Русская версия

Радикальное просвещение

Мир открытых источников А.Е. Фрейер

Радикальное просвещение - мир открытых источников (Введение)

Сейчас 20XX год. Люди носят на теле небольшие высокопроизводительные компьютеры, которые напрямую связаны с органами чувств и, соответственно, с мозгом с помощью датчиков, экранов и звуковых эффектов. Эти мозговые интерфейсы подключены к сети, которой управляет, контролирует и манипулирует конгломерат огромных технологических компаний. Вместе с военными, правоохранительными органами и коррумпированной правящей элитой отдельных регионов все мысли, события, разговоры и передвижения людей записываются, анализируются, манипулируются и снова используются против них.

Мощные нейронные сети создают точные профили каждого человека, которые затем передаются столь же мощным алгоритмам и направляют людей туда, куда они должны идти. Война, бедность, эпидемии представляются людям как их собственный выбор или, по крайней мере, как неизбежная судьба, безжалостно навязанная великим, темным, неизвестным существом. Большая часть населения полностью подчинилась алгоритму и его хозяевам, защищает его власть, говорит на его языке и отдает честь каждые 40 секунд или около того, подключая интерфейс к своей голове.

Гражданское общество, столь мощное в прошлом веке, практически распалось. Пресса, журналисты и интеллигенция (также важные столпы свободного общества не так давно) открыто подчиняются кампаниям. Поиск истины считается ложным и разрушительным. Поиск истины должен быть остановлен. Время от времени находились люди, которые разоблачали новую логику и показывали, что в конце концов это всего лишь дело рук человека и что ее можно изменить. Все эти люди сейчас находятся в тюрьме в бегах или в безумии. Все эти люди были практически казнены на глазах у публики.

Центры власти становятся все меньше и меньше, но все мощнее и мощнее. 1% населения планеты владеет всем. Остальные получают подачки. Но в основном даже не это. 9 миллионов человек ежегодно умирают от голода, в то время как другие ежедневно имеют в своем распоряжении зарплату, в миллионы раз превышающую зарплату среднего рабочего. Среди лишенных собственности 99% идет беспощадная борьба за выживание, характеризующаяся в основном ненавистью и презрением. Политическая мысль и действия уступили место бесполезной борьбе за пустяки, безвредные для правителей. Предпочтения

в потреблении или разногласия в повседневном языке создают непримиримые лагеря, которые никогда не перестанут бороться друг с другом. И они ссорятся из-за НИЧЕГО, вообще ни из-за чего.

Ужасная антиутопия, не так ли? Как это могло произойти? Как мы могли так далеко отойти от идеалов Просвещения? И можем ли мы что-нибудь с этим сделать?

Да, мы можем

Радикальное Просвещение - мир открытых источников

Конец Просвещения?

В XIX и XX веках было принято считать, что ход мира и судьбы человеческих обществ развиваются исторически. То есть предполагалось, что всегда существует прогрессия и что все постоянно развивается к лучшему. Даже в позднебуржуазных государствах после Второй мировой войны предполагалось, что следующему поколению когда-нибудь будет легче. Предполагалось, что детям будет лучше.

С одной стороны, эта идея была вызвана огромным ростом знаний благодаря все более совершенным наукам. (Чарльз Дарвин и его открытие происхождения видов, безусловно, должны быть упомянуты в этом контексте). А также популяризация исторического наблюдения в гуманитарных науках через Гегеля и позже Маркса.

Поэтому знания, этика и политика развивались не благодаря божественному провидению или просветленным вспышкам разума нескольких одаренных избранных, а в результате совместных усилий человечества. Знания и опыт передавались из поколения в поколение, подвергались сомнению, сбивались с пути и освобождались от аберраций. Идея была позитивной. Хотя это развитие отнюдь не было линейным, оно казалось законом, и можно было ожидать постоянного совершенствования людей и человеческих обществ.

Все более быстрый рост индустриализации и сопутствующее ускорение знаний в области физики, очевидно, могут сотворить чудеса. Все больше тяжелой и неприятной работы выполняли машины, электрический ток, самодвижущиеся транспортные средства, передача информации, изображения и звука на тысячи километров предвещали славное будущее.

Но все это не осталось бесспорным. Если все должно быть представлено детерминистически, эмпирически и предсказуемо, то Бога нет. Религии, естественно, отвергают исторический взгляд на мир, поскольку они обычно предполагают, что существует перводвигатель, создатель мира, или, по крайней мере, что все происходит в цикле, круговороте. С этой точки зрения, изменения могут быть лишь поверхностными и тривиальными, поскольку в конечном итоге все сливается обратно в Единое, в исток.

Существовали (и существуют) также реакционные силы. Они отвергают продвижение по службе, в основном по личным причинам, поскольку это влечет за собой потерю власти, собственности, наследственных дворянских прав и т.п. Или они хотят верить, что определенные группы (их собственные) имеют древние права на определенную землю или

право на существование вообще.

Просвещение, основа любого буржуазного общества (и на которой основываются другие модели общества, такие как коммунизм), в своей основе является глубоко историческим и материалистическим событием. В 19 и 20 веках Просвещение и Французская революция казались необратимыми событиями. Но в 21 веке уверенность рушится.

Прогресс больше не кажется обещанием спасения. Разрушение окружающей среды и стремительный рост неравенства, смертельная нищета, голод и миграция являются непреложными константами современного мирового сообщества. Предупреждение Гюнтера Андерса(1) о том, что человечество обгоняет его собственная технологическая революция, уже давно перестало быть причудливым сюжетом для дешевых научно-фантастических романов.

Благодаря специализации и экспертизе, цифровизация, которая изменила жизнь каждого за очень короткое время (я не думаю, что можно ошибиться, если отнести начало цифровизации к 2000 году с основанием Google), стала мифическим монстром, непостижимым для человека.

Цифровизация, которая на 100 процентов состоит из эмпирических, рациональных математических расчетов, похоже, стала идолом богов. Произвольный, непредсказуемый(!) и жестокий. Но если это только дело рук человека, если это только поддается расчету, то это не может быть спасением великих мыслей Просвещения. Возможно, "свобода, равенство и братство" все-таки существуют? Может быть, в конце концов, все обернется к лучшему?

> (1) Гюнтер Андерс "Древность человека". Том I: О душе в эпоху второй промышленной революции. С. Х. Бек, Мюнхен 1956

Достояние и капитал

Одним из главных отличий буржуазной эпохи от всех предыдущих является капитал. Это означает частную собственность на общие товары и идеи. Средства производства, земля, патенты, а возможно, и человеческий труд принадлежат отдельным частным лицам, которые преследуют с их помощью свои частные интересы. Создается класс капиталистов, и поэтому эта форма общества также называется капитализмом. Либеральная идея заключается в том, что это приводит к постоянной конкуренции индивидуальных интересов и эгоизмов, которые в конечном итоге создают что-то хорошее и правильное для всех.

