

Главное про Korni3 и сетевые коммуникации

Главные моменты

Основной враг общества - цензура, модерация, ложь. Цензура - это средство манипуляции народом, способ скрыть альтернативные аргументы, способ лгать. Цензура - санкции в области информации. в США, например, цензура выключила из инфополя российские каналы, российская точка зрения не звучит, сми обосновывают лживую народным массам военные вторжения в страны (Афганистан, Ирак, Ливия, Россия, Югославия, Украина,...) Люди верят сми и готовы даже одобрить применение ЯО властями. Все это результат наличия самой возможности цензуры. Цензуры не должно быть ни у кого, вообще не у кого. Опыт показывает, что цензура становится инструментом для лжи и манипуляции.

1. Главная проблема , решаемая korni3 - проблема цензуры, точнее : "исключает блокировку доступа к контенту". Метод решения юридический, а не технический - все копии данных для приложений у пользователей есть локально, принадлежат пользователю, а все приложения НЕ работают через сеть самостоятельно - поэтому их можно публично развивать, обновлять итд. С каким именно контентом они работают локально при этом не известно. korni3 сводит коммуникацию к простому обмену файлами по сети.
2. korni3 имеет просветительскую миссию. Мы бесплатно распространяем знания и курсы по сетевой безопасности, редкие книги, исторические сведения, интервью, исторические документы, резервируем доступ к сканам, полит информацию по теории власти, политическую и экономическую аналитику, компьютерные технологии, фото и видео произведений искусства, исторические подписанные и легитимные приказы, влияющие на жизнь общества итд. Мы хотим дать людям инструмент личного цифрового суверенитета. Суверенный интернет начинается с личного суверенитета и свободы доступа к знаниям для каждого человека.
3. Борьба с цензурой и модерацией на этом не заканчивается - остаётся проблема анонимности.
 - a. korni3 предлагает не предлагает конкретный сетевой транспорт, наоборот , предлагается использовать все виды сетевого транспорта. можно использовать любые способы передачи файлов, анонимные в том числе.

- b. мы создадим скрипты, которые позволят использовать все возможные способы синхронизации файлов.
 - c. полностью Анонимная передача на данный момент не в первом приоритете, но уверяю: достаточно легко реализовать анонимность например средствами вида vpn , vds servers,... тем людям, которых это действительно волнует. Мы уважаем индивидуальную степень паранойи каждого человека.
 - d. Важным методом борьбы с цензурой является изобретенная мной "обязывающая лицензия контента" (требуется коллективное обсуждение этой идеи и возможно, ее доработка, всё таки я не юрист по образованию и что -то мог упустить.)
4. Я ищу способы усилить экономику своей страны, сделать людей богаче сильнее и независимее. У нас в стране много предателей и саботажников. Я работал много лет в области науки, технологий, электроники, программ, управлял сложными проектами, создавал системы планирования, управления и управления знаниями, занимался робототехникой и др. Нам требуется запустить "настоящий народный инвестиционный процесс" для модернизации страны и себя, освободив часть связанных средств. Нужно исключить всех паразитов из производственных и торговых цепочек, убрать все комиссии, любые платежи которые мы не хотим платить итд. Для этого надо переделать интернет торговлю, мы должны для этого даже изменить суть и название. (и, считаю : это должно перестать быть торговлей, это может быть равнозначный обмен, в котором не будет прибыли и наценок). Но конечно люди должны решать как и чем это должно быть, поэтому в базе я просто создаю приложение для поиска поставщиков и покупателей и обеспечиваю возможности им связаться. Тут важно цензура и модерация так же не может быть осуществлена в такой системе.
5. Цензура и модерация на выборах - страшный для кармы злодея способ сломать жизни многих людей и крупная общественно значимая ложь. Наука создала способы, чтобы избежать мошенничества на цифровых голосованиях. уже сейчас есть способы как провести голосования и честные цифровые легитимные референдумы. Такая возможность планируется к запуску в рамках системы korni. Я вижу пока уровень голосования "мы жители района X против свалки Y", в котором невозможность подделать результат и возможность получить юридически значимый результат - это и есть ценная правда - лучший враг лжи.

