

ЯН
ХЕГЛЕР

МАНИФЕСТ КРИПТОНАРХИСТА



Альтер-фабрика

Ян Хеглер

Манифест криптоанархиста

«Страта»

2017

УДК 004 + 681 + 32.019
ББК 66.7

Хеглер Я.

Манифест криптоанархиста / Я. Хеглер — «Страта»,
2017 — (Альтер-фабрика)

ISBN 978-5-9500888-5-8

Криптоанархизм – философия, суть которой в том, чтобы использовать сильную криптографию для защиты приватности и личной свободы. Криптоанархисты – люди, которые поддерживают философию криптоанархизма. Они считают, что криптография защищает людей от слежки в Интернете и уверены, что законы математики сильнее человеческих законов и что без шифрования сообщений и информации личная жизнь людей пострадает. Их глобальная цель – Интернет доверия. Это явление можно отнести к сфере социально-политической идеологии, направленной на борьбу за свободу слова, тайну личности и частной переписки. Только в качестве основного инструмента этой борьбы криптоанархисты видят не стачки, митинги и уличные протесты, а математические алгоритмы и глубокое шифрование. Возможно ли реализовать в киберпространстве социально-технологические модели, которые многие современные эксперты считают утопиями? Книга знакомит с мнениями авторитетных специалистов в различных областях современной науки.

УДК 004 + 681 + 32.019
ББК 66.7

ISBN 978-5-9500888-5-8

© Хеглер Я., 2017

© Страта, 2017

Содержание

Миссия серии «Альтер-фабрика»	7
Вместо вступления: криптоанархизм в современном обществе	8
Чего хотят криптоанархисты?	12
Конец ознакомительного фрагмента.	17

Ян Хеглер

Манифест криптоанархиста

© Хеглер Я., текст, 2017

© ООО «Страта», 2018

Миссия серии «Альтер-фабрика»

Серия «Альтер-фабрика» представляет другой, то есть альтернативный привычному, взгляд на экономику, бизнес, управление.

Мы живем, работаем, принимаем решения в мире, который часто и скорее по привычке называют то капитализмом, то постиндустриальным обществом, то цифровой цивилизацией.

Но этот мир подвижнее, изменчивее и многообразнее стандартных определений. В этом мире безостановочно возникает и конкурирует множество вариантов экономической системы, общественного устройства, культурного кода.

Это мир альтернатив. В нем товары, технологии, идеи создают пространство выбора. И выбор здесь не пассивное выражение согласия или предпочтения. Выбор – это творческое решение. Выбор другого варианта, отличного от привычного, – это способ создать перспективный ресурс, технологию, бизнес-модель, стиль жизни.

Миссия серии «Альтер-фабрика» – продуцировать идеи, расширяющие концептуальное пространство выбора и легко превращающие символический ресурс альтернативного видения в реальный ресурс оригинальных бизнес-решений.

В серию войдут работы практикующих предпринимателей, менеджеров, бизнес-консультантов, чьи решения опираются на альтернативное видение рынков, организаций, бизнес-процессов.

Также в рамках серии будут публиковаться книги ученых, чье альтернативное видение современной экономики нашло международное признание и создает актуальную перспективу выработки инновационных моделей и технологий производства, потребления, организации и управления.

Дмитрий Иванов, научный редактор серии

Вместо вступления: криптоанархизм в современном обществе

Нам посчастливилось жить в удивительное время – время перемен. И главным драйвером этих перемен является бурное развитие информационных технологий, которое мы наблюдаем на протяжении последних десятилетий. Эволюция технологий меняет привычный нам мир, причем меняет его кардинально и качественно, открывая принципиально новые горизонты в развитии общества.