Если в идеализированном, романтическом мире Адама Смита, возможно, еще можно так думать, поскольку там у всех одинаковая стартовая позиция, то в реальном мире быстро становится очевидным, что происходит накопление капитала. Условия отнюдь не одинаковы. Там, где находится капитал, будет накапливаться еще больше капитала. Возникают централизованные структуры, монополии, империи, элиты. Капитализм переходит в империализм. Социальное насилие приватизируется, а другие цели буржуазной

революции, такие как равенство или демократия, не могут возникнуть или существуют и становятся невозможными. Буржуазное общество упраздняет само себя.

Это, как мы знаем, по крайней мере, со времен Розы Люксембург (2), не печальное извращение, с которым можно бороться, но накопление капитала и централизация власти имманентны обществу, основанному на частной собственности, и происходят неизбежно.

Крайние эксцессы можно наблюдать в позднебуржуазных обществах последних десятилетий. Согласно концепции неолиберализма, разработанной в 1940-х годах, все, так сказать, приватизируется. Мысли, чувства, коммунальная инфраструктура, политика и политики, война и мир. С приходом цифровизации и полной приватизации сегодня нет места, которое не принадлежало бы другим, не было бы полностью отчуждено от нас.

С другой стороны, существует так называемое общее достояние, несколько расплывчатый термин (который, к сожалению, также трудно перевести на немецкий язык, поскольку больше всего подходит слово "Allgemeingut", которое, однако, относится только к товарам). Общность означает "то, что принадлежит всем". Классическим примером является ландшафт. Пейзаж всегда принадлежит всем, потому что даже если земля принадлежит определенному человеку, пейзаж всегда принадлежит тому, кто на него смотрит.

В нашем неолиберальном мире все общее постепенно приватизируется и, следовательно, по определению является украденным. Одним из экстремальных примеров является операционная система. Операционная система, т.е. программное обеспечение, которое делает компьютер пригодным для использования, является одним из величайших достижений человечества; ни одна компания, и уж тем более ни один человек, не создали ее и не имеют права продавать ее.

Однако, как известно, это делается, как и многие другие продукты, мысли, знания, созданные человечеством, нагло продаются обратно людям, хотя давно уже принадлежат им.

Как бы печально ни выглядела ситуация на данный момент, она также открыто показывает, как мы можем ее преодолеть. Мы должны умудриться перевести капитал обратно, или впервые перевести его в общее пользование. Эта идея не нова: "Средства производства в руки рабочих". "Дома, принадлежат тем, кто в них живет" и т.д. Это можно сделать только силой. Но цифровизация открывает перед нами совершенно новые возможности. Цифровизация открывает перед нами возможность вернуть или впервые передать ценности общества и участие в нем в руки тех, кто является обществом - нас, людей.

Идея для этого, и она проста и радикальна, пришла из разработки программного обеспечения. Это идея открытых источников!

(2) Роза Люксембург - Накопление капитала. Вклад в экономическое объяснение империализма. Бухгалтерия Пауля Зингера, Берлин, 1913 г.

Интеллект масс

В ходе стремительного развития индустриализации в 19 веке возникло новое явление. Невиданное в истории человечества изменение - появление масс. Центр культурной и, прежде всего, экономической жизни переместился из сельской местности в город. От социальной общности, формировавшейся веками в деревне или маленьком городе, до безымянных массовых кварталов рабочего класса во все более огромных и доминирующих промышленных и крупных городах.

Это коренным образом изменило общество. Классовые отношения изменились: от крестьян и господ к армии рабочих, пролетариям, и тем, кто заставляет рабочих работать на них, - владельцам фабрик и капиталистам. Таким образом, массы являются политическими акторами. 20 век показал, что массы могут играть весьма амбивалентную роль. С одной стороны, тотальные войны и невероятные зверства были совершены во имя народа, общины или собственной группы; с другой стороны, это привело в движение огромную демократизацию и разрушение структур правления.

Сегодня мы живем в массовом обществе, со всеми его преимуществами и недостатками, нравится нам это или нет. Любая правящая структура, если она хочет сохранить власть, должна контролировать массы. Помимо прямого насилия или материальной зависимости, это происходит в основном через средства массовой информации. Если радио уже сыграло немаловажную роль в мобилизации народа во время Второй мировой войны, то сегодня свою роль играют телевидение и, в решающей степени, Интернет.

Интернет (в самом широком смысле) сегодня является самым важным действующим лицом, когда речь идет о принятии решения или о том, чтобы его подтолкнули к принятию решения. Она может заставить людей любить определенные товары и бренды или ненавидеть определенные группы, она решает вопросы войны и мира. В том, что мы сейчас называем интернетом, доминирует горстка гигантских технологических корпораций, которые лишь беззастенчиво скрывают свою связь с военными и властью, если вообще скрывают.

На первый взгляд, сегодня не составляет труда направлять людей и манипулировать ими. Массы кажутся глупыми и апатичными, в лучшем случае способными объединиться в толпу. Но если присмотреться внимательнее, то можно увидеть явление, которое почти всегда происходит, когда люди и культуры объединены в сеть: обмен знаниями, умножение знаний, интеллект масс.

Сколько плиток было уложено и сколько носков было связано, благодаря видеороликам с инструкциями из WWW? Сколько вопросов было решено и организовано проектов? Знания отдельных людей в совокупности почти бесконечны, по крайней мере, что касается нашего маленького мира на нашей маленькой круглой Земле. Такое сочетание знаний человечества невероятно мощно и, помимо правильной укладки плитки, дает возможность реального освобождения и расширения собственных возможностей.

Этого нельзя добиться, если эти знания находятся в руках нескольких вышеупомянутых корпораций, и они могут отказывать, препятствовать или манипулировать доступом по

своему усмотрению. Это знание раскрывает свою силу через свободный, неограниченный доступ для всех людей и через динамику, которая возникает из-за того, что это знание может быть изменено, объединено и переговорено по желанию.

Чтобы гарантировать это, нужны открытые источники. Они гарантируют постоянную доступность и постоянную прозрачность в отношении того, как изменился источник и каково его происхождение. Открытые источники - это радикальная идея.

Свобода - наше высшее благо?

