Теория строения скрытых систем

Коваленко Геннадий Александрович

Аннотация. Существующие определения анонимности и безопасности конечных пользователей в сетевых коммуникациях часто являются расплывчатыми, неясными и противоречащими друг другу. Такая реальность восприятия стала следствием недостающей теоретической основы, которая могла бы структуризировать, и в некой степени даже стандартизировать, основные подходы к построению или использованию скрытых систем[1]. Практическая реализация, которая далеко вышла за пределы теоретического понимания, становится в конечном счёте деструктивной и стагнирующей формой выражения скрытых систем, отодвигающая на второй план развитие их содержания. Понимание термина «анонимность», посредством декомпозиции его составляющих, способно дать оценку дальнейшего вектора развития анонимных и безопасных систем.

Ключевые слова: скрытые системы; анонимные сети; клиент-безопасные приложения; тайные каналы связи; сетевые архитектуры; сетевые модели; стадии анонимности; теоретически доказуемая анонимность; полиморфизм информации; мощность доверия; мощность анонимности; централизованные сети; децентрализованные сети; гибридные сети; механизмы анонимизации трафика;

Содержание

[1]Скрытые системы — множество сетевых технологий направленных на обеспечение и поддержание приемлемого уровня анонимности конечных субъектов (отправителя и получателя) в совокупности с безопасностью объектов (информацией). При этом анонимность и безопасность могут реализовываться в разной степени, что делает класс таких систем достаточно обширным. К системам подобного рода относятся анонимные сети и клиент-безопасные приложения.

1. Введение

Вся история тайнописи, защиты информации, стеганографии и криптографии сопровождалась антагонизмом двух сторон – нападающими и защищающими информацию как объект, передаваемый по линии или линиям связи [1][2]. В определённые периоды времени лидировали нападающие, когда все действующие системы становились полностью взламываемыми. В другие временные интервалы одерживали победу защищающие, когда таковые находили новые, более качественные способы защиты информации. В любом случае, атакующие представляли собой инициализацию всех последующих процессов, находивших уязвимости, недостатки определённых схем и эксплуатирующих их для получения нужных сведений. Всегда и во всей описанной истории нападающие играли двоякую роль – разрушения и созидания, когда с одной стороны, на базе краткосрочных интересов, их действия приводили к некоему отчаянию защищающих, понимающих бессмысленность и бесперспективность накладываемой безопасности, с другой стороны, уже на базе долгосрочных интересов, их действия приводили к полностью противоположным результатам – укреплению защищающих механизмов, где по мере понимания векторов нападения защищающие создавали иные, более качественные системы, противопоставляющие себя старым методам атак. Таким образом, вся история защиты информации являлась единством и борьбой противоположностей, в своём открытом, транспарентном представлении.

Если брать во внимание криптографию, как основной и базовый ориентир методов и средств защиты информации, то можно с уверенностью говорить об абсолютном опережении защищающей стороны над атакующей. Во второй половине XX века криптография вышла из составляющей искусства (своей классической формы) и переродилась в полноценную науку (современную криптографию) благодаря работам Клода Шеннона, стандартизации шифра DES, открытию асимметричной криптографии, хеш-функциям и цифровым подписям. Все данные явления положительно сказались на разработке и переустройстве схем безопасности, когда в аналогичном всплеске начали зарождаться криптографические протоколы, пригодные для обширного множества частных и общих задач. Постепенно и поэтапно появлялись алгоритмы, такие как RSA, Elgamal, Serpent, AES, SHA256, Keccak и

протоколы, такие как Diffie-Hellman, Messi-Omura, Kerberos, TLS и т.д. эффективных способов взлома которых в настоящее время так и не было найдено, даже спустя десятилетия их открытого криптоанализа с присущими вознаграждениями.

Всё вышеописанное, на первый взгляд, являясь положительным со стороны защиты информации, является на деле фиктивным, потому как нападающие неявным образом меняют свои векторы нападения, фрагментировано синтезируясь с защищающими. Плавное течение борьбы и единства атакующих с защищающими приостанавливается как только появляется синтез средств массовой информации с компьютерными технологиями. Множеству атакующих становятся бессмысленны прямолинейные взломы (по крайней мере в гражданском секторе), как того требовалось ранее. Нападающие, в новой парадигме, постепенно разделяются на две категории, где первые всё также продолжают противостоять более новым средствам защиты информации, выбирая путь классического криптоанализа и развития квантовых технологий [3], а вторые начинают выбирать путь взлома за счёт своего слияния со средствами массовой информации и её защищающими, становясь тем самым совершенно иной формой, отличной от примитивно атакующих и/или защищающих. Данная формация, являясь одновременно защищающей и атакующей стороной для одних и тех же лиц, не совершенствуется, как это было всегда ранее при обнаружении уязвимостей, потому как ей становится выгоден сам фактор системной незащищённости.

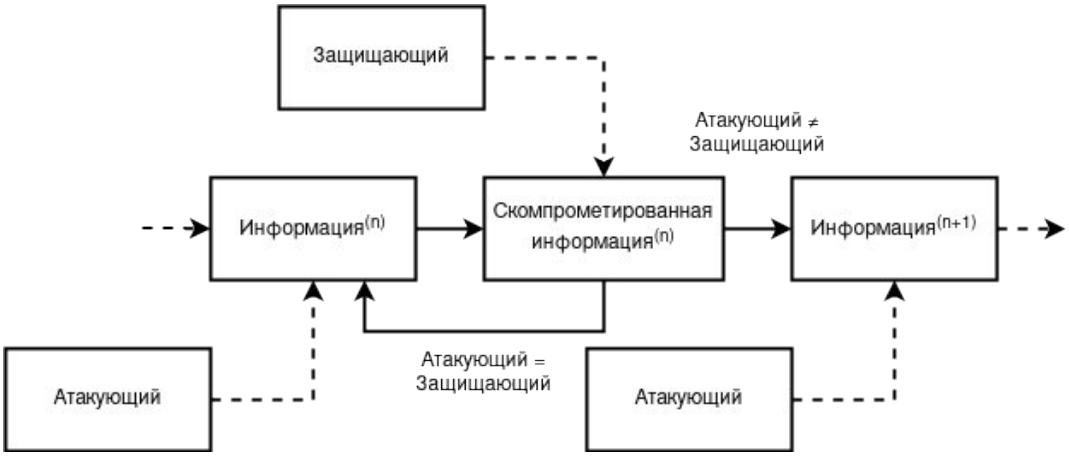

Рисунок 1. Развитие средств защиты информации (n) посредством действий атакующих и защищающих сторон. Слияние атакующих и защищающих способно порождать стагнацию в развитии средств защиты информации

Вышеописанная форма синтеза атакующих и защищающих представляет собой множество сервисов связи (социальные сети, форумы, мессенджеры и т.д.), поток информации которых превосходит все оставшиеся виды коммуникаций. Защита информации клиентов обуславливается необходимостью её сдерживания от других сервисов. Нападение на информацию обуславливается необходимостью её продажи другим сервисам, либо выдачи государственному аппарату. Таким образом, будучи выдвигаемым сервисом связи, таковой противоречиво начинает выполнять две совершенно разнородные, противоположные функции. Основной причиной данной проблематики становятся устаревшие модели угроз со стороны защиты информации, которые до сих пор акцентируют массовое внимание на новые или старые криптоаналитические атаки и на разработку квантовых компьютеров, которые дают лишь малый эффект, либо дадут таковой только в будущем. Сейчас же, мы имеем дело с куда более специфичной формой нападения, которая продолжает и будет продолжать выполнять свои неявные функции.

В современных реалиях, обществом, будучи расположенным в виртуальном коммуникационном пространстве, всё сильнее начинает ощущаться нехватка настоящего уровня безопасности конфиденциальной информации и непосредственного уровня анонимности. Каждая компания, корпорация, правительство пытаются узнать и узнавать о человеке как можно больше разнородной информации – пол, вес, возраст, материальное положение, страна, город, улица проживания, политические взгляды, выбираемая одежда, предпочтения в еде, отношения, друзья, родственники, телефон, электронная почта, биометрические данные, паспортная информация, тип устройства, интересы, хобби, образование и т.д. Такая перемешанная масса данных связанных между собой лишь и только одним её субъектом становится ценнейшей информацией, выражающей «человеческий капитал», отличительной особенностью которого становится репродукция потребления. Логичным интересом для «сборщика» такого рода информации становится её последующая продажа третьим лицам для получения экономической выгоды и экономического влияния. При монополизации или сговорных картелях таковых «сборщиков» становится возможным уже дальнейшее политическое влияние, направленное в первую очередь на подавление конкуренции и расширение системы, а также на сдерживание установленных и устанавливаемых императивов.

Изложение данной работы направлено на анализ становления таковых систем и на отличительные их особенности со стороны безопасности объекта (информации) и субъекта (пользователя, клиента системы). Из первичного анализа становится возможным выявление вектора развития последующих, более качественных сетевых коммуникаций. Большинство нижеизложенного материала проходит сквозь призму диалектической триады «тезис – антитезис – синтез». Таковой подход позволяет выявлять не только лишь основные векторы развития будущих систем, но и их последующие качества, характеристики, как сочетания N-ого количества бывших парадигм. Помимо прочего, такой подход позволяет более детально рассматривать и ныне существующие системы, выявлять их недостатки, противоречия, способные играть роль в последующих деконструкциях и фазах отрицания. Поэтому само введение становится истоком и началом зарождения проблемы.

1.1. Сетевые коммуникации

Развитие Интернет-коммуникаций, со стороны информационной безопасности, условно можно представить в становлении трёх этапов, каждый из которых вбирает в себя основные характеристики предыдущих, синтезируя их воедино. В начале можно неявным образом выделить три основные формы сетевых коммуникаций: централизованная, децентрализованная и гибридная, на примере приложений Google, BitTorrent и Tor. Но как будет показано далее, в разделе «Парадигмы сетевых коммуникаций», таковые формации являются лишь частными представителями более общих концепций. Поэтому нужно анализировать данный раздел исключительно как начальное представление о развитии, но не как итоговую модель. Таковое описание становится необходимым в установке вектора дальнейшего повествования.

Децентрализация, как первичная форма Интернет-коммуникаций в целом, появляется на фоне академических исследований [4, с.70], повлекших за собой глобальное развитие информационных технологий. Первичная система представляла собой не только внешний прогресс, относительно себя, но и имманентную эволюцию, выявляя в своей реализации отрицательные стороны и внутренние противоречия. Фактором дальнейшего развития и одновременно гибели стала проблема масштабируемости связей типа «клиент-клиент». Сложность в построении широковещательных и широкомасштабных соединений

постепенно влекло за собой потребность в промежуточных узлах, основаниях концентрации линий связи типа «клиент-сервер», тем самым, зарождая ядро централизации, как основную точку отчёта всей дальнейшей проблематики.

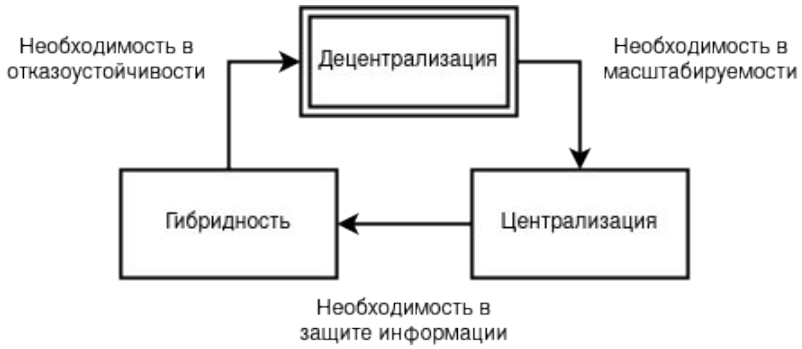

Рисунок 2. Условное развитие Интернет-коммуникаций посредством решения недостатков предыдущих формаций

Централизация, как вторая форма развития Интернет-коммуникаций, появляется на фоне разложения и отмирания первичной, децентрализованной оболочки [5]. Представляя свои плюсы масштабируемости, централизация начинает претерпевать внутренние этапы развития, как итерации наложения слоёв абстракций и отрицания децентрализации, противоречиво становясь для последней фазой её собственной эволюции. При каждой новой итерации своего прогресса, централизованная система всё сильнее масштабируется, всё более углубляется корнями, всё чаще репрезентирует себя, образовывая тем самым симулякры [6, с.151] второго порядка. Одновременно с этим, система постоянно и планомерно нейтрализует внешние атаки, ранее являвшимися губительными для её ядра, но ныне безвредными для её функционирования, подобно атакам в обслуживании [4, с.869] (DDoS) или эксплуатации уязвимостей с учётом изъятия внутренней информации сторонними лицами. С течением времени, продолжая развиваться и масштабироваться, система постепенно начинает порождать общество всё более абстрагируемое от понимания её первичного механизма, всё более догматичное и фрагментированное. Инициатор системы становится её созерцателем, система становится воспроизводством созерцателей. В итоге централизованная структура запускает инициализацию своих внутренних интересов, инвертированно направленных на пользователей, тем самым кардинально изменяя способ взаимодействия с ними. При выстроенном императиве, система начинает образовывать множество симулякров третьего порядка ориентируемых на незначимость или скрытность истинного уровня безопасности, подменяя реальность иллюзорностью происходящего в своём внутреннем слое за полями «сконфигурированных» абстракций. Итогом таковых ложных представлений становится «театр безопасности» [7], направленный на поддержание имеющегося порядка вещей (системы), с целью сокрытия реального уровня соблюдаемой конфиденциальности.

Внешние угрозы информационной безопасности хоть и становятся полностью безвредными для централизованных систем в ходе их постоянной, постепенной и планомерной эволюции, но такое утверждение ничего не может говорить об отсутствии внутренних угроз. Само масштабирование начинает порождать внутренние угрозы, быть противоречием системы, её развитием и конечным отмиранием. Всё большее расширение, продолжительная концентрация связей, неостановимая монополия соединений вызывают аккумулятивную реакцию внутренних интересов её же участников. Внутреннему сотруднику компании теперь становится выгодно продавать информацию об её пользователях при всё

большем расширении системы; государству становится выгодно концентрировать линии связи в одном сингулярном пространстве, открывая более удобный спектр возможностей контроля за обществом и его деятельностью; рекламодателю становится выгодно вкладывать свои средства в массовую систему с наиболее релевантным алгоритмом выдачи рекламы на базе конфиденциальной информации клиентов, повышая тем самым свою прибыль [8][9]. В результате, вышеприведённые проблемы информационной безопасности становятся неразрешимыми централизованными системами, потому как последние продолжают руководствоваться исключительно механизмом неостановимого стремления к собственной масштабируемости и постоянной репрезентации, за счёт чего самолично, неосознанно и планомерно продолжают возобновлять эти же самые проблемы. Таким образом, жизнь централизованных систем начинает постепенно и прямо пропорционально зависеть от количества и качества выстроенных слоёв абстракций, от форм без содержания, от копий без собственных оригиналов, направленных на единственного созерцателя и зрителя данного спектакля – клиента системы, лишь с той единственной целью, чтобы доказать своим «совершенным» существованием финальность и фатальность централизации.

Гибридность, как третья форма развития Интернет-коммуникаций, начинает отрицать централизацию, как нежизнеспособную систему в условиях защиты информации, и в то же самое время, синтезировать результат отрицания с децентрализацией. Оставляя масштабируемость, но отрицая внутреннее развитие централизации, образуется синтез внешнего развития децентрализации, как способа транспарентного доказательства функционирования без слоёв абстракций и симулякров третьего порядка. Такая система становится маловосприимчивой к внутренним и внешним атакам, т.к. более не существует внутреннего сотрудника, разглашающего данные клиентов; государству становится не под силу эффективно контролировать информацию; рекламодателю становится невыгодно вкладывать свой капитал. Подобный прогресс являет собой также и относительный регресс, потому как сама жизнеспособность системы начинает зависеть от участников выдвигающих себя на роль её поддержания, подобно энтузиастам, волонтёрам или нодам, способным получать прибыль от донатов или внутреннего механизма (криптовалюты). В любом случае, в таких системах более не существует постоянного финансирования, а централизованные системы, в частности и само государство, начинают быть враждебными к её существованию [10]. Порождённость централизацией и враждебность к ней становятся ключевыми факторами противоречия и главным фактом последующего разложения гибридности, посредством её планомерного разделения, расщепления и совершенствования.

Децентрализация, как четвёртая форма развития Интернет-коммуникаций, становится масштабируемой и одновременно безопасной средой для пользователей. Более не существует проблем гибридности, потому как ликвидировать систему централизацией с этого момента становится невозможным из-за её полностью ризоморфного характера, как отрицания иерархического. Любой пользователь становится в конечном счёте олицетворением самой системы, её участником и формой поддержания. На данном этапе безопасность информации начинает эволюционировать и переходить на более качественную ступень безопасности её субъектов. Система децентрализованная, в ходе продолжительной и поэтапной эволюции, лишается всех своих первичных недостатков начальной формы и становится, в конечном счёте, снятием итераций отрицания в лице ранее забытого типа связи «клиент-клиент».

1.2. Влияние централизации

В настоящее время лидирующей формой выражения сетевых коммуникаций является вторая ступень развития. Централизованная оболочка становится наиболее долгоживущей средой, потому как таковая вбирает в себя наибольшее количество противоречий, парадоксально успешно сочетающихся между собой. Запутанность подобных связей отодвигает время их конечного распутывания посредством создания альтернативных решений. И действительно, предыдущая система, а также все последующие представляют собой в неком роде примитивы, явно обладающие своими преимуществами и недостатками, но что важнее всего – отсутствием явных противоборствующих сторон внутри самой системы.