Если внимательно проанализировать историю цивилизации, мы обнаружим сразу несколько характерных точек бифуркации, в которых казавшийся доселе неизменным вектор развития общества резко сменил свое направление. Первой такой точкой стало изобретение письменности, позволившее не только значительно упростить процесс передачи информации и консолидировать в материальной форме ее источники, но дало заметный толчок в развитии экономической, юридической, многих других систем и социальных институтов. Второй важной вехой в истории человечества было возникновение книгопечатания – это изобретение открыло путь к тиражированию информации, ее быстрому распространению и в конечном итоге предоставило доступ к источникам для широких слоев населения. Третья определяющая ступень в эволюции нашей цивилизации – рождение в XX столетии кибернетики и появление компьютеров. На данном этапе информация, как явление, избавилась от материальных носителей, полностью обретя свою современную виртуальную форму. Наконец, следующей ступенью постиндустриальной революции, которую мы переживаем прямо сейчас, стало развитие и широкое распространение криптографии, а также появление блокчейна.

♦ **Блокчейн (англ. *blockchain*) – это выстроенная по определенным правилам непрерывная последовательная цепочка блоков, содержащих информацию. О техническом значении этого термина мы поговорим позже, пока лишь упомянем, что именно на основе блокчейна построены все распространенные сегодня в мире криптовалюты. Именно эти технологии, по мнению целого ряда авторитетных IT-специалистов и энтузиастов кибернетики, лягут в основу общества будущего – цифрового общества, лишенного несправедливости и неравенства.**

Какой же смысл вкладывают эти энтузиасты в понятие «цифровой цивилизации», на каких законах и принципах они планируют строить такое общество? Если обратиться к многочисленным сетевым публикациям, а также довольно редким (и в основном, англоязычным) академическим источникам, можно прийти к очевидному выводу, что большинство из них представляют собой гремучую смесь из социологии и психологии масс с легкой примесью технических терминов, что в совокупности дает весьма посредственное и трудное для понимания чтение. Более того: лишь единичные из этих источников более или менее четко описывают саму проблему, вокруг которой фокусируются вопросы развития цифровых технологий в разрезе общества. Гораздо глубже и полнее вопрос освещается на различных дискуссионных площадках и в социальных сетях, иногда перерастая в весьма агрессивную полемику, но и там вместо самого предмета обсуждения, как правило, лишь некоторые прикладные аспекты использования тех или иных технологий. Видимо, в рамках подобного дискурса все стороны по умолчанию предполагают, что объект хорошо известен каждому, и по этому поводу уже давно достигнут полный и всеобщий консенсус. Вместе с тем, даже для самого понятия криптоанархии до сих пор не дано однозначного, исчерпывающего и стопроцентно устраивающего всех определения.

В своей работе «Криптоанархия, кибергосударства и пиратские утопии» известный публицист, философ и преподаватель Северо-Западного Университета Питер Ладлоу пишет:

«По какой-то причине большинство из нас считает, что анархисты – это самые настоящие фрики с длинными лохмами, швыряющие бутылки с коктейлем Молотова в окна добропорядочных банков. На самом деле анархия не имеет ничего общего с такими представлениями».

С точки зрения многих современных анархистов, государства в том виде, в котором они существуют на сегодняшний день, выполняют функции посредников между населением и социальными институтами, играют роль централизованного механизма, реализующего сбор и перераспределение материальных благ с использованием инструментов насилия. Современная модель экономики и социального устройства строится на управлении материальными ресурсами, при которой граждане, отдавая часть вырученных в результате производства добавленной стоимости средств, вправе рассчитывать на получение определенного комплекса услуг, таких как, например, защита прав и свобод, гарантия соблюдения законов, а также, не в последнюю очередь, – выполнение целого комплекса процессуальных действий при заключении сделок, исполнении контрактов и обеспечении законности подобных актов. Основной недостаток такого механизма заключается в том, что сама государственная система в целях поддержания собственной работоспособности потребляет значительные ресурсы. *Один из основных тезисов идеологии криптоанархистов как раз и кроется в том, чтобы исключить из схемы социального устройства «лишних», по их мнению, посредников, переложив контрольную функцию на плечи современных информационных технологий, и в первую очередь – криптографии.*

Согласно определению, приведенному в «Википедии», криптоанархизм – это философия, призывающая к использованию сильной криптографии для защиты приватности и личной свободы. Этот термин впервые появился в журнале «Тайм», в статье «Who Should Keep the Keys?», опубликованной 14 марта 1994 года. А в материале «Кто такие криптоанархисты и нужно ли нам их бояться?» электронный журнал RUBASE дает более развернутое определение этому явлению:

♦ «Криптоанархизм – философия, суть которой заключается в том, чтобы использовать сильную криптографию для защиты приватности и личной свободы.