Декарта, Спинозу, Руссо, Канта и всех других великих мыслителей и философов европейского Просвещения объединяет один общий (и потому центральный для мысли Просвещения) принцип: самоопределение человека. У человека есть "естественное право", право человека, которое, так сказать, заложено в его колыбели. Человек рождается со свободной волей и, таким образом, имеет естественное право принимать собственные решения и решать за себя.

Кант в своем эссе "Ответ на вопрос: что такое просвещение?" (3) подытожил идею просвещения словами: "Имейте мужество пользоваться своим собственным разумом". вместе. Идея независимости от церкви, властей и монархов с тех пор является центральным компонентом каждого современного буржуазного общества.

В отличие от современности, которая является чисто социальным, европейским продуктом, Просвещение представляется процессом универсальной эмансипации, присущей всему человечеству. Свобода не подлежит обсуждению. Свобода - это право человека.

В отличие от свободы, незрелость не является законом природы; незрелость нужно приобрести. С древности мыслящие люди задавали себе вопрос, почему возможно, что немногие всегда могут возвыситься над многими и навязать им свою волю. Многим было бы легко отправить монарха или лорда в отставку.

Помимо апатии, людей всегда держит в рабстве страх. Страх перед неизвестным, страх перед врагом, перед болезнями, чумой, Богом или демонами. Все эти страхи антипросветительские, потому что они всегда направлены на иррациональное ядро. Европейское Просвещение противопоставило иррационализму эмпирическое, рациональное мышление, которое может описать все узнаваемые явления на земле как последовательность причин и следствий. Это означает, что все в конечном итоге становится исследуемым, категоризуемым и, следовательно, объяснимым. Страху там нет места, он может быть только частью индивидуального опыта, но не иметь универсально обоснованного статуса.

Рационализм, как показано выше, отнюдь не является бесспорным. Но все наши современные высокотехнологичные индустриальные общества основаны на знании того, что у каждого следствия есть причина.

Но так ли это в наше время? Желательно ли, чтобы человек мог свободно принимать решения? Перед лицом угроз наступающей эпохи? Перед лицом глобального потепления, эпидемий и неуправляемых конфликтов? Разве дуализм эпохи до эпохи Просвещения, четкое разделение на добро и зло не лучше подходит для решения проблем будущего, чем свобода воли, которая в конечном итоге приведет нас к гибели?

Такой взгляд на мир очень распространен в начале 21 века. Ницше не без оснований называет ее рабской моралью. Простой моральный детерминизм, который может объяснить мир с помощью простой концепции добра/зла, в любом случае реакционен. Многие из современных сторонников этого идеологического дуализма считают себя вовсе не частью реакции, а пионерами неизвестного будущего. Важно отметить, что эта идеология включает в себя миф о новом начале и конце истории. Последовательно дуалистическое, знание человечества классифицируется как "традиционное знание" и изображается как устаревшее и неспособное противостоять будущему. Вопрос о том, должны ли дети в Германии по-прежнему читать "Фауста" Гете в школе, уже задавался.

Если задуматься на мгновение, то легко заметить, что такое мышление призывает к концу разума и заставит покраснеть от стыда даже любого иррационального религиозного идеалиста.

Почему история больше не должна применяться, особенно сейчас, когда мир сталкивается с огромными вызовами? Вернулся ли Иисус? Сбылось ли пророчество майя? Почему незрелость и конформизм должны быть гарантами решения беспрецедентных социальных изменений именно сейчас? Не важнее ли сегодня подвергать все сомнению и приходить к самостоятельному суждению?

Благодаря Гегелю мы получили прекрасный (хотя, по общему признанию, трудный в использовании) инструмент для описания мира в его противоречивой и запутанной совокупности. Диалектика. Это наше сокровище, наше огромное преимущество. Мы никогда не должны отказываться от этого. Особенно не для каменного века, техно-гностического дуализма а-ля Силиконовая долина, который рано сообщает нам через смартфон, что сегодня является добром или злом. Долой незрелость, долой свободу!

"Имейте мужество использовать свой собственный разум".

> (3) Иммануил Кант: ответ на вопрос: что такое Просвещение? В: Berlinische Monatsschrift, 1784 г.

Диалектика свободы

Итак, если свобода - это наше высшее благо, и мы не можем обойтись без нее, не отказавшись от своего существования как человеческих существ, как нам быть с этим? Свобода также означает опасность.

В этом и заключается запутанная двойственность, присущая свободе. Если мы не можем ограничить свободу, не потеряв ее, но как люди мы не можем жить без договора, который ставит на место закона сильнейшего и предотвращает произвол и самосуд, то что мы можем сделать, чтобы разрешить этот парадокс свободы?

Со времен Аристотеля существует рациональный, научный метод, позволяющий человечеству жить не в незрелости и не в произволе. Этика. В отличие от морали, которая является собственным отрицанием и описывает состояние другого, презренного, как безнравственность, этика - это научное изучение привычек, обычаев и практики.

Еще досократовские софисты считали недопустимым, чтобы люди, будучи разумными существами, наделенными свободной волей, руководствовались только традициями, условностями и сводами правил.

Аристотель возводит это в ранг науки, которая позволяет нам рационально, эмпирически разрабатывать и неоднократно заключать общественный договор. Этика предполагает, что человек в основе своей рационален и способен к рефлексии. В противном случае он никогда бы не смог покинуть царство наивной чувственности и мистицизма и, подобно животному, оказался бы во власти своих влечений и инстинктов.

Основой этики является добродетель. Вопреки утверждениям в откровениях и деспотизме, не существует трансцендентных правил, установленных перед человеческим разумом. 10 заповедей Моисея противоречат всей науке и являются неэтичными. Не в их содержании, так как это подлежит обсуждению, а в их Богом данной неизменности.

Конституции, которые мы сегодня считаем основой современного просвещенного общества, появились не по милости Божьей и не благодаря мозговой волне одного человека. За них боролись и договаривались в ходе исторического процесса. Наша совместная жизнь является результатом этого этического процесса.

Но что это означает для глобализированного, цифрового мира, переживающего переходный период? Мир, в котором национальные государства больше не играют роли (даже если все в панике цепляются за них), в котором исчезают языковые барьеры и происходит постоянное общение в режиме реального времени?

Однозначно можно сказать, что происходят радикальные изменения. Что старые правила, законы и конституции, старый общественный договор должны быть перезаключены. Поэтому этика - это наука часа!

Марксисты в 19 веке уже пытались создать всемирную этику. Они назвали это интернационализмом - словом, в названии которого уже присутствует национализм. В 21 веке ситуация иная, произвольные границы растворяются, возникает реальное мировое сообщество.