Читай так же

- [Корни - Часто задаваемые вопросы](#) TODO link
- [Korni3](#) TODO линк на документацию к утилите

Что собой технически представляют файлы kornі3

файлы kornі3 - результат работы утилиты kornі3 . Утилита манипулирует данными по командам прикладных приложений , для которых kornі3 является системой хранения данных.

Другими словами можно сказать, что действия над базами данных многих прикладных приложений превращаются утилитой kornі3 в множество файлов. Приложения могут поставляться разными поставщиками, это могут быть даже скрипты управления данными пользователя которые пользователь сам сочинил.

По самим файлам невозможно точно сказать частью какой базы данных какого приложения они являются, это можно только предположить и на какое конкретное множество файлов разбита эта база.

Невозможно определить и утверждать так же для одной и той же базы одного и того же приложения с многими пользователями является ли она единой или это две и более не связанные базы разных группы пользователей, вплоть до отдельных баз каждого пользователя.

Невозможно даже, имея на руках все эти базы, только по ним доказать как именно коммуницировали пользователи и коммуницировали ли вообще (даже случайные ссылки друг на друга в текстах могут быть фейком и симуляцией коммуникации, которой реально могло не быть).

Для системы управления данными kornі3 сеть не является необходимой. Kornі3 может работать без сети, приложения на этой системе строятся так, чтобы специально не использовать сеть.

kornі3 полагается на сторонние способы обмена данными. Все коммуникации сводятся к свободному обмену файлами. Для обмена файлами существует множество публичных и анонимных способов, так, kornі3 рекомендует кооперацию между системами, и развивает партнерское сотрудничество с сетевыми транспортом решающих задачи обмена файлов. обмениваться файлами kornі3 можно даже просто меняясь флешками и жесткими дисками в случае если весь интернет заблокируют или на войсковой передовой, где использование радио связи ограничено и опасно для жизни бойцов из-за военных действий неприятеля.

kornі3 сильно защищен от цензуры т.к. копии необходимых файлов есть у каждого их владельца на личном персональном носителе и могут передаваться неисчислимым множеством способов.

база данных kornі3 формируется из отдельных изменений распределенных по файлам, она содержит сумму изменений и правок. каждая правка имеет метку времени, автора в виде аккаунта kornі3 , и цифровую подпись. изменения складываются в таблицы базы данных. Приложения видят все правки, а не только последнюю. Консистентность данных обеспечивается приложением а не системой хранения, для этого существуют отдельные методы. (на базовом уровне например можно реализовать swarm транзакции, таких методов довольно много). kornі3 как система хранения не обеспечивает транзакций и консистентности т.о. и многоверсионна - каждый пользователь может иметь разный набор данных в приложениях.

Прочие технологии коммуникации

"обязывающая лицензия контента"

Одна из нескольких технологий корректной синхронизации файлов опирается на такие основания.

- Подарки получать можно всегда. Подарки не запрещены. Получить подарок неожиданно может кто угодно.
- Если не знаешь, что в коробке подарка то получение такого подарка никогда не может быть нарушением.
- Дарить можно анонимно. Анонимный человек имеет право озвучить ультиматум и имеет право быть выслушан.
- Ультиматум может содержать оферту.
- Если ситуация внезапно сложилась так , что Вы обязаны - нужно исполнить обязательство. (казино, спор, страховой случай, контракт ...)

- *Нужно по возможности исполнить свое обязательство: "выслать владельцу его собственность, если она находится у Вас"*
- *Любой человек может выставить обществу свои требования (пусть даже и смехотворные)*
- *Отдельный человек может игнорировать требования другого человека ко всему обществу.*
- *Каждый человек вправе отказаться исполнять свои обязательства, оценив риски.*

Чтобы запретить обмен по этому способу необходимо (но не достаточно), как минимум, разрушить эту опору.