В отличие от других систем, в централизованных открыто прослеживаются два вида дифференцированных интересов, где с одной стороны находятся обладатели сервисов связи, с другой – пользователи этой системы. Первым становится выгодна такая парадигма вещей, потому как они овладевают всей информацией проходимой через них и хранимой у них. Это выгодно не только со стороны экономического влияния (реклама, продажа конфиденциальной информации, явные и неявные подкупы и т.д.), но и со стороны политического контроля (пропаганда государственной или маркетинговой позиции, блокирование оппозиционных или «неправильных» мнений, явные и неявные шантажи, лоббирование интересов и т.д.). Само влияние, как тень, накладывается на субъектов подобных сервисов, поэтапно переводя их в категорию типичных объектов исследования рынка. Вторым становится выгодна парадигма использования сервиса без какой-либо нагрузки на своей стороне, с условиями хорошего соединения, большого хранилища и качественного дизайна UX/UI (user experience / user interface). Внешнее представление таковых действий становится с одной стороны неким описанием симбиоза, когда сервисы создают всю инфраструктуру для клиентов с целью своего будущего экономического и/или политического влияния, в то время как пользователи начинают использовать данную систему для комфортной взаимосвязи с другими её участниками. С другой стороны эти же действия становятся последующей формой паразитизма сервисов над её участниками, потому как вектор развития сервисов при достижении N-ого количества клиентов, при достижении некой критической массы, перевоплощается, интвертируется и становится, в конечном итоге, платформой связи живущей не для клиентов, а за счёт них. Теряя из виду причинно-следственную связь жизнеспособности данного механизма, пользователи перестают осознавать на сколько масштабной начинает быть итоговая система сбора личной и конфиденциальной информации. Ироничным образом таковые клиенты становятся единственной моделью противопоставления сервисам связи, единственной силой способной изнутри разрушать системы, живущие за счёт них, а не для них. Если таковые субъекты смогут не только найти, но и успешно перевести все свои возможные интересы на иные системы, представляющие близкие к ним стремления – интересы большинства, то централизованные механизмы постепенно и поэтапно начнут замещаться гибридными, децентрализованными альтернативами, начнут отмирать и, в конечном счёте, станут формой остатка всего множества сетевых коммуникаций.

В настоящее время можно наблюдать явный факт зарождения альтернативных систем, где гибридные становятся всё масштабнее в применении (Bitcoin, Tor), а одноранговые в некоторых аспектах становятся даже более эффективным аналогом многоранговых систем, на примере протокола BitTorrent при передачи файлов [11]. Такие действия должны были бы приводить к скорейшему отмиранию централизации как таковой, но в реальности этого не случается, потому как централизация обладает свойством долгоживучести, являющимся

ключевым и многофакторным сценарием, обуславливаемым нижеизложенными составляющими.

1. Явные интересы одних (прибыль, контроль) и абстрактные интересы других (коммуникация, поиск информации) приводят последних лишь к пассивным возражениям, бунтам без какого-либо сокрушительного результата при понимании бесконтрольности ими генерируемой информации. С другой стороны, как раз такое противоречие является наиболее важным, потому как оно инициирует медленное, поэтапное, но всё же развитие альтернативных решений. Примером такого поведения стала в своё время гласность проекта PRISM [12], которая смогла сыниициировать массовые недовольства населения всего мира, а также развитие приложений нацеленных на безопасность информации и анонимность пользователей. Тем не менее, никакого фатального результата такая ясность не принесла. Все созданные приложения становились лишь частным случаем более общей коммуникационной модели, а монополии и корпорации всё также продолжили сотрудничать с государственным аппаратом.

2. Комфортность использования сервисов начинает постепенно и неявно накладываться на текущий уровень безопасности, в некой степени отодвигая его на второй план, потому как конечные клиенты, с большей долей вероятности, начинают выбирать более производительную систему, чем безопасную и медленную [13, с. 239]. Со стороны компаний и корпораций дизайн может диктоваться, видоизменяться, подвергаться моде, тем временем как безопасность остаётся всегда процессом без окончания, сложным, невидимым, и как следствие, менее значимым для обычных пользователей. Подобная дифферентная реакция клиентов на комфортность и безопасность становится в определённой степени выгодна производителю за счёт снижения затрат на реальную безопасность разрабатываемых или поддерживаемых систем.

3. Централизованные системы по своей экономической природе всегда движутся к концентрации соединений, своеобразной монополии, из-за чего множество сервисов явным и неявным образом начинают объединяться, расширяться, срастаться, что также может приводить к более успешным подавлениям иных систем – гибридных, децентрализованных или малых централизованных вследствие конкуренции. При достижении определённой критической массы концентрации соединений централизованные системы начинают выстраивать за счёт экономического влияния – политическое, вследствие которого штрафы (со стороны самой компании) за утечку информации становятся меньше стоимости найма специалистов по информационной безопасности, где не малую роль играют антимонопольные компании, являющиеся всё таким же порождением централизованных механизмов, редко по настоящему и на практике противостоящим монополиям [14][15][16]. При таком сценарии, репрессивные меры, направленные на уменьшение количества и качества утечек информации (со стороны внутренних сотрудников компании), начинают нести более юридический характер [17]. В следствие всего этого, монополистическим централизованным системам становится избыточна реальная безопасность.

4. Экономический базис существования централизованных систем не позволяет выйти из существующего императива вещей, потому как сама централизация является

лишь следствием экономической необходимости в управлении ресурсами, в том числе и человеческими. Разрыв парадигмы приведёт неминуемо к банкротству и к факту последующего поглощения остаточных ресурсов другой, более успешной централизованной системой.

5. Централизованные системы представляют собой более гибкие формы при создании новых коммуникационных технологий, потому как игнорируют, либо минимизируют безопасность клиентской составляющей и располагают всеми нужными ресурсами, а также всей необходимой пользовательской информацией для осуществления успешных итераций обновления. Таковые свойства позволяют централизованным механизмам быстрее разрабатывать и эффективнее внедрять новые решения, опережая на несколько шагов альтернативные системы.

6. Децентрализованные системы обладают свойством «коррозии» централизованными формами [18]. Такое свойство является следствием высокой стабильности централизованных коммуникаций, при которых децентрализация всегда будет стремиться к выстраиванию более быстрых, качественных соединений за счёт установления ограниченного множества стабильных или стабилизирующих узлов, что неминуемо будет приводить к концентрированию последующих соединений и к относительному регрессу ризоморфных составляющих.

Таким образом, развитие постцентрализованных сетевых коммуникаций становится делом далёкого будущего. Противоречий накапливается с каждым разом всё больше, что продолжает играть двоякую роль. С одной стороны противоречия приводят систему к собственному отмиранию за счёт выявления явных недостатков, которые приходится постепенно решать и исправлять. С другой стороны большое количество накопленных противоречий также становится и фактором сдерживания к отмиранию системы за счёт необходимости в более длительном анализе её составляющих. В любом случае, на гниющей, разлагающейся и репрезентируемой, самовосстанавливающейся почве уже виднеются малые ростки будущих сетевых коммуникаций, способных обеспечивать настоящий, а не фиктивный, уровень безопасности конечных пользователей, защищающий их личную и конфиденциальную информацию. Всё дальнейшее изложение нашей статьи будет акцентировано на анализе подобных систем.

1.3. Основная проблематика

При рассмотрении вопросов, базируемых на безопасности каналов связи, использующих криптографические протоколы с участниками *A* – отправителем и *B* - получателем, а также с доверенным участником *T*, концентрация внимания сосредоточена в большей мере как раз на последнем. Это логично, ведь доверенный, промежуточный субъект информации *T* становится «законно» установленным атакующим первоначальными субъектами *A* и *B*, способным совершать MITM атаки (man in the middle) и переводящим систему в неустойчивое состояние, состояние требующее абсолютного доверия [19].

Приведённая атака ссылается на нерешённую проблему доверия[2], разрушительную и губительную по своей сути, но при этом затмевающую более скрытую и деструктивную, мощь которой в современном мире превосходит прямолинейные MITM атаки. Одной из задач нашей статьи является выявление данного метода нападения, его анализ и последующие решения.

Возможность атаки со стороны принимающего субъекта *B* есть суть проблемы, возникающая на фоне криптографических протоколов адаптируемых под защиту связи «клиент-сервер», где сервер выдвигается как получатель информации, а клиент как отправитель. При этом, в большинстве случаев, сервер вовсе не является настоящим получателем, а представляет собой лишь промежуточный, интерстициальный узел, как это изображено на *Рисунок 3*, целью которого является связывание двух и более клиентов между собой, образуя тем самым условно новый тип связи «клиент-клиент», который в свою очередь полностью игнорируется криптографическими протоколами. Такая проблема критична в самом базисе компьютерных сетей, т.к. выдаёт всю информацию субъектов (интересы, сообщения, контактную информацию, политические взгляды и т.д.) в предельно открытом, прозрачном, транспарентном состоянии субъекту-посреднику [20][21]. Примером такого явления могут служить современные мессенджеры, социальные сети, форумы, чаты, файловые сервисы и т.д., где общение не происходит напрямую, как это предполагается во множестве криптографических протоколов, а всегда проходит сквозь стороннюю точку, представляющую собой сервис или платформу связи.

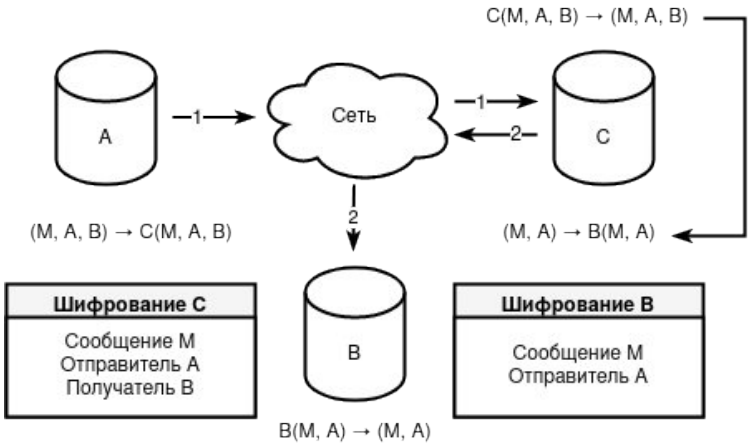

Рисунок 3. Коммуникация субъектов *A*, *B* посредством общего сервиса *C*

Описанное явление начинает претерпевать кардинальные изменения, т.к. возвращает фундаментальную проблему и задачу классической криптографии — борьбу с прослушиванием, которая должна была решиться (и решилась теоретически) лишь с появлением раздела асимметричной криптографии [22]. Данная апория куда серьёзнее и значимее, нежели классическая MITM атака и требует куда меньшее количество затрат

[2]Проблема доверия — невозможность построения безопасной, монолитной и саморасширяющейся системы, основанной полностью на криптографических алгоритмах для конечных субъектов, без использования промежуточных узлов, удостоверяющих идентификацию абонентов, либо без сторонних каналов связи с заранее установленным доверием. Задача возникает на фоне сложности передачи публичных ключей. В децентрализованных, ризоморфных системах данная проблема куда более значима, т.к. оставляет лишь метод использования сторонних каналов связи, то-есть прямого доверия, через которое уже может образовываться сеть доверия.

атакующего для слежки большего количества атакуемых. Это становится паноптикумом современного общества, где атакующие и атакуемые меняются местами, инвертируют способ слежения и делают заложника инициатором собственного подслушивания. Теперь жертвы самостоятельно подключаются к заведомо прослушиваемой связи, выбирают множество возможных опций слежения за собственным «Я», в то время как атакующие лишь создают аналогичные соединения, воспроизводят платформы слежения в таком необходимом количестве, чтобы затмевать своим присутствием сам факт существования более защищённых альтернатив. Таким образом, с одной стороны конфиденциальность современных сервисов становится лишь декорацией, театром безопасности, симулякром ссылающимся на несуществующую, гипостазированную безопасность, как на магическое слово маркетинга, а с другой стороны само удобство сервисов начинает быть фундаментом, мыслью, философией, пропагандой противопоставляющей себя безопасности, конкурирующей с ней, постепенно и незаметно заменяющей её, как «Cymothoa exigua».

Таковое развитие инициализирует возникновение систем доверия, где не только сами доверительные узлы становятся атакующими, но и промежуточные получатели, что приводит к куда более значительным и значимым рискам компрометации хранимых и передаваемых объектов между истинными субъектами. Эволюционируя, система начинает поддерживать неявные соединения между разнородными платформами связи, дублируя информацию на множество платформ с целью последующего массового сбора информации, обмена, маркетинга и продажи релевантной рекламы. В результате все вышеописанные факторы приводят к явному нарушению конфиденциальности конечных пользователей системы с определённым деанонимизирующим последствием.

Тем не менее безоговорочно аннигилировать такую систему доверия не представляется возможным из-за реального ухудшения оптимизации и производительности программ, последующих трудностей построения архитектуры приложений, и в конечном счёте, из-за невозможности полного искоренения доверия как такового [23, с.267]. Таким образом, необходимо не уничтожать, а заменять данную систему более безопасной, отодвигать её на второй план, в нишу, в которой только она способна быть полезной. Во всех других случаях, необходимо строить и разрабатывать иные системы, механизм которых стремился бы к уменьшению мощности доверия[3], в которых собственная структура представляла бы защиту объектов и анонимат субъектов. К системам подобного рода уже частично относятся анонимные сети, клиент-безопасные приложения и тайные каналы связи, анализ и развитие которых представлено в последующих разделах и подразделах.

2. Парадигмы сетевых коммуникаций

Все сетевые коммуникации строятся на определённых топологиях, архитектурах задающих последующее их применение. Топологию можно рассматривать как со стороны

[3]Мощность доверия — количество узлов, участвующих в хранении или передаче информации, представленной дли них в открытом описании. Иными словами, такие узлы способны читать, подменять и видоизменять информацию, т.к. для них она находится в предельно чистом, прозрачном, транспарентном состоянии. Чем больше мощность доверия, тем выше предполагаемый шанс компрометации отдельных узлов, а следовательно, и хранимой на них информации. Принято считать одним из узлов получателя. Таким образом, нулевая мощность доверия $|T| = 0$ будет возникать лишь в моменты отсутствия каких-либо связей и соединений. Если $|T| = 1$, это говорит о том, что связь защищена, иными словами, никто кроме отправителя и получателя информацией не владеют. Во всех других случаях $|T| > 1$, что говорит о групповой связи (то-есть, о существовании нескольких получателей), либо о промежуточных узлах, способных читать информацию в открытом виде.

более низкого уровня, вида «звезда», «ячеистая», «шина», «кольцо» и т.п. [24][25], так и со стороны более прикладного уровня, как «многоранговая», «одноранговая», «гибридная» [26]. На первый взгляд, таковые определения дают однозначные соответствия: «многоранговая» = «звезда» ИЛИ «звезда + иерархическая» ИЛИ «иерархическая», «одноранговая» = «ячеистая» ИЛИ «полносвязная», «гибридная» = «иерархическая + полносвязная» ИЛИ «звезда + ячеистая» и т.д. Но по мере изучения будут явно прослеживаться противоречия таковых суждений, при которых «одноранговая» архитектура может становиться «звездой», «гибридная» – «иерархической» и прочее.

За основу терминологии сетевых архитектур будет браться именно прикладной уровень, т.к. низкоуровневый, в большей мере, описывает не как само взаимодействие субъектов между собой, а как способ технической коммуникации между таковыми точками. Если выбирался бы низкоуровневый подход в плане описания, то он несомненно порождал бы дополнительные противоречия, при которых, как пример, иерархическая система становилась бы системой децентрализованной. В это же самое время, многоранговая архитектура, изучающая взаимодействие субъектов между собой, предполагает, что таковая иерархичность как раз наоборот является следствием централизованности системы.

2.1. Сетевых архитектуры

Многоранговые сети делятся на две модели: централизованные и распределённые. Централизованная или классическая клиент-серверная архитектура является наиболее распространённой моделью из-за своей простоты, где под множество клиентов выделяется один сервер, выход из строя которого приводит к ликвидации всей сети. Распределённая многоранговая система предполагает множество серверов, принадлежащих одному лицу или группе лиц с общими интересами, на множество клиентов, тем самым решая проблему уничтожения сети при выходе из строя одного или нескольких серверов. Из вышеописанного также следует, что классическая централизованная структура является лишь частным случаем более общей распределённой модели, или иными словами, сам факт распределённости становится следствием централизации. Сети на основе многоранговой архитектуры расширяются изнутри, относительно своего ядра, и не допускают расширения извне.

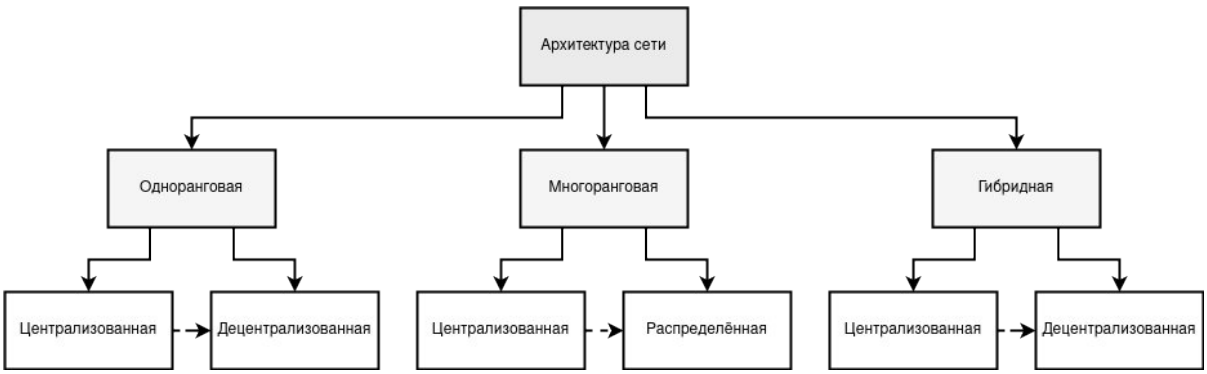

Рисунок 4. Сетевые архитектуры и их декомпозиция в моделях

В одноранговых (peer-to-peer) системах все пользователи однородны, имеют одинаковые возможности, могут представлять одни и те же услуги маршрутизации [4, с.792]. Сами одноранговые сети могут быть разделены на три модели: централизованные, децентрализованные и распределённые (последняя – условно). Централизованные

одноранговые сети представляют собой соединения на базе одного или нескольких, заранее выделенных или динамически выделяемых серверов-ретрансляторов, исключение которых приводит к блокированию всей сети. Отсутствие прав серверов в такой модели начинает порождать равноправность их клиентов. Распределённые сети не выделяют какой-либо центр или узел связи, сохраняя факт одновременной и полной коммуникации узла со всеми другими узлами, иными словами, со всей сетью. Иногда под распределённой связью подразумевают также необходимое *N*-ое количество соединений, необязательно со всей сетью. В децентрализованных сетях становится возможным образование неравномерного распределения соединений и появление «неофициальных» узлов-серверов, часто используемых другими узлами в качестве последующей маршрутизации. Таким образом, децентрализованная модель, в своём определении, начинает быть более подверженной концентрированию линий связи, чем распределённая модель. Тем не менее, распределённая модель является лишь конфигурацией децентрализованной и полноценно, в отрыве от последней, рассматриваться не может. Сети на основе одноранговой архитектуры расширяются извне, за исключением начальной фазы одноранговой централизации.