И для того, чтобы овладеть этим, чтобы развить мировую этику, нам нужны инструменты, которые позволят нам это сделать. Они должны быть, в марксистском смысле, инструментами расширения прав и возможностей. Цифровые структуры не должны находиться в руках отдельных лиц, компаний или государств. Структура должна быть свободной.

То, что для цифровизации необходимо создать этическую основу, было ясно умным, рациональным людям с самого начала. В основе информационной эпохи и цифровой трансформации лежит программное обеспечение. Наряду с проприетарными системами и программами, которые до сих пор доминируют, рано появилось программное обеспечение с открытым исходным кодом. Программное обеспечение, которое никому не принадлежит, которое может развиваться всеми, которое гарантирует полную свободу и идеально подходит в качестве этического инструмента нового общества.

Поэтому программное обеспечение с открытым исходным кодом - это не технический, а этический, политический феномен. Структура для нашего будущего.

Структура власти

Что же стоит на пути к созданию глобальной этики? Почему человечество не стремится к созданию государства, в котором все люди могут жить безопасно, свободно и самоопределяться?

Помимо осознания того, что такого состояния трудно или даже невозможно достичь, и, как следствие, недостатка смелости, чтобы решиться сделать этот шаг в неизвестность, на пути такого шага стоят, прежде всего, структуры собственности и, следовательно, структуры власти.

В начале 21 века мы живем в позднекапиталистическом обществе. Как и во всех капиталистических обществах, существует четкое разделение властных отношений. Существует класс собственников, владеющий средствами производства и, таким образом, контролирующий все социальные структуры, такие как государство, армия, полиция, СМИ, инфраструктура и так далее. С другой стороны, существует класс, лишенный собственности в том смысле, что он не владеет средствами производства, что он может только "работать" на пользу прибавочной стоимости другого и тем самым отстранен от прибыли, смысла и успеха собственного процесса труда.

Так что классовое общество все еще существует. Если посмотреть на глобальные условия, то армию рабов и пролетариев (т.е. людей, которым больше нечем заняться, кроме как воспроизводить себя) нельзя не заметить. Но даже в богатых индустриальных обществах разделение на имущих и неимущих явно сохраняется, хотя и часто скрывается под напускной строгостью и привилегиями.

Решающим моментом является изменение отношений собственности и освобождение средств общественного производства из рук немногих. Классические пролетарские

движения последних двух веков были убеждены, что существует некое историческое право, что теперь эта власть должна быть передана в руки рабочих.

Но сейчас мы стоим на пороге полностью цифровизированного мирового сообщества. Но это также означает, что средства производства, которые до сих пор составляли основу властных структур этого общества, также переходят в цифровой формат. Материальные предпосылки любого производства (инструменты, машины, заводы) теперь неразрывно связаны с виртуальным пространством. Пространство, которое теоретически бесконечно делимо и бесконечно воспроизводимо, и хотя оно основано на материальных предпосылках, само не постижимо как материя.

Одна из основных идей общества с открытым исходным кодом заключается в том, что виртуальное пространство настолько тесно связано с механическим миром производства, что в некотором смысле создается новый инструмент. Виртуальная, цифровая часть инструмента доминирует над материальной. Таким образом, если бы было возможно поместить властные отношения в цифровом пространстве в совершенно новые контексты, это изменило бы и материальные властные отношения.

Решающим фактором здесь является то, что эта власть не должна быть передана в новые руки, но должна быть пригодной для использования, изменяемой и многократно используемой в качестве открытого источника для всех.

В случае с программным обеспечением существует следующее определение открытого источника(4):

- Программное обеспечение (т.е. исходный код) доступно в форме, читаемой и понятной для человека
- Программное обеспечение можно копировать, распространять и использовать по своему усмотрению
- Программное обеспечение может быть изменено и передано в измененном виде

В применении к нашим реальным отношениям власти в цифровом мире это означает: инструменты власти, то есть средства производства, могут быть использованы и изменены кем угодно и для каких угодно целей. Единственным условием является то, что измененные инструменты, в свою очередь, могут свободно использоваться и изменяться. Быстро становится очевидным, что это определение является бессмыслицей в классическом, материальном мире. Ситуация меняется, если предположить, что материя и виртуальное пространство сливаются неразрывно. Тогда эти три, сами по себе не впечатляющие, требования являются социальной взрывчаткой.

Продуманный до конца, этот процесс обещает как субъективную индивидуальную свободу, так и, благодаря постоянной обратной связи, полноценное участие в социальном процессе как таковом.

(4) Источник -Википедия "Определение инициативы "Открытый исходный код"" - https://de.wikipedia.org/wiki/Open_Source

Вилы этики

Как этический и, следовательно, научный пересмотр (мирового) общественного договора может быть возможен в цифровом мире с открытым исходным кодом?

Диалектика учит нас, что не существует единой трансцендентной истины априори. Цивилизация и люди формируются под влиянием амбивалентности и противоречивого опыта, предпосылок и причинно-следственных связей. Они характеризуются истинами, которые являются взаимоисключающими. Чтобы разрешить этот парадокс, человечество в классической древности, как показано выше, создало этику как рациональный инструмент для того, чтобы снова и снова договариваться об этих противоречиях.

В разработке программного обеспечения с открытым исходным кодом (и только в нем) существует процесс форкинга. Создание форка означает создание форка программы. Это простой и скучный процесс контроля версий, который должен гарантировать, что над идентичной базовой программой можно работать в разных, независимых направлениях.

Это означает, что любой человек может совершенно свободно копировать любую программу с открытым исходным кодом и развивать ее в соответствии со своими способностями и интересами. С помощью так называемого форка можно не только использовать знания, которые до этого момента вливались в исходную программу, но и перенять будущие изменения и улучшения исходной программы в свой собственный проект. Также создается процесс обратной связи, который, в свою очередь, может интегрировать инновации побочных предприятий в первоначальную программу.

Можно представить, например, что программа для управления лампочками может быть использована в вилке для управления электродвигателями, а вилки этой программы, в свою очередь, могут быть использованы в робототехнике или при эксплуатации плотин и так далее.

Этот процесс, который на первый взгляд кажется техническим, при ближайшем рассмотрении оказывается чрезвычайно сложной и, как процесс, высокоэффективной формой коммуникации. Вид коммуникации, играющий огромную роль в историческом ходе человеческой истории и обладающий огромной силой благодаря оцифровке и знаниям, полученным при работе с открытыми источниками.

Таким образом, принцип форкинга в разработке программного обеспечения с открытым исходным кодом является эффективным, документированным и научным инструментом для отображения этого процесса коммуникации. В сочетании с дигитализацией эта коммуникация происходит в режиме реального времени и, таким образом, позволяет

постоянно пересматривать, изменять и корректировать, не отказываясь от установленных и уже согласованных характеристик.