Криптоанархисты считают, что криптография защищает людей от слежки в Интернете и уверены, что *законы математики сильнее человеческих законов* и что без шифрования сообщений и информации личная жизнь людей пострадает. Криптоанархисты – это люди, которые поддерживают философию криптоанархизма. Глобальная цель криптоанархистов – Интернет доверия. Это такой коллективный краудфандинговый проект – глобальный независимый интернет-провайдер, который находится в коллективной собственности и реализован через спутниковый Интернет и пиринговые фемсоты. Этот Интернет будет изначально закриптован и анонимизирован, также в него будет имплементирована расчетная система, основанная на подписях и репутации пользователей».

Таким образом, можно прийти к выводу, что криптоанархизм – сам по себе явление в большей степени конструктивное, нежели деструктивное. Иными словами, данное явление можно отнести к сфере социально-политической идеологии, направленной на борьбу за свободу слова, тайну личности и частной переписки. *Только в качестве основного инструмента этой борьбы криптоанархисты видят не стачки, митинги и уличные протесты, а математические алгоритмы и глубокое шифрование.*

Одним из ключевых аспектов широкого распространения подобных идей в обществе можно назвать доступность современных технологий шифрования и наличие большого количества реализующего эти технологии программного обеспечения, в том числе – свободно распространяемого и имеющего открытый исходный код. Именно это не в последнюю очередь открывает для современных IT-специалистов и простых пользователей, симпатизирующих идеям криптоанархизма, широкое пространство для деятельности и поистине безгранич-

ное поле возможностей. *А развитие блокчейна позволяет делегировать значительную часть государственных функций, связанных с регулированием и контролем, самому компьютерному сообществу перенести их в киберпространство.* Безусловно, государство, как цивилизационный институт, не может не противиться подобной конкуренции, вызывающей внутри него центристские силы, направленные на общую децентрализацию регулирующих функций. Отсюда – все те репрессивные меры противодействия, которые проводятся сегодня против этого комплекса явлений, в том числе на законодательном уровне.

Перенос в киберпространство регулирующих и управляющих функций может осуществляться с использованием технологии блокчейна. Впервые этот термин появился как название распределенной базы данных, реализованной в анонимной платежной системе «Биткоин», из-за чего блокчейн часто относят к транзакциям в различных криптовалютах, однако технология цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки.

Блок транзакций – специальная структура для записи информации, которая должна быть формально завершенной и подтвержденной. Транзакция считается завершенной и подтвержденной, когда проверены ее формат и подписи, и когда сама транзакция объединена в группу с несколькими другими; она собирается в специальную структуру – блок. Блок содержит заголовок и список транзакций, то есть операций, сведения о которых хранятся в нем. Содержимое блоков также может быть проверено, поскольку каждый блок содержит информацию о предыдущем. Все блоки выстраиваются в цепочку, которая содержит информацию обо всех совершенных когда-либо операциях в базе.

Самый первый блок в цепочке – первичный блок (англ. *genesis block*) – рассматривается как отдельный случай, поскольку у него отсутствует родительский блок. Создаваемые в рамках системы блоки должны отвечать целому ряду математических и функциональных критериев. Удовлетворяющие критериям блоки отправляются в сеть, включаясь в распределенную базу блоков, а информация о них сохраняется в других блоках. Регулярно возникают ситуации, когда несколько новых блоков в разных частях распределенной сети называют предыдущим один и тот же, то есть цепочка может ветвиться. Распределенная база данных блокчейн формируется как непрерывно растущая цепочка блоков с записями обо всех совершенных в системе транзакциях. Копии базы или ее части одновременно хранятся на множестве компьютеров сети и синхронизируются согласно формальным правилам. Информация в блоках не зашифрована, доступна в открытом виде, но отсутствие изменений удостоверяется криптографическим способом.