Гибридная система объединяет свойства многоранговых и одноранговых архитектур, пытаясь взять и удержать как можно больше положительных и меньше отрицательных качеств. Сама гибридность системы может рассматриваться в разных значениях и проявлениях, как пример на уровне топологий: «шина + кольцо», «кольцо + полносвязная», «звезда + ячеистая» и т.д., или на уровне прикладного рассмотрения: «одноранговая + многоранговая». Плюсом многоранговых архитектур становится возможность разделения логики на серверную и клиентскую, а также более быстрая и/или статичная скорость маршрутизации. Плюсом одноранговых архитектур становится высокая отказоустойчивость за счёт внешнего расширения сети и возможность построения безопасной, а также масштабируемой «клиент-клиент» связи. Минусом гибридных архитектур на ранних стадиях развития является их возможный, осуществимый и более вероятностный переход в многоранговые системы (по сравнению с одноранговыми) за счёт большого уплотнения серверов принадлежащих одному лицу, либо группе лиц с общими интересами.

2.2. Архитектурные модели

Развитие сетевых архитектур в плане синтеза безопасности и анонимности проходит вследствие движения принадлежащих им моделей. Весь нижеизложенный анализ данного раздела будет действенен только в пределах исторически-длительного развития скрытых систем и не пригоден к обширному историческому анализу всего развития одноранговых, многоранговых или гибридных сетевых архитектур в целом. Так например, если отбросить определения безопасности и анонимности, а взять в качестве основы только сетевые коммуникации, то ARPANET, являясь зарождением первой формы одноранговой децентрализации, порождает сеть Интернет, которая становится второй, финальной, эволюционированной формой одноранговой децентрализации, что будет на корню противоречить нижесказанному. Также, если исходить только из безопасности, игнорируя при этом полностью или частично анонимность, то исторически сеть Napster, являясь одноранговой централизованной моделью, моментально (после своего отмирания) порождает одноранговую децентрализованную сеть Gnutella, как синтез многоранговой и одноранговой централизации, что также противоречит части нижесказанного, потому как исключает фазы и этапы возникновения гибридных архитектур. Далее, если же исходить только из анонимности, игнорируя безопасность, то исторически становится невозможным целостное определение многоранговой архитектуры, потому как таковая, становясь

отрицанием анонимности, становится одновременно и её исключением. Через исключение в свою очередь становится невозможным целостное рассмотрение многоранговой распределённой модели, потому как таковая в своей совокупности начинает уже содержаться в гибридных архитектурах, которые и становятся способными самостоятельно воссоздавать первично качественную анонимность, что является непосредственным противоречием. Таким образом, весь нижеизложенный материал необходимо пропускать через призму развития безопасности и анонимности как единого неразрывного целого.

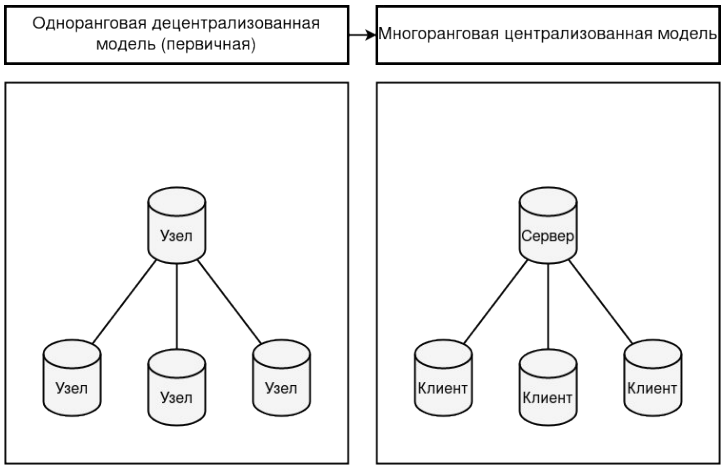

Рисунок 5. Становление многоранговой архитектуры из первичной одноранговой децентрализованной модели

Становление многоранговой централизованной (классической) системы является следствием отрицания одноранговой начальной децентрализованной модели, как формы нежизнеспособной к нарастающим реалиям масштабируемости. На данном этапе одноранговый узел, словно единая личность, расщепляется, чтобы собраться вновь, на два субъекта – клиента и сервера. Таковое разделение предполагает разграничение прав между обработкой информации со стороны сервера и её инициализацией со стороны клиента. В подобной системе информация становится отчуждённой от её первичного создателя и переданной в «руки» сервиса хранения. Клиентам, в такой парадигме, становится избыточно, проблематично, и даже архаично, создавать прямолинейные связи между друг другом, потому как их информация благоприятно начинает переходить в удобочитаемое и отсортированное состояние без добавочных проблем и трудностей в плане ручной настройки соединений и способа хранения данных. Инициализация единой точки отказа становится главным фактором развития иерархичности, но никак не точкой сопутствующего разрушения, как это было с первичной децентрализацией, когда таковая не могла эволюционировать без собственной деструктуризации. Когда многоранговая классическая, централизованная система начинает нести бремя значительных рисков компрометации всей хранимой информации она прогрессирует, вбирая в себя частично свойства первичной децентрализации и подстраивая их под собственный императив. Таким образом начинают зарождаться многоранговые распределённые системы.

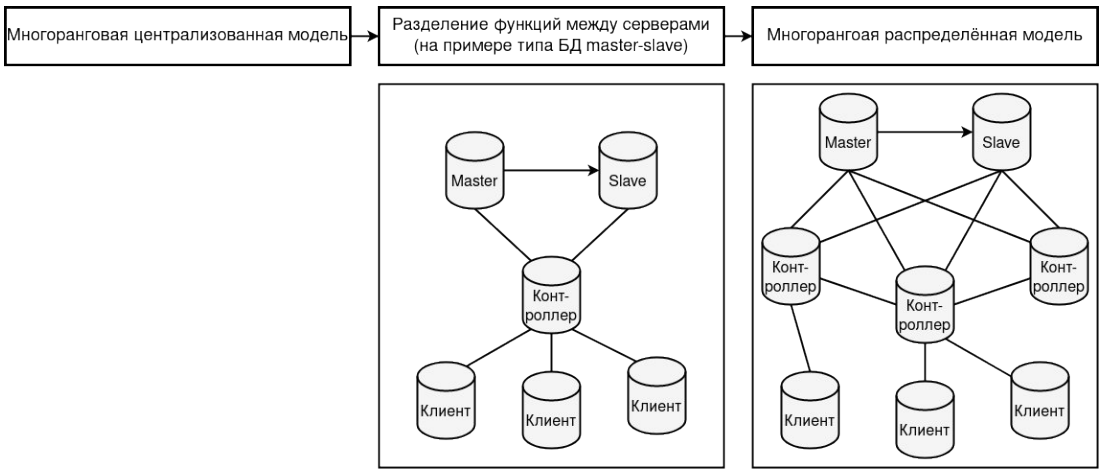

Рисунок 6. Развитие многоранговой архитектуры на примере типа БД «master-slave»

Становление многоранговой распределённой системы из классической централизованной является важным составляющим фактором эволюции существующих иерархических сетей. Данное «разложение», как отрицание явной централизации, начинается на этапе разделения функций, приравнивая сервер к определённому действию, как это изображено на *Рисунке 6*. В такой начальной фазе, сервера становятся взаимосвязанными общей целью обслуживания, но не скованными выполнением общих задач. Из этого следует, что отказ в обслуживании одного сервера начинает влиять только на частную задачу (текущего сервера) и продолжает влиять на общую цель (группы серверов). Таким образом, затрагивая один сервер, сама система продолжает функционировать, хоть и не выполняя полный спектр запланированных действий. Последующей фазой развития уже становится взаимозаменяемость серверов, выполняющих узкоспециализированную задачу, посредством их дублирования, тем самым решая проблему отказоустойчивости в целом. В данном контексте стоит заметить, что иерархичность структуры продолжает сохраняться, даже при добавлении множества серверов с однородными функциями, не перерастая в одноранговую систему полноценно. Представленное явление проходит в следствие внутреннего алгоритма расширения системы, доступ к которому осуществляется наиболее высшими звеньями уже существующей и выстроенной иерархической цепи, а также в следствие бессмысленности существования узкоспециализированных одноранговых узлов вне всей системы. Поэтому, даже если внутри централизованных систем будет существовать *N*-ое количество одноранговых, сама сеть не перестанет быть многоранговой, до тех самых пор, пока будет существовать механизм восстановления и удержания иерархичности, а также до тех пор, пока одноранговые узлы будут оставаться специализированными конкретным задачам. Т.к. иерархичность в любом своём проявлении является следствием централизации, её закономерным развитием, то во всех последующих упоминаниях под термином «централизация» будет пониматься именно конечная фаза эволюции многоранговой архитектуры — распределённая модель.

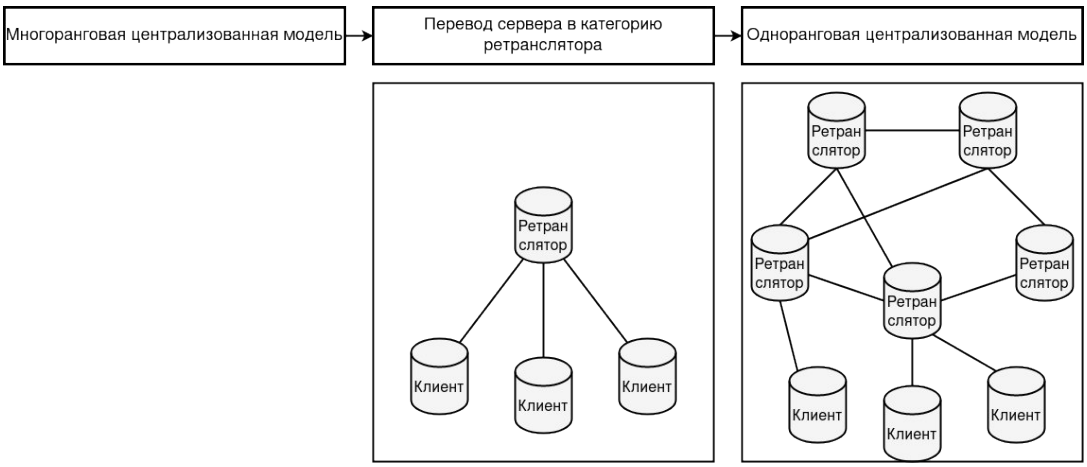

Рисунок 7. Становление одноранговой централизованной модели на примере перевода категории сервера в категорию ретранслятора

Становление одноранговой централизованной системы является следствием «переосмысления» многоранговой централизации, её отрицанием. Инвертируя способ взаимодействия между клиентом и сервером, данная модель делает последнего лишь держателем сети, придатком коммуникаций. В такой системе все пользователи становятся однородными и равноправными только за счёт отсутствия прав сервера, главной функцией которого, в конечном счёте, становится перенаправление информации между клиентами сети. Вследствие этого, сервера в одноранговой централизации лишаются дополнительных прав многоранговой архитектуры, лишаются быть полноценными посредниками между несколькими субъектами, тем самым и лишаются функций сохранения, обработки и выдачи получаемой информации. При поверхностном анализе, централизация одноранговая, как этап развития сетевых коммуникаций, становится лишь упрощением централизации многоранговой. При более же углубленном анализе выявляется, что таковая модель способна не только дублировать сервера практически в неограниченном количестве (за счёт отсутствия какой бы то ни было логики кроме ретрансляции), что частично отсылает нас к способу функционирования многоранговой распределённости, но также и расширяться извне, что присуще более одноранговым архитектурам. Таким образом, можно утверждать, что одноранговая централизация[4] становится в некой степени альтернативным вектором развития многоранговой централизации.

[4]Одноранговая централизованная модель, в своём финальном проявлении, является достаточно отказоустойчивой системой, потому как позволяет ретрансляторам расширяться извне, тем самым ликвидируя потенциальную зависимость и уязвимость от многоранговых систем. Примером начальной формы одноранговой централизации может являться сеть Napster, а примерами финальной формы могут выступать такие системы как протокол BitTorrent, в котором под ретрансляторами понимаются трекеры, а также сеть Gnutella2, где под ретрансляторами понимаются хабы (в терминологии данных сетей).

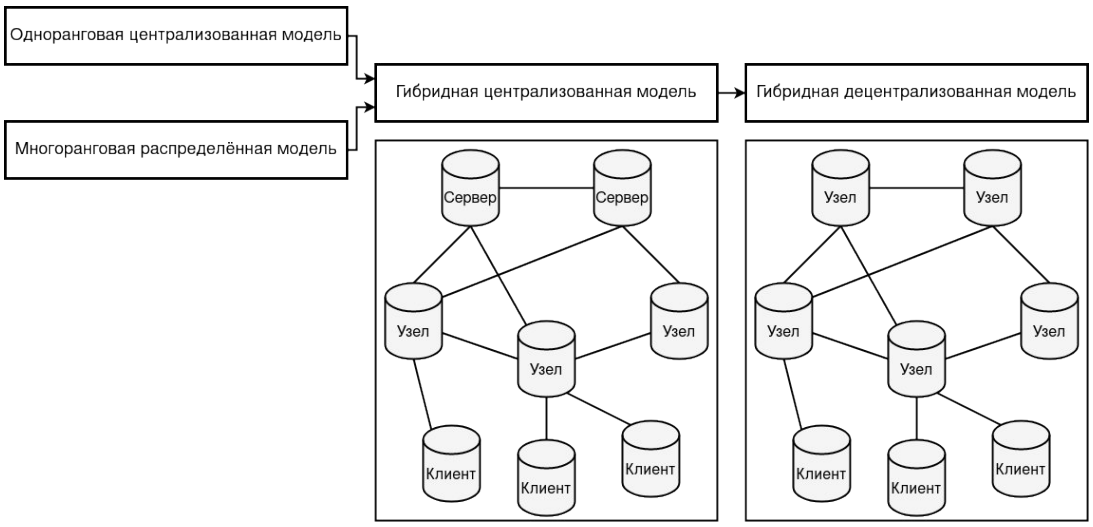

Рисунок 8. Развитие гибридной архитектуры на базе синтеза одноранговой централизованной и многоранговой распределённой моделей

Становление гибридной архитектуры проходит в следствие синтеза одноранговой централизации и многоранговой распределённости. С одной стороны, одноранговая централизация частично избавляет систему от ядра внутренней иерархии, разбавляя её внешними одноранговыми связями. С другой стороны, многоранговая распределённость преобразовывает примитивные редирект-функции, изменяя их форму дополнительными действиями, и тем самым сохраняет внешнюю иерархию между сервером-клиентом. Внешним противоречием гибридности, на первый взгляд, становится сильная схожесть либо с многоранговыми распределёнными моделями, либо с одноранговыми децентрализованными. В совокупности же, гибридная архитектура представляет собой скорее переходное состояние, то-есть фазу развития систем и их моделей, нежели собственное и статичное положение. И действительно, гибридная архитектура описывается как синтез одноранговой централизации с многоранговой распределённостью, являясь причиной их последующей негации, приводимой уже к определению децентрализованной модели одноранговой архитектуры, как единовременного отрицания одноранговой централизации и многоранговой распределённости, то-есть отрицания гибридности. Именно поэтому, гибридная архитектура на этапе своего становления имеет больше свойств схожих с централизацией, где отличительной особенностью данной модели становится способность к единовременному внешнему (свойственно одноранговым архитектурам) и внутреннему (свойственно многоранговым архитектурам) масштабированию. В последующем, по мере своего развития, гибридность претерпевает ряд метаморфозов и становится в конечном счёте неотличимой (относительно некоторого множества субъектов) от децентрализованной модели. Это можно наблюдать на примере сетей Tor и Bitcoin, которые являясь одновременно гибридными, представляют разнородный вид гибридности, где в одном случае Tor более приближен к распределённой модели многоранговой архитектуры (централизованной модели гибридности), а Bitcoin к децентрализованной модели одноранговой архитектуры (децентрализованной модели гибридности).