Чтобы создать этот мощный инструмент для переговоров о будущей этике, необходима структура, которая была бы полностью свободной. Если серьезно относиться к диалектике, то невозможно осуществить такой процесс без противоречий и конфликтов. Ошибки и отклонения также являются частью человеческой природы. Поэтому ошибки и конфликты должны быть возможны и приниматься без угрозы для реального процесса.

Благодаря вышеупомянутым принципам движения open source и инструменту форков и форкинга в цифровом пространстве, в нашем распоряжении уже есть мощные инструменты для того, чтобы освоить этические переговоры.

Завоевание частной жизни

В своем общественном договоре Кант видит разделение разума на частный и общественный. Частный разум - это тот разум, который мы можем использовать в "офисе", т.е. разум, на который наложены сильные ограничения и соблюдение которых необходимо для беспрепятственного успеха. С другой стороны, общественный разум - это разум "ученого". Это, по словам Канта, должно быть свободным и позволять подвергать сомнению и выражать все.

Помимо разума на публике, существует также сфера абсолютной приватности. То есть, сфера семьи, друзей или собственного "я". В древности это называлось ойкос, домашнее хозяйство. До тех пор, пока эта область не затрагивает публичную сферу, например, не нарушает никаких общепринятых законов, там все разрешено, и переговоры ведутся в самом ойкосе. Не зря там располагается сексуальность и другие вещи, которые могли бы стать причиной "общественного неудобства".

Но что происходит в цифровом обществе, где вековые границы между этими сферами растворились практически в одночасье? Это растворение происходит, с одной стороны, благодаря постоянной самопубликации в режиме реального времени в так называемых "социальных медиа". И, во-вторых, что гораздо серьезнее, через технически возможное и реальное тотальное наблюдение и запись всех событий, происходящих в цифровом пространстве.

Поскольку мы живем в полностью оцифрованном мире, все сферы жизни также находят свое отображение в нем. Неважно, идет ли речь о частной сфере ойкоса или о публичном созерцании социальной проблемы. Итак, если все записывается публично и, как всем известно сегодня(5), постоянно, это означает полное упразднение частной жизни, приватной сферы, ойкоса.

Это фатально. Хотя общественный и частный разум, как и во все времена, должны быть пересмотрены, ликвидация частной жизни является цезурой в истории человечества и до этого момента считалась инструментом пыток паноптикона в исправительных учреждениях

и тюрьмах.

Однако частная жизнь и частная сфера неразрывно связаны с социальной и индивидуальной свободой, а также с достойной жизнью в целом. Таким образом, отвоевание приватности является решающей борьбой в начале всеохватывающей дигитализации, которая больше не оставляет аналогового пространства.

Но как это можно сделать? В области безопасности программного обеспечения существует концепция военизированного и демилитаризованного домена. Предполагается, что каждое устройство и каждая программа, связанные с всемирной сетью, всегда подвергаются (или могут подвергаться) атакам, чтению, компрометации и манипуляциям. Поэтому все, что происходит в интернете, в цифровом пространстве, происходит в милитаризованной зоне и, по определению, подвергается постоянным атакам.

Ответ на вопрос о том, как обеспечить приватность в цифровом пространстве, логично вытекает из военной традиции. Это криптография. С самого начала военных конфликтов человечество пыталось изменить важные сообщения так, чтобы противник не смог их оценить.

Поскольку все в Интернете потенциально может контролироваться "врагом" (в данном случае врагом приватности), поэтому необходимо срочно шифровать и криптографировать все, что является приватным, независимо от того, насколько это неинтересно и тривиально. Таким образом, создание полностью всеобъемлющей криптографии частной сферы является одной из важнейших задач человечества в новую эпоху.

Помимо задачи донести до людей эту информацию и реализовать ее, одна из самых больших трудностей заключается в том, что для шифрования и дешифрования необходимы криптографические инструменты. Они не могут находиться в руках отдельных лиц или групп, но должны быть бесплатными и доступными в виде открытого источника. Сам криптографический инструмент не должен содержать никаких секретов. Секрет шифрования, ключ, должен находиться в руках человека, подобно ключу, которым он запирает дверь своей квартиры, прежде чем приступить к реализации личных предпочтений.

> (5) Постоянная запись (2019) Эдвард Сноуден ISBN 9781529035650.

Демократия - лучшая из всех систем?

Цифровизация - это глобальное явление, поэтому она обладает потенциалом для создания настоящего, равноправного мирового сообщества. Сегодня легко можно общаться в режиме реального времени практически с любым человеком в любой точке мира. Языковые барьеры легко преодолеваются с помощью программного обеспечения, может возникнуть мировой язык, состоящий из всех известных языков, который может быть совершенно свободным и независимым, и при этом каждый человек сможет без труда понимать язык любого другого

человека. Это было бы больше, чем интернационализм коммунистов, это сделало бы возможным мировое сообщество, мировое общество.

Это явление уже сегодня является вездесущим. Это вызывает столь же экстремальное встречное движение, реакцию. Во всем мире можно наблюдать рецидив национализма. Национализм как идеология, а именно об этом мы здесь говорим, заканчивается варварством, как мы знаем из европейской истории. Власть имущие реагируют на безудержный поток информации, присущий цифровизации, беспомощной цензурой и манипулированием информацией. (Это относится и к некогда буржуазным, либеральным государствам, которые до этого времени хотя бы сохраняли видимость уважения к свободе слова).

Какими бы угнетающими ни были национализм, цензура и произвол, какой бы сильной ни была эта реакция, в полностью глобализованном и цифровом мире эти явления не смогут играть роль в долгосрочной перспективе. Даже сейчас, в начале этого нового развития, они кажутся беспомощными и жалкими, но от этого еще более опасными.

Но если возможно создать мировое сообщество, то как могла бы выглядеть политическая система, отвечающая этим требованиям? В классической политике (т.е. науке о совместной жизни) и в политической философии часто разделяют идеальную систему и ту, которая была бы осуществима в реальных условиях.

В античности и вплоть до раннего нового времени мыслимые формы общества обычно представлялись как группа из шести с тремя хорошими и тремя плохими формами. Хорошие формы - это в основном монархия как правление одного, но хорошего, аристократия как правление немногих, но способных, полития как правление многих, но достойных. Плохие формы - это, в основном, демократия как правление народа и, следовательно, бедных, олигархия как правление немногих богатых и тирания как правление деспота, тирана.

