мира.

Виртуальный мир имеет частичное отображение реального мира в памяти компьютера, без искусственных сложностей, которые не устраивают таких потребителей в реальной жизни. Поэтому виртуальный мир всегда будет находить своих сторонников, как минимум, среди неудовлетворенных людей.

Виртуальный мир становится одним из важнейших признаков глобального информационного пространства. Он появился не на пустом месте. И до виртуального мира в головах многих людей всегда существовал мир воображения, идеализированный от реальных проблем. Это мог быть мир фольклора, сказок, литературных произведений, в частности, фантастики. Компьютер позволил себе превратить эти умо-

зрительные образы отдельных людей в систему виртуальной реальности. Это уже не сказки, не голая фантастика. Это образные герои, образные сцены, отношения, существующие в мировоззрении людей, но в определенной форме идеализации. Удачно выразился М. Хайм, сравнив виртуальное (представляемое) пространство с «информационным эквивалентом вещей» тогда, когда оно отражается в сознании человека.

Технической основой виртуального мира все-таки является формализованное цифровое отображение всего материального, что имеет аналоги в физическом мире, и что находит отображение в голове его создателей. Контакт виртуального и физического миров осуществляется при помощи огромного количества смарт-техники, позволяющей при помощи, опять-таки, программных продуктов осуществлять их сопоставление, соизмерение, угадывать адекватность одного и другого. И объемы этой техники, и ее возможности постоянно растут. По данным Т. Стьюарта, уже в конце XX века сопоставимость для приобретения в США технологического оборудования и информационной техники соотносилось как $107 млрд и $112 млрд [18]. Численность персонала, который работал в информатике, увеличилась с 17 % в 1990 году до 59 % в 2010 году.

Уровень социальной безопасности этих людей сегодня под вопросом. И этому имеется много причин. Назовем только одну из них: защита личного пространства человека, функция, записанная в Уставе ООН при создании этой организации.

Очевидным является всепроникающая способность смартфонов, в частности, посредством развития их как источников платежей в метро, магазинах, банках, оплат за услуги. На первый взгляд, удобная платформа, позволяющая человеку чувствовать себя уверенно в ситуациях, связанных с многочисленными платежами. Однако, как показали исследования Международного института компьютерных наук,

среди многочисленных приложений, идентификаторов, без которых такие опции невозможны, около 17 тысяч (!) предназначены для сбора, передачи и обработки конфиденциальной информации о пользователе, с явными нарушениями его прав. Используются легальные средства, разрешаемые, например, *Google*, в том числе, фотокамеры, рекламные индикаторы для подбора объявлений, идентификаторы типа *Android*, связанные с *IMEI*, *MAC*-адреса и др. Индивидуальная безопасность уничтожается при сборе и обработке постоянных идентификаторов, которые сопровождают человека на всем протяжении работы с приложениями. Отслеживается геолокация пользователя. Потребитель смарт-техники читается как открытая книга для самых различных задач и целей, в том числе, криминальных.

30-летний юбилей всемирной паутины общество встретило в некоторой растерянности. По мере своего развития *World Wide Web* рассматривался, как эффективный инструмент для создания беспроблемной жизни с высокими и доверительными социальными стандартами. Но от первоначальной идеи Тимоти Бернерс-Ли о «всемирности» и социальности» той интернациональной информационной платформы, которая базируется на интернет-коммуникациях, о таком преимуществе, как отсутствие единого руководства сетью, о независимости от правительств и бизнеса при помощи единых стандартов в интернет-коммуникациях, обеспечивающих единую социальную систему www, общество постепенно пришло к существующему ныне порядку вещей. Виртуальный мир сегодня по-своему угрожает миру реальному, он привнес в него вполне объективные угрозы.

Но обратимся еще раз к первому предложению этой главы. В сказуемом «тонет» закладывается достаточно глубокий смысл опасности для самого человека, которая связана с существованием ГИП. Огромные бескрайние объемы самой различной информации – это и благо, но это и зло. Посколь-

ку информация имеет способность не только накаливаться, но и распространяться, как бы самостоятельно, без права ее владельца. А значит, информация может быть ликвидным товаром, может продаваться и покупаться. Информация может иметь конфиденциальный характер, нести в себе персональные данные о ее владельце или авторе. Информацией можно воспользоваться для преступных целей или других неблаговидных действий. С развитием интернета такие действия происходят постоянно и стали системным явлением.

Одно из таких действий названо термином хакер (англ. *to hack* – обтесывать, делать зарубку), в последующем «взломщик», цель которого – проникнуть в компьютерную программную продукцию, нарушить ее целостность, в том числе, с преступными намерениями. Хакерские преступления по незаконному вмешательству в работу программного продукта самого различного назначения на ранних этапах этого явления вызвали соответствующую реакцию в виде антивирусного обеспечения для отдельных персональных компьютеров. Но, с развитием сетевого, межкомпьютерного обеспечения, интернета, разработка хакерских программ пошла далее. Взлом компьютерного программного обеспечения в самых различных вычислительных и управляющих системах дал возможность проникновения в самые секретные области человеческой деятельности: военную, разведывательную, финансовую, в область промышленных и коммерческих секретов, раскрытие персональных данных. Эта деятельность потребовала ответных подходов и мер по защите от таких проникновений и вмешательств. Так постепенно сформировалась область деятельности и область знаний под названием кибербезопасность.

Изначально кибербезопасность, как область знаний, относилась к чистому противодействию взломам компьютерных программ, нарушениям их целостности. Постепенно стала формироваться правовая база для подобных «действий-

противодействий» в различных странах по-своему. Только в начале XXI века мировое сообщество стало принимать киберпреступления на юридическом уровне, формируя среду для адекватных наказаний.

Актуален инженерный аспект этой области знаний. Уже понятно, что только программными методами влиять на безопасность общества в глобальном информационном пространстве не получится, исходя именно из глобальности явления ГИП. Актуальными становятся эргономические, экономические и социальные аспекты этой деятельности.

Сегодня общество подошло к другой составляющей термина «кибербезопасность», связанной с защитой человека, как субъекта этого вида безопасности. Многочисленные научные работы в этой области дали основание обратиться к необходимости обеспечения физической, биологической, социальной безопасности человека, как участника системы «машина-человек».

Собственно глобальность явления ГИП стала причиной существенного расширения задач и проблем, которые ставятся мировым сообществом перед кибербезопасностью как наукой.

1.2 Семантика термина «кибернетическая безопасность». С чем нельзя согласиться

В основе биологической сущности человека, как и всех других представителей живого мира, лежат три парадигмы, обеспечивающие его существование как особи. Это условия сохранения энергетического баланса (питание, отдых, затраты энергии на добывание пищи), воспроизводство себе подобных, а также обеспечение собственной безопасности или защита своей жизни. Из этих трех парадигм последняя по-

степенно перешла и в социальный статус, обеспечивая требуемый уровень безопасности не только для жизни, но и для защиты от болезней, психических потрясений, защиту и сохранение экономического благосостояния и социального благополучия. Безопасность в рамках глобального информационного пространства относится к таким парадигмам, которые в современном обществе игнорировать не получится.

Термин «безопасность» существует многие века и всегда играл одну из наиболее важных ролей в любых жизненных процессах, как индивидуальных, так и общественных. При этом особо важно, что его смысловое значение всегда относилось к объекту безопасности, к человеку. Обеспечение безопасности означало сохранение жизни, а позднее, и здоровья человека. Безопасность во время войны – это защита тела солдата от поражения соответствующими средствами воздействия (стрелой, саблей, пулей, осколками и др.). Соответственными были и средства защиты человека. Период Великих морских открытий был связан с массовым мореходством, и качество кораблей, их ходовые параметры были особенно важны, потому что за ними стояла жизнь людей, результат их деятельности. Именно они определяли уровень безопасности для человека. Со временем, общество пришло к пониманию товарного производства, торговли не потому, что были такие пожелания. Жизнь заставляла переходить к производственной специализации, а за ней и к специальной торговой деятельности, к различным видам профессиональной деятельности вместо универсальности дворового хозяйства только потому, что это способствовало повышению продуктивности, увеличивало общую товарную массу, обеспечивало экономическую и социальную безопасность человека. Подчеркнем, речь идет об объекте безопасности – человеке.

В мирное время безопасность человека обеспечивалась, прежде всего, в процессе трудовой деятельности, занимавшей большую часть его жизни. Появилась безопасность че-

ловеческого труда. Многие области жизнедеятельности требовали к себе отношения безопасности. Безопасность от пожаров, от окружающей природной среды, от опасностей в различных отраслях промышленности – химической, атомной, электротехнической, металлургической, энергетической, в различных областях быта и др. Домостроение – это тоже безопасность от внешних условий. Надежность машин, средств передвижения – это тоже безопасность. Надежность электрических сетей и предохранение от электрического тока, механические ограждения от падения с высоты – это тоже безопасность человека.

С появлением вычислительных машин и других источников сверхвысокочастотных генераторов основное внимание с позиций безопасности человека уделялось электромагнитной безопасности для человека со стороны ламп, электронно-лучевых трубок мониторов и др. [19, 20, 21]. Когда стало ясно, что тактовая частота компьютерных микросхем и чипов является определяющим звеном для обеспечения быстродействия персональных компьютеров, эта реальная опасность была успешно проигнорирована, и сверхвысокочастотные приборы, по существу, опасные по воздействию почти на любую биологическую систему, получили преимущества над безопасностью и здоровьем человека [22]. В этом случае, безопасность человека пасовала перед электронно-лучевыми мониторами и микросхемами первых персональных компьютеров и последующих за ними технических систем.

Норберт Винер назвал кибернетикой науку о связи живых организмов и машин [23]. В современном понимании, кибернетика – это наука об общих закономерностях процессов управления и передачи информации в машинах, *живых организмах и обществе* (курсив автора) [24].

Если для кибернетики (в переводе с греческого – κυβερνητιχη), как искусства управления, человек является

субъектом деятельности, то для кибернетической безопасности человек – это объект воздействия. В работе [25] признается, что кибербезопасность, кроме защиты от вирусных атак, должна обеспечивать защиту от манипулирования общественным сознанием. То есть автор учитывает человеческий фактор в системе кибернетической безопасности. В работе [26] проблемы кибербезопасности связываются с защитой от угроз для систем управления и, одновременно, от посягательств на общественные человеческие ценности.

В работе [27] дана одна из многих формулировок термину «безопасность», как «…науки, изучающей природные, техногенные, социальные, экономические и другие процессы образования, развития и взаимодействия субъектов, объектов, окружающей среды и их комбинаций с целью выявления источников опасностей, определения их характеристик и формирования законов и других нормативных актов, устанавливающих понятия, требования, рекомендации и методики, выполнение которых должно гарантировать *защищенность интересов отдельной личности и общества* в целом от всех выявленных и изученных источников опасности». Мы намеренно подчеркнули объектность этого термина, относящуюся к человеку. Человек, в свою очередь, является одним из двух элементов системы «человек-машина», где, в нашем случае, под термином «машина» следует понимать все относящееся к киберпространству, обеспечивающему функционирование кибернетической системы «пользователь-ГИП».

Из этого следует, что понятие «кибернетической безопасности» может быть описано в таком виде: это предотвращение ущерба, который мог бы нанести один человек другому при помощи несанкционированного вмешательства некоторого деформирующего программного продукта в основное программное обеспечение. Такой программный продукт – это не что иное, как инструмент, при помощи которого дос-

тигается результат. Логика подсказывает, что, в более расширенном смысле, понятие безопасности, в том числе и кибернетической безопасности, определяется уверенностью человека в том, что ничто не угрожает ему, его биологическому здоровью, психологическому состоянию, в равной степени как и его социальному благополучию или экономическому благосостоянию.

С появлением термина «кибербезопасность», в корневом составе которого находится слово «безопасность», и огромного пласта науки, связанной с защитой программного обеспечения от нештатных проникновений, мы увидели, что этот термин никаким образом не относился к защите здоровья пользователя по изложенным выше признакам. Эта область знаний, по праву своего появления, занялась именно безопасностью функционирования самих машин в той же самой «человеко-машинной» системе, где роль машины играет компьютер, его программное обеспечение, а позднее, компьютерные сети, интернет, новые коммуникационные технологии. Они оттеснили вторую часть системы, а именно, человека, от его безопасности в пользу других социальных преимуществ: удобства миниатюрной техники с широкими возможностями, доступа к весьма ценной и обширной информации, совершенно нового формата широкого общения и т. д.

Казалось, что дороги «безопасности» и «кибербезопасности» разошлись навеки. Однако, с развитием информатизации, с приходом новых технологий и коммуникационных сетей, получивших социальное отображение в обществе, с ростом возможностей для самого человека, появлялись и новые аспекты опасности, связанной и с кибератаками, и с интеграцией такой «машины» в преступную среду, а также с изменениями основ общения в сетях. Все это представляет собой несколько иной предмет для исследования – возврат к безопасности человека в информационном пространстве.

Здесь «информация» – это только среда, в которой человеку может быть нанесен ущерб. И безопасность относится, прежде всего, к пользователю, т. е. к человеку. В самом простом изложении, психику человека в процессе обработки информации и принятия решения в первом приближении можно представить в виде системы из двух блоков – сознания и подсознания.

Прием информации и выдача решения осуществляется сознанием человека, а обработка информации – и сознанием, и подсознанием в комплексе [28]. Получается, что без участия человека кибернетические системы работать не могут, по крайней мере, в пределах современных систем искусственного интеллекта. И получается, что и конечный объект кибербезопасности, области защиты компьютера от проникновения и защиты информации – человек, и конечный объект безопасности в системе «человек-машина» остается один и тот же – пользователь, человек. Система становится все более похожей на функционально двуединую систему, с которой все время приходится иметь дело в процессе любой трудовой деятельности. Там, где труд и опасность сосуществуют друг с другом и не могут проявляться в отдельности: нет опасности без труда и нет труда без абсолютной опас-ности.

В литературе описан результат одной из реальных кибератак на единую цифровую информационно-управляющую систему электроподстанций, в результате которой происходит перепрошивка цифровых устройств или удаление на них системного и прикладного программного обеспечения и, как результат, повреждение дорогостоящего первичного оборудования и варианты несанкционированного попадания персонала под действие электрического тока [29]. Это прямая угроза жизни человека, причиной которой была кибератака на программное обеспечение.

Еще один убедительный пример воздействия на человека результатов хакерских атак распространен в литературе,

например, [30]. На одном из автопромов бывшего СССР программист вносил изменения в программное обеспечение таким образом, чтобы на конвейере происходили сбои, в результате чего в учете терялись объекты готовой продукции или комплектующих деталей. Причем, никто из персонала – потребителя этой отчетности, не догадывался об афере, потому что не имел доступа к программному обеспечению. Вносимые поправки стабилизировали ситуацию и давали хакерам двойную выгоду: за счет укрытия материальных ценностей и за счет стимулирования труда по исправлению «ошибок» ПО. Таким образом, хакерская атака влияла, прежде всего, на людей, обеспечивающих рабочий процесс, что сказывалось на их зарплате, показателях труда, приводило к конфликтным ситуациям.

Новой области знаний, кибербезопасности, приходится проходить методологически очень трудный путь к определению своей терминологии и понятийности, соизмерения своих целей и задач с равнозначными знаниями в других областях безопасности человека.

Ведь по большому счету, кибернетическая безопасность своими задачами на сохранение в целостности машины и ее программного продукта стремится к тому, чтобы обеспечить уровень безопасности каких-то аспектов человеческого существования. Рассмотрим несколько ключевых понятий из науки под названием кибернетическая безопасность.

1. Конфиденциальность информации отображает такое состояние информации, при котором право доступа к ней находится только у субъектов этого права.

2. Доступность информации – это право на открытую информацию со стороны владельца для свободного доступа. Эта особенность лежит в основе так называемых доверительных протоколов в блокчейн технологиях.

3. Целостность информации – это сохранение информации от несанкционированных изменений в результате внешнего вмешательства.

Все эти нарушения: нарушение прав обладателя и раскрытие информации; разрушение целостности информации; ограничение разрешенного доступа к открытой информа ции – все это нанесение ущерба пользователю, то есть человеку.

В таблице 1.1 представлены формулировки понятий большей части областей знаний по безопасности. Обратим внимание на то, что в абсолютном большинстве типов безопасности объектом присутствует человек или условия его существования. Исключение составляет кибернетическая безопасность. В различных источниках, включая нормативные документы, формулировки отличаются. Общее только то, что в них отсутствует или почти отсутствует человек.

Этому имеется объяснение, связанное с тем, что изначально и предмет исследования, и субъект здесь принадлежали компьютеру, технике, машине, существовавшей, все-таки, не самостоятельно, а в системе «человек-машина». Компьютер, интернет, социальные сети пока не имеют возможностей для самостоятельного существования. Человек является неотъемлемой составляющей такой системы. Пока актуальными были задачи защиты от внешнего воздействия на программное обеспечение компьютера, такая ситуация всех устраивала. И на то, что устойчивая работа компьютера экономила рабочее время и защищала психику пользователя, а свободное от вирусов программное обеспечение давало правильный расчетный результат, смотрели как на нечто дополнительное и не главное. Разработчики науки считали, что защита от хакеров, от кибернетических преступлений и есть основная задача кибернетической безопасности. И в некотором временном промежутке это себя оправдывало. Но не всегда.

Таблица 1.1 – Определение понятия безопасности для некоторых областей знаний

№	Тип безопасности	Понятие в принятых терминах
1	2	3
1	Военная безопасность	Это состояние защищенности организма **человека** от внешнего поражения средствами вооружения боевого противника
2	Безопасность труда	Это состояние **защищенности работников**, обеспеченное комплексом мероприятий, исключающих воздействие вредных и (или) опасных производственных факторов на **работников** в процессе трудовой деятельности (Википедия)
3	Безопасность жизнедеятельности	Это состояние **защищенности человека** в условиях окружающей среды от негативных и опасных воздействий антропогенного и естественного происхождения и достижение комфортных или безопасных условий жизнедеятельности (Википедия)
4	Пожарная безопасность	Это состояние **защищенности личности**, имущества, общества и государства от пожаров и огня (Википедия)
5	Химическая безопасность	Это состояние, при котором исключаются условия для химического заражения или поражения **людей** (Википедия)
6	Экологическая безопасность	Допустимый уровень негативного воздействия природных и антропогенных факторов экологический опасности на **человека**

Окончание таблицы 1.1

7	Электромагнитная безопасность	Область знаний о вреде, наносимом **человеку** электромагнитным излучением
8	Кибернетическая безопасность	1. Процесс использования мер безопасности для обеспечения **конфиденциальности**, целостности и доступности данных и меры по защите систем, сетей и программных приложений от цифровых атак (*Cisco*). 2. Воплощение всех мер защиты сетей, приложений и устройств от угроз, **сохранение корректной работы организаций** (*Linkas*). 3. Раздел информационной безопасности, в рамках которого изучают процессы формирования, функционирования и эволюции киберобъектов, для выявления источников киберопасности, образующихся при этом, определение их характеристик, а также их классификацию и формирование нормативных документов, выполнение которых должно гарантировать защиту киберобъектов от всех выявленных и изученных источников киберопасности (Википедия)

Достаточно аргументированную позицию изложил А. С. Алпеев в своей работе [31]. Мы будем ссылаться на эти исследования, потому что здесь, пожалуй, впервые сделана попытка соединить воедино объект, предмет и субъекты изучения для целой отрасли науки – кибернетической безопасности. По данным Алпеева: «Кибербезопасность – условия

защищенности от физических, духовных, финансовых, политических, эмоциональных, профессиональных, психологических, образовательных или других типов воздействий (*на человека – В. В.*) или последствий аварии, повреждения, ошибки, несчастного случая, вреда или любого другого события в киберпространстве, которые могли бы считаться нежелательными» [31].

Автор идет далее, небезосновательно настаивая на том, что «… термин «кибербезопасность» является производным от родового термина «безопасность», таким образом, что «кибербезопасность» представляет собою часть понятия «безопасность», *наделяемую некоторыми специфическими особенностями*, которые должны составить вторую часть определения термина «кибербезопасность», следующую за родовым словом». В этом его следует поддержать. Очевидным является то, что однокорневые термины должны иметь одинаковое смысловое наполнение.

Рассмотрим семантику (смысловое наполнение) предмета наших исследований, термина «кибернетическая безопасность», сокращенно «кибербезопасность», в ряду сложноподчиненных однокорневых терминов, которые уже существуют: производственная безопасность, химическая безопасность, экологическая безопасность, пожарная безопасность и др. Все подобные термины состоят из двух слов, одно из которых – подлежащее, отражающее основополагающую тематическую принадлежность термина, а именно, «безопасность», имеет самостоятельное смысловое значение. А второе – это второстепенный член, показывающий принадлежность подлежащего к той или иной области знаний или деятельности: военной, трудовой и т. д. Причем, второе слово, по смыслу, подчинено первому. Иными словами, сущность этих двухсловных терминов, их существительное – это «безопасность». А приложение этого термина к чему-то, его

прилагательное – кибернетика, химия, экология, радиация и т. д.

Смысл безопасности заключается в словосочетании: «без опасности». Корневое слово «опасность» означает угрозу жизни, здоровью, существованию. Эти понятия характеризуют объект опасности только как живое существо, которое опасается потерять способность к существованию – жить, осуществлять свою деятельность. Приведем примеры.

Вулканическая деятельность – это одна из распространенных форм материального и энергетического обмена между различными составляющими земной коры и поверхностью планеты. Для неживой природы вулкан не представляет опасности. Это всего лишь форма существования неживой природы. Опасность вулканического извержения относится только к живому существу, в том числе, к человеку, находящемуся в зоне извержения.

Землетрясение – это стандартная форма высвобождения энергии тектонического сжатия плит. Оно тоже не может представлять опасности для неживого мира и, наоборот, представляет опасность для всего живого, в том числе, для человека, попавшего в зону землетрясения.

В человеко-машинной системе безопасность, отнесенная к понятию «машина», определяется другими словами: исправность, надежность, безаварийность работы, целостность системы, сохранение работоспособности, время наработки на отказ, неразрушаемость, сохранение принципов работы системы, ремонтопригодность, долговечность и др.

В 2013 году вышло постановление Кабинета Министров Украины № 62 «Про затвердження технічного регламенту безпеки машин», согласно которому «встановлюються вимоги до машин щодо захисту життя або здоров'я *людини*» (курсивом выделено автором). В 2017 году в Украине были приняты «Вимоги *безпеки та захисту здоров'я* під час використання виробничого обладнання *працівниками*»

(НПАОП 0.00-7.14-17), согласно которым утверждается приоритет человека, как фактора безопасности при работе с любыми машинами. В целом, под безопасностью машин в технической документации подразумевается способность выполнять требуемую функцию в состоянии, при котором отсутствует недопустимый риск *для человека*.

Например, безопасность автомобиля – это совокупность конструктивных и эксплуатационных свойств автомобиля, направленных на сохранение *жизни и здоровья человека*. Это же относится и к глобальному информационному пространству, как к системе «человек-машина». Здесь безопасность – это требования к компьютерному оснащению, программному продукту и характеру информации, не вызывающие у пользователя нарушения здоровья, его социальности.

Информацию о предмете исследования, опасностях дает признанная во всем мире классификация опасностей:

– по источнику возникновения, опасности делятся на шесть групп опасностей: природные, техногенные, антропогенные, экологические, социальные и биологические;

– по характеру *воздействия на человека* опасности делятся на пять групп: механические, физические, химические, биологические и психофизиологические. Это признаки опасностей.

Рассмотрим смысловое наполнение двух частей составного термина «… ая безопасность».

Любой сложноподчиненный термин, из числа основополагающих, должен иметь свои составляющие смысловые элементы, отражающие предметы и их принадлежность, в частности, *объект воздействия, субъект воздействия и предмет воздействия.* Для единосмысловых сложных терминов эти семантические элементы должны совпадать, чтобы исключить двойственное толкование самих терминов.

Таблица 1.2 – Безопасность, как функция влияния на жизнь и здоровье человека

№	Тип безопасности	Субъект воздействия	Объект воздействия	Предмет воздействия
1	2	3	4	5
1	Военная безопасность	Боевая единица противника	Участник боевых действий, боец	Нарушить целостность организма путем ранения или потери жизни
2	Безопасность труда	Техническая система (ТС) или технологический процесс (ТП)	Работник, обеспечивающий функционирование ТС или ТП	Нарушить здоровье, привести к потере жизни или профзаболеванию
3	Безопасность жизнедеятельности	Окружающая антропогенная и техногенная среда, в том числе, в экстремальных параметрах	Человек в системе окружающей среды	Нарушить комфортные или безопасные условия жизнедеятельности
4	Пожарная безопасность	Огонь, температура в зоне горения	Человек, материальные ценности	Разрушить материальные ценности, привести к потере человеческой жизни

Окончание таблицы 1.2

1	2	3	4	5
5	Химическая безопасность	Химически активные вещества	Человек в зоне воздействия химических веществ	Химическое воздействие: отравление, химический ожог и др.
6	Экологическая безопасность	Окружающая природная среда	Человек в зоне антропогенных факторов	Нарушить здоровье человека, привести к заболеваниям, потере жизни
7	Электромагнитная безопасность	Электромагнитные излучения	Человек в зоне электромагнитного излучения	Нарушить здоровье человека, целостность организма
8	Кибернетическая безопасность I	Несанкционированный индуктор в программном обеспечении	Программное обеспечение, элементы киберпространства (КП)	Нарушить целостность программного обеспечения, элементов «КП»
9	Кибернетическая безопасность	1. Несанкционированный индуктор в программном обеспечении. 2. Многообразие информации	Пользователь программного обеспечения	Деформировать участие пользователя в системе, нарушить его здоровье или благосостояние

Это положение в науке никем и никогда не оспаривалось. Осмыслим эти элементы.

Субъект воздействия – это предмет или лицо, оказывающее некоторое воздействие с определенной целью.

Объект воздействия – это предмет или лицо, на которое оказывается воздействие и, тем самым, зависимое от субъекта.

Предмет воздействия – элемент, который понятнее всего описан в юридических терминах и обозначает функцию, при помощи которой осуществляется действие в системе.

Как показано в таблице 1.2, все семантические однокорневые термины в качестве объекта воздействия со стороны любого типа «опасности» принимают человека. И предмет воздействия в системе, по своему функциональному назначению, связан, в первую очередь, с нарушением здоровья или жизни человека, как объекта воздействия. Для всех, кроме термина «кибернетическая безопасность». В таблице 1.2 мы намеренно обозначили этот термин с уточнениями I и II, первый из которых содержит в качестве объекта воздействия, а значит, защиты от него, элементы киберпространства (КП) – программное обеспечение (ПО), целостность компьютера, гаджетов, сети. Именно на них направлена защита в кибернетической безопасности. Во втором случае, предлагается в качестве объекта воздействия обозначать, все-таки, пользователя, то есть, человека. Все нарушения технического характера в данной системе, так или иначе, сказываются на состоянии пользователя, участие которого в системе типа «человек-машина» сразу существенно деформируется, включая здоровье, возможности продолжать работу, финансовые и социальные потери и др. В свою очередь, игнорирование безопасности по элементу «машина», то есть, именно того, чем сейчас занимается «кибербезопасность», является недопустимым, так как любая индукция или вмешательство в ра-

боту составляющих компонентов киберпространства носит, чаще всего, элемент преступления и требует не только исправления системы, но и наказания хакера.

Обратимся к теории эргатичности, применительно к системам «человек-машина», понимая *равнозначность и равноправность* этих двух составляющих элементов системы. Все, без исключения, типы безопасности человеко-машинных систем, так или иначе, связаны с простым алгоритмом: нарушение в работе машины, как по техническим, так и по организационным причинам, ведет к аварии, что, в свою очередь, приводит не только к нарушению работы самой машины, но и к нарушению целостности организма, потере здоровья, смерти работника, в зависимости от степени нарушения. В равной степени, разрушение «машины» или нарушение в действиях «человека» приводит к нарушению работы системы в целом. Эргатические свойства являются объективной реальностью, потому что эта система неразрывна и не может существовать в отдельности от своих ключевых элементов.

Все это относится и к кибернетическим системам, в составе которых также два основополагающих элемента: киберпространство и пользователь, в самой различной их интерпретации. Поэтому, подчеркивая актуальность огромной работы в области кибернетической безопасности, по защите киберпространства от внешнего вмешательства, следует обратить внимание и на второй элемент системы, на пользователя, его физическое, психическое стояние, понимая, что без этого не может быть эффективной работы системы в целом.

Этим еще раз подчеркивается, что кибернетическая безопасность, как область знаний, относится в равной степени и к наполнителям киберпространства, и к пользователю услугами этого «пространства», и имеет право в равной степени изучать вопросы защиты программного продукта от разрушения или проникновения, и условия комплексной

безопасности, необходимые для пользователя этой условной «машины». И под ущербом любого негативного кибернетического воздействия следует понимать не только деформацию или разрушение программного продукта, но и все последствия для пользователя, других участников системы, например, в технологиях распределенного реестра – блокчейна, в социальных сетях, включая моральный ущерб, воздействие на психику, физиологию, социальность больших групп участников.

В настоящей работе мы выделим только одну из многих групп такого воздействия на человека – социальные и экономические факторы. Они уже сейчас видятся как особенно многочисленные, многосторонние и весьма влиятельные, оказывающие огромное влияние на человека в социальных сетях, на технические возможности «машины» из собственно киберпространства, на развитие всей промышленности для создания и эксплуатации компьютерной техники, всего софта, многочисленных гаджетов, смарт-карт для блокчейн технологий и др.

Хотелось, чтобы это стало существенным аргументом в пользу смыслового расширения понятия «кибернетическая безопасность», понимая, что такой поход только обогатит эту науку и даст возможности для появления новых результатов.

Далее в работе мы рассмотрим некоторые вопросы опасностей, связанных для человека, находящегося в глобальном информационном пространстве интернета, социальных сетей, других видов телекоммуникаций. Полагая, что все эти и другие виды опасностей есть предмет для исследований в области знаний, которая сегодня носит название «кибернетическая безопасность», мы не предлагаем способы защиты от этих опасностей, хотя многие из них лежат на поверхности, а иные требуют более серьезных исследований, которые лежат за пределами этой книги и требуют своих авторов.

1.3 Очевидные опасности глобальной информатизации для общества

С тех пор, как в мире появились первые признаки глобальной информатизации, человечество спорит о преимуществах и недостатках всемирного информационного пространства. Подобные споры преследовали и другие подобные глобальные изобретения. Так было и при создании радио и телевидения, и при освоении атомной энергии, и при создании генно-модифицированной продукции. Подобные реакции общества имели место и при распространении табакокурения, наркотических средств, массового употребления алкоголя [32]. Многие из этих споров не утихают по сей день и широко описаны в самой разной литературе.

По своему многообразию, разносторонности и информативности глобальное информационное пространство может быть сравнимо с внутренним миром самого человека. Может быть, поэтому ГИП, по существу, стало своеобразной экологической нишей для человека, в которой оно находит все, что ему необходимо с точки зрения нематериального мира: знания, информацию, эмоции, общение, то, что недостает отдельному человеку в реальном мире. Отсюда такая его зависимость от интернета, от социальных сетей. Отсюда и все компьютеромании, и уход в виртуальное пространство, и замена реального общения, круга реальных людей и близких на мир образов, виртуальных отношений, мир, который в большей степени подвластен лично пользователю, чем, часто более жесткий, реальный мир.

Как чувствует себя человек в такой искусственной социальной среде? Взаимодействие, с глобальным, всеобъемлющим информационным пространством – это актуально, в первую очередь, для самого человека. Уровень комфортности такого сосуществования может давать стимулы к даль-

нейшему развитию, или, наоборот, накапливаемый дискомфорт может привести к усугублению системы или поиску новых направлений развития для самого глобального информационного пространства.

С другой стороны, глобальное информационное пространство и само давно уже стало неотъемлемой частью социальной системы, центральной частью которой является человек.

Глобальное информационное пространство, как экологическая ниша, для многих людей становится более приемлемым, безопасным, чем реальный мир. Это одно из многих качеств, делающих привлекательными информационные системы. Но существуют и другие качества и свойства ГИП, которые могут или уже влияют на человека в данной системе.

Происходит сопоставление процессов восприятия информации на традиционных бумажных и электронных носителях. Но и этого мало. Мы имеем дело с всепроникающей системой и, поэтому, должны отследить влияние большей части свойств ГИП, в частности, человеческий милитаризм, государственное вмешательство, национальные факторы, защита персональных данных, гуманизм, возможные взаимоотношения с нарождающимся искусственным разумом и др.

Рассмотрим их.

Одними из первичных признаков этого являются опасность со стороны ГИП для здоровья человека, его всеобъемлемость, мониторинговость [33]. По степени влияния на человека, ГИП со временем выходит на передовые позиции в обществе, оказывая и положительное, и негативное влияния на социум в целом, его экономику, науку, политику, образование [34]. Изначально ГИП проявляется как инструмент для созидания и развития, но уже сейчас имеет признаки инструментария для разрушения, подавления и даже удобова-

римого методологического обеспечения для глобального авторитарного управления миром.

Вопрос вопросов. Что несет позитивного для человечества глобальное информационное пространство, и чем за это придется (приходится) расплачиваться людям?

Безусловными позитивами глобализации информационного пространства являются унификация и упрощение доступа к огромным массивам любой информации, удобство ориентирования в информационном пространстве, упрощение форм общения между людьми.

С подобной ситуацией, связанной с доступностью информации, общество столкнулось уже в XVIII веке, на заре массового тиражирования печатной продукции, в связи с резким ее удешевлением и доступностью [32]. Уже к концу XIX века в цивилизованном мире существовало более 15 тыс. изданий газет и журналов. Только в азиатских колониях европейских государств издавалось около 300 периодических изданий. Правда, параллельно были запущены процедуры национальных цензур, которые успешно продержались до конца XX века и благополучно сошли «на нет» в XXI веке. В современном глобальном информационном пространстве цензуры, как таковой, нет и каждый – сам себе рецензент, цензор, и защитник. И результаты не заставили себя ожидать: деформация и неправдивость информации. Это первая проблема, которая пришла к нам вместе с ГИП. Но не единственная из тех, что прямо влияют на безопасность экосистемы человека.

Информационные ресурсы интернета действительно очень сильно теряют от собственной недостоверности, недобросовестности и вседозволенности отдельных пользователей. Причин две. Одна заключается в том, что по подсчетам специалистов 95 % информации, размещенной в интернете, относится не к сгенерированной (новой) информации, а является перепечатками, копиями чужой информации, так

называемыми рерайтами и репостами, то есть, компилятами и копирами, уровень искажения информации в которых весьма велик. При этом дублированная информация существенно искажается и далеко не всегда соответствует первоначальной. И это вторая причина.

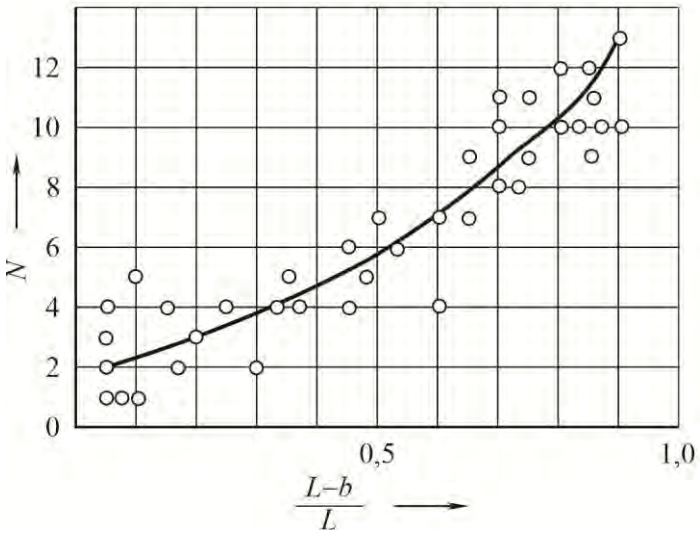
Иными словами, 95 % информации в интернете не представляет интереса для пользователей-аналитиков, способствует засорению информационного пространства, наносит ущерб пользователю [32]. Самый простой из существующих способов выявления недостоверной информации – сравнение с аналогами – в электронных средствах информации не срабатывает из-за высокой степени повторяемости, дублирования данных в различных источниках. В качестве критерия достоверности принимают иногда рейтинг сайта, авторитет его авторов. Но и это не защищает от ошибок. Глеб Павловский подчеркнул: интернет – идеальный инструмент для запуска в массовое сознание любой дезинформации [35], любой ошибки. Этому способствует отсутствие какой-либо цензуры, объективных рецензий, всего того, что сопровождало в XX веке бумажные средства информации.

Появилось даже понятие инфодемии, как явления восприятия массовой дезинформации, запускаемой в информационные сети для узкого и целенаправленного влияния на мнения, сознание и даже мировосприятие огромного количества неподготовленных к ответной реакции людей. Чаще всего эта манипуляция создавалась в пробном варианте для обеспечения целенаправленных акций: покупки некоторых групп товаров, в особенности, медицинских, для влияния на определенные секторы экономики, связанные с массовым участием в них людей: питание, туризм, маршрутные перевозки (авиа, ж/д и др.), приобретение современной бытовой техники, коммуникационные услуги, в частности, смартфония. Примером может служить многолетняя экспансия компании *Microsoft* на рынок компьютерной техники с последо-

вательными разработками новых персональных компьютеров: 286, 386, 486, пентиумов многочисленных модификаций, которые обновлялись пользователями, несмотря на то, что и физический, и технический срок эксплуатации предыдущей техники не исчерпывался.

Но вернемся к дезинформации в интернете.

Интересные наблюдения автора, члена нескольких специализированных советов по защите кандидатских и докторских диссертаций. Глубина научной новизны диссертационных работ связана напрямую с соотношением числа источников литературы – электронных и бумажных (рис. 1.1).



N – число замечаний рецензентов по научной новизне диссертации; L – общее число литературных источников, используемых в диссертации; b – число бумажных источников информации, на которые ссылается автор

Рисунок 1.1 – Влияние ссылок из интернет-источников на научные результаты диссертационных работ

Общая зафиксированная динамика такова. Чем больше использовано электронных источников в списках литературы, тем больше страдает степень научной новизны и достоверность работы. Тем больше замечаний со стороны рецензентов по этим критериям диссертаций. И наоборот.

Чаще всего это связано с низкой достоверностью электронных источников, большим числом ошибок и искажений в них. Иллюстрация: в одном из специализированных советов по защите диссертаций по экономике была отклонена кандидатская диссертация, научная новизна и теоретические выкладки которой не вызывали сомнений. Причина отклонения работы заключалась в ошибочности исходных данных, которыми автор работы воспользовался из интернет-источников и, как следствие, в целом неверные выводы по результатам выполненных исследований [32].

Третьей проблемой, как это ни странно, стали большие объемы информации, часто очень поверхностной, без глубокого смыслового содержания. Подобная информация, которая также засоряет ГИП, в целом дает очень мало «пищи для ума» [32]. Рост объемов информации в ГИП сегодня неумолим. Удвоение интернетовской информации происходит каждые два года на протяжении последних восьми лет (рис. 1.2).

По данным того же интернета, к концу 2013 года информационный объем в электронных сетях достиг примерно 2,8–2,95 *z*-байта ($1 \cdot 10^{20}$ байт) и к 2020 году прогнозируемый объем информации возрастает до 40 *z*-байт [36, 37]. Характер этой информации крайне многообразен и не подлежит систематизации в данной работе. Достаточно того, что каждую секунду в мире передается 2 млн интернет-сообщений.

Объем и качество информации в интернете, на первый взгляд выступает в качестве выдающегося блага. Тем не менее, далеко не всегда этот показатель выступает в качестве генератора новых идей, открытий, изобретений, законов, закономерностей. По некоторым данным, интернет стал именно той платформой, на которой ярким цветом разгорелось

такое явление, как плагиат. Эта тема требует отдельно исследования. В Украине появился законопроект № 3353 о внесении изменений в некоторые законодательные акты относительно защиты авторского и смежных прав в интернете. Понастоящему защитить авторское право в интернете может регламентированная законом система электронных жалоб, где и подающего жалобу, и нарушителя будет легко идентифицировать. При этом, споры должны решаться только в судебном порядке с четко определенной ответственностью сторон [37].

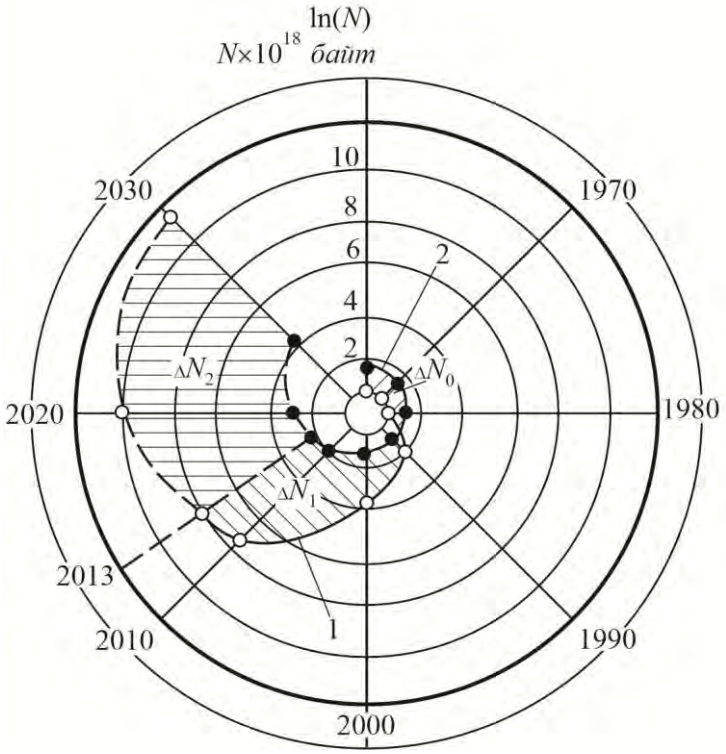


Рисунок 1.2 – Суммарные объемы информации в электронных (1) и аналоговых (2) источниках на 2013 год

Суммарная аналитичность массивов повторяемой информации ГИП крайне невысока. Под аналитичностью будем понимать возможность получать новые выводы, новые знания из исходного читаемого материала. Исследования компании IDC свидетельствуют, что аналитической обработке подлежит только 0,4 % всей цифровой информации в интернете [39]. Но аналитичность и этой информации невелика, из-за ее неполноты, сокрытия ключевых и смысловых объектов и, еще раз подчеркнем, недостоверности отдельных данных.

Появилось даже определение «информационный шум», под которым понимается избыточность информации в коммуникативной среде, вызывающая функциональную деформацию ее систем [40]. К источникам такого шума В. П. Полудина [41] относит, в частности, сетевую рекламу (медийную, контекстную, геоконтекстную, *product placement* и др.), спам, результаты оптимизации поисковой выдачи, или *SEO*, вирусный маркетинг; репост и рерайт; флуд, флейм, холивар, троллинг, эльфинг и др. Все они по существу являются излишней информацией в интернете, которая засоряет информационное пространство. И реальных ограничений этому валу нет.

С этих точек зрения, развитие информационных и социальных сетей, по мнению специалистов, явно не способствует развитию аналитических способностей у пользователей, росту уровня образованности у людей. «Образованщина» – назвал это явления поверхностного образования великий российский писатель А. Солженицын.

Ученые Мэрилендского университета в своих исследованиях подтвердили неоднозначность освоения студентами электронных и печатных текстов [42]. При предпочтительном восприятии студентами электронных текстов, большей скорости прочитывания материала, общее понимание прочитанного было выше для печатных текстов. Способно-

сти применить материал на практике в случае его восприятия с печатных носителей было на порядок выше, чем при работе с электронными текстами. Эффективность моторной памяти была выше при восприятии информации с печатных носителей, а зрительная память давала преимущества при восприятии материала с электронных носителей. Степень запоминания печатных текстов оказалась выше, чем при запоминании электронных текстов. Вывод может быть неоднозначным, но в целом, по результатам исследователей, в учебном процессе он определенно в пользу печатных носителей информации.

Безудержный рост объемов информации в электронных носителях давно уже вошел в противоречие с биологическими способностями человека к усвоению этой информации. Погружение человека в информационное пространство неограниченных объемов влечет за собой рост не только психологической, но и биологической зависимости человека от компьютера, что отражается в гемодинамике, изменении артериального давления, нарушениях в работе периферической нервной системы и мозговой деятельности, нарушающихся психомоторных реакциях и др. До сих пор очень мало научных данных о влиянии сверхслабых электромагнитных полей на организм человека.

Увеличение объемов информации приводит к существенной социальной зависимости человека от компьютера. По данным *Union National des Associations Familiales* (Франция) в течение года дети проводят 150 часов времени с родителями, 850 часов – с учителями и 1400 часов с компьютерами [43]. При этом человек чаще всего идет по пути наименьшего сопротивления: при возрастании информационной нагрузки включаются механизмы поверхностного усвоения, фиксации информационных заголовков и аннотаций, без какой-либо аналитики. Вновь проявляется некоторый весьма высокий «уровень бесполезности» информации (рис. 1.3). «Полез-

ность-бесполезность» информации можно опосредовано оценивать по числу обращений и ссылок на эту информацию. Судя по исследованиям *IDC* [44], степень бесполезности (для аналитической обработки) информации в интернете достигает 99 %. К слову, уровень бесполезности информации на бумажных носителях в XIX веке сводился к единицам процентов, а к концу XX века поднялся до 40 % (но не до 99 % же) за счет развития идеологических и политических публикаций и увеличения объемов обширной ежедневной прессы. Сегодня невостребованной для аналитики в интернете является до 99 % информации.

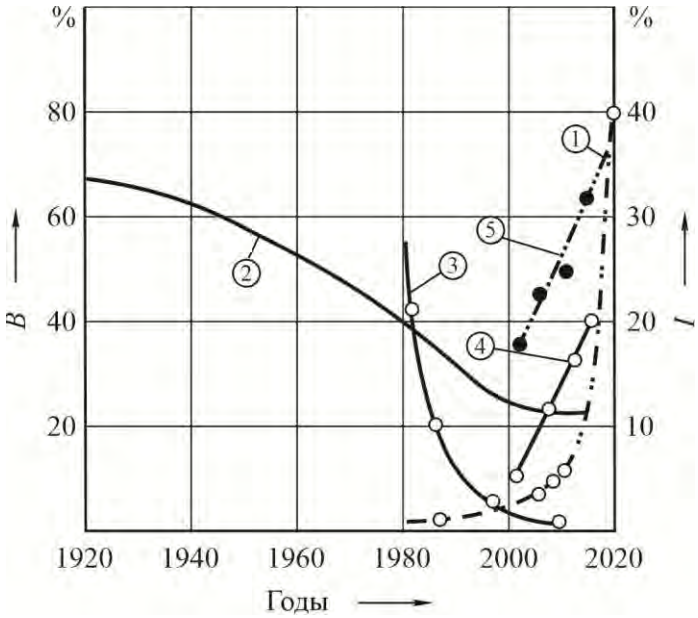


Рисунок 1.3 – Востребованность информации на бумажных (2) и электронных (3) носителях, в том числе, полнотекстовых (4) в сопоставлении с динамикой роста информации в интернете (1)

Несомненным спасением для науки являются базы полнотекстовых изданий (ПТИ) – журналов, статей, монографий. Создано большое количество порталов. Еще пять лет назад в них размещались только короткие аннотации, справочный и библиографический материал. Сейчас только в России издается 4000 полнотекстовых научных журналов, работают сайты *Public.ru*, *Integrum*, Ланс и др., в Украине работают проекты издательства периодики компании *EBSCO Publishing*, проект *ELibUkr* «Электронная библиотека Украины». Создание и участие в корпорациях полнотекстовых и зданий является приоритетом не только для современных библиотек, но и для крупных книжных издательств [45, 46]. Тем не менее, полнотекстовые издания сегодня занимают информационную нишу 0,004 % всего ГИП, что, в конечном результате, обеспечивает их аналитичность на уровне объемов бумажных носителей информации и не более. В активе преимуществ ПТИ – только доступность и представительность информационной выборки, экономия от использования бумаги. На рис. 1.3 представлена кривая (5), которая суммирует востребованность в информационных источниках на бумажных и электронных носителях за последние годы. Очевиден рост показателя.

В глобальном информационном пространстве существует одно качество информации, которое трудно переоценить для человечества. Это возможности для сохранения мирового информационного наследия в виде оцифрованных рукописей, уникальных книг, списков, научных трудов, опубликованных когда-либо в единственном экземпляре. Это позволяет элементарно тиражировать такие источники и делать их менее уязвимыми для уничтожения.

В частности, такой глобальный проект, как Мировая цифровая библиотека (*World Digital Library*), в которую должны войти отсканированные и оцифрованные материалы мирового литературного наследия, дошедшие до нашего

времени и в единственном экземпляре существующие в отдельных библиотеках университетов, муниципалитетов, правительств, архивов и др., где доступ к ним со стороны большинства населения планеты просто невозможен. Такие оцифрованные источники не уничтожаются из-за их тиражирования по цифровым хранилищам и практически вечны. Остается сожалеть, что все это происходит уже после таких мировых событий, как Пунические войны, легендарная осада греками Трои, европейские инквизиции и крестовые походы, наполеоновские войны, многочисленные гражданские войны, две мировые войны XX века, фашизм, сталинизм, колоссальные политические цензуры, в результате которых миллионами гибли уникальные рукописи, существовавшие в одном экземпляре и уже невозвратно потерянные для человечества.

Демократический доступ к уникальным источникам знаний дает право надеяться на то, что такие количественные показатели будут иметь развитие в совершенно иных статистически обусловленных качественных сторонах. А именно, возрастает роль тех умов, которые при уникальности ставших доступными источников, могут делать нестандартные аналитические выводы и получать новые научные результаты только за счет доступа к таким источникам. В научной среде существуют различные и неустойчивые мнения относительно возможностей для усвоения научного материала, записанного на различные типы носителей.

Ученые из Дартмутского колледжа установили зависимость качества восприятия информации от типа ее носителя. Исследованию подлежали молодые люди в возрасте от 20 до 24 лет. Для них степень восприятия текстового материала на бумажных носителях оказалась более чем в два раза выше, чем при использовании электронных текстов по критерию правильных ответов на контрольные вопросы по текстовому смыслу. Участники эксперимента, которые читали распеча-

танные тексты, в 1,4 раза лучше отвечали на логические вопросы, связанные с текстовым смыслом, имели более полное представление о картине прочитанного в целом, в то время как чтецам электронных текстов более запоминались отдельные детали. Результаты исследований весьма неблагоприятны для электронных средств считывания текстовой информации. Тем не менее, пользователи электронных текстов быстро адаптировались при обучении и улучшали свои результаты. Вывод, который делают ученые, заключается в следующем: цифровые устройства оказывают существенное влияние на качество работы с информацией, по сравнению с ее бумажными аналогами, что требует своего дополнительного осмысления.

Но это далеко не последние исследования в этой области, сам факт которых показывает, что они относятся к обеспечению безопасности человеческого мозга, генерации знаний и понимания значимости и эффективности того наследия, которое сегодня имеется в распоряжении человечества.

Отдельно следует рассмотреть преимущества и недостатки электронных средств в виде подписки периодических изданий. К первым относятся явные: агрегация больших информационных массивов; экономия денег на подписке, возможность работы с релевантными публикациями, тематические подборки материалов, наличие архивов, одновременный доступ неограниченного числа пользователей и др. Но немало и недостатков, затрудняющих работу с полнотекстовыми изданиями. Это выборочная представительность номеров печатных изданий, сложность поиска по ключевым словам, иногда присутствие устаревших текстовых форматов, отображений печатных версий, возможный психологический барьер, физиологическое несоответствие компьютерной техники, утомляемость при длительной работе на компьюте-

ре [32]. Все это умножается на растущие объемы информации, которыми пользуются в интернете.