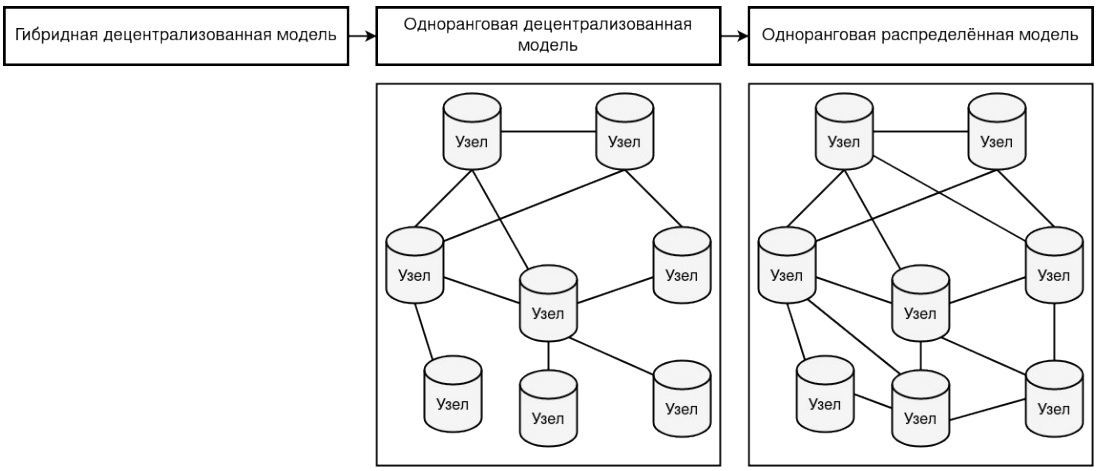

Рисунок 9. Развитие одноранговой децентрализованной модели на примере дальнейшей эволюции в лице распределённой модели

Становление одноранговой (финальной) децентрализованной системы не является прямым следствием развития централизованной модели. Централизация одноранговая по историческим причинам способствовала инициализации децентрализованной философии, но не за счёт последовательных этапов улучшения, а за счёт фактора нежизнеспособности, слабости в «сожительстве» с многоранговой системой [27] в начальной фазе своего существования. Последняя в буквальном смысле «поглотила» примитивную одноранговую централизацию, прервала этап её эволюции, привела к концентрированному методу выстраивания связей и иерархическому способу существования системы. Таким образом, децентрализованная модель должна была стать более качественным выражением и проявлением одноранговой архитектуры, чем централизованная. Итогом такого процесса стало объединение клиентской составляющей с серверной частью, породив тем самым узлы связи, как отдельные сетевые единицы коммуникации, возникшие из эволюции гибридных архитектур. Частным случаем продолжительного развития одноранговой децентрализации является становление распределённой системы, как следствия нарастающей концентрации линий связи со стороны децентрализованной модели, претерпевающей этапы «коррозии» централизацией и приводимой к возникновению «узких» мест среди нескольких сетевых множеств. Противоречием децентрализованных моделей является их постоянное движение к сосредоточению соединений, от хаотичности к порядку, от безопасности к отказоустойчивости, — таковыми становятся основные векторы регресса децентрализации основанные на выборе наиболее стабильных узлов. Решением становится иная и более качественная концентрация линий связи, основанная на объединении узлов посредством многочисленных соединений, в противовес единому центру коммуникаций, и как следствие, фактор стабильности возобновляется, но в уже количественном выражении узлов.

2.3. Замкнутость моделей

Метаморфозы сетевых моделей кратко представляются через призму детерминированного конечного автомата, изображённого на *Рисунке 10*, состояния которого изменяются по мере исторической на то необходимости и направленности. Так например, действия (*a, d, g*) можно рассматривать как необходимость в переосмыслении, во внешнем отрицании, (*b, f*) – необходимость в развитии, во внутреннем отрицании, (*c+e*) – необходимость в объединении, в синтезе отрицаний. Из всего вышеприведённого возможно составить выражения, относящиеся к развитию каждой определённой модели, где

многоранговая централизация = (*a*), многоранговая распределённость = (*ab*), одноранговая централизация = (*ad*), гибридная централизация = (*abc*+*ade*), гибридная децентрализация = (*abc*+*ade*)(*f*) и, в конечном итоге, одноранговая децентрализация = (*abc*+*ade*)(*fg*).

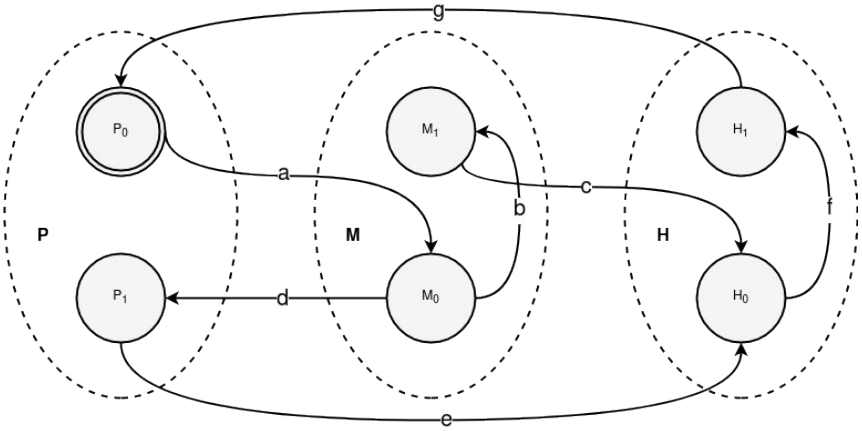

Рисунок 10. Конечный автомат развития сетевых архитектур посредством движения их моделей, где {P, M, H} – сетевые архитектуры: P – одноранговая, M – многоранговая, H – гибридная

На основе этого, стоит отметить, что развитие децентрализованной модели не является примитивно однородным, как это может показаться на первый взгляд, потому как таковая система в своём историческом понимании приобретает двойственное значение. С одной стороны, децентрализация становится первичной формой сетевых коммуникаций, инициализацией и точкой отчёта всех последующих архитектурных решений. С другой стороны, децентрализация, посредством этапов отрицаний и снятия, начинает быть более совершенной формой, и в конечном счёте выражением финализации форм движения сетевых архитектур. Таким образом, по исторически-закономерным причинам, первичная децентрализация вырождается только в многоранговую централизацию, а конечная её форма — в более высокую стадию децентрализации. В итоге, децентрализация становится замыканием всего сетевого развития, одновременно являясь его началом и финалом.

3. Определение скрытых систем

Скрытые системы представляют собой общий и обширный класс сетевых коммуникаций способных поддерживать анонимность субъектов и безопасность передаваемых объектов. В определённой степени таковые системы могут быть нацелены на безопасность передаваемых объектов в степени большей, отодвигая анонимность на второй план, либо наоборот, делая систему анонимной, но полноценно не заботясь о безопасности объекта после получения точкой назначения. Но так или иначе, в любом из представленных случаев таковые системы полноценно никогда не исключают свои второстепенные качества, что даёт возможность определённых комбинаций. При данных композициях сочетаются свойства и безопасности, и анонимности, что делает таковые системы полными. Полные скрытые системы, в свою очередь, являются решением основной проблематики данной работы.

3.1. Анонимные сети

Скрытые, тёмные, анонимные сети — есть сети, соединяющие и объединяющие маршрутизацию вместе с шифрованием. Маршрутизация обеспечивает критерий анонимности, направленный на субъекта, субъектов или их связь, шифрование — критерий конфиденциальности, с опциональной целостностью и аутентификацией, направленный на объект. Без маршрутизации легко определяются отправитель/получатель, без шифрования легко определяется передаваемое сообщение и/или его состояние по ходу факта передачи [4, с.912]. Таким образом, только в совокупности этих двух свойств сеть может являться или оставаться скрытой [28][29].

В современном мире большинство скрытых сетей представляют оверлейные соединения, иными словами соединения, которые основаны на уже существующей сети (например, сети Интернет). Но так или иначе, это не говорит, что скрытые сети не могут существовать сами по себе и быть однородной структурой, т.к. первоначальная архитектура может быть изначально нацелена на анонимность и безопасность, как например, это описано в проекте NETSUKUKU [30]. Именно по историческим причинам, современные скрытые сети имеют оверлейные уровни безопасности.

Любая анонимная сеть основывается либо на одноранговой (ризоморфной), либо на гибридной (комбинированной) архитектуре сети, исключая при этом многоранговую (иерархическую). Последняя архитектура является прямым отрицанием анонимности, направленным на её подавление посредством концентрации линий связи. Гибридная же архитектура совмещает в себе некоторые свойства многоранговой и одноранговой архитектур для большей эффективности в передаче информации, жертвуя при этом некоторыми моделями угроз.

По скорости и способу распространения информации выделяют два вида анонимных сетей – с низкими и высокими задержками [31]. Системы с низкими задержками ставят в качестве базовой необходимости скорость, эффективность транспортирования информации между истинными её субъектами, при этом уровень анонимности таковых сетей недостаточен для противопоставления атакам со стороны внешних глобальных наблюдателей (как доказательство фактора существования сильной анонимности). Системы с высокими задержками ставят в качестве базовой необходимости высокий уровень анонимности, в том числе и направленный на противодействие глобальным наблюдателям, но при этом скорость передачи становится в таковых сетях самым главным недостатком. Из вышеописанного следует классическая проблема проектирования безопасных систем – выбор компромисса между производительностью и безопасностью. В качестве примеров систем с низкими задержками выделяют Tor, I2P, Tarzan и т.д., а с высокими задержками – Mixminion, Herbivore, Dissent и т.п.

Маршрутизация в анонимных сетях не является примитивной и ставит эффективность распространения объектов опциональным параметром (низкие / высокие задержки), потому как главной целью становится создание запутывающего алгоритма (анонимизатора), который приводил бы к трудоёмкости анализа истинного пути от точки отправления до точки назначения. Производительность, эффективность «чистой» маршрутизации теряется, заменяясь особенностью алгоритма. В таких условиях, сами скрытые сети становятся медленными и сложными в применении (в том числе и с низкими задержками), что также частично или полноценно отодвигает их прикладное и повседневное использование в настоящее время.

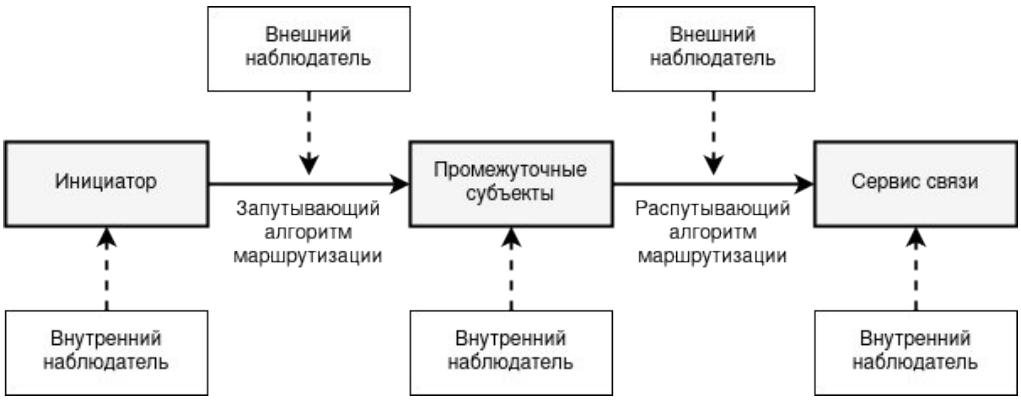

Рисунок 11. Внешние и внутренние наблюдатели (атакующие) в критериях запутывающего алгоритма маршрутизации

В задачах такого типа маршрутизации лежат модели угроз, в которых учитываются возможности атакующих. Главным антагонистом в подобных условиях становится государство, как внешний, глобальный наблюдатель, способный просматривать в широком масштабе распространение объектов по сети. В таком случае алгоритм маршрутизации должен уметь запутывать внешнего противника, не предоставлять возможности выявлять закономерности отправления, получения, запросов и ответов участниками анонимной сети. Другими, и не менее серьёзными противниками, являются внутренние атакующие, когда сами её же участники становятся отрицанием системы, её разложением. Предполагается, что внешние наблюдатели, помимо анализа трафика сети, способны также блокировать работающие узлы в системе, тем самым рассматривая их уникальные комбинации и паттерны поведения. Внутренние же наблюдатели способны наполнять сеть кооперируемыми узлами и совершать помимо маршрутизации также дополнительные действия, как отправление и получение информации. Наблюдатели без дополнительных функций называются пассивными атакующими, в противном случае – активными. В таких реалиях алгоритм маршрутизации должен отстранять буквально каждого субъекта (отправителя, получателя и промежуточного) от полноценного анализа принимаемой и отправляемой информации.

В своей совокупности, в синтезе, сговоре внешних и внутренних атакующих, способны проявляться атаки, которые ранее были бы невозможности по отдельности. Абстрагировано, основные методы нападений, как множества, можно изобразить в виде *Таблицы 1*. При этом, из определения активных атак выясняется, что таковые являются надмножеством пассивных, то-есть $A \in C$ и $B \in D$. Также внешние атаки условно можно разделить на две составляющие, два подмножества: $\{B_1, B_2\}$ и $\{D_1, D_2\}$, где множество $\{B_2, D_2\}$ является представлением внешних атак с глобальным наблюдателем, а $\{B_1, D_1\}$ следовательно без него = $\{B \setminus B_2, D \setminus D_2\}$.

	Внутренние атаки	Внешние атаки
Пассивные атаки	A	B
Активные атаки	C	D

Таблица 1. Пассивные / Активные и Внутренние / Внешние нападения как множества векторов направленных на анонимные сети

Анонимные сети могут обладать разными моделями угроз в зависимости от способа своего применения, а также в зависимости от своих бюджетных или технических ограничений. На основе этого формируется три вида анонимности:

1. Анонимность связи между отправителем и получателем. Представляет слабую модель угроз, потому как даёт возможность наблюдателям фиксировать факты отправления и получения информации истинными субъектами сети. Подобные системы несут малые накладные расходы, и, как следствие, могут применяться в довольно обширном множестве реализаций. Примером таковых сетей являются Tor, I2P, Mixminion.

2. Анонимность отправителя или получателя. Данная сеть имеет усреднённую модель угроз, в том плане, что таковая скрывает только факт отправления или только факт получения информации одним из субъектов (либо отправителем, либо получателем). Подобные системы могут быть хорошо применимы лишь в частных реализациях, как противопоставление анонимности по отношению ко второму субъекту, где не требуется защита отправителя (допустим при обращении к скрытому сервису через ботнет) или получателя (допустим при обращении к сервису в открытом Интернет-пространстве).

Примером таковых сетей может являться сеть, где отправитель транспортирует полностью зашифрованное сообщение всем участникам сети, расшифровать которое может только тот, у кого есть приватный ключ ориентированный на данное сообщение (если здесь конечно используется асимметричная криптография). Теоретически все могут узнать отправителя информации, но узнать получателя и есть ли он вообще крайне проблематично, потому как в теории получателем может оказаться каждый, т.к. каждый получает эти сообщения.

Другим примером может являться сеть, где по определённому периоду генерируется информация всеми участниками сети и отправляется одному серверу посредством нескольких несвязанных между собой общими целями и интересами (не находящимися в сговоре) маршрутизаторов. Получатель-сервер расшифровывает всю информацию и (как пример) публикует её в открытом виде, в следствие чего, все участники сети получают информацию от множества анонимных отправителей.

3. Анонимность отправителя и получателя. Представляет выражение сильной модели угроз, потому как скрывает единовременно и факт отправления, и факт получения информации. Так например, если предположить, что получателю всегда необходимо отвечать отправителю, иными словами воспроизводится модель типа "запрос-ответ", то в такой системе становится невозможным применить "анонимность отправителя или получателя", т.к. отправитель рано или поздно станет получателем, а получатель - отправителем, а потому и модель угроз на базе второго типа начнёт регрессировать и станет моделью на базе первого типа - "анонимность связи между отправителем и получателем". Подобные системы из-за своих вычислительных сложностей и ограничений часто являются малоприменимыми на практике. Примером таковых сетей могут служить DC-сети.

Первый пункт относится к критерию несвязываемости, в то время как второй и третий пункты к критерию ненаблюдаемости [31]. Критерий ненаблюдаемости уже включает в себя критерий несвязываемости. Если пойти от обратного и предположить ложность данного суждения (то-есть, отсутствие несвязываемости в ненаблюдаемости), тогда можно было бы при помощи несвязываемости определить существование субъектов информации и, тем самым, допустить нарушение ненаблюдаемости, что является противоречием для последнего.

Вышепредставленные пункты становятся также проблематичными в плане более подробного описания, потому как становится неизвестным условие – насколько отправитель и получатель анонимны друг к другу, и следует ли считать неанонимность друг к другу нарушением анонимности, тем более, если таковые связи строятся на взаимной деанонимизации друг друга. Поэтому следует учитывать ещё два дополнительных внутренних свойства, относящихся к любому из вышепредставленных пунктов:

1. Система разграничивает абонентов информации. В такой концепции существует три возможных случая: 1) отправитель анонимен к получателю, но получатель известен отправителю; 2) отправитель известен получателю, но получатель анонимен к отправителю; 3) отправитель и получатель анонимны друг к другу. Примером являются 1) анонимный доступ к открытому Интернет ресурсу; 2) анонимное получение информации из ботнет системы со стороны сервера-координатора; 3) анонимный доступ к скрытому ресурсу в анонимной сети.

2. Система связывает абонентов информации. В такой концепции отправитель и получатель способны открыто идентифицировать друг друга по множеству связанных признаков. Системы построенные на данном пункте часто ограничены в своём применении, но, так или иначе, остаются способными представлять анонимность субъектов, в том числе и на уровне критерия ненаблюдаемости.

Скрытыми сетями с теоретически доказуемой анонимностью принято считать замкнутые, полностью прослушиваемые системы, в которых становится невозможным осуществление любых пассивных атак (в том числе и при существовании глобального наблюдателя) направленных на деанонимизацию факта отправления и/или получения информации, или на деанонимизацию связи между отправителем и получателем с минимальными условностями по количеству узлов неподчинённых сговору. Говоря иначе, с точки зрения пассивного атакующего, апостериорные знания, полученные вследствие наблюдений, должны оставаться равными априорным, до наблюдений, тем самым сохраняя равновероятность деанонимизации по N-ому множеству субъектов сети.

Из специфичной формы маршрутизации выявляются критерии на основе которых можно утверждать, что сеть является анонимной. Так например, сети Tor, I2P, Mixminion, Herbivore, Crowds и т.п. являются анонимными сетями, потому как обеспечивают анонимность субъектов за счёт существования запутываемой маршрутизации, и минимальную безопасность объектов в коммуникациях между инициаторами и платформами связи. Сети RetroShare, Freenet, Turtle, Bitmessage и т.п. напротив, не являются анонимными сетями, т.к. маршрутизация представляет собой только сам факт передачи (в некой степени и специфичный из-за гибридного или однорангового характера сетевой архитектуры), транспортирования информации без непосредственного применения запутывающего алгоритма, хоть самолично системы и обеспечивают высокий уровень безопасности объектов.