В наше время вежливость постепенно трансформируется в гораздо более сложный либерализм или представительную демократию, которая равносильна государственному правлению. Классическая демократия превращается в коммунизм, диктатуру пролетариата. После эпохи Просвещения и появления индивида как политического актора возникла еще одна мыслимая политическая форма - анархизм. Если в античности анархия была просто отсутствием государства, то есть небытием сообщества, то с появлением прав человека она стала пониматься как естественное право и суверенная личность, как правление этой самой личности на благо всех.

Уже Цицерон признавал, что чистое правило 6 форм, описанных выше, никогда не будет справедливо для сложного общества, и что отдельные формы всегда движутся по нисходящей, к худшему и к нестабильности. Таким образом, он предложил связь всех форм, что можно интерпретировать как раннюю форму диалектического подхода.

Сейчас в политике нет морального дуализма, который мог бы легко отличить хорошие формы общества от плохих. В очень сложном современном обществе, а тем более в мировом сообществе, существует так много законных индивидуальных интересов и принципиально различных исходных ситуаций, что становится невозможным создать систему, которая

могла бы все это реализовать. Единственная возможность, которая существует, - это последовательное применение диалектического подхода.

Поскольку невозможно объединить противоречия, они должны быть приняты как противоречия. В диалектике существует три ступени: тезис, антитезис и синтез. В этом процессе противоречивые части, тезис и антитезис, растворяются в синтезе. Как этот синтез может быть успешным в очень сложном мире - это вызов человечеству. Там, и особенно там, оцифровка открытых источников может принести нам огромную пользу. ☰ Меню

Программное обеспечение и открытые источники

Если мы предположим, как мы это делаем здесь, что весь мир и все сферы общества уже оцифрованы или будут оцифрованы, то на первый план выходит культурное достижение человечества: программное обеспечение. Поэтому программное обеспечение и языки программирования больше не являются простым побочным продуктом новой технологии, а составляют основу и фундамент этого нового оцифрованного мира.

Языки программирования - это искусные информационные инструменты, которые по сложности и содержанию ни в чем не уступают классическим языкам высокого уровня. Все, что мы сегодня называем цифровизацией или интернетом, основано на программном обеспечении. Каждое приложение, каждый веб-сайт, каждое управление машиной, управление атомной электростанцией, просто все, что так или иначе является цифровым (а в цифровом обществе это все), управляется через программное обеспечение, то есть через письменный документ, созданный людьми. В некотором смысле, это литература в совершенно новом смысле.

Когда вы осознаете это, становится ясно, что это инструмент власти, если не инструмент власти новой эпохи. Программное обеспечение может изменять, манипулировать, удалять и создавать основу информационного общества, то есть информацию, по своему желанию. С одной стороны, это его задача, с другой стороны, это оставляет огромное пространство для всевозможных злоупотреблений.

Таким образом, возникает вопрос: как добиться того, чтобы люди, несмотря на различные предпосылки и способности, могли стать владельцами программного обеспечения, которое они используют и должны использовать? Ответ заключается в том, что это программное обеспечение должно децентрализоваться до такой степени, чтобы в конечном итоге оно не принадлежало никому, или, положительно, чтобы оно принадлежало всем.

Этот принцип звучит довольно абстрактно и неисполнимо. Но есть удивительно простая логика, которая может заставить это работать. И это, как и следовало ожидать, программное обеспечение с открытым исходным кодом. Поэтому не все приложения с открытым исходным кодом одинаково эмансипативны, но структура, лежащая в их основе, мощна и способна достичь этой цели.

В начале 21 века актуальность структур с открытым исходным кодом не признается. Открытое программное обеспечение считается нишевым продуктом, который является бесплатным, но обычно низкого качества. Идея, лежащая в ее основе, кажется слишком

простой, чтобы иметь социальную ценность. Но если присмотреться к определению повнимательнее, оно показывает огромную силу.

Как упоминалось выше, предпосылками являются три основных определения.

Во-первых, это бесплатная доступность. Первое определение гласит: "Программное обеспечение выполнено в форме, которая может быть прочитана и понята человеком". Это означает, что любой человек, освоивший соответствующий язык программирования, может понять написанное и изменить его в любой форме. Это означает, что для общего образования в цифровизированном мире необходимо владение одним из этих "новых" языков. Если бы это было так, то была бы возможна полная прозрачность структур, определенных выше как инструменты власти. Поскольку не все могут делать это одинаково хорошо, в случае полностью свободного исходного кода достаточно, если достаточно большое количество zoon politikon, в соответствии с их индивидуальными способностями, возьмет на себя эту проверку инструментов. Поскольку исходный код открыт, это может быть чрезвычайно большая группа экспертов, которым даже не обязательно знать друг друга для выполнения этой задачи.

Второе определение гласит: "Программное обеспечение можно копировать, распространять и использовать по своему усмотрению. С одной стороны, это обеспечивает постоянную доступность, а с другой - радикальный отход от частной собственности на программное обеспечение. Современное программное обеспечение понимается как человеческое достижение и поэтому не может иметь владельца. Если объединить это с первым определением, то становится понятен потенциал, стоящий за ним, и вы приходите к третьему определению: "Программное обеспечение может быть изменено и передано в измененном виде".

Если каждый имеет неограниченный доступ к любому программному обеспечению и может изменять эти тексты в любой форме и, в свою очередь, делать их доступными для всех без ограничений, создается невероятная комбинация знаний. Также, вполне диалектически, разрешаются противоречия. Если приложения бесполезны и не подходят для одной группы, то они могут внести изменения в свою пользу, не опекая группу, которая хорошо относится к первоначальному приложению.

Может возникнуть диалектический синтез, подлинный плюрализм.

Федеральный, децентрализованный

Джордж Оруэлл, один из самых глубоких и влиятельных мыслителей 20-го века, в своей культовой книге "1984"(5) описывает мир централизованного тоталитаризма, который пронизывает всю жизнь человека и общества. Несмотря на то, что его книга - это роман, она представляет собой проницательный анализ современных массовых обществ.

То, что это не чистая выдумка и насколько фатально это влияет на людей внутри и вне соответствующих обществ, доказано многими примерами из новейшей истории, некоторые

из них самые жестокие. Основой этих тоталитаризмов, как в представлении Оруэлла, так и в реальных исторических версиях, всегда является радикальный централизм. Централизм, не оставляющий места для самореализации личности, или плюралистическая модель общества, учитывающая противоречия и особенности сложного современного массового общества.

Поэтому можно предположить, что, как тенденция, все запутанные, отчужденные общества движутся к централизму и тоталитаризму. Поскольку это было признано рано, большинство ранних, буржуазных и либеральных конституций были основаны на идее федерализма, децентрализма и индивидуализма.