В 2020 году всего около 4,5 млрд людей так или иначе пользовались интернетом. В развитых странах до 95 % молодежи не могут представить себе жизни без гаджетов. Для сравнения, в 2002 году таких пользователей в мире насчитывалось 380 млн человек. Динамика весьма высокая, чтобы не обращать внимания не только на положительные, но и на отрицательные качества, которые вносит в нашу жизнь всемирная паутина.

Самое простое и типичное перечисление пунктов вреда, который наносится интернетом обществу [46], включает:

– глобальную интернет-зависимость и уход от реальных проблем;

– биологические нарушения зрения, психики, статизм для организма;

– формирование специфической криминальной среды;

– потерю индивидуальности людей, вторжение в личное пространство каждого человека;

– наличие вредной информации и опасных последствий – порно, фейки, вирусы, насилие, кровь, дезинформация, незаконные финансовые операции и отъем денег;

– вынужденно-добровольное погружение в виртуальный мир, потеря общения, индивидуализация общества.

Добавим к этому постепенное и глубокое снижение гуманистической ценности и эмоционального наполнения информации.

Сегодня двести килобайт обычного письма, полученного по интернету, не вызовут у получателя тех эмоций и описаний, которые были увековечены Великим мастером пера, Львом Николаевичем Толстым в романе «Война и Мир». Речь идет о письме Николушки Ростова, написанном им домой после сражения при Кремсе (Австрия), в котором он принимал участие и во время которого был ранен. Сегодня

информация такого объема будет прочитана, освоена и «перекрыта» другой информацией, не менее важной и тоже сиюминутной.

Автор же романа потратил более четырех страниц драгоценного текста романа, чтобы описать всю гамму чувств, которые испытывали члены семейства Ростовых, в сотый раз перечитывая это трехстраничное письмо в присутствии детей, приживалок, друзей, знакомых, гувернеров, нянь, и графиня Ростова «… всякий раз с новым наслаждением и всякий раз открывала по этому письму новые добродетели в своем Николушке». Отец видел в письме гордость за своего сына, защитника отечества, юного офицера, мать была несчастна и счастлива одновременно, что сын жив и ранение не тяжелое, Соня сияла от счастья, что Николушка вспомнил о ней с любовью, Наташа гордилась братом-героем, Петя – по-хорошему завидовал брату-офицеру, каждый раз ставя себя на его место. Чтение и перечитывание занимало несколько дней. И эта масса чувств и эмоций была вызвана только одним письмом на нескольких страницах, это всего 150–200 современных килобайт информации. Но какой?

Вряд ли читатель сможет найти в современном информационном арсенале нечто, способное вызвать у него такой же эмоциональный всплеск или подобную информационную насыщенность. Двести килобайт информации. Их цена в современном информатизированном мире. Можно задаваться вопросом: что мы нашли в глобальном информационном пространстве и что мы потеряли?

Это далеко не полный перечень таких негативов. Существуют более локальные, но вполне конкретные опасности для отдельных людей и для общества в целом. Любой из известных видов опасностей, так или иначе, связывают с двумя причинами: искажением информации, ее фейковостью, ложью и с незащищенностью своих персональных данных,

В современных интернет-сетях каждый пользователь в 9-ти случаях из 10-ти остается один на один с проблемами безопасности своих персональных данных, с проблемами финансовой безопасности. Специалисты все чаще отмечают в связи с возрастающей преступностью в интернете, что опасности, появляющиеся в социальных сетях, прежде всего, ложатся на их пользователя. Пользователь сам решает, воспользоваться ему информацией из интернета или нет, допускать к ней сторонних участников или нет. И делает он это в полном осознании, что информация может быть не только фейковой, но и опасной в самых различных направлениях ее использования. Она может нанести вред самому пользователю. При ее трансляции дальше, она может нанести вред другим пользователям, независимо от желания первого пользователя.

Пользователь практически всегда сам несет ответственность за свои данные в интернете, за правильность опубликованного там материала. Мы давно ушли от такого понятия, как внешняя цензура. Трещит по швам доверие к банкам. С одной стороны, это форма публичности, демократичность системы, с другой – требует осторожности и серьезного недоверия к материалам из интернета к их объективности и достоверности, что существенно снижает эффективность пользования большими объемами информации.

Пользователь должен быть уверенным, что подаваемая им информация не будет использована против него. Необходимо внимательно следить за своей информацией в социальных сетях, в системах банковской информации и др. Например, если человек анонсирует будущую свою поездку, она может стать поводом для проникновения в его жилище в момент его отсутствия по данным его анонса.

Огромное количество тестовых программ, которые предлагаются в интернете, дают возможности для изучения общественного мнения, получения системы типа «обратная

связь» при принятии управленческого решения. Но этим же оружием пользуются и для выделения конфиденциальных данных о человеке, его финансового состояния, пользуются высказываниями в тестах, в частности, для формирования социального портрета, кошелька человека и получения аргументов для воздействия на него с целью киберограбления. Кроме того, не следует без повода принимать участие в сомнительных тестовых программах, поскольку, в частности, все эти тесты требуют доступа к аккаунту пользователя. Кроме того, частыми являются приписки о том, что сайт просит разрешения на размещения сообщений от имени пользователя.

Рекомендации об ограничении числа своих контактов, предупреждения о недопустимости указывать в профилях свои телефоны, адреса почты, тем более домашние адреса и др. явно не лишние в таких ситуациях. И многие сайты в социальных сетях уже сегодня представляют определенные услуги по ограничению доступа к персональным данным своих пользователей, обеспечивая, таким образом, их безопасность от преступного элемента в информационном пространстве.

Продолжительное нахождение пользователя под давлением указанных выше факторов постепенно приводит к проявлению опасностей психического характера. Зависимость от социальных сетей в мире уже признается в качестве заболевания. Постепенно открываются специализированные клиники для таких пациентов, лечение которых проводится методами, аналогичными тем, которые применяются для лечения нарко- или алкогольной зависимости.

При этом способы выведения из зависимого состояния, по совместному мнению врачей из Алжира, Норвегии, сопоставимы с кокаиновой зависимостью [48]. По крайней мере, при присутствии такого человека в социальных сетях имело место повышение активности тех же нейронных центров в мозге, что и при потреблении кокаина. Лечение сводится к

психотерапевтическому переключению внимания от виртуального мироощущения на реальное и медикаментозному воздействию на такие центры.

В своей книге «Десять аргументов в пользу того, чтобы удалить свои аккаунты в соцсетях прямо сейчас», ее автор, Джарон Ланье утверждает, что социальные сети способны подавлять волю пользователя, вынуждают расставаться с многими общечеловеческим качествами, такими как свобода воли, сопереживание, постижение истины, подавляют воображение и вообще аналитические процессы, что уже само по себе представляет угрозу всему человечеству, если, конечно общество не пересмотрит свое отношение к творчеству в пользу автоматов. Изначальная ориентация социальных сетей как полезных инструментов для общества постепенно перерождается в свою противоположность, заставляя людей становиться поставщиками и обработчиками данных для таких сетей. В результате, данные о самом человеке, улавливаемые каждую минуту, становятся базой для свободного доступа, нарушая право на индивидуальность.

Современные дети уже получили собственное структурирование на *Z*-субъектов и на *Y*-субъектов. К первым относят молодежь от 10 до 24 лет, ко вторым – дети до 10 лет от роду. Доктор Дж. Тейлор считает, что этим группам молодежи свойственны такие качества, как клиповость, неспособность к сосредоточению, способность постоянного отвлечения на любой внешний фактор, привыкание к собственному виртуальному миру, внутренняя зависимость. Это так называемые механизмы *BUMMER* (сокращение от *Behaviors of Users Modified*, *and Made into an Empire for Rent* – «поведение пользователей изменено и сдано в аренду империи». Под империями понимаются *Google*, *Facebook*) [49].

Как результат, молодежь с трудом концентрирует свое внимание на каком-то одном объекте в силу виртуальной отвлеченности и сталкивается с такими следствиями, как поте-

ря способности к анализу прочитанного, запоминанию, выражению своего мнения о предмете обсуждения. Теряются способности к критическому мышлению. В среднем, подростки способны выдерживать концентрацию мысли не более, чем на полминуты [50]. Теряются навыки чтения.

Неприятности и опасности сопровождают человека – пользователя продуктами глобального информационного пространства на всем протяжении такого общения. С одними из этих проблем следует усиленно бороться, так как они антагонистичны как для всего общества в целом, так и для отдельного человека. По отношению к другим вызовам необходимо адаптироваться, изменять многие, ранее считавшиеся незыблемыми социальные, экономические и другие устои, подстраиваться к таким изменениям, если они являются основополагающими для развития современного общества. Это непростой путь, в котором научные знания в области кибернетической безопасности будут крайне актуальными.

1.4 Глобальное информационное пространство как социальная ниша для современного человека

Глобальное информационное пространство обладает одним важным качеством. Оно практически не признает границ. В любой стране существуют поисковые системы, социальные сети, существуют средства коммуникаций американцев с японцами, африканцев с азиатами, россиян с украинцами. За небольшим исключением, например, в Китае, который ограничивает доступ иностранных поисковиков и сайтов в рамках проекта «Золотой щит» и защищает свое информационное пространство от мировых сетей, заменив их своими контентами, это так. Тем не менее, даже закрытый Китай не отказывается от пользования поисковиками *Google*, *Yahoo*,

Bing, отфильтровывая результаты поиска технических и экономических новинок мировой информационной сети, потому что эта информация является крайне полезной для китайской экономики и отказываться от нее в масштабах государственной политики Поднебесная не хочет.

Информация и ранее никогда не удерживалась в рамках границ одного государства. Разве сохранили китайцы секреты производства шелковой нити в IV–V веке, либо Южная Америка удержала в тайне секрет получения каучука и ростки каучукового дерева, или африканские колонизаторы – секреты выращивания какао-бобов? Все секретное когда-нибудь становится явным. Это знали разведчики или шпионы (как кому нравится) всех крупных держав мира. И не в наше время, а значительно раньше. Любое новое вооружение могло держаться в тайне до первой битвы, а затем его перенимали страны-соседи. Никакие тайны не смогли удержать знания об атомном оружии у монополиста. Постепенно атомное оружие, как средство для гарантий ненападения, появилось в других странах. Информацию трудно удержать. Об этом писал еще Норберт Винер, отец современной кибернетики.

Так что такое сегодня глобальное информационное пространство, где его реальные границы, кому оно принадлежит, с кого можно спросить, кому пожаловаться? Отсутствие существенной регламентации условий существований человека в этой системе – это совершенно новое состояние нашего общества, которое позволяет определять это пространство как специфическую социальную нишу для любого человека, даже если он не является участником ГИП, интернета, а только опосредованно пользуется его преимуществами в магазине, в поезде, при оформлении социальных документов, поездках в отпуск по туристическим путевкам. Подобная ниша весьма расплывчата, многообразна и полифункциональна, что делает ее трудно узнаваемой. Только то-

гда, когда отдельный человек попадает в область интернет-зависимости либо в руки киберпреступников, либо теряет свою идентичность как личность из-за расшифрования его персональных данных, он начинает искать защиты не в этом кибернетическом пространстве, а у самого общества, помимо самих источников этих опасностей.

Отсутствие границ, массовость информации, а также полная ликвидация какой-либо цензуры, дало основания для распространения в этом пространстве огромного количества искажений и изменений в социальном устройстве нашего общества [41, 51, 52]. А отсутствие, например, защиты персональных данных, вместе с перечисленными ранее проблемами, если пока и не ограничивает число пользователей, то снижает содержательную часть информационного пространства. Что, в свою очередь, умаляет общую ценность совокупного ресурса информационного поля, делает его в определенной мере проблемным для миллионов пользователей. Но, самое главное, это источник социального дискомфорта и психологического напряжения для таких людей.

Самый простой пример. С целью унификации налогообложения для каждого члена общества вводятся идентификационные номера. Как обоснование борьбы с международным терроризмом, вводятся электронные паспорта, «универсальные карты» с биометрическими данными на каждого человека. Если паспорт, как бумажный носитель, существует в единичном экземпляре, то электронный паспорт или универсальная карта имеют особенность кочевать по различным электронным базам данных и попадать в ненужные руки [32]. Все эти данные сведены в единую международную электронную структуру и могут использоваться всеми странами мира. Тем более, если подобные электронные базы данных попадают в руки криминалитета. Даже сегодня на рынке можно свободно купить недорого базы данных и служебную информацию, например, с паспортных столов практически

всех областей нашей страны, информацию, скачанную с серверов министерств и ведомств не только Украины, но и многих других стран. Размеры «цифрового портретирования» среднестатистического человека (объем информации о нем), создаваемые за день, превышают объем информации, которую за это время создает сам человек. Сегодня около 45 % подобной информации в интернете нуждается в полной защите [53]. Подобные базы данных при определенных обстоятельствах несут угрозу любому человеку, угрозу его социальной безопасности [54]. В основе ее лежит «прозрачность» жизни любого человека, что само по себе противоречит основополагающим документам ООН о правах человека на защиту своей индивидуальности от внешнего посягательства, противоречит конституциям большинства государств, противоречит самому факту существования человека, как индивида в обществе себе подобных. Ведь даже стремление человека к собственному, отдельному жилью, к отдельной комнате, кабинету диктуется потребностями не только в физической, но и социальной безопасности. Не удивительно, что даже сам факт тайного прослушивания телефонных разговоров признается далеко не правомочным действием не потому, что при этом выдаются какие-либо секреты, а своим вмешательством в личную жизнь человека, в его социальную безопасность.

В 2016 году профессор Бернс из США экспериментально установил, что мобильные дополнения к *Facebook* способны обеспечивать тотальное прослушивание разговоров пользователями смартфонов. Дополнение используется пока только для того, чтобы выводить рекламу на наиболее важные разговоры клиентов [55]. В этом же году немецким телеканалом *Norddeutscher Rundfunk* (*NDR*) опубликована информация, согласно которой известный браузерный плагин *Web of Trust* (*WoT*), которым пользуются почти 140 млн пользователей, был уличен в слежке за многими своими кли-

ентами и продаже конфиденциальной информации (в том числе, финансовые и коммерческие секреты, результаты отдельных полицейских расследований, интимная жизнь госслужащих) третьим лицам [56]. Оплата таких услуг превышает официальный доход самой сетевой компании. В результате от услуг плагина отказались такие браузеры, как *Mozilla Firebox*, *Opera*, *Google Chrome*. Подобные случаи еще раз демонстрируют факт незащищенности цифровой информации о субъектах пользования в сетях самого разного уровня.

В 2020 году популярный сервис *ZOOM* оказался под шквалом критики за то, что записанные в нем разговоры, контакты, даже видеоконференции и приватные разговоры оказались в свободном доступе, и конфиденциальная информация свободно растеклась по интернету. Учитывая, что только в течение одного дня сервером пользуются не менее 20 млн людей, утечка весьма болезненная для защиты персональных данных. Приватная компания *Zoom Video Communications* и раньше торговала персональными данными, в частности, для пополнения информационных ресурсов *Facebook*. В *Facebook* появился новый вид мошенничества, связанный с созданием идентичных профилей для заявки на дружбу с последующими «просьбами денег» от друзей, проникновением в личную информацию, в особенности для доступа к индивидуальным данным: паролям, счетам. Отследить липовые профили в аккаунтах весьма сложно [57].

Можно только перечислить некоторые другие направления, которые приходят в социальный уклад человека благодаря ГИП. В частности, это принципы трансгуманизма [58, 59], вмешательство в биоинформационную среду человека, направления на создание пост-человека за счет расширения его способностей, перемещения его физиологического разума и эмоций в имплантируемые цифровые носители (об этом уже говорят в научной среде, заказываются подобные исследования). Сошлемся и на нано-био-информационные комму-

никативные технологии (НБИК-технологии), целью которых является изменение форм сознания человека [59]. Подобные исследования уже проводятся по заказу Национального Научного Фонда США с 2002 г. В частности, результаты таких исследований лежат в основе уже имеющихся патентов, например, [61]. Технически возможно осуществлять лазерное маркирование лба и наносить невидимые для глаза метки типа штрих-код.

Важным качеством интернета становится потенциальная возможность достижения взаимного биофизического сращивания пользователя и сети посредством вживления микрочипов в человеческие органы с последующей непрерывной передачей информации о пользователе в некоторые базы данных. Например, Мексика стала одной из первых стран по массовому вживлению микрочиповых имплантантов. В 2014 году таковых в стране было уже 58 тыс. Развитие этого направления идет по двум взаимодополняющим направлениям: миниатюризация и расширение функциональности [62].

В компании И. Маска разрабатывается технология нейрокомпьютерной интеграции (*neural lace*). Имеется информация о разработке новых коммуникационных возможностей биологического интернета (*Bi-Fi*), в основе которого, в частности, прямая загрузка информации в мозг человека и его подключение в сеть на биологическом уровне посредством биологических клеток организма человека. А также, связанная с ней технология получения глазных линз, которые вживляются через глазную жидкость в глаз человека, врастают туда в виде экрана, подключаемого к сети. Такие технологии, основанные на прямой загрузке информации в мозг, без участия естественных органы чувств человека, находят применение в современной медицине для слепых и глухих людей.

Имеющиеся уже сегодня, социально невозможные, методы позволяют осуществлять технотронный контроль за денежными потоками не только отдельных банков, но и каждого человека через его электронные карточки. Данные на каждого неблагонадежного человека могут заноситься в определенные ограничительные базы типа *Stop-List* (электронные черные списки), ограничивающие некоторые виды активности конкретного человека. И этим уже пользуются в самых различных целях: правительства, отслеживая должников, неплательщиков налогов, алиментов, а также криминал, отслеживая финансовые потоки приватных лиц и компаний, грабители, воры-домушники и многие другие.

Можно сослаться на исследования по сингулярности, как области предсказуемого сращивания, синтеза человека с компьютером, первоначальная цель которых состоит в синхронизации поисковых компьютерных систем с эмоциональным фоном человека и возникновении суперразума [63]. Украина устойчиво идет в фарватере подобных глобалистических процессов. По крайней мере, закон № 1049 «О едином демографическом реестре», принятый Верховной Радой Украины 02.10.2012, говорит об этом однозначно. В стране уже появились потребители этого закона. В частности, приватный консорциум «ЭДАПС» уже сегодня претендует на гарантированное законом право формирования тотальной базы электронных данных на всех жителей страны, по наперед заданному реестру, который позволит ему контролировать каждого гражданина не только из живущих в Украине 42 млн, но и тех, кто ушел из жизни. И это не государственная, это частная компания!

Единый государственный реестр – потенциальное поле деятельности для вымогателей, всех, кто желает посчитаться с конкурентом по бизнесу, электронных воров, рейдеров, черных риелторов, может служить системой тотальной слежки.

Следом за интернетом последовало появление глобальных управляющих сетей. Уже сегодня *Google* через свои поисковые системы удерживает данные, по разным источникам, на 2,5–3,3 млрд людей, контролирует большую часть мировой экономической и технологической информации [64]. Первоначальная благая цель такого управления – контроль за поддержанием жизнедеятельности человека, повышение качества жизни посредством прямого беспроводного контакта мозга с окружающей информационной средой, транспортом, финансовыми и технологическими системами. Возможная конечная цель – единая система управления человечеством. Система, с возможностями подчинения себе индивидуального разума каждого, влияющая на него вне зависимости от желания индивида.

В составе глобального информационного общества уже появились понятия *E-government*, *E*-управление. Это аббревиатуры, которые расшифровываются как электронные правительства. Это модное и весьма актуальное *IT*-изобретение уже нашло применение в таких странах, как Сингапур, США (проект *FirstGov*, сливший воедино около 20 тысяч электронных сайтов департаментов страны), Великобритания, Эстония и даже Молдова, которая с 2010 года начала внедрение электронного правительства в своей стране. Система позволяет на трех уровнях: *G*2*C* – «правительство гражданам»; *G*2*B* – «правительство бизнесу»; *G*2*G* – «правительство правительству» осуществлять огромный перечень услуг и решений, которые ранее выполнялись только в присутствии клиента или только в бумажном варианте, требующем согласований, подписей, длительного «хождения по кабинетам».

Выгода заключается в том, что заходя в сервер соответствующего правительственного раздела, можно без волокиты зарегистрировать брак, получить в электронном виде любую справку, направить заявление в полицию, оформить любую лицензию, открыть за пару часов новый бизнес, провести

любую тендерную процедуру, избавив клиентов от коррупционных схем, заплатить налоги, участвовать в бюджетном управлении государства или местности и т. д. Повышается степень общественного контроля над работой правительства. При этом экономится бюджет, собственное время клиента, его нервы, упрощается ведение документооборота между ведомствами, повышается качество управления госаппаратом, уменьшается число чиновников и т. д. Все это делает многих граждан активными сторонниками такой электронной системы. Если бы не одно «но»... Оно заключается в том, что для функционирования всей системы *E-government* требуется огромное количество баз индивидуальных данных на каждого члена общества. Но и в этом нет ничего страшного, если эти базы данных были надежно защищены. В противном случае, огромные массивы данных о каждом из нас могут оказаться в нечистоплотных руках.

Зададим себе вопрос: как мы отнесемся к тому, что Ваши потенциальные «любознатели» будут иметь информацию о Вашем здоровье, о результатах Ваших анализов? Как будет воспринята Вами открытая информация не только об адресе проживания, но и обо всех ваших родственниках? О заплаченных налогах и о динамике Ваших приобретений и покупок. О кодах Ваших электронных документов, в том числе, финансовых. А как же все это будет согласовываться с правами личности, с тем, что записано в конституциях большинства правовых государств? Речь идет об оцифровывании практически всех индивидуальных данных о каждом гражданине страны. С возможной утечкой этих данных в свободную информационную сеть. Ведь гарантий на конфиденциальность никто давать не может. По крайней мере, пока не будут работать так называемые квантовые компьютеры, любая информация в которых по замыслу вообще не может быть вскрыта без искажения. То есть варианты имеются, но для этого нужно то, чего еще человечество не придумало. В ли-

тературе прямо показано, что на сегодня более 90 % утекающей из сетей информации – это персональные данные, которые воруются с целью последующей перепродажи [64].

И это только первичный уровень информации, которую можно скачать. Но есть еще и вторичный уровень, который получается в результате аналитической обработки первичной информации. К ней относятся балансы предприятий и компаний, фонды оплаты труда, конфиденциальные источники доходов, источники информации, штаты и налоги, договоры и соглашения, многие из которых носят строго не разглашаемый характер, все то, что составляет коммерческую тайну любой компании, предприятия.

Самое интересное может произойти с системой электронных подписей субъектов этих баз данных, которая должна быть неотъемлемой составляющей *E-goverment*, начиная с членов правительства, подписи которых «стоят» крайне дорого для специфического контингента, и кончая рядовыми гражданами, для которых оцифрованная подпись, в случае ее электронного взлома, означает доступ к любым злоупотреблениям, в сравнении с которыми современные хакеры покажутся учениками средних школ. Речь идет о провоцировании совершенно нового типа преступлений и формировании специфической криминальной среды в обществе.

Как видим, проблема пока находится только в области умения хранить безопасность баз данных. Эта проблема может найти свое решение.

Все? Нет. Не следует забывать о том, что глобальные базы данных являются и основой для злоупотреблений самим *E-government*, то есть электронным правительством. Это самый прямой путь для глобального контроля практически за каждым членом общества, за способом их жизни. А это уже угроза экосистеме под названием «человек и общество». Подобные эксперименты могут иметь непредсказуемые соци-

альные последствия, с чем уже будет невозможно не считаться.

Глобальное информационное пространство своеобразно, но очень активно влияет на политические процессы в мире. Причина кроется именно в глобальности этого явления, которое не знает государственных границ и в этом смысле противоречит самому понятию «государство». Общество становится перед выбором: всеобщее киберпространство или информационный суверенитет. Отдельные страны защищают свои границы от проникновения внешних информационных потоков. Например, Китай весьма ревниво относится к собственной версии интернета. Допуск к иностранным сайтам ограничивается государственной цензурой. Все веб-страницы подлежат сортировке по ключевым словам, что делает недоступным любой материал, представляющий опасность для государственной идеологии. Крупнейшие зарубежные поисковые системы типа *Google*, *Microsoft*, *Yahoo* вынуждены следовать этим правилам в обмен на доступ к китайскому рынку. Вся информационная продукция собственного производства подлежит обязательной регистрации, что облегчает доступ к ее контролю.

Но это единичные случаи. Чаще всего интернациональное киберпространство является причиной не только политических недоразумений и конфликтов, но уже и поводом к военным столкновениям. Технически сейчас все это возможно. Тогда война может переместиться в область виртуальных ресурсов, но с вполне конкретными результатами для противоборствующих сторон. Это и глушение чужих информационных средств, и введение налагаемых активных сигналов с целью доставки идеологической информации на территорию противника, и блокирование работы электронных боевых средств противника, и многое другое. Многие государства уже сегодня ставят кибернетические опасности даже более острой проблемой, чем международный терроризм. В ре-

зультате появляются военные структуры, занимающиеся защитой военных компьютерных сетей, собственной информации. При этом четких линий стратегии кибероборонных мероприятий пока не создано ни в одной стране мира.

На июльском 2016 года саммите НАТО в Варшаве уже был поставлен вопрос о противодействии кибератакам на информационные сети этой международной организации, что в соответствии со статьей 5 Вашингтонского договора будет считаться фактом нападения на весь Атлантический блок. Это может накладывать на многие государства необоснованную ответственность за любые хакерские атаки на соседние страны. Например, хакерские атаки в 2007 году на систему электронного правительства Эстонии принесли этой стране многомиллионные убытки и могли стать причиной военного конфликта между НАТО и Россией, по принадлежности инициативы этих атак.

Велика роль интернета и в разжигании современных межэтнических конфликтов. Это тема отдельного подробного исследования. Достаточно сказать, что поводом для концентрации боевиков из многих стран на пространстве ИГИЛ в 2015 году стало именно огромное количество видеороликов и фотографий с изображениями пыток, изнасилований, убийств детей и женщин, сброшенных в интернет джихадистами. При этом никакой реакции мирового сообщества на такую информацию в свободных сетях, как правило, нет. Интернет и сегодня является держателем многих конфиденциальных данных секретного характера для различных секретных экстремистских группировок. Это развязывает руки террористам всех мастей, делает их поступки геройскими, подражательными для тех, кого называют садистами и кому нет места в цивилизованном мире. Это одна из причин концентрации на этих территориях таких субъектов. Современные социальные сети уже ставят перед своими пользователями задачу распознавания «языка вражды» и создания законода-

тельных и чисто программных продуктов, позволяющих «фильтровать» и не допускать разжигание ненависти между пользователями, ксенофобию в сетевых контактах, включая как прямые оскорбления, так и завуалированные выражения [66].

Не отстают от информационного прогресса и милитаристы всех уровней. Глобальное информационное пространство представляет собой идеальный случай создания системы тотальной слежки, тотального контроля за почти любыми сегментами общества. Современное ГИП – это всеохватывающее «энергетическое» поле, в котором, в той или иной степени, задействовано почти все население планеты, там большинство персональных данных каждого из нас, там большая часть самой секретной информации о деятельности правительств, крупных и малых компаний, личные переписки и простых людей, и лидеров государств. Разве можно допустить, что военные люди смогут пройти мимо такого ресурса, способного при известной изворотливости ума доставить обществу столько неприятностей, сколько их по пространственному охвату, по глубине влияния не может представить даже ядерная бомба?

Можно утверждать, что на Земле уже давно ведутся так называемые цифровые войны. Больших или меньших масштабов, но они существуют. В них появляются победители и побежденные, эти войны дают преимущества в политике своим государствам. Сегодня цифровые войны уже действительность. Пока неузаконенная.

В 2016 году, уже после разоблачений Э. Сноудена в 2013 году, в печать поступили сведения о всеобъемлющих архивах существующего кибервооружения, находящегося в арсенале АНБ США, где уже сейчас над ним трудятся почти 2000 специалистов. Сама по себе такая утечка, в равной степени, как и информация Э. Сноудена, не является чем-нибудь из рук вон выходящим. В море информации трудно

что-либо утаить, по крайней мере, на некотором протяженном временном отрезке.

В частности, к такому оружию относятся так называемые уязвимости нулевого дня, программы-имплантанты, не имеющие на сей день противодействия, которые способны обнулить нужные программные продукты в системах *Cisco*, *Huawei*, *Juniper* и др. в самой различной последовательности и выборочности.

Агентство Национальной Безопасности США, наиболее технически продвинутая спецслужба в мире, активно сотрудничает с главными поставщиками информации – компаниями *Google*, *Yahoo*, *Microsoft*, *Facebook* и др. Китай, например, уже несколько лет назад отмежевался от традиционных форм сотрудничества с этими компаниями только по причине обеспечения своей кибербезопасности. Китайцы стали массово отказываться от услуг американских вендоров *Cisco*, *Juniper* в пользу подобного китайского массового продукта файрвола *TopSec*, по своим масштабам уже сейчас сравнимого с *Huawei*, но который не известен широкому пользователю в мире. Китайцы принципиально ограничивают свой бизнес от проникновения американского программного продукта, стараясь разрабатывать собственные аналогии, и имеют от этого свои дивиденды как в экономическом, так и в политическом плане. Показательно, что одной из декларируемых задач АНБ на сегодня является агрессивный поиск критических уязвимостей подобных китайских систем.

Американские специалисты пытаются кодировать все более или менее значимое программное обеспечение, существующее в мире. Цель – систематизировать основные уязвимости и создать собственную секретную паутину для их выборочного обнуления. Причем, ни разу специалисты АНБ не ставили в известность компании-производители такого продукта об их уязвимости. Весной 2016 года несколько вендоров, в частности, *Fortinet*, *Cisco*, *Juniper,* объявили о зави-

симости своих программных продуктов от уязвимостей из внезапно опубликованных каталогов АНБ США. Причем, возраст некоторых уязвимостей измерялся несколькими годами. Напрашивается вывод о целевом направлении таких работ в АНБ – реализация секретных планов тотального контроля и слежки в глобальном информационном пространстве. Причем, если даже ФБР США подотчетна суду, то АНБ выведена из-под судебной юрисдикции. Почему?

Техническая разведка США сегодня обладает самым эффективным арсеналом средств для ведения разнообразных атакующих действий против любой информационной системы в мире. Такое кибероружие обладает широкой функциональностью. Одно из них, в частности, вирус *Stuxnet*, позволило американцам в 2006 году приостановить иранскую ядерную программу обогащения урана. Вирус предназначен для поражения системы управления завода по обогащению урана в г. Натанзе. Программа маскировала штатные режимы работы центрифуг, в то время, как они одна за другой выходили из строя. Предварительно эта программа тестировалась на подобных центрифугах, доставшихся американцам от режима Каддафи из Ливии. В результате иранская ядерная программа была заторможена на годы.

Администрация киберпространства Китая на протяжении многих лет проводит проверку продаваемых мобильных устройств Apple, якобы по подозрению в шпионаже. На самом деле, Китай системно заставляет компанию поделиться секретами своих технологий в обмен на доступ к китайскому рынку средств коммуникаций, который является на сегодня вторым в мире по емкости. Этим страна обеспечивает собственную кибербезопасность [67].

Кибероружие успешно используется соответствующим службами США, Великобритании, Израиля в своих операциях уже несколько лет. Пентагон в 2006 году объявил о создании в своем составе отдельного киберкомандования для ко-

ординации и управления кибервооружениями, эффективность которых, по мнению создателей, превышает эффективность бомб и многих чисто военных операций. Эту цепь развития можно продолжать еще долго. Чем это может закончиться? В частности, это относится к функциям военной и промышленной разведок, получению скрытой информации путем считывания с цифровых носителей, агентурной вербовки путем манипулирования персональными данными человека, применению современных систем обработки информации, внедрению технологий цифрового обучения методам подавления средств активного воздействия на население и др.

С развитием известной немецкой концепции четвертой научной революции «Индустрия 4.0» становится все более приемлемой и стратегия «Общество 5.0» [68]. Она впервые принята правительством Японии в качестве стратегии государства в области *dg*-технологий, которая связана в равных долях и с производственными секторами экономики, и с решением социальных проблем в области глобального информационного пространства, и интернет-технологий, как отображения социальной ниши для человека.

Попробуем пофантазировать. Человечеству уже в недалеком будущем, имея в арсенале инструменты, подобные ГИП, по силам создать некий электронный разум, позволяющий решать определенный круг этических и нравственных задач относительно самого человека. Таким образом, например, можно разрешить вечное противоречие, свойственное роду человеческому, противоречие между его возможностями и потребностями, между способностями и неуемными желаниями.

Собственно, государство было придумано человечеством именно для того, чтобы каждый его член соизмерял свои потребности с интересами всего общества. И система государственных правовых норм призвана искусственно ограни-

чивать противоречия между потребностями и возможностями каждого члена общества, приводя их к некоторому общему знаменателю (насколько эффективно, судить истории). Сам человек, в силу своих биологических привычек, как и любое другое существо, живущее на этой планете, не способен преодолевать многие нравственные пороки, такие как «не убий», «не укради» и т. д., потому что они противоречат процессу естественного отбора. И если для хищника не существует нравственной проблемы, например, «убить – не убить жертву », то для человека, наделенного разумом, эта проблема крайне актуальна и является причиной многих противоречий и вопросов. Самому человеку с ними не справиться и не пресечь системные качества, заданные природой и придуманные разумом и обществом. А вот альтернативный компьютерный ум сможет справиться с этой задачей. Справиться помимо человека, поставив его поступки в подчинение таким своим решениям. Глобальное информационное пространство позволяет человеку, в некотором временном интервале, привыкнуть к такой парадигме. А это же путь к безнравственности, то есть в ту сферу, в которой человек всегда отличался от любого другого животного.

Только это будет уже иная цивилизация. Не человеческая. Или не совсем человеческая. Такая модель, в принципе, имеет право на существование даже не как гипотетическая. По крайней мере, общество показывает свое согласие с ней, в частности, своим подпаданием под глобальное информационное пространство. Подобная модель еще раз подчеркивает одновременную пропасть между глобальными информационными пространствами и слабо подготовленным к этому обществом, с одной стороны, и тонкую границу, отделяющую человечество от проникновения в его среду самых разных кибернетических систем, в частности, систем с четкой логикой, с другой стороны. И это может оказаться началом

совершенно неизвестных «мутаций» человечества в сторону иного, совершенно рационального разума.

Итак, сформировавшееся глобальное информационное пространство обещает человеку доступ к почти любым по объему и легко доступным источникам информации. Но при этом социальная безопасность человека, его объективная биологическая психика, способности к гармоничному развитию подвергаются определенной и серьезной опасности. Мы являемся свидетелями появления виртуального мира, привлекательного, интересного, познавательного, но и опасного для психики человека, в особенности, молодежи. За счет информационной вседозволенности и недостоверности получаемой информации, неспособности человеком «перерабатывать избыточную информацию», происходит снижение его способностей к аналитическому восприятию и творческой переработке информации (в особенности в научном мире). Как следствие, в жизни людей, далеко не спонтанно, появляются новые формы тотального информационного контроля и специфические качества, присущие глобальному управлению в обществе. И, безусловно, негативным фактором является появление новых видов преступлений, рост интернет-преступности, перед которой пока пасуют не только обычные граждане, но и правительства, страны, общество в целом [32].

Для каждого государства, для каждой экономической системы, для каждой компании, для каждого субъекта общества существует и ждет своего решения проблема защиты собственного информационного ресурса от внешнего нежелательного проникновения. Современная наука возлагает свои надежды в решении этого вопроса на так называемые квантовые когерентные компьютеры (ККК), в основе которых – считывание информации только пользователем основного уровня. Внедрение в базы данных сторонних пользователей по принципу, заложенному в ККК, ведет к уничтоже-

нию такой информации. Все эти факторы несут как прямую, так и опосредованную системную угрозу биологическому и социальному благополучию человека. Так что же такое интернет-пространство в экосистеме человека – благо или ущерб? Истина, как всегда, находится посередине. Не такие простые отношения ожидают наше общество в сравнении с глобальным информационным пространством, которое формируется самим же этим обществом. Мы видим, что в той социальной нише, которую человек сам себе приготовил, в виде глобального информационного пространства, его ожидает еще немало сюрпризов, которые или придется преодолевать, находя новые решения проблем, или отказываться от таких ниш, в пользу более адаптируемых под нашу социальную систему, потому что с прогрессом спорить очень трудно.

II

Социальность и кибербезопасность

2.1 Некоторые качества стадности и ее опасности в современном информационном сообществе

Постепенные изменения в социальности современного общества также, в определенной степени, зависят от влияния глобального информационного пространства. Наше «цифровое» общество постепенно приобретает новые качества, которые, наряду с позитивом, заложенным в нем, представляют, в некотором смысле, и угрозу – для человека, для сообщества людей в целом

На первый взгляд, компьютеризация, отход от личного общения в пользу виртуальности – это путь к индивидуализации в обществе. Однако, можно осторожно утверждать и то, что с развитием цифровых технологий, постепенным и повсеместным интегрированием их в повседневную жизнь человека в виде сетевого продукта, появления новых способов общения, коммуникативных связей и технологий, средств индивидуальной поддержки этих сетей, общество снова начинает приобретать давно забытые и условные качества стадности, только на ином, более развитом, витке своей истории. В этом качестве уживаются и положительные моменты, связанные с развитием коллективизма у людей. Это новые качественные свойства позволяют человеку получать весьма неожиданные социальные блага. Но они не изменяют своей предметной направленности.

Существует обратная сторона современного стадного эффекта, проявляемого через глобальные информационные

системы в обществе. И она может представлять угрозу для многих областей человеческой деятельности, в том числе, профессиональной, творческой, то есть там, где требуется индивидуальный подход, там, где необходимо проявление личных качеств человека. И не только. К ним относятся и такие неожиданные метаморфозы, как вновь проявляемые свойства всеобщей стадности, группирование по инстинктам, а не по смыслу или содержанию. Такие неожиданные изменения пока не очень заметны, но они уже проявляются через результативность массовых коммуникаций, формы массового общения, группирование по предпочтениям индивидов и их интересам. На первый взгляд, многочисленные работы в области развития индивидуализации личности говорят о противоположном [1, 2, 3, 4, 5]. Тем не менее, существуют многие интересные данные [6] и исследования [7, 8], которые, по существу, не противоречат им, но дают возможность оценить и другую, более опасную для человека, сторону этого явления.

Сегодня стадный эффект не несет в себе функции физической или социальной безопасности, как это было тысячелетиями назад. Зачем же он нужен человеку сегодня? Следует отличать стадность и коллективизм, термины, которые несут различную смысловую нагрузку. Под стадностью понимается некоторый механизм, лежащий в основе инстинкта самосохранения человека. Современная интерпретация добавляет к этому еще способность человека проявлять интуитивные качества неосознаваемого аналогизма в общении. Коллективизм – это осознанное главенство интересов группы людей над интересами отдельной личности, признающей приоритет общественного блага над личным и добровольно подчиняющей свои интересы интересам общества [9].

В преддверии когнитивной революции, человек обладал стадными инстинктами, без которых 20 тысяч и более лет назад ему было не выжить. Но тогда *sapiens* был далек от

мыслительных и творческих процессов, от научного созидания. Стадные инстинкты того уровня оберегали каждого члена такого общества от врагов, давали пищу, общие для всех блага, возможности для размножения. Стадные эффекты были основой для обеспечения безопасности: физической, социальной. Несмотря на то, что лидеры общества и в те времена отличались своими ярко выраженными индивидуальными качествами, отличающими их от других индивидов, субъектов общества. Лидер, как правило, силен индивидуально, максимально независим или стремится к независимости: моральной, физической. Только высокая индивидуальность делала субъекта настоящим лидером в «стаде». И это был путь к индивидуализации на многие века. Количество лидеров увеличивалось пропорционально появлению новых иерархически зависимых областей деятельности, экономики, самого социума. Этому способствовала и дифференциация наиболее активных людей по уровням лидерства, и воспитание индивидуальности в каждом человеке.

Сегодня качества, приобретенные человеком за многие тысячелетия, такие как индивидуальность, способность к мышлению, логике, рассуждению, альтернативности суждений, аналитическим выводам, и связанные с этим системные знания, абсолютно противоречат прежним стадным инстинктам.

Тем не менее, стадные инстинкты в обществе начинают проявляться с другой стороны. Не нужно считать, что стадные инстинкты ушли из нашей жизни навсегда. По данным исследований в университете г. Лидса, 95 % современных людей проявляют стадные качества, в частности, делают «как все», «как всегда», стараются «не отличаться, не выделяться» и т. д. Все это не ново и нам хорошо знакомо. Фактор стадности присутствует в интернете [10], и оспаривать это бессмысленно.

Со стороны сформированного сегодня глобального информационного пространства, это, в частности, унификация и доступность информации о каждом человеке, унификация правил поведения человека в глобальном информационном пространстве, вне зависимости от страны проживания, религии, национальности, профессиональности и др. Поскольку стадный инстинкт лежит в основе инстинкта самосохранения, одно из проявлений последнего в условиях глобального информационного пространства связано с интуитивной потребностью защитить свое индивидуальное пространство от внешнего проникновения.

В современном глобальном информационном пространстве пока нет защиты от массового произвола информации. И в этом неиссякаемом информационном потоке сосредотачивается для общего пользования информация о каждом его члене. «Все про всех». Эта модель является подосновой для проявления отдельных стадных инстинктов, например, неосознанных действий, интуиции в ходе системного информационного взаимодействия. Этому же способствует гипертрофированное стремление к «коллективному» творчеству в не самых качественных его проявлениях в интернет-сетях.

Эффект принятия решений там, где доминирует стадное мышление, весьма искажается, что не может обезопасить результат от ошибок или опасных решений, приводящих к непоправимым последствиям в любых системах: экономических, производственных, государственных, социальных. Любой проект решения сталкивается с дилеммой: а что об этом подумают другие участники? На основании экспериментов, проведенных с группами пользователей, занятых принятием решений в экономической сфере, авторы [11] отмечают: «Проблема с просмотром чужой информации заключается в том, что люди склонны к стаду с другими». Под «другими» понимались те участники эксперимента, варианты принятия

решений которых были открыты для всех остальных, и они ими пользовались, обращаясь к этим «другим», как к арбитрам, для своих собственных вариантов решений. Элемент стадного эффекта в мышлении налицо. Придуман даже так называемый эффект Рингельмана, показывающий, что творчество в команде и творчество индивидуальное существенно отличаются в пользу первого [12]. Причина состоит и в распылении ответственности, и в подавлении инициативы, и в снижении координации, приводящей к результату.

Это способы проявления искаженной активности в глобальном информационном пространстве, настолько, насколько оно позволительно самим пространством. Схемы проявления стадных качеств повторяются на более высоком уровне развития общества, и форма их проявления, и унифицированный алгоритм не изменяется. Безусловно, конечный результат будет соответствовать современному социальному строю, но по семантике он будет соответствовать тому, что называется стадным эффектом.

Рассмотрим небольшой пример.

Схема I: «*Траву сжевал → переварил → отторгнул из организма*». Как все. Оставшаяся энергия пошла на жизнеобеспечение. Эта усредненная схема для любого стадного животного, существа, не обладающего мыслительными процессами.

Схема II: «*Информацию получил → воспринял → забыл (отторгнул)*». Как и остальное большинство. Остаточные знания пошли на генерацию некоторых новых знаний. Это может стать усредненной схемой современного пользователя информационными сетями, интернетом. Но она структурно похожа на первую схему.

Налицо сопоставимость информационной «жвачки» для нашего мозга и биологической жвачки для травоядных, стадных животных. Между этими категориями очень много общего. Параллели очевидны. Это ли не основа для иной фор-

мы коллективизма, который таковым назвать уже трудно? В большей степени, это одно из качеств стадности, только на более высоком уровне интеллекта. Безусловно, нам пока еще далеко до полного состояния стадности, но сегодня эти качества уже проявлены. И одна из причин здесь – в глобальных информационных сетях, в которых люди просто «утонули».

Полный возврат к стадному образу жизни невозможен априори. Но возможен его современный вариант на новом витке истории. Определенные качества из этого образа современное общество приобретает. Это:

– усреднение и унификация качеств человека, по которым его оценивают в обществе;

– тотальная не укрытая персональная информация о каждом человеке;

– возможность отслеживать социальный каждый шаг любого человека;

– глобальные базы данных об индивидуальных биологических, социальных, экономических, политических особенностях человека. Человек перестает быть уникальностью, понемногу теряет свою биологическую и социальную индивидуальность;

– унификация мыслительных процессов, вращающихся только вокруг заранее подготовленных для общества тем. Вбрасывание в общественное сознание новых, отвлекающих тем, актуальность которых регулируется в масштабах глобального информационного пространства;

– потребность в псевдоколлективном творчестве.

Если сегодня еще чего-то из этого перечня мы не знали или кто-то об этом еще не догадывается, то это уже скоро будет данностью или уже станет известно. В информационном мире спрятать что-либо невозможно. К этому нас уже начали приучать. А общность индивидуальности – это одно из проявлений качества стадности.

Но и назад пути уже нет.

Общество и ранее сталкивалось с такими проблемами, например, в начале аграрной революции, когда кочевой образ жизни постепенно переходил в вынужденно оседлый, связанный с обработкой полей, выращиванием культурных растений, необходимостью защищать эти поля, а в равной степени и свои жилища возле этих полей от посягательств соседей. Тогда же общество постепенно и сознательно пошло по пути создания государственных структур, ограничивающих свободу отдельного человека. Государству постепенно передавались права следить за выполнением определенных правил, позволяющих членам общества быть защищенными от внешнего и внутреннего произвола. Об индивидуальности каждого члена общества (кроме ярко выраженных лидеров, имена которых, по большей мере, остались в истории) почти не вспоминали. Но это было 20 тысяч лет назад.

Можно только перечислить некоторые признаки глобального «отупения» общества (в том числе, по данным источников [13, 14]). Подобный перечень читатель может сам сопоставить с огромным количеством публикаций в прессе, литературе, чтобы согласиться с их существованием. Сюда относится, в частности, следующее.

1. Кажущаяся социально-политическая активность массы людей в интернете с лихвой компенсируется еще одним стадным качеством – легкой их управляемостью при принятии конечных решений.

2. Социальная раскрепощенность в сетях для многих является синонимом отсутствия собственных моральных ограничителей: «То, о чем никогда не сказал бы при визуальном контакте, в сетях можно написать свободно».

3. Совсем мало читается классической литературы. Мировое классическое литературное наследие становится почти невостребованным, в том числе, в театрах, фильмах. Доступность простых видеорядов заменяющих классическую литературу в оригинале. Постепенно деформируется огромный пласт нравственности в обществе. Качества, которые

закладывались мировым литературным наследием на протяжении многих сотен лет [15], уже не являются доминирующими.

4. Общество мало интересуется классической историей. В виртуальном режиме история становится лишней. Нельзя забывать мудрое изречение великих: общество, не знающее своей истории, не имеет будущего.

5. Появление альтернативных, иногда популистских, теорий, в истории, естествознании, экономике. Варианты необоснованных искажений классических основ отдельных наук в интернете со стороны недобросовестных ученых.

6. Огромное количество *неподтвержденных* научных фактов в виде гипотез, опровергающих современную науку. Уход многих ученых от основ научной практики, как критерия истины, достоверности.

7. Появление существенного пласта псевдонаучных знаний, которые никто не опровергает ввиду невозможности упреждать их появление, предупреждать конструктивным обсуждением и научной критикой.

8. Огромное количество дублированной информации, смысл и достоверность которой рассеивается, теряется, искажается, подается с ошибками, изменениями по сравнению с оригиналом.

9. Искажение информации (в том числе, отчетной) в области экономики, безопасности, торговли, обороны, что представляет опасность для людей, приводит к нарушениям в работе целых отраслей, компаний и даже государств.

10. Глобальное влияние на молодежь той большей части информации, которая подается в ограниченном, усеченном варианте, позволяющем иметь только представление о предмете этой информации, без глубокого ее анализа.

11. Упадок процессов запоминания информации, как ненужных. Отсутствие (за ненадобностью) моторических методов ежедневной тренировки памяти.

12. Ограничение аналитических способностей у потребителей информации. Усеченная информация постепенно перестает быть основой для получения новых, аналитических знаний.

13. Огромное количество плагиата, недобросовестности при размещении материалов в интернете и на других носителях.

14. Раньше для защиты от таких сущностей использовались механизмы государственного влияния, в частности, цензура. Этот механизм сегодня несет в себе негативные признаки потому, что, как и любым другим инструментом, цензурой пользовались не только во благо, но и для политических и других ограничений: «С водой выплеснули и ребенка».

15. Спросим у авторитетных современных ученых: нужна им цензура в виде контроля за плагиатом, недостоверными научными данными? Мы получим положительный ответ в девяти случаях из десяти. И в данном случае, вынесение любых научных знаний на широкое обсуждение в интернете не приводит к положительным результатам по известным причинам, которые связаны с глобальным информационным пространством.

Этот далеко не полный перечень таких признаков. Однако за ними даже в представленном объеме просматриваются те же отличия, с которыми человек сталкивался еще 20 тысяч лет назад [16], в начале когнитивной революции.

Можно сослаться на то, что история развивается по спирали, на каждом новом витке которой впитывает в себя новые качества исторических объектов и событий, которые могут преломляться через призму современности. Все это касается и новых форм стадности, с которыми приходится сталкиваться нашему обществу. При этом важно не допускать одинаковых ошибок, которые могут становиться антагонистическими.

Сюда относятся и наши перечисления, которые при определенных условиях могут стать такими же непреодолимыми, паллиативными, как во время когнитивной революции стали, например:

– потребность в массовом переселении людей;

– «перегрузка памяти» многих поколений, «ловушки роскоши», в которые попадали и племена, и отдельные властители, и целые государства из-за появившихся ранее неизвестных ресурсов;

– безопасность своего земледелия и животноводства от посягательств соседей, приводившая к появлению войн, как крайне опасного способа разрешения социальных и политических противоречий, и многое другое, что имеет аналоги в современности.

Стадность, с новыми акцентами в современном обществе, причиной которой стало глобальное информационное пространство, – это не простое обобщение прошлого с будущим, а сигнал ко многим опасным и необратимым последствиям, с которыми нам предстоит иметь дело в будущем. И степень безопасности, которая может быть обеспечена в данном случае, зависит от процессов формирования условий и правил взаимодействия глобального информационного пространства и человека в системе «человек-машина».

2.2 Интерпретационные изменения свойства «понимание» в ГИП как показатель опасности для человеческого разума

Современные программы искусственного интеллекта позволяют осуществлять самые различные образовательные проекты в области образования и науки, позволяют распознавать любые образы и формы, отвечать на любые вопросы,

обеспечивать любые системы персональной навигации, играть в шахматы на уровне гроссмейстеров, водить автомобили и самолеты без участия человека, осуществлять переводы с любых языков на любые языки мира, заниматься диагностикой практически любых заболеваний. Кажется, что это направление в инженерии является наиболее перспективным и не имеет видимых преград в развитии. Существует устойчивое мнение, что уже в середине 20-х годов нашего века искусственный интеллект сможет заменить человека и достичь его уровня во многих областях его деятельности. Но не факт, что этот прогноз сбудется, как и многие другие прогнозы – освоения космического пространства, клонирования людей и заселения Марса.