Лицензия-оферта запроса файлов

имеет такое общее содержание:

- *Я - человек, из плоти, крови и костей, рожденный и живущий на планете Земля, желаю остаться анонимным. Я интересуюсь содержимым перечисленных ниже файлов в личных целях. Предполагаю, что файлы распространяются по *Common Public License* т.е. являются "всеобщим достоянием", на этом основании я хочу их получить. Если файлы являются Вашей собственностью, то согласно данной оферте Вы теперь обязаны добровольно передать их копии мне в дар на общих основаниях без условий и гарантий. Считаю, что все копии файлов в этом списке являются Вашими, даже если Вы не знакомы с их содержанием и не знаете откуда они у Вас возникли и Вы можете их копировать для меня, если я получу их любым способом, то буду считать их копии своими и Вы с этим согласны. Считаю, что имею право владеть пользоваться и распоряжаться копиями этих файлов. Я никак не могу убедиться, что после получения мной мои копии файлов с такими именами будут равны вашим копиям файлов с такими же именами и Вы тоже не можете быть в этом уверены и мы оба принимаем этот факт. (Имя файлов не обязано всегда соответствовать одному и тому же содержанию файла). С момента, как только Вы создадите копию файла и/или получите эту оферту (не важно по каким причинам), я автоматически считаю, что это уже моя копия файла и Вы обязаны передать её мне, решение о передаче своего файла Вам принимать не нужно, Вы лишь обязаны*

передать мне мою копию. Мой ультиматум вам: Если Вы решите не выполнять свою обязанность по данной оферте (т.е. оставить теперь уже мои копии файлов у себя), то делайте это так, чтобы ни я, и никто другой, об этом вашем нарушении условий данной оферты никак не узнал - для Вас это безопасное решение, никаких последствий не последует. такой отказ от оферты - влечет отказ от обязательств.

<список файлов>

Комментарии к тексту лицензии:

У файла есть владелец и автор. в тексте фигурирует как "файл" так и "копия файла".

Имя файла в некотором роде идентифицирует файл, но лучше всего идентифицирует файл его содержимое, которое не известно стороне получателя.

заявленная цель получателя (получатель не гарантирует ее достижение): ознакомиться с содержимым и завладеть копией файла. Владелец может так же копировать свой файл и отдавать его копию кому-то. Будет ли цель достигнута до или после этих событий - личное дело каждого получателя. Получатель ничего не гарантирует, запрашивая файл, даже не гарантирует, что у него будет в результате такая же копия как у отправителя.

Равенство так называемых копий не волнует в целом никого в этой паре , ни отправителя ни получателя по таким причинам:

1. если файл идентифицируется хешами контента в имени файла, то получатель может после получения проверить это соответствие заново вычислив хеши.
2. если же файл кроме прочего внутри себя содержит микро-документы с наборами изменений таблиц данных, то эти наборы сами по себе содержат цифровые подписи и все нужные атрибуты чтобы не беспокоиться о корректности этих данных. некорректные данные система игнорирует. проверка подписей позволяет исключить поддельные записи, а если файл содержит бесполезные данные то пользы в нем нет и он может быть удален.
3. если отправитель не сообщил все изменения которые у него имеются - он вправе сделать это. т.к. это его копии и ему решать передавать ли их вообще и передавать ли их полностью. Спасибо, как говориться , и на том, что передал.
4. атака типа "человек по середине" не имеет смысла в этом случае т.к. получатель может проверить сам все полученные данные на корректность

Правомерность передачи данных.

Обращаю внимание, что системы обмена файлами работают с данными а не с информацией. Для них файлы - это сущности без смысла и такие системы нигде и никогда смысл данных не анализируют и не принимают никаких решений.