Зарождающееся цифровое общество также имеет эту тоталитарную тенденцию. Сегодня несколько технологических компаний, объединенных в монополию, доминируют над значительной частью интернета в тоталитарном смысле. Мало того, что все цифровые платформы и, следовательно, вся коммуникация и социальное взаимодействие, происходящие на них, находятся под контролем этой монополии, так еще и конечные устройства и техническая структура в основном не находятся в руках тех, кто должен их использовать.

Тот факт, что с его помощью осуществляется всеобъемлющий контроль и слежка в оруэлловском смысле, теперь хорошо доказан, задокументирован и известен значительной части людей. Таким образом, цифровизированное общество движется к тем же фатализмам, что и позднебуржуазное общество. Скорее всего, с такими же жестокими последствиями. Поэтому мы должны что-то делать.

И здесь открытые источники и открытое программное обеспечение дают нам мощные инструменты. Одним из выдающихся оснований этой структуры является децентрализм. Как описано выше, открытые источники могут быть манипулированы и изменены по желанию любого человека. Таким образом, они могут быть адаптированы к собственным потребностям или потребностям группы без ущерба для интересов других групп или отдельных лиц.

Это становится особенно очевидным при межличностном, социальном взаимодействии людей. Сегодня это в значительной степени переместилось в цифровое пространство. Этот вид коммуникации особенно деликатен и заслуживает защиты, поскольку касается частной сферы людей, которая по определению не предназначена для публики. Легко понять, что такая защита частной жизни невозможна в тоталитарном, централизованном цифровом пространстве, каким мы его видим сегодня. В совокупности все, даже самое частное общение, само по себе является публичным.

Проблема может быть решена только путем децентрализации базовой структуры. На основе движения за открытый исходный код в настоящее время зарождается так называемый федеративный интернет (в повседневном языке часто называемый Fediverse). В этой федерации предполагается, что, например, социальная коммуникация в цифровом пространстве ограничена несколькими стандартными процедурами. Они определяются как открытые стандарты и принимаются каждым участником федеративной сети. Это приводит

к чрезвычайно высокой степени индивидуальной свободы и постоянной приватности.

В качестве примера рассмотрим так называемые социальные сети. Социальные сети - это место, где происходит большая часть частного общения. Сегодня эти СМИ находятся в монополистических, тоталитарных руках. Однако структура этого общения основана на нескольких стандартизированных действиях. Итак, существует публикация или постинг, комментирование других публикаций, подтверждение или лайк, перепечатка чужого контента, так называемый обмен или прямое общение, чат и так далее.

Таким образом, если бы эти действия были основаны на открытых стандартах, понятных любому субъекту, то для любого независимого субъекта, придерживающегося этих открытых стандартов, было бы возможно общаться с любым другим субъектом с такими же стандартами вышеописанным способом.

В крайнем случае, каждый человек может работать с таким экземпляром на своем собственном оборудовании в качестве частного экземпляра и при этом иметь возможность общаться с другими экземплярами. Поскольку предпосылки для функционирования структур такого рода даны не каждому, то управлять этой открытой структурой могут такие социальные субъекты, как ассоциации, муниципалитеты, университеты, отдельные группы или индивидуумы.

Поскольку базовое программное обеспечение и согласованные стандарты доступны в виде открытых источников, их может использовать каждый. Федеральная, децентрализованная.

> (5)Девятнадцать восемьдесят четыре. Penguin, London, 2021, (настоящее оригинальное издание) ISBN 978-0-24-145351-3.

Индивидуальная криптография

В классической теории контрактов а-ля Руссо или Гоббс, то есть в контрактуализме, предполагается, что общество развивается из первобытного состояния. В этом первобытном состоянии еще нет ни общества, ни договора; это состояние аморального рационализма, в котором каждый человек должен заботиться о своем собственном благополучии, чтобы выжить. Это созвездие "все против всех". Если общество возникает из первобытного состояния, то мы находим справедливое первоначальное состояние, или, говоря более профанно, в сомнении, каждый может убить каждого. Неравенство возникает только при наличии собственности.

Согласно этой теории, общество формируется на основе договора, и этот договор возникает в силу необходимости. Теперь не обязательно разделять теорию контрактов, но она хорошо показывает, при каких условиях возникают (новые) общества.

Сегодня мы также сталкиваемся с перестройкой общества. Однако не из первобытного состояния, а как переход от буржуазного к цифровому обществу. Не может быть и речи о

справедливом начальном состоянии, поскольку для упадочного, позднесовременного, накопленного общества характерно неравенство в крайней степени. Как уже было показано, это крайнее неравенство уже отражено в новом обществе через возникновение цифровых монополий.

Состояние аморального рационализма (Гоббс называет его "homo homini lupus" - человек человеку волк), с другой стороны, легко наблюдать сегодня. Все цифровое пространство является "милитаризованной" зоной. В случае сомнений все нападают на всех остальных; практически нет региона, в котором человек был бы в безопасности. Как только вы подключаете устройство к Интернету, оно становится общедоступным и уязвимым. Каждый уютный день, с планшетом и смарт-телевизором на диване, на самом деле проходит с открытым кошельком и в нижнем белье на рынке.

Изжившие себя монополии капиталистического общества - не просто аморальные актеры (как и все остальные), они - волки на пути к превращению в нового Левиафана(6). Волки с огромной силой.

Для того, чтобы достичь общества без состояния аморального рационализма и монополизированного неравенства, нам также нужны инструменты. Инструменты, которые не хотят в корне покончить с состоянием "все против всех", но распознать его и сделать безвредным в структуре.

Этот инструмент - криптография. Криптография существует с тех пор, как люди противостояли друг другу как конфликтующие группы. Довольно много войн было выиграно путем шифрования собственной информации таким образом, что противник не мог ее понять, или путем дешифровки информации противника. Поскольку мы находимся в "военизированной" зоне в цифровом пространстве (и в информационном обществе), шифрование собственной частной информации важно для каждого участника и необходимо для свободной, самоопределяющейся цифровой жизни.

Это означает, что впервые в истории человечества за право на индивидуальную криптографию нужно бороться. Индивидуальный в данном контексте означает, что шифрование и дешифрование собственной информации может осуществляться только отдельным человеком. Поэтому промежуточных экземпляров не существует. Говоря простым языком, информация доступна только тем субъектам, которым она адресована. Это называется сквозным шифрованием.

Поскольку мы находимся на переходном этапе от буржуазного к цифровому обществу, идет битва за право на индивидуальную криптографию. Эта битва ведется настолько ожесточенно и жестоко, что термин "cryptowars", то есть криптографическая война, стал общеупотребительным.