Информационное пространство всех видов насыщено информацией о преимуществах и недостатках искусственного интеллекта. Следует обратить внимание на то, что с ростом объемов знаний об искусственном интеллекте мнения ученых о его опасности для человека существенно расходятся.

От математика и философа Джан-Карло Роты исходит ключевой вопрос: «Сможет когда-либо искусственный интеллект преодолеть барьер понимания?» Поскольку, что не существует компьютерных продуктов в виде искусственного интеллекта, которые были бы ориентированы не просто на обучение или обеспечение знаниями, но на *понимание* сущности вещей.

Понимание (лат. *Intellectus*) – универсальная операция мышления, связанная с усвоением нового содержания, включением его в систему устоявшихся идей и представлений [17]. Понимание, с точки зрения ГИП, является специфической операцией мышления и занимает в ряду мыслительных процессов важную роль. Такую же, как, по отношению к пониманию, занимает функция *воображения,* к которой нам придется еще обратиться.

Понимание сущности вещи – это предмет исследования Аристотеля. Только такое понимание (именно *сущности*) Аристотель соизмерял с понятием «знание». То, что непонимаемо, не представляет собой знания. Современный искусственный интеллект по своей сути не способен к пониманию сущности вещей. Для искусственного интеллекта характерно понимание-вспоминание по аналогии, то есть понимание (усвоение) как аналог известного в его смысловой интерполяции.

На протяжении многих столетий познавательной деятельности не приходилось опровергать идеи Аристотеля и Платона. Но не теперь. Сегодня искусственный интеллект претендует на знания без понимания. Пытаясь представить, что сумма информации – это и есть знание. Насколько этот аспект может представлять опасность для человека, зависит от вектора развития глобального информационного пространства, его инженерного наполнения, качества участия в нем самого человека.

Созданы весьма эффективные программы «глубокого обучения», в которых используются огромные массивы данных для обучения сложных компьютерных программ, например, «нейронные сети» [18, 19, 20]. Существуют программы распознавания объектов, например, человеческих лиц, путем сопоставления оцифрованных объектов с суммой цифр, предлагаемых как базовая матрица. Существуют программы распознавания человеческой речи и ее записи в виде текстовых символов. Компьютеры дают возможность такой цифровой обработки благодаря своим огромным запасам памяти. Созданы программы распознавания любых финансовых схем, включая банковые транзакции, в частности, с целью выявления таких из них, которые противоречат действующему законодательству. Но для этого, опять-таки, включаются механизмы программного сопоставления того, что распознается, с тем, что уже было. Подобные системы искус-

ственного интеллекта способны на неправильные ответы, ошибки в системах, которые приводят к катастрофам там, где человек этого не допустил бы в силу некоторых особенных качеств человеческого интеллекта.

Принимая во внимание термин «понимание», мы должны соизмерять его с термином «вспоминание», соотнося его с тем объемом информации, которая была ранее запомнена машиной. В лингвистике же термин «понимание» связан с завершенным смысловым образом, как результатом психофизического действия.

Небольшой эксперимент, доступный каждому из популярной литературы. Слова: «человеку с непокрытой головой нужна шляпа» в англ. интерпретации звучит: «*the bareheaded man needed a hat*». Типовая программа распознавания речи переводит эту фразу как «человек, руководимый медведем, нуждается в шляпе». И так далее.

Программы распознавания образов во многом зависят от «шума» в виде полутонов, времени дня, угла падения света на объект, электромагнитных помех и др. Все это может искажать распознаваемый образ до неузнаваемости. Программы искусственного интеллекта могут становиться ненадежными в зависимости от тех ситуаций, когда объект должен додумываться до реального образа способом «узнавания» по отдельным доступным чертам или особенностям, которые присущи этому объекту. Это способ «дорисовывания, додумывания». Примерно, как это делает ум человека, считывая с текста или неоновой рекламы буквы, написанные в виде полутеней от падающего света. Полутени дают представление об объеме объекта, в данном случае – букв, форма которых далека от принятых, только потому, что человек, смотрящий на них, «дорисовывает» в голове эти буквы и быстро считывает понимаемую, таким образом, информацию.

До сих пор никакие, в том числе современные, обучающие программы не ориентированы на формирование функции «понимания образа».

Понимание образа резко отличается от его распознавания. Распознать предмет можно фотографированием, если на фото изображен завершенный образ. Если в образе не достает завершенных отличительных черт, он может быть распознан компьютером с ошибкой, которая далее станет искажением некоторых принятых решений или результатов работы. Мозг же человека в этом случае «дорисовывает» исходный образ, включая механизмы понимания того, с чем имеет дело. Искусственный интеллект не обладает механизмами додумывания, дорисовывания, домысливания до нестереотипного образа. По крайней мере, на современном уровне развития систем искусственного интеллекта, кроме логического распознавания компьютер не способен понимать сущность объекта. Мозг же человека для этого включает механизмы *образной экстраполяции*. Компьютер способен только на подобное *интерполирование* объекта в заданном объеме.

По всей видимости, в основе процессов понимания лежит не просто оцифрованная информация об объекте в виде двоичных математических кодов компьютерных машин. Человек для *понимания* сущности объекта пользуется параллельной информацией, которую мозг одновременно получает и обрабатывает от первичных органов внешнего раздражения: зрения, слуха, языка, осязания, обоняния, то есть «языка общего познания», которым владеет не только человек, но и все другие живые существа на Земле. Причем, это владение далеко не самое унифицированное. Мы с удивлением говорим о том, насколько развито обоняние у слепых кротов, какими являются акустические способности летучих мышей, вовсе не реагирующих на видимый свет. Обонятельные рецепторы акул позволяют им распознавать запах крови в воде на расстоянии в несколько километров, при этом зрением эти

животные не блещут. Таких примеров множество. Суть всех их заключается в том, что обладатель такой информации способен не просто распознавать образ при помощи своих органов чувств, но при помощи рефлексных матриц «дорисовывать» этот образ в мозгу, передавая соответствующие импульсы своим мышцам для ответной реакции на эти объекты. Человек является наиболее развитым в этом ряду только благодаря тому, что к своим природным органам чувств он сумел добавить мыслительную деятельность на уровне образного сравнения, экстраполятивного домысливания и др. Именно благодаря мышлению он имеет преимущества перед другими биологическими особями с их развитыми первичными органами чувств, в свою очередь, имеющими параметрическое преимущество перед человеком. Именно этого качества – *понимания образа*, его сущности, обладателем которого является человек, до сих пор нет в искусственном интеллекте. И он не скоро появится.

Еще одно явление, *стереотипность,* легко преодолевается мозгом человека, но становится непреодолимым препятствием для систем искусственного интеллекта. Понимание и стереотипность – это два антагонизма, один из которых ориентирован на экстраполирование, а второй – на приверженность к ранее известным знаниям. Первое свойственно человеку, а второе, как раз, компьютерам, знаниям, которые вмещены в глобальное информационное пространство.

Какими бы ни были исчерпывающими базы данных о состоянии объекта, всегда найдутся такие ее параметры, которые не вписываются в стандартные рамки. Примером служит известный «эффект бабочки», как системной первопричины для многих самых глобальных изменений в хаотических процессах. Другим примером является эффект «слона в спальне», в основе которого несопоставимость объекта «слон» с объектом «спальная комната». Искусственный интеллект в силу стереотипности не воспримет такие сочетания

и сделает ошибку при чтении, достигая уровня своей ненадежности.

Слова из книги Педро Домингоса «Верховный алгоритм»: «Люди опасаются, что компьютеры станут слишком умными и захватят мир. Но реальная проблема в том, что они слишком глупы, и они уже захватили его». Пока это только опосредованное управление людьми, посредством привязывания природного интеллекта человека к огромным массивам оцифрованной для удобства пользования информации. И только. Следует понимать, что большинству людей (возможно, исключение составляют некоторые ученые, аналитики, которым по роду деятельности требуется обработка больших баз данных), нет надобности в таких объемах информации, как избыточных, не соответствующих решаемым задачам.

Феномен *избыточности информации* – это болезнь нашего века, с которой обществу все равно придется справляться радикально. Потому, что человек не должен становиться сателлитом в любой системе «человек-машина», изначальное предназначение которой – в расширении соизмеримых возможностей собственно человека, но не машины.

Профессор Мелани Митчел из Портлендского университета назвала это фундаментальным барьером на пути развития искусственного интеллекта.

Мало того, по данным исследователей из Стенфордского университета, искусственный интеллект научился при помощи «нейронных сетей» искажать суть реальных объектов, дополняя их несуществующими элементами, например, при аэросъемках улиц городов [21]. Программа обработки фотоснимков детализировала те объекты, которых не было в реальности, путем кодирования одного типа изображений в совершенно другой. Происходило незаметное для человеческого глаза изменение цветов, которые легко считывает компьютер, их генерация в виде зашифрованных сигналов, кото-

рые потом отражались на снимках независимо от человека. Причем эти действия носили системный характер. Это подтверждает отсутствие интеллектуальности такого алгоритма, его свойство копирования, но не понимания.

Любое понимание должно определяться целью, целесообразностью, которая связана с потребностями человека. Понимание обеспечивает установление связи раскрываемых новых свойств объекта познания с уже известными субъекту, формирование операционального смысла новых свойств объекта и определение их места и роли в структуре мыслительной деятельности. Когда же субъекту нужно понять уже известное событие или явление, то понимание совершается без актуального участия мышления – это понимание-вспоминание

Важным качеством человеческого мышления является **воображение**, как инструмент для запуска механизмов понимания. Его можно назвать инструментом для экстраполирования существующего знания для знания будущего. Можно показать, что ГИП не только тормозит процессы понимания, но и искажает процессы воображения. Воображение включает в себя, в первую очередь, структурирование предмета, его функциональное назначение, смысловую нагрузку, которую несет этот предмет. Такие функции компьютеру пока не подвластны. Это функция, прежде всего, человека. Но участие в глобальном информационном пространстве несет опасность угнетения и потери этого важнейшего качества мыслительного процесса человека. Попробуем это показать.

Однако, воображение может играть и негативную роль в системе восприятия интернета. Оно может быть связано с искажениями информации о персоналиях, которые, так или иначе, формируют неверные предпосылки для виртуального социального общения. Исходная позиция – отсутствие контроля за тем, что размещается в социальных сетях. У пользователя нет собственного объективного способа контроля за

достоверностью информации, и чаще всего он воспринимает фейковую информацию в сетях как действительную и объективную.

Как создается фейковая ловушка? Автор информации о себе приукрашивает события, себя, свои поступки, свой социальный статус. В сеть выбрасывается позитив, далекий от объективного состояния вещей. Помещаются фото десятилетней давности, указывают на несуществующие профессии, крутой интерьер, машины, туристические места, вымышленные имена. Радикальный обман. Цель – привлечь к себе внимание. Пользователь тянется к таким «лидерам», к людям, кажущимся успешными, стремится поднять свой объективный статус за счет общения с ними. И получает фейк. Разочарование.

Те, кто этим занимаются, также не освобождены от проблем. Несоответствие объявленному в сетях требует от автора постоянного напряжения ради сохранения выдуманного имиджа. Со временем происходит раздвоение личности, так называемое состояние двоемыслия, когда приходится вживаться в придуманный образ, вовремя переходит к реальной жизни и т. д.

Наиболее уязвимая часть пользователей – подростки, люди с неокрепшей психикой, те, кто заводит закрытые странички в сети, для друзей, обособленно. В них можно быть самим собой – расстроенным, неопрятным, без навязчивого контроля со стороны старших.

Существуют данные о том, что *Instagram* представляет наиболее опасную роль для психического здоровья молодежи. Здесь, в наибольшей мере поддерживается иллюзия идеального, далекого от реалий действительности состояния. Присутствующая созерцательность культивирует тревогу, собственную несостоятельность, способствует развитию депрессивных состояний. Ученые университета штата Пенсильвания показывают, что знакомство с такой информацией существенно занижает собственную самооценку, если срав-

нение не в пользу потребителя. Он более критично оценивает свои данные, достижения, необъективно оценивает свои результаты на фоне фейковых сведений о мнимых «лидерах» таких сетей. В результате появляется новое качество – зависть. Она является наиболее распространенным побочным эффектом участия в таких сетях. Появляется зависть не только к лидерам сетей, но и к своим друзьям, партнерам, к образу жизни других людей, это становится наваждением и существенно меняет образ жизни человека – в худшую сторону. Потребности резко расходятся с возможностями, что вызывает раздражение (другому можно, а мне нельзя), неудовлетворенность, неумение справиться с психологическими нагрузками – на фоне постоянной подпитки с стороны интернет сетей.

Постепенно происходит самоизоляция человека в пользу виртуального общения, там, где больше позитива без каких-либо усилий.

Появилось даже понятие фейсбук-депрессия. Ощущение ненужности, изолированности, как следствие – копание в жизни совершенно незнакомых людей, появление ощущения собственной убогости, никчемности. Это неумение адекватно оценивать информацию, анализировать ее, обеспечивать необходимую степень визуализации объекта.

Социальные сети представляются сегодня, как эффективный механизм активного влияния на людей. В нем системно используется тот факт, что люди очень зависимы от мнения окружающих, как в положительном, так и в отрицательном спектре. Социальные сети являются плодотворной почвой для усугубления этой зависимости. Зависимости от значительно большего, чем в реальности, количества людей и в значительно большем объеме информации. Причем, как правило, на безальтернативной основе.

Нужно не забывать, что интернет – это всего лишь способ общения. А все проблемы, которые появляются при его использовании, принадлежат людям и порождаются людьми.

Результат такого общения во многом зависит от устойчивости психики человека, его личных качеств, в том числе, способности к анализу, пониманию сущности, с которой приходится сталкиваться в интернете, к пониманию воспринимаемой информации. Поэтому, воображению, как функциональной стороне понимания, следует уделять особое внимание в масштабах глобального информационного пространства.

2.3 Влияние глобального информационного пространства на некоторые творческие способности человека

Существует ряд индивидуальных свойств человека, на которые нельзя не обращать внимания, в связи с его взаимодействием с глобальным информационным пространством и его потенциальной опасностью для таких качеств, как понимание сущности предмета, творческие и мыслительные процессы, созерцание, сопереживание, восприятие, эмоции. Одним из них является воображение, как одно из предшествий для понимания. Тем более, что сам факт появлении в глобальном информационном пространстве так называемого виртуального образотворчества не мог произойти без развитого воображения пользователя. И столкнуться со способностями к пониманию, как важнейшей компонентой человеческого мышления.

Воображение необходимо человеку, чтобы из существующего представить несуществующее [22]. Присутствие воображения – это неизменное условие профессионализма во многих областях деятельности, связанных с прогнозированием, планированием, моделированием, проявлением свойств памяти, изобретательством, проявлением способностей к познанию, мышлению. Прежде всего, для ученых, работа кото-

рых во многом заключается в том, чтобы на основе анализа существующих данных получить некоторый новый, доселе неизвестный результат: гипотезу, открытие, изобретение [23]. Воображение – это неизменный спутник любого человека творческих профессий: художника, актера, поэта, инженера, археолога. Когда нужно в самой простой вещи увидеть то, что не видели другие люди. Отсюда – великолепие картин Пикассо, шедевры Шекспира и Пушкина. Трудно сформировать логику представления целого по некоторым частностям, например, в исторических либо археологических исследованиях, и т. д.

Воображение играет существенную роль и в повседневной жизни, давая возможность человеку существенно расширять свою палитру эмоционального мира, делать жизнь более насыщенной, красивой, многообразной. Отсутствие воображения обедняет нашу жизнь. Иными словами, воображение – это важнейшая часть психического состояния человека, от которой человеку отказываться просто невозможно.

Согласимся, что общество, во все времена, достойно культивировало в себе это качество, как источник гениальности для отдельных людей, источник восхищения этой гениальностью со стороны остальной части общества, как важнейший инструментарий прогресса, и не собирается от этого отказываться.

Попробуем поставить вопрос об исчезновении этого качества в обществе, как второстепенного, не имеющего существенного значения для людей. И общество потеряет огромную часть своей человечности. Мы потеряем вектор на развитие общества. Потому что с утратой воображения потеряют свой смысл, в частности, наука, культура, спорт, образование как синонимы процветания. И мы придем к мнению, что человеческое воображение следует оберегать, развивать с детства, независимо от того, станет ребенок гением или

нет, воображение у него должно развиваться. Вероятно, существует некоторый совокупный потенциал воображения для всего общества, который складывается как результат проявления воображения каждого его члена.

Отсюда правомочен вывод о том, что воображение человека необходимо развивать как совокупный потенциал всего общества. Неразвитое воображение является признаком слабого интеллекта общества [24].

Очевидным является то, что глобальное информационное пространство, как сфера активного влияния на общество, не может не влиять на этот важнейшие показатель в качестве фактора психологической безопасности для каждого его пользователя и для общества в целом [25, 26, 27]. В основе этого, в частности, крайне низкая информативность материала, закладываемого в интернете, узость его восприятия для последующего анализа и получения объективных выводов.

Зададимся целью убедиться, насколько развивается или угнетается функция воображения у человека, долгое время имеющего дело с информацией, систематически извлекаемой из глобального информационного пространства. Нас будет интересовать произвольное репродуктивное и творческое воображение согласно классификации [28]. Тем более, что воображение рассматривалось Л. С. Выготским как необходимый, неотъемлемый момент мышления, особенно творческого, так как в мышление всегда включены процессы прогнозирования и предвосхищения.

В исследованиях принимали участие 153 студента старших курсов инженерных специальностей вузов Украины (кроме специальностей *IT*), в основном активных пользователей информационных сетей. Каждый из них, в повседневной жизни, в сутки проводит в интернет-сетях не менее 4–5 часов свободного времени. По условиям эксперимента испытуемые отказывались от пользования интернетом на протяжении шести месяцев. Некоторая часть вернулась в ин-

тернет после двух месяцев, некоторая – после четырех месяцев. Всего 126 студентов приняли участие в полном объеме проводимого эксперимента. И еще 27 студентов, которые по различным причинам вышли из эксперимента, но продолжали наблюдаться в тестовом режиме, что дало дополнительную информацию по изучаемому вопросу.

Суть эксперимента заключалась в том, что периодически, раз в месяц, с самого начала каждому испытуемому, который отказался от пользования интернетом, предлагалась контрольная черно-белая карточка, на которой в завуалированной форме многообразия обводных и плавных одноцветных линий были «зашифрованы» определенные силуэты предметов, фигур и других узнаваемых объектов природы, быта, стилизованные лица или профили людей, животных и др. (рис. 2.1).

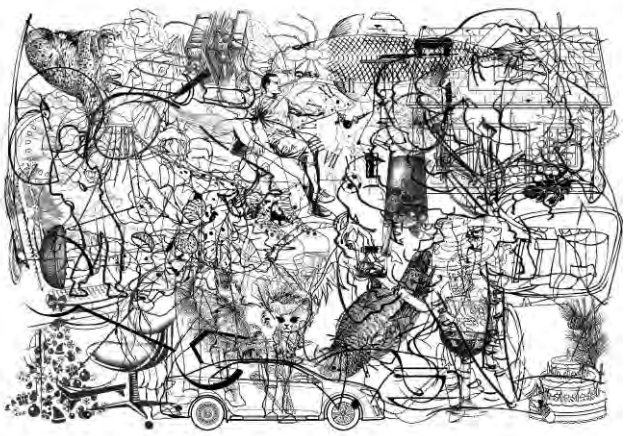


Рисунок 2.1 – Пример одной из карточек для тестирования воображения. Автор тестовых карт М. В. Долгая

Для того чтобы опознать ту или иную фигуру, силуэт, необходимо было максимально включать свои способности к

воображению, потому что фигуры, как правило, были представлены не в полном объеме и могли «дорисовываться» как образы в воображении испытуемого. Карточка позволяла увидеть и «домыслить» до 50 фигур или предметов самого различных свойств, размеров, смысла по всей ее плоскости. Качество воображения каждого участника эксперимента оценивалось по суммарному количеству узнанных и обозначенных силуэтов на карточке на протяжении всего испытания при их статистической обработке. Кроме того, для эксперимента была отобрана отдельная контрольная группа из 24 людей старшего возраста, которые являются изначально пассивными в интернете и не проявляют себя в социальных сетях [24]. Их показатели также контролировались ежемесячно. Результаты представлены в виде расчетных значений математического ожидания статистической выборки данных и его среднеквадратичного отклонения в таблицах 2.1 и 2.2.

Таблица 2.1 – Результаты для контрольной группы (численность 24 человека)

Отмеченные силуэты, количество	
В начале эксперимента K_0	В конце эксперимента K_{IV}
33±0,4	36±0,8

Чтобы учитывать фактор привыкания испытуемых к образам и фигурам, которые можно увидеть на тестовых карточках, исходя из данных участников контрольной группы (табл. 2.1), ведем уточняющий коэффициент:

$$\lambda_{0-\mathrm{VI}} = M(K_0)/M(K_{\mathrm{VI}}), \qquad (2.1)$$

где: $M(K_0)$ – математическое ожидание начальных численных значений угаданных силуэтов участниками контрольной группы; $M(K_{\mathrm{VI}})$ – математическое ожидание численных

значений угаданных силуэтов участниками контрольной группы по окончании эксперимента (через шесть месяцев) [24].

Таблица 2.2 – Результаты для экспериментальной группы (численность *N*, человек)

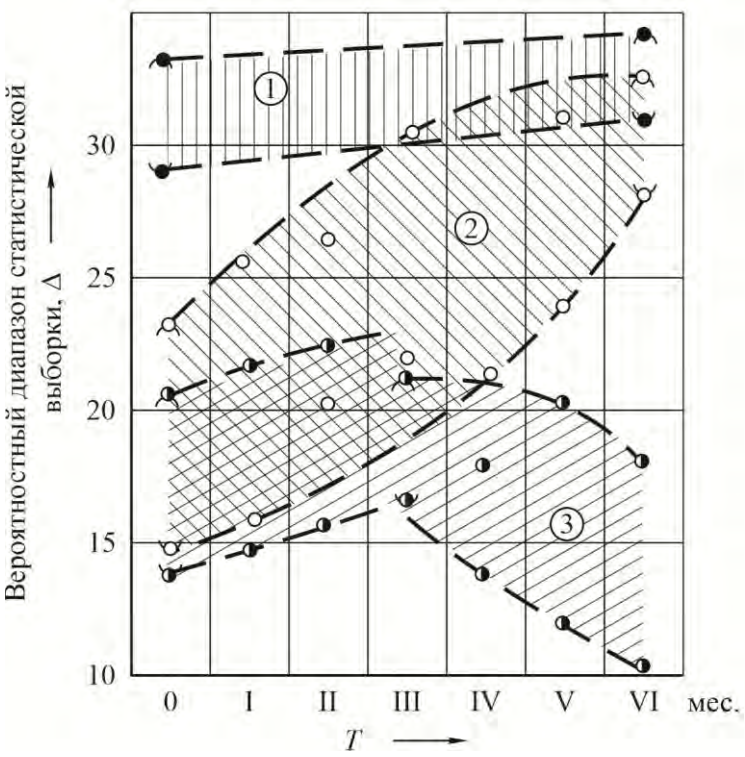
$T_{эксп.}$, мес. / N, чел.		6 / 126	4 / 16	2 / 11
Отмеченные силуэты по месяцам в эксперименте	0	21±0,7	25±0,2	19±0,9
	I	**23±0,7**	**23±0,5**	**20±0,5**
	II	**26±0,5**	**29±0,9**	**21±0,9**
	III	**29±0,9**	**28±0,8**	*21±0,7*
	IV	**28±0,5**	**29±0,9**	*17±0,4*
	V	**30±0,4**	*25±0,6*	*18±0,3*
	VI	**34±0,6**	*19±0,8*	*15±0,7*

В процессе обработки полученных данных для экспериментальной группы, каждое из них соответственно умножалось на коэффициент ($\lambda_{0-VI} = 0{,}917$, см. табл. 2.1).

Изначально было видно, что с учетом вероятностного разброса данных, экспериментальная группа имела исходные результаты по уровню воображения в 1,35–1,74 ниже, чем исходные данные, которые показывала контрольная группа. По окончании эксперимента эти соотношения были иными: контрольная группа имела условные показатели воображения всего в 1,24 раза выше, чем испытуемые.

На графиках, построенных методом огибающих кривых (рис. 2.2), очевидна тенденция к зависимости предложенного

показателя уровня воображения для испытуемых от их участия в интернете. В целом для групп, которые прошли эксперимент в полном объеме, среднестатистические данные по представительной выборке после полугодового эксперимента дают данные об увеличении условного показателя воображения в 1,62 раза [24].



1 – контрольная группа;
2 – экспериментальная шестимесячная группа;
3 – экспериментальная двухмесячная группа

Рисунок 2.2 – Динамика изменения условного показателя воображения пользователей интернета

Для групп, которые участвовали в эксперименте не полный его период – это увеличение составило соответственно 16 % (за четыре месяца) и 10,5 % (за два месяца). При этом в двух последних случаях у испытуемых после окончания эксперимента уровень контролируемого показателя падал за два последующих месяца на 52,6 % и на 40 % соответственно [24].

По сравнению с контрольной группой экспериментальная группа испытуемых имела результат в начале испытаний около 57,1 % от показателей контрольной группы, а в конце испытаний – 80,6 %.

Такие упрощенные исследования могут в первом приближении дать ответ на вопрос: действительно ли активная работа в интернете способствует угнетению функции воображения человека? Ответ является положительным.

Следует понимать механизмы, способствующие проявлению такой закономерности. Они, по нашему мнению, связаны со спецификой подачи информации в интернете. Любая аналитическая информация, в особенности научного и научно-популярного, познавательного, культурологического и др. направлений, имеет три составляющие:

– входная постановочная часть информативного изложения, показывающая то, о чем может идти речь в данной информации;

– ядро информации или собственно описательная ее часть, дающая основания для анализа этой информации, ее сопоставления с другими источниками и альтернативными ее видами;

– резюмирующая часть, в которой следуют определенные выводы по сути описания, заложенного в ядре информации [24].

Подобная модель относится в основном к полноценной, полноформатной информации: печатным статьям, книгам, рефератам, описаниям патентов. Однако на сегодня в интер-

нете полноценная информация в виде полнотекстовых публикаций составляет не более 0,004 % всего объема информации. Как правило, существующий в интернете стиль относится к реферативному, сжатому изложению почти любой информации. Стиль такого изложения существенно отличается от печатного ограниченностью ядра информации, то есть ее подробного описания, а иногда и резюмирующей его части. Остается только постановочная часть. В условиях массовости такой информации в интернете формируется принципиально иная методология ее восприятия со стороны потребителя. Чаще всего, изложение материала связано с первой его составляющей, входной постановочной частью и в меньшей степени – с ядром информации и с ее резюме. Эти части, как правило, читатель должен додумывать сам или искать дополнительные источники. А поскольку лавинообразный способ доставки информации пользователю в интернете ограничивает время ее усвоения, как правило, такая информация остается не обработанной для последующего аналитического использования. Это так называемая «информация к сведению». Чаще всего такая информация не подлежит глубокому анализу и последующим из него новым логическим выводам [24].

Другой частью глобального информационного пространства, которая влияет на аналитичность информации, является безусловная ее повторяемость в интернете и резкое снижение достоверности, связанное с ошибками при репостах, дублированиях сведений и, часто, с намеренными искажениями повторной информации. В современном интернете, по данным [29], 95 % информации представляет собой неоднократно дублированная информация.

В этом заложена существенная проблема для пользователей информацией, которая заложена в интернете. Она связана с резким уменьшением мыслительных процессов, так называемой аналитичности, когда из полученной информа-

ции путем сопоставления, анализа, иных выводов, можно генерировать новую информацию. А значит, мы подошли к тому, что называется воображением для любого человека [24].

Таким образом, ни в коей мере не умаляя достоинств глобального информационного пространства в целом, следует еще раз подчеркнуть, что интернет в виде еще одной опасности несет в себе способности к опосредованному влиянию на творческие процессы, характерные для человека и лежащие в основе всего современного прогресса.

Существует прямая зависимость угнетения воображения и мыслительных процессов для определенных категорий из числа пользователей интернета. У испытуемых, которые на длительный период были изолированы от информационных сетей, показатели воображения начинали несколько улучшаться и, наоборот, по окончании эксперимента – опять падали. В качестве причин, отражающих влияние интернета на развитие или угнетение этой важной составляющей сознания пользователя, можно отметить особую реферативную специфику подачи информации в интернете, ее объемную избыточность, искажаемость и повторяемость, что приводит к снижению возможностей для эффективного аналитического применения.

2.4 Осознанная ложь и глобальное информационное пространство

Ценность достоверной информации в обществе всегда была высокой, вне зависимости от того, что она собой представляла. В древнем мире или в средние века информация военного содержания, в зависимости от ее объективности, могла стоить существования целых держав. Человек, принесший неправдивую информацию, часто лишался жизни.

Искаженная информация торгового характера могла обернуться огромными убытками не только для тех самых торговцев, но и для государства в целом. Риски, связанные с искусственным искажением информации экономического характера и в те времена были соизмеримы с рисками для жизни целых городов или отдельных категорий людей в обществе – производителей, торговцев, потребителей. Все эти риски остаются реальными и сегодня. Цена достоверной информации сопоставима с причиняемыми при этом убытками в масштабах целого государства.

Таким образом, ложная информация в глобальном информационном пространстве представляет угрозу безопасности, в первую очередь, для человека.

Факты материалистического содержания (известные нам законы природы, закономерности природных явлений, свойства материалов природных и искусственных и многое другое из того, чем пользуется человечество) составляют только небольшую часть знаний о природе, вселенной, человеке, о его Земле. Мы вправе считать, что большая часть знаний даже сегодня пока остается неизведанной, и к их познанию лучшие умы человечества стремятся каждый день. Тем важнее сохранять в объективности те знания, которыми уже владеет человечество. Любое их искажение, утеря достоверности ведет к постепенной потере смысла этих знаний. К потере самих знаний.

Действительно, мы уже никогда не узнаем тех природных закономерностей, которыми владели египетские или ацтекские жрецы, знания, которые были в сожженных фолиантах Александрийской библиотеки, труды древних ученых, накопленные столетиями и уничтоженные в библиотеках нацистской Германии и многое другое. Общество вынуждено вновь открывать законы, постигать истины, которые уже когда-то были постигнуты. Это цена утерянных знаний. И это цена человеческой безопасности. Но это еще не самый главный ущерб. Утерянная информация способствует появлению

новой, часто искаженной информации о том же предмете или сущности, например, в истории [29, 30]. А эта искусственно искаженная информация, распространяясь как новая истина, приводит к искажению иногда самой сущности науки. То же, только в локальных объемах, относится и к искусственному искажению знаний в глобальном информационном пространстве.

По данным автора, только в период пандемии коронавируса в 2019–2020 годах в интернет было вброшено до 70 % искаженной или обманной информации о состоянии дел с заражениями, способах лечения и защиты от вируса, источниках приобретения лекарств и защитных средств, статистике о поражении населения, фейки об экономических потерях и кризисах мировых валютных бирж и компаний. Наряду с объективной информацией эта информационная ложь, помноженная на человеческий страх, легко спутывала тактики борьбы с пандемией в целых странах и приводила к людским жертвам, которых можно было бы избежать без учета обманной информации из интернета.

Учеными Массачусетского технологического университете показано, что в период с 2006 по 2017 годы из 127 тыс. постеров и «ретвитеров» в социальной сети *Twitter* более 70 % носили ложный характер [32]. Массовая ложь на одной из самых посещаемых социальных сетей мира должна была стать абсурдом в обществе. Но не стала. Владельцы сетей самостоятельно пытаются научить пользователей отличать массовую ложь от правды в сетях [33]. Риторический вопрос об опасности такой массовости.

Сложнее всего мириться с продолжением этого явления в средствах массовой информации, но еще более неприемлемо, когда информационная ложь имеет развитие в государственных информационных системах, а также в законотворчестве. Об этом писал еще Желю Желев, болгарский писатель, публицист, а позднее первый президент Республики Болгарии. Это состояние так называемого двоемыслия [34], опре-

деляемого как способность поддерживать два или более противоположных или противоречивых убеждений сразу, встречается в самых различных местах огромного информационного поля [35]. В любых социальных сетях можно этому научиться за два дня общения. Это ли не опасность, настигшая человека благодаря глобальному информационному пространству?

Общество становится все более объективно зависимым от растущих объемов ложной информации. Сегодня, в силу инженерного и правового обеспечения, это следует принимать как должное, как то, что не имеет обратного направления. Это связано, прежде всего, с необратимостью развития самого глобального информационного пространства. Несравнимыми являются все время появляющиеся новые возможности этого явления (глобального информационного пространства), за которые общество готово платить даже объективностью информации, объективностью знаний. Мы становимся зависимыми от новых инструментариев, теряем способности существовать без них. Эта зависимость становится обязательной. Это одна из известных исторических опций, на которые указывал еще Норберт Винер в 1950 году в работах [36, 37]. Общество поставлено перед условием – массовый отказ от объективности знаний либо разработка новых методов защиты от нападений в состязаниях за правду. Эпоха информации постепенно превращается эпоху дезинформации [38]. Подобные этические тренды в коммуникациях сегодня имеют право на существование, поскольку они могут указывать на вектор, по которому оно будет развиваться дальше.

С этикой коммуникаций в сетях связано и такое явление, как «*флуд*». В переводе этот термин означает «поток» (*flood*) и несет смысловую нагрузку «спонтанный поток чего-то». В сетях он приобрел сленговое значение «потока ненужной, не тематической информации», которая на интер-

нет-сленге не соответствует *сабжу*, то есть предмету обсуждения. И постепенно стал вполне небезобидным явлением для пользователей. Флуд следует отличать от так называемого «*оффтопика*», то есть сообщения, о котором предупреждается как о не тематическом. Это, а также «*флеймы*» представляют собой сленговые слова, касающиеся новой формы информационного диалога, новых форм общения в сетях. Флуд существенно выделяется в этой системе своим негативом, который он привносит для пользователей сети

Проявляется флуд как спонтанная помеха обычному интернет-общению в сетях: на форумах, в чатах и т. д. Часто эта информация запускается с целью, по мере возможностей, исказить общение в интернете. Как и всякий род деятельности, флуд находит своих профессионалов, которые уже на других условиях запускают подобные помехи в различные сети, целенаправленно мешая общению своим бессмыслием, навязчивостью и периодичностью самопроизвольного вмешательства. Сегодня профессиональный флуд – это достаточно большие объемы периодически повторяющейся не тематической информации, часто простые наборы цифр и букв, которые не только засоряют интернет-пространство, но и вызывают негативные эмоции у пользователей, иногда выбивают человека из состояния равновесия, мешают его логике и другому. На первый взгляд, бессмысленная информация, своей настойчивостью, бесцеремонностью вмешательства в системы интернет-общения напоминает поведение отдельных людей, копирует логику их действий и достигаемые при этом результаты. Часто флуды вызывают гнев и провоцируют конфликтные ситуации там, где без них можно было бы обойтись.

Флудизм становится массовым, он проникает в телефонную связь, искажает суть многих коммуникаций, в том числе, оговариваемых определенными соглашениями, договоренностями, на основе которых заключаются многие сдел-

ки: деловые, коммерческие, социальные и другие. Часто, сами того не замечая, флуды распространяют люди с неуравновешенной психикой, испытывающие неудовлетворенность в жизни, тем самым повышая свою искусственную значимость в некотором виртуальном для них пространстве.

Цель флудов далеко не всегда бессмысленная. Флудят и для того чтобы навредить, сорвать нужные переговоры, если это целенаправленные действия. Флуды ставятся источником информации или исходного положения для самых разных хакерских атак. Часто флуд содержит огромное количество на первый взгляд не взаимосвязанных вопросов, анкет, которые используются для нанесения ущерба компьютерной системе в виде хакерского воздействия. За счет одалживания флудами генерирующих ресурсов снижается степень защиты информации, расположенной, например, в сетевых «облаках», если ими пользуются в это время.

Разновидность флуда, так называемый *вайп*, обозначает пустую тему в чате, засоряющую его. Он является причиной бессистемной траты времени в интернете. Часто встречающиеся фоновые музыкальные сопровождения, М-флуды, также направлены на появление раздражения у пользователя, которое мешает сосредоточиться на собственных материалах. Самое главное, что сегодня информационные сети никак не защищены от флудизма. Технически это невозможно. Причем выловить флудиста бывает весьма непросто. Потому что они такие же пользователи сетей, как и остальные их участники. Их отличие – чисто человеческие качества, такие как бесцеремонность и привнесение негатива в общение с себе подобными.

Эйфория от вседозволенности и отсутствия любой цензуры стала спусковым крючком ко многим негативным процессам, связанным с информационным беспределом, который имеет собственное качественное название – ложь. И наравне с безусловными преимуществами, которые мы полу-

чили от бесконечного моря информации, появляются новые виды обмана, преступлений, появляются ранее не существовавшие проблемы для самых различных слоев населения, становятся далекими от науки многие результаты этой деятельности, что само по себе уже становится проблемой для общества развития, если мы себя таковым считаем.

Общество находится перед дилеммой. Что является предпочтением, безбрежное море информации, в которой можно получить ответ на любой вопрос, пользуясь огромными массивами знаний, в том числе, и недостоверными, огромные возможности цифровых технологий, связанные с всемирной информационной паутиной. Либо ограничения, которые дают доступ не ко всей информации, а только к проверенной, достоверной, бесфейковой. Министерство общественной безопасности Китая в 2016 году запустило интернет-сервис китайского аналога Твиттера – *Sina Weibo* для отслеживания ложной информации с последующим наказанием источников искаженной информации. По мнению властей страны, ложная информация крайне вредна для общества и может приводить к социальным взрывам, панике.

Ответ, как всегда, может находиться в «золотой середине». Нужны правила, определяющие существование любой информации, правила ее появления, движения, съема, пользования, расширения, копирования. Нужна ответственность за **качество информации**. Термин, под которым следует понимать именно безопасность для человека, которую несет современный информационный прорыв. Перспективный, но опасный для общества.

Компилятивные процессы при подготовке научных работ, списывание целых диссертаций, научный плагиат – это уже следствие затеянного в глобальном информационном пространстве и почти узаконенного права на ложь. Общество постепенно привыкает ко лжи в интернете и переносит это

качество в повседневную жизнь. Поэтому морально общество сегодня не готово бороться с компилятом и плагиатом.

Министр, ректор, бизнесмен может украсть целую диссертацию – и ничего не произойдет. Потому, что те, кого это касается, станут защищать свои авторские интересы, но все остальное общество, узнав о постыдном случае, просто отмахнется или промолчит. Мотив: в интернете такого добра море. Именно поэтому, интернет, не только как источник знаний, но и как источник морали, сегодня не выдерживает никакой критики.

Современное глобальное информационное пространство дает огромные возможности для искажения информации, ее утери в первоначальном виде. Количественные характеристики ГИП, связанные с вольным доступом к любой информации, постепенно переходят в качественно иное ее состояние, в частности, связанное с искажением собственно информации до такой степени, что дальнейшее ее использование ведет к лавинообразным процессам появления новых недостоверных знаний. На самом простом уровне, это должно приводить к огромным тратам времени и сил для перепроверки, что не всегда удается сделать. А значит, такая информация уходит от пользователя, как опасная для последующего применения. В этом заключается ценность достоверной информации в современном мире.

Интернет часто паразитирует на информационном голоде. Когда смысловая полнота информации подменяется ее избыточным объемом, недостоверностью, противоречивостью, тезисным изложением. Причем далеко не всегда на умеренном бытовом уровне, но и на научном. В этом плане, общество оказалось не подготовленным к существованию в условиях глобального информационного пространства.

В инженерии существуют закономерности развития технических систем, которые носят название закона «согла-

сования-рассогласования», в основе которого лежат правила согласованного действия различных частей технической системы. Без такого согласования машина не сможет работать. В общественных отношениях не существует такого закона в прямой интерпретации. Но огромные массы информации, не всегда достоверного наполнения, постепенно расшатывают эту систему, допускают именно рассогласование по различным информационным потокам, которое есть и не что иное, как заведомая ложь. В основе любого перемещения информации лежит условие наименьшего ее искажении при передаче [39]. Искажение информации при передаче становится причиной рассогласования на этапе ее освоения тем, кто ее принимает и обрабатывает. Если судить с позиций упомянутого инженерного закона, то такая искаженная информация не просто дает неправильный результат у данного пользователя, но, трансформированная им же, она переходит к другому пользователю и уже он ее видоизменяет (сознательно или неосознанно) и направляет далее в информационное пространство. Такое движение с некоторой периодичностью приводит к тому, что первоначальная информация теряет свой исходный смысл и изменяется, иногда, до противоположного значения и может становиться дезинформацией. Это спонтанная дезинформация, которая заложена в самой сущности информационной коммуникации и является почти неизбежной в условиях глобального, не контролируемого информационного пространства. Это искажение информации. Но это еще не ложь.

Ложь в смысле заведомой неправды – это иная категория состояния информации в глобальных информационных сетях. Она появляется, как осознанная и умышленная деятельность субъекта передачи информации, которая заведомо не соответствует действительности. Чаще всего такая работа связана с преследованием определенных корыстных интере-

сов. Этим ложь отличается от спонтанно развивающейся сетевой дезинформации. Методы образования ложной информации известны давно [40, 41], но все они присутствуют в информационных сетях. Это, в частности:

– запредельное преувеличение реальных фактов;

– приукрашивание событий;

– полная или частичная подмена информации на информацию противоположного значения;

– использование фантазийных и мифотворческих подходов по принципу: чем более нереальна информация, тем она более доверительна;

– организованная ложь, как основа для ее доверительности, в том числе, от источника – тоталитарной системы;

– абсолютное игнорирование научных подходов, как источник противоположности для лжи, в подготовке и трансляции информации.

Важное свойство информационной лжи подмечено Н. Бердяевым еще в 30-е годы прошлого столетия, когда о глобальной информации никто не догадывался. Ложь в любых проявлениях изменяет структуру сознания человека [39]. «Необычайное возрастание лжи в мире и лжи оправданной, не сознаваемой как порок, определяется, прежде всего, экстериоризацией совести, … то какая угодно ложь может оказаться оправданной».

Возникает парадоксальная, на первый взгляд, мысль. А не являются ли фейки, флуды, спамы и другая искажающая или ложная информация, появляющаяся, как продукт отсутствия цензуры, сами по себе фактом самодостаточной и самостоятельной цензуры внутреннего содержания для пользователя этой информации? Такая вынужденная «цензура» требует умения пользоваться ею. Чем более явной является ложная информация, тем менее она подлежит проверке и отторгается, потому, что тем меньше на нее обращают внимания, как на очевидную ложь. И наоборот, более скрытая по-

тенциально фейковая информация в большей мере подлежит проверке.

Например, необходимость выделения из больших объемов непроверенной информации той ее части, которая является объективной – это задача самого пользователя, и решается она для каждого из них по своему алгоритму. Для одного таким алгоритмом будет собственный опыт, для другого фильтром будет здравый смысл. Третий будет опираться на условное общественное мнение либо результаты условного «социального опроса». Фильтром может стать и критическая часть обсуждений выделенного материала, например, в научных обсуждениях.

Сам факт: искажение информации в сетях может постепенно превращаться в свою противоположность, а именно, специфический вид децентрализованной цензуры. Этот момент требует своего более глубокого исследования и может быть интересен для дальнейшего анализа.

Является ли все это неумолимым злом для общества? Ответ: и да, и нет. «Да» – в силу общепринятых правил, которые сформировались в обществе на протяжении многих веков и социальных потрясений, которые не приемлют вмешательства в дела морали, гуманизма и индивидуализма человека. «Нет» – потому, что нам еще придется переосмысливать роль и функции глобального информационного пространства, в том числе, и по указанным социальном критериям. И то, что сегодня является недопустимым, в том числе, и отдельные факторы индивидуальности каждого человека, нравственные критерии разума, и его противоположности – алгоритмизация интеллекта, через небольшой промежуток времени покажется нам не таким уж и опасным. А со временем мы привыкнем к этому и будем делиться информацией всех видов, в том числе, о своей индивидуальности, с первым встречным потребителем, получая взамен от него ту информацию, которую сегодня каждый из нас скрывает, как лич-

ную. Такой подход, вне всякого сомнения, изменит и мораль общества, и его парадигмы к развитию. Глобальное информационное пространство уже сейчас выступает в качестве самостоятельной составляющей социального процесса, в которой последний как бы растворяется.

В современном мире глобальной информатизации и цифровизации, массовые проявления лжи в интернете становятся существенной опасностью и для научного мира, и для пользователей информации в любых областях человеческой деятельности. Обществу в любом случае придется обращать на это внимание, бороться с ложью, которая в интернете стыдливо называется организованными вбросами фейковой информации, а на самом деле, с ЛОЖЬЮ, к которой общество постепенно привыкает. Такая опасность не может оставаться без внимания, если интернет будет и далее претендовать на статус глобального и полезного информационного пространства для всего человечества.

2.5 К вопросу о типичности блокчейн технологий в инжиниринге

Технологии блокчейна, или блокчейн технологии, сегодня на слуху у всей активной части человечества [42, 43, 44, 45, 46, 47, 48]. Без преувеличения, эти технологии, в основе которых доверительность и инкогнитивность, имеют распространение в мире существующих технологий, управления, сервиса и других областей деятельности. Мы наблюдаем проникновение блокчейн технологий в самые различные области, в наиболее мощные компании, такие как *IBM*, *BOSH*, *AliBaba*, *Amazon Uber*, *Samsung*, *General Electric* и др.

В равной мере, как интернет стал независимым от посредников, хранителем огромного пласта цифровой информации, так технологии блокчейн постепенно становятся не-

зависимым от посредников, хранителем и распорядителем интернета ценностей, интернета вещей. Этим он привлекателен для инжиниринга.

«Интернет вещей» является связующим звеном между современным виртуальным цифровым миром и реальным физическим миром, в котором привык существовать человек. О блокчейне сегодня говорят как о:

– технологии децентрализованного распределенного реестра всего, что подлежит систематизации;

– возможности и потенциале новой технологической платформы в различных областях жизни;

– гигантской цепи уверенности во всем;

– доверительном продукте;

– хранителе правды [41].

Блокчейн описывается как технология распределенного реестра. Все блоки связаны между собой в непрерывную последовательную цепочку таким образом, что для легализации любого последующего блока необходима информация о предыдущих блоках. Это постоянно накапливаемая и дополняемая база данных обо всех транзакциях, без права их удаления или корректировки. Главное достоинство блокчейна – это система цифровых «печатей», или меток, благодаря которым придается законность и незыблемость каждого последующего коллективного протокола (блока) транзакций в зависимости от предыдущего [42]. Вторым достоинством блокчейн технологии является ее прозрачность для всех участников: о размерах сделки, ее пути, но не о личности адресата.

В целом, блокчейн технология позволяет однозначно свести воедино в оцифрованном виде персональные данные любых собственников и их физическую собственность, без опасности ее дублирования в привязке к другому собственнику. Это кадастры различного назначения, право собственности, регистрация любых прав, предусмотренных законодательством, соглашений, контрактов и многое другое. Основ-

ными методами достижения результата являются цифровизация материальных ресурсов и их токенизация, то есть привязка принятой единицы учета и актива любого ресурса к объему некоторой деятельности (например, ценным бумагам, сертификатам, деньгам, энергии, лекциям, академическим часам). Токены, как право действия, можно передавать, продавать, занимать в рамках пиринговой сети блокчейна.

Финансовый сегмент применения блокчейна является только одним из многих, на которые может претендовать эта уникальная технология. Чаще всего блокчейн технологии связывают с биткоином, с такими терминами, как майнинг, транзакции, доверительные протоколы, хэш-функции и др. Это отпугивает обычных пользователей. Любое применение технологии видится в цифровизации и доверительном обмене самой различной документацией: договорами, завещаниями, свидетельствами, патентами, гарантийными обязательствами, долговыми расписками, медицинскими историями болезней, анализов, учебно-методическими материалами, научными данными, бытовой документацией, и др. Но это не все. Применение технологии и, особенно, ее перспективы впечатляют.

Создание и развитие системы удобных смарт-устройств и смарт-контрактов расширяет эту технологию на область, которую называют «интернет вещей», делая любой оцифрованный предмет уникальным и узнаваемым в системе распределенных реестров. Например, платформы онлайн-платежей типа *PayPal*, автономные логистические системы в транспорте типа *Uber*, в энергетике типа *dron-service* электрических сетей или системы учета распределенных мини-источников энергии, умные системы переработки отходов всех видов и классификаций, независимый мониторинг состояния окружающей среды, погодных условий, цифровизация коммунальных услуг, контроль за износом инженерных сооружений и машин, строительная индустрия и распределе-

ние недвижимости, заводы вещей с распределенными реестрами всех материальных потоков, начиная с многокомпонентного сырья, готовой продукции и отходов с обязательными смарт-чипами, позиционирующими каждый компонент или деталь. Это интернет-торговля и *IT*-маркетинг, умные и энергоэффективные дома и многое другое из «интернета вещей» [43, 44, 45, 46, 47].

Собирательный образ системы, которая предназначена для реализации блокчейн технологии, включает: участников системы, соответствующую компьютерную базу и сети, общее согласование о предметах сделок в системе, знания о формах и способах записи информации в системе, соглашение о системном доверии для всех участниках системы (*P2P – peer-to-peer*, равноправность участников), соглашение об инкогнитивности персональных данных, программное обеспечение и доступ к майнингу путем создания индивидуального электронного кошелька [49].

Ключевые термины системы:

– **ключ доступа**, это специальным способом полученный набор автоматически сгенерированных символов в одном из форматов хранения (*Hex*, *WIF*, *WIF*-сжатый) в электронном кошельке. Ключи доступа бывают общие (открытые) и приватные (индивидуальные);

– **транзакция,** это процесс проведения некоторой логически завершенной сделки (соглашения) между двумя участниками системы, результаты которой записываются в протоколы всех участников системы. В более широком смысле, под этим термином в блокчейн технологиях следует понимать любое согласованное и легализованное участниками действие в отношении другого участника;

– **доверительный криптографический протокол,** это последовательность записей о действиях (сделках) участников по передаче оцифрованной информации или информационном обмене в определенном временном отрезке. Обеспе-

чивается на основе конфиденциальности данных об участниках, аутентификации сторон сделки, невозможности отказа от сделки и целостности записанных ранее данных;

– **распределенные реестры** блокчейна, это децентрализованная база оцифрованных данных о предмете транзакций, которая хранится и обновляется каждым из участников сети;

– **майнинг,** это предоставление индивидуального вычислительного ресурса участника системы для обеспечения жизнедеятельности некоторого виртуального ресурса этой системы. Процедура майнинга – это решение математической задачи, в ходе которой вычисляется число, которое не является больше заданного целевого уровня сложности. Суть этого числа заключается в присвоении ему права «опечатывания» очередного протокола распределенного реестра;

– **хеш-функция,** в общем, как математическая операция свертки, представляет собой функцию, которая обеспечивает преобразование массива входных данных любой заданности в битовую строку установленной длины, выполняемое скрытым алгоритмом. Такой алгоритм составляет основу блокчейн технологии. Преобразование, производимое хеш-функцией, называется хешированием. Алгоритм хеширования в блокчейн технологиях выдает случайное битовое число (между 1 и $2^{256}-1$), состоящее из символов, расположенных в произвольном написании, неизменное на протяжении всего майнинга и после него;

– **токен**, это единица учета. Аналог ценных бумаг и действий над ними в системе блокчейн технологий[49].