3.2. Клиент-безопасные приложения

Клиент-безопасные приложения или приложения базируемые на безопасной линии связи «клиент-клиент» представляют собой абстрагирование передаваемых / хранимых объектов от промежуточных субъектов, тем самым приводя мощность доверия $|T|$ к своему теоретически минимально заданному значению. В таких условиях, клиент-безопасные приложения являются ключевым фактором в построении тайных каналов связи. Частным случаем связи «клиент-клиент» становится сквозное (end-to-end или E2E) шифрование [20].

Основным следствием пониженной мощности доверия становится возможность доказательства безопасности приложения, ориентируясь только на его клиентскую составляющую. Это в свою очередь говорит, что ранее существующие сервера, как сервисы связи, теперь являются лишь промежуточными узлами, созданными для транспортирования, маршрутизации, либо хранения информации в полностью зашифрованном или аутентифицированном виде. Любое редактирование существующей или создание ложной информации на стороне сервиса будет сразу же обнаружено клиентской составляющей.

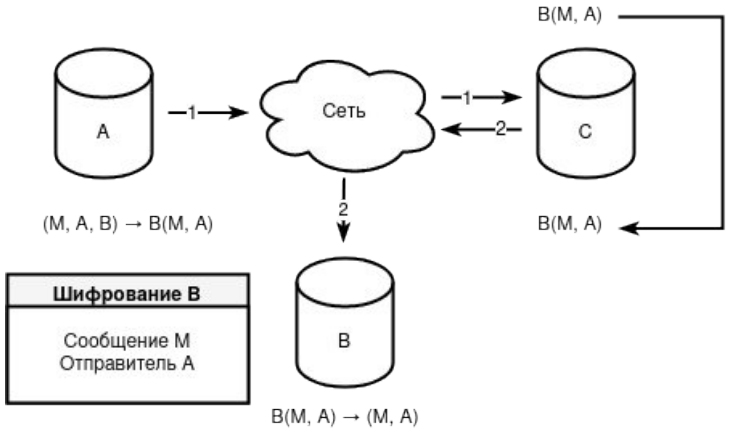

Рисунок 12. Общая схема клиент-безопасных приложений

Одной из основных особенностей таких систем является криптографическая идентификация субъектов информации. Так как подобные системы более не являются многоранговыми, то субъекты становятся неспособными применять в чистом и привычном виде схемы типа «логин/пароль» в целях своей авторизации. Авторизация и последующие аутентификации относительно всех клиентов сети образуются из асимметричной пары ключей. Публичный ключ (или его хеш) становится в конечном счёте идентификацией субъекта, а все посылаемые пользователем сообщения подписываются приватным ключом, тем самым аутентифицируя инициатора связи. Схема «логин/пароль» способна применяться в таких системах, но уже локально, для защиты приватного ключа конкретно выбранного участника сети.

Клиент-безопасные приложения могут быть крайне разнородными в своём проявлении и именно поэтому способны становиться альтернативой классическим сервисам связи. Так например, вполне реальным является замена существующих мессенджеров, социальных сетей, форумов, распределённых хранилищ, цифровых валют и т.д. на приложения с безопасной линией связи типа «клиент-клиент». Таким образом, клиент-безопасные приложения становятся новыми платформами связи, более качественными в своём проявлении, чем классические централизованные альтернативы.

3.3. Тайные каналы связи

Секретные, тайные, эзотерические каналы связи — есть соединения, располагаемые в заведомо замкнутом, незащищённом, враждебном окружении и имеющие характеристики безопасной передачи информации. В отличие от определения [32, с.147], в нашем случаем под тайными каналами будут пониматься системы «неорганически вживляющиеся» в уже существующие сети. При этом анонимность, родственная скрытым сетям, не является базисом секретных каналов связи и, следовательно, может быть отброшена из-за ненадобности или по необходимости. Из такого краткого определения можно выделить две формы тайных каналов связи:

1. Первой формой тайных каналов связи можно считать сохранение экзотеричности субъекта и эзотеричности объекта, благодаря использованию криптографических методов преобразования информации. Но стоит также заметить, что такой принцип сохраняется и при использовании стеганографических методов [33], поскольку субъект остаётся открытым, а объект продолжает быть закрытым (только вместо сокрытия информации, скрывается сам факт её существования). При этом, если в секретных каналах связи используются именно криптографические методы, то они не ограничиваются только идентификацией субъектов (целостностью, аутентификацией), но также и применяют практику шифрования объектов (конфиденциальность). Примером такого поведения может служить использование программ типа PGP [32, с.785][34] на форумах, мессенджерах, социальных сетях.

2. Второй формой тайных каналов связи можно считать скрытые сети с теоретически доказуемой анонимностью, способных имманентно сводить и передавать информацию внутри единого, сингулярного приложения-сервиса, связывающего всех субъектов изнутри. Так как приложение-сервис начинает располагать полным знанием того, кто является отправителем и кто является получателем, то сам сервис становится полным олицетворением сетевых коммуникаций на основе которых может располагаться тайный канал связи. При всём этом, такое приложение, в задаче о тайных каналах связи, аналогично и равносильно глобальному внешнему наблюдателю, в задаче о построении анонимных сетей.

Тайные каналы связи не стоит считать отдельным видом скрытых систем, потому как таковые являются лишь и только способом применения клиент-безопасных приложений или анонимных сетей на специфичном уровне. Тем не менее, всё становится не таким простым и очевидным, как только начинает происходить анализ становления тайных каналов связи. Вкратце, секретные каналы связи представляют собой сетевую абстракцию, которая может рассматриваться как способ инициализации безопасных оверлейных систем. Такое суждение неминуемо приводит к противоречию, потому как начинает инверсивно и рекурсивно указывать иное место в иерархии связей становления скрытых систем, представляя тайные каналы связи инициатором развития анонимных сетей и клиент-безопасных приложений, а не наоборот, как это было описано ранее. Но именно свойство «неорганической вживляемости» является решающим фактором по которому становится невозможным считать тайными каналами связи большинство безопасных оверлейных соединений. Под «неорганической вживляемостью» понимается использование оверлейного соединения поверх прикладного уровня связи, когда первичная система уже полностью выстроилась и функционирует с определённой целью. Поэтому, как пример, нельзя полноценно считать тайными каналами связи безопасные или анонимные сети, базируемые на сети Интернет. Но это не говорит о том, что сама сеть Интернет не может содержать тайных каналов связи на

своём функционируемом уровне. Как пример, определённые поля в протоколе IP (адрес источника = *N*-бит при существовании нескольких принимающих узлов с разными адресами, контрольная сумма = *N*-младших подобранных бит и т.д.) или TCP (порт источника = *N*-бит при существовании нескольких принимающих процессов с разными портами, опции = 2 байта, контрольная сумма подобно примеру из IP и т.д.) могут содержать изменяемые по мере необходимости биты, что способно приводить к распространению (утечке) информации на специфичном уровне работы самой сети. Это как раз и указывает на эзотерический способ применения тайных каналов связи, и подтверждает тот факт, что таковые не образуют соединений и не являются инициализаторами связей, потому как лишь внедряются, на своей «паразитической» основе, в уже существующие сети. Можно также сказать, что тайные каналы связи представляют собой свойство гипертелии (сверх окончания), когда дополняют базовую систему вспомогательными, второстепенными функциями, которыми таковая ранее не обладала.

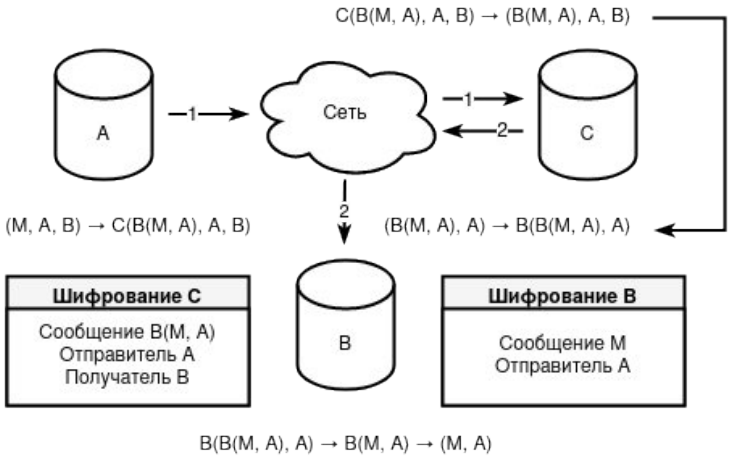

Рисунок 13. Общая схема тайных каналов связи

Тайные каналы связи, использующие стеганографию, всегда имеют некий контейнер, в который помещается истинное сообщение [33, с.8]. Под контейнером может пониматься ложное, неявное, сбивающее с пути сообщение, которое чаще всего носит нейтральный характер. Из этого также следует, что в зависимости от размера контейнера, зависит и размер самого исходного сообщения, тем самым, стеганографический подход рассчитан на сообщения малых размеров и мало пригоден для передачи целых файлов. Примером контейнера может служить изображение, аудио-запись, видео-файл, то есть всё, что может хранить дополнительную или избыточную информацию, которая останется незаметной для человеческих глаз и ушей. Одним из примеров сокрытия информации может служить замена каждого старшего бита в изображении, битами исходного сообщения. Таким образом, если размер изображения (то есть, контейнера) будет равен 2MiB (без учёта метаданных), то максимальный размер исходного сообщения (в лучшем случае) не будет превышать 256KiB.

Использование стеганографии, вместе с криптографией, может помочь в случаях, когда имеется повышенная вероятность или возможность нахождения скрытого сообщения в контейнере за время меньшее, чем необходимое. Тем самым, даже если исходное сообщение было найдено, оно будет иметь шифрованный вид. Здесь стоит учитывать тот факт, что при шифровании размер информации увеличивается (добавляется хеш, подпись, текст дополняется до блока), а из этого уже следует, что максимальный размер исходного сообщения уменьшается.

Существует ещё один, третий способ сокрытия информации, относящийся к криптографическим, но при этом обладающий некоторыми стеганографическими свойствами, качествами, особенностями [32, с.720]. Это не является последовательным объединением, использованием методов, как это было описано выше, а скорее оказывается их слиянием, синтезом и симбиозом. В таком методе истинная информация скрывается в цифровой подписи ложного сообщения на основе общего, согласованного ключа, где главной чертой и исключительностью является стойкость ко взлому, сродни сложности взлома цифровой подписи. При этом, сама подпись — есть контейнер, скрывающий существование сообщения методом аутентификации ложной информации.

Теоретически, тайные каналы связи рекуррентно могут находиться и в других секретных каналах, либо анонимных сетях (по причине того, что тайные каналы связи могут воссоздаваться совершенно в любых системах и ситуациях), тем не менее, подобный подход является очень сомнительным (по причине избыточности накопленных слоёв шифрования), специфичным (по причине редкости практического использования) и затратным (по причине уменьшения производительности программ, уменьшения ёмкости контейнеров).

Из-за высоких накладных расходов (в частности описанных выше), в тайных каналах связи (как правило) не предполагается существование сервисов связи, присущих анонимным сетям, в том числе и в своей второй форме. Иными словами каждый получатель становится конечной точкой маршрута, а не возможным промежуточным субъектом, ретранслирующим информацию истинному субъекту с заранее известным, транспарентным открытым текстом.

4. Развитие сетевой анонимности

Термин «анонимность» представляет собой достаточно сложное и комплексное понятие, потому как таковое всегда зависит от контекста. Так например, анонимность может предполагать собой использование псевдонимов при письме или живописи, использование масок с целью сокрытия лиц при законных и незаконных действиях, в благотворительности с отсутствием каких бы то ни было инициалов, в Интернете с целью сокрытия своего сетевого трафика и т.д. Чтобы дать более точное понимание анонимности, необходимым следствием является сокращение способов использования данного термина. В нашей статье наиболее важной становится анонимность направленная на сетевые коммуникации.

Сетевая анонимность хоть и является более узким термином, или вернее сказать подмножеством термина «анонимность», но до сих пор остаётся комплексным понятием. Единственным отличием становится независимость от контекста, потому как контекстом становится сам факт сетевых коммуникаций как среды исследования. Это и позволяет конкретизировать анонимность, деструктуризировать комплексность и выявлять основные векторы её развития.

4.1. Стадии анонимности

Потому как сетевая анонимность есть объект фрагментированный со стороны определений и терминологий, то можно предположить неоднородность и факт становления, развития в определённых этапах. Вкратце, анонимность становится возможным трактовать как некую градацию, поэтапность, которой присуще шесть стадий, выявляющих процесс её формирования посредством фаз отрицаний и внутренних противоречий.

1. Первая стадия является исходной точкой анонимности, тезисом, монадой примитивно не представляющей анонимность, пустотой инициализирующей мощность

анонимности[5] $|A| = 0$. Примером является существование только прямого, прямолинейного, примитивного соединения «клиент-клиент» между двумя одноранговыми субъектами, что равносильно их стазисному состоянию. По причине отсутствия промежуточных субъектов мощность доверия на данном этапе представляет минимально возможную величину.

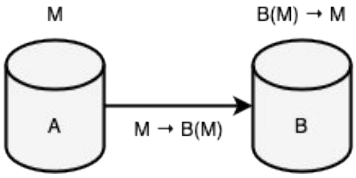

Рисунок 14. Первая стадия анонимности (прямое соединение)

2. Вторая стадия, становясь антитезисом, начинает отрицать первый этап, приводить систему к первичному метастазису, изменять собственным преобразованием способ взаимодействия между субъектами, добавлять к своей оболочке новую роль промежуточного узла, сервера, подчиняющего всех остальных субъектов к частно-личному сервису. Таким образом, архитектура становится многоранговой, клиенты начинают зависеть от платформ связи, а мощность анонимности повышаться до константного значения. Этап обеспечивает (инициализирует) только анонимность «клиент-клиент», но игнорирует при этом анонимность «клиент-сервер», что и приводит к статичной мощности анонимности $|A| = 1$. Иными словами, сервер начинает обладать достаточной информацией о клиентах, клиенты в свою очередь начинают коммуницировать посредством сервера, что приводит их к фактическому разграничению, к взаимной анонимности и зависимости от общей платформы. В данной ситуации стоит заметить, что анонимность и безопасность идут вразрез друг с другом, противопоставляют себя друг другу, т.к. с одной стороны безопасность связи «клиент-клиент» становится скомпрометированной и дискредитированной, и в то же время, с другой стороны её же анонимность становится инициализирующей и первой простейшей формой анонимата. Такое противоречие (ухудшения безопасности и улучшения анонимности, и наоборот) не является случайным, а представляет собой правило и

---

[5]Мощность анонимности — количество узлов, выстроенных в цепочку и участвующих в маршрутизации информации от отправителя до получателя, при этом, не будучи никак связанными между собой общими целями и интересами. Из этого следует, что многоранговая архитектура по умолчанию имеет мощность анонимности $|A| = 1$ (вне зависимости от количества серверов). Нулевая мощность анонимности $|A| = 0$ возникает при существовании прямых соединений между субъектами (иными словами при отсутствии какой бы то ни было маршрутизации).

$$|A| = |Q(R)|,$$

где R – множество узлов участвующих в маршрутизации,
Q – функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами.

Так например, если $R = \{A, B, C\}$ — это множество узлов участвующих в маршрутизации, а подмножество $\{A, B\} \in R$ — кооперирующие узлы, то $Q(R) = [\{A, B\}, \{C\}]$ и, как следствие, $|A| = |Q(R)| = 2$.

Термин мощность анонимности $|A|$ взят как следствие термина множества анонимности A, подразумевающее R-ое количество субъектов способных совершать действия в системе по отдельно взятой транзакции. В отличие от множества анонимности, мощность анонимности ставит дополнительное ограничение, при котором узлы находящиеся в сговоре считаются за одного узла.

закономерность, в чём можно будет убедиться далее. Описанную стадию вкратце именуют псевдо-анонимностью, а клиентов — анонимами.

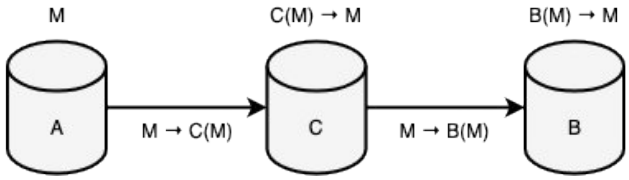

Рисунок 15. Вторая стадия анонимности (соединение посредством сервиса)

3. Третья стадия, являясь синтезом предыдущих стадий, представляет примитивную маршрутизацию, а следовательно и примитивную анонимность, нескольких прокси-серверов несвязанных между собой. Именно на данном этапе сеть становится раздробленной, неопределённой, гибридной за счёт чего и повышается мощность анонимности методом стремления к статичному значению $lim_{|A|\to C}$, где C — количество прокси-серверов. Данный метод предполагает выстраивание цепочки узлов, через которые будет проходить информация. Мощность анонимности на данном этапе действительно повышается, но и безопасность самих субъектов ещё никак не обеспечивается. Связано это всё потому, что шифрование на данном этапе есть свойство добавочное (сродни второй стадии), не обеспечивающее защиту связи «клиент-клиент», а следовательно, и не приводящее к уменьшению мощности доверия. На *Рисунках 16, 17, 19* изображён абстрактный субъект *@*, способный быть как настоящим получателем, так и промежуточным субъектом — сервисом.