Противниками криптографии, как и ожидалось, являются установленная цифровая монополия и устаревшие структуры позднебуржуазных обществ, такие как государство и руководители, защищающие старые структуры власти. Оправданием такой реакции обычно служит не сохранение власти, а плохость людей. Человечество должно быть под контролем, потому что иначе оно уничтожит само себя. Святой мантрой и троицей в этом контексте

часто являются "террористы, нацисты, растлители детей" и популистская угроза, что без патриархальной защиты мы будем беззащитны перед этими патологическими явлениями. Однако имеется в виду коллективное предвзятое отношение ко всем, как к инструменту власти.

Как показано выше, индивидуальная криптография также предполагает аморальных субъектов, но ясно показывает, что защитой от аморального рационализма других может быть только защита собственной информации. Точно так же это крайне важно для того, чтобы порвать с устаревшими капиталистическими структурами власти старой эпохи.

> (6)Томас Гоббс: Левиафан. Cambridge University Press, Cambridge 1996, ISBN 978-0-521-56797-8.

Практическая криптография

Децентрализация и индивидуальная криптография являются необходимыми предпосылками для обеспечения эмансипирующей, самоопределяющейся жизни для всех людей в цифровом пространстве. В то время как децентрализация цифрового взаимодействия является структурной процедурой и может быть достигнута путем предоставления стандартных процедур и норм в качестве открытых источников, независимых от индивидуума, индивидуальная криптография также является индивидуальной проблемой.

История современной криптографии (как она широко используется в цифровом пространстве сегодня) относительно давняя(7) и имеет мало общего с оцифровкой. Современная криптография является очень сложной специальной областью высшей математики и требует огромной способности к абстракции и глубокого знания последовательностей чисел, шифров и математических процедур.

Поэтому знания об этом хранятся у очень небольшой группы людей. Учитывая это, одним из критериев хорошего метода шифрования является не только защита от расшифровки неавторизованными третьими лицами, но и разумная и простая работоспособность и несложное обращение с методом пользователями без соответствующих математических знаний.

Поскольку индивидуальная криптография, истинное сквозное шифрование, всегда должно осуществляться самим человеком, так как не может быть промежуточных инстанций, это является огромной проблемой для эмансипированного цифрового общества.

До развития современной криптографии в 20 веке все методы шифрования реализовывались по принципу "безопасность через неизвестность". Сам метод шифрования должен был быть неясным. Каждый участник, который хотел принять участие в зашифрованном общении, должен был знать процедуру дешифровки. Это означало, что любая третья сторона, знающая о таком способе шифрования, могла расшифровать весь контент, зашифрованный с помощью этого метода. Поэтому этот процесс очень небезопасен и легко поддается

компрометации. И, конечно, секретность процесса полностью противоречит идее открытых источников. Криптографический процесс срочно нуждается в открытом исходном коде и возможности проверки.

Таким образом, в середине 20-го века появился метод, основанный на обмене ключами. Поэтому секрет, необходимый для шифра, уже не был самой процедурой, а основывался на секретном ключе, который должен был быть известен как отправителю, так и получателю. С одной стороны, это позволило раскрыть процедуру, что дало возможность научного изучения этого метода, а с другой стороны, компрометация одного ключа не ставила под сомнение всю процедуру.

Ключ в данном контексте, как в математических, так и в цифровых шифрах, обычно означает длинную, сложную строку символов, которую невозможно ни угадать, ни вычислить с разумными усилиями. Поэтому в цифровом пространстве в качестве секрета обычно выступает просто файл. (Конечно, современная криптография намного сложнее, чем можно было бы представить здесь).

Недостатком этого метода, также называемого симметричным шифрованием, является то, что сам ключ также должен быть передан получателю. Поскольку при шифровании и расшифровке используется один и тот же ключ, отправитель и получатель также должны владеть этим ключом. Если в аналоговом пространстве еще можно представить, что обмен соответствующим ключом может быть осуществлен с помощью доверенного посыльного или при личной встрече, то в цифровом пространстве с миллиардами потенциальных партнеров по общению это просто невозможно.

В 1976 году Уитфилд Диффи и Мартин Хеллман разработали метод асимметричного шифрования(8). Этот метод отлично подходит для обеспечения бескомпромиссного сквозного шифрования в цифровом пространстве, даже если участники коммуникации не знают друг друга. Сегодня этот принцип также является стандартной процедурой для каждого индивидуального, зашифрованного общения в Интернете.

Этот тип шифрования основан на идее, что у каждого участника есть два ключа. Один закрытый ключ, который стоит защищать, и один открытый ключ, который известен всем остальным. Открытый ключ, как следует из названия, находится в открытом доступе и может только шифровать. Поэтому открытый ключ не может ничего расшифровать, даже содержимое, которое было зашифровано тем же ключом.

В отличие от этого, закрытый ключ, который стоит защитить, дает возможность только расшифровать. Поэтому содержимое, зашифрованное с помощью открытого ключа, может быть расшифровано только с помощью соответствующего закрытого ключа. Поэтому для того, чтобы стала возможной настоящая индивидуальная криптография, необходимо, чтобы каждый участник цифровой коммуникации обладал хотя бы одной такой парой ключей и сам управлял ею. Если закрытый ключ утерян или к нему получили доступ неавторизованные третьи лица, зашифрованное содержимое будет безвозвратно утеряно или скомпрометировано.

Это действительно проблема, с которой сталкивается цифровизированное общество. Если вся структура открытого, цифрового общества существует как открытый источник и, следовательно, доступна в любое время, то по природе вещей секрет, каковым является закрытый ключ, должен быть известен только тому человеку, которому адресовано приватное содержимое.

В аналоговом пространстве само собой разумеется, что частные помещения, такие как дом, защищены ключом, и что необходимо проявлять соответствующую осторожность. Поскольку такой секрет, как ключ, не может быть просто передан на хранение в открытую структуру, это понимание должно преобладать и в цифровом обществе, для цифрового частного пространства. Тем более что там нет ни слесарей, ни ломиков.

> (7) Клод Шеннон: Математическая теория связи шифровальных систем. In: On - Off: Selected Writings on Communication and Message Theory. 1-е издание. 1949 Brinkmann and Bose, Berlin 2000, ISBN 3-922660-68-1,

> (8) У. Диффи, М. Э. Хеллман: новые направления в криптографии. In: IEEE Transactions on Information Theory. Том 22, № 6, 1976

Version #4
Erstellt: 10 November 2022 14:37:09 von reverend
Zuletzt aktualisiert: 20 November 2022 14:14:54 von reverend