Терминология этим не ограничивается, принимая во внимание достаточную сложность и необходимое упорство в освоении технологии.

Каждый участник, независимо от того, является ли он юридическим или физическим лицом, обладает двумя ключами доступа в систему, создаваемыми одним из извест-

ных методов, например, «*Brain Wallet*» или по адресу «*bitaddress.org*.»: один из них общепринятый, распознаваемый всей системой (*Account Extended Public Key* – ***AEPuKey***), а второй – индивидуальный, принадлежащий только участнику (Account *Extended Private Key* – ***AEPrKey***). Индивидуальный ключ доступа – это особая криптограмма, хешируемая (создаваемая) некоторым алгоритмом шифрования в одном из равнозначных форматов хранения (*Hex*, *WIF*, *WIF*-сжатый), которая дает участнику право персонального доступа к ресурсам (криптовалюта, доступ к счетам фирм, информационные ресурсы, *know-how* компаний), представляющим ценность в системе. Публичный или открытый ключ система генерирует сама на основе индивидуального ключа, который участник получает уникально. Владение приватным ключом позволяет всегда вспомнить открытый ключ, но не наоборот. Далее последовательность алгоритма блокчейна включает следующее [49].

1. Каждый участник системы обладает обезличенной информацией об оговоренных заранее ресурсах всех других партнеров пиринговой (*P2P*) сети.

2. Системная работа заключается в проведении последовательных **транзакций** (некоторый материальный обмен, платежи, перевод денег со счета на счет и др.), между любыми двумя участниками системы. Обезличенная цифровая информация об этом объявляется всем участникам для записи в следующей строке индивидуальных протоколов.

3. Запись информации о новой, необработанной транзакции осуществляется всеми участниками в свои протоколы под одинаковым номером сделки с указание времени сделки и является обязательной для всех.

4. Периодически с равным интервалом конкретная транзакция обрабатывается путем проверки и подписи индивидуальным ключом всеми участниками на предмет ее возможности, наличия ресурса у автора транзакции (рис. 2.3).

Заполняемый, таким образом, последовательностью транзакций доверительный протокол лежит в основе огромной цепи распределенных реестров блокчейна [49].

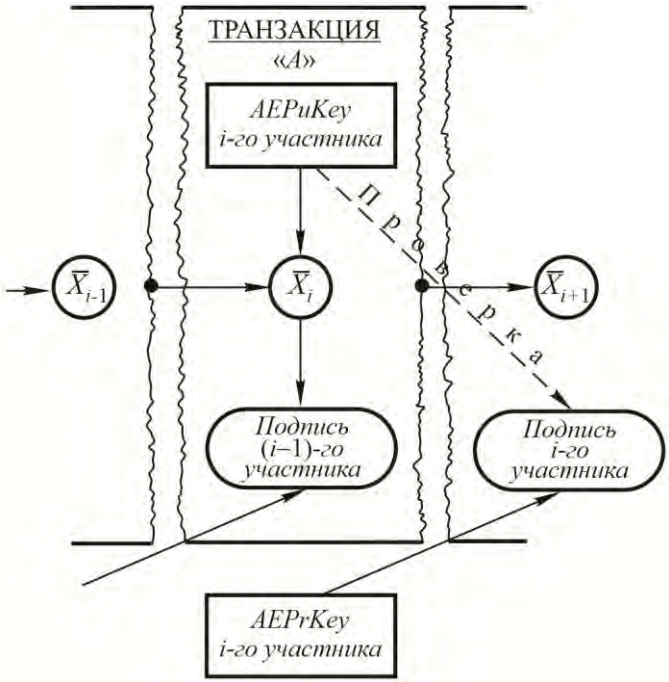


Рисунок 2.3 – Схема учета и подтверждения транзакции «*A*» *i*-м участником системы

5. Протокол транзакций, заполненный полностью (например, *N* записей в одном доверительном протоколе), в дублированном виде присутствует у всех участников системы с указанием времени операции. Например, в системе биткоина каждые 10 минут проверяются все транзакции, они получают одобрение и сохраняются в блоке, *соединенном с предыдущим*, образуя, таким образом, непрерывную цепь блоков. Каждый последующий блок соотнесен с предыду-

щим, без него не существует, и только тогда является действительным и доступным для просмотра всеми желающими.

6. Полностью заполненный протокол с транзакциями «опечатывается». Поиск единой для всех участников системы «печати» осуществляется самими участниками в процессе **майнинга.** Осуществляется майнинг при участии **конвертатора** (назовем его так, для простоты понимания) со скрытым алгоритмом генерации случайных битовых рядов. Майнинговое оборудование участника, например, видеокарты, мощные процессоры или специальные *asic* устройства, позволяет хешировать очередной этап «опечатывания» протокола и, после процедуры проверки, легализуется и помещается в распределенные реестры. Это сложный специфический алгоритм, позволяющий, за счет использования электроэнергии генерации требуемого кода, получать вознаграждение (например, в технологиях биткоина, это определенная часть криптовалюты, обеспеченная затратами электроэнергии) [49].

7. Конвертатор – машина одностороннего действия. Важной особенностью конвертатора является отсутствие обратного действия. Конвертатор, представляющий собой «черный ящик», в основе которого находится алгоритм, названный авторами как *SHA*-256, при помощи определенной **хэш-функции** генерирует **хеш-код** (*HK*)**,** состоящий из случайным образом набранных букв и цифр. Входными данными для конвертатора являются данные об оцифрованном содержании протокола транзакций «*A*», цифровой код $\overline{X}_{i-1}$ предыдущего протокола, хешированный при его «опечатывании». Это данные, которые майнер загружает в компьютер (рис. 2.4).

Решение задачи осуществляется многократно, до достижения результата. По данным Дино Марка Ангаритиса, на 2015 год среднее число таких решений для каждой майнинговой задачи составляло $3 \cdot 10^{20}$ хешей, что не всякому ком-

пьютерному ресурсу под силу [43]. Появление таких инструментов, как *ASIC*-майнинг, резко снижает эффективность самых современных видеокарт в алгоритме *SHA*-256 (для биткоина), которыми владеет приватный майнер в домашних условиях. Уже запущен процесс «индустриализации» майнинга, когда крупные компании, занимающиеся этой процедурой, за счет крайне высоких мощностей имеют преимущества и получают большую часть вычислительных мощностей системы, максимально централизуя одну из главных операций блокчейна, «снимают» весь результат вне конкуренции [49].

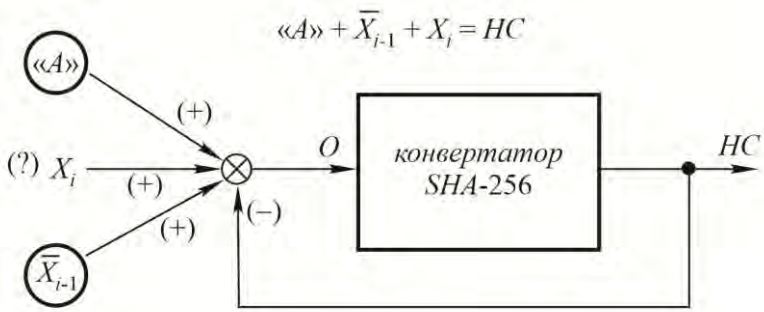


Рисунок 2.4 – Упрощенная модель майнинговой операции

8. На основании исходных данных майнер, при помощи мощностей своей компьютерной системы, подбирает необходимый код x_i для нового протокола примерно в такой упрощенной интерпретации (рис. 2.4):

$$«A» + \bar{X}_{i-1} + X_i = HC$$

Собственно **майнинг,** т. е. уже подобранное число $X_i = \bar{X}_{i-1}$, которое дало бы нам указанное равенство, осуществляется компьютерной системой методом подбора случай-

ных чисел. Успех поиска зависит от мощности компьютерного оборудования, видеокарты, энергии и времени, затрачиваемых на майнинг. По данным И. Камински [48], усредненное количество энергии, расходуемое на операции майнинга в современном мире, соизмеримо с расходами энергии на острове Кипр [49].

9. Участник майнинга, первым нашедший число $\overline{X}_i$, сообщает его всем остальным участникам системы, и после его проверки всеми участниками путем простой подстановки в программу *SHA*-256, опечатывает *i*-й протокол и кладет его в папку. Найденное число, обозначенное как $\overline{X}_i$, и является «печатью» для заполненного протокола с транзакциями всех участников системы за последнее время.

10. Таким образом, любой из «опечатанных» протоколов становится достоянием истории. Его уже невозможно переписать, изменить, так, чтобы никто этого не заметил. Эта функция подтверждения (консенсуса) называется **«*proof-of-work*»** или ***PoW*,** – доказательство работы**.** (Реже можно использовать консенсус типа **«*Proof of Stake*», *PoS*,** доказательство владения). Любая последующая корректировка протокола участником системы легко выявляется другими участниками простым и условным подбором: если $«A»+\overline{X}_{i-1}+\overline{X}_i \neq HC$, это значит, что кто-то нарушил целостность протокола. Испорченный протокол будет ликвидирован, а нарушивший участник, в зависимости от целей такой корректировки, может заменить свой испорченный протокол, либо выйти из числа участников системы [49].

11. Если один исключительный участник не подтвердил правильность майнинга числа $\overline{X}_i$, при том, что все остальные его подтвердили, идет дальнейшая проверка: либо этот участник неправильно записал найденное другим участником число $\overline{X}_i$, либо у него неправильные записи в протоколе транзакций, либо он нарушил правила работы. В этом случае

исключительный участник уничтожает свой испорченный протокол и копирует правильный протокол у партнеров, либо выбывает из системы.

12. Тот, кто предложит первым правильно найденное число $\bar{X}_i$, будет награжден за добавление блока поощрением, но не за счет других участников системы.

13. Возможен вариант, когда некто взломал цепочку и нарушил последовательность протоколов с «печатями». Теоретически он может начать свою собственную цепочку из искаженных транзакций (рис. 2.5). Но она легко вычисляется любым из участников, потому что один человек не в состоянии сравниться со скоростью транзакций всей остальной группы, с последовательным дублированием записей в протоколах партнеров по системе. Цепочки этого «некто» всегда будут короче, чем у остальных участников, что легко контролируется ими [49].

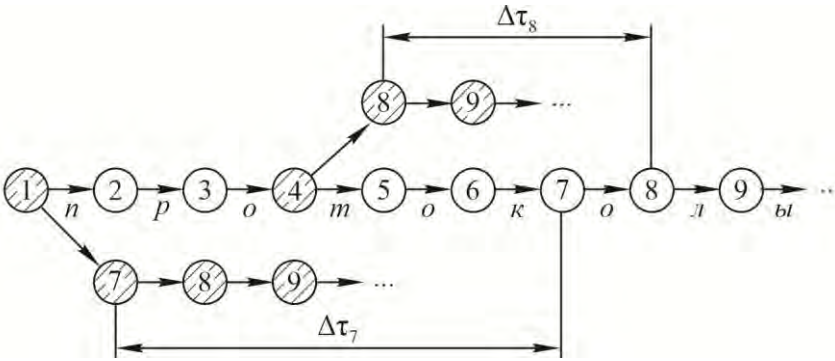


Рисунок 2.5 – Механизм нарушения и распознавания целостности пиринговой сети

Много говорится о недостатках блокчейн технологий, относя к ним, например, низкую пропускную способность сетей, недостаточную киберзащищенность персональных данных в некоторых случаях. Называется юридическая не-

приспособленность этих технологий к существующим законодательствам многих стран и др.

Блокчейн технологии охватывают все большие области для применения, и результаты свидетельствуют о том, что за ними большое будущее. Сегодня мы вправе ожидать появления унифицированного и универсального механизма простого и надежного от взломов программного продукта, позволяющего большому количеству потребителей эффективно создавать локальные технологии типа распределенного реестра для решения самых различных задач децентрализации работы. Такого, какими в свое время стали оболочка *Windows*, пользовательский *Office*, интернет-сети и облачные технологии, универсальные инструментарии для повседневного применения [49].

2.6 Социальность блокчейн технологий как вариант развития общества

Суть блокчейн технологий заключается в том, что они вовлекают в систему распределенных отношений партнеров, ранее не доверявших друг другу, и делают их вынужденными доверителями для всех участников системы. Современная блокчейн технология – это большой распределенный регистр любых оцифрованных материальных и не только, ценностей, в основе которого лежат многофункциональные доверительные протоколы, которые совершенствуются, развиваются, делают эти технологии все более приспособленными для пользователей, в том числе, и с позиций их безопасности. Из парадигмы чисто технической понятие блокчейн постепенно переходит в категорию социальную, социально-экономическую, требующую своего количественного содержания, смыслового наполнения, превращающую его, по существу, в

один из важнейших критериев, влияющих на большое количество сторон жизнедеятельности нашего общества [43].

Важным свойством блокчейн технологий является неограниченность доступа к системе для любого количества участников и любого количества операций, которые называются транзакциями, при абсолютной уверенности в прозрачности действий всех участников и сохранении инкогнитивной информации. Такие, по существу, демократические основы, в рамках которых изначально сформировался блокчейн, обещают для него широкое поле деятельности в современном обществе. Постепенно создается социальная платформа для этого нововведения и для его перспективы.

История позволяет нам судить о том, что подобные революции в области познания были характерны и для других периодов жизни человека.

Первым регистратором познания всего окружающего для человека был солнечный или рассеянный от небосклона свет, фотоны которого специфически отображались в сетчатке человеческого глаза, отражаясь от всех предметов в обозримом природном диапазоне, делая эти предметы уникальными, узнаваемыми для первобытного человека, отличными друг от друга, в частности, благодаря свойству цветовой дифракции. Как результат такой «маркировки» отраженных в свете окружающих предметов, человек начал разбираться в этом мире, стал осознанно отличать небо от воды, землю от деревьев, себя от других людей и животных, другие живые существа, отдельные предметы, цвета, объемы, расстояния, причем постепенно включая в это познание их качественные отличия. «Маркировка» светом (цветом) была тогда главным мерилом реального мира. Далеко не сразу человек научился различать все цвета радуги. Даже на заре Киевской Руси славяне мало отличали синий цвет от серого, а наиболее яркий красный цвет был у них в почете, как наиболее распознаваемый. Зрачок человеческого глаза развивался в направлении

освоения более широкого частотного спектра света от 380 до 740 нм. Ультрафиолетовый и инфракрасный диапазон в биологическом смысле оказался недостижимым для человеческого глаза. Именно поэтому многие явления природного мира оказались недостижимыми для человеческого сознания: невидимое тепловое излучение, солнечный ультрафиолет и др.

Звуковой природный диапазон в пределах 16 Гц – 20 кГц для человека существовал всегда. Со временем появился осознанный, генерируемый самим человеком звук, отражаемый барабанными перепонками и слышимый человеком, потом – согласованные и рациональные сочетания звуков в виде отдельных слов. В виде членораздельной речи звук стал не просто «маркировать» акустическим сигналом отдельные предметы, но давал им более точную и красочную качественную оценку, отобразил те стороны вещей, которые ранее были доступны только в созерцательном виде, но не подлежали простейшей маркировке в виде слова-аналога. Ролевым апофеозом звука стала музыка, сочетания отдельных звуков, которых в природе ранее не существовало. Но для человека музыка стала маркером наиболее чувственных категорий: добра и зла, прекрасного и низменного, отделяла наиболее эмоциональные для человека оттенки многих вещей. Здесь человек переиграл саму Природу.

Не менее значимая для человека тактильная и обонятельная «маркировка» предметов имеет свою историю, адекватную изложенной выше.

Современный цифровой мир, в частности, «реестр вещей» или «интернет вещей», как продукт блокчейн технологий, в XXI веке дает в руки человека совершенно новый оценочный инструмент для «маркировки», такой же, как свет или звук, при помощи которого открывается или должен открыться мир, ранее человеку недоступный. Потому, что оцифрованные предметы, сохраняя свои качества, принима-

ют на себя ранее неиспользованные свойства унифицированности, а значит, сопоставимости там, где этого ранее не могло быть. Например, световой или звуковой мир не могли сопоставить в одинаковых размерностях дерево и волну, дождь и траву, папоротник и вулкан, компьютер и ветряную мельницу. Трудность заключалась в несопоставимости физических параметров, определяющих состояние этих предметов или их функционирование. Цифровые технологии единых распределенных реестров – смарт-конекты позволяют не только в совершенно ином виде представлять эти предметы и давать им совершено новую, качественную оценку, но и равнозначно оперировать ими.

Таким образом, в историческом плане, в сознании человека постепенно происходили процессы обмена с окружающей средой:

– световой «маркировочной» информацией, дающей представление об окружающем мире;

– акустической «маркировочной» информацией, дающей более глубокое представление о качественной стороне этого мира;

– цифровой «маркировочной» информацией, унифицирующей все эти предметы в виде одной единственной операбельной платформы.

В основе оцифрованного мира, вложенного в децентрализованные протоколы – любые предметы, любые вещи, понятия и правила, реальный обмен между ними. Общее в этом обмене – унифицированность, уникальность и узнаваемость для любой оцифрованной вещи, предмета в пределах, достигаемых зрением, слухом, распознаванием, пониманием.

Важно, что цифровая «маркировка» всего, что окружает человека, до конца пока еще не оценена нами. Как можно оцифровать и записать осязаемые предметы в виде высокоскоростных электрических сигналов и постоянно к ним обращаться, сопоставлять их, управлять ими? Пока это только

начало некоторого пути, который человек все равно пройдет. И сколько на этом пути будет открытий, разочарований, счастья и трагедий – неизвестно. Потому, что мы в начале дороги, которая носит много названий, но для которой есть одно название – блокчейн – цепочка блоков.

В обществе сегодня не актуальны споры на тему социальности самого общества. Коммунистические идеи равенства, социализм, опошленные апологетами прошлого, надолго отбили охоту обсуждать идеи социальной равнозначности, как неприемлемые, проигравшие спор с капиталистической системой (см. например, [16, 34]). Тем не менее, цифровой мир XXI столетия вынуждает нас обращаться к подобным идеям, но уже совершенно с другой, неведомой нам ранее, стороны. Со стороны рационального распределения благ, гарантированных научно-техническим прогрессом. Еще в далекие 60-е годы XX века Римский клуб рассматривал доклады М. Месаровича, Д. Медоуза [50, 51], посвященные рационализации и равнозначности распределения и потребления товарных и трудовых ресурсов по планете, подчеркивая, что дешевая рабочая сила и углеводороды, поступающие в развитые страны Европы и США из стран третьего мира явно неравнозначны и нерациональны к ответному распределению потребляемых ресурсов, и не только продуктовых, но и других, которые обеспечивали необходимый уровень жизни людей, в пользу развитых стран. Мировой порядок на долгие годы застыл на отметке активного недоверия между странами, между нациями, между религиями, между отдельными людьми, относящимися к различным профессиональным, творческим, социальным группам.

По крайней мере, это относится к доверию между теми, кто имеет разный доступ к новым технологиям, к новым социально-экономическим проектам. Например, отличия между теми, кто создает и реализует новые технологии, и теми, кто не имеет к ним доступа, весьма существенны. Допустить

в качестве гипотезы состояние равного доступа к интеллектуальной собственности даже не реально, потому что на этом держится вся современная экономика мира, формируются крупнейшие активы всемирных компаний *Microsoft*, *Apple*, *Amazon* и др., скопивших свои капиталы на доверии людей в ценность услуг интернета, информационных сетей, биткоинов. Общего доверия в мире все это не добавило.

И одним из движущих звеньев в обеспечении доверия может оказаться система распределенных реестров и доверительных протоколов, то есть, блокчейн технология. Если, конечно, наука сумеет приспособить ее к огромному количеству систем, которые сегодня управляют обществом, его технической и экономической мощью.

Интересное мнение высказал известный социолог Юваль Ной Харари, поставив блокчейн технологии в социальной лестнице на уровне таких непреходящих ценностей, как религия, нации, деньги, то есть обладающие некоторыми почти абсолютными качествами [16]. Таким стратегическим качеством для блокчейна является обеспечение доверия между людьми.

Это не первая попытка в обществе уйти от централизации в сторону согласительного доверия и децентрализованного управления. В конце XX века Люк Скайуокер одним из первых оценил возможности интернета, Всемирной паутины, как инструментария для изменения современного индустриального мира, в котором правит меньшинство тех, кто деньгами, имуществом, сформированной веками экономикой, информационным влиянием удерживает власть над большинством. В том числе, пользуясь услугами центральных правительств, старыми средствами информации, также централизованными, зависящими от этого меньшинства. Предполагалось, что всемирная паутина будет способна разорвать порочность централизации и внести в общество хотя бы азы доверительности, независимости от меньшинства в пользу

большинства. Это ли не несбывшиеся идеи идеального демократизма, социализма? Не получилось. Мы являемся свидетелями того, как распределенные реестры всемирной паутины и интернет с его исключением влияния со стороны любой цензуры, попали в традиционную систему накопительного капитала и превратились в ряд суперкомпаний (*Facebook*, *Amazon*, *Twitter* и многие другие), которые вновь централизовали наши мысли, «пирамидизировали» нашу информацию, персональные данные, поставили их на службу той же самой прибавочной стоимости. Но без прибавочного продукта, как это водится в конце XX – начале XXI веков.

В основе процедур централизации различных областей деятельности человека лежит одно из важных его качеств – эгоцентризм, нежелание индивида рассматривать иную, кроме своей, точку зрения на вопросы главенствования в системе. Избавиться от этого качества почти невозможно, примерами чего изобилует литература и история. Такая позиция, как правило, выгодна для самого индивида и является потерей для всех остальных. Она может иметь вид иерархической пирамиды, в которой на каждом более высоком уровне стоят индивиды с собственным удовлетворяемым эгоцентризмом. Такая система в принципе не сопоставима с распределенными правами и обязанностями, как это предполагается в блокчейн технологии, и может являться серьезным препятствием для ее распространения. Поэтому, эта технология стала новой ступенью для реализации идей децентрализации и формирования доверия в постиндустриальном обществе.

«Интернет вещей», еще один продукт блокчейн технологии, – это один из способов переложить ответственность за тотальное недоверие между людьми с человека на неодушевленные предметы. Сети «интернета вещей» имеют свойство самоподдержки вне зависимости от производителя, распределителя, продавца. Условием доверительности в таких сетях является тотальная информированность всех участников сис-

темы обо всех, без исключения, сделках, транзакциях. В основе этой технологии несколько отдельных качеств, делающих ее эффективной [42]:

1 – мгновенный доступ к любым оцифрованным материальным активам;

2 – точность соотнесения предложения и спроса в системе заявленных и оцифрованных предметов;

3 – возможности снижения затрат на кредитование и риски обменных операций;

4 – оптимизация сотрудничества с партнерами по бизнесу в направлении коллективной работы, например, за счет краудсорсинга;

5 – преимущества распределенного капитала.

Блокчейн технологии можно представить в виде одноранговой плоской поверхности равноправных участников, каждый из которых имеет возможности любого согласованного транзактирования в координатах плоскости. Эти технологии предполагают, вместо иерархического доверия от низшего уровня к высшему, переход к добровольному одноранговому доверию равноправных участников (рис. 2.6). В социальном смысле, это фактор развития децентрализованных доверительных отношений в обществе.

Далеко не всегда децентрализация системы способна ее развивать. Если система по своей сущности обязана строиться на основе централизованного управления, обеспечивать централизованный контроль или учет, то вписать ее в технологии блокчейна будет нереально. Это может относиться, например, к банковским системам, для которых централизованный учет является основой существования и функционирования. Сюда может быть отнесена и система стратегического планирования на уровне отдельного государства, когда только высший уровень менеджмента может быть ответственным за социальное обеспечение общества, и государственная правовая система (с небольшими оговорками).

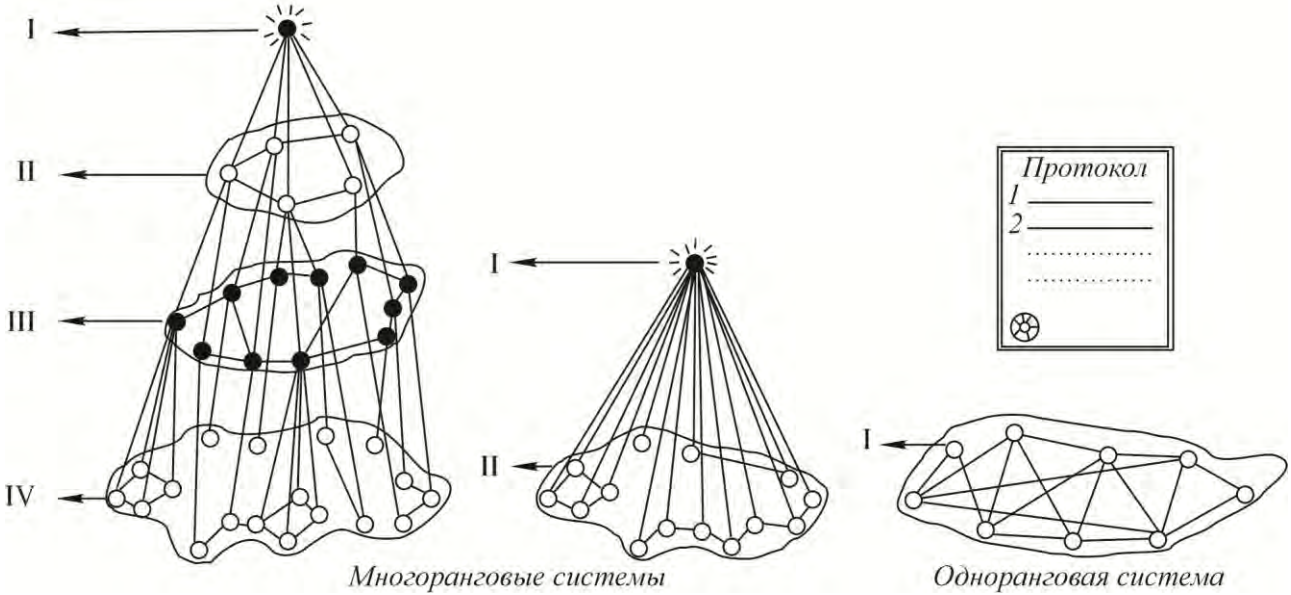


Рисунок 2.6 – Эволюция систем централизованного вынужденного доверия к одноранговым доверительным системам блокчейна

Но и децентрализация в интернете также не есть истина. Регистрируясь в *Facebook*, например, мы считаемся потребителями услуги, на самом деле являясь источником формируемой централизованно прибыли на продукцию, суть которой – информация. Огромные массивы сосредоточенной информации о персональных данных участников сети – это наиболее ликвидный товар в современном цифровом обществе, причем стоимость этого товара постоянно растет, составляя основу истинного богатства компании.

Но и здесь в блокчейн технологии существует своя идеология. Она состоит в том, чтобы возвратить идею открытого чат-форума для любой информации независимо от диктата централизованных регистраторов и контролеров. Распределенный реестр участников такой сети, без таких собственников, как, например, *Facebook* и *Twitter*, поможет избавиться от такого дополнения к нашему сервису, как распределенная база персональных данных об участниках сети. Этому способствуют, в частности, новые программные приложения для децентрализованной сети типа *Social Linked Data* (*Solid*) Тимоти Джона Бернерса-Ли [52], оставляющие за пользователем особенное право владения собственными персональными данными в распределенных реестрах. Аналогичные задачи ставит перед собой программная продукция компании *ECSA* (*Economic Space Agency*), дающие возможности для расширения прав потребителей сетевого пространства сохранять свои персональные данные при участии в сетях. Подобные программные продукты при их дальнейшем развитии станут контраверсионными для таких компаний, как *Facebook*, *Twitter* и др.

Создание системы учета при помощи распределенных реестров и доверительных протоколов, которая никогда не «забывает» состояние любой предыдущей транзакции, в определенной степени, противоречит еще одному важному качеству, которое культивируется в обществе. Это распреде-

ленная во времени способность прощать грехи, долги, проступки отдельных людей. Общество во все века поощряло способности многих правителей прощать долгосрочные долги и провинности, общество гордилось своими способностями к состраданию за проступки, сроки давности которых были достаточно велики. Человек как бы показывал свои преимущества перед не мыслящими биологическими существами. Перебороть это качество весьма не просто.

Блокчейн технология вносит существенное социальное изменение в эту систему. Она ничего не забывает. Безотзывные транзакции присутствуют в системе блокчейна крайне долгое время, по крайней мере, до тех пор, пока существуют базы данных распределенных протоколов. Это противоречит самой идее всепрощения в человеческом обществе и может являться антагонизмом для этой технологии, с которым нам придется сосуществовать, который нам придется решать, преодолевать либо смиряться (?).

Доверительные протоколы позволяют эффективно решать вопросы о подтверждении репутации в бизнесе. Если ранее банк мог отказать в кредите по самой простой причине, связанной с неизвестностью субъекта в неподтверждаемом микро-, малом бизнесе, то участие таких представителей в блокчейн операциях получения и возврата малых кредитов и других финансовых операций, с коллективным доверительным потенциалом и на основе цифрового удостоверения личности каждого участника системы, само по себе является проверяемым (протокольные блоки) и подтверждаемым уровнем репутации участника.

Но не все так просто.

При определенных условиях сплошная биткоинизация в неподготовленном обществе может привести и к существенной радикальной нестабильности, хаосу, криминализации общества за счет тех, кто, пользуясь физическим превосходством и угрозами, сможет перенаправить на свои интересы

все информационные и материальные потоки, созданные блокчейн технологиями.

Нельзя обойти и такую проблему в распределенных реестрах потребителей, как конфликт интересов групп пользователей и отсутствие какого-либо арбитража при отсутствии централизации в управлении. Примерами могут являться конфликты в системе биткоина, которые привели к появлению альтернативной валюты *BCH* к *BTC*, конфликты интересов в платформе *Ethereum*, для преодоления которых был даже создан альтернативный программный продукт *Plasma*, а также предприняты попытки создания альтернативных реестров. В целом проблема конфликтов интересов еще недостаточно изучена, хотя опыт *Ethereum* и *Bitcoin* может обобщаться и давать информацию к размышлению.

Обращая внимание на глобальность и высокую эффективность этих технологий, следует упомянуть и те проблемы, которые связаны с распространением блокчейн технологии.

1. Недостаточно развитая инфраструктура телекоммуникаций, препятствующая участию в системе отдельных пользователей (например, при общественном голосовании).

2. Высокая стоимость услуги [53] и преимущественно наличная экономика, в мировом теле которой более 40 % составляет микро-, мелкий и лавочный бизнес [54]. Такие компании, как «*Abra*», уже представляют глобальные платформы для решения задач управления любыми цифровыми активами, а совместно с блокчейн технологией создают приложения, обеспечивающие максимальный уход от наличной экономики. Это станет возможным только при условии, когда каждый смартфон получит возможности стать персональным банкоматом.

3. Недостаточная грамотность людей. Проблема их способности работать в сети, пользоваться гаджетами, проявлять умение на уровне пользователя работать в основном программном продукте, незнание основ персональной безопасности. Например, опыт *AOL* с 2,3 млн греческих подписчиков, электронные адреса которых, по незнанию, дрей-

фуют теперь в интернете, массовое спамирование и отсутствии интернет-этикета разрушили эту систему [55, 56].

4. Недоступность блокчейн технологии для среднестатистического гражданина. Существуют принципиальные возможности покупать, продавать, сдавать в аренду с помощью смартфонов, использовать их как персональный банкомат для оплаты и получения денег, для зарабатывания денег, для оплаты услуг и игры на бирже, приобретения и продажи акций и многого другого, недоступные для неподготовленного пользователя. При условии полного доверия к участникам системы. Однако, большая часть людей не может этого осуществлять по причине сложности для них технологии блокчейн, недоступности инженерной техники, необученности.

5. Мы вправе требовать от государства обеспечения сплошной сетевой грамотности населения, как фактора развития государства, наравне с общей грамотностью. Нужны простые компьютерные школы, например, при вузах.

6. Сложность программного обеспечения, необходимость создания гаджетов и программ, полностью адаптированных под обычные знания человека в области базовых образовательных наук: математики, физики, лингвистики, логики и др.

7. Требование в институтах общества лидерства этих институций. Как противодействие таким явлениям, как коррупция, местничество и др., блокчейн может изменить моральную парадигму общества в целом, при некоторых глобальных усилиях всего общества.

Социальность такого уникального явления, как блокчейн технологии, далеко не изучена и, при определенных тенденциях в обществе, может стать препятствием для их распространения в современном мире. Но этим еще раз подчеркивается их глобальность и крайняя актуальность для общества XXI века, необходимость их развития и изучения не только с технической, но и социально-экономической точки зрения.

III

Экономика и кибербезопасность

3.1 Коммерческое доверие как экономическая парадигма *dg*-общества

Мировая торговля и коммерческие отношения составляют основу экономик абсолютного большинства стран мира. Важнейшей основой таких отношений является уровень доверия между субъектами торговли и других экономических отношений. Из парадигмы чисто психологической, понятие «доверия» постепенно переходит в понятие экономическое, требующее своего количественного содержания, смыслового наполнения, делающее его по существу экономическим показателем, влияющим на товарообороты, оборачиваемость финансовых средств, доходы предприятий торговли и др. К этому общество подталкивают принципиально новые технологии учета коммерческих операций, степень доверия к партнерам, банкам, логистическим системам и др. В частности, речь может идти о технологиях распределенных реестров, о блокчейне, о глобальном информационном пространстве, о сетевых технологиях и децентрализованном распределении ресурсов.

Доступность сетевой информации через любые информационные каналы: спутники связи, радиосигналы, телефоны, сотовую связь, кабельное ТВ, логистические системы движения материальных потоков, признание интернета базовой потребностью для общества (ООН, 2016 г.), принципиально низкая стоимость доступа сделали интернет не только всепроникающим инструментом, но и эффективным спосо-

бом зарабатывания денег, основанным на доверительности участников. Возможности для оцифровывания любого предмета, документа, любой материальной ценности постепенно приводят к сопоставительной унификации всего и вся. Можно рассчитывать, что *dg*-общество, на этой основе, постепенно перейдет и к принципиально новым экономическим законам и отношениям, которые упростят эти отношения, сделают их более прозрачными и достоверными для потребителей, без огромной бюрократической прослойки, которая системно тормозит естественный путь натурального отбора и природной конкуренции. Вне сомнения, интернет, как инструментарий таких изменений, должен соответствовать определенным требованиям и, в частности, с точки зрения безопасности для его пользователей, если речь идет о вмешательстве в такие области, как коммерция, экономика.

Например, современное общество, в особенности его молодежная часть, постепенно приходит к идее получения социальных изменений не внутри общественной системы, а вне ее. И хочет этого. Но не с помощью голосования, а другим равнозначным и долее равноправным способом. Одним из механизмов такой альтернативы может являться технология блокчейн и ее доверительные протоколы. Отдельные страны, например, Великобритания, Австралия, Канада, не приняли методы централизованной регистрации населения и унифицированной для всей страны *ID*-карты людей, принимая во внимание такие общечеловеческие ценности, как неприкосновенность жизни и индивидуальная безопасность человека.

Уже на начальном этапе развития интернета как системы в нем проявились такие качества, как способности к капитализации всей *dg*-информации, вмешательство в индивидуальное (в том числе, внутреннее) пространство человека и др. Любые аргументы в пользу того, что интернет имеет позитивное социальное назначение, пасуют пока перед тем, что

на нем можно зарабатывать огромные деньги. В очередной раз в истории развития общества, *социальность не устояла перед естественным отбором и его детищем – бизнесом, неудержимым накоплением капиталов, как формой развития общества, подавляя интересы большей его части в угоду меньшей.* Только на более высоком социальном уровне, на уровне социального доверия между участниками таких систем.

Источник доходов в сетях, – это не только всеобъемлющая реклама или платные новинки информационного пространства. Это и контроль за доступом к информации, монополизм отдельных *IT*-компаний и появление надконкурентной среды на основе огромных баз данных, концентрация сугубо конфиденциальной информации в отдельных руках, формирование системы негласного отслеживания личного пространства каждого человека, дезинформация и утечки информации в сетях, пропаганда, криминальные манипуляции и появление собственного преступного сообщества, как традиционное отражение всех проявлений в нем высоких и низменных материй.

Темпы развития всемирной паутины давно опережают результаты ее эксплуатации. Мир оказался не готовым к таким темпам. Оказалось, что создание знаний из доверительной информации стоит значительно дешевле и осуществляется значительно быстрее, чем создание материальных товаров. И имеет высокую, не в пример материальным товарам, рыночную цену.

Обратим внимание на то, что интернет высвобождает определенные ресурсы. В первую очередь, это средства визуальных коммуникаций и обеспечивающие их технические системы. Это, в частности, места общения людей по интересам: библиотеки, театры, кинозалы, спортивные площадки, парки, офисы, газеты или их варианты и др. Все это можно определить в старой терминологии, как «домашние кухни»,

где еще в XX веке люди общались больше всего. Этот ресурс прошлого сегодня становится все более невостребованным. Рано или поздно, перед обществом станет задача научиться рационально пользоваться таким высвобожденным экономическим ресурсом, причем не как альтернативой всемирной паутине, а как согласованным ресурсом, дополненным в своей нише социального доверия.

Решение этих проблем, по мнению многих аналитиков, лежит в социально-правовом поле и имеет вектор направленности в плоскость глобальных соглашений. Т. Бернерс-Ли назвал их конституцией интернета, которая может позволить при помощи технических средств, законов и правил исключить вмешательство государств и отдельных корпораций в личное пространство отдельного человека без его разрешения, без тотального контроля за индивидуальными данными пользователей. Для этого необходима новая архитектурная среда для хранения данных с открытым кодом доступа, исключающая, как ненадобный, всякий контроль над пользователями и основанная на доверительности между участниками. Бернерс-Ли назвал такую систему хранения данных *PODS* (*personal online data stores*).

В условиях зарождавшейся в древнем мире торговли уровень доверия между покупателем и продавцом был минимальным. Продавец мог продать некачественный товар под видом качественного. Покупатель мог рассчитаться поддельными деньгами, в пределе, обанкротив продавца. Перекупщик рисковал резервированными на время купли-продажи товара деньгами. Ростовщик не мог полностью доверять заемщику средств, довериться подтверждающим документам кредитуемого субъекта. И если они не вызывают доверия, или не появился некто третий, кто выступит гарантом финансовой сделки, кредит не будет выдан. Сдающий деньги в депозит испытывает недоверие к банку на предмет возврата суммы депозита, который осуществляется банком весьма не-

охотно, потому что, как правило, рассинхронизированными во времени были денежные потоки кредита и депозита. И так далее.

Последовательно вместе с деньгами человек создал учетный реестр (гроссбух), в котором помещал записи о сделках, данные о товаре, услугах, об оплате сделки, когда их количество измерялось сотнями, а количество людей (*N*), принимающих участие в них, измерялось тысячами. Такие учетные записи становились условными «документами доверия», в которых делались записи о достоверности таких сделок. В 1494 году итальянский математик, один из основоположников современных принципов бухгалтерских учетов Лука Бартоломео де Пачоли впервые систематизировал знания по написанию бухгалтерской документации, в том числе, по учетным книгам. Но даже после этого не утихла вражда между церковью и предпринимательством [1]: добрый христианин не мог быть ростовщиком или предпринимателем, а тем более, вести учетные гроссбухи с двойной системой записи в учетных документах, обозначенных другим великим итальянцем Леонардо Фибоначчи как основы современной ему экономики, без которой тогда не обходился ни один торговец.

Трудно переоценить важность учетных записей в экономике. Их цели совпадают с целями, которые ставили перед собой создатели блокчейн технологий. Это отслеживание сделок, фиксация их во времени, доказательность сделок, или транзакций, взаимное соблюдение обязательств большой группой участников системы. Учетные документы позволяют нейтрализовать форму взаимного недоверия. Учетные книги создаются на каждом предприятии, в региональной и национальной экономиках в виде финансовых отчетов, балансовых нормативов, учетных записей движения денег и товаров.

Существует мнение [2] о том, что именно двойная учетность в бухгалтерии, распространившаяся в Европе в конце XV – начале XVI веков, стала основой для зарождения капиталистических отношений в феодальной экономике отдельных стран (Британии, Нидерландов, Испании). Но даже после этого легальные учетные записи оставались главным документом, подтверждающим доверительность сделок и финансовых потоков.

В качестве примера можно привести стремительный взлет банкиров Дома Медичи из Флоренции, без ведома которых не осуществлялась ни одна торговая сделка в средневековой Европе. Одним из важных аргументов для ведения финансового бизнеса в Старом Свете они поставили именно учетные записи по таким сделкам, владелец которых, имел влияние на весь сегмент торгового бизнеса. На основании этой базы данных Дом Медичи мог держать под контролем практически всю экономику итальянских герцогов, французских и испанских королей, германских правителей при наличии полного доверия к этому Дому. Такой порядок вещей существовал, благодаря протоколам подписываемых записей дебита и кредита, как системы двойной учетности и возможности ретроспективного отслеживания достоверности и законности большинства сделок.

Пользуясь в дальнейшем системой двойных учетных записей, зародившаяся банковская система могла осуществлять переводы денег без их физической доставки. Существенно ускорился оборот денежных средств, что повлекло за собой увеличение прибылей, рост капитала. В основе этого лежало правило «доверия» к банкам [3].

О том, что системы централизованного управления, например, банки, не могут быть субъектами доверия, свидетельствует многое. Подтверждением этому является, например, опыт банка *Lehman Brothers*, который в 2007 году по отчетам имел прибыль в $4,2 млрд, а в следующем году обан-

кротился [4], имея фиктивные балансы и несостоявшиеся сделки, сокрытые долги, финансовые приписки и неоцениваемые инвесторами связанные с этим возможные риски [5].

Одной из причин замедления активности предприятий мелкого и малого бизнеса является ограничение доступа к кредитным финансовым ресурсам, в особенности, для покрытия периода доставки товаров, сырья, комплектующих от экспортера к зарубежному покупателю. Степень недоверия к сопроводительной документации мелкого и малого бизнеса весьма высока и небезосновательна. Опасность ошибочного, или чаще, намеренного дублирования принятых средств под залог партии товара, становится одной из глобальных проблем для развития такого бизнеса в условиях продвижения наукоемкой продукции на внешний рынок. Применение распределенных блокчейн-реестров и создание доверительных неуничтожаемых протоколов позволило бы в любой момент времени всем участникам движения товаров проследить подобные дублирования и полностью исключить подобные риски. По самым скромным подсчетам, мелкий и малый бизнес из расчета оборота на каждые $1000 мог бы иметь дополнительно доход в $80–200.

Но уже в 2005 году известный криптограф Йен Григ из компании *Systemics* предложил создавать третью учетную запись в виде программируемого специальным образом контента, как независимого реестра записей, доступного всем пользователям для просмотра, но защищенного от любых изменений, что защищало такой учет от любых подтасовок. А через несколько лет появился Сатоши Накамото...

Доверительные протоколы и система двойных ключей: общедоступного и сугубо индивидуального, восстановили в обиходе экономичность термина «доверие». Была впервые введена система учета, не требующая государственного обеспечения. Субъекты системы могли ее контролировать, но не изменять по своему усмотрению.

Старая добрая учетная книга гарантировала факт выполнения сделки, являлась инструментом, помогающим сохранять степень доверия. Современный распределенный реестр и доверительные технологии блокчейна ставят системы учета на уровень децентрализованного доверия ко всем партнерам по системе. Учетный реестр, составленный по правилам технологий блокчейна, позволяет получить абсолютно надежную запись. Эта запись может играть роль истины, на которую можно всегда ссылаться.

Поэтому вопрос об экономичности термина «доверие» может иметь основание.

Современные блокчейн технологии просто заставляют нас считать доверие важнейшей экономической субстанцией. Так ли это? Обезличенные доверительные протоколы, известные всем участникам системы, позволяют избегать централизованного управления и контроля, ставят огромное количество решаемых проблем в зависимость от делегированного доверия каждого участника.

Вместе с децентрализацией информации приходит централизация доверия [6]. Эта формула требует не только перестройки законодательной базы многих стран мира, но и изменения отношений между людьми. Блокчейн технологии, при широком их использовании, потребуют от людей большего доверия под гарантии всех остальных участников. Психологически это очень сложно, если принимать во внимание степень глобального недоверия, которое существует в мире между отдельными людьми, религиями, нациями, группами по интересам, наконец, национальными правительствами почти всех стран без исключения. Сейчас мы имеем систему тотального недоверия в обществе. Оно связано, прежде всего, с тотальным социальным неравенством, которое культивируется как один из способов обеспечения конкурентности между людьми, ухода от искусственного, социального равенства. Обществу придется решать глобальную задачу поиска

сути примирения, согласия, доверительности, доброжелательности в людском общении, правил, которые лучше всего изложены в религиозной литературе, в частности, в Библии, в Коране и др.

«Децентрализованная экономика также требует централизованного доверия» [3]. Эта старая истина, которая была рождена и развита еще в работах молодых социалистов А. Сен-Симона, Р. Оуэна, молодого К. Маркса, П. Кропоткина и др., но пока так и не нашла адекватного применения. И может стать наиболее непреодолимым препятствием в глобальном распространении блокчейн технологий в современном обществе. Потому, что децентрализованная экономика является пока не решенным и неразрешимым противоречием в мире. Ни руководители компаний, ни правительства отдельных стран, ни финансовые межгосударственные институты не готовы к передаче центральных полномочий в распределенные реестры участников. Должно пройти много времени в ожидании и появлении новых технологий, подобных блокчейну, их массовая реализация на практике. Пока новое не станет очевидным, пока мы эволюционным путем не придем к экономической демократии и не будем ее сравнивать с экономическим хаосом, как это случилось с идеями кропоткинского анархизма, бесталанно изувеченного историей и превратившегося в свою абсурдную противоположность.

Высшая степень доверия – это индивидуальная ответственность за свои действия по отношению ко всем участникам некоторого множества сделок, когда доверие становится нормой.

Как количественно можно определять степень доверия?

В социологических науках доверие определяется как ставка в отношении будущих непредвиденных действий других [7]. В психологии – это самостоятельная относительно

независимой формы веры, основанной на акте отношений. Ф. Фукуяма дает понятие доверия как «… ожидание того, что члены общества будут вести себя честно, проявляя готовность к взаимопониманию в соответствии с общепризнанными нормами» [8]. В экономике существует понятие доверия, как позитивных ожиданий определенных действий окружающих, которые влияют на выбор индивида, когда он должен начать действовать до того, как станут известными действия других.

Сказуемые типа «непредвиденные действия», «форма веры», «ожидание» явно не способствуют количественным оценкам предмета исследования. Используются методики социологического опроса, методы анализа фактических данных, которые также не дают количественных оценок предмету исследований. В работе [9] сделана попытка определить количественный показатель сводного индекса доверия при помощи эмпирических коэффициентов, отражающих результаты социологического опроса и коэффициента, получаемого путем расчета статистических данных определенных групп показателей. По утверждению самого автора, это оценочный метод, справедливый для узкого круга экономических систем.

Информацию о том, как можно рассчитать количественно коммерческое доверие, нам может дать блокчейн технология, в основе которой – распределенные протоколы знаний, требующих максимального и добровольного доверия от всех участников системы. Один из возможных вариантов расчета – по количеству участников сделки доверия. Один человек сможет доверять другому. Можно доверять двум, трем знакомым. Это не меняет ситуации. Это один уровень доверия. А если доверять приходится десятку людей, да еще кто-то из них незнаком с вами, то это уже другой уровень доверия. Причем, доверять двум или шести десяткам партне-

ров – тоже не имеет принципиального отличия. Напрашивается простой вывод: в первом приближении, уровень доверия – это может быть десятичный логарифм от количества (N) участников доверительного процесса $L = \lg N$. Условная величина $L = 0$ означает полное отсутствие доверия ввиду того, что это сугубо централизованная система, состоящая из одного субъекта. Величина $L \geq 2$ означает, что в доверительных отношениях находятся, по крайней мере, сто и более человек. Величина $L \geq 3$ означает, что взаимным доверием пользуются тысячи человек. Это, по крайней мере, определенная логичная шкала доверия. И шкала ответственности перед всеми.

Т. Фридман описал наш интернет-мир, как плоскость, в которой пребывает и экономика, и общество, и культура [10] вне иерархий и цензуры. Современная двухмерная (плоскостная) цифровая экономика типа «деньги-товар-деньги» в виде численных рядов, не предусматривала третьего измерения, например, в виде согласованных **доверительных действий** отдельных индивидов на следующем уровне, без централизованного вмешательства банков (рис. 3.1).

При введении третьей координаты – уровня доверия ($L = \lg N$) в системе происходит вынужденный всплеск деловой активности и уже на первом уровне ($L_1 > 1$) (мы видим увеличение количества сделок, а при $L_1 > 2$ следует ожидать роста количества участников доверительной системы, независимо от ее смыслового содержания).

Мир пока далек от системного феномена распределенного доверия. А ведь этот феномен бесконечно расширяет спектр доверительных участников. Если в традиционной сделке принимают участие два или другое ограниченное количество участников, то сделка в системе распределенного доверия может быть приемлема для неограниченного коли-

чества обезличенных участников, знающих о сути той или иной сделки (см. рис. 3.1). Ответственность за транзакции в этом случае возлагается не на банки, а распределяется между всеми участниками и вынуждает их быть перекрестными доверителями в системе.

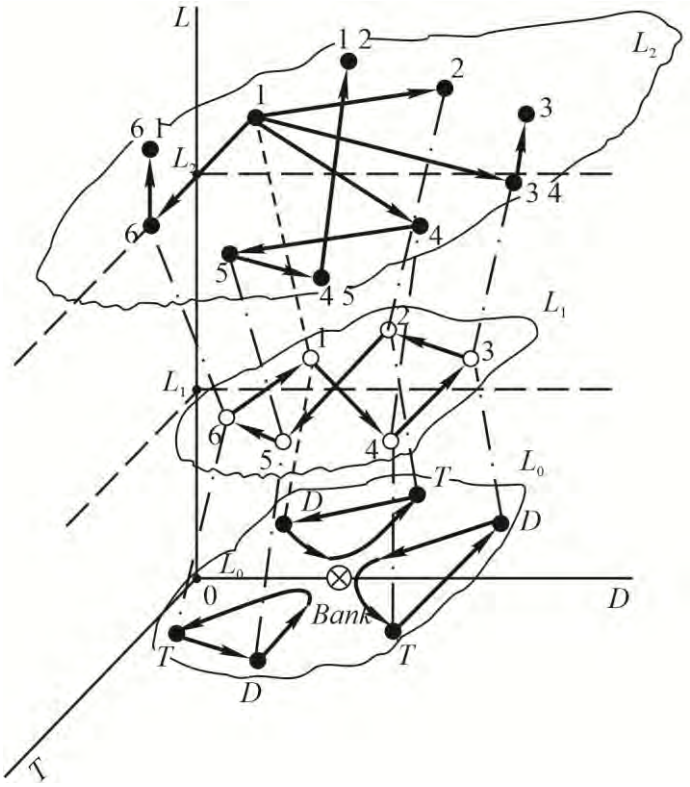


Рисунок 3.1 – Система товарно-денежных отношений при централизованном управлении (L_0) и в случае доверительных реестров распределения (L_i)

Сегодня уже никто не сомневается, что система распределенного доверия – это то, без чего что в последние годы тормозилось развитие интернет-сетей в целом [11].

В предложенной интерпретации численный уровень доверительности растет с увеличением числа участников транзакций (табл. 3.1).