Копия файла попадает получателю потому, что он захотел и заявил о условиях передачи, а не потому, что кто-то рассылал их. По этим условиям отправитель становится обладателем копии файла принадлежащей получателю в момент копирования файла еще до того, как он, возможно принял решение отправить файл (причина копирования своего файла у него может быть абсолютно любая, так же причиной является получение офферты). Далее отправителю уже нет необходимости принимать решение о передаче копии файла т.к. по условиям заявленной и прочитанной лицензии это будет уже не его копия, а копия файла, владельцем которой является получатель, который заранее обязал отправителя отправить копию получателю или не отправлять её (без объяснения причин). с правовой точки зрения здесь нет и не может быть распространения отправителем, но возможно нарушение обязательств отправителя отправлять получателю его собственность, о котором никто не узнает, и получатель об этом никуда не заявит, если это нарушение обязательств произойдет.

Данные (копии файлов) которые перечислены в списке файлов отправитель обязан передать получателю, можно передать уже любым способом, включая даже выкладку на любые промежуточные внешние ресурсы.

Обвинить в их содержимом нельзя ни получателя ни отправителя ни посредников передачи т.к. :

1. получателя нельзя обвинить т.к. он не знает, что ему отправят и не знает, что получит и возможно при передаче его обманут и он получит искаженные данные. Он не имеет никакого умысла. только желание получить свои копии файлов и, возможно, ознакомиться с ними, если ему удастся как-то открыть эти файлы и когда либо вообще получить технические возможности и условия увидеть какое-то содержимое которое в них закодировано прямо или косвенно.
2. отправителя нельзя обвинить т.к. он делает то, что обязан сделать по условиям лицензии (открытая оферта). он передает не свои копии файлов владельцу этих копий по запросу владельца - это типичное исполнение контракта. Содержимое файлов системы передачи файлов не анализируют никогда. (+ Система корни кодирует данные так, чтобы не было однозначного соответствия отображаемым в приложениях данных, содержимому индексной базы данных и файлов с наборами изменений т.е. это кодирование осуществляется на ином уровне, данные распределяются по многим файлам с непонятным именем сформированным

машиной). Списки имен запрошенных получателем файлов и списки имен имеющихся у отправителя файлов не имеют в общем случае никакой связи, получатель мог заинтересоваться ими, получив имена, например, и из других источников, но, впрочем, в публикации непонятных имен файлов нет никакого нарушения - это только имена файлов созданных машиной по стандартному шаблону удобному самой машине. Нет возможности понять связь этих имен и данных которые есть в приложении.

3. нельзя обвинить посредников в способствованию передаче т.к. передача и её условия заранее согласованы. её сторонами является получатель и отправитель, посредник только обеспечивает техническую возможность, если его привлекли к этому процессу (оба согласились, что это возможно). Для посредника это чужие файлы и он не имеет права заглядывать в них. при необходимости файлы шифруются, чтобы посредник не мог их прочитать при "лишнем любопытстве". Если вдруг посредник решит препятствовать передаче - в этом нет проблемы, оба участника к этому готовы (выберут иного посредника).

Общая схема ещё раз

Отправитель : публикует списки файлов которые у него есть , имена файлов сформированы машиной и по ним понять ничего нельзя.

Получатель : откуда то узнал эти имена, захотел ознакомиться и завладеть предположительно копиями файлов с такими именами.

Получатель: опубликовал оферту - соглашение в котором её текст, список файлов, и предпочтительный способ получения файлов. Получатель обращается к любому из абонентов.

Отправитель : заинтересовался лицензией-офертой, ознакомился с ней. В результате Узнал, что обязан создать копии своих файлов, которые автоматически тут же становятся копиями получателя, которые затем уже обязан отправить их владельцу-получателю. От этих обязательств и копирования и отправки отправитель может отказаться без последствий.