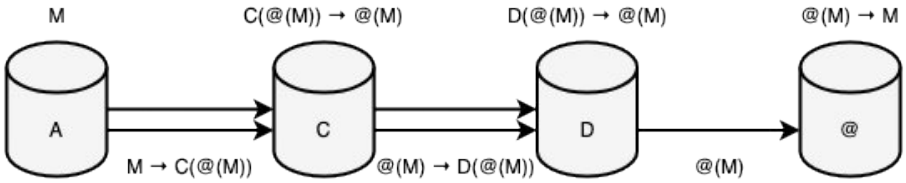

Рисунок 16. Третья стадия анонимности (Proxy транслирование)

4. Четвёртая стадия, как развитие третьего этапа, инициализирует способ изменчивости, полиморфизма информации[6] посредством её множественного шифрования, туннелирования. К такому этапу относятся VPN сервисы (виртуальные частные сети) как *N*-ое сочетание прокси-серверов со внутренними слоями шифрования [35], где мощность доверия и мощность анонимности эквивалентно третьей стадии. Отличительной особенностью четвёртого этапа является существование выходных узлов, постепенно «раскрывающих» истинную информацию, созданную до первичного туннелирования на

[6]Полиморфизм информации — свойство изменчивости передаваемого объекта при множественной маршрутизации несколькими субъектами сети, разграничивающее связь субъектов посредством анализа объекта. Так например, если существует три субъекта сети $\{A, B, C\}$ и объект P, который передаётся от A к B и от B к C соответственно, то внешний вид информации P_1 и P_2 должен определяться как $[P_1 = (A \to B)] \neq [P_2 = (B \to C)]$, где $P \notin \{P_1, P_2\}$, $P_1 \neq P_2$, (B не связывает $\{P_1, P_2\}$ с P) и (A не связывает $\{P_1, P\}$ с P_2) и/или (C не связывает $\{P_2, P\}$ с P_1). В большинстве случаев полиморфизм информации достигается множественным шифрованием объекта: $[E_2(E_1(P)) = (A \to B)] \neq [E_1(P) = (B \to C)]$, при котором интерстициальный субъект B становится неспособным связать $\{E_2(E_1(P)), E_1(P)\}$ с P, а субъект C неспособен связать $\{E_1(P), P\}$ с $E_2(E_1(P))$.

отправляющей стороне, из-за чего и появляется возможность к сокрытию метаданных, связующих инициатора сообщения и сервер назначения. В связи с этим, данный этап изменяет способ маршрутизации, придаёт ему свойство полиморфизма как изменчивости закрытой информации по мере перехода от одного узла к другому, и отстраняет промежуточные узлы к анализу и сравниванию шифрованной информации. Таким методом скрывается настоящая связь между субъектами посредством их объекта, а следовательно и анонимат начинает обретать более истинный характер, при котором стремление системы к увеличению и сдерживанию мощности анонимности становится более качественным, в сравнении с третьей стадией.

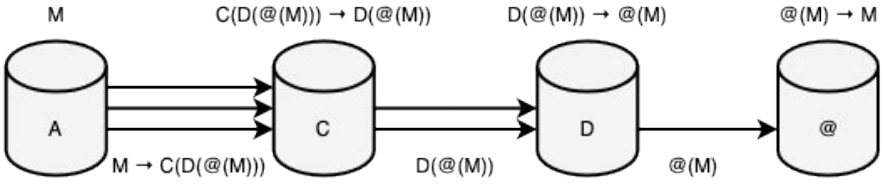

Рисунок 17. Четвёртая стадия анонимности (VPN туннелирование)

5. Пятая стадия, являясь синтезом первого этапа и отрицанием третьего, становится точкой окончательной замены сетевого адреса криптографическим, при которой идентификация субъектов отделяется от концепции сетевых протоколов, подчиняя узлы абстрактно-криптографической модели. Строятся платформы сетевой связи как базисы, поверх которых разрастаются криптографические соединения, инкапсулируя взаимодействия субъектов со своим основанием. Именно на данном этапе мощность доверия вновь становится минимально возможной величиной, а потому и все приложения построенные на пятой стадии анонимности, имеют уровень безопасности зависимый только (или в большей мере) от качества самой клиентской части. Примером такой стадии могут являться чаты, мессенджеры (Bitmessage), электронная почта, форумы (RetroShare), файловые сервисы (Freenet, Filetopia), блокчейн платформы (Bitcoin, Ethereum) и т.д. [36][37], где главным фактором идентификации клиентов становятся криптографические адреса (публичные ключи, хеши публичных ключей). Сеть начинает представлять собой не только гибридный, но и одноранговый характер поведения узлов с возможным и дополнительным динамическим способом определения мощности анонимности, как $0 < |A| \leq N$, где N — количество узлов в сети, обуславливаемым слепой, заливочной маршрутизацией [4, с.398] и криптографической идентификацией. При этом, стоит заметить, что на данном этапе не существует какого бы то ни было полиморфизма информации (как это было в четвёртой стадии), что приводит к внутренним противоречиям одновременного прогресса и регресса анонимности. Поэтому пятую стадию можно вкратце охарактеризовать игнорированием анонимности (экзотеричностью) со стороны субъекта и её сохранением (эзотеричностью) в передаваемом объекте. На *Рисунке 18.* под сетью понимается переключение системы из состояния сетевой идентификации к идентификации криптографической, вследствие чего происходит абстрагирование информации об отправителе для получателя и о получателе для отправителя непосредственно.

Рисунок 18. Пятая стадия анонимности (соединение посредством абстрактной сети)

6. Шестая стадия приводит к единовременному отрицанию и синтезу четвёртой стадии, как системы неориентированной на анонимную идентификацию субъектов, и пятой стадии, как системы ненаправленной на анонимную связь между субъектами. В такой синергии объединяются свойства полиморфизма (анонимное связывание) и криптографической идентификации (анонимное определение), что приводит не только к анонимату отправителя информации, но и к обезличиванию получателя, вследствие чего определение анонимности становится более качественным и цельным. Мощность анонимности на данном этапе становится эквивалентно четвёртому этапу, равно как и мощность доверия (причина ухудшения мощности доверия относительно пятой стадии приведена в подразделе «Проблематика безопасности анонимных сетей»). Примером шестой стадии является большинство скрытых сетей, наподобие Tor (onion routing) [38], I2P (garlic routing) [39], Mixminion (mix network) [40] и т.д. На *Рисунке 19.* изображён прототип функционирования системы Tor с запросом ориентированным на внутренний ресурс (в качестве упрощения показана схема с двумя промежуточными узлами).

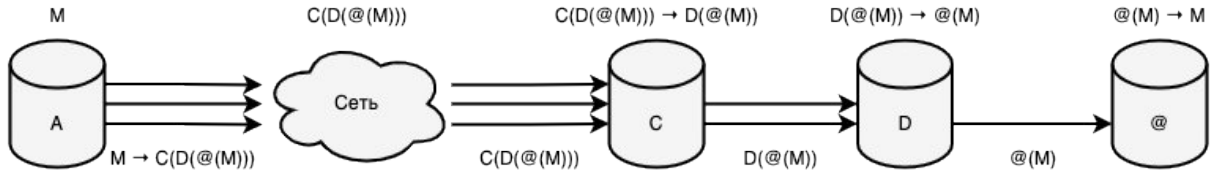

Рисунок 19. Шестая стадия анонимности (абстрактная сеть + туннелирование)

Стоит заметить, что четвёртая и пятая стадии появляются параллельно друг другу, что приводит к сложности (а скорее даже к невозможности) точного опознавания и определения последовательности развития анонимности в целом. Такой порядок стадий был взят по количеству качественных изменений. Так например, в четвёртой стадии (относительно третьей) был добавлен только полиморфизм информации, в то время как в пятой стадии была уменьшена мощность доверия, появилась криптографическая идентификация, возник новый способ маршрутизации и вернулась поддержка одноранговых соединений. С другой стороны, пятая стадия также справедливо могла стать четвёртой, базируясь не на развитии анонимности субъектов, а на развитии безопасности объектов. В таком случае, пятый этап являлся бы финальной формой, в то время как текущая четвёртая стадия не проектировалась бы вовсе.

Также стоит отметить, что вторая и пятая стадии анонимности характеризуются имплозивным характером поведения информации в степени большей, чем все остальные стадии, потому как первые предполагают не только метод распространения объектов, но также и способность их сдерживания для последующего извлечения и потребления. Такие стадии именуются платформами связи, т.к. сама коммуникация между субъектами начинает обеспечиваться не только поточным транспортированием объектов (как самого факта передачи), но и «подгрузкой», посредством промежуточных субъектов, ранее сохранённых

объектов, в основании которых уже содержится информация об отправителе и/или получателе. Другие же стадии абстрагируются от конечного потребителя информации и акцентируют внимание только на сам способ передачи. Исключением всего вышесказанного является лишь первая стадия анонимности, где сам факт передачи является одновременно и способом финального получения информации.

Защита, определяемая связью «клиент-клиент», зарождается на моменте первой стадии анонимности и в последствии сразу же заменяется клиент-серверным шифрованием второго этапа. Такая быстрая подмена и разложение прямой коммуникации на платформу связи обусловлена неспособностью и ограниченностью первой стадии к эксплозии, расширению сетевых «границ», при которой субъекты не способны массово связываться без создания промежуточных узлов. Последующее и более качественное возрождение безопасной «клиент-клиент» коммуникации, убирающее ограничение в расширении, появляется на пятом этапе и ровно там же заканчивается, потому как целью всех последующих стадий уже является сокрытие субъектов информации посредством методов транспортирования объекта на базе криптографических адресов, где более не ставится вопрос истинности принимающей стороны.

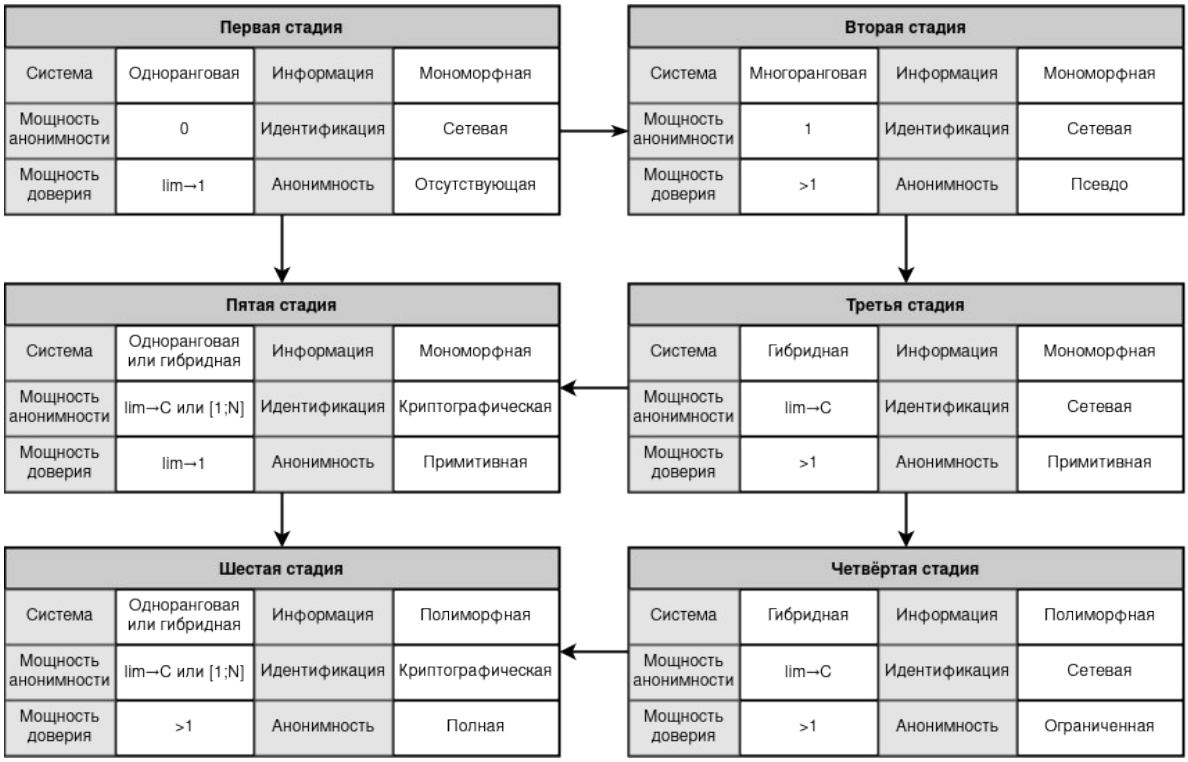

Рисунок 20. Развитие анонимности как процесс формирования стадий

Главным достоинством пятой стадии анонимности является возможность к идентификации субъектов в одноранговых и гибридных системах на основании криптографических методов, что ведёт к целостности, а также к аутентификации передаваемой информации, не зависимой от сторонних узлов и серверов [41, с.223]. Дополнительно может появляться свойство конфиденциальности, где информация начинает представлять собой суть секретного, тайного, шифрованного, а не открытого и общего объекта. Но и само свойство конфиденциальности на данном этапе — есть дополнительный критерий, а следовательно, может быть удалён, если таковой является избыточным для самой

системы. Как пример, в криптовалютах имеются свойства целостности и аутентификации, но не всегда конфиденциальности.

На основе пятой стадии анонимности становится возможным формирование тайных каналов связи первой формы как это представлено на *Рисунке 21*. Такое свойство достигается появлением криптографической идентификации субъектов, благодаря которому становится возможным абстрагироваться от сетевой идентификации.

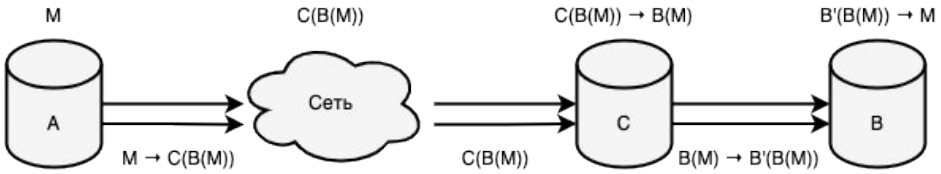

Рисунок 21. Тайный канал связи на базе пятой стадии анонимности, где *A, B* – отправитель / получатель, *C* – сервис связи

Из всего вышесказанного можно вывести основные критерии (пункты) анонимности на базе которых будет доступно формирование анонимных сетей с повышенным уровнем безопасности (полные скрытые системы).

1. Анонимность обязана быть внутренней, относительно анализа со стороны узлов, и внешней, относительно анализа трафика сети. Данный критерий должен обуславливаться разрывом связи между субъектами посредством их объекта на основании запутывающего алгоритма маршрутизации.

2. Анонимность обязана иметь инкапсулированные и абстрагированные псевдонимы между отправителем и получателем к первичной идентификации на базе сетевых коммуникаций. Данный критерий должен обуславливаться разрывом связи между идентификацией сетевой и криптографической.

3. Анонимность обязана предотвращать сохранение данных и метаданных в транспарентном состоянии для промежуточных узлов. Данный критерий должен обуславливаться заменой всех платформ связи пятой стадией анонимности, тем самым уменьшая мощность доверия до теоретически возможного минимума.

Второй пункт является в определённой степени упрощением, потому как разрыв связи должен происходить также и между двумя криптографическими идентификациями разнородных систем сливаемых между собой в одну цельную, а не только между сетевой и криптографической идентификациями. Так например, если объединяется пятая и шестая стадии между собой, то криптографическая идентификация одного и того же субъекта должна «раздваиваться» под пятую и шестую стадии соответственно. Таким образом, в подобном синтезе идентификация субъекта должна быть выражена как последовательность идентификаций вида «сетевая → криптографическая (шестая стадия) → криптографическая (пятая стадия)».

Скрытая система наделённая только первыми двумя пунктами является анонимной сетью. Скрытая система наделённая только последними двумя пунктами является клиент-безопасным приложением. Скрытая система надёланная сразу тремя критериями анонимности является полной и принадлежит не отдельной стадии анонимности, а их

комбинациям. Система наделённая только одним пунктом из трёх не является скрытой. Под системой с первым пунктом может пониматься VPN туннелирование, а под вторым – централизованные сервисы связи. Не существует систем исключительно с третьим пунктом, ровно как и комбинации третьего пункта с первым, потому как третий критерий является лишь следствием второго (обратное суждение неверно). Все вышеприведённые дескрипции можно представить в более кратком списке описания примеров:

1. Выстроенная «цепочка» VPN сервисов ∈ первый критерий
2. Централизованные сервисы связи ∈ второй критерий
3. Анонимные сети = (первый ∩ второй) критерии
4. Клиент-безопасные приложения = (второй ∩ третий) критерии
5. Полные скрытые системы = (первый ∩ второй ∩ третий) критерии

Таким образом, на основании вышеприведённых критериев обязанностей вида «быть, иметь, предотвращать» можно выявить базовое определение анонимности относительно общего типа скрытых систем, где под сетевой анонимностью будет пониматься разрыв большинства логических связей между транспортируемым / хранимым объектом и его субъектами, а также между сетевой и криптографической идентификациями.

При этом стоит заметить, что данное определение является всё же абстрактным, т.к. не указывает конкретный и поддерживаемый критерий анонимности той или иной скрытой системой. Так например, по данному определению неизвестной переменной является уровень анонимата отправителя и/или получателя в скрытой сети, потому как неизвестны сами механизмы и векторы анонимизации. Иными словами приведённое обозначение не определяет кого или что именно защищает данная система – отправителя, получателя, их обоих или только их связь. Тем не менее, эта же абстрактность приносит одновременно и ясные границы в определении анонимата между разнородными системами по стадиям анонимности.

4.2. Регресс мощности доверия

При существовании и полной реализации, а также доступности скрытых сетей, проблема, связанная с мощностью доверия, возвращается. Это кажется парадоксальным, ведь сама задача ещё решилась на пятой стадии анонимности, когда мощность доверия становилась минимально возможной величиной. Сложность заключается именно в том, что при достижении анонимности, стремление к уменьшению мощности доверия начинает игнорироваться, становиться второстепенным и добавочным критерием, в то время как стремление к увеличению мощности анонимности начинает переходить в доминируемое состояние. Таким образом, осуществляется трансфузия двух свойств, где анонимные сети начинают инициироваться противоположным, инволютивным действием к пятой стадии анонимности, а именно — игнорированием анонимности (экзотеричностью) со стороны передаваемого объекта и её сохранением (эзотеричностью) в субъекте.