Таблица 3.1 – Возможные транзакции при различных уровнях доверительности L_i между участниками (по данным рис. 3.1)

№	Уровень доверительности	Число участников (позиций), N	Число вариантов, ν	ν/N
1	L_0	6	3	$3/6$
2	L_1	6	6	$6/6$
3	L_2	10	36	$36/10$

Количественная оценка доверия может быть и иной, например, в процентном содержании до 100 %. Но практика показывает несостоятельность таких оценок, если в основе лежат современные доверительные технологии, для которых 100-процентный результат не идеал, а вполне реальное и стандартное состояние. И наоборот, **более** низкий процент доверительности полностью блокирует работу системы.

Таким образом, проблема определения уровня доверия в экономической среде общества, которое неуклонно идет по пути цифровизации (*dg*-общество), существенно актуализировалась с появлением технологий блокчейна, доверительных протоколов и распределенных реестров. В этом случае, двухмерная модель формулы «товар-деньги-товар» становится узконаправленной и должна уступать место моделям с

третьим измерением, например, уровнем доверительности в экономической системе.

3.2 Риски, связанные с хождением криптографических валют на международных финансовых рынках

В современном финансовом мире криптографическая валюта завоевала место под солнцем, являясь объективной данностью, обладающей своими ценными и не очень качествами. В любом случае, мировая общественность признала за криптовалютами право на существование. Причем, в большей степени криптографическая валюта здесь сыграла роль не как способ накопления денег и механизм осуществления денежного оборота, а как продукция компьютерных программных технологий нового поколения, которые избавляют две паритетные стороны любого обменного процесса от каких-либо посредников. Это очень важное качество операций, типа блокчейн привлекает к ним огромное количество людей и целые компании, которые находят применение новым компьютерным технологиям в самых различных областях человеческой деятельности. И не беда, что эти технологии, в первую очередь, проявили себя эффективно на финансовом поле, в попытках сформировать новое отношение к деньгам [12].

Мировая финансовая система весьма неоднозначно реагирует на появление криптографической валюты. Игнорировать ее уже не удается. Но признавать за ней права полноценных денег почти никто не берется. Даже такие страны, как Германия, Япония, Швейцария, США, которые признают за криптографической валютой весьма условный аналог денег и пускают их в оборот на своих торговых рынках, очень

осторожны в собственной юридической обоснованности этих действий, объясняя их, прежде всего, необходимостью вводить это явление в некоторое регулируемое правовое поле, снижая риски кибермошенничества. В некоторых странах (Сингапур, Россия, Болгария, Эстония) подобная легализация этого явления сопровождается обязательными акцентами на товарную сущность виртуальных монет, как некоторую программную продукцию, обязательно облагаемую налогом. Используется такое понятие как «частные деньги», которое, по-видимому, может иметь право на обозначение криптографической валюты с тем, чтобы обеспечить ей определенные права, отличные от прав традиционных валют (Германия). Присутствует термин «биржевой актив» (Норвегия). Но не валюта. При этом все делают акцент на высокие степени рисков, связанных с допуском криптовалют на финансовые рынки [12]. Но за ними уже текущий суммарный рыночный объем в $32 млрд, с чем нельзя не считаться.

Комиссия по финансовым преступлениям США очень осторожно относит биткоин к децентрализованной «валюте» с признаками виртуальности и требует лицензирования подобной деятельности, но, в то же время, склонна к освобождению криптовалют от НДС. По этому алгоритму пытается работать и Евросоюз, и Таиланд. Франция, в свою очередь, весьма осторожно относится к этому явлению, ограничивая хождение биткоинов, как явного источника криминала, не допуская их к финансовым операциям.

Китай, по этой же причине, запретил свободное хождение криптовалюты в стране, заявив, что биткоин и ему подобные не являются реальной валютой, и наказывает банки, которые обеспечивают ее участие в коммерческих сделках, ссылаясь на их потенциальную криминальную составляющую *и способности к киберпреступлениям* [12].

На сегодня ни одна страна в мире не обладает убедительным законодательством, позволяющим регулировать от-

ношения хотя бы с одним видом криптовалюты, например, в налоговом поле, или в области объективных финансовых обменных операций, или в области формирования системы денежных обязательств по отношении к криптовалюте, включая кибермошенничество.

Следует не забывать, что за криптовалютой остается ничем не ограниченное право риска быть средством для отмывания денег, обладать возможностью уклонения от налогов, влиянием на права потребителей товаров, быть способными к уходу от декларирования имеющихся активов всех видов, а также обладать запредельной шкалой рисков, связанных с операциями с криптовалютой – купля, продажа, обмен, конвертация [12]. То есть быть предметом киберпреступлений.

И, безусловно, это риски, связанные с приостановкой участия субъекта криптографических операций в сети подобных себе потребителей криптографической валюты или его полным уходом из этого рынка и потерей своих вкладов. На сегодня ни одна страна в мире не обладает убедительным законодательством, позволяющим регулировать отношения хотя бы с одним видом криптовалюты, например, в налоговом поле, или в области объективных финансовых обменных операций, или в области формирования системы денежных обязательств по отношению к криптовалюте. Не забудем, что за любыми деньгами стоит, в пределе, некий товар. Сколько товара, столько и денег необходимо. Поскольку деньги – наиболее ликвидный из имеющихся условных товаров [3]

В конце 2017 года впервые на товарные рынки США решением комиссии по срочной фьючерсной торговле сырьевыми товарами была допущена торговля посредством криптографической валюты. Но при этом признается, что биткоин, как компьютерная продукция, должен иметь статус товара. И не более. Потому, что по своим свойствам, в частности, сопоставлению относительно существующей товарной массы

(а именно, ее обеспеченности), торговым процедурам, налоговому законодательству, в конечном результате, *сегодня биткоин не имеет прямого отношения к деньгам,* а генерируется только благодаря определенным компьютерным программным действиям и энергозатратам на генерирование, как программный продукт, товар. В этом контексте возможности покупки товаров при помощи криптовалюты должны рассматриваться как безвалютный обмен «товар-товар», при условии постоянной динамичности и поддержки движения самого биткойна в интернет-сетях. По крайней мере, Национальная Комиссия по ценным бумагам США (*SEC*) упорно не признает за криптовалютой объективных качеств денег и занимается мониторингом этого рынка. Правда, отдельные штаты страны были вынуждены создавать некоторые правила оборота криптовалют, признавая за ними, тем не менее, только права некоторых товарных активов [12].

Пример деятельности ФРС США говорит сам за себя. Многое может сказать то, что эта организация стоит на страже интересов доллара, как общемировой валюты, но пока никак не проявляет обеспокоенности по поводу активности биткоинов и других криптовалют. Почему?

Но есть еще более убедительные примеры. В мире существует 15 компаний, совокупные активы каждой из которых превышают размер $1 трлн (табл. 3.2). При этом 11 из них представляют финансовый бизнес США, 3 – Европейский Союз и одна из Японии. Как правило, такие компании в первую очередь должны реагировать на подобные изменения на финансовых рынках, потому что они могут принести для них колоссальные потери. Но пока таких реакций на финансовых рынках со стороны этих компаний мы не видим. Это при том, что криптографическая валюта не имеет за собой обеспеченности каким-либо товаром или произведенными услугами, то есть является необеспеченной виртуальной валютойс[12].

Таблица 3.2 – Клуб компаний с финансовыми активами более $1 трлн

№	Наименование компании	Сумма денежных активов	
		$ трлн	%
1	*BlackRock Inc*. (*USA*)	5,7	19,79
2	*Vanguard Group* (*USA*)	4,4	15,28
3	*State Street Global Advisors* (*USA*)	2,6	9,03
4	*Fidelity Investment* (*USA*)	2,3	7,99
5	*J. P. Morgan Asset Management* (*USA*)	1,9	6,60
6	*BNY Mellon* (*USA*)	1,8	6,25
7	*Amundi* (*France*)	1,6	5,56
8	*Legal & General Investment Management* (*UK*)	1,3	4,51
9	*Government Pension Investment Fund* (*Jp*)	1,2	4,17
10	*PIMCO* (*USA*)	1,0	3,47
11	*Capital Group* (*USA*)	1,0	3,47
12	*Northern Trust* (*USA*)	1,0	3,47
13	*PGIM* (*USA*)	1,0	3,47
14	*Wellington Management* (*USA*)	1,0	3,47
15	*Norges Bank Investment Management*	1,0	3,47
	ВСЕГО активов:	28,8	100

Ради уточнения роли необеспеченности денег в мировой экономике приведем цифры: мировой финансовый долг в 2017 году достиг $133 трлн, что в 19–26 раз больше всей массы обеспеченных товарами и услугами денег. Причем,

доля США и их компаний в мировой долговой корзине составляет более $17 трлн, доля стран ЕС – $15,5 трлн, доля Японии – примерно $12 трлн [3].

Прочность современной экономики можно измерять, например, количеством экономических кризисов, потерями каждого государства и отдельных людей. А можно измерять резистентностью к современным вызовам, одним из которых уже сегодня можно считать появление виртуальных денег в виде изменяющихся криптографических валют, их роли в современных денежных отношениях [12].

Денег всегда не хватает. Это психологический факт. Поэтому люди принимают во внимание любую возможность «оприходовать» свой труд, свои запасы: в виде золотых украшений, золотых монет, депозитных вкладов, устойчивой валюты, в частности, долларов или евро и, теперь, доступных (пока) цифровых денег. Без учета их ликвидности, надежности, способности быть предъявленными к оплате за товар или услуги. Когда «деньги» принадлежат не тому, кто их заработал, а тому, кто имеет доступ к этому коду, знает пароли к его упаковке. Вне государственных контролирующих систем. Поэтому, криптовалюта – по-настоящему кошмар для налоговых служб...

В некоторой степени появление системы криптоплатежей биткоин стало реакцией безопасности общества на произвол мировых финансовых монополий, его ответом на заражение финансовой сферы «вирусом» необеспеченных денег. Однако, подобный «вирус» таким же «вирусом» вылечить невозможно. Однозначно можно говорить о том, что биткоины представляют собой также вариант необеспеченных денег, а их хождение в финансовых системах способствует развитию кризисных явлений в мировой экономике. Сегодня невозможно со стопроцентной гарантией говорить о том, что биткоин найдет свою нишу в мировой финансовой системе. Возможно, что и он уйдет в небытие. Но как вари-

ант необеспеченных денег, как денег, не имеющих товарного содержания.

Почему сегодня количество пользователей криптовалюты измеряется миллионами и при этом постоянно растет? Почему периодически появляется в интернете информация о том, что биткоины становятся субъектами торговых операций то в одной, то в другой компании? Почему дозировано поступает информация о том, что разрешающие организации в отдельных странах дают зеленый свет биткоинам, но при этом стыдливо утверждают, что все-таки биткоин, как компьютерный продукт, должен иметь статус товара, но не денег? Рынок криптовалюты постоянно кем-то «подогревается» периодически и малыми дозами. Перефразируя известный французский оборот, напишем: «ищите деньги». В нашем случае это как раз подходит [12].

Можно не сомневаться, что в основе всех криптографических валютных операций все-таки лежит доллар. Его нужно продать или заложить, чтобы получить в конечном результате условную монету биткоин. Стоимость ее на 1 января 2017 года – $1000, стоимость условно на 1 июня 2017 года – $5 тыс., $11 тыс. – на 1 декабря 2017 года. На конец 2017 года это уже $20 тыс. А дальше? А дальше, возможные $50 тыс. – на 1 июня 2032 года? Где предел такого роста? Только за 2017 год биткоин вырос в цене в 20 раз! За год! Клондайк для опытных биржевых игроков! Но почему-то финансовые биржи не спешат допускать криптографическую валюту для полноценных операций. Опасаются обвала? Возможно. Но возможно и нет. Потому, что биткоин не настолько силен в межвалютных операциях, как доллар, йена, евро. Но многотысячные процентные прибыли впечатляют? Ни доллар, ни йена, ни евро такой прибыли ни на одной бирже никогда не давали. И давать не будут. Потому, что запредельные ставки реальной валюты могут привести к обвалу торговли по всем другим биржам, торгующим товаром.

Деньги так себя вести не могут. Это уже не деньги, а нечто иное [12].

По своим свойствам, в частности, сопоставлению относительно существующей товарной массы (а именно ее обеспеченности), торговым процедурам, налоговому законодательству, в конечном результате, **сегодня биткоин не имеет прямого отношения к деньгам**, а генерируется только благодаря определенным компьютерным программным действиям, как программный продукт, товар. В этом контексте возможности покупки товаров при помощи криптовалюты должны рассматриваться как безвалютный обмен «товар-товар», при условии постоянной динамизации и поддержки движения самого биткоина в интернет-сетях. По крайней мере, Национальная Комиссия по ценным бумагам США (*SEC*) упорно не признает за криптовалютой объективных качеств денег и занимается мониторингом этого рынка. Правда отдельные штаты страны были вынуждены создавать некоторые правила оборота криптовалют, признавая за ними, тем не менее, только права некоторых товарных активов [12]. Поэтому на вопрос, криптовалюта – это деньги или нет, можно с уверенностью в 99 % сказать – нет. И дело здесь не в кибербезопасности.

Возможна альтернатива: либо криптовалюта сегодня представляется суперликвидным товаром со специфическим источником происхождения, либо современная экономика сегодня стоит на пороге невиданных изменений (это тот самый 1 %), что само по себе, представляет опасность для общества. Прежде всего, изменений относящихся к товарообменным операциям, из которых вскоре напрочь уйдет свойство эквивалентности по отношению к деньгам. Это уже следствие опасности для общества, для благополучия отдельного человека, которую несет существование биткоина.

Трудно сразу понять такие перспективы, но совершенно новые особенности торгового обмена могут стать явью.

Например, когда избыточная масса существующей в мире традиционной валюты и, прежде всего, доллара будет покрываться с избытком совершенно иной, дорогой, но высоколиквидной валютой (криптографической, например), которая, поглотив долларовую массу, тем не менее, не станет ее альтернативой по причине своей виртуальности и отношению к производимому товару, но откроет дорогу к обмену на самое себя некоторых промежуточных ликвидных активов. К ним гипотетически могут быть отнесены отдельные группы сверхликвидных товаров: нефть, газ, вода, отдельные виды пищевых продуктов, наиболее эффективные виды вооружений. Ведь умудрились мы торговать «Киотскими» квотами на чистый воздух? Может быть нечто еще. Но это нечто должно взять на себя роль промежуточного универсального обменного продукта, субвалюты, которая будет способна поглотить избыток существующих действующих денег по отношению к мировой товарной массе [12].

Но не подобной ли субвалютой, пока товарной, является биткоин? Правда, это уже будет не торговля в традиционном смысле. Возможно, в ее основе будет, на первых порах, «перегретый» неравномерно распределенными товарами современный мировой рынок, который со временем уменьшится в объеме, по мере потребления всех этих товаров. То, что за криптографической валютой никак пока не предусматривается собственного участия в получении прибавочной стоимости товарной продукции, может быть в перспективе основанием для замирания производства всех нужных, но объективно нерентабельных товаров и услуг, может стать основанием для существенных перекосов в ценовых политиках всех уровней [12].

Следует не забывать о важнейшей социальной опасности, которая следует за криптографическими валютами. За ними остается ничем не ограниченное правило быть средством для отмывания денег, возможности уклонения от нало-

гов, влияние на права потребителей товаров, уход от декларирования имеющихся активов всех видов, а также запредельная шкала рисков, связанных с операциями с криптовалютой – купля, продажа, обмен, конвертация. И, безусловно, риски, связанные с приостановкой участия субъекта криптоопераций в сети подобных себе потребителей криптовалюты или его полным уходом из этого рынка и потерей своих вкладов. На сегодня ни одна страна в мире не обладает убедительным законодательством, позволяющим регулировать отношения хотя бы с одним видом криптовалюты, например, в налоговом поле, или в области объективных финансовых обменных операций, или в области формирования системы денежных обязательств по отношении к криптовалюте.

Биткоины являются реальным примером трансформаций сущности современных денег. И, по-видимому, цифровые деньги в таком аспекте себя еще далеко не исчерпали. Социальная и экономическая опасность в этом случае присутствует, по крайней мере, на исходных этапах развития этого кластера глобального информационного пространства.

Современные технологии блокчейна, основа появления криптографической валюты, безусловно, найдут свое собственное применение в самых различных областях, хотя бы потому, что в их основе лежит грамотная попытка при помощи информационных сетей создать альтернативную современным банкам систему доверительных отношений без посредников. Но только в качестве товарного продукта, продаваемого, покупаемого, производимого. Систему, как будто бы, защищенную от внешнего проникновения к хранящимся данным посредством верифицированных цифровых «печатей».

Именно эта способность блокчейн операций делает их интересными в самых различных областях человеческой деятельности. Например, в области Интернета вещей, о чем пишет в книге «Революция блокчейна» Алекс Тэпскотт. В компании *Intel* создана платформа, при помощи которой можно

отслеживать сети поставок морепродуктов. Группа компаний *AusPost*, *PwC*, *Alibaba Group*, используя методику блокчейна, создала систему «*Food Trust Framework*» для управления цепями поставок пищевых продуктов с одновременным контролем качества и прозрачности поставок. Даже корпорация *Bosch* уже сумела использовать приложение блокчейна для предупреждения кибермошенничества при контроле показателей счетчика автопробега автомобилей. Широкое поле для применения этих технологий открывается в логистике, в маркетинговых операциях.

Только из этого краткого перечня можно судить об универсальности системы подобных смарт-технологий, как надежного способа обмена ценностями, материальными потоками, благодаря широким возможностям блокчейна в областях создания новых типов рыночных отношений и новых рынков товаров с функциями рынка ресурсной оптимизации.

Но это будет уже совершенно другая для нашего общества сверхсовременная экономика, как продукт глобальной информационной сети. Это может быть экономика репутаций, экономика взаимного внимания и доверия, своеобразная «услужливая» экономика, адаптированная под потребителя. Экономика, которая совершенно не будет нуждаться в государстве. Экономика, основанная на совершенно иных, пока не совсем понятных, правилах и условиях. Такая экономика может иметь право формироваться, как переходная альтернатива от современной экономики, базирующейся на бесконтрольном печатании денег, неуправляемом развитии необеспеченности мировой валюты товарами и услугами, к экономике, в большей мере децентрализованной, без необеспеченных валют. В ее основе может быть положено общее правило: каждая торговая операция должна понемногу «поглощать» часть массива прошлых необеспеченных денег. В качестве такого поглотителя возможна криптовалюта. *Такая экономика может носить форму промежуточного звена на пути перехода к совершенно иной децентрализованной миро-*

вой экономике, ориентированной на правила существования глобального информационного пространства, со всеми его достоинствами и недостатками [12]. Риски, связанные с движением криптовалюты, по всей вероятности, невозможно сконцентрировать в одной работе. Тем не менее, один из скрытых рисков, связанный с отказом от хождения реальной денежной валюты, тенденции, которая просматривается во многих странах мира, можно отследить. И, безусловно, велика роль денег в этих изменениях. Одним из критериев здесь может быть готовность каждой страны, входящей в систему мировой торговли, к отказу от торговли за наличность на самом низком уровне – на уровне обывателя в пользу их цифровых аналогов (табл. 3.3).

Готовность страны к отказу от наличности в финансовых расчетах в пользу цифровых аналогов денег показывает степень адаптации ее к новым правилам торговли и определяется несколькими критериями. В первую очередь, это индекс цифровой эволюции в экономике страны. Он показывает возможности финансовых организаций управлять деньгами, обозначенными в цифровых кодах при условии сохранения и поддержания их реальной стоимости. То есть, способности к валютному обмену при помощи компьютерных программ, цифровых кодов. Но при этом важна готовность населения к переходу к цифровым деньгам, наличие компьютерных кабинетов, кошельков, наличие инфраструктуры, например, для интернет торговли и т. д. [12].

Абсолютная «цена» наличности – это индекс паритетности между наличными деньгами и их цифровыми аналогами. Определяется весовым показателем устойчивости национальной валюты к другим валютами, в первую очередь, к доллару. При этом актуальным является сохранение возможности для обеспечения стоимости денежной массы за счет перехода к цифровым деньгам.

Полный отказ от кэша в пользу цифровых аналогов денег обеспечить пока не возможно ни в одной стране мира. Но вектор в направлении постепенного уменьшения кэша просматривается почти во всех относительно экономически развитых странах.

Таблица 3.3 – Готовность отдельных стран к отказу от наличных денег (по данным работы [13]; пояснения по тексту)

№	Страна	Абсолютная «цена» наличности	Индекс цифровой эволюции	Характеристика перехода к цифровым деньгам
1	Швеция	0,4	57	В стране сохраняется возможность для создания реальной стоимости денег за счет ускорения перехода к цифровым деньгам
2	Дания	0,5	51	
3	Кения	0,3	18	
4	Турция	0,65	33	
5	Южная Корея	4,4	51	Устойчивость экономики страны к переходу на цифровые деньги при сохранении их реальной стоимости
6	Япония	5,5	47	
7	США	7,5	54	
8	Филиппины	5,8	20	
9	Египет	8,5	18	
10	Россия	8,5	26	
11	Бельгия	15	45	Максимальный потенциал для создания реальной стоимости за счет приоритета инвестиций для перехода в цифровую плоскость
12	Германия	18	48	
13	Франция	36	48	
14	Мексика	26	28	
15	Индия	82	22	

Отказ от наличной валюты либо снижение объемов ее хождения в торговых и других операциях будет способствовать изменению правил мировой торговли и мировых торговых отношений. Такой процесс невозможен без существенных потрясений для любой финансовой системы.

Сделаем вполне обоснованное допущение о том, что риски, связанные с уходом от кэша, могут иллюстрироваться, например, сборкой катастроф Уитни. Подобная сборка Уитни в координатах *OXYZ*, где *X* отражает абсолютную денежную массу, отнесенную к изменяющейся его части $\left(M_k / \Delta K\right)$, которой оперирует финансовая система государства, Y – временная координата (T) (годы), а Z – динамика изменяющегося кэша $\left(\Delta K\right)$, который существует в стране в данный отрезок времени и показывает область финансовой неустойчивости, которая может существовать в условиях хождения конкретной валюты. В указанных координатах энергетическая функция сборки Уитни описывается уравнением типа

$$W(\Delta K) = 0,5\frac{\mathrm{d}(0,25\Delta K^4 + \left[0,5b\Delta K^2 M_k + cT\Delta K\right])}{\mathrm{d}\,\Delta K} =$$

$$= \Delta K^3 + bM_k\Delta K + cT$$

Общая расчетная тенденция такова: чем больший в стране объем кэша, отнесенный к его изменяющейся части $\left(M_k / \Delta K\right)$, тем вероятнее, что движение в сторону его уменьшения приводит к необратимым изменениям в национальной экономике. Но это в пределе. Практика несколько иная. Например, зависимость $\Delta K\left(T\right)$ согласно данным [13] для стран с различной экономикой, представлена в табл. 3.4.

В сравнении с данными таблицы 3.3 можно говорить о многообразии финансовых ситуаций, относительно рисков перехода на электронные денежные обороты для разных стран. Тем не менее, такие риски существуют всегда.

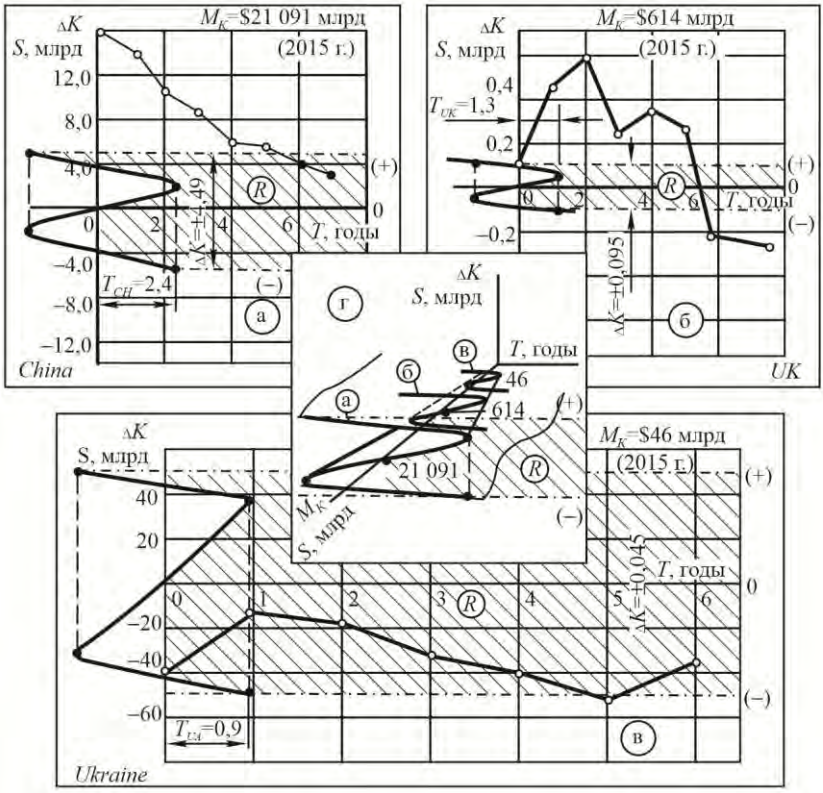
Таблица 3.4 – Динамика движения кэша (ΔК) в разных странах мира ($, млрд)

Страна	Период контроля, годы							Характеристика групп
	2008	2009	2010	2011	2012	2013	2014	
США	4,25	3,53	3,37	2,92	2,05	1,35	0,65	Устойчиво избавляются от кэша
Китай	14,8	13,1	11,38	9,31	6,96	4,10	2,17	
Индия	0,74	0,65	0,47	0,21	0,35	017	0,05	
Швейцария	0,54	0,40	0,39	0,15	0,18	0,093	–0,045	
ОАЭ	0,14	0,13	0,12	0,09	0,10	0,73	0,16	
Южная Корея	0,69	0,82	0,65	0,45	0,51	0,35	0,58	Балансируют в области финансовой устойчивости
Швеция	0,022	0,061	0,062	–0,02	0,0	–0,04	–0,06	
Беларусь	–0,00	0,00	–0,00	0,00	0,00	–0,02	–0,02	
Великобритания	0,21	0,47	0,57	0,28	0,34	0,24	–0,012	
Польша	0,01	0,067	0,060	–0,01	0,04	0,00	–0,04	Балансируют в области профицита или дефицита
Румыния	–0,00	–0,00	–0,01	–0,01	0,01	–0,04	–0,04	
Чехия	–0,02	–0,00	0,00	–0,03	–0,00	–0,02	–0,03	
Южная Африка	–0,01	–0,01	–0,02	–0,05	–0,02	0,00	–0,01	
Украина	–0,04	–0,02	–0,02	–0,04	–0,04	–0,06	–0,04	

Кибернетические риски, связанные с ликвидацией кэш-массы в государстве, зависят от скорости этого процесса (ΔK), отношения ко всей денежной массы (M_k) и продолжительности во времени (T). Для области финансовой неустойчивости, связанной с уменьшением кэша, предложена расчетная параметрическая зависимость вида $\Delta K = 1,3 \cdot T^2 - 5,6 \cdot T + 5,9$ (рис. 3.2). Тогда каждая из экономик будет по своему соотноситься со временем и скоростью ликвидации кэша. Выделим несколько ярко выраженных групп стран в зависимости от их адаптации к цифровым денежным технологиям (табл. 3.3) и относительно их движения в сторону уменьшения собственного кэша (табл. 3.4).

К первой группе относятся страны, которым не нужны дополнительные усилия к переходу на электронный финансовый оборот. Это Китай, Дания, Финляндия, Новая Зеландия (рис. 3.2, а). Эти страны проявляют осторожность, ориентируясь на партнеров по международной торговле, таким образом, чтобы не дестабилизировать своими инициативами собственную твердую валюту. Тем не менее, например, Китай, Швейцария в этой группе системно сбрасывают свой кэш. И страны из этой же группы: Южная Африка, Турция и др. пока не готовы к такому переходу, но сохраняют возможность при внешней поддержке их национальных валют (табл. 3.3, 3.4). Правда, не для всех, и это очевидно, такая поддержка возможна [12]. Динамика движения их общего кэша такова, что минимизация реальной валюты пока не приводит к рисковым отношениям в экономике (рис. 3.2, а).

Вторая группа стран весьма адаптирована к возможностям перехода к электронным деньгам. Это Великобритания, США, Япония, Нидерланды, Южная Корея и др. Высокий индекс цифровой эволюции в финансовой сфере при устойчивости цены собственной валюты тому доказательство (рис. 3.2, б и табл. 3.4). Но и США, и Япония в настоящее время настойчиво снижают свой кэш в пользу электронных денег.



а) избавляющихся от кэша (Китай, Дания, Новая Зеландия, Тайвань, ...);

б) балансирующих в зоне финансовой устойчивости (Британия, США, Южная Корея, Швеция, ...);

в) балансирующих в зоне финансовой неустойчивости (Украина, Чехия, Венгрия, ...);

г) поверхность неустойчивости при управлении финансами. R – области финансовых рисков

Рисунок 3.2 – Риски, связанные с уменьшением массы кэша, для некоторых государств мира

И третья группа стран, прежде всего лидеры Европейского Союза готовы к такому переходу, но ограничены возможностям своих партнеров по Союзу, в частности, Испанией, Чехией, Польшей, Литвой и др., для которых нужны существенные инвестиции для поддержания стоимости вращающихся в этих странах национальных валют: злотого, кроны и др. [12].

Украина, как и некоторые другие государства бывшего Советского Союза, относится к промежуточным странам, в которых государственный кэш будет существовать еще весьма долго, потому что финансовая система страны на протяжении многих лет устойчиво находится в зоне самых разных финансовых рисков и не обладает собственными возможностями для системного избавления от наличности (рис. 3.2, в).

В целом следует предполагать, что неизбежность отказа от наличных денег в пользу цифровых аналогов диктуется всеми изменениями, которые претерпевает современная торговля, ее растущие объемы и необходимые для этого скорости денежных оборотов. Но надо понимать, что это может привести к существенным изменениям в самих торговых процедурах, изменить сущность балансов в торговле, что может привести к непредсказуемым последствиям, не всегда лояльным для многих стран, в особенности с недоразвитой, в настоящем понимании, экономикой [12].

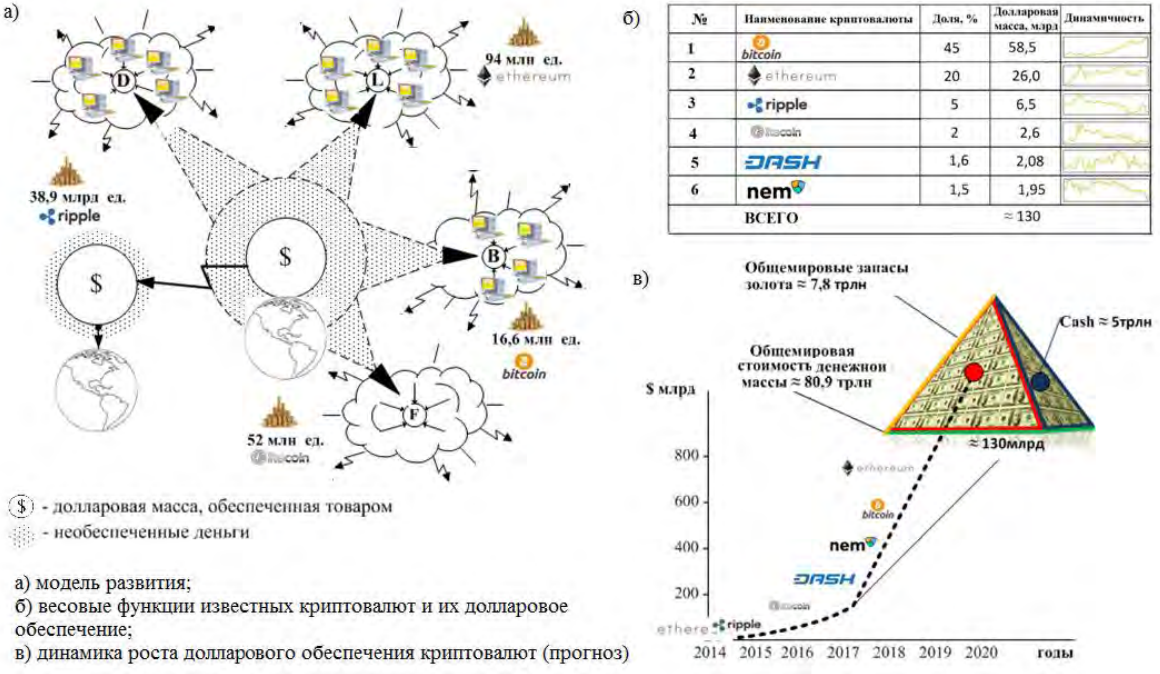
Криптографическая валюта – не единственное оригинальное изобретение в области современных финансовых технологий. Существуют и обратные тенденции создания валют местных сообществ, дополнительных корпоративных валют, валют городов и общин, которые появляются как результат соглашения между теми, кто собирается пользоваться этими валютами в обход официальных платежных средств, но на законных основаниях. Известные «бристолики», местная валюта г. Бристоль (Великобритания), являются наиболее удачным примером [12].

Другим примером может служить система милебонусов, впервые созданная союзом пяти крупнейших авиа-

компаний мира с целью повышения маркетинговой привлекательности перелетов за счет накопления премиальных миль при перелетах. Но постепенно бонусные «мили» в виде платежных карточек стали играть роль платежных средств не только при перелетах, но и при покупке других билетов, при аренде автомобиля, оплаты гостиниц, различных туристических услуг, покупки товаров. Сегодня этими компаниями выпущено на рынок более 14 трлн авиа-«миль», которые, параллельно существующим валютам, пускаются в оплату за огромное количество товаров и услуг. Четырнадцать триллионов «миль» – это, как минимум, в два раза больше, чем вся долларовая наличность в мире. За «милями», безусловно стоят реальные мировые валюты, доллары, фунты и др., в том числе, необеспеченная товаром их часть. Это «валюта», которая путем перераспределения, отражается в балансовых цифрах этих авиакомпаний, и потому она применима в качестве оплатного средства.

Еще одним примером может служить созданная в Японии система *Fureai Kippu* («билеты заботы»), применяемая для начисления бонусов за услуги в самых различных областях, которые затем расходуются на обслуживание более, чем 1,8 млн престарелых людей по тем услугам, которые им не представляются действующей японской медициной. Такие бонусы также превратились в валюту сообщества. Таких примеров множество. И они становятся действенной альтернативой для мировой финансовой системы, перетягивая на себя определенную часть товаров и услуг, которые были произведены за счет реальных валют [12].

Эти альтернативные не валютные системы оказывают как свое положительное влияние, например, на развитие местного малого бизнеса, на социальные системы поддержки, так и отрицательное влияние, способствуя увеличению количества платежных средств, не обеспеченных реально произведенным товаром или услугами, способствуя развитию инфляционных процессов.



№	Наименование криптовалюты	Доля, %	Долларовая масса, млрд	Динамичность
1	bitcoin	45	58,5	
2	ethereum	20	26,0	
3	ripple	5	6,5	
4	litecoin	2	2,6	
5	DASH	1,6	2,08	
6	nem	1,5	1,95	
	ВСЕГО		≈ 130	

а) модель развития;
б) весовые функции известных криптовалют и их долларовое обеспечение;
в) динамика роста долларового обеспечения криптовалют (прогноз)

Рисунок 3.3 – Место и роль криптовалюты в современной мировой экономике (гипотеза)

Вернемся к биткоинам и их роли в современной экономике, связанной с возможностями мировой торговли. Имеет право на существование следующая гипотеза относительно перспектив биткоина (стр. 185, рис. 3.3).

Таблица 3.5 – Весовые функции некоторых наиболее популярных криптовалют на конец 2017 года (по данным работы [14])

№	Наименование криптовалюты	Курс, $/монета	Эмиссионное ограничение, число монет	Потенциальный размер кэша, $
1	*Bitcoin* (*BTC*)	19000	21 млн	400 млрд
2	*Darkcoin* (*DASH*)	14	22 млн	300 млн
3	*Litecoin* (*LTC*)	33	84 млн	2,77 млрд
4	*Feathercoin* (*FTC*)	0,43	185 млн	80 млн
5	*Primecoin* (*XPM*)	3,56	14 млн	50 млн
6	*Peercoin* (*PPC*)	6,04	48 млн	290 млн
7	*Namecoin* (*NMC*)	8,0	21 млн	168 млн
8	*Freicoin* (*FRC*)	0,7	100 млн	70 млн
9	*Eathereum* (*ETH*)	460	28 млн	13 млрд
	ВСЕГО			416 млрд

Становится все более похожим на то, что биткоин – это развивающийся проект, соавторство которого принадлежит в

конечном результате тем, кто сегодня породил лавинообразные процессы появления необеспеченных денег [3]. Цель – уменьшить общее давление на мировую экономику со стороны совокупной массы необеспеченных денег, в первую очередь, доллара. В этом случае легко предположить, что биткоин, как губка, напитавшаяся массой этих долларов, вращающихся в мировой финансовой системе, в некоторый момент «лопнет», и подомнет под себя огромное количество необеспеченной денежной массы, тем самым подняв условную ценность оставшейся ее части до необходимого в мировой торговле уровня. Это шанс остаться доллару «на плаву», укрепить эту валюту еще на долгое время. Это шанс не развалить мировую торговлю и избежать потрясений, подобных мировым войнам. Если сегодня криптовалюта занимает нишу в $420 млрд, то через два-три года эта ниша может составить более $1 трлн, что уже сопоставимо с суммами необеспеченных денег (стр. 186, табл. 3.5).

Опыт создания таких пирамид уже давно накоплен, хотя и дискредитирован во всем мире. Так что грех им «не воспользоваться» на благо «золотого тельца». Результатом может быть появление нового крепкого доллара, который попрежнему будет составлять основу мировой торговли [12].

Для этого необходимо соблюдать определенные условия для собственно проекта «биткоин», а именно:

– нельзя объявлять биткоин общепризнанной валютой, по крайней мере, официально, но следует поддерживать к ней подобный интерес, как к неофициальной валюте (в настоящее время условие соблюдается);

– способствовать вовлечению в проект максимального количества людей, обладающих свободными активами и валютой (условие соблюдается);

– стимулировать возможности для накопления биткоинов у резидентов с обеспечением условия необратимости (соблюдается периодически);

– по возможности, ограничивать развитие свободной торговли за биткоины, но не запрещать вовсе, способствуя их накоплению у резидентов (пока соблюдается);

– стремиться не подорвать авторитет доллара в этой игре (условие соблюдается на правах роста ликвидности биткоина);

– уходить от официального сопоставления доллара и биткоина.

Таким образом, почти все эти условия для реализации такого проекта до сих пор соблюдаются. Намеренно или спонтанно – пока остается непонятным. Но как гипотеза самопроизвольного или запланированного процесса по указанному алгоритму, она имеет право на существование.

Существует мнение, что с развитием электронных денег мировая торговля претерпит весьма существенные изменения далеко не косметического характера, что не может не быть опасностью для стабильности всего общества, по крайней мере, на начальных этапах таких изменений. Из торговли *уйдет изначальное понятие эквивалентности обмена*. Причиной этому будет являться «плавающий» курс электронных денег, определяемый только спросом и предложением на них во время каждой конкретной операции, динамичностью этих операций, и не обеспеченный другими материальными ценностями. Но без участия государственных организаций, отвечающих за стабильность национальной валюты. К этому уже давно существуют предпосылки, в частности, связанные с диспропорциями между стоимостью различных товаров относительно вкладываемого в них человеческого труда в зависимости от его качества (физический или интеллектуальный, энергоемкий или экономный, зависящий от способа переработки сырья, эффективности и так называемой наукоемкости технологий и т. д.).

При этом мир вынужден будет претерпевать существенные потрясения, вызванные потерей эквивалентности не только в отношении отдельных товаров, но и в отношении

многих национальных экономик, среди которых будут выделяться два типа: универсальные, рассчитанные на производства широкой корзины потребительских и других товаров, и моноэкономики, рассчитанные на производство монопродукции, зависимые от условий внешней торговли, от импорта огромного количества товаров, от финансового дисбаланса между экспортом и импортом, который по идее должен покрываться только разницей между спросом и предложением.

Существенным является и риск, связанный с изменчивостью курса биткоина, так называемой его волатильностью. Известно, что биткоин защищен от инфляции ограничениями в выпуске 21 млн монет, но при этом не обеспечен ни золотом, ни фиатными валютами и никакими другими стабильными активами. Высокая волатильность курса биткоина – диапазон может колебаться в течение года в пределах 100–300 %, что используется иногда для курсовой торговли биткоинами. Но, в целом, неустойчивость курса – это актуальная проблема, которая вызывает сомнение к этой субвалюте. Для снижения таких рисков создана система криптовалют, привязанных к некоторым стабильным и ценным активам, например, в привязке к фиатным деньгам (наиболее неприемлемый вариант), нефти, золоту, в привязке к другим криптовалютам, к выпуску ничем не обеспеченных монет биткоина. Это так называемые стейблкоины, несвободная криптовалюта, стоимость которой привязывается, например, к доллару, к унции золота, к другой криптовалюте.

Вариант стейблкоинов – это попытка уйти от конкретного риска, это своеобразный мостик между биткоином и теми финансовыми операциями, которые требуют стабильности, в частности, средство хранения капитала, его обмена, расчета, покрытия межкурсовых издержек, то есть там, где требуется стабильная валюта.

Общее здесь является следующее свойство криптовалют: выигрывая в децентрализации, криптовалюта проигры-

вает в волатильности. И, наоборот, выигрывая в волатильности, в степени стабильности, криптовалюта, тут же, проигрывает в доверительности. И стейблкоины – это только вариант ухода от социально-экономического риска, который сам по себе не является наиболее эффективным, но свидетельствует о том, что варианты поиска решения существуют.

По всей видимости, остановить движение денежных альтернатив типа биткоин в мире уже не под силу никому. Электронные средства платежей, развитие интернета, привыкание к этим системам платежей со стороны населения дают право надеяться на их развитие только в правовом поле, с позиций и объективности, и повышения безопасного пользования электронными заменителями традиционных денег, рассчитывать на существенные изменения условий традиционной торговли, как одного из краеугольных видов человеческой деятельности.

Не является ли вектор на развитие криптографических валют ответом на современные мировые экономические кризисы? Не являются ли электронные деньги финансовой «пеной» для современной экономики? А может, электронные деньги, через многие катаклизмы, которые предстоит пережить, станут или уже являются способом коренной ломки традиционной экономики и зарождения новых экономических законов и новых экономических отношений в обществе потребления? Создавая новые опасности для процессов стабилизации мировой экономики последних лет.

Не будем торопить события. К тому же, в литературе встречаются и другие альтернативные мнения относительно подобных новшеств, как о некоторых глобальных финансовых пирамидах, основанных не на пропорциональности доходов и расходов, а на самых низменных качествах человека, как субъекта новых видов кибермошенничества в области того же самого глобального информационного пространства и возможностях современных информационных сетей, пользователи которых еще не раз будут и удивлены, и обнадеже-

ны, и обескуражены новыми возможностями цифровых технологий недалекого будущего [12].

Подобные гипотезы могут иметь место, если дать волю фантазии, на предмет развития криптографических валют в том понимании, в котором нам их сегодня подают, в частности, если общество будет подведено к пониманию того, что криптовалюты имеют перспективу движения в качестве новой валюты, с совершенно новыми свойствами и качествами. Либо в виде иных проектов, на которые сегодня так щедра наша мировая экономика.

3.3 Финансовые киберпреступления как форма опасностей для человека

Во все времена, под преступлением понималось действие, которое нарушало действующие законы и подлежало уголовной ответственности. Модификации этого определения были связаны, чаще всего, с формами управления обществом, государственным строем и определенными правилами, оговариваемыми людьми различных сословий .

Преступная деятельность, к сожалению, всегда существовала в обществе и является неотъемлемой частью морали или аморальности этого общества, одной из форм перераспределения материальных и моральных ценностей. Многочисленные формы преступлений со временем изменялись, уходили одни, появлялись другие, соответствовавшие времени, социальному и экономическому устройству. Еще ни одному социальному строю или государству не удалось побороть преступность. Любые формы существования человека и государственных строев обязательно со временем порождали свою преступную среду. Лицо типичного преступника столь многообразно, существует столько его образов и среди низших слоев общества, и среди его лидеров, и среди обывате-

лей, и среди интеллектуалов. Мы не сможем провести достаточные исследования в этой области, тем более, что их предостаточно. Нас более интересует опасность, исходящая от преступной среды, которая имплементирована в глобальное информационное пространство, существует и развивается там по таким же законам, по которым она появлялась и развивалась в других общественных или даже государственных средах.

Появление такой многогранной и всеобъемлющей социальной ниши, как глобальное информационное пространство, было просто обречено на появление там преступной среды. Потому, что ГИП и его составляющие, в частности, такие как, собственно, информация обо всем, изначально привлекли к нему не только хакеров, но и финансовых преступников, представителей преступных группировок, мафиозных групп и одиночек, способных к работе с этим специфическим предметом. Появился новый вид преступника, обладающий специальными знаниями в области информатики, имеющий опыт работы в информационных сетях, владеющий знаниями по криптографии. Это и профессионалы, и талантливые самоучки. Недаром, долгое время правовая наука терялась в вопросах наказания за такую деятельность, и многие хакеры уходили от наказания, не получая надлежащей государственной, а иногда и общественной оценки. Но появились и новые жертвы таких преступлений, в частности, пользователи интернет из числа благополучных граждан, неблагополучных людей, узнавших, что такое интернет-зависимость [15].

Предмет преступной деятельности в интернете может быть связан с использованием персональных данных о человеке с целью завладении его имуществом путем грабежа, с шантажом, с целью вымогательства, провокациями, связанными с принуждением использования служебного положения человеком. Но наиболее частыми являются киберпресту-

пления в финансовой сфере, как наиболее продуктивной, с точки зрения преступника.

Финансовые преступления, которые связаны с интернетом, имеют свои корни еще со времен появления безналичных денег, когда финансовые операции осуществлялись на основании не всегда достоверных документов, например, пресловутые авизо, кредитные операции, оффшорные накопления огромных, необлагаемых налогами безналичных средств, за которыми всегда стоят банки или другие поручители, фиктивные фонды и трасты с их не всегда обеспеченной доверительностью и многое другое. Имея такую почву для процветания финансовых преступлений, с которыми не всегда получалось успешно бороться, стали почвой для формирования субъектов подобных киберпреступлений и объектов таких преступлений, предметом которых являлся именно масштабный инструментарий в виде информации, доступ к которой был либо крайне легким, либо обеспечивался посредством взлома, вмешательства в программный продукт субъектов, хранителей финансовых ценностей, обеспечивавшего деятельность всех выше перечисленных инструментов.

Сам факт сосредоточения в одном источнике знаний огромных объемов весьма полезной и актуальной для многих видов человеческой деятельности информации, в том числе, персональной информации о самых различных людях, с различными социальным положением, уровнем доходов и богатства, информации о деятельности компаний, банков, привлекает в эту нишу большое количество преступников, целью которых является незаконное обогащение.

Простой пример. Раньше для ограбления банка преступникам требовалось организовать группу подельников с определенными техническими навыками, готовить специальное оборудование для взлома систем технической защиты или сигнализации, осуществить физическое проникновение в хорошо защищенный банк, идти на возможное физическое

устранение свидетелей и пр. для достижения цели – ограбления. Чтобы ограбить банк и украсть оттуда деньги, нужно было, по крайней мере, туда войти.

Сегодня такие преступления тем более опасны, что имея на вооружении сетевое оборудование общего пользования, подбирая коды и пароли, взламывая сервера банков, современный киберпреступник способен, не выходя из помещения присутствия, взломать счета подходящего банка, вписаться в его финансовые документы и за счет безналичных финансовых проводок похитить необходимую, подчас просто огромную сумму денег, спрятав ее за счет многочисленных финансовых проводок от дальнейшего поиска. Такое преступление требует более интеллектуальных действий, но не требует физического риска. Поэтому они становятся более предпочтительными, даже для неподготовленных технически преступников, которые, в этом случае, вынуждают выполнять интеллектуальную работу наемных партнеров из числа качественных программистов. Электронные деньги снимаются хакерами, не выходя из собственной квартиры. Физические трудозатраты прошлых и современных преступлений стали несоизмеримыми.

Финансовые киберпреступления являются сегодня одними из наиболее важных опасностей, которым подвергается любой человек в современном оцифрованном обществе, когда при приобретении любой покупки или услуги приходится не расплачиваться наличными деньгами, а полагаться на условную услугу банка, хранителя личных сбережений человека. При каждой такой операции человек подвергается двойной опасности. Во-первых, любая ошибка банка при финансовом обеспечении деятельности клиента может привести к потере денежных ресурсов. А во-вторых, возможности современных хакеров позволяют вмешиваться в банковские отношении с клиентом посредством изъятия денег с безналичных счетов, пользуясь украденными персональными дан-

ными, паролями пользователей, или, например, считыванием кодов доступа во время самой типичной налично-безналичной транзакции.

Уже в момент написания этой работы пришла информация о крупных утечках персональных данных (имена, номера социального страхования, данные кредитных карт 15 млн держателей банковских карт *Nong Hyup Card*, *Lotte Card*) в Южной Корее, а также персональные данные 6 млн пользователей почты *Yahoo* в январе 2014 года [16, 17]. Люди потеряли огромные средства на электронных счетах.

Люди пока не научились ни на программном, ни на аппаратном уровнях надежно защищать цифровую информацию от проникновения извне. Именно этим, а также распространенностью и доступностью информации обусловлен безудержный рост финансовой киберпреступности. Это еще один существенный недостаток ГИП, как части системы «человек-машина» применительно к человеку.

Европейская комиссия только в 2000 году признала киберпреступления незаконными действиями, представляющими опасность для человека и подлежащими уголовному преследованию [18]. Наиболее типичными здесь являются следующие финансовые преступления: отъем денег с банковских счетов, несанкционированный доступ к персональным базам данных человека, кибератаки на корпоративные сети и серверы, с целью нарушения работы предприятия или компании, создание соответствующих вирусов. Появились и неизвестные ранее виды преступлений – «интернет-сговор» с целью синхронизации антисоциальных либо экономических действий, «сетевые войны», «интернет-терроризм», «интернет-забастовки». Все это создает угрозу экономике, финансовым системам целых стран и является важной причиной процессов современной дестабилизации мирового общества. Это угроза социальной и политической безопасности, очень часто – угроза физическому состоянию отдельного человека,

угроза социальной безопасности. Формируется собственная преступная интернетовская субкультура, в которую уже входят представители интеллектуальной рабочей силы.

Шестой технологический уклад, к которому относятся *IT*-технологии, теперь объединяет традиционных рабочих для таких действий в интернете и формирует новую интеллектуальную элиту, которая уже осознает себя на уровне пролетариата и по заработкам, и по социальному положению. Такие «пролетарии» теперь выполняют роль членов преступных группировок, они формируют свою оправдательную мораль, свой индивидуальный шарм, рейтинговую систему авторитетности и другие символы преступного общества. В основе этого общества – опасность для людей.

В течение последних 10 лет число финансовых киберпреступлений увеличилось в 300 раз, а их ущерб измеряется десятками миллиардов долларов [18, 19]. Нашла свою нишу в интернете и традиционная преступность – в виде сайтов по продаже наркотиков, оружия, проституционных услуг – самых доходных статей преступного бизнеса. Достаточно сказать, что только благодаря порно-сайтам доходы от этого бизнеса возросли в 2,5 раза, а доходы от распространения наркотиков – в 3–3,5 раза [20]. Сюда же относятся сайты террористических организаций, порталы фашиствующих, воинствующих националистических организаций.