Таким образом, сведения обо всех транзакциях, то есть операциях, совершенных когда-либо в системе блокчейн, хранятся сразу на множестве компьютерах пользователей сети и могут быть подтверждены в любой момент без всяких усилий. **Эту информацию невозможно подделать.** Например, если на этом принципе будет построена база данных собственников земельных участков или объектов недвижимости, в ней нельзя будет «засекретить» какие-либо записи или подменить их «задним числом», поскольку все сведения обо всех операциях с объектом базы хранятся в распределенной системе, и несанкционированные изменения просто не будут подтверждены системой и не смогут считаться легитимными.

Апологеты блокчейна считают, что на этом принципе можно построить не просто защищенные, анонимные и децентрализованные платежные системы (таковые существуют во множестве уже сегодня), но также финансовые институты, подобные современным банковским, системы, способные заменить нотариат, биржи или краудкрафтинг (и это сейчас уже тоже технически реализовано).

♦ **Финальной точкой процесса «блокчейнизации» современного общества многие криптоанархисты видят создание своеобразного трансграничного «цифрового государства», под которым понимается, как правило, не территориальное, а соци-**

альное образование людей, объединенных новой, «цифровой» идеологией и доктриной.

Возможно ли реализовать в киберпространстве подобные социально-технологические модели, которые многие современные эксперты считают утопиями? Авторитетные специалисты в различных областях современной науки имеют различные мнения на этот счет, и с этими мнениями нам хотелось бы познакомить читателей.

Чего хотят криптоанархисты?

Существует множество людей, искренне верящих в то, что с развитием криптографии и информационных технологий сам собою наступит рай на земле. Кое-кто, наоборот, считает такую точку зрения инфантильной, полагая, что подобные надежды связаны с непониманием действующих в современном обществе социальных процессов, вследствие чего и рождаются всевозможные утопии. Чья точка зрения возьмет верх, покажет время, однако, прежде чем судить о возможных последствиях пришествия новой цифровой эпохи, необходимо разобраться в деталях исповедуемой криптоанархистами идеологии. Кроме того, было бы неплохо понять, кто такие криптоанархисты вообще и чем они отличаются от других обитателей мира компьютерных технологий.

В современной прессе отчего-то принято смешивать криптоанархистов, вирусописателей, программистов и хакеров воедино. Получается не слишком аппетитное, и, главное, несъедобное блюдо. В одной из публикаций на BBC:

«Если вас еще ни разу не взламывали, не “сливали” вашу личную переписку и не шантажировали краденными интимными фото, считайте, вам повезло. Наша жизнь, как личная, так и политическая, становится все более прозрачной, и деваться от этого некуда.

*Недавно вирус Petya.A атаковал компьютеры по всему миру, больше всего парализовав системы украинских ведомств. В последнее время хакеры все чаще взламываются в политическое поле – чего стоит история взлома баз данных комитета Демократической партии или “слив” документов Всемирного антидопингового агентства, целью которого было не вымогательство, а обнаружение общественно значимой информации. Это тренд, поддерживаемый в том числе деятельностью сайта Wikileaks, который пропагандирует максимальную гласность. Другой современный **тренд, провозглашающий всеобщую прозрачность – это технологии блокчейн, предлагающие людям проводить операции в криптовалюте.** Блокчейн подразумевает доступность всех данных о транзакциях и их неизменяемость, что гарантирует безопасность сделки. Но во что пытаются превратить наш мир стоящие за этим программисты? Как на политике и экономике отражаются технологические прорывы современности?»*

Как видим, этот «глас вопиющего в пустыне» не делает большой разницы между хакерами, распространителями вирусов и блокчейном. Вместе с тем разнообразие видов в мире высоких технологий намного шире того, что сумели вспомнить и перечислить авторы из BBC. Вот что говорит по этому поводу аналитик одной из ведущих российских антивирусных компаний Павел Шалин, пишущий под литературным псевдонимом Валентин Холмогоров:

«Всякий раз, когда в Интернете или традиционных СМИ я вижу новостные заголовки из разряда “Хакеры организовали очередную вирусную атаку” или “База данных интернет-магазина была похищена хакерами”, мне нестерпимо хочется отыскать написавшего это журналиста и стукнуть его по голове чем-нибудь тяжелым. Когда-то, работая редактором компьютерного журнала, я безжалостно вымарывал подобные строки из поступавших в издательство материалов. “Почему ты с таким упорством защищаешь хакеров?” – недоумевали коллеги. “Потому что они ни в чем не виноваты”, – всякий раз отвечал я.

*Истинное происхождение термина “хакер” сейчас, наверное, установить уже невозможно: предполагается, что оно зародилось в кампусах и аудиториях Массачусетского Технологического института еще в 60-х годах прошлого столетия. Бытует мнение, что словечко попало в обиход компьютерщиков из жаргона хиппи, где глагол *to hack* означал отнюдь не “взламывать”, как это считается сейчас, а “соображать”, “врубаться”. Собственно, в 70-х хакерами как раз и называли тех, кто “врубается” в принципы работы компьютеров, глубоко понимает происхо-*

дящие в них процессы – то есть высококвалифицированных IT-специалистов, программистов, разработчиков. Хакеры – это прежде всего исследователи, настоящие ученые из мира высоких технологий, те самые косматые парни в очках, сквозь толстые стекла которых можно поджигать муравьев. Настоящие хакеры никогда не взламывали чужие приложения или серверы ради наживы и уж тем более не совершали преступлений – разве что порой использовали свои знания для организации безобидных розыгрышей.

Говорят, один предприимчивый парень, сконструировав *bluebox* – устройство, позволявшее “обманывать” аппаратуру телефонных сетей, – однажды сумел дозвониться самому Папе Римскому. Порой хакеры использовали свои умения в личных целях, но все равно старались не наносить компьютерным системам и их пользователям серьезного вреда. По большому счету, хакерами можно назвать Стива Возняка и Билла Гейтса, Линуса Торвальдса и Ричарда Столлмана. Даже создатель первой в истории человечества электронно-вычислительной машины Конрад Цузе был своего рода хакером, хотя в его времена такого понятия не существовало вовсе.

Для парней, взламывающих программы или удаленные серверы с целью наживы, а также разрабатывающих различные средства обхода систем лицензионной защиты, всегда существовало отдельное название – крэкеры. Специалистов по взлому телефонных сетей принято называть фрикерами. Тех, кто использует в незаконных целях банковские карты и системы электронных платежей – кардерами. Отдельную категорию компьютерного андеграунда составляют вирусописатели, создающие и распространяющие вредоносное ПО. Эту разношерстную компанию также составляют многочисленные кланы, имеющие довольно-таки узкую специализацию: тех, кто пишет код, нередко называют вирмейкерами, так называемые крипторы упаковывают и шифруют вредоносные приложения, впариватели занимаются раздачей вирусов и троянцев населению, а ботоводы реализуют на черном рынке различные “услуги” с помощью принадлежащих им ботнетов, например, рассылку спама или DDoS-атаки. Существуют интернет-мошенники, выманивающие у доверчивых жертв деньги при помощи специально созданных сайтов или с использованием методов социальной инженерии. Такую деятельность нередко называют фродом, от английского термина *fraud* – “мошенничество”, а самих мошенников зовут фродерами. Жуликов, использующих личную информацию потенциальной жертвы в целях обмана или вымогательства, именуют скамерами, нередко они паразитируют на сайтах знакомств и промышляют в социальных сетях. Кто такие спамеры знает, наверное, каждый. Нередко злоумышленники используют хакерские методы для несанкционированного доступа к компьютерным системам. Но таких людей все-таки правильнее именовать киберпреступниками, считать их хакерами в классическом понимании этого слова – все равно, что называть системный блок ПК процессором. И неправильно, и раздражает.