Передача: напрямую , указанным получателем способом, или через посредника , вероятнее всего зашифрованная "копия файлов" попадает к получателю от кого-то из множества абонентов, получивших оферту. Удостовериться, что "копия файла", действительно является копией никто достоверно не может и это всех устраивает. Утверждать, что передавалось именно такое содержимое тоже никто не может и это всех участников устраивает. Получатель вправе выдавать свою копию за оригинал и это тоже всех устраивает (любой

человек вправе выдавать свои файлы за оригинал и давать им любые имена). Утверждать, что у получателя оказалась конкретная копия файла от конкретного отправителя нельзя, ведь читали оферту и получили по ней обязательства сразу несколько абонентов. Утверждать, что файлы полученные получателем в результате имеют такой или иной контент по конкретной причине никто не может по причинам указанным выше и утверждать что-то про "контент" тоже ничего нельзя т.к. на уровне "данных" такого понятия нет.

Не смотря на все, казалось бы, нарушения "привычной логики" система корни корректно обрабатывает все эти ситуации и надежно работает.

немного другая оферта

Другой вариант Оферты:

Я человек рожденный и живущий на планете Земля из крови, плоти и костей предлагаю Всем читателям сего оферту: По этой оферте у Вас обязательно возникают обязанности. Вы вправе отказаться от своих обязательно возникающих обязанностей по этой оферте без последствий. Если Вы получили эту оферту или у Вас имеются любые из файлов с именами из списка ниже (это акцепт), то Вы дополнительно обязуетесь 1) создать для меня копию каждого совпадающего по имени файла, которая в этот миг (начало копирования) становится моей 2) передать мне мою копию файла по указанному мной адресу, указанным мной способом, 3) а я обязуюсь её принять. Что находится в этих моих копиях файлов я не знаю и Вы, вероятно, тоже и меня это не интересует т.к. я понимаю, что в процессе передачи файлы могут быть искажены. Проверить соответствие моей копии и вашей я не могу и вы не можете. Ни я ни Вы не обязаны доверять друг другу и такая задача перед Вами и мной не ставится. Никаких гарантий ни я ни Вы не даём. Я вправе владеть пользоваться распоряжаться моими копиями файлов. "Копии файлов", которые я получу в результате могут отличаться по содержанию и быть не равны Вашим копиям файлов и мы оба принимаем этот факт. Отказаться от обязательств Вы может как полностью по всем файлам, так и частично - по некоторым файлам, без последствий. Отказ от исполнения обязательств влечет отказ от оферты.

"Cryptomator"

1. папка с файлами шифруется , в том числе имена файлов подвергаются шифрованию и перемешиваются (как например делает приложение Cryptomator)
2. системы синхронизации синхронизируют файлы результатов шифрования между абонентами.

Анализ рисков.

Допустим злоумышленник, который хочет обвинить участников в обмене узнал ключ шифрования и вошел в группу в которой происходит обмен. Он получил копию общей папки с файлами.

Может ли он понять какие файлы кто распространил?

- установить соответствие файла в расшифрованной папке и файла в зашифрованном контейнере сложно но можно. но это ничего не даёт
- в korní3 файлы наборов изменений имеют автора - это автор изменений , идентифицируется публичным ключом а системе korní3. однако на транспортном уровне такие адреса отсутствуют. задача в теории выполнимая, но на практике может оказаться не выполнимой.

если использовать вместо/вместе с cryptomator IPFS то файлы бьются на блоки а имена кодируются в других блоках.... блоки именуются по хешам ... роутинг в ipfs оверлейный и отследить в оверлее откуда пришел тот или иной блок сложнее.

Правильное кодирование имен файлов и шифрование с разбиением на блоки - надежный хороший способ развязать имена файлов в системе korní3 и блоки ... но и тут есть методы найти соответствие файла и реального адреса.

темная сеть

чтобы никак не установить связь с физическим сетевым адресом надо использовать сервисы ftp например в i2p .

анонимный месенджер

в bitmessage например делается публичный известный всем канал. туда анонимно можно публиковать свои списки файлов и способы получения файла , или torrent файлы слепков своих контейнеров

Там могут быть адреса... но это дело каждого как получать файлы... Тут важно, что не пришить ничего потому, что человек не обязательно автор всех раздаваемых файлов, связь тут такую не установить.