Мощности для вскрытия персональных данных и объемы торговли ими за последние десять лет впечатляют. В 2013–2014 годах кибератака на финансовые сети компаний *Target* и *Home Depot* позволила изъять из пользования вскрытые данные по 100 млн кредитных карточек. Программа *ZeuS*, созданная российскими хакерами, на протяжении почти 10 лет обеспечивала доступ к секретной информации многих банков и компаний, позволяла осуществлять покупки секретной информации за биткоины и инсайдерские сделки. Общая сумма бизнеса превысила $100 млн. Программа не

взламывает банковские счета, а кодирует программный продукт компании, предназначенный для автоматизации финансовых операций, извлекает его и продает в таком виде для дальнейшего взлома.

С 2001 года заработал *Web*-сайт под названием *CarderPlanet*, который по существу стал первым в интернете воровским ресурсом для обмена, продажи кредитных паролей, взломанных кредитных корточек, номеров украденных банковских счетов. Задействована платная реклама, появился собственный финансовый оборот, свой электронный форум, позволяющий осуществлять реальный сбор информации для будущих финансовых киберпреступлений. Сайт имел свои степени защиты от проникновения, собственную систему регистрации. Огромное количество пользователей таких сайтов – в России и Украине.

Торговля персональными данными в самых различных вариантах стала одним из наиболее престижных и выгодных бизнесов в мире.

В целом, киберпреступность постепенно стала одним из наиболее опасных для общества злом, связанным с интернетом, глобальным информационным пространством, с открытыми списками персональных данных [21]. Этой информацией заполнены современные медиа. Можно привести только несколько примеров. В 2000 году хакеры взломали платежные системы провайдера электронных платежей *E-Money* и похитили базы данных по платежным карточкам 38 тысяч клиентов. Затем подобная акция была предпринята в отношении Web-сайта *Western Union,* где был получен доступ к персональным данным 16 тыс. клиентов. Кроме прямых потерь, компании подверглись шантажу и были вынуждены оплатить за будущую конфиденциальность хакерам крупные суммы денег. В 2003 году зафиксирована самая крупная на тот период хакерская атака на интернет-ресурс по обслуживанию карточек *Data Processing International*, в результате

которой были вскрыты персональные данные на 8 млн пользователей. Защищаясь от преступной среды, например, королевская прокуратура Великобритании получила возможность преследовать тех интернет-пользователей, которые входят в социальные сети под вымышленными именами и «проявляют агрессию» по отношению к другим людям, считая это формой онлайн-преступности [22].

Как в новом и специфическом продукте криминальной среды, в киберпреступности и киберрасследованиях все чаще проявляется ранее не существовавшая практика вынужденного всеобщего недоверия к субъектам таких расследований, включая собственно сотрудников управлений по делам киберпреступлений. Примером может служить дело сотрудника ФБР Эрнеста Хилберга, который с 2005 по 2009 годы системно преследовался из-за работы со своими киберагентами из числа жителей Украины, которых он успешно курировал по делу о сайте *CarderPlanet*, а также других активных субъектов электронных взломов. Прокуратура США не имела возможностей доказать непричастность самого Хилберта к киберпреступлениям, против которых он работал. Настолько тонкая граница между действиями преступников и их преследователями требует совершенно нового законодательства для защиты последних в современном максимально информатизированном обществе.

Одной из важнейших форм воздействия глобального информационного пространства на человека является искажение правового поля, в котором существует общество и человек. На протяжении многих лет существования глобального информационного пространства и его инструментариев, общество так и не смогло дать однозначной правовой оценки даже не самому виду этих преступлений, а правовой оценке опасности, которой подвергается и отдельный человек, и все общество, пользуясь благами этой новой и современной социальной ниши. Только одно перечисление юридических

документов, составляющих область кажущейся безопасности от киберпреступности, показывает слабую правовую готовность общества к реакции на все опасности, угрожающие человеку [23, 24, 25]. Это, в частности:

– Конвенция ООН против транснациональной организованной преступности 2000 года;

– Окинавская «Хартия глобального информационного общества» 2000 года;

– Женевская Декларация принципов «Построения информационного общества» 2003 года;

– Тунисская программа для информационного общества, принятая в 2005 году;

– Программа «Информация для всех», принятая ЮНЕСКО в 2001 году.

Доступ к цифровым технологиям и их использование в качестве инструментария для доступа к другим цифровым технологиям – это один из главных ключей, при помощи которых можно иметь целенаправленный доступ к секретам банков, отдельных фирм, финансовым проводкам, денежным накоплениям и др. Включая технологические секреты, которые, благодаря компьютерным взломам, стали доступными для хакеров. На этих правилах была создана наиболее современная система преступлений, связанных с работой любых предприятий.

Например, с целью оптимизации производственных процессов, синхронизации всех без исключения логистических операций на предприятии, последнее вводит системы цифрового управления потоками сырьевых и продукционных материалов. Это дает огромные преимущества в виде векторных направленных поставок продукции фирмам-потребителям, исключает потребность в складских помещениях, в промежуточных погрузочно-разгрузочных операциях, снижает временные издержки. Иными словами, цифровая синхронизация в технологических процессах сбалансированного по материальным потокам предприятия позволяет получать

существенную экономию и, таким образом, становится эффективным инструментарием в любом производстве. Кроме того, цифровая продукция на предприятиях присутствует в виде компьютерной обработки изображений самого разного назначения: сканеры штрих-кодов, системы допуска к отдельным подразделениям, в виде индивидуальных данных работников, имеющих изолированный доступ к информации и т. д. Это наиболее прогрессивные технологии с современной логистикой и надежным партнерством.

На первый взгляд, что можно получить от взлома таких программ? Только временные сбои в логистике предприятия, до тех пор, пока программа не будет восстановлена, что решается абсолютно просто, одним дублированием таких программ. Тем не менее, такие преступления стали весьма эффективными и, самое главное, трудно доказуемыми. Хакеры научились выводить из строя целые предприятия, принимающие участие в строгих графиках кооперативных поставок. Нужно только выбрать одно предприятие, производящее ключевое изделие, без которого конечный кооперативный продукт выпущен не будет. Уже сейчас имеется информация о таких атаках на отдельные компании.

Сеть заводов *AW North Carolina* (США), специализирующаяся на производстве автомобильных деталей для компаний *Toyota* (Япония) в 2017 году подверглась кибератаке. Были заблокированы производственные линии, производящие комплектующие детали для автомобилей. Компьютерные взломщики обладали информацией о графиках работы, режимах технологического процесса. Ежечасные потери фирмы составляли $270 тыс. Огромное количество рабочих оставалось без зарплаты не только в Каролине, но и в Японии, в Китае. Атака грозила остановкой конвейеров еще на 12 корпоративных предприятиях. Цена вопроса состояла в выкупе права разблокирования компьютерных программ компании *AW North Carolina* в размере $10 млн, что сопоставимо с совокупным ущербом этих предприятий в течение

полусуток. Логика преступления состояла в том, чтобы требуемый выкуп был сопоставим с величиной ущерба, чтобы сделать сделку реальной для пострадавшей стороны. Предприятие испытывает давление не только от преступников, но и от партнеров по бизнесу, что делает их сговорчивее и платежеспособнее.

Уже с 2015 года 2673 предприятия США стали жертвами подобных киберпреступлений и обратились за помощью в ФБР. Но многие идут на вынужденную сделку с преступниками и не обращаются за помощью. Компания *Lloyd's of London* представила суммарный ущерб от таких преступлений только за 2016 год. Это $450 млрд.

В основе таких киберпреступлений лежит главная логика: выбить производство из ритмичного графика, разрушить ритмичность материальных потоков, разорвать обязательную контрактную связь между предприятиями-партнерами и поставить перед фактом угрозы огромных финансовых потерь. Нарушение логистики большинства существующих производств четвертого-пятого технологических укладов способно приводить к весьма существенным потерям, ради избегания которых компания готова платить преступникам, даже не прибегая к услугам полиции. Потому, что современный процесс расследования по времени явно не успевает за последствиями преступления.

Следует вывод о том, что методы рассматривания подобных киберпреступлений должны быть пересмотрены в направлении поиска системно быстрых подходов к следам и источникам таких преступлений. Это становится особой формой следственных действий, которая в настоящее время быстро развивается.

Одним из способов воздействия на производственный процесс является поиск в технологической цепочке такого временного интервала, в рамках которого изделие может находиться в данном состоянии только кратковременно. Например, в пищевой промышленности – это период окисления

продуктов, их кратковременное тепловое состояние. Это временные интервалы, в течение которых изделие или его часть испытывают фазовые изменения (испаряются, конденсируются, мгновенно плавятся и кристаллизируются). В металлургии и других отраслях, это, например, нарушение режимов термической обработки изделий. В автомобильной промышленности это производство широкого спектра деталей и узлов, без которых дальнейшая сборка и, тем более, продажа конечного продукта, невозможна. Иногда приостановка технологического процесса приводит к повреждению изделия или полуфабриката, получению явного брака в массовом количестве. Скрытой формой таких атак является блокирование части управляющих программ, отвечающих за последовательность обработки детали, когда теряются определенные незначительные по времени технологические процессы, приводящие к массовому появлению брака. Примерами могут служить массовые отзывы готовых автомобилей с рынка продаж самыми знаменитыми компаниями, например, Тойота, Мицубиси.

В основе таких диверсий лежат знания основ таких технологических процессов. Именно поэтому в преступные группы хакеров попадают специалисты в области инженерии, в области современных технологий. Тем самым расширяется сам спектр преступной среды.

Подобные атаки осуществляются и относительно банковских технологий. Нет надобности блокировать счета и снимать с них деньги, переводить их по многочисленным банковским проводкам в другие хранилища. Достаточно изменить технологии обслуживания клиентов банков, обеспечив хаос, чтобы потребовать от жертвы некоторой денежной компенсации.

Компьютерный вирус *Petya A,* поразивший в 2017 году Украину, нанес ущерб не только банкам и информационным сетям, но и телефонным станциям, электрохозяйству и метро многих городов страны, аэропортам, предприятию «Новая

почта», торговой сети «Эпицентр», сети заправок *WOG* и ТНК, телеканалам «24» и *ATR*. Приостановлены были все диагностические и другие операции в медицинских учреждениях, люди оказались без экстренной медицинской помощи. В списке вымогателя, запустившего вирус *WannaCry,* – десятки предприятий Украины, банки «ОТП-банк», «Ощадбанк», «Укргазбанк», «Киевэнерго», ДТЭК, «Укрпочта», тысячи устройств по всему миру.

Примеров таких значительно больше, чтобы стоило более активно заниматься этой проблемой в рамках более тщательных исследований.

Кибернетическая преступность и ее финансовая компонента являются одной из наиболее важных опасностей, которые связаны с современным глобальным информационным пространством. Здесь представлены наиболее крупные финансовые потери, которые несут и банки, и компании, и государство, и отдельные люди. Если на протяжении веков, преступность в самых негативных проявлениях была связана с лишением человека жизни, грабежами, воровством, относящимся, как правило, к отдельному человеку или нескольким людям, то современная преступность характеризуется не просто отъемом имущества, а огромными масштабами этой деятельности и отношением ее одновременно к огромному количеству людей. Эти свойства киберпреступности требуют от сообщества совершенно иных правовых реалий, иной степени вины за такие преступления, иных форм наказания для таких преступников. Правовая компонента этой работы должна стать одним из факторов, который позволит феномену глобального информационного пространства не только остаться на плаву, но занять подобающую ему социальную нишу, развиваться и становиться истинно нужным для общества.

IV

Инженерия и кибербезопасность

4.1 Ожидаемые и реальные риски в блокчейн технологиях

Появившиеся, благодаря сетям интернет, возможности для суперкоммуникаций там, где ранее они были просто невозможны, не только упростили человеческое общение, но привнесли элементы коммуникативности, которые ранее были неприменимыми, как неэтичные, опасные для жизни, запрещенными по причинам криминала и т. д. Многие исследователи обращали внимание на эти негативные стороны сетевого общения и предрекали ему определенные угнетающие трансформации.

Существует предположение, что именно обесконеченное сетевое общение стало предпосылкой появления пятой вычислительной парадигмы [1] в виде технологий блокчейна, которые по своей универсальности и уникальности обещают стать в обществе некоторым функциональным сетевым продуктом нового универсального поколения. Ради этого, видимо, можно смириться и с четвертой, одной из последних на сегодня суперкоммуникационных информационных парадигм.

Далее все идет по спирали.

Сегодня в мире активно обсуждаются и реализуются проекты применения технологий блокчейна. В основе стоят возможности этого компьютерного продукта, которые связаны с такими его качествами, как надежность, универсальность и отсутствие посредника. Можно обобщить: техноло-

гии блокчейна применимы там, где имеются любые дискретные материальные потоки и где до этих технологий существовала необходимость в некотором *операторе, принимающем на себя посреднические функции* между источником и потребителем. Поэтому реальные и субъективные риски становятся определенным препятствием на пути распространения современных технологий в различных отраслях бизнеса и хозяйства [2].

Напомним, что, в некотором приближении, блокчейн операция – это многофункциональная информационная технология учета некоторых обобщенных активов, например, регистрация движения дискретного материального потока между участниками определенной группы, каждый член которой обладает вполне конкретной, но обезличенной и неизменяющейся информацией обо всех транзакциях внутри этой группы. Регистрации таких транзакций являются вполне объективными и независимыми от внешнего проникновения и осуществляются без какого-либо посреднического исполнения. В учетной основе блокчейн операции находится алгоритм, сжимающий каждый актив любого размера до короткого кода из 64 символов (ХЕШ), который становится уникальным для данного документа, однозначно идентифицирует его для пользователей, но не восстанавливает исходную информацию и не позволяет ее изменять после так называемого майнинга. Такое определение технологий блокчейна весьма общее, но для наших целей в этой работе вполне применимо, так как позволяет найти общие признаки для возможностей их широкого использования [2].

Технология, которая вначале стала основой для появления целой области так называемых «виртуальных валют», уже сегодня находит широкое применение, в том числе, вне финансовых систем (табл. 4.1), как новая организационная парадигма для организации и учета активов в любом виде человеческой деятельности.

Главные ее условия:

– наличие достаточной группы потребителей, которые не хотят зависеть от посредника;

– отсутствие единого управляющего центра (децентрализация);

– единственность записываемых данных и отсутствие возможности копирования [2].

Таблица 4.1 – Некоторые области применения технологий блокчейн (кроме финансовой)

№	Область применения	Компании	Примечание
1	2	3	4
1	Изменения в банковской индустрии устранением многих посреднических операций	«*Goldman Sachs*» (США), *UBS* (Швейцария)	Работает
2	Всемирная система внедокументальной идентификации личности на базе платформы *Microsoft Azure*	Компания «*Microsoft*» – проект *ID*2020. Компании «*Avanade*» и «*Accenture*»	Проект
3	Управление торговлей недвижимостью	*Crypto Realty Group*, платформа «*Deedcoin*»	Работает
4	Контроль за потоками сырьевых материалов в условиях реального производства (стартап «*Blockapps*»)	Компания «*BHP Billiton*» и компания «*ConsenSyS*»	Работает

Продолжение таблицы 4.1

1	2	3	4
5	Введение защищаемой цифровой документации от несанкционированного доступа	Компания «*Maersk*» и *IBM* (США)	Проект
6	Технологии страховой защиты морских грузоперевозок	Стартап «*GuardTime*» и компания «*Maersk*» (США)	Проект
7	Обмен, хранение медицинских данных и записей	Стартап «*Ontology*»	Проект
8	Контроль за цепями поставки морепродуктов	*INTEL*	Работает
9	Идентификация музыкального контента	*Open Music Initiative* (*OMI*)	Работает в тестовом режиме
10	Технологии противодействию подделкам продуктов питания «*Food Trust Framework*»	*Alibaba Group, AustPost*, *PwC*	Работает
11	Контроль и оптимизация учета показателей пробега автомобилей	Корпорация *Bosch*	Работает
12	Технологии защиты любых списков, регистрации избирателей, подсчета голосов на выборах	–	Проект

Окончание таблицы 4.1

1	2	3	4
13	Стартап-индустрия, как источник инвестиций в технологии завтрашнего дня	Компания «*Pitch Ventures*» (США)	Проект
14	Децентрализация кодирования медиа-информации, ее хранение, распространение	Стартап «*Videocoin*» (США)	
15	«3*D*- интернет» технологии в образовании и глобальные аудитории для постижения самых современных знаний	Стартап «*SocratesCoin*» (США)	Проект

На самом деле отраслей для прорыва в области блокчейн технологий значительно больше. Предполагаемые области применения блокчейн технологий, где операндами могут стать не отдельные лица, а коллективы людей, заинтересованных в:

– технологиях рационального распределения товарных ресурсов, прежде всего пищевых продуктов на планете;

– контроле за распространением заболеваний, пандемий, новых видов болезней;

– контроле за распространением по планете некоторых видов млекопитающих, насекомых, вредителей [2].

Их список с каждым днем расширяется. Например, как следует из отчета банка *Credit Suisse,* для пользователей платежными инструментами типа *Visa*, *Mastercard*, *WorldPay* «технология блочных цепей не представляет большого риска» [2]. Но так ли это?

Так ли уж универсальна эта компьютерная технология? Можно ли сомневаться в ее основных качествах: универсальности для материальных потоков и объективности ухода при этом от посредника (самого главного достоинства блокчейна)? Оценить это можно только практикой, причем эта практика уже в ближайшем будущем даст нам существенную пищу для анализа. Представим некоторые, наиболее часто встречающиеся риски, связанные с использованием рассматриваемых технологий (табл. 4.2).

В литературе можно найти и другие риски, с которыми сталкивались пользователи. Рассмотрим некоторые из них.

Первым аргументом против кажущейся универсальности является пресловутое правило «Атака 50 % +», когда более половины участников группы задаются целью исказить майнинговые данные. Теоретически это возможно, практически – весьма спорно при достаточно большом количестве игроков в группе. Главный аргумент: меньшинство не сможет обмануть большинство. Например, при нынешнем состоянии майнинга биткоинов такой сговор практически невозможен, так как пользователей этой системы миллионы. Но это относится к вариантам организации массовых финансовых потоков. А как быть с конкретными логистическими операциями, в которых принимает участие ограниченное количество участников? Контроль более половины всех майнингов дает возможность инкогнито переписать всю историю транзакций в виде удобной ее версии и пользоваться своими ресурсами несколько раз. Правило защиты от «Атаки 50 % +» может быть преодолено весьма просто. С целью нарушения работы предприятия-конкурента, или с целью увода части материального потока из-под контроля блокчейна, например, при помощи подставных участников, осуществляющих кольцевой обмен. Нет надобности представлять здесь такие схемы [2].

Таблица 4.2 – Риски по источникам возникновения, связанные с использованием блокчейн технологий в известных областях человеческой деятельности

№	Наименование риска	Характеристика риска
1	2	3
От производителя блокчейн технологий		
1	Несопоставимость технических возможностей для пользователей	Ограничения в виде пропускных способностей генерующих. систем для пользователя. Низкая скорость работы из-за криптографии
2	Появление отдельного сегмента неконтролируемой торговли	Потеря полного контроля со стороны Закона за торговлей, например, запрещенным товаром
3*	Отсутствие правового поля	Вызывает сомнение в коммерциализации блокчейн продукции и уход от известных правил ведения бизнеса
4*	Правило «Атака 50 % +»	Риски для ограниченных групп пользователей. Способность обойти партнеров по схеме «подставных фигур»
5*	Отсутствие наработанных организационных методик и единых правил применения	Огромное количество неотработанных и ошибочных технологий применяемых в отраслях
6	Неустойчивость к программным взломам блокчейн	До настоящего времени отсутствуют эффективные способы защиты от хакеров
7	Вмешательство в энергетический ресурс общества	Несопоставимость энергозатрат и реальной стоимости блокчейн продукта

Окончание таблицы 4.2

1	2	3
От потребителя блокчейн технологий		
8	Распространение нелегального контента, неправомерной информации	Угроза всем участникам сети из-за репликации инородных файлов как заслуживающих доверие
9	Скрытое отсутствие анонимности	Прозрачность финансов в блокчейн операциях – прямая опасность для компаний
10	Безосновательный уход от посредничества в областях, где оно актуально	1. Движения финансов в компаниях. 2. Криминал, отмывание денег. 3. Некоторые виды торговли
11*	Недостаточность критического понимания сути блокчейн технологий	Восприятие большинством пользователей технологий блокчейн как объекта типа «черный ящик» и связанные с этим нарушения и ошибки
12*	Способности к вмешательству в отдельные монополии	Участие бизнеса в неконтролируемых им операциях в пределе ведет к его разрушению
13*	Риск криминальных акций	Отмывание обезличенных денег и др.

* – общепринятые риски

Нужно понимать, что в материальных транзакциях они могут иметь право на существование и ради защиты против них следует уже сейчас искать противоядие. Получается, что

выгодность майнинга является залогом успеха в безопасности блокчейн операций, но чем меньше майнеров, тем система становится более опасной, в особенности, в нефинансовых применениях.

Число доверителей в блокчейн операциях представляется весьма важным рисковым критерием. Если по этим операциям работают миллионы пользователей – результат понятен. Правило «50+1» не сработает. Если потребителей немного, как в любой системе взаимного обмена, то пользователи будут стремиться к расширению числа партнеров. Это один из скрытых механизмов для таких процессов, как создание огромных корпораций из некогда разобщенных фирм, это путь к монополизму на рынке со стороны этих корпоративных объединений. Этот риск сегодня еще не очевиден, но логика такова, что с ним придется справляться в будущем. Блокчейн технологии вне сферы финансов пока не дают решения этой проблемы. Кстати, компании, владеющие блокчейн технологиями, уже сегодня ориентируются на свои способности к разрушению некоторых монополий на биржевых рынках посредством вовлечения в неконтролируемую ими децентрализацию. Под такой удар недавно попала компания *National Securities Clearing Corporation* (*NSCC*), которой удалось защитить свои интересы, но сам факт уязвимости этого бизнеса от блокчейн компаний ставит проблемы соответствующих рисков перед ними [2].

Блокчейны – это всегда риск оказаться вне правового поля. По крайней мере, сегодня это выглядит именно так. Но подвижки в этом вопросе – это вопрос времени. Уже в 2018 году 22 страны Евросоюза подписали соглашение о создании Европейского партнерства в сфере блокчейн технологий для повышения эффективности вызывающих доверие и ориентированных на пользователя цифровых услуг [3]. По данным агентства Прайм, европейские специалисты подготовят запуск единых для Евросоюза приложений с использо-

ванием технологии распределенных реестров для государственного и частного секторов. Пытаясь заполнить нишу, международная организация по стандартизации (*ISO* – *International Organization of Standardization*) решила, что международный технический комитет по вопросам разработки стандартов для технологии блокчейн (***ISO/TC*307**) [4] создаст систему стандартов для содействия функциональной совместимости технологий блокчейн, в том числе, ради повышения безопасности и снижения существующих рисков в этих технологиях [2].

Обсуждаемые проблемы с правовым статусом блокчейн операций связаны, например, с операциями типа **краудфандинг**, – децентрализованное обновление финансовых ресурсов, в частности, в моделях одноранговых накоплений средств вне систем централизованного обслуживания. Например, при помощи платформ типа *Kickstarter*, *Indiegogo* или *Swarm* – краудфандинговой платформы, используемой для накопления средств для стартапов в области цифровых валют. Существование вне правового поля таких действий. когда в них задействованы многие частные компании, например, с участием в долевом капитале, не может быль полностью легальным, потому что нарушает законодательство о ценных бумагах. Риски в краудфандинговых операциях достаточно велики. Уже сегодня они привели к судебным разбирательствам в компаниях, которые не хотят делиться доходом с обладателями таких децентрализованных платформ как *Manna*, *Swarmops*, *DPP* и др.

Следующая проблема рисков может иметь место в некоторых случаях безосновательного ухода от посредничества, фактора, который считается главным функциональным достоинством блокчейн технологий. Да, в тех случаях, о которых чаще всего упоминается в литературе – финансовые операции, работа через банки, такой подход может быть обоснованным. Но если мы говорим о том, что блокчейн

операции претендуют на универсальность как технологии будущего, к такому их качеству следует присмотреться внимательнее [2].

Контроль следует рассматривать как систему обратной связи в управлении. Классическая система управления подразумевает существование в ней обратной связи: положительной, стимулирующей развитие, или отрицательной, препятствующей разрушению системы под действием входящих сигналов. Одной из форм существования таких систем является подсистема контроля. В обществе это может быть государственный контроль, общественные формы контроля и другие обратные связи.

Стоит задаться вопросом: так ли уж плоха контролируемость в обществе? По большому счету, уход от контроля, в пределе, может изменить всю государственную систему: могут перестать действовать законы в пользу их цифровых альтернатив, отпадут за ненужностью контролирующие организации в пользу технологий типа блокчейна. Уйдет в небытие обратная связь в системах управления, как аксиома управления. Стоило бы и роль посредника рассматривать как одну из компонент, обеспечивающих обратную связь. Неконтролируемая торговля – это когда осуществляются логистические цепочки без посреднического контроля. Можно потерять контроль за торговлей наркотиками, людьми, фальшивой валютой и т. д., что приводит к потере государственности [2].

Следующим узким местом в любых блокчейн операциях, в особенности, если число пользователей зашкаливает (что естественно), является несопоставимость объемов скачиваемой информации и мощностей большинства персональных компьютеров обычных пользователей. От этого зависит доступ к сети, оперативность получения скачиваемой информации, ее проверка, осуществление платежей или других транзакций. Вариант использования одного центра, как

альтернатива хранению, сразу же противоречит одноранговости в идеологии блокчейна, а именно, отсутствие единого посредника. Это риски, с которыми большинство пользователей справляются, например, за счет простых online-кошельков, временно (надеюсь) уходя от технологий блокчейна и по-прежнему доверяя серверам. Пропускная способность сети биткоина может составить не более 7 транзакций в секунду. Для примера, скорость обработки у банковской системы *Visa* – несколько тысяч подобных операций в секунду. Скорость записи транзакций в системе биткоинов составляет не более 0,0166 в секунду. При этом после появления соответствующей записи время ожидания увеличивается в пять раз, так как каждый раз системно считываются все произведенные ранее записи без исключения. Таким образом, риск технических возможностей сегодня превышает актуальность ухода в децентрализацию транзакций перед риском иметь посредника. Но это – пока [2].

Еще один риск связан с уже сейчас появляющимися прототипами программ-взломщиков алгоритмов типа блокчейн. Да, такой вирус может быть распознан пользователями этих баз данных и будет распознан. Но программа может вмешаться в базы данных, повредить их и сделать непригодными для использования.

Можно надеяться, что блокчейн технологии получат достаточный уровень безопасности, при их применении в так называемых квантовых компьютерных системах, данные которых по принадлежности к квантовым способам хранения квантовых битов (кубитов) не имеют права сохраняться при искусственном их вскрытии, например [6].

Но таких компьютеров пока нет, и появление их еще долго не предвидится. Хакерские взломы таких программных продуктов могут стать существенным препятствием для их массового применения в самых различных областях. По мнению руководителя отдела блокчейн технологий *Bank of*

New York Mellon А. Батлина, сегодня еще не существует решений, отвечающих за защиту от взлома, с гарантиями для конфиденциальности правовых документов, публичной информации, разрешения споров и транзакций в системе блокчейна [3].

По мнению немецких специалистов, технологии блокчейн уже используются для распространения незаконных, вредоносных данных и нелегального контента [7]. Об этом свидетельствуют и данные Интерпола. При этом хакеров привлекает именно главное свойство технологии – неизменность и неистребимость хеша, как носителя этого контента.

Одним из результатов научной конференции «*Financial Cryptography and Data Security*» стало сообщение немецких ученых из Аахена о выявленных ими 1600 «чужих» добавленных файлов в содержимом в блокчейне, в том числе, детскую порнографию. Там же утверждается, что «помимо распространения нелегального контента, блокчейн также может использоваться для распространения инородного программного обеспечения» [2].

Вне всякого сомнения, не до конца оценен и риск необоснованного вмешательства блокчейн операций в энергетический ресурс общества. На первый взгляд, затраты электроэнергии на майнинговые действия при помощи компьютеров высокой мощности несопоставимы со стоимостью самого биткоина. Но это только на волне ажиотажа. Если принять во внимание возможную системность такой работы, энергетические затраты на нее могут стать сопоставимыми с энергозатратами крупных металлургических предприятий в год. Энергетические затраты здесь появляются как расплата за децентрализацию, как следствие массовости системных пользователей. Этот вопрос требует более полного изучения в данной книге.

Существует и широко обсуждаемый риск криминальных акций при использовании блокчейн технологий. Прежде всего, это возможность обезличенного и бесконтрольного вкладывания денег в криптовалюту с целью их «отмывания». Здесь поле деятельности огромное, и не существует механизмов их контроля по причине отсутствия посредника или контролера. Не всегда следует убирать контроль. Но это проблема правовая, и с ней все равно следует считаться и изучать [2].

Декларируемая анонимность в блокчейн операциях тоже далеко не всегда является реальностью. Скрытое отсутствие анонимности без присутствия посредника, когда донор транзитирует средства в системе блокчейна, а рецептор их получает, и последний, по крайней мере, оповещается об объеме ресурсов донора и, главное, может видеть историю его транзакций. Согласимся, что это уже не анонимность. Для компаний – участников блокчейн операций открытость финансов, прозрачность покупок-продаж, финансовая характеристика клиентов, количественные данные счетов, чем сразу воспользуются конкуренты, в определенных условиях, могут привести к банкротству.

Можно оценить реальность указываемых рисков при помощи экспертных оценок, которые дают две группы специалистов из числа разработчиков платформ блокчейн применительно к различным областям, и потребители этих платформ из числа представителей бизнеса, банковской сферы. Всего в исследованиях участвовало 68 человек, которые по 10-балльной шкале дали оценку реальности рисков, указанных в табл. 4.2. На рис. 4.1 представлены результаты подобной экспертной оценки [2].

В большинстве случаев экспертные оценки представителей двух указанных групп существенно разнятся. Это так называемый парад интересов, который всегда присутствует при продвижении нового товарного продукта. Тем не менее, по ряду позиций (в табл. 4.2 они обозначены звездочками)

оценка рисков, данная производителями и потребителями практически сходна. Это соотносится с проблемами правового обеспечения блокчейн процедур, опасности так называемый «Атаки 50 % +», опыта, рациональности и критичности при применении технологий блокчейн в различных областях бизнеса и др. Кроме того, существуют риски криминальные и риски активного вмешательства в конфиденциальные дела компаний.

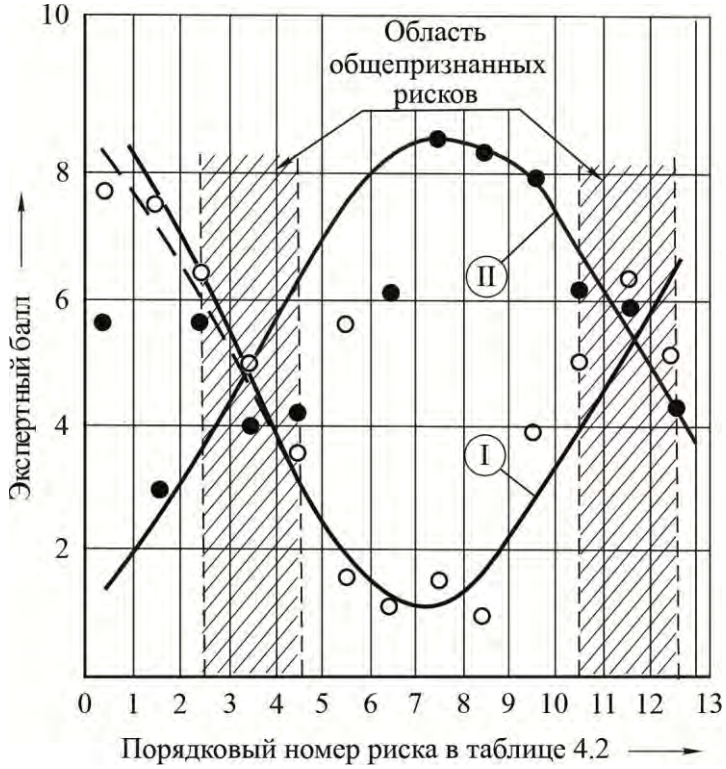


Рисунок 4.1 – Экспертная оценка значимости риска по указанным номерам в таблице 4.2

Мы имеем возможность утверждать, что существующие реальные и потенциальные риски в известных технологиях блокчейна – это не приговор, но возможность в будущем найти решение этих проблем, предупредить их влияние на инновационные процессы в обществе, обеспечить безопасность человека в нашем стремительно меняющемся мире.

4.2 Энергетическая безопасность и проблемы глобального информационного пространства

Учитывая массовость участия людей в интернете, использования огромного количества компьютерной техники, гаджетов самого различного назначения, следует обратить внимание на проблемы энергопотребления для этого вида деятельности. В литературе часто встречаются предупреждения относительно запредельных объемов потребляемой электроэнергии в системах интернета, при работе в социальных сетях, в системах биткоина, блокчейн технологиях, например [8]. В частности, ссылки на такие данные, как общий объем мощности средств, которые используются для майнинга криптовалюты, достигает размеров $9 \cdot 10^3$ МВт, свидетельствуют о том, что эта проблема существует. Такая цифра дает возможность для оценочного расчета количества расходуемой электроэнергии на эти цели.

В самом упрощенном варианте энергетические расходы, связанные с глобальным информационным пространством, относятся к компьютерному оборудованию, которое используется для работы в этом пространстве.

Для оценочного расчета потребностей компьютерной техники в электроэнергии при работе в ГИП, воспользуемся эмпирической формулой

$$A\cdot[N_k\tau_c + N_{\text{ож}}(24-\tau_c)] = E_{\Sigma}\ ,\ \ \times 10^6\ \text{МВт·ч}$$

Здесь: τ_c – средняя продолжительность работы в интернете для одного пользователя в сутки, ч;

N_k – мощность одного пользовательского компьютерного оборудования, кВт;

$N_{\text{ож}}$ – мощность одного компьютера в режиме ожидания, кВт;

$A = 1,2\cdot 10^6$ – расчетный коэффициент, учитывающий годовую загруженность техники и суммарное количество пользователей в сетях интернет.

На рис. 4.2 представлены расчетные данные об энергопотреблении при систематической работе в интернете и при устойчивой продолжительности этой работы в течение каждого дня и вероятность соотнесения приведенной мощности одного компьютерного устройства к продолжительности ежедневной работы его пользователя. Разброс данных, в зависимости от приведенной мощности используемых технических средств, весьма существенный, от 1,5- до 2-кратного значения, что свидетельствует о том, что эти данные можно использовать только как оценочные в исследованиях, а сама проблема энергетических затрат в интернет системах требует более тщательного изучения.

Наиболее часто «сидят» в интернете пользователи с компьютерным оборудованием локальной мощностью не более 0,6 кВт (в течение 2,25 часа ежедневно с вероятностью 0,89). Пользователи с профессиональным оборудованием мощностью не менее 1,6 кВт работают в интернете по 5,2 часа в день с вероятностью 0,705 (рис. 4.2). Если допус-

тить, что все 3,3 млрд пользователей в интернете работали бы каждый день, в пределе, по 10 часов на компьютерном оборудовании, с суммарной мощностью $9 \cdot 10^3$ МВт, расходы на электроэнергию достигли бы 40 % мирового потребления (рис. 4.2). Безусловно, это умозрительное суждение, но оно показывает, что без существенных изменений в компьютерной инженерии в пользу суперэнергоэффективных технологий интернет и соответствующие ему технологии не выживут и глобальное информационное пространство потеряет свою привлекательность для огромного количества пользователей.

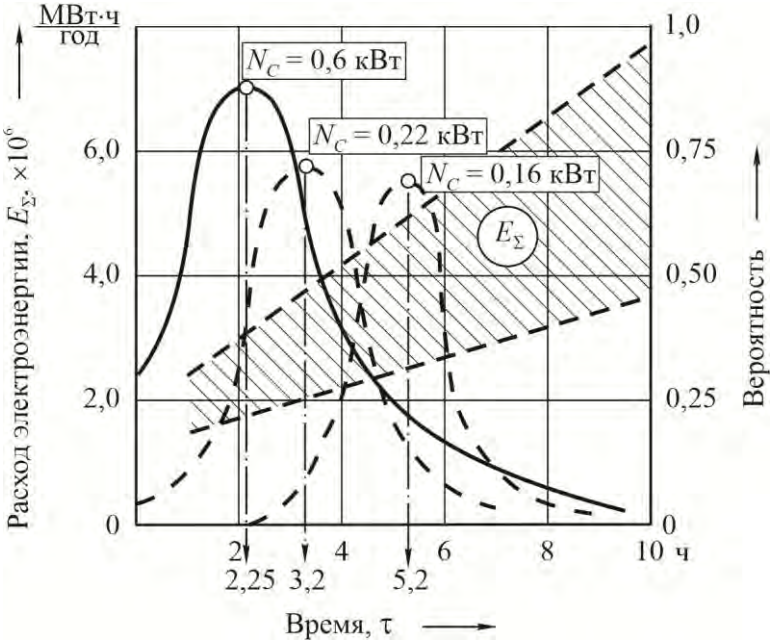


Рисунок 4.2 – Расчетное энергопотребление при работе в интернете при устойчивой продолжительности в течение каждого дня и вероятность соотнесения приведенной мощности одного компьютера к продолжительности ежедневной работы его пользователя

Диапазон энергетических затрат в целом при использовании интернета стал уже соизмеримым с энергозатратами на многие другие виды деятельности человека и является их крупной составляющей. Учитывая темпы развития всего, что связано с глобальным информационным пространством, можно судить о том, что эта составляющая общего количества энергии, потребляемой человеческой цивилизацией, и дальше будет иметь тенденцию к увеличению. А это, в свою очередь повлечет за собой нормативное перераспределение энергоресурсов между отраслями экономики во многих странах [9].

Энергетическая зависимость интернет технологий, кроме своей очевидности, несет и ряд проблем для экономики, для человека.

В более сложном варианте, энергетические затраты в ГИП связаны с применением современных компьютерных технологий, таких как, например, блокчейн технологии и их наиболее эффективный продукт, биткоин, эфириум и другие виртуальные валюты.

По существу, условный автор блокчейн технологий или технологий распределенных реестров, Сатоши Накамото, своей работой [10] поставил перед обществом альтернативу обмена всеобщей доверительности на энергетические расходы, связанные с так называемыми процедурами майнинга. Майнинг представляет собой процедуру поиска, а в действительности – перебора вариантов необходимого цифрового кода для «опечатывания» очередного доверительного протокола с использованием системы типа «черный ящик», имеющей специализированную узконаправленную программу выбора случайных кодов.

На основании исходных данных майнер, при помощи мощностей своей компьютерной системы, подбирает вариант кода x_i для нового протокола примерно в такой упрощенной интерпретации (рис. 2.4 из второй главы):

$$A + \bar{X}_{i-1} + x_i = HC.$$

Здесь: A – содержание текущего протокола, который необходимо опечатать;

$\overline{X}_{i-1}$ – цифровой код для «опечатывания» предыдущего протокола;

x_i – текущее содержание поискового кода, то есть тот самый необходимый код для текущего протокола;

HC – хеш-код, сгенерированный программой «черного ящика» из числа случайных символов.

Собственно **майнинг,** т. е. подбор числа $x_i = \overline{X}_{i-1}$, которое дало бы нам указанное равенство, осуществляется компьютерной системой методом подбора случайных чисел. Успех поиска зависит от мощности компьютерного оборудования, видеокарты, энергии и времени, затрачиваемых на майнинг. Количество хеш-райт наборов постоянно растет в прогрессии к числу освоенных биткоинов. Соответственно, растут и энергозатраты на хеширование нового кода $x_i = \overline{X}_{i-1}$. Безусловно, это весьма упрощенное и приблизительное пояснение работы системы майнинга, но его достаточно, чтобы искать энергетические зависимости, относящиеся к блокчейн технологиям.

Биткоин, несмотря на убежденность создателей о сугубой децентрализации и инклюзивности системы, на самом деле имеет одну, достаточно централизованную контрольную функцию. Это технологические энергозатраты, которые контролируются и могут, при определенных усилиях, давать информацию о состоянии системы и быть доминирующим фактором для нее. Активность майнера сводится к перебору вариантов решения задачи определения нужного хеша. Эта работа требует:

– доступа к источнику электрической энергии;

– соответствующей мощности компьютерного оборудования;

– скорости его работы;

– высоких объемов хеширования.

Самым узким местом для блокчейн технологий биткоина является доступ к электроэнергии. Майнинг не может осуществляться без использования источников электроэнергии.

Наравне с приобретением дорогостоящего майнингового оборудования, статья энергозатрат является пока непреодолимым препятствием в развитии блокчейн технологий. По данным И. Камински, усредненное количество энергии, расходуемой на операции майнинга, в современном мире соизмеримо с расходами энергии на острове Кипр [11]. Дино Марк Ангаритис показывает на 2015 год среднее число решений по поиску хеша для каждой майнинговой задачи в количестве $3 \cdot 10^{20}$ хешей, что далеко не всякому компьютерному ресурсу под силу [12]. Оценки расходов электроэнергии на операции майнинга, по различным литературным источникам, весьма отличаются, показывая лишь достаточно большую величину, сравнимую с энергопотреблением таких стран, как Швейцария, Кувейт [13], Австрия, Аргентина [14, 15] и др. Создатель индекса *Digiconomist* А. де Врис считает, что с применением самого современного компьютерного оборудования, на майнинг должно расходоваться не менее $15 \cdot 10^6$ МВт·ч мировой электроэнергии в год и даже цифра в $30 \cdot 10^6$ МВт·ч не предел, потому что система современного майнинга, включая режимы работы, – это своеобразный «черный ящик» [16]. По данным [17], уже проведенная генерация 18 млн биткоинов потребовала около $20 \cdot 10^6$ МВт·ч или 0,13 % всего энергопотребления в мире. По данным [18], при общем мировом потреблении энергии в $158 \cdot 10^9$ МВт·ч, генерация биткоинов $9{,}6 \cdot 10^6$ стоила всего $9{,}6 \cdot 10^6$ МВт·ч или 0,006 % мирового расхода.

По данным А. Нараяна [19], в мире в 2018 году было затрачено на биткоины $1{,}8 \cdot 10^6$ МВт·ч энергии. В 2019 году

по данным [20], общие затраты на биткоин – $53 \cdot 10^6$ МВт·ч. Расчетные данные немецкого математика М. Страубе [21] показывают годовое потребление энергии не менее $14 \cdot 10^6$ МВт·ч. По словам ученых из Лаборатории им. Лоуренса в Беркли, предполагалось, что к 2020 году энергоэффективность отрасли может повыситься на 45 %, Условный рост составил всего 3–5 %.

В целом, такие сравнительные и многочисленные оценки дают информацию лишь о том, что не существует достоверных методов оценивания энергетических затрат при майнинге и, в целом, для блокчейн технологий.

Переход процедур майнинга к крупным специализированным компаниям, обладающим огромным технологическим ресурсом, приводит к тому, что многие страны начинают лимитировать доступ к источникам электроэнергии для них. Сами фермы, как правило, создаются в регионах с дешевой электроэнергией и свободным энергетическим балансом. Тем не менее, Китай, охватывающий более 80 % мирового рынка майнинга, ввел ограничения на энергоресурсы, используемые для криптовалюты, не только по лимитам, но и по привилегиям в ценовой политике. Отдельные штаты в США, канадские, итальянские поставщики постепенно вводят подобные лимиты для своих майнинговых ферм, специальных «цехов», включающих большое количество мощных видеокарт. Компании-майнеры всерьез рассматривают вопросы создания собственных энергетических мощностей, сугубо под майнинговые цели.

С увеличением объема операционного фонда биткоинов, принимаемых в работу, увеличивается сложность задачи по перебору вариантов поиска хеша, растет его длина записи, что делает задачу поиска хеш-ответа значительно сложнее, что, в свою очередь, требует существенного увеличения потребления энергии. Только за период с 2016 по 2020 годы, по данным [22], сложность хеширования биткоина увеличилась

в 5 раз, что также не могло не сказаться на росте энергозатрат.

Усредненное время транзакций, входящих в очередной блок, определяющее скорость этих операций, с 2012 года менялось в достаточно широких пределах [22, 23] в зависимости от нагрузки на систему.

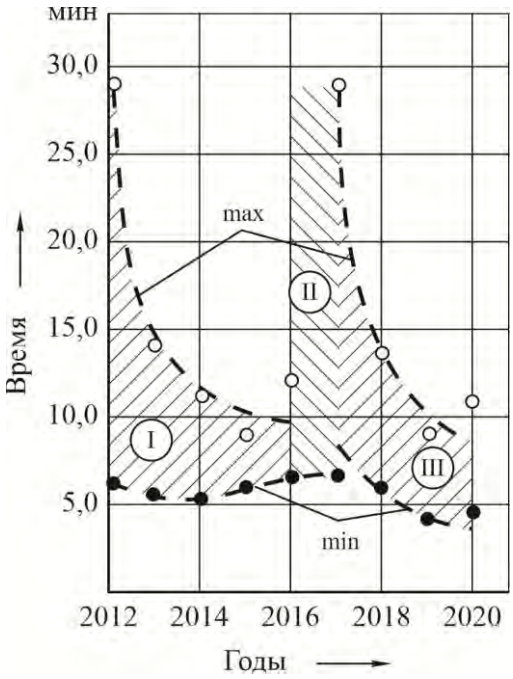


Рисунок 4.3 – Динамика усредненной продолжительности транзакции и подтверждения майнингового блока (по данным источника [23])

Устойчивая динамика (рис. 4.3) здесь наблюдается только в связи с появлением новых майнинговых устройств и технологий, например, в период активного майнинга приватными участниками в 2012–2016 годы (область I) на базе первых *GPU*-видеокарт в начале 2010-х годов, объединения

майнинговых ферм, или в период 2017–2020 годы (область III), когда появилась более мощная системная майнинговая техника: современный *ASIC* (*Application Specific Integrated Circuit*)-майнинг, в частности, ставшая известной система *ASIC Antiminer S*9, *Bitmain S*9, «облачный» майнинг, более традиционные *Antiminer S*7, *Antiminer D*3 компании *Bitmain* [23], использующие алгоритм *Scrypt*. В общей сложности, современный майнинг биткоина осуществляется устройствами, суммарная мощность которых превышает $9 \cdot 10^3$ МВт

Динамика усредненных ежедневных транзакций с 2010 года представлена на рис. 4.4.

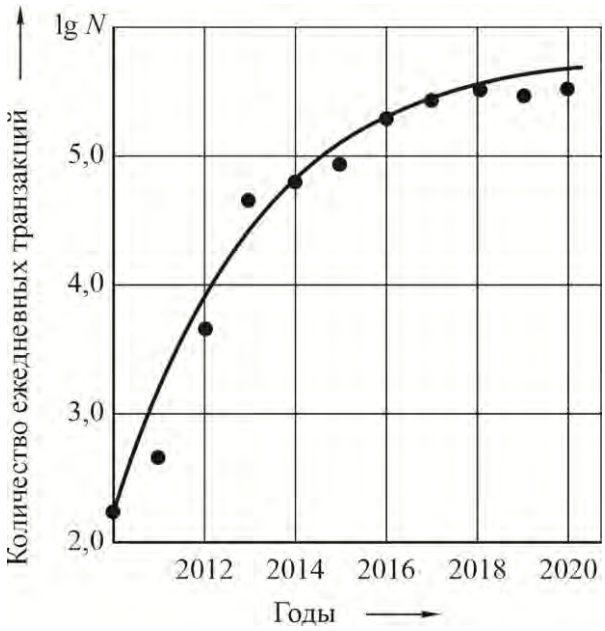


Рисунок 4.4 – Динамика ежедневных подтверждаемых транзакций в системе биткоина (по данным источника [25])

Только с апреля 2019 года по март 2020 года суммарный хешрейт биткоинов находился в пределах от 40 до 100 *TH/s*, при возрастании сложности задачи майнинга в 2,5 раза [26]. Безусловно, от этого следует ожидать и роста энергозатрат на единицу криптовалюты, расчетные данные которых представлены на рис. 4.5.

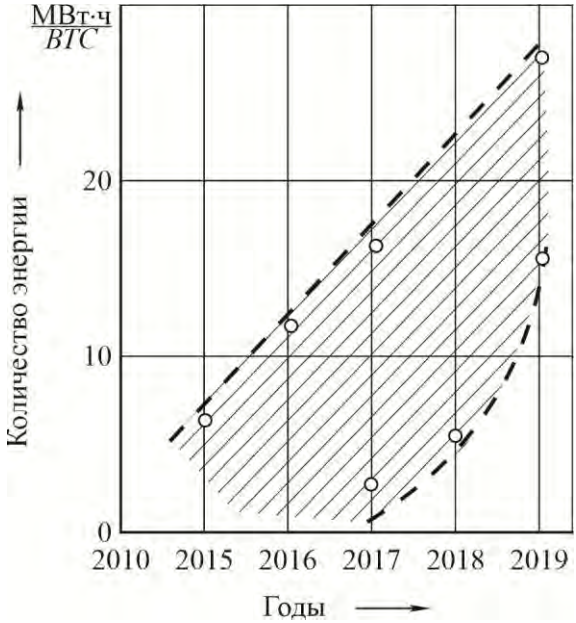


Рисунок 4.5 – Расчетная энергетическая емкость биткоина по годам

В 2010 году хешрейт майнинга одного блока из 50 биткоинов составлял $1 \cdot 10^{-11}$ *TH/s*, или на один биткоин приходилось $0,2 \cdot 10^{-12}$ *TH/s* [27]. Позднее, после каждых 250 тыс. отработанных блоков (12,5 млн биткоинов) система заявляла новый размер блока, из 25 биткоинов, хешрейт каждого из

которых составлял уже $1,4 \cdot 10^{-11}$ *TH/s* [27, 28], а после 2015 года каждому из 12,5 блоковых биткоинов требовалось уже $4,5 \cdot 10^{-11}$ *TH/s*. Рост числа переборов вариантов нахождения нового хеша также требовал роста затрат энергии от инженерной техники (рис. 4.6, а). Логично утверждать, что пересмотр объема одного блока в сторону его сохранения или увеличения может способствовать энергосбережению, это вариант, который может обсуждаться. Хешрейт таких объемов уже не подвластен приватным майнерам, а для крупных компаний будет обходиться в перебор вариантов, обозначаемых числом с 21 нулем (*zetta*) и при такой мощности последние монеты биткоинв теоретически должны потребовать $n = 1 \cdot 10^{24}$ единиц хешрейта (рис. 4.6, б).

Если принимать во внимание, что аппаратные мощности для хеширования у всех участников должны работать круглые сутки, можно, таким образом, рассчитать энергетику и транзактирования, и майнинга. На практике режимы работы майнеров (исключая компании для профессионального майнинга) далеки от равномерности, что делает любые балансовые расчеты интегральных энергозатрат только оценочными. Можно показать, что эти расчеты далеки от реальных. Именно поэтому для технологии блокчейна трудно подобрать достаточно объективную систему расчета энергозатрат.

Усилиями Мишель Раухс из Кембриджского центра альтернативных финансов разработан индекс потребления энергии биткоином *CBECI* (*Cambridge Bitcoin Electricity Consumption Index*), при помощи которого запущен в реальном времени счетчик общего потребления электроэнергии в сети биткоинов. На сегодня это наиболее эффективная методика и реальные данные по энергозатратам в блокчейн технологиях.