Ну, а расхожее слово хакер, некогда обозначавшее просто высококлассного компьютерного специалиста, оказалось затерто до дыр не разбирающимися в вопросе журналистами, которые низвели IT-профессионалов до уровня компьютерных преступников и киберзлодеев. Масла в огонь подлили многочисленные онлайн-выдания, благодаря стараниям которых ныне хакером себя мнит любой школьник, купивший на “Горбушке” диск из серии “1000 программ для взлома Интернета”.

В мире существует множество IT-специалистов, которых можно назвать настоящими профессионалами своего дела. Это системные администраторы, поддерживающие целые кластеры серверов, это программисты, пишущие сложный код, это эксперты по информационной безопасности, архитекторы операционных систем, и, конечно, вирусные аналитики, исследующие опасные угрозы. И все они – немножко хакеры. Вот почему я отношусь к людям, которые заслужили право именоваться именно так, с большим и искренним уважением, ведь хакер – это звучит гордо».

Вместе с тем, с Валентином Холмогоровым солидарны далеко не все эксперты. В частности, в своем интервью Русской службе BBC автор книги The Politics of Bitcoin и доцент Университета содружества Виргинии Дэвид Голамбия озвучил несколько иное мнение. Приводим это интервью.

Голамбия видит в деятельности хакеров и культуре сливов наподобие тех, что осуществляет Wikileaks, не пользу для общества, где такие игроки нередко разоблачают преступления на государственном и других уровнях, – а наоборот, разрушение. Благородные идеи, которыми объясняют свои поступки люди вроде Эдварда Сноудена, считает Голамбия, на самом деле несут в себе зерно терроризма. А влиятельные IT-корпорации не только ограждают людей от вмешательства государства в их личную жизнь, а попутно ставят под угрозу суверенитет целых стран.

BBC: Ситуация ныне неоднозначная. У нас есть «Фейсбук», который соединяет два миллиарда людей, с его лайвами, которые вот-вот заменят телевидение; у нас есть сервисы вроде Skype, которые позволяют простым людям включаться в прямой эфир телеканала из автозак-ов во время массовых протестов; блокчейн, который подрывает существующую идею мировой экономики, Wikileaks как идеал радикальной гласности; у нас есть сквозное шифрование, которое вроде бы уберегает нас от «Большого брата» и одновременно – Большие данные, которые позволяют корпорациям узнать о нас больше, чем знаем о себе мы сами. Все это очень противоречиво и сбивает с толку, если честно. Как вы считаете, к чему же все это нас ведет?

Дэвид Голамбия: Куда все это ведет? Я об этом думал. Меня крайне беспокоят две группы людей, одну из которых прозвали криптоанархистами, а другую – киберпанками. Так они называли себя в конце 1980-х – начале 1990-х годов. И они существуют до сих пор.

Джулиан Ассанж, например, представитель как раз группировки киберпанков. Они написали дорожную карту будущего, которая поначалу казалась какой-то бредовой научной фантастикой с правым уклоном. Теперь она нам такой уже не кажется.

Биткойны, например, есть в этих ранних разработках киберпанков. Цель этих людей – подорвать все формы демократического правления с представительными структурами. Гораздо проще понять, что они хотят разрушить, чем то, что они хотят построить. Понятно, что они ненавидят, а вот что любят – не очень.

В 1994 году сотрудник Intel Тим Мэй написал «Шифрономикон» – сборник вопросов и ответов о криптоанархизме. Он основывался на более раннем «Манифесте криптоанархиста» также авторства Мэя. В «Шифрономиконе» уже прослеживаются идеи введения криптовалют и технологии блокчейна. Как мне видится (это похоже на то, что происходит сейчас с крайне правой политикой в отношении Интернета, что называют неофеодализмом, неореакционизмом), то, что эти люди строят – корпорации феодального типа, этикие феодальные анклав.