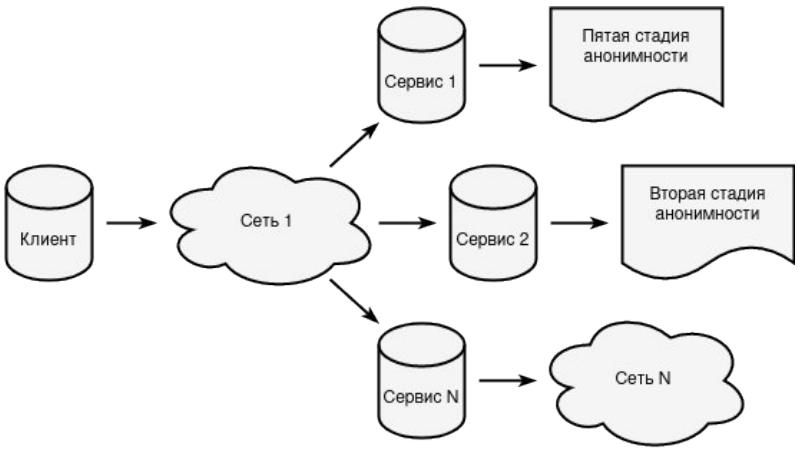

Рисунок 22. Взаимодействие скрытых сетей со внутренними сервисами

Сутью проблемы становится возможность создания сервисов связи внутри скрытых сетей не основанных на пятой стадии анонимности (*Рисунок 22*), что приводит к возникновению приложений на базе второй стадии, представляющих угрозу информационной безопасности. Это связано с тем фактом, что анонимные сети, в массе своей, базируются на принципах третьей стадии анонимности, в которой игнорируется истинность получаемой стороны. Подобная абстрагируемость неявно порождает возможность централизации внутри ризоморфных систем, тем самым, косвенно приводя к потере настоящей безопасности транспортируемых объектов.

В качестве примера можно привести сеть Tor. Доступ к сервису осуществляется вполне анонимно, но при этом сам способ хранения информации в данном приложении полностью зависит от его владельца. Это приводит к тому, что мощность доверия будет приближаться к обычному среднестатистическому сервису построенному на мощности анонимности равной единице. В итоге, становится безразличным сама среда работающего приложения, т.к. первоначальная проблема доверия будет оставаться в неизменно исходной форме со стороны второй стадии анонимности.

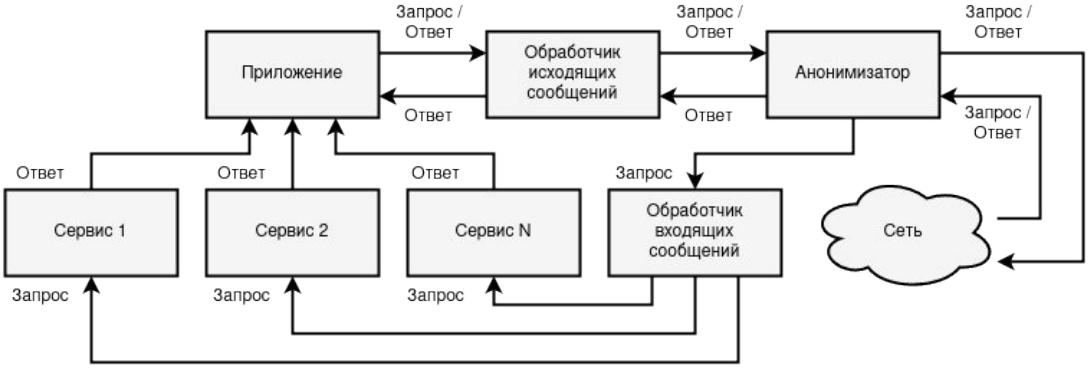

Рисунок 23. Пример архитектуры приложения анонимной сети с несколькими принимающими сервисами

Решить данный вопрос возможно лишь ограничением допустимых сервисов со стороны самой скрытой сети. Таким образом, анонимная сеть в своей базе и основе должна быть имманентной и имплозивной, содержать *N*-ое количество приложений построенных только на пятой стадии анонимности. Доступ к любым другим сервисам, не имеющих пятую стадию анонимности, или скрытым сетям, не реализующих безопасную архитектуру, должен быть

закрыт и ликвидирован. Только методом ограничений и соединений, будет возможна синергия свойств анонимности и безопасности. Примером таких сочетаний могут служить связи Tor+Bitcoin, I2P+Filetopia и т.п., или более монолитные технологии Monero [45], Dash [46] и т.д. Только на данном основании скрытые системы становятся полными.

4.3. Первая^ стадия анонимности

При начальном рассмотрении первой стадии анонимности выражается простейшая форма, инициализирующая развитие анонимата, при которой прямолинейность соединений создаёт примитивность её организации. Но при дальнейшем и более детальном анализе анонимных сетей можно заметить исключительно противоречивое свойство первой стадии анонимности, сперва исключающее, а при пересмотре образующее теоретически абсолютную анонимность в свойственной прямолинейности субъектов. Данное качество возникает при генерации объекта способного скрывать всю информацию о субъекте, включая сам факт своей передачи и своего хранения. В подобной системе не существует никакой фактической маршрутизации, выражаемой в промежуточных субъектах, что автоматически исключает все стадии выше первой. На основе такого качества выявляется два парадокса.

1. Первая стадия анонимности исключает из своего рассмотрения промежуточные субъекты. Если данная стадия переходит в состояние анонимной сети, то внутри неё способны зарождаться сервисы связи, основанные либо на второй, либо на пятой стадиях анонимности. Таким образом, получатель в анонимной сети становится не равен конечному получателю в условиях прямого соединения, что противоречит определению первой стадии анонимности.

2. Мощность доверия в первой стадии анонимности имеет минимально возможную величину. Если данная стадия переходит в состояние анонимной сети, то внутри неё способны зарождаться сервисы связи, основанные на второй стадии анонимности. Таким образом, появляются промежуточные узлы исполняющие роль конечных получателей, что приводит к повышению мощности доверия и начинает противоречить определению первой стадии анонимности.

Все парадоксы базируются на самой двойственной форме первой стадии, когда таковая одновременно вбирает в себя и выраженное транспортирование объекта, и конечное его хранение. Парадоксы своим существованием фактически расщепляют двойственность и образуют новое подмножество, как неявную градацию первой стадии анонимности. Во всех последующих упоминаниях вышеописанный этап с присущими парадоксами будет отображаться как «первая^ стадия анонимности», со знаком циркумфлекса. В качестве примера существования первой^ стадии анонимности выделяют скрытые сети базируемые на проблеме обедающих криптографов [42] (DC-сети), такие, как Dissent [43] и Herbivore [44]. Чистая форма первой^ стадии анонимности (выраженная в DC-сети) приводит к следующим недостаткам.

1. Масштабируемость. Первая^ стадия анонимности приводит к необходимости выстраивания большого количества прямых соединений, что приводит к проблеме масштабируемости, где каждый новый пользователь обязан подключаться ко всем существующим участникам сети. Проблема решается переводом первой^ стадии

анонимности на градации высшего порядка, образуя промежуточные узлы полностью не влияющие на уровень анонимности в сети. Dissent переводит систему на третью стадию анонимности, Herbivore на третью при локальной топологии и на пятую при глобальной.

2. Коллизии. В один период времени может существовать только один отправитель сообщения. При параллельной генерации сообщений двумя и более участниками сети происходит коллизия, приводящая к наложению информации. В большей части исследований проблема решается выставлением расписания генерации сообщений, что в определённой степени приводит к алгоритмам последовательного выполнения, исключающим параллельные действия. Для схем подобного рода в Dissent используются перемешивания, а в Herbivore малые группы.

3. Чистая анонимность. В исходном виде анонимность первой^ стадии идёт в полном отрыве от безопасности передаваемого объекта, где распространение информации происходит только на основе широковещательного соединения, при котором получателем сообщения является вся система. Для обеспечения безопасной линии связи от отправителя до единственного получателя (истинного или промежуточного) должен происходить переход первой^ стадии анонимности на пятую градацию в концепции тайного канала связи.

Таким образом, первая^ стадия анонимности, как чистая форма выражения анонимата, является сложно применимой в современных реалиях из-за критичных недостатков, что приводит к необходимости комбинировать данную стадию с градациями высшего порядка. Также можно выявить интересную закономерность, которая разделяет первую стадию анонимности на два вектора развития — на доказуемую безопасность объектов без анонимности субъектов (классическая первая стадия) и доказуемую анонимность субъектов без безопасности объектов (первая стадия с противоречиями или неклассическая форма первой стадии) при нешироковещательных соединениях.

Первый вектор базируется на безопасности объектов, вследствие чего, становится возможным последующий полиморфизм информации, как метод построения запутывающей маршрутизации в лице множественного шифрования. Второй вектор базируется на анонимности субъектов, вследствие чего, становится необходимым совмещение с тайным каналом связи, как методом нацеленным на обеспечение безопасности объектов. Оба вектора в конечном счёте сводятся в точке анонимности субъектов с приемлемым уровнем безопасности объектов на основе криптографической идентификации, как это изображено на *Рисунке 24*.

Из всего вышесказанного стоит выделить несколько важных составляющих, которые могут приводить к противоречиям первой^ стадии анонимности в терминологии анонимных сетей, либо к определению анонимности для скрытых сетей.

1. Маршрутизация. Первая^ стадия анонимности в своей минимальной реализации не предполагает промежуточных субъектов, что может приводить к ошибочным суждениям об отсутствии маршрутизации, и в частности – запутывающей маршрутизации. Ложность тезиса можно доказать тем фактом, что участники сети на базе первой^ стадии анонимности кооперируют и объединяют информацию в одну выходную последовательность бит, где даже при связи «*все-ко-всем*» передаётся уже «скрещиваемая» информация, что, в свою очередь, становится запутывающим

алгоритмом маршрутизации. В отличие от множественного шифрования, при котором информация распространяется посредством системы, в первой^ стадии анонимности сама система изнутри начинает генерировать полиморфную информацию. Поэтому ложность тезиса базируется исключительно на предположении того, что «полиморфизм информации = множественное шифрование», что не есть верно, потому как «множественное шифрование ∈ полиморфизму информации», ровно как и «алгоритм запутывающей маршрутизации первой^ стадии анонимности ∈ полиморфизму информации».

2. Криптографическая идентификация. Первая^ стадия анонимности в своей минимальной реализации не предполагает криптографической идентификации субъектов, что может приводить к ошибочным суждениям об отсутствии разрыва связей между сетевой и криптографической идентификациями. Ложность тезиса базируется исключительно на индивидуальной идентификации каждого отдельного субъекта в определяемом им действии, в то время как сети на базе первой^ стадии анонимности предполагают комплексную, коммуникационную модель идентификации всего множества субъектов, где криптографическая идентификация подтверждает действие отдельного субъекта самой системой и направляет таковое действие на эту же систему, как на единственного получателя. Иными словами, коллективное действие субъектов инициирует действие системы, вследствие которого сама же система получает сообщение. При смене, удалении, либо добавлении нового участника, суммарная криптографическая идентификация, выражаемая в идентификации системы, аналогично изменяется.

Таким образом, первая^ стадия анонимности, хоть и обладает специфичной формой алгоритма запутывающей маршрутизации и криптографической идентификации, тем не менее, она полностью подходит под определение анонимных сетей, как со стороны терминологии, так и со стороны определения анонимности.

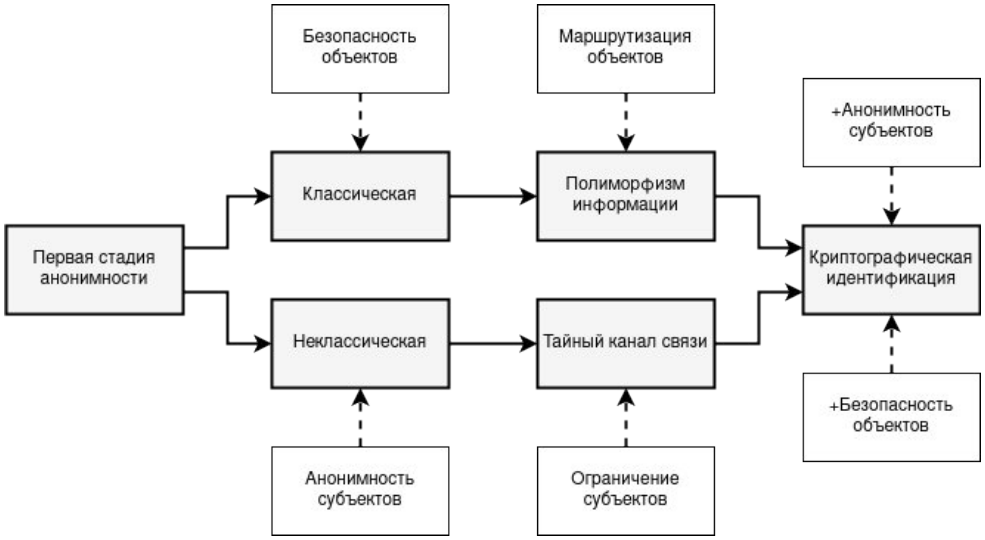

Рисунок 24. Двойственный вектор развития скрытых сетей относительно первой стадии анонимности для нешироковещательных коммуникаций

Из всего вышеописанного мощность доверия $|T|$ первой^ стадии анонимности становится эквивалентна количеству её участников $= N$ без инициатора связи $|T| = N-1$, а

мощность анонимности $|A|$ начинает стремиться к количеству участников сети без инициатора связи $lim_{|A| \to N-1}$. Это является хорошим показателем противоречия между безопасностью передаваемых объектов и анонимностью субъектов, потому как первая стадия, как оригинальный, классический вектор развития скрытых систем, обладает полностью инверсивным определением равным $lim_{|T| \to 1}$, $|A| = 0$.

Далее, если начать анализировать подобным же методом оставшиеся стадии анонимности, то можно заметить явным образом схожие противоречия и на стороне пятой стадии, при условии, что таковая система становится скрытой сетью, нацеленной на реализацию запутывающей маршрутизации отличной от множественного шифрования. Так например, если трактовать пятую стадию анонимности как первую стадию с задержками связи, иными словами, абстрагироваться от существования промежуточных субъектов (т.к. таковые не нарушают безопасность связи типа «клиент-клиент»), то можно свести второе противоречие первой стадии к пятой. И действительно, если пятая стадия анонимности также является платформой связи с постоянным стремлением к уменьшению мощности доверия, как и первая, то в таком случае становится возможным порождение анонимных сетей, неминуемо приводящих к аналогичным противоречиям в существовании промежуточных субъектов с повышенной мощностью доверия. Таким образом, ответвление оригинальной формы пятой стадии анонимности, с присущей ей противоречивостью, будет называться далее пятой^ стадией анонимности.

В результате всего вышеописанного, анонимные сети, как подмножество скрытых систем, выражаются лишь и только первой^, пятой^, шестой стадиями анонимности. Шестая стадия формируется в синтезе четвёртой и пятой стадий. Первая и пятая стадии становятся скрытыми сетями лишь в своих противоречивых формах. Формирование противоречивых стадий анонимности становится возможным лишь вследствие стремления системы к уменьшению мощности доверия. Если такого свойства не наблюдается, тогда система остаётся непротиворечивой основному вектору развития стадий анонимности.

4.4. Множественное шифрование

Если анализировать непосредственно саму полиморфную информацию, в момент её маршрутизирующего перемещения по сети, как этап наложенных итераций шифрования, то можно наблюдать точно заданную тенденцию при которой размер информации будет стремиться к собственному уменьшению. Связано это с тем фактом, что подобная информация инициализируется на отправляющей стороне и постепенно финализируется на пути к принимающей. Такая закономерность способна выявлять роль субъектов информации, при которой достаточно проанализировать лишь размер информации с позиции двух отправлений $(A \to B) \to (B \to C)$ и если информация, в таком случае уменьшается на заведомо известную величину D[7], то это свидетельствует о крайне высокой вероятности, что

[7]Детерминированная разница размеров информации между шифрованной и открытой версией, имеющая единственный слой шифрования. Зашифрованная информация состоит из шифрованного заголовка, шифрованных данных (основной информации), шифрованной случайной строки, шифрованного сеансового ключа, шифрованного публичного ключа, хеша, шифрованной подписи и доказательства работы. При этом, динамическим размером обладает только поле с основной информацией, в то время как все остальные поля имеют статические размеры, что и приводит к возможности анализа информации по динамике постоянного стремления к уменьшению, исходя из её константной дифференции.

сам узел *B* является только промежуточным получателем. Чтобы решить данную проблему, необходимо рассматривать структуру информации со стороны его размерности. Так например, если сообщение размером *S(P)* создаётся на отправителе и сразу же шифруется всеми слоями размером равным *S(E)*, то результатом такой функции является размер полиморфной информации $S(P) + S(E) = S(E(P))$. При этом, т.к. *S(E)* предполагает собой все слои шифрования, то данный размер можно представить в виде суммы каждого отдельного шифрования, где $S(E) = \Sigma_{i=1}^{n} S(E_i) = S(E_1) + S(E_2) + ... + S(E_n) \rightarrow S(E_n(...(E_2(E_1(P)))...)) = S(E(P))$. При этом каждый отдельный слой шифрования $S(E_i)$ равен любому другому слою $S(E_j)$, что даёт тождество вида $S(E_1) + S(E_2) + ... + S(E_n) \equiv nS(E_1) = S(E)$. Таким образом, проблема представлена удалением каждого отдельного элемента $S(E_i)$ из общей суммы *S(E)*, что также приводит к постоянному уменьшению числа *n* на единицу и к детерминированному вычислению $D = S(E_i)$. Решением задачи является добавление пустой, неиспользуемой информации V_i случайного размера к каждому элементу $S(E_i)$, что, следовательно, приведёт к метаморфозу свойств детерминированности числа *D*, переходящего в алеаторность посредством неравенства $S(V_i \,||\, E_i) \neq S(V_j \,||\, E_j)$ и к невозможности представления размера $S(V \,||\, E)$ через выражение $nS(V_1 \,||\, E_1)$.