почта для всех (законных целей)

Вариант когда почтовый ящик = копия хранилища

- заводим на любом сайте почтовый ящик. заводим там аккаунт гость, под которым любой может смотреть почту.
- клиент ПО заходит на почту и смотрит письма не удаляя их. в них файлы - их получает.
- либо пишем сам- себе , вкладывая в письма файлы.

Почтовые ящики бывают 100 ГБ и очень недорогие. заблокировали - легко перешли на новый почтовый адрес.

да, почтовый сервис на провайдере хранит адреса и цифровой след. но это **для относительно законных дел.**

Вариант , когда почтовый ящик - способ сообщить p2p адрес для обмена.

у абонентов может быть почта.

- приложение korni3 может в аккаунте korni3 хранить и почту абонента - тогда абонент деанонимизирован. Или
- или в приложении есть анонимное множество почтовых адресов, предположительно абонентов этой группы.

сетевой синхронизатор может осуществлять по почте примерно такой диалог:

1. я прошу список файлов. прошу файлы
2. ответ содержит адрес где их можно взять , сами файлы пересылать не нужно - это может стать причиной блокировки почты.
3. человеку пользоваться этим ящиком не обязательно.

Преимущества : почтовые сервера - реально самая старая и рабочая децентрализованная система коммуникаций, но тут она работает против цензуры для любых приложений.

облачные хранилища файлов (для законных целей)

- делается публичный контейнер с формой для загрузки файла.
- все (без авторизации) туда шлют свои файлы - они складываются в контейнер с автоматически придуманными именами.
- софт сканирует файлы в облачном контейнере начиная с даты - и забирает те, которых не хватает.

тут хорошо что аккаунта на хранилище не нужно заводить.

заблокировать могут.... но придется блокировать большие хостинги, целые датацентры , где денные корпораций и госкорпораций - возмущений слишком много будет тогда.

php хостинг для сайта (для относительно законного)

- на любом хостинге делается сайт из 1-2 x php форм для принятия файлов определенного типа.
- клиенты шлют на формы файл. скрипт их проверяет и складывает на диск.
- всем виден набор этих файлов и их можно скачать.

Могут заблокировать, но создать такой новый сайт скриптом - секунды.

Причем его новый адрес в общий канал (или даже по почте) клиенты его подхватывают и все работает дальше. опять же : если есть шпион то его легко вычислить: надо чаще самому менять сайт и даже делать их много и например одним клиентам давать одни сайты а другим - другие и смотреть кого блокируют а кого нет.

Тут важно, что система может работать на обычных почтовых аккаунтах.

Другой вариант

надо php положить на сайт а файлы отсылать в другое место, чтобы к сайту было не придраться - там данных никаких нет вообще. тогда легко менять место хранения быстрее чем заблокируют, хоть каждые 5 минут менять адрес - никаких проблем. А сайт со скриптом никаких данных содержать не будет.

ipfs подобные решения

Global File System - проект открытого сообщества, который сам по себе обладает защищенностью от атак. Он решает задачу "присутствия моих файлов в глобальной сети" без серверов. Проект имеет gateway's но их легко запустить на любых адресах одной командой и не они обеспечивают основной способ коммуникации там. Фактически это глобальный файловый оверлей поверх DHT. Запрет DHT в теории возможен, но ipfs может использовать любые адреса dht bootstrap узлов которые легко менять.

VPN свой или арендованный

на ssh машине можно запустить vpn , создав на нем свой и несколько гостевых аккаунтов.

можно соединяться с участниками анонимно (от провайдеров и других лиц) внутри сети vpn. если отключаться и подключаться к разным хамам vpn - можно обмениваться файлами достаточно анонимно.

Перечисление методов синхронизации файлов

Читайте статью [Методы синхронизации файлов](#) TODO link - методы которые могут быть задействованы пользователем для удобного обмена файлами kornі3