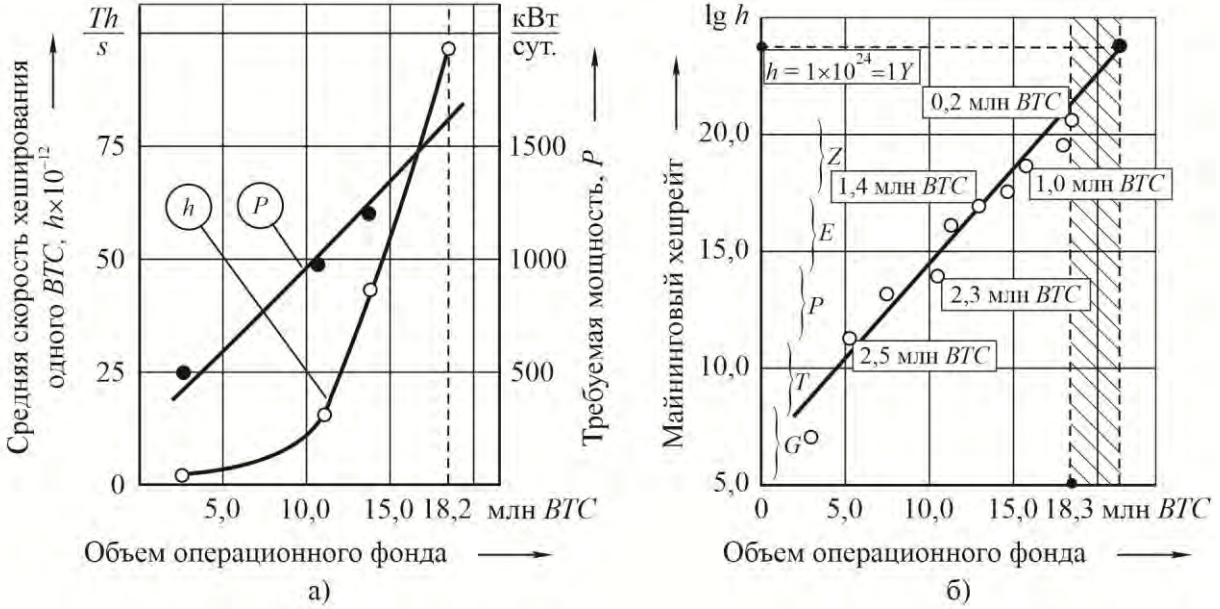
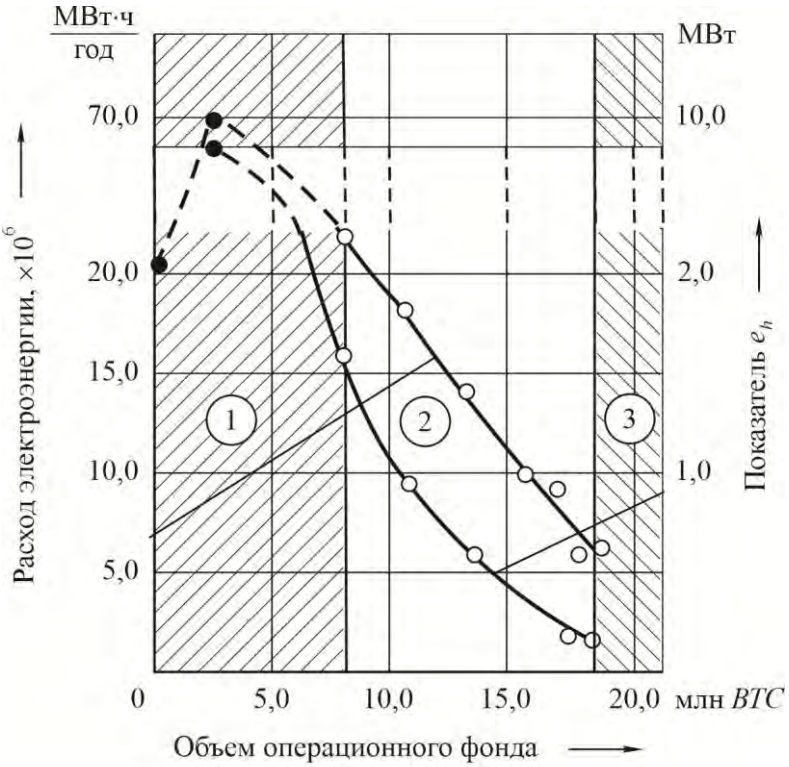


Рисунок 4.6 – Динамика хеширования одного биткоина и потребности в мощном оборудовании (а) для обеспечения необходимой мощности хешрейта в зависимости от освоения всего операционного фонда биткоинов (б) (по данным источника [30])

На март 2020 года (момент написания работы) индекс изменялся в пределах $(33,5 \div 99,1) \cdot 10^6$ МВт·ч [15], что составляет 0,21 % от мировых поставок электроэнергии [30]. Показано, что в год генерируется $12,5 \cdot 6 \cdot 24 \cdot 365 = 657$ тыс. биткоинов, таким образом, что один биткоин в 2020 году обходится в 96,4 МВт·ч (правда, расчетные данные, рис. 4.5, дают результат вполовину заявленного в данном источнике). При средней цене 1 кВт·ч в \$0,07, стоимость расходуемой электроэнергии на майнинг одного биткоина составляет \$4820. По тем же данным М. Раухс [16], в 2018 году энергозатраты на один биткоин составили 33 МВт·ч и стоил он \$2310. Эта цифра соизмерима с нашими расчетами (рис. 4.5). Очевидным является рост как энергозатрат на получение одного биткоина, так и доля энергоемкости в его себестоимости. Несмотря на увеличение объемов хеширования и энергетической ценности каждого последующего биткоина, общие затраты электроэнергии на майнинговые операции в системе биткоина системно снижаются (рис. 4.7). Причина этого, пока, только в тех возможностях, которые представляют нам разработчики современного майнингового оборудования, и только.

Профессиональный майнинг все более ориентируется на малые формы энергосбережения, например, вместо алгоритма доказательного консенсуса типа *PoW* (*Proof-of-Work*), – использование системы *PoS* (*Proof-of-Stake*) как способа сокращения потребления энергии майнинговым оборудованием и обеспечения безопасности системы. Следует отметить, что график (рис. 4.7) не учитывает такие пояснения, как, например, банкротство компании *Mt.Gox* и потерю в 2014 году более 750 тыс. единиц биткоина, или выпуск финальной версии *Bitlicense*, как развитие проекта биткоина в 2015 году, или скандал 2013 года с *Web*-сайтом «*Silk Road*», замешанным в использовании системы биткоинов для тор-

говли наркотиками, что, очевидно, не могло не влиять на динамику и на энергетику хеширования и поддержки транзакций в этой системе.



1 – область оценочных данных;
2 – область расчетных данных;
3 – область прогноза.

Рисунок 4.7 – Динамика суммарной энергоемкости рынка биткоинов с 2000 по 2020 годы и приведенная энергетическая ценность одного биткоина

Более точно генерированную энергоемкость биткоинов отображает размерная величина энергопотребления, приведенная не только к одному биткоину, но и к одному хешрейту в его логарифмическом отображении:

$$e_h = \frac{E_{\text{общ}}}{N_{btc} \cdot \lg H}.$$

В формуле учитывается не только снижение количества генерируемых биткоинов во временном интервале, но и рост объемов требуемого хешрейта в этом же интервале. Эти показатели взаимосвязаны и сопровождают дальнейшее развитие блокчейн технологии биткоина. Показатель e_h, в отличие от энергоемкости, на графике показывает возможность к минимальному насыщению энергоемкости биткоина с приближением к запрограммированному пределу в 21 млн биткоинов (рис. 4.7). Условия технологии биткоина таковы, что дуплекс $N_{btc} \cdot \lg H$ постоянно растет, своим существованием уменьшая приведенную цифру энергоемкости биткоина. При этом следует подвергнуть сомнению данные в оценочной области «1», которые, по всей видимости, искажены в литературных источниках и отличаются от оценочных расчетных данных (рис. 4.2). При этом данные по энергетическим затратам за последние годы в большей мере более корреспондируются между собой.

С другой стороны, по данным *Digiconomist*, на биткоин в 2019 году приходилось около 100 млн финансовых транзакций в год. С традиционными же финансовыми инструментами проводится 500 млрд транзакций в год, то есть в 5000 раз больше. Но на одну традиционную финансовую транзакцию тратится в среднем $3 \cdot 10^{-7}$ МВт·ч энергии, а на майнинг одного блока (9 байтов) в биткоине нами подсчитано – 96,4 МВт·ч. Таким образом, 100 млн транзакций требуют почти $1 \cdot 10^4$ МВт·ч энергии (без майнинга), а 500 млрд традиционных финансовых операций требуют $15 \cdot 10^4$ МВт·ч. При этом следует учитывать, что, с приближением к завет-

ному числу 21 млн биткоинов, энергоемкость каждого из них растет в геометрической прогрессии и достижение отметки в $150 \cdot 10^6$ МВт·ч наступит очень быстро. Уже сейчас очевидно, что растущая сложность майнинга биткоина должна быть сопоставима с его энергоемкостью, постепенно ставшей естественным ограничителем в любых системах блокчейна.

Генерация оставшихся до 2032 года 2758 тыс. биткоинов (суммарно 99,8 % всего пула биткоинов), путем экстраполирования к нынешнему состоянию, может потребовать энергозатрат более, чем $0,9 \cdot 10^9$ МВт·ч, что может составить уже 4,3 % от мирового потребления электроэнергии и будет равнозначно экономическим потерям от производства товаров на сумму $50 млрд. Это фактическая плата за доверительность. На это сегодня мало обращают внимания, потому что уже 80 % биткоинов находятся в работе, а энергетического коллапса не видно.

Майнинг биткоинов за период с 2015 по 2020 годы вырос с 13,1 до 18,2 млн единиц виртуальной валюты, а потребление электроэнергии – с $4,5 \cdot 10^6$ до $20 \cdot 10^6$ МВт·ч, то есть более, чем в четыре раза. Тем не менее, рентабельность биткоина остается крайне высокой. Для средней цены 1 кВт·ч в $0,05÷0,07 энергозатраты на майнинг одного биткоина составляют около $2160, при рыночной цене этой криптовалюты в пределах $6,5÷8,7 тыс. (на момент написания материала).

Несмотря на системный рост объемов хеширования и энергетической ценности каждого сгенерированного биткоина, в системе этой блокчейн технологии происходит снижение общих энергетических затрат. Учитывая популярность и перспективы развития, в частности, биткоина, возможности для децентрализации и доверительности при получении этого продукта, в который уже поверили миллионы людей, мы вправе ожидать появления более энергоэффективных технологий, простых и удобных, позволяющих большому количеству потребителей создавать локальные системы распределенного реестра.

4.3 Человек как потребитель блокчейн технологии. Что для этого нужно?

Вопросы, связанные с актуальностью блокчейн технологий, как одного из актуальных продуктов глобального информационного пространства, постоянно возникают в литературе, в электронных средствах информации. Диапазон вариантов отношения к данному изобретению колеблется от почти полного скепсиса [32, 33 34, 35] через огромный пласт недоверия и надежды [36, 37, 38], до публикаций, которые рассказывают о прорывных направлениях для данной технологии [12, 39, 40], связывают опыт крупных и небольших компаний в ее освоении. Общим здесь является интерес к предмету исследования, который подчеркивает не только его актуальность, но и возможности для совершенствования.

Отталкивает от этого изобретения, как ни странно, опыт его применения в наиболее продвинутом проекте – криптовалютном, в биткоине. Успешный проект, в силу его непонимания, либо сопротивления со стороны традиционной мировой централизованной банковской системы, попыток использования в криминальной среде, непременных ошибок и потерь, стали причиной такого отношения со стороны части общества.

С другой стороны, безусловно выигрышные стороны блокчейна, заключающиеся в отсутствии централизованного управления и контроля, прозрачности операций с любыми материальными (и не только) потоками и при любом количестве партнеров, полной приватности для всех участников системы, привлекают к этой технологии огромное количество потенциальных сторонников и пользователей, которые, тем не менее, входя в мир блокчейна, пасуют перед сложностью системы, отсутствием методических разработок, позво-

ляющих принимать участие, создавать свои блокчейн системы, для решения самых различных прикладных задач, опыт, который мог бы стать основным аргументом в пользу этого актуального изобретения.

Когда технология становится общепризнанной, к ней относятся, как к данности, изучая, в том числе, и ее опасности для человека. Одной из таких опасностей в блокчейн технологиях является отсутствие общепринятого смыслового понимания работы системы. Для массового пользователя системы распределенных реестров, не стремящегося к приобретению новых монет путем майнинга, являются закрытыми сами процедуры поиска новых кодов, хэширования, подтверждения достоверности протоколов, что вызывает определенное недоверие и скептицизм, а значит понимание потенциальной опасности от применения блокчейна. Здесь чисто субъективное отношение со стороны человека становится препятствием для развития этой технологии.

Обобщенные знания о блокчейн технологиях для обычного пользователя весьма поверхностны. В связи с этим непременную ценность представляют публикации, которые системно и разумно упрощают отношение к блокчейну, абсолютизируя его наиболее важные особенности [37, 41]. Безусловно, не во всех случаях, требующих децентрализации, найдет применение новая технология. Там, где существует абсолютное и взаимное недоверие к участникам («всех ко всем»), такая система потребует огромного количества вычислительным мощностей, что будет делать эту технологию явно нерентабельной. В других случаях, когда блокчейн применяется к распределению и учету материальных или информационных потоков между обезличенными субъектами, возможно фрагментарное использование блокчейна.

Нужен опыт, нужны исследования возможностей применения блокчейна в социальных системах, например, в выборных процедурах, социологических работах, где степень

децентрализации может регулироваться в зависимости от устойчивости системы к внешним управляющим воздействиям. В частности, область, где возможности блокчейна высоки, – это уже известные системы смарт-контрактов, где в договорных условиях существуют возможности уйти от чисто юридических, разночитаемых походов к новому правилу «код есть закон». Математический код. Правда, для этого нужно иметь подготовленных узкопрофильных специалистов из числа понимающих язык программирования, на котором записан контракт. Но это может стать более убедительным аргументом, чем взаимоисключительные суждения юристов в традиционном правовом поле. Здесь формализованный алгоритм и безальтернативная математическая функция, заложенная в его основе, становятся более аргументированным доводом, чем разновекторное толкование закона.

Не стоит упрощенно переводить всю технологию блокчейна на примеры генерации криптовалют, биткоинов. Криптовалютные блокчейны, одними из первых, стали приносить ощутимые результаты, в силу своей развитости и привлекательности для субъектов системы. Децентрализованные системы цифровых платежей не проявят себя в полной мере, еще, по крайней мере, до тех пор, пока не исчезнет инициативный майнинг, как способ генерации новых монет, и пока не останется только формализованный майнинг, предназначенный единственно для «опечатывания протоколов».

Другие проекты блокчейна, менее известные, упрощенные по своей сути, явно слабо доработаны до конечного результата. Поэтому в литературе, как правило, такие проекты описываются упрощенно или минимально информативно. Тем не менее, системы блокчейна не только развиваются, но и видоизменяются (правда, пока также в области криптовалют), но уже понятно, что эти технологии имеют перспективы, ставки на них весьма высоки, и отмахнуться от этого уникального изобретения просто так уже не удастся.

Общеизвестные признаки новой типичной блокчейн технологии:

– отсутствие централизованного управления, контроля, влияния посредников;

– защищенность от несанкционированного доступа к базам данных, материальных активов, составляющих сущность протоколов;

– демократичность права доступа к базам данных в установленном порядке;

– упорядоченный сбор транзакций в информационные блоки, с последовательным объединением их в цепочки и распределенные реестры;

– существование распределенного реестра протоколов операций некоторого вида, известных всем участникам;

– возможность проведения транзакции и создания адресов на основе классической ключевой схемы открытого (*publik*) и закрытого (*privat*) ключей доступа;

– существование личного ключа доступа к собственным данным транзакций, защищающего персональные данные от проникновения;

– открытая обезличенность транзакций всех других участников системы, достигаемых открытым ключом доступа;

– специализированная технология кодирования очередного протокола транзакций, позволяющая оставаться неизменными данные этих протоколов при любых внешних атаках.

Существует еще множество других отличительных признаков, которые могут оказаться не важными для внешнего пользователя при использовании технологии в практических целях.

Пока блокчейн технологии осваивают только специально подготовленные специалисты, профессиональные программисты. Сумеет ли когда-нибудь обычный пользователь

применять сложную технологию распределенных реестров для организации своего бизнеса, своей компании, обеспечить для себя оптимальные потоки сырья, применять ее для решения маркетинговых, финансовых задач, не постигая специфической сути алгоритмов Накамото, внутренних механизмов майнинга и хэширования?

Такой опыт человечество накопило. Пользователи колеса, самого известного изобретения человечества, на протяжении двадцати тысячелетий не имели представления о силах трения качения и скольжения, не знали закономерностей существования колесной пары. Но это не мешало им использовать многочисленные повозки, колесницы, арбы, телеги, другие предметы качения, превращая вращение колеса в поступательное движение повозки, заменяя скольжение.

Более 80 % современных владельцев автотранспорта даже не подозревают о том, как работает карбюратор, инжектор, коробка передач или современный двигатель внутреннего сгорания. Тем не менее, они водят автомобили, имея под рукой всего несколько устройств для управления: руль, рычаг переключения передач, пару педалей, несколько кнопок и упрощенный алгоритм их использования.

Более близкие примеры. Освоение персональных компьютеров с довольно сложным программным обеспечением, софтом, позволяющим образно управлять сложными расчетами, а позднее, и созданием «офиса», привело относительно неподготовленного пользователя к несложной процедуре освоения этой удобной техники. Еще один пример связан с созданием и развитием информационных сетей, когда массовый пользователь должен был выйти из рамок отдельного компьютера и найти коммуникационные возможности для огромного количества самых различных гаджетов. Пользователь легко принял относительно несложную систему навигации в мире информационных сетей, в появившихся как грибы системах типа *Facebook*, *Twitter*. Далее пришла пора ос-

ваивать глобальное информационное пространство, уметь искать нужную информацию в огромных объемах баз данных, осваивать пути или цепочки, по которым можно было найти нужное. И опять в силу вступило правило – для массового пользователя система максимально упрощается, из ее интерфейса исключаются все внутренние механизмы, системы обеспечения, цифровизированные алгоритмы. Пользователю оставляется только внешняя среда системы, «набор кнопок с пояснениями в виде простейшего алгоритма». Такой конечный продукт считается готовым к использованию, о чем свидетельствует масштаб его применения на практике.

То есть опыт доведения сложной технологии до простого пользователя, технологии, не обремененной специальными подробностями и символами, существует. Его получение – актуальная задача современных *IT*-технологий, и, в первую очередь, блокчейна.

В литературе достаточно описаний работы технологии блокчейна, его преимущества, способы устранения недостатков, области применения в различных отраслях человеческой деятельности. Да, в первую очередь, все вращается вокруг самой продвинутой технологии блокчейна – криптовалюты, но и там далее узких специалистов либо подготовленных майнеров дело не пошло, тем более, что современный майнинг уже не подвластен обычным пользователям из-за своей высокой энерго- и вычислительной емкости. Во всем мире им уже занимаются специализированные компании. Все ожидают времени, когда же биткоин станет не только накопительным, но реальным и общепризнанным платежным средством (история с 21 млн монет и 2040 годом). Пока профессиональные или обзорные публикации дают очень мало возможностей для практического применения этой, безусловно, актуальной и перспективной, но весьма непростой технологии.

Следует понимать, что именно из всего этого многообразия требуется знать массовому пользователю, а что знать не обязательно. И что нужно знать такому потребителю, чтобы использовать технологию блокчейн в своих целях (следует отличать массового пользователя и создателей, наладчиков блокчейн технологии для конкретной компании)?

На наш взгляд, для того, чтобы использовать эту современную технологию, массовому пользователю требуются следующие знания (рис. 4.8): знание основ работы с компьютером и информационными сетями, знания в области логистики, опыт работы в компании. Нужно разбираться в правилах доступа в уже существующую систему блокчейна и правила коммуникаций с другими участниками системы, а именно.

1. Условия допуска:

– право вхождения в систему распределенных реестров (accessibility);

– правило формирования открытого ключа доступа (*PublicKey*);

– правило формирования закрытого ключа доступа (*PrivatKey*).

2. Условия коммуникаций:

– правила общения с другими участниками в системе;

– унифицированный «лист» для записи транзакции;

– подтверждаемое наличие активов, которые применяют обезличенные партнеры в системах транзакций;

– механизм и право контроля всех транзакций и обезличенных данных всех участников системы;

– право голоса при внесении изменений в алгоритм кодирования и отвода неверных хешей;

– правила, позволяющие использовать в работе минимальное количество вычислительных мощностей для обработки полной копии реестров.

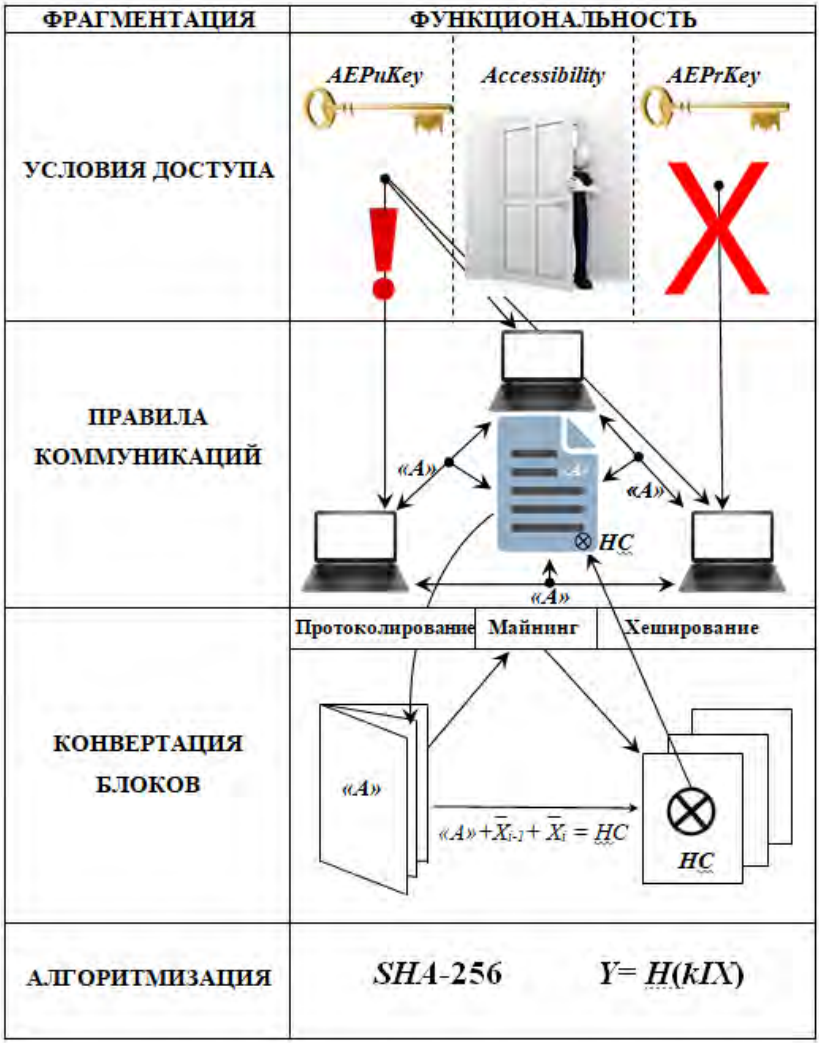


Рисунок – 4.8. Функциональная схема блокчейна для массового пользователя. «*A*» – протокол последовательности транзакций; *AEPuKey* – ключ открытого доступа в систему; *AEPrKey* – ключ приватного лоступа в систему; *Accessibility* – право доступа и правила участия в системе транзактирования, майнинга, его оценки и опечатывания блоков

Что не обязательно знать массовому пользователю (участнику обменных транзакций, не стремящемуся к выигрышу новых биткоинов):

– механизм проверки и подтверждения записей в реестре, цель которого заключается в легализации новых монет;

– особенности работы алгоритмов типа *SHA*-256;

– особенности майнинга в системе;

– разделение прав и возможностей пользователя и майнера в системе; сегодня майнер и пользователь, – это одно лицо. После события «21 млн» ситуация, возможно, изменится;

– порядок обеспечения и степень надежности программного кода.

Такое разделение возможностей и способностей в системе пользователей сразу может упростить доступ к блокчейн технологии и отделить чистого пользователя от профессионального «настройщика» системы в любой компании. Предложенная схема может быть видоизменена, тем не менее, оставаясь максимально упрощенной и безальтернативно применимой для массового пользователя. Важным моментом является достижение адаптивного уровня понимания системы для такого пользователя.

В целом, прикладные вопросы инженерии (помимо специфической и чисто программной продукции в компьютерном мире) в кибернетической безопасности далеко не исчерпываются представленным материалом. Они достаточно обширны и имеют свое продолжение в самых различных исследованиях.

V

Вклад информационной инфраструктуры в понимание безопасности человека. Наследство от революций

Сосуществование человека и информационной инфраструктуры, в том числе, ее инженерного сопровождения, в современном обществе признается как данность, без которой дальнейшее развитие не представляется возможным. Человек уже не сможет обходиться без компьютера, без социальных и других информационных сетей. Понятие информационной инфраструктуры дает представление о месте и роли человека в ней. Под информационной структурой следует понимать совокупность информационных систем и организационно-технических структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия людей. Это следствие информационной революции, в которой наше общество живет уже на протяжении нескольких десятков лет. Живет и удивляется, как можно было жить ранее без этой безотказной «оболочки».

Информационная революция является одой из многих, которые пережило человечество в своей истории. Каждая последующая революция давала людям определенный толчок в развитии и в продолжение всей своей истории изменяла экономику и общественные формации, государственный строй и социальные отношения, выдвигала новых лидеров, которые являлись носителями новых идей и реализовывали их, изменяя сознание общества, его архитектуру. Каждая из революций, какую бы иерархию она не представляла, способствова-

ла развитию производства, знаний о природе, науки, общественного сознания, давала в руки людей новые инструменты и технологии. Любая революция имела свои достоинства, которые делали ее по настоящему революционной, имела свои минусы, которые тормозили и затрудняли развитие ее идей, но со временем, первые по значимости превышали вторые и результаты революции укоренялись в обществе. Существуют общие особенности и качества этих революционных процессов, знание которых дает возможность учитывать прежние ошибки самого различного уровня и масштаба, не допускать либо минимизировать прогнозируемые риски и потери, которые сопровождают эти явления.

Интересны сроки начала и окончания таких революций. Если сравнивать продолжительность когнитивной (~30 тыс. лет) и аграрной (~7 тыс. лет) революций, то по продолжительности они отличаются на порядок столетий, а, в сопоставлении с продолжительностью научной революции (~500 лет) сроки сократились на несколько порядков [1]. Это же относится к современной нам информационной революции. Темпы развития ее основных позиций измеряются несколькими десятками лет, что в сравнении даже с научной революцией является уникальным достижением. Оно показывает не только актуальность новых изменений, но и готовность общества к ее восприятию.

Еще один результативный показатель – это рост численности населения связанный со сроками конкретной революции. Объектами когнитивной революции были от силы 100–200 тысяч людей и ее идеи развивались тысячелетиями. Объектами научной революции уже стали 5 млрд человек, а информационной – 7,7 млрд человек и их идеи были внедрены в общественное сознание и дали практический результата на протяжении нескольких десятков лет. Одна из причин заключается в мощной транзитивности идей таких революций, скорости распространения основных парадигм нового.

В особенности, это относится к информационному взрыву, свидетелями и участниками которого являемся мы.

Весьма интересную информацию дает сравнительный анализ качественных характеристик различных революций. Такой анализ позволяет найти определенные параллели и более объективно понять динамику развития общества в условиях современной информационной революции. Поэтому, подробная таблица результатов сопоставления качественных сторон самых различных изменений революционного характера крайне важна для наших исследований (табл. 5.1).

Безусловно, по истечении многих лет и даже веков, определить все проблемы и недостатки, например, аграрной или экономической революций не представляется возможным. Их наверняка, было значительно больше, чем показано в таблице 5.1. История забывает многие из возникавших проблем и недостатков, ошибок и потерь, оставляя только самые значимые. Тем не менее, можно представить себе большую часть из перечня проблем, с которыми столкнулось общество, например, при переходе от доисторического существования к культурному, от собирательства к активному земледелию и животноводству, от примитивных индивидуальных производств к промышленному производству и т. д. Сформированный при этом уровень общения привел к субъектному коллективизму, а последующий статус оседлости выдвигал на первый план не просто защиту территорий для собирательства, но защиту своих полей, расположившихся рядом поселений, городов от завоеваний иноплеменников, создание для этих целей определенных вооруженных формирований, профессионализацию воинов. Требования безопасности для человека стали наиболее важными, которые привели к развитию государственности и современных ему изменений в обществе. Этот требовало огромных социальных и экономических перестроек, о которых сегодня мы уже позабыли.

Таблица 5.1 – Некоторые сопоставительные признаки наиболее типичных социально-экономичных и других революций в истории человечества

Очевидные эффективности, связанные с революционными изменениями	Очевидные проблемы, связанные с революционными изменениями
1	2
1. Когнитивная революция (около 50 тыс. лет назад). Население 200 тыс. человек (цифра оценочная)	
1. Рост объема серого вещества. 2. Развитие способностей к обучению. 3. Прямохождение. Развитие хватательных и других способностей. 4. Совместное воспитание детей как одна из основ коллективизма. 5. Переход к вершинам пищевых пирамид. 6. Приручение огня. 7. Появление языка, мыслительных процессов, общения. 8. Освоение природных закономерностей, помогающих человеку при собирательстве. 9. Появление обменных операций, предшествовавших торговле	1. Энергозатраты на обслуживание серого вещества увеличились в 10 раз и составили 25 % всех энергозатрат человека. 2. Сужение бедер у женщин привело к росту смертности при родах. 3. Развитие ранее неведомых заболеваний костной системы, связанных с прямохождением. 4. Быстрый прорыв во власть: состязания личностей, войны. 5. Упрощение в переваривании пищи. Сокращение длины кишечника. Ослабление жевательных инстинктов. Канцерогенные вещества. 6. Проявление элементов «теории сплетен» как формы когнитивного развития. «Сплетни-вымыслы-мифы-правила-законы», как прообраз будущего государственного устройства

Продолжение таблицы 5.1

1	2
2. Аграрная революция(около 10 тысяч лет назад). Население 1–4 млн человек	
1. Переход к земледелию, к оседлости. 2. Освоение зерновых культур. 3. Вода и земля становятся ресурсом. Потребности в поливной воде. 4. Создание и развитие специфических хозяйственных земледельческих орудий. 5. Качественные изменения в питании. Препятствие голоду. 6. Появление понятия индивидуального жизненного пространства: дом, деревня, город. 7. Формирование домашнего индивидуального хозяйства как экономической потребности для человека. 8. Сезонные циклы производства. Высвобождение времени для других видов производительной работы и отдыха. 9. Ощущение будущего. Планирование еды, доходов, рождаемости, соотносимой с едой, доходами. 10. Потребности в порядке, защите, законах, государственности. 11. Появление торговли, торгового обмена. 12. Переход от натурального к товарному производству.	1. Защита оседлых территорий. 2. Развитие агрессивности, потребность в войне. 3. Развитие алчности, жадности, тяги к власти, богатству. 4. Рост вероятности насильственной смерти. 5. Сужение знаний о природе в сравнении с «собирателями». 6. Изменение структуры нагрузок на скелет. Новые болезни костной системы. 7. Ухаживание за культурными растениями: прополка, полив, уборка, расчистка, подкормка. 8. Дополнительные затраты энергии при оседлости, большей статичности для организма. 9. Первые попытки изменить природу «под себя»: каналы, города, расчистка земель, вырубка леса. 10. Появление монополии на власть, государства, узурпация власти, полиция – внутренняя армия, не для врагов, а для своих. 11. Появление производственной эксплуатации как формы социально-экономических отношений.

Продолжение таблицы 5.1

1	2
13. Освоение территориального пространства для торговли. 14. Повышение роли торговли в межгосударственных отношениях	12. Формирование первоначальной экономической элиты как основы для последующей политической власти
3. Экономическая (промышленная) революция (начало около XVI века). Население 600 млн человек	
1. Свободный рынок – закон природы. 2. Появление универсального эквивалента – денег. 3. Деньги как форма взаимного доверия между людьми. 4. Появление банков и банковской системы. 5. Овеществление кредитной системы как основа веры людей в будущее. Кредиты как овеществленная вера в будущее. 6. Появление знаний о Земле, о неизвестных территориях. 7. Специализация труда, повышение интенсивности труда. 8. Появление коллективных специализированных предприятий и систем (мастерские, фабрики, мануфактуры). 9. Формирование нового типа классического естествознания. 10. Появление и развитие прикладного естествознания.	1. Инфляция, обесценивание денег, потеря учета. 2. Появление кредитных и земных отношений как форма ограничения свободы человека. 3. Необоснованность доверия к появляющимся финансовым системам. 4. Накопительный и обманный капитал. 5. Формирование монопольных систем в экономике. 6. Проявление свойства финансовых экспансий со стороны банковской системы. 7. Отрыв крестьян от земли для работы в промышленных монополиях. 8. Появление наемного труда как форма финансового закрепощения людей. 9. Формирование устойчивой династической экономико-политической элиты в отдельных странах.

Продолжение таблицы 5.1

1	2
11. Предпосылки для появления новых демократических форм управления государством	10. Появление и развитие в государственной системе династических форм управления
4. Научная революция (начало около XVII века) Население 0,7 млрд человек	
1. Расширение возможностей для воспроизводства. 2. Знание стало производительной силой. 3. Частичное избавление от крайнего проявления нищеты, голода. 4. Эффективное использование энергии всех видов, способности ее взаимных превращений. 5. Только научная революция может помочь погасить кредитные системы. 6. Промышленная революция основана на конвертации видов энергии. 7. Расширение сырьевой базы производств за счет ранее недоступных районов и источников. 8. Рост номенклатуры искусственных неприродных материалов. 9. Обеспечение избыточными пищевыми ресурсами при уменьшении числа рабочих рук благодаря промышленным методам развития скота и птицы.	1. Рост потребления энергии на одного человека в 10^3 раз. 2. Урбанизация, развитие городов, угнетение природы. 3. Направленность на глобализацию. 4. Зависимость от времени, временная регламентация, графики, режимы, системные потоки. 5. Исчерпаемость существующих источников энергии и сырья. 6. Лавинообразный рост отходов пропорциональный росту объемов потребляемого сырья. 7. Искусственная деформация большинства природных экосистем, вывод их из состояния динамического равновесия. 8. Экологическая деградация биологических систем. 9. Превышение предложения над спросом. Искусственный шопинг. Этика консъюмеризма. 10. Неравномерность распределения товарных ресурсов по планете. 11. Искусственное занижение потребительской ценности товаров. Рост послеэксплуатационных отходов.

Продолжение таблицы 5.1

1	2
10. Снижение зависимости человека от природных условий. 11. Углубление специализации, ее трансформация в науку и общество. 12. Понимание роли человека на планете. 13. Появление новых научных направлений в классической и прикладной науке. 14. Понимание науки как движущей силы в мировой экономике. 15. Изменение модели научной деятельности в пользу ее коммерциализации и прикладного предназначения	12. Изменение философии существования человека «от голода – к ожирению», «инвестируй-покупай»… 13. Использование результатов научных знаний в пользу милитаризма. 14. Опасности современных войн. 15. Возможности уничтожения человечества и планеты. 16. Обострение экологических проблем в обществе. Ухудшение состояния окружающей природной среды. 17. Появление экономических и милитаристских супердержав. 18. Перераспределение сырьевых и продуктовых ресурсов на планете в пользу развитых стран
5. Информационный взрыв (конец XX – начало XXI века). Население 7,7 млрд человек	
1. Глобализация и повсеместность информации в мире. 2. Доступность информации и равноправие в потреблении. 3. Рост объемов информации. 4. Новые виды информации и ее источники. 5. Демократизация информационного обеспечения. 6. Появление социальных сетей. 7. Равный доступ к средствам социальных коммуникаций.	1. Недостоверность информации. 2. Потеря аналитичности в информационном обеспечении. 3. Повторяемости информации в интернете. 4. Загрязнение информационного пространства неиспользуемой информацией. 5. Снижение информационной насыщенности единицы информации в ГИП. 6*. Утверждение ложной информации как новой опасности для человека.

Продолжение таблицы 5.1

1	2
8. Возможности для интеллектуальной человеческой деятельности. 9. Массовая цифровизация отдельных сторон общества. 10. Расширение коммуникативности. 11. Появление новых форм общения для человека. 12. Расширение возможностей для проявления творчества человека. 13. Появление новых форм доверительности в обществе. 14. Отсутствие цензуры. 15. Изменение форм общения. 16. Глобализация отношений. 17. Новая социальная ниша для человека. 18. Появлении принципиально новых информационных технологий в обществе. 19. Новые формы социальности в обществе. 20. Появление альтернативных финансовых систем. 21. Новые формы коммерческих отношений в обществе. 22. Новые формы структуризации общества (по интересам и др.). 23. Появление новых областей знаний в науке.	7*. Появление кибернетической опасности для человека. 8*. Появление хакеров, влияющих на программный продукт. 9*. Отсутствие понимания роли человека в проблемах кибербезопасности. 10*. Появление новых форм преступлений в киберпространстве. 11*. Появление преступников новой, интеллектуальной формации. 12*. Отсутствие защиты персональных данных пользователей в ГИП. 13*. Потеря идентичности и сопо-ставимости для субъекта отношений 14*. Тенденции к потере индивидуальности для человека в ГИП. 15*. Появление новых видов и форм опасностей для здоровья человека в ГИП. 16*. Изменения в физиологии человека, появление новых болезней, связанных с нахождением в ГИП. 17*. Риски от криптовалют для современного финансового рынка.

Окончание таблицы 5.1

1	2
24. Появление «интернета вещей». 25. Появление новых интеллектуальных сообществ. 26. Появление новых предпочтений в обществе. 27. Отсутствие границ в системах сетевого общения. 28. Формирование новых отношений в обществе	18*. Недостаточная международная юридическая база для существования ГИП. 19. Появление интеллектуального пролетариата. 20. Снижение уровня воображения в творчестве. 21. Проявление качества стадности на новом витке развития человечества

*– относится к проблемам кибернетической безопасности

Внимательный анализ большинства проблем, с которыми столкнулось наше общество при проведении глобальной информационной революции, также ставит безопасность, во всех ее проявлениях, на одно из первых мест. Из двадцати произвольно указанных в таблице 5.1 позиций, относящихся к очевидным проблемам, связанным с информационными изменениями, двенадцать, так или иначе, относятся к безопасности человека по тем параметрам, по которым ранее, в «доинформационный» период, человек не испытывал чувств опасности для жизни или здоровья. Безусловно, таких признаков значительно больше [2, 3], и следует отдавать должное некоторому субъективизму этих данных, но они лишний раз подчеркивают актуальность проблем кибернетической безопасности, области знаний, которая пришла к нам вместе с компьютеризацией, вместе с появлением глобального информационного пространства, но постепенно расширяется на субъекта этого пространства, человека.

Эти же признаки присутствовали и в эпохи других глобальных изменений: экономических, научных, когда риски для жизни и здоровья человека возрастали в пропорции с

увеличением социальных, экономических, политических и других изменений и благ, вызванных революционными или даже эволюционными изменениями. Сошлемся, например, на проблемы производственной безопасности периода промышленной революции, на проблемы ядерной, бактериологической безопасности периода научной революции и др., о которых ранее общество и не подозревало. Но, если в прежние времена, движущей силой аграрной, экономической или научной революций была физическая сила либо внешняя энергия, то уже информационная революция, и, в особенности, современный ее этап, имеет в своем арсенале не только принудительно-силовые, но и развитые социально привлекательные способы влияния на огромные массы людей.

В подобных сопоставлениях очевидны многие параллели предыдущих периодов, которые успешно были преодолены людьми, и этот опыт должен быть для нас актуальным, если мы стремимся к тому, чтобы современное информационное сообщество было привлекательным, дало свои плоды и приносило пользу.

В каждой из революционных эпох были свои риски и свои достижения. Поскольку нас интересует первое, мы попробуем выделить риски каждого из указанных периодов по следующим группам:

– риски социального характера;

– риски биологического и гигиенического характера

– риски криминального и экономического характера

– риски технического характера.

Для каждой из указанных эпох были риски, относящиеся к указанным группам. Например, риски биологического характера для когнитивной революции были связаны с появлением ранее неизвестных заболеваний костной системы, с сужением бедер у женщин и ростом смертности при родах, с упрощением переваривания пищи, уменьшением длины кишечника. Для периода информационной революции к ним

относятся новые опасности для опорно-двигательного аппарата и костных тканей человека, угнетение отдельных групп мышц, тенденции к потере психологической устойчивости и индивидуальности для человека в ГИП.

Социальные риски времен когнитивной революции были связаны с проявлением состязания личностей, вождей, войнами. А в период аграрной революции и развития собственности, к социальным рискам относились развитие алчности, жадности, тяги к власти, богатству, появление монополии на власть, государства и т. д. Промышленная революция столкнула общество с появлением экономических и милитаристических супердержав, неравномерностью распределения товарных и других ресурсов, опасностью современных войн на тотальное уничтожение. Свои риски социального характера свойственны и для периода информационной революции. Это появление нового вида опасности (кибернетической) для человека, появление ранее неизвестного вида противостояния (кибернетического) между отдельными государствами, риск к потере идентичности и сопоставимости для субъекта отношений.

Подобные параллели можно продолжить, ссылаясь на данные таблицы 5.1 и множество других литературных источников. Все они отражают общие черты, сопровождающие существование человека в ходе революций глобального масштаба. Это свидетельствует только о том, что закономерности, связанные с рисками, с которыми столкнулось наше общество во время информационного взрыва, существовали и в другие периоды развития общества. Этими закономерностями следует пользоваться, хотя бы ради того, чтобы исключить некоторые из опасностей, которые могут замедлять, затруднять, препятствовать развитию того, что уже сегодня видится как неизбежность для человечества. В частности, можно говорить о предмете и смысле современной кибернетической безопасности.

Кибернетическая безопасность стала важнейшей сопровождающей парадигмой новой социальной революции, которую назвали информационной, парадигмой современного глобального информационного пространства в направлении его утверждения в самых различных областях жизнедеятельности человека [4].

Но, в сравнении с безопасностью обеспечивающих технических систем [5, 6], постепенно проявлялись и становились актуальными знания в тех областях безопасности, которыми ранее не занималась кибернетическая безопасность. Это знания о безопасности человека, прямой или косвенной, но связанной с существованием компьютеров, их программного обеспечения, информационных и социальных сетей, глобального информационного пространства. Все эти новые составляющие целого комплекса научных и прикладных знаний оказывали влияние на человека, как положительное, так и отрицательное [6], вынуждая специалистов по защите компьютерной техники сопоставлять решение своих задач с решением задач защиты человека, его здоровья и жизни, в зависимости от компьютерных вирусов, хакеров, преступлений, потери экономической самостоятельности, самоидентичности, потери жилья или работы в компаниях, попадающих под хакерские атаки, потерю личных средств, попадание под обман в результате пользования непроверенной информацией, деформацией собственных жизненных устоев, в результате длительного пользования компьютерами и их продуктами – играми, способами общения, фейками, лайками и другими интересными приобретениями.

Новая область знаний пересекается со смежными науками, такими как безопасность труда человека по отраслям экономики, промышленности, военная безопасность, экология и др. Собственная ниша этих знаний в науке вполне сформирована и имеет возможности для дальнейшего развития, при определенной их систематизации. В том числе, в

области кибернетической безопасности. Не исключается при этом вариант, когда кибербезопасность станет одним из самых узких мест при дальнейшем развитии этой области знаний и деятельности, как основополагающей в современном обществе [7].

Перечень данных, представленных в таблице 5.2, показывает, что, помимо чисто инженерных проблем, связанных с защитой от хакеров, незаконного взлома программного продукта, в кибернетической безопасности, как области знаний, существуют еще и социально-экономические, и физиологические, и гигиенические, и многие другие риски для человека, относящиеся к глобальному информационному пространству.

Безусловно, представленный перечень не может претендовать на полноту материала, как, впрочем, и вся книга. Это только небольшой фрагмент существующих и потенциальных опасностей и вредностей, с которыми человек сталкивается или может столкнуться в процессе активной работы в интернете, в социальных и других сетях. Он может быть показателен, чтобы принять, в качестве данности, актуальность проблем, связанных с безопасностью человека в таких человеко-машинных системах.

Представляет интерес экспертная оценка всей совокупности затронутых в работе факторов риска, экспертами со стороны специалистов в областях, связанных с кибернетической безопасностью в самых широких ее аспектах. Подобная работа была проведена с более чем 100 специалистами в области *IT*-технологий, сетевыми менеджерами, медиками, гигиенистами, юристами, представителями национальной полиции и прокуратуры, учеными-экономистами, социологами и менеджерами. Каждому из них для анализа был предложен на выбор перечень факторов из следующих четырех групп, сформированных из расширенных материалов таблицы 5.1:

– риски социального характера;

– риски биологического и гигиенического характера;

– риски криминального и экономического характера;

– риски технического характера, к которым относятся защита софта, компьютерного оборудования от внешнего проникновения и другие технические вопросы.

Экспертам, в качестве дополнения к собственным материалам, была предоставлена информация, систематизированная из доступных источников [1–18] о фактах, связанных с предметом анализа.

Ранговая экспертная оценка опасности того или иного фактора риска осуществляется по единой методике. Каждому эксперту из фиксированного количества экспертов (*K*) в рамках каждой из четырех групп рисков предлагается оценить по десятибалльной системе ранг x_i^k каждой опасности в своей группе. Приведенная ранговая оценка конкретного эксперта определяется как $X_i^k = \alpha^k \cdot x_i^k$. Здесь: k – порядковый номер эксперта; i – порядковый номер фактора риска из группы, которому выставляется оценка x; α^k – показатель признания авторитета эксперта ($\alpha^k \le 1$) оценивается самим экспертом и хранится в тайне от других экспертов. Авторитет эксперта весьма условно определялся основными его научными результатами, а именно:

– значимостью публикаций в *Scopus WoS*, участием в специализированных научных конференциях;

– ученой степенью и ученым званием в рассматриваемой и смежных областях знаний.

Математическая обработка результатов эксперимента выполнена по стандартным методикам теории вероятности путем определения математического ожидания $M_e(x)$ экспертных оценок всей генеральной совокупности и среднеквадратического отклонения $\sigma(x_i), i = 1,1,N$.

Таблица 5.2 – Параметрические данные о характере опасностей и вредностей для человека в глобальном информационном пространстве

№	Наименование фактора и группы факторов опасностей и вредностей	Число экспертов и ранговая экспертная оценка ($M_e \pm [\sigma]$)		Число зафиксированных случаев в литературе
1	2	3		4
I. Риски социального характера (число экспертов – 37)				
1	*Появление кибернетической опасности для человека*	37	6,9±0,3684	13
2	Отсутствие понимания роли человека в проблемах кибернетической безопасности	35	4,9±0,1098	8
3	*Недостаточная международная юридическая база для существования ГИП*	35	7,5±0,0645	32
4	Потеря идентичности и сопоставимости для субъекта отношений	37	4,1±0,0645	6
5	*Отсутствие защиты персональных данных пользователей в ГИП*	33	8,5±0,4279	64
6	Утверждение ложной информации как новой опасности для человека	34	5,0±0,0739	60
7	Появление киберпротивостояния между отдельными государствами	33	4,2±0,2021	4

Продолжение таблицы 5.2

1	2	3	4	5
II.	**Риски биологического и гигиенического характера (число экспертов – 16)**			
1	*Изменения в физиологии человека, появление новых заболеваний, связанных с работой в ГИП*	16	6,8±0,4005	17
2	Появление новых видов и форм опасностей для здоровья человека в ГИП	16	6,4±0,2958	9
3	*Тенденции к потере психологической устойчивости и индивидуальности для человека в ГИП*	16	7,7±0,2111	16
4	*Опасности для опорно-двигательного аппарата и костных тканей человека*	16	9,6±0,1953	63
5	Вынужденно высокая продолжительность нахождения перед компьютером	16	5,1±0,3897	6
6	Эргономические проблемы рабочих мест перед компьютером	16	5,0±0,0911	4
III.	**Риски криминального и экономического характера (число экспертов – 29)**			
1	*Появление новых форм преступлений в кибернетическом пространстве*	25	8,4±0,1847	10
2	Появление преступников новой, интеллектуальной формации	25	7,0±0,4169	25
3	*Риски от криптовалют для современного финансового рынка*	29	7,9±0,2815	18

Окончание таблицы 5.2

1	2	3	4	5
4	Возможности для изменения изначального понятия эквивалентного товарообмена в мировой экономике	29	6,0±0,3418	40
5	*Отсутствие защиты от проникновения в компьютерную программную продукцию и в персональные данные пользователей*	24	9,4±0,2871	9
6	Кража интеллектуальной собственности, размещенной в глобальном информационном пространстве	25	6,6±0,3483	36
IV. **Риски технического характера (число экспертов – 18)**				
1	*Появление хакеров, влияющих на компьютерный программный продукт*	18	9,1±0,0931	13
2	Зависимость общества от суперразвитого программного обеспечения и его энергетических потребностей	18	7,1±0,4218	28
3	*Ограничения в виде пропускных способностей генерирующих систем для пользователя. Низкая скорость работы софта из-за криптографии*	18	8,3±0,5132	18
4	Огромное количество неотработанных и ошибочных технологий, применяемых в отраслях бокчейна	18	6,2±0,2173	79
5	*Нарушение телекоммуникационных систем*	18	7,7±0,097	25

Примем также, что частотная характеристика фактора риска – это логарифмическое значение событийности в год. Определяется посредством мнения экспертов, с учетом данных из литературных источников [8–18], а также данных самих экспертов, и зависит от важности фактора, частоты его проявления в информационном поисковом поле (S – число событий в 2019 году, на момент проведения исследований). Результаты экспертных оценок совместимы с данными о частотных характеристиках факторов риска. Эти данные отображены на рис. 5.1, где каждая из групп факторов риска поставлена в зависимость от значения частоты фактического появления события в логарифмическом масштабе.

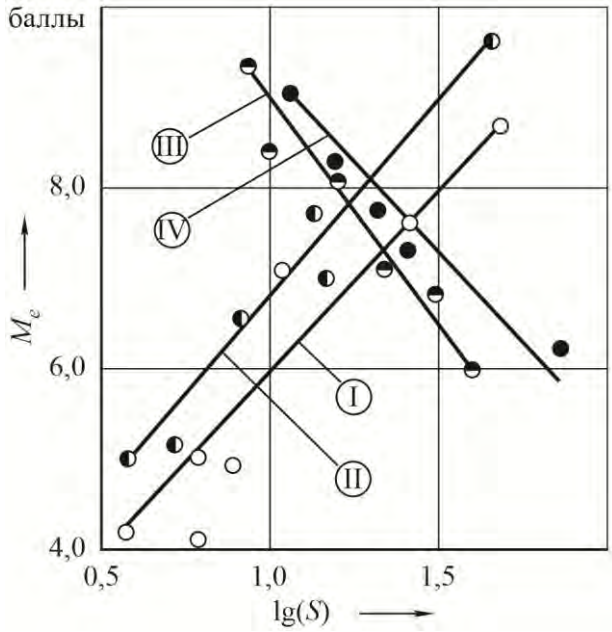


Рисунок 5.1 – Экспертная оценка рисков, осознаваемых для человека в глобальном информационном пространстве, в зависимости от частоты рисковых событий

Полученный результат интересен своей динамикой. Если сопоставить аппроксимированные линейные функции зависимостей $M_e = f\left[\lg(S)\right]$, полученных методом наименьших квадратов, появляется одинаковость возрастания таких функций для первой и второй групп факторов риска и одинаковость убывания этих функций для третьей и четвертой групп факторов риска (рис. 5.1).