В этой системе люди **могут получить невероятную власть благодаря деньгам или приобретению самых совершенных технологий, переманиванию лучших программистов на свою сторону. И тогда мир окунется в перманентную войну, даже еще глубже, чем сейчас.** Томас Гоббс говорил о войне, которая столкнет всех со всеми. И это то, что, как мне кажется, происходит сейчас в мире. Эти люди заявляют, что борются именно с национальным государством, потому что оно провоцирует войны и прочие беды (и это так). Но то, что они предлагают взамен, еще хуже. Потому что это, если можно так выразиться, мир в перманентном состоянии терроризма, где любое существо – против любого другого существа. Без каких-либо всеобъемлющих политических структур.

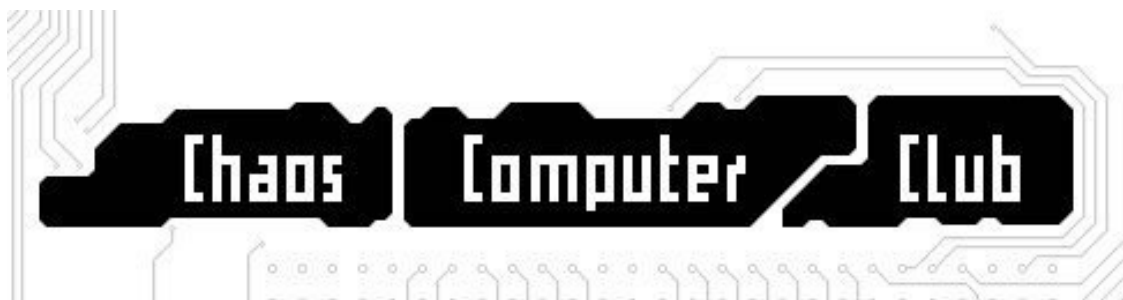
BBC: Вы пишете, что блокчейн – оплот правого экстремизма. Что вы имеете в виду под словом «экстремизм»? Именно вот этот терроризм, о котором сейчас сказали?

Д. Г.: Необязательно. Терроризм может происходить от разных политических сторон. Я это вижу стратегией, а не определенной политической точкой зрения. Понятно, что методы

этих групп жестокие. И есть некоторое сходство между тем праворадикальным насилием, которое мы видим в США, и тем, что есть в Европе или других местах. И, если честно, очень забавно наблюдать, как эти люди обсуждают [запрещенное в России] «Исламское государство». «Исламское государство» использует хитрые методы, все эти WhatsApp, Signal и так далее. Это потрясающий пример распространенного по большой территории, децентрализованного, неиерархического, негосударственного субъекта. Именно того типа, который восхваляют криптоанархисты. Это не выглядит, как свобода. Совсем не обязательно, что они поддерживают террористов, они даже могут себя нарочито от них отграничивать. *Но ведь на самом-то деле цель у них одна: отсутствие контроля и во многих случаях распространение хаоса, ярость по отношению к любому, кто им покажется заслуживающим того.*

ВВС: Вы назвали Джулиана Ассанжа, а кого бы еще вы причислили к таким людям? Марка Цукерберга?

Д. Г.: Нет, он не стоит на первом месте моего списка. В первую очередь я бы указал на людей вроде Джулиана Ассанжа, которые представляют себя мастерами криптографии, исследователями по кибербезопасности. Это члены Chaos Computer Club¹, которые посещают ежегодные хакерские конференции. Они все полны злости.



Как по мне – так они выглядят настоящими протофашистами. Даже одеваются так же. Они эстетизируют политику и прославляют абстрактное понятие свободы, которое, по моему мнению, не имеет ничего общего с тем понятием свободы, которое заложено в более вменяемых людях. И они, прежде всего, говорят о том, что хотят уничтожить, и мало что понимают о том, что хотят взамен.

ВВС: Вы наверняка слышали о недавнем взломе систем вирусом Petya.A? Вы сейчас говорите о хакерах, которые занимаются чем-то подобным?

Д. Г.: Именно. И надо быть готовыми, что такое будет происходить все чаще. Я не знаю, кто именно за этим стоит, возможно, мы никогда не узнаем. Но это и есть вот эта децентрализованная, неиерархическая, негосударственная... Хотя это вполне могло быть сделано руками государства, кто знает? Множество вовлеченных в это людей продают свои хакерские утилиты. Вот зайдите в так называемую глубокую паутину, где можно покупать разные вещи биткоинами и другой криптовалютой. Самым популярным товаром там являются как раз хакерские утилиты. И когда кто-то предлагает это ограничить, люди из криптомира начинают беситься. «Да как вы смеете ограничивать нашу свободу распространять инструменты для уничтожения чужого добра?» – говорят они. Так что я ждал: что-нибудь этакое произойдет, и жду продолжения.

ВВС: Как вы думаете, что правительства будут предпринимать на этот счет?

¹ Chaos Computer Club (CCC) – сообщество хакеров, основанное в 1981 году в Германии. Регулярно проводит международные съезды хакеров и выступает за доступность информации для всех. В 2013 году хакеры CCC смогли обойти дактилоскопическую защиту на iPhone 5s.

Д. Г.: Это, конечно, сложный вопрос. И я думаю, есть зависимость от размера этих стран. Более мелкие государства вообще рискуют потерять свой суверенитет. Знаете... хакеров и государство пытаются как-то разграничить... А на деле получается: первое, что делают правительства – нанимают хакеров. И эти хакеры становятся частью правительств.

Вот очень интересно: у нас в США многие ненавидят АНБ, ЦРУ и службы разведки, но вообще-то многие, кто работает внутри этих организаций, делают как раз хакерскую работу. Эдвард Сноуден тоже был частью этого мира – до того как обнародовал его секреты. В США сейчас такая ситуация: правительство «захватило» крупные корпорации. И это вообще-то совпадает со старым экономическим определением фашизма. И что происходит? У мелких государств, у которых нет таких ресурсов, как у США, «отъедают» суверенитет.

В то же время и в США корпорации «отъедают» внутреннюю власть у правительства. Я, конечно, не футуролог, не знаю, что будет дальше. Но я вижу, что вне США американские корпорации яро стараются перехватить ту силу и влияние, что есть у власти в этой стране.

Посмотрите на ООН. Там случайно оказались люди хакерского и корпоративного типа, которые работают над тем, чтобы подорвать власть в различных государствах под эгидой диджитал-свободы. Я не могу представить, чтобы хакеры могли свергнуть власть в США, Китае или России, или, возможно, даже в большинстве стран Евросоюза, но посмотрите на «брекзит» – это один из примеров активности хакерского типа, которая имела целью разорвать суверенную... странную, но суверенную сущность.

Другая тема, которая муссируется в СМИ сейчас, – это недоверие стран Евросоюза к Google. Компания в ответ тоже ненавидит ЕС, потому что он пытается регулировать ее деятельность. Что справедливо. И некоторые аргументы Google против этого совпадают с аргументами, которые хакеры приводят в защиту криптовалют и свободы в Интернете. Кто знает, общаются ли они вообще между собой напрямую? Но повестка состоит в том же самом – отвергать право Евросоюза противостоять политике корпораций. Они даже хотят влиять на законы. Суть борьбы между ЕС и Google еще и в том, что у ЕС гораздо более строгие правила относительно конфиденциальности данных, чем у США. И Google этого не выносит, говорит: «Да как вы смеете вырабатывать свой собственный режим конфиденциальности?!»

ВВС: Хотя если вспомнить историю с айфоном «филадельфийского стрелка», когда ФБР требовала у Apple разблокировать его устройство, а компания отказалась...

Д. Г.: Ну вот тогда хакерская община и движение за свободу Интернета, и корпоративное общество – они тогда встали все одной стеной. А что было-то? Был абсолютно законный ордер. Сноуден нам говорил об обысках без ордера, но тут-то был всего один законный ордер для одного человека. И если это – не обеспечение правопорядка, то что тогда?!

Конец ознакомительного фрагмента.

Текст предоставлен ООО «ЛитРес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на ЛитРес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.