Наиболее важные факторы риска из группы социальных показателей (рис. 5.1) – это отсутствие эффективной юридической базы, слабость защиты персональных данных и сам факт существования кибернетической опасности для человека. При этом частота повторяемости этих факторов в течение одного года достаточно высокая (от 10 до 65 случаев, отмеченных в литературных источниках), что свидетельствует об их актуальности. Риски, связанные с воздействием глобального информационного пространства на организм человека, эксперты оценивают как достаточно актуальные из-за ситуаций с заболеваниями опорно-двигательного аппарата, появлением новых видов заболеваний и потери психологической устойчивости организма. Больше всего на такой оценке настаивают эксперты-медики. Ежегодная частота таких опасностей находится в пределах от 17 до 60 зафиксированных случаев (по данным литературных источников).

Криминальная составляющая рисков оценивается экспертами несколько выше, чем их социальная составляющая. И в качестве наиболее опасных рисков называются новые формы преступлений, отсутствие защиты от хакерских проникновений в индивидуальные данные и опасности от криптовалют на экономическом рынке. Но частота фиксации таких факторов, по крайней мере, описываемых в литературе, невысока (8–18 случаев в год). И, наконец, в области инженерных и технических рисков со стороны внешнего киберпространства эксперты обоснованно выделяют опасность хакерских атак, нарушение телекоммуникаций и проблемы с

быстродействием компьютерных систем с частотностью таких случаев за год, зафиксированных экспертами от 15 до 65.

Примечательно, что оценка экспертами рисков криминального и инженерного характера, в зависимости от частоты их фиксации в литературных источниках (рис 5.1, III и IV группы рисков), по убывающей представляется ими как уже вполне устоявшиеся в сознании проблемы.

В то же время, риски, связанные с социальными и биологическими проблемами, оцениваются экспертами по возрастающей (I и II группы рисков) в зависимости от частоты их фиксации, по крайней мере, в литературе. Этим подчеркивается их актуальность для системы в целом и свидетельствует о том, что научное сообщество все более начинает уделять должное внимание именно факторам человеческой безопасности в глобальном информационном пространстве.

Таким образом, мы еще раз подтверждаем, что проблемы безопасности человека в глобальном информационном пространстве становятся все более рельефными, понимаемыми сообществом и расширяющими понятие кибернетической безопасности как науки, в совокупности других подобных наук о человеке.

ЗАКЛЮЧЕНИЕ

Кибернетическая безопасность сформировалась как самостоятельная наука на протяжении последних трех десятилетий. В основе ее все это время находились методы и средства защиты программного продукта, компьютерного оборудования от вирусов, несанкционированных проникновений, вмешательства в базы данных и многое другое, что связано с безопасностью, прежде всего, элементов инженерного обеспечения. В условиях сформировавшегося глобального информационного пространства безопасность технических систем, отвечающих за накопление, запоминание, преобразование и трансляцию информации, имела преимущества перед тем, без чего эти системы существовать не могли. Без человека, без пользователя этими системами, этой информацией. И даже результаты защиты от компьютерных вирусов, защиты от проникновения в программный продукт или базы данных и др. в этой области знаний почти никак не переносились на человека, как одну из равноправных составляющих системы «человек-машина». В кибернетической безопасности практически не было исследований, относящихся к элементам безопасности второго члена системы – «человека», работающего в этой системе. Тем не менее, даже самый простой анализ показывает, что результатом защиты от «вирусов» в программном обеспечении еще двадцать лет назад была простая экономия времени для пользователя, избавляемого от необходимости исправления и восстановления программной продукции, повторных расчетов, потерь информации, нарушения работы компьютерной техники, психологических срывов и других вмешательств в человеческую безопасность. Кибербезопасность сегодня отвечает за три составляющие: техническая система, информационный процесс, пользователь. Человек все больше «срастается» со своими гаджетами, компьютерами, сетями. Поэтому, потребность в

кибербезопасности для человека будет постоянно расти, ориентируясь именно на него. Не просто так появилось на весь мир изречение Илона Маска на Всемирной конференции по искусственному интеллекту в Шанхае в 2019 году о современных людях как о почти киборгах, уже не способных существовать без мира гаджетов и информационных костылей. Их сосуществование – это новое состояние для человека, новая психика, новые опасности, новые формы мышления. Формы, зависимые от цифровых видов информации, от взаимоотношения человека и «цифры».

Одновременно с появлением и развитием глобального информационного пространства появились новые опасности и вредности, делающие участие в нем человека более проблематичным и для здоровья, и даже для жизни. Это реакция пользователя ГИП на появление самых разнообразных видов преступлений, на искажение информации в социальных сетях, на откровенную ложь, принимаемую за правду, и на запредельные объемы подаваемой информации, весьма поверхностные по смыслу и не подлежащие дальнейшему аналитическому осмыслению. Это реакция человека, в особенности молодого, на существование информационной «жвачки», искажающей реальное состояние вещей в природе и в обществе. Все это постепенно приводит к искажению человеческой морали, становится угрозой нравственности для молодежи и многое другое. ГИП – это система функционирования информации, проникающая во все уголки человеческой жизни. В экономику, в инженерию, в социум, в бизнес, в образование, медицину и многое другое. Все эти области, так или иначе, связаны с существованием в них человека, с его активностью, с обеспечением для него определенного благосостояния и благополучия.

Настоящая монография призвана обратить внимание на упущения в той области знаний, которой она посвящена. Кибернетическая безопасность в своей методологии требует

учета реакций человека на реальные опасности со стороны глобального информационного пространства.

Возможно, мы встретим другую точку зрения специалистов по защите информационного пространства в тех функциях, которыми они сейчас занимаются, и которые ориентированы только на безопасное функционированиекомпьютерных систем и другого инженерного обеспечения? Следует сохранять уверенность в том, что эта область знаний является важной и неотъемлемой составляющей кибернетической части системы «человек-машина», крайне актуальной, потому, что, посредством обеспечения безопасной работы «машины», дополняются суммы знаний о защите человека, как конечной инстанции таких систем безопасности. Но это только часть проблем, которые следует изучать в науке о кибернетической безопасности. Не менее важной составляющей для этой науки должна стать безопасность человека во всех ее проявлениях в глобальном информационном пространстве и его производных. Это должно иметь отражение во всех нормативных документах, регламентирующих функционирование ГИП.

Следует признать, что наука о кибернетической безопасности, по терминологии семантически совпадающая с другими областями знаний о безопасности человеческой деятельности, стала неотъемлемой составной частью этих знаний. Признаком такого соответствия является интеграция соответствующих знаний из области кибернетической безопасности в другие смежные науки: военную безопасность, безопасность жизнедеятельности, химическую и радиационную безопасность. Но кибербезопасность должна иметь возможности и для обратных этому процессов: использование знаний о природе человека, его жизнеобеспечении, психологических и физиологических аспектах трудовой деятельности, особенностях функционирования человеческой памяти, воображения, представления и других качеств человека, с

которыми сегодня сталкиваются, например, специалисты по искусственному интеллекту в областях его дальнейших перспектив, в том числе, взаимодействия человека с носителями искусственного интеллекта. Эти знания давно перешли границу фантастики и рассматриваются сегодня как данная реальность. И знания о возможностях проявления когнитивности могут существенно помочь не только специалистам по искусственному интеллекту, но и обезопасить человека от опасностей возникновения конфликтов между ними. Такие пересечения научных знаний всегда были источником развития науки, и кибернетическая безопасность – не исключение.

Само понимание глобального информационного пространства дает право смотреть на кибернетическую безопасность, как на системообразующую область знаний для целого ряда научных направлений, таких как компьютерные науки, киберлингвистика, информатика, теория управления, биомедицина и медицинская инженерия, и др. В каждой из них можно выделить знания по кибернетической безопасности в такой интерпретации, которая дает возможность их использования для развития новыхнаучных направлений.

Следует понимать, что эта наука, как и все, что связано с исследованиями в области глобального информационного пространства, способна дать миру еще много новых открытий. Но, самое главное, она способна оградить наше оцифрованное сообщество от возврата к прошлому, как альтернативы будущему по причинам, связанным с искажением социальности человека, его социальной безопасности, явлением, с которым мы постоянно сталкиваемся и которое требует своих решений на благо человека. Потому, что вектор прогресса имеет только одно направление, вперед.

С проявлением новых технологий интернета с его новыми способами и средствами коммуникаций и распространения информации произошло изменение восприятия реальности для человека, появилась новая среда обитания. Появи-

лись новые эффективные технологии – *IoT* (интернет вещей), креативная экономики, *sharing economy*, краудфандинг и краудсорсинг, доверительные технологии в управлении и бизнесе, системы *E-health* и *E-government*. Упрощаются многие бытовые вопросы, более доступными «не выходя из дома» становятся дистанционное образование и медицинская помощь. Вся информация о человеке хранится в цифровом виде и является доступной всем. Но и вся информация о компаниях, ресурсах, ценах, наличии лекарств и авиабилетов, общение с любым партнером, включая ранее недоступных *VIP*-персон, высокая степень доверительности, гарантированная огромным количеством партнеров-свидетелей в любой области деятельности, все это, со своими плюсами и минусами, постепенно становится реальным в этой новой среде обитания. Постепенно мы сталкиваемся с отходом от понятий рационализма в коммуникациях в сторону иррациональных действий и иррационального восприятия мира посредством телекоммуникативных технологий. При общении в сетях главным становится не рационализм, а коммуникативность, интерес, эмпатия, настроение, иррационализм. Мы перестали замечать, что отпадают навыки ручного письма, как ведущей функции в культуре человечества, не говоря уже об утратах в развитии моторики конечностей и изменениях в мозговой деятельности. К функции письма общество шло долгие тысячелетия, от шумеров до ренессанса с расцветом первопечатания. Современная перспектива: без компьютера и экранных технологий наш потомок не сможет написать ни строчки. Письменность постепенно заменяется на речь и ее надиктованные транскрипции в виде переработанных программой электронных продуктов и сообщений. Письмо, каллиграфия, шариковая ручка, без чего еще в XX веке не представлялось ни образование, ни экономика, ни государственная деятельность, ушли в прошлое. Современные дети значительно проще разбираются с экранными тех-

нологиями, чем с алфавитом или письмом, способны без посторонней помощи быстрее освоить любой гаджет, чем устный счет, письмо или теорему Пифагора. Кстати, в этом имеется свой особый смысл: современные цифровые технологии, включающие в основном зрительную память, в том числе, в обучении, почему-то значительно более эффективны, чем прошлые, основанные на моторных реакциях памяти, по крайней мере, для маленького ребенка. Письмо перестало быть всеобъемлющей ценностью. И мы даже не обратили на это внимания, как не обращаем внимания на сопутствующие этому физиологические изменения, пока небольшие, но постепенно развивающиеся. Не следует этого пугаться, не следует по таким поводам бить в набат, потому что прогресс не остановить. И общество без ручного письма и угнетенных моторных реакций станет другим, получив взамен сумму других преимуществ, которыми до этого люди не пользовались.

Человек ориентируется в мире, где его знания, в определенной мере, перенесены в память компьютера, в память глобального информационного пространства. Оно выполняет роль ненавязчивой поддержки там, где мозг человека не справляется с объемной информацией. Но в случае отсутствия такой поддержки человек проявляет свойства беспомощности в самых простых ситуациях. Нужно ли этого бояться? Является ли это опасностью, которая может преследовать человека в глобальном информационном пространстве?

Такое уже было в истории человека. Сошлемся на интересного Юваля Н. Харари и его книгу «*Sapiens*. Краткая история человечества». Собирательство, в котором человек был субъектом, требовало от него огромных прикладных знаний о природе, значительно больших и специфических, чем прикладные знания о природе современного человека. Чтобы найти пропитание этим методом, надо было знать и места, где рос тот или иной плод, и перечень плодов съедоб-

ных и ядовитых, ссылаться на времена года в его динамике, уметь разбираться в климатических условиях не менее, чем сегодняшний гидрометеоцентр. Нужно было в совершенстве владеть приемами прямохождения и, при этом, уметь лазать по деревьям, плавать, далеко прыгать, прятаться от сильных врагов в этом трехмерном пространстве и еще отстаивать свои права в собственном обществе. Не зная законов природы, человек имел колоссальный эмпирический опыт и эффективно его использовал в прикладном значении.

С приходом земледелия, скотоводства, новых религий, с появлением новых способов ренессанса, а затем и появлением новых энергетических ресурсов, становлением научной революции, постепенно человек, за ненадобностью, стал забывать свои знания о прикладной природе, о методах активного собирательства. Их постепенно заменяли знания о торговле, механике, тепловой энергетике, электричестве, ядерных теориях и т. д. Прежние знания за небольшим исключением пожаловали на полку забвения. Все это привело не просто к изменению парадигмы быта человека, но к изменению приоритетов в культуре общества, его представлениях о природе. Прежние знания стали не нужными. И ничего, мир не перевернулся. Произошла подмена одних знаний другими знаниями и навыками, под них подстроились и культура, и экономика, и все общество. Появились совершенно иные формы общения, соответствующие новым знаниям. В равной степени, как теряются сегодня навыки ручного письма, письменного и устного счета и др., которые для нас подменяются компьютером. Новые современные формы общения посредством экранных технологий вводят в нашу жизнь предпочтение новым смысловым показателям, таким как отношения, желания, настроение, эмпатия. Они становятся новой формой объективности. Ушли в прошлое родовые отношения, многочисленные вожди и герои-одиночки, короли и султаны. Новые знания потребовали и других экономиче-

ских, и других социальных отношений, нового государственного устройства, новых форм доверительности. Через все это нам еще придется пройти.

Сегодня человек, освоившийся в глобальном информационном пространстве, как правило, более успешен в жизни, в карьере и даже в быту. Вокруг него формируется новая мини-среда, новый контент общения, новые жизненные ресурсы, включая денежные, совершенно новые отношения с друзьями. В основе всего – новый мир интернета, экранных и других современных технологий. И, в основе этого, потребность человека к общению, пониманию собственной полезности, всему тому, что иррационально он получил от информационной сети, от интернета.

Если считать все достоинства и недостатки глобального информационного пространства и его инструментариев, то первых значительно больше. А вторые, к сожалению, составляют предмет той науки, которую мы здесь рассматриваем, кибернетической безопасности. Именно этот факт является доминирующим в проблеме понимания смысла этой области знаний. Это не только безопасность компьютерных программ и сетей от внешнего вмешательства, но и безопасность человека во всех его массовых проявлениях. Тем более, что глобалистика в информатике уже привела человечество к новым социальным стандартам, к новым перспективным управленческим технологиям. И назад пути уже нет.

Общество, в лице ГИП, получило своеобразный «сад расходящихся тропок», описанный Хорхе Луисом Борхесом в своем одноименном рассказе. Аллегория «сада расходящихся тропок» заключается в том, что в системах развития не обойтись без реализации сразу всех вариантов развития, они дают направления новым тропкам, те где-то пересекаются, где-то расходятся, давая многообразие вариантов, так же, как в булевой алгебре двоичный код для двух позиций 00, 01, 10, 11 в конечном результате приводит к необозримому объему цифрового запоминания, сформулированного в таких двоичных кодах.

Глобальное информационное пространство предоставило человечеству беспрецедентный случай многообразия развивающихся направлений, своеобразных «тропок Борхеса», дающих право не выбора, а разностороннего развития. Внутри этого многообразия – направление на обеспечение безопасности, это та «тропка», которая не даст привести к самоуничтожению одного из наиболее современных универсальных инструментариев для всего человечества.

И задача у нас не заниматься выбором той из тропок, которая приведет к прогнозируемому развитию, а развиваться во всех возможных направлениях, понимая, что многообразие все равно приведет к процветанию.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

К первой главе

1. Уэзерфорд Дж. Чингисхан и рождение современного мира / Пер. с англ. Е. Лихтенштейна. М. : АСТ, Владимир: ВКТ, 2008. 493 с.

2. Сайт Internet Society (ISOC). URL: http://www.isoc.org

3. Зиновьева Е. С. Международное управление интернетом: проблемы, подходы, перспективы. *Вестник МГИМО*. № 6. 2010. С. 167–173. URL: http://www.rocit.ru/inform/index.php3?path=regulation Управление и регулирование Интернет.

4. Bloom H. Global Brain: The Evolution of Mass Mind the Big Band to the 21st Century. Hoboken^ Wiley, 2001.

5. Харари Ю. Н. Homo Deus. Краткая история будущего. М. : Синдбад, 2016. 496 с.

6. Кинг Б. Эпоха дополненной реальности / Б. Кинг; при участии А. Лайтмана, Дж. П. Рангасвами и Э Ларка. М. : Олимп-Бизнес, 2018. 528 с.

7. Бескаравайный С. Бытие техники и сингулярность. М. : Рипол Классик, 2018. 476 с.

8. Ковалева Н. Н. Информационное право России. М. : Дашков и К, 2008. 359 с. URL: https://lib.sale/informatsionnoe-pravo-rosii/ponyatie-globalnogo-informatsionnogo.html.

9. Добровольская И. А. Понятие «информационное пространство»: различные подходы к его изучению и особенности. *Вестник РУДН*, Ср.: Литературоведение. Журналистика, 2014. № 4. С. 140–144.

10. Koster F. Globalization, Social Structure, and the Willingness to help Others: a Multilevel Analysis Across 26 Coun-

tries. *European Sociological Review*. 2007. Vol. 23, No. 4. P. 540.

11. Chandrasekhar, C. P. How Global is the IT Industry? *Political Affairs*. 2006. September-October. URL: http://www.politicalaffairs.net/article/ articleview/4276/1/216.

12. Макаров В. П. Формирование глобального информационного пространства. *Тенденции современного мира. Вестн. Моск. Ун-та*. Сер. 18. Социология и политология. 2005. № 3. С. 3–18.

13. Нагирная А. В. Принципы развития глобального информационного пространства. *Фундаментальные исследования*. 2013. № 6 (ч. 6). С. 1462–1467.

14. Вся статистика интернета на 2020 год – цифры и тренды в мире и в России. URL: https://www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/

15. Crang M. Public Space, Urban Space: Would the Real City Please Stand Up? *Urban Studies*. 2000. Vol. 37. № 2. P. 301–317.

16. eBay запустила магазин в виртуальной реальности. Shopolog. URL: https://www.shopolog.ru/news/ebay-zapustila-magazin-v-virtual-noy-real-nosti/

17. Савельев Д. А. Мировое информационное пространство как предмет международно-правового регулирования технологии информационного общества / Интернет и современное общество : Материалы Всероссийской объединенной конференции. Санкт-Петербург, 2001. С. 201–220.

18. Стьюарт Т. Интеллектуальный потенциал. Новый источник богатства организаций / Новая индустриальная волна на Западе: Антология. 2012. С. 375.

19. Седов Д. С., Махина В. И. Иванченко М. Н. Влияние электромагнитного излучения, создаваемого персональным компьютером на здоровье человека. *Bulletin of Medical Internet Conferences*. 2012. Vol. 2. P. 920–922.

20. Ушаков И. Б. Оценка физических характеристик мониторов современных персональных компьютеров с позиций стандартов безопасности и характера деятельности. *Безопасность жизнедеятельности*. 2002. № 7. С. 19–22.

21. Шведов Г. И., Друганова Л. П., Шаева Т. В. Негативные факторы воздействия компьютера на здоровье человека. *Научно-медицинский вестник Центрального Черноземья*. 2008. № 32. С.85–88.

22. Опасность электромагнитного излучения. URL: http://medalternativa. info/entry/ elektromagnitnye-izluchenija/

23. Винер Н. Кибернетика и общество / пер. с англ. Е. Г. Панфилова. М. : Издательство иностранной литературы, 1958. 199 с.

24. Ожегов С. И. Толковый словарь русского языка. М. : Изд-во «Азъ», 1992. 680 с.

25. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия. *Вопросы кибербезопасности*. № 1(2). 2014. Р. 22–27.

26. Старовойтов А. В. Кибербезопасность как актуальная проблема современности. *Informatization and communication*. 2011. № 6. Р. 4–7.

27. Ежемесячное приложение к журналу «Стандарты и качество». Экологические аспекты проблем надежности и безопасность технических систем. «Основные понятия безопасности» / Алпеев А. С. М., 1994, вып. 7.

28. Богданов А. М., Мохор В. В. О кибербезопасности в широком смысле. *Information Technology and Security*. № 1(3). 2013. С. 5–18.

29. Осак А. Б., Бузина Е. Я. Влияние человеческого фактора при обеспечении кибербезопасности на надежность объектов электроэнергетики и живучесть электроэнергетических систем. *Актуальные проблемы гуманитарных и естественных наук*. № 12(83). 2015. Ч. II. С. 174–178.

30. Первый хакер в СССР. Остановил конвейер ВАЗа и остался на свободе. URL: http://yandex.ru/yandsearch? lr=213& text=%D0%BF%D0%B5%D1%80%D0%B2%D1%8B%D0%B9 +%D1%85%D0%B0%D0%BA%D0%B5%D1%80+%D1%81% D1%81%D1%81%D1%80&csg=5649%2C41594%2C12%2C25 %2C3%2C0%2C0.

31. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность. *Вопросы кибербезопасности*. 2014. № 5. С. 39–42.

32. Волошин В. С., Федосова И. В. Экологическая безопасность глобального информационного пространства. *Вісник Приазовського державного технічного університету. Серія: Технічні науки*. 2014. Вип. 29. С. 243–250.

33. Nevvit T., Barrington S. The Communication Ecology: Re-representation versus Replica. Toronto, London, Sidney: Butterworth. 1982.

34. Чуйкова Л. Ю., Чуйков Ю. С. Вопросы истории традиционного природопользования в содержании исторического модуля учебного экологического пространства. *Гуманитарные исследования*. 2013. № 2(46). С. 118–122.

35. Почепцов Г. Дезинформация / под. общ. ред. Н. Лигачевой, Г. Петренко. Киев : Изд. Паливода А. В., 2019. 248 с. URL: https://go.detector.media/wp-content/uploads/2019/ 10/Disinformation_Pochepcov_book_WEB. pdf

36. Сколько информации мир генерирует каждую минуту? URL: https://22century.ru/ popular-science-publications/ data-never-sleeps

37. Чернецова Н. С., Тешина П. С. Интернет как средство информационного влияния глобального масштаба. *Известия вузов. Поволжский регион. Экономические науки*. № 1(7). 2018. С. 65–74.

38. В Украине объявляется борьба с пиратством в интернете, что теперь нельзя? URL: http://hyser.com.ua/tehnology/v-ukraine-obyavlyaetsya-borba-s-piratstvom-v-internete-chto-teper-nelzya-83912.

39. Большие данные (Big Data). URL: http://www. Tadviser.ru/index.php/%D0%A1%D1%82%0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BE%D0%BB%D1%8C%D1%88%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_(Big_Data)

40. Полудина В. П. Информационный шум в интерете как проблема потребления коммуникаций. URL: http://ecsocman.hse.ru/data/2013/02/11/1251419219/Poludina_2011_5.pdf.

41. Полудина В. П. Социальная топография Интернета /Рунета/Виртуализация межуниверситетских и научных коммуникаций: Методы, структура, сообщества. М. : СОПСО, 2010. С. 19–40.

42. Маркова Т. Б. Чтение, как составная образа жизни: бумажная книга и/или электронный текст. *Библиосфера*. 2013. № 4. С. 7–15. URL: https://cyberleninka.ru/article/n/chtenie-kak-sostavnaya-obraza-zhizni-bumazhnaya-kniga-i-ili-elektronnyy-tekst/viewer.

43. Федоров А. В. Медиаобразование будущих педагогов. Монография. Таганрог : Изд-во Кучма, 2005. 314 с. URL: http://window.edu.ru/resource/616/36616/ files/ifap22.pdf

44. Официальный сайт International Data Corporation (IDC). URL: https://www.idc.com/

45. The writing is on the web for science journals in print. *Nature*. V. 397. pp. 195–200.

46. Алфимов М. В. Эра электронных библиотек. *Независимая газета. Наука*. №11. 1999. С. 2.

47. Арестова О. Н., Бабанин Л. Н., Войскунский А. Е. Мотивация пользователей Интернета. URL: http://cyberpsy.ru/articles/ internet_user_motivation/

48. Всемирный доклад о наркотиках. ООН. Нью-Йорк, 2016. URL: https://www.unodc.org/ doc/wdr2016/V1604259_ Russian.pdf

49. Опасные гаджеты: какие навыки дети теряют из-за смартфонов? URL: https://etcetera.media/pokolenie-smartfonov-kakie-navyiki-deti-teryayut-iz-za-gadzhetov.html

50. Модестов С. А. Информационное противоборство как фактор геополитической конкуренции. М.: 1999. С.46.

51. Расторгуев В. Н. Среда пребывания: принципы информационной политики / Экологическая адаптация общества на постсоветском пространстве. М. : 2000. С. 134–139.

52. Серегин А. В. Информационное пространство: функции, границы, перспективы развития / Экологическая артерия. М., 2000.

53. Объем данных в интернете вплотную приблизился к 500 экзабайтам. URL: Hitech.news.ru/article/19May2009/net volume.

54. Rosenzweig M. Win-Win Ecology: How Earth Species Can Survive In The Human Enterprise. ClarendonPress. ISBN 0-19-515604-8. 2005.

55. Facebook прослушивает пользователей. URL: https://112.ua/obshchestvo/facebook-proslushivaet-polzovateley-chtoby-vyvodit-reklamu-na-osnove-besed-professor-315487.html

56. Браузерный аддон Web Of Trust продавал данные пользователей. URL: https://xakep.ru/2016/11/08/wot-fail/

57. В Facebook появился новый вид мошенничества. URL: https://tehnot.com/v-facebook-poyavilsya-novyj-vid-moshenni chestva/

58. Аргонов В. Ю. Искусственное программирование потребностей человека: путь к деградации или новый стимул развития? *Вопросы философии*. 2008. № 12. С. 22–38.

59. Четвериков О. Н. Диктатура «просвещенных»: Дух и цели трансгуманизма. М. : Издатель Геннадий Маркелов, 2018. 160 с.

60. Удалов В. В., Медведев Д. А. Феномен NBIC-конвергенции: реальность и ожидания. *Философские науки*. 2008. № 1. С. 97–117.

61. Thomas W. Heeter. Method for Verifying Human Identity Electronic Sale Transactions. Патент США №5878155. 1999.

62. Холмс Л. «Норма» и «патология» в использовании Интернета / What is «Normal» Internet Use? Leonard Holmes, Ph.D. Перевод: Щепилина Е. А. URL: http://psynet.carfax.ru.

63. Новоселов А. В. Технологическая сингулярность как ближайшее будущее человечества. URL: http://andrej.virtualave.net/ Articles/singularity.html.

64. Google Аналитика. URL: https://analytics.google.com/analytics/web/provision/#/provision.

65. Наталия Касперская. «Миллиарды заработал пока Цукерберг, а остальные этих миллиардов не заработали». Интервью. URL: www.bfm.ru/news/236364.

66. В соцсетях вводится цензура на «язык вражды». URL: https://www.charter97. org/ru/news/2016/6/1/207133/.

67. Гаджеты Apple угроза национальной безопасности? URL: http://portaltele.com.ua/news/officially/gadzhety-apple-ugroza-natsionalnoj-bezopasnosti.html.

68. Цифровое общество – это сверх интеллектуальное общество. URL: http://www.gazetaprotestant.ru/2017/08/cifrovoe-obshhestvo-eto-sverx-intellektualnoe-obshhestvo/

Ко второй главе

1. Бауман З. Индивидуализированное общество. М. : Логос, 2005. 390 с.

2. Сеннет Р. Падение публичного человека. М. : Логос, 2002. 424 с.

3. Иноземцев В. Л. Зигмунд Бауман и его индивидуализированное общество. *Высшее образование в России*. 2004. № 1. С. 142–145.

4. Бацекова А. А. Концепция индивида и индивидуализации в теориях З. Баумана и У. Бека. *Вестник МГУ*. Сер. 18. Социология и политология. 2018. Т. 24. № 1. С. 71–75.

5. Грязнова Е. В., Афанасьев С. В. Индивидуализация человека в информационной социализации. *Философская мысль*. 2017. № 1. С. 17–29.

6. Петришев Е. Стадный инстинкт: почему интеллект в толпе исчезает. URL: https://www.spb.kp.ru/daily/26583/3599767/

7. Лебон Г. Психология народов и масс. М. : Академический проект, 2011. 238 с.

8. Эффект лайка. Стадный инстинкт в интернете. URL: http://aktiv.com.ua/archives/9481.

9. Википедия. URL: https://ru.wikipedia. org/wiki/%D0%9A%D0%BE%D0%BB%D0%BB%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B8%D0%B7%D0%BC.

10. Стадный инстинкт: миллионы мух не могут ошибаться? URL: https://mir24.tv/articles/16340810/stadnyi-instinkt-milliony-muh-ne-mogut-oshibatsya.

11. Da, Zhi and Huang, Xing, Harnessing the Wisdom of Crowds (December 1, 2018). Available at SSRN. URL: https://ssrn.com/abstract=2731884 or http://dx.doi.org/10.2139/ssrn.2731884.

12. Эффект Рингельмана: почему вместе работать хуже, чем по отдельности. URL: https://l-a-b-a.com/blog/923-6-sovetov-kak-uluchshit-ehffektivnost-komandy.

13. Гринин Л. Е., Марков А. В., Коротаев А. В. Макроэволюция в живой природе и обществе. 2-е изд. М. : Книжный дом «Либриком», 2009. 248 с.

14. Марков А. В., Коротаев А. В. Гиперболический рост в живой природе и обществе. М. : Книжный дом «Либриком», 2009. 200 с.

15. Хагуров Т. А. Кризис модерна и образования. *Фундаментальные аспекты психического здоровья*. 2011. № 4. С. 16–26.

16. Харари Ю. Н. Sapiens: Краткая история человечества / пер. с англ. Л. Сумм. М. : Синдбад, 2016. 520 с.

17. Понимание / Словарь по логике. М. : Туманит, изд. центр ВЛАДОС. А. А. Ивин, А. Л. Никифоров. 1997.

18. Галушкин А. И. Нейронные сети. Основы теории. М. : Изд. Горячая линия – телеком. 2010. 289 с.

19. Хайкин С. Нейронные сети. Полный курс. 2-е изд. М. : Издательский дом «Вильямс», 2006. 1104 с.

20. Барский А. Б. Нейронные сети: распознавание, управление, принятие решений. М. : Финансы и статистика, 2004. 380 с.

21. ИИ научился скрывать информацию, чтобы подделывать результаты работы. URL: http://internetua.com/ii-naucsilsya-skryvat-informaciua-cstoby-poddelyvat-rezultaty-raboty.

22. Лега В. Н. История западной философии. Ч. 1. Изд. Православного Свято-Тихоновского гуманитарного университета. 2016. 461 с.

23. Альтшуллер Г. С., Верткин И. М. Рабочая книга по теории развития творческой личности. Кишинев : МНТЦ «Прогресс», Картя Молдовеняскэ. 1990.

24. Волошин В. С. Влияние глобального информационного пространства на некоторые творческие способности человека. *Вісник Приазовського державного технічного університету. Серія: Соціально-гуманітарні науки та публічне адміністрування*. Вип. 3. 2019. С. 5–10.

25. Харрис Р. Психология массовых коммуникаций. СПб. : Прайм-Еврознак, 2002. 448 с.

26. Greenfield P. M. Mind and Media: The Effects of Television, Video Games, and Computers. Cambridge Mass.: Harvard University Press, 2004. 232 p.

27. Как компьютерные игры меняют мозг человека. URL: http://netaddiction.ru/689.

28. Выготский Л. С. Психология искусства. Ростов н\Д : Феникс, 1998. 480 с.

29. Nevvit T., Barrington S. The Communication Ecology: Re-representation versus Replica. Toronto, London, Sidney: Butterworth (Butterworth-Heinemann Ltd). 1983. 192 p.

30. Морозов Н. А. Христос. (История человечества в естественнонаучном освещении). М.–Л. : Госиздат, 1924–1932.

31. Льюис Г. К. Исследования о достоверности древнейшей римской истории. Ганновер, 1852. Lewis G. C. Untersuchungen uber die Glaubwurdigkeit der altromschen Geschichte… – Hannover, 1858.

32. Vosoughi S., Roy D., Aral S. The spread of true and false news online. *Science.* 2018, Vol. 359, Issue 6380, pp. 1146–1151. URL: https://science.sciencemag.org/content/359/6380/1146.

33. Ложь в Сети: как распознать недостоверную информацию в интернете? URL: https://aif.ru/society/web/kak_raspoznat_nedostovernuiu_informatciiu_v_internete.

34. Желев Ж. Фашизм. Тоталитарное государство. М. : Изд. «Новости», 1991. 151 с.

35. Альтман Ю. И. Двоемыслие, как рассогласование ценностных ориентаций: интегративно-психологический подход. *Russian Journal of Education and Psychology*. № 5(49). 2015. С. 599–606. URL: www.sisp.nkras.ru.

36. Винер Н. Человеческое использование человеческих существ: Кибернетика и общество / Общая редакция и предисловие Э. Я. Кольмана. М. : Изд. иностранной литературы, 1958.

37. Винер Н. Человек управляющий. СПб. : Питер, 2001. 283 с.

38. Опасная человечность: зачем нам разумный искусственный интеллект? URL: http://internetua.com/opasnaya-cselovecsnost-zacsem-nam-razumnyi-iskusstvennyi-intellekt-

39. Настин И. В. Психолингвистика. М. : Изд. МПСИ, 2007. 139 с.

40. Мелитан К. Психология лжи. М. : А. Сомов, 1903. 30 с.

41. Бердяев Н. А. Парадокс лжи. *Человек*. 1999. № 2. *С.* 102–108. URL: http://www.odinblago.ru/paradoks_lzhi.

42. Машина правды. Блокчейн и будущее человечества / Пол Винья, Майкл Кейси; пер. с англ. М. Сухотиной. М. : Манн, Иванов и Фербер, 2018. 320 с.

43. Тапскотт Д., Тапскотт А. Технология блокчейн: то, что движет финансовой революцией сегодня / пер. с англ. К. Шашковой, Е. Ряхиной. М. : Эксмо, 2018. 448 с.

44. Генкин А., Михеев А. Блокчейн: как это работает и что нас ждет завтра. М. : Альпина Паблишер, 2018. 592 с.

45. Tompson C. Apple Has a Smart Home Problem: People Don't Know They Want It Yet. *Business Insider,* June, 2015. URL: www.businessinsider.com/apple-home kit-adoption-2015-6.

46. McKinsey An Executive's Guide to the Internet of Things. August 2015. URL: www.mckinsey.com/Insights/business_Technoligy/An_executives_guide_to_the_Internet_of_Things?cid=digital-eml-alt-mip-mck-oth-1508.

47. Пряников М. М., Чугунов А. В. Блокчейн как коммуникационная основа формирования цифровой экономики. Преимущества и проблемы. *International Journal of Open Information Technologies*. 2017. Изд. МГУ. URL: https://cyberleninka.ru/article/n/blokcheyn-kak-kommunikatsionnaya-osnova-formirovaniya-tsifrovoy-ekonomiki-preimuschestva-i-problemy.

48. Kaminska I. Bitcoin's Wasted Power-and How It Could Be Used to Heat Homes. FT Alphaville, *Financial Times,* September 5, 2014.

49. Волошин В. С., Федосова И. В., Мироненко Д. С. К вопросу о типичности блокчейн-технологий в инжиниринге. *Вісник Приазовського державного технічного університету. Серія: Технічні науки.* 2019. Вип. 39. С. 151–159.

50. Медоуз Д. и др. Пределы роста / пер. с англ.; Предисл. Г. А. Ягодина. М. : Изд-во МГУ, 1991. 208 с.

51. Mesarovic M., Pestel E, Mankind at the Turning Point: Second Report to the Club of Rome. New York: E P Dutton; 4th Printing edition, February 1, 1975.

52. URL: https://github.com/solid/solid#about-solid.

53. ITU Releases 2014 ICT Figures. URL: www.itu.int/net/pressoffice_releases/2014/23.aspx#VEfavolF_Kg

54. Волошин В. С. Белопольский Н. Г. Феномен денег. К. : Освита Украины, 2018. 462 с.

55. Эндрю Кин. Ничего личного: Как социальные сети, поисковые системы и спецслужбы используют наши персональные данные. М. : Альпина Паблишер. 2016. 244 с.

56. Всемирная книга фактов ЦРУ, статистика по грамотности. URL: www.cia.govlibrary/publications/the-world-factbook/fields/2103.html#136

К третьей главе

1. Aho J. Confession and Bookkeeping: The Religious, Moral and Rhetorical Roots of Modern Acounting. New York, State University of New York Press, 2006. 384 p.

2. Poovey M. A History of the Modern Fact. Chicago. University of Chicago Press, 1998. 254 p.

3. Волошин В. С., Белопольский Н. Г. Феномен денег. К. : Освита Украины, 2018. 462 с.

4. Lehman Brothers Holding inc. Annual Report Pursuant to section 13 or 15 of the Securities Exchange Act of 1934 for the Fiscal Year Ended November 30, 2007. URL: https: //www.sec.gov/Archives/edgar/data/806085/00011046508005476 /a08-3530_110k.htm.

5. Goldstein J. Repo 105: Lehman's «Accounting Gimmick» Explained, 2010. URL: http://www.npr.org/sections/ money/2010/03/repo_lehman_accounting_gi.html.

6. Винья П., Кейси М. Машина правды. Блокчейн и будущее человечества / пер. с англ. М. Сухотиной. М. : Манн, Иванов и Фербер, 2018. 320 с.

7. Sztompka P. Trust: a sociological theory. Cambridge, University press. 1999. 214 p.

8. Фукуяма Ф. Доверие: социальные добродетели и путь к процветанию. М. : Изд. АСТ ; Ермак, 2004. 271 с.

9. Ерошин Д. А. Количественная оценка уровня доверия: проблемы и перспективы. Кострома: *Вестник КГУ им. Некрасова*. № 4. 2011. С. 108–111.

10. Friedman T. The World is Flat: A Brief Historu of the Twenty-First Century. Farrat,Straus and Giroux, 2005. 74 p.

11. Тапскотт Д., Тапскотт А. Технология блокчейн: то, что движет финансовой революцией сегодня / Пер. с англ. К. Шашковой. М. : Эксмо, 2018. 448 с.

12. Волошин В. С., Лямзин А. А. О некоторых особенностях криптовалют и их роли в современном финансовом мире. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. 2017. Вип. 16. С. 6–15.

13. ForexStandard. Рынок Форекс: новости, прогнозы и аналитика. URL: https://forexstandard.ru/.

14. Spydel. LiveJournal. URL: http://ic.livejournal.com/ spydell/

15. Зверянская Л. П. Интернет-зависимость как основная причина развития киберпреступности. *Фундаментальные*

и прикладные исследования: проблемы и результаты. 2015. № 17. С. 239–43.

16. Сеул усилит контроль за финансовыми учреждениями. URL: ria.ru.world/20140121/990452107.html.

17. Банковские технологии. URL: http://www.banktech.ru /news/dannye-15-mln-klientov-yuzhnokoreyskih-bankov-popali-k-moshennikam

18. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы. Омск. 2009. 480 с.

19. Осипенко А. Л. Организованная преступность в сети интернет. *Вестник Воронежского института МВД России*. № 3. 2012. С. 10–13.

20. Кузнецов А. В. Борьба с преступлениями, совершенными с использованием сети интернет. *VI Международная научно-практическая конференция «Право и интернет»*. М., 2004. С. 77–7.

21. Васильев А. А., Демин К. Е. Электронные носители данных как источники получения криминалистически значимой информации : учеб. пособие. М. : Моск. гос. обл. ун-т, 2009. 198 с.

22. Клэй А., Филипс К. М. Зарабатывать на хайпе. Чему нас могут научить пираты, хакеры, дилеры и все, о ком не говорят в приличном обществе / пер. с англ. Е. Деревянко. М. : Изд. ООО «Э», 2018. 217 с. URL: http://maxima-library.org/knigi/genre/b/419639?format=read.

23. Талипова Л. Р. Международно-правовая регламентация киберпреступности. *Гуманитарные, социально-экономические и общественные науки*. № 3. 2016. С. 121–123.

24. Правовая база и права человека. Киберпреступность. Мод. 3. Организация Объединенных Наций. Вена, 2019. 45 с.

25. Всестороннее исследование проблемы киберпреступности. Организация Объединенных Наций. Нью-Йорк. 2013. 330 с.

К четвертой главе

1. Мелани Свон. Фрагмент книги «Блокчейн. Схема новой экономики». URL: http://www.management.com.ua/ims/ims268.html.

2. Волошин В. С. Ожидаемые и реальные риски в блокчейнтехнологиях. *Теоретичні і практичні аспекти економіки та інтелектуальної власності*. 2018. Вип. 17. С. 6–14.

3. Tadviser. Государство, бизнес, IT. URL: http://www.tadvier.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain).

4. В Австралии разработают стандарты для блокчейна. *Инвест-Форсайт. Деловой журнал*. № 16. 2017. URL: https://www.if24.ru/v-avstralii-razrabotayut/

5. Евросоюз создал партнерство для развития блокчейн. *Журнал «Плас. новости, технологии»*. 2018. URL: https://www.plusworld.ru/daily/tehnologii/evrosoyuz-sozdal-partnerstvo-dlya-razvitiya-blokchejn/

6. Валиев К. А. Квантовая информатика: компьютеры, связь и криптография. *Вестник РАН*. 2000. Т. 70. № 8. С. 688–695.

7. Блокчейн может использоваться для распространения нелегального контента. *SecurityLab*. URL: https://www.securitylab.ru/news/492202.php.

8. Расходы на майнинг биткоина превысили его стоимость. URL: https://finance.liga.net/cryptoeconomics/novosti/rashody-na-mayning-bitkoina-prevysili-ego-stoimost.

9. Статистический ежегодник мировой энергетики 2019. URL: https://yearbook.enerdata.ru/

10. Bitcoin: A Peer-to-Peer Electronic Cash System/ Satoshi Nakamoto, 2009. URL: https://bitcoin.org/bitcoin.pdf.

11. Kaminska I. Bitcoin’s Wasted Power-and How It Could Be Used to Heat Homes. *Financial Times*. 2014. September 5.

URL: https://www.ft.com/content/384a349a-32a5-11e4-93c6-00144feabdc0.

12. Тапскотт Д., Тапскотт А. Технология блокчейн: то, что движет финансовой революцией сегодня / пер. с англ. К. Шашковой, Е. Ряхиной. М. : Эксмо, 2018. 448 с.

13. Пятин А. Эксперты сравнили энергозатраты на майнинг биткоина и на обеспечение электричеством Швейцарии URL: https://www.forbes.ru/tehnologii/379291-eksperty-sravnili-energozatraty-na-mayning-bitkoina-i-na-obespechenie.

14. Новый индекс CBECI предполагает, что биткоин потребляет больше энергии, чем Швейцария. URL: https://bitnewstoday.ru/news/novyy-indeks-cbeci-predpolagaet-chto-bitkoin-potreblyaet-bolshe-energii-chem-shveytsariya/

15. К концу этого года биткоин будет потреблять столько же энергии, как целая Австрия. URL: https://www.facepla.net/the-news/tech-news-mnu/5863-%D0%BC%D0%B0%D0%B9%D0%BD%D0%B8%D0%BD%D0%B3-%D0%BF%D0%BE%D1%82%D1%80%D0%B5%D0%B1%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5.html

16. Сколько сейчас майнинг потребляет электричества? URL: https://masterok.livejournal.com/4485604.html.

17. Bitcoin Mining Now Consuming More Electricity Than 159 Countries Including Ireland & Most Countries In Africa. URL: https://powercompare.co.uk/bitcoin/

18. Биткоин-майнинг и потребление энергии / пер. материала Л. Уиза. URL: https://vc.ru/crypto/30588-bitkoin-mayning-i-potreblenie-energii

19. Демченко Д. Майнинг биткоина занимает почти 1 % потребления энергии в мире URL: https://ain.ua/2018/08/27/majning-bitkoina-zanimaet-1-potrebleniya-energii-v-mire/

20. Bitcoin Energy Consumption Index. URL: https://digiconomist.net/bitcoin-energy-consumption.

21. Palacio N. S. Blockchein : A technological tool for sustainable development or a massive energy consumption network.

Bionatura. 2018. Vol. 3. № 4. URL: http://revistabionatura.com/files/2018.03.04.11.pdf

22. Среднее значение времени подтверждения. URL: https://www.blockchain.com/charts/median-confirmation-time?timespan=all.

23. Графики Биткоин. URL: https://www.blockchain.com/ru/charts.

24. Оборудование для майнинга криптовалют 2019 – ASIC и GPU-фермы. URL: https://mining-cryptocurrency.ru/oborudovanie-dlya-majninga/

25. Подтвержденные транзакции в день. URL: https://www.blockchain.com/ru/charts/n-transactions?timespan=all.

26. Общая хэш-ставка (TH/s). URL: https://www.blockchain.com/ru/charts/hash-rate.

27. Крутов В. Главный фактор успешности майнинга. Все о добыче Bitcoin – за 5 минут. URL: https://www.rbc.ru/crypto/news/5e578c759a79479afbbdb2ad.

28. Дурдыева Д. А., Трапизонян А. А. Состояние криптовалютного рынка и перспективы развития биткоина. *Инновационная наука*. 2017. № 01-1. С. 43–47.

29. Саакян А. Г. Криптовалюта как первичный инструмент в формировании валютного регулирования государства. *Научный вестник Южного института менеджмента*. 2015. № 4. С. 17–20.

30. Статистический ежегодник мировой энергетики. URL: https://yearbook.enerdata.ru/electricity/world-electricity-production-statistics.html.

31. Биткоин Хешрейт график. URL: https://bitinfocharts.com/ru/comparison/bitcoin-hashrate.html.

32. Фрэнк Уэбстер. Теории информационного общества / пер. с англ. М. В. Арапова и Н. В. Малыхиной ; под ред. докт. филол. наук, профессора Е. Л. Вартановой. М. : Аспект Пресс, 2004. 220 с.

33. Nouriel Roubini. Crypto is the Mother of All Scams and (Now Busted) Bubbles While Blockchain Is The Most Over-Hyped Technology Ever, No Better than a Spreadsheet / Database. New York University, October 2018. URL: https://www.banking.senate.gov/imo/media/doc/Roubini%20Testimony%2010-11-18.pdf.

34. Храмцовская Н. А. Технология блокчейна как инструмент управления документами и электронного документооборота. *Делопроизводство*. № 3. 2018. С. 34–39.

35. Шесть мифов о блокчейне и Биткойне, или Почему это не такая уж эффективная технология / Маланов А. Е. Kaspersky Lab. URL: https://habr.com/ru/company/kaspersky/blog/336036/

36. Аммус С. Краткая история денег / пер. с англ. М. Сухотиной ; науч. ред. Н. Решетняк. М. : Манн, Иванов и Фербер, 2019. 272 с.

37. Генкин А., Михеев А. Блокчейн. Как это работает и что нас ждет завтра / ред. А. Петров. М. : Альпина Паблишер, 2018. 592 с.

38. Кастельс М. Информационная эпоха: экономика, общество и культура / пер. с англ. под науч. ред. О. И. Шкаратана. М. : ГУ ВШЭ, 2000. 608 с.

39. Табернакулов А., Койфманн Я. Блокчейн на практике. М. : Альпина Паблишер, 2019. 260 с.

40. Машина правды. Блокчейн и будущее человечества / Пол Винья, Майкл Кейси; пер. с англ. М. Сухотиной. М. : Манн, Иванов и Фербер, 2018. 320 с.

41. Лихачев Н. Н. Самое понятное объяснение принципа работы блокчейна. URL: https://tjournal.ru/41306-samoe-ponyatnoe-obuasnenie-principa-raboti-blokcheina//2017.

К пятой главе

1. Харари Ю. Н. Sapiens. Краткая история человечества / пер. с англ. Л. Сумм. М. : Синдбад, 2016. 520 с.

2. Salim H. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. Massachusetts Institute of Technology, 2014. 157 p. URL: http://www.ic3.mit.edu.

3. Convettion on Cybercrime. Budapest, 23/11/2001. URL: http://www.coe.int.

4. Кузнецов С. Кибербезопасность в 21 веке. *Открытые системы СУБД*. № 5. 2013. URL: https://www.osp.ru/os/2013/05/13036002

5. Cohen A. The Willie Sutton Theory of Cyber Securty, 2015. URL: http://www.securityweek.com.

6. Katz. E. M., Claypoole T. F. Willie Sutton Is on the Internet: Bank Security Strategy in a Shared Risk Environment, 5 N. C. Banking Inst. 167 (2001). URL: http://scholarship.law.unc.edu/ncbi/vol5/iss1/8.

7. Безкоровайный М. М. Татузов А. Л. Кибербезопасность – подходы к определению понятия. *Вопросы кибербезопасности*. Вып. № 1(2). 2014. С. 22–27. URL: http://www.cyberleninka.ru.

8. ProstoCoin. URL: https://mail.google.com/mail/u/0/#inbox/FMfcgxwHMsRmwwXXGDTRbtTCSGTTLzDt

9. 20 интернет-ресурсов для специалистов по информационной безопасности. URL: https://geoline-tech.com/top-20-sites-about-information-security/

10. Anti-Malware. URL: https://www.anti-malware.ru/

11. Security Lab. URL: http://www.securitylab.ru/

12. Угрозы информационной безопасности. SearchInform. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/ugrozy-informatsionnoj-bezopasnosti/

13. ТОП-5 полезных ресурсов и кибербезопасности. URL: https://indevlab.com/ru/blog-ru/top-5-poleznyh-resursov-o-kiberbezopasnosti/

14. Информационная безопасность. IT-news. URL: https://www.it-world.ru/it-news/security/

15. Кибербезопасность. ITCua. URL: https://itc.ua/tag/kiberbezopasnost/

16. Тег: Кибербезопасность. Новости о цифровой безопасности. URL: https://rb.ru/tag/cybersecurity/

17. Security News. URL: https://security-news.today/cybersecurity/

18. Trend Micro. Экстренные новости о безопасности и аналитика. URL: https://www.trendmicro.com/ru_ru/security-intelligence/breaking-news.html.

Вячеслав Волошин

Кибернетическая безопасность.
Социальные и прикладные вопросы

Ответственная за выпуск: Кришталь А. И.
Верстка: Кришталь А. И.
Оформление обложки: Долгая М. В.

Подписано в печать 05.01.2021.
Формат 60x84/16. Бумага офсетная.
Усл. печ. л. 17,09
Тираж 300 экз.

ИД «Освита Украины»
ФЛ-П Маслаков Руслан Алексеевич
Свидетельство о внесении субъекта издательского дела
в государственный реестр издателей, изготовителей
и распространителей издательской продукции
ДК №4726 от 29.05.2014 г.

«Небольшие различия в начальных условиях рождают огромные различия в конечном явлении»

Жюль Анри Пуанкаре