Хоть на данном этапе и невозможно определить число *D*, т.к. оно уже становится случайным, исходя из выражения $S(V_i \,||\, E_i)$, тем не менее, стремление полиморфной информации к своему собственному разложению остаётся, а это говорит, что остаётся возможным вероятностный анализ его размерности. Также, если идти от обратного и предположить, что существует отправление вида $(A \rightarrow B) \rightarrow (B \rightarrow C)$ и при этом, первая информация оказывается меньше последующей, то данный факт говорит только о том, что вторая информация является самостоятельно сгенерированной и считается либо запросом, либо ответом, а узел *B* либо отправителем, либо получателем. Одним из решений данной проблемы может являться создание отдельного поля в отправляемой информации, указывающего на следующего получателя (будь то истинного или промежуточного) с той лишь целью, чтобы маршрутизатор мог дополнять информацию на некую величину размера M[8], приводящую к константному размеру K[9] [28, с.6]. Данный способ удаляет

$D = S(E(P)) - S(P)$,

где *S* - функция вычисления размера информации,
E - функция шифрования информации,
P - первоначальная информация.

[8]Переменная величина *M* применяется для замещения удалённых слоёв шифрования, сохраняя размер любой стадии полиморфной информации на уровне константной величины *K*.

$M_n = \sum_{i=1}^{n} S\left(V_i \,||\, E_i\right)$,

где $S(V_i)$ - размер случайной информации для каждого слоя шифрования,
$S(E_i)$ - размер отдельного слоя шифрования,
n - количество удалённых слоёв шифрования.

[9]Константная величина *K* является доминирующей концепцией большинства скрытых сетей, т.к. скрывает объём передаваемой информации посредством фиксации размерности информации (объём может частично разглашать функцию транспортируемой информации или её динамику, что является уязвимостью и приводит к необходимости решения).

$K_j = S(P) + \sum_{i=j}^{n} S\left(V_i \,||\, E_i\right) + M_{j-1}$,

вышеописанные проблемы полностью, но выдаёт промежуточным узлам дополнительную информацию о последующих получателях информации, одним из которых станет истинный получатель. Критичный характер данной проблемы приведёт к негэнтропии, автоматической деградации скрытой системы, где будет существовать возможность формирования списка потенциальных получателей на основе ограничения диапазона множества узлов всей сети и приводящий к зарождению выходных нод, определённо знающих (или вероятностно распознающих) истинных получателей.

Ещё одним и более радикальным способом решения проблемы является использование случайной величины R[10], вместо константной величины K. В то время как сама уязвимость и проблема образуется и воссоздаётся из детерминированности полиморфизма, то и константная величина K порождённая ей же, не способна в корне предотвращать схожие проблемы. На место величины K встаёт величина R, приводящая к хаотичности размерности информации, к диффузии детерминированных качеств и к неопределённому выявлению субъектов информации. Такой подход базируется на необходимости генерации вероятностной псевдо-информации случайного и большего размера (чем истинная) на маршрутизирующей или принимающей стороне. Таким образом, промежуточный / принимающий узел начинает становиться одновременно и псевдо-получателем для всех остальных участников сети.

Из вышеописанного также следует вывод, что если $X \in$ {информация *меньшего размера*, информация *большего размера*}, а $Y \in$ {*отправитель / получатель, маршрутизатор*}, то при их импликации $X_i \rightarrow Y_j$ все суждения будут являться ложными. Доказать хаотичность действий вероятностной величины R и неразрешимость детерминированного анализа можно следующими логическими выражениями:

1. Если новая информация меньше предыдущей, то субъектом данного объекта является истинный отправитель, либо получатель.

Ложно, т.к. маршрутизатор может «раскрыть» информацию, тем самым уменьшив его размер.

2. Если новая информация меньше предыдущей, то субъектом данного объекта является маршрутизатор.

Ложно, т.к. ответ может быть меньше запроса.

3. Если новая информация больше предыдущей, то субъектом данного объекта является истинный отправитель, либо получатель.

Ложно, т.к. маршрутизатор может сгенерировать псевдо-информацию большего размера.

где j - стадия полиморфной информации,
n - количество слоёв шифрования.

[10]Случайная величина R является противоположной концепцией константной величины K и представляет неопределённость размерности информации со стороны маршрутизирующей стороны, где с вероятностью 1/2 может быть создана и отправлена новая, «пустая» псевдо-информация случайного и большего размера, скрывающая, посредством алеаторности, дальнейший анализ динамики истинной информации.

4. Если новая информация больше предыдущей, то субъектом данного объекта является маршрутизатор.

Ложно, т.к. ответ может быть больше запроса.

Для второго и четвёртого пунктов также действенно следующее правило — если истинный запрос/ответ по логике приложения всегда меньше ответа/запроса, то положение вероятностным образом меняется на противоположное при использовании переменных величин $\{V_1, V_2, ..., V_n\}$.

В результате всего вышеописанного нельзя однозначно ответить, что какое-то решение является наилучшим при использовании в анонимных сетях. В некоторых случаях становится невозможным использование константной величины *K*, как пример, в анонимизации сетевого трафика при соблюдении критериев ненаблюдаемости. В большинстве других случаев становится проблематичным правильное использование случайной величины *R*, т.к. сложность реализации будет приводить ко множеству «подводных камней» и, как следствие, к более затруднительному анализу безопасности итоговых систем. Ещё одним ответом на данный вопрос может становиться создание анонимных сетей либо с отсутствующим полиморфизмом информации, либо с отсутствующим множественным шифрованием, как частным случаем полиморфизма информации. Взамен отсутствия полиморфизма, будь то в общем случае или только в его частной реализации, будет теряться множество прикладных применений.

5. Анализ сетевой анонимности

Анонимные сети базируются на определённых шаблонах, конструктах или примитивах проектирования, в которых учитываются роли субъектов и конструируемые модели угроз. В наиболее простых случаях используется только один шаблон проектирования, в других используются уже комбинации подобных паттернов, что может приводить к некоторым улучшениям, новым возможностям и параллельно к усложнению итоговой логики приложения.

5.1. Свойства

Один и тот же шаблон проектирования может обладать разными, вариативными механизмами своего исполнения – свойствами. Отличительным признаком множества свойств друг от друга становится механизм выдачи итоговой информации на базе входной, принимаемой последовательности. Данные свойства обладают качествами, позволяющими им, в зависимости от задачи, предоставлять определённый уровень анонимности, производительности и применимости.

1. «*Поточность*» $S_p(f, X) = f(X)$. Если на вход алгоритму поступает информация *X*, тогда необходимое действие *f*, как ответ, должно выполняться сразу после обработки входной последовательности *X*. Представляет наилучшее качество производительности вычислений (в сравнении с другими свойствами) за счёт уменьшения качества анонимности. По количеству способов применения является лидирующим свойством. В качестве примера сеть Tor и луковая маршрутизация, которая не имеет каких-либо программных задержек при передаче информации между узлами.

2. «*Периодичность*» $T_p(f, X, t) = t \rightarrow f(X)$. Если на вход алгоритму поступает информация *X*, тогда необходимое действие *f*, как ответ, должно выполняться только

после совершения периода равного t зависимого или независимого от времени поступаемой информации X. Может представлять высокое качество анонимности за счёт уменьшения качества производительности вычислений. Имеет самое малое количество способов применения из-за своих накладных расходов. В качестве примера можно привести сеть Herbivore и устанавливаемое расписание генерации.

3. «*Аккумулятивность*» $A_p(f, X_i, k) = k \rightarrow f(X_1, X_2, ..., X_k)$. Если на вход алгоритму поступает информация X_i, тогда необходимое действие f, как ответ, должно выполняться только после принятия k-ого количества другой информации X. Представляет хорошее качество анонимности за счёт уменьшения качества производительности вычислений. Имеет ограниченное количество способов применения. В качестве примера сеть Mixminion и перемешанные сети (Mix networks).

5.2. Конструкты

Шаблоны проектирования анонимных сетей (далее конструкты) представляют собой специфичную коммуникацию между несколькими субъектами, изображаемую в виде графов. За счёт способа коммуникации между узлами и вбираемых свойств, таковым конструктом, определяются дальнейшие и возможные способы использования выстроенной схемы. Конструкты условно можно разделить на три вида: генезис, базовые, составные. Генезис конструкт создаёт "почву" для формирования базовых конструктов, наиболее минимальных форм. Базовые конструкты формируют составные, с более конкретными уникальными свойствами, которые можно использовать в строении анонимных сетей.

I. *Генезис конструкт*

1. «*Генерирование*» $G_c(X) = X$. Генезис конструкт, представляющий факт генерации, инициализации или отправления информации X. Никаким образом не представляет анонимность, но является необходимой составляющей для инициирования всех действий. Таковой конструкт предполагает своё использование по умолчанию, потому как является прародителем всех последующих конструктов и следовательно обозначается просто как X.

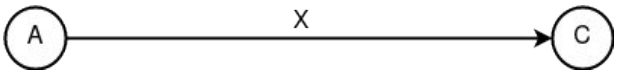

Рисунок 25. Генезис конструкт «генерирование»

II. *Базовые конструкты*

1. «*Следование*» $F_c(X) = X'$. Базовый конструкт, представляющий полиморфизм информации в своей простейшей форме. Лежит в основе VPN-сервисов и часто применяется анонимными сетями по причине простоты образования свойств несвязываемости между субъектами информации посредством объекта. Предполагается, что информация X' - это более раскрытая версия информации X, и на примере множественного шифрования такое качество можно описать как $X=E(E(M))$, $X'=E(M)$, $X''=M$, где M - открытое сообщение, а E - функция шифрования.

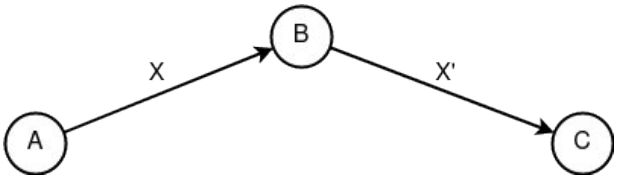

Рисунок 26. Базовый конструкт «следование»

2. «*Распространение*» $D_c(X, n) = (X)^n$. Базовый конструкт, представляющий собой в чистой форме широковещательную связь, за счёт которой появляется возможность сильного абстрагирования сетевой и криптографической идентификаций друг от друга, посредством слепой маршрутизации. Таковой конструкт можно наблюдать в приложении Bitmessage.

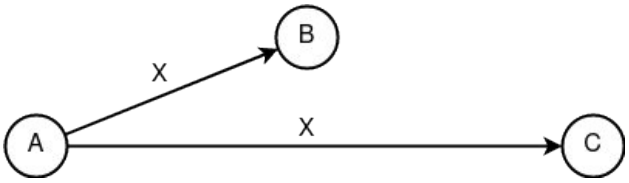

Рисунок 27. Базовый конструкт «распространение»

3. «*Запутывание*» $E_c(n) = {\sim}X_{G(n)}$, где ${\sim}X = \{{\sim}X1, {\sim}X2, ..., {\sim}Xn\}$ – множество всех ложных сообщение, n – количество всех возможных случайных сообщений, G – функция случайного выбора элемента из множества $\{1, 2, ..., n\}$. Базовый конструкт, представляющий собой в чистой форме ложность факта отправления информации ${\sim}X$. Невозможно применять в чистой форме из-за отсутствия самого факта передачи истинной информации, поэтому служит исключительно композитной частью для составных конструктов.

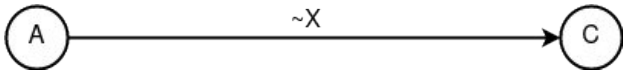

Рисунок 28. Базовый конструкт «запутывание»

III. *Составные конструкты*

1. «*Перемешивание*» $P_c(X, Y) = F_c(X, Y) = (F_c(X); F_c(Y)) = (X'; Y')$. Составной конструкт, представляющий собой суммирование конструктов «следование». Позволяет улучшать критерий несвязываемости субъектов посредством неопределённости состояния передаваемого объекта. Такой составной конструкт можно наблюдать в Mixminion сетях, где основной упор делается как раз на перемешивание входной информации.

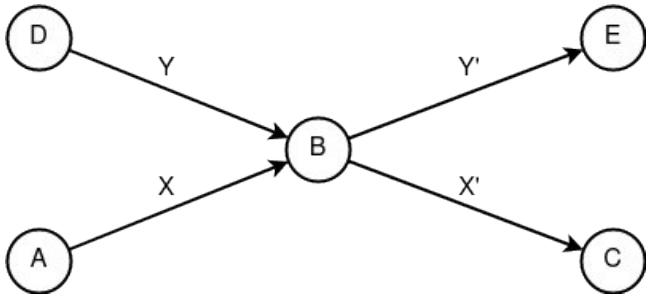

Рисунок 29. Составной конструкт «перемешивание»

2. «*Расщепление*» $S_c(X, m, n) = (X; D_c(E_c(n), m)) = (X; (\sim X_{G(n)})^m)$. Составной конструкт, представляющий собой сочетание базовых конструктов «распространение» и «запутывание». Позволяет улучшать критерий несвязываемости субъектов посредством формирования ложных, запутывающих сообщений.

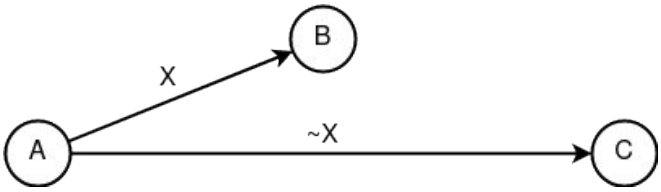

Рисунок 30. Составной конструкт «расщепление»

3. «*Сведение*» $M_c(X, (\sim X_{G(n)})^m) = M_c(X, D_c(E_c(n), m)) = (X; Ø) = X$. Составной конструкт, представляющий собой сочетание базовых конструктов «запутывание» и «распространение». По своей сути является обратным действием к составному конструкту «расщеплению».

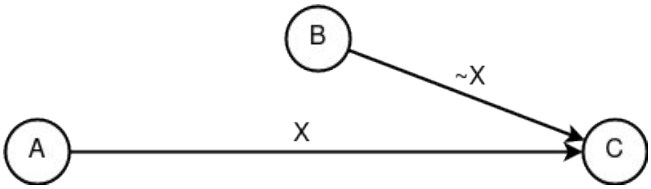

Рисунок 31. Составной конструкт «сведение»

5.3. Алгебра связей

Теперь, как только были сформированы конструкты можно начинать использовать и свойства, ориентируемые на данные конструкты. Так, в качестве примера, становится возможным формирование связи между конструктом «Генерирование» и свойством «Периодичность» следующим образом: $G_cT_p = T_p(G_c, X, t)$. В таком случае, само отправление информации X (а точнее множества информаций вида X_i) от одного абонента к другому будет периодичным по времени t.

Также, конструкты, в отличие от свойств, имеют возможность накладываться друг на друга, или формировать определённые композиции своих функций. Так например, если существует некий абстрактный конструкт A_c, то невозможно применять одновременно операции типа $A_cS_pT_p$, $A_cT_pA_p$, $A_cA_pS_p$ и т.д. Тем не менее, за счёт комбинации конструктов появляется возможность комбинировать и свойства. Так например, становится возможным

применять разные свойства следующим образом: $A_cS_p+A_cT_p$. Плюс к этому существует возможность комбинировать конструкты с одним свойством по типу $A_{c1}A_{c2}T_p$.

В следствие этих наблюдений, можно заметить, что конструкты и свойства зависимы друг от друга, но имеют разные пропорции зависимостей, что легко наблюдается в возможности создавать *N*-ое количество конструктов с одним лишь свойством, но в невозможности создавать *N*-ое количество свойств с одним конструктом. Связано это в первую очередь с тем, что конструкты определяются наследованием предыдущих, более базисных конструктов.

Некоторые конструкты могут неявным образом порождать побочные конструкты, становясь в определённой степени динамичными структурами. Так например, базовый конструкт «следование» может неявным образом порождать составной конструкт «перемешивание». Некоторые анонимные сети оставляют такой критерий динамичности (Tor), другие напротив пытаются исключить «следование» и сделать «перемешивание» статичным конструктом (Mixminion). Связь между одним принципом и другим соблюдается лишь посредством выбора необходимого свойства. Например, динамично порождаемое «перемешивание» является следствием свойства «поточность» конструкта «следование», в то время как статичный конструкт «перемешивание» обуславливается свойством «аккумулятивность».

Связь конструктов и свойств располагает также своими специфичными операциями. Предположим, что существуют некие множества абстрактных конструктов $\{\#c_1, \#c_2, \#c_3, ..., \#c_N\}$ и абстрактных свойств $\{\#p_1, \#p_2, \#p_3, ..., \#p_N\}$. На этих множествах становится возможным выделение следующих операций.

1. «*Сложение*» $(\#c_1\#p_1)+(\#c_2\#p_2) = \#c_1\#p_1+\#c_2\#p_2$. Сложение является некоммутативной операцией, иными словами $(\#c_1\#p_1)+(\#c_2\#p_2) \neq (\#c_2\#p_2)+(\#c_1\#p_1)$, и неассоциативной, иными словами $\#c_1\#p_1+(\#c_2\#p_2) \neq (\#c_1\#p_1)+\#c_2\#p_2$. Сложение выражает собой последовательные действия.

2. «*Соединение*» $(\#c_1\#p_1);(\#c_2\#p_2) = (\#c_1\#p_1;\#c_2\#p_2) = \#c_1\#p_1;\#c_2\#p_2$. В отличие от сложения, соединение объединяет два значения, не синтезируя их в одно. Является некоммутативной, но ассоциативной операцией.

3. «*Произведение*» $n(\#c\#p) = (\#c\#p)+(\#c\#p)+...+(\#c\#p)$ (*n раз*) $= \#c\#p+\#c\#p+...+\#c\#p$ (*n* раз). Произведение коммутативно, то есть $n(\#c\#p) = (\#c\#p)n$.

4. «*Композиция*» $\#c_2(\#c_1\#p_1) = (\#c_2\#c_1\#p_1) = \#c_2\#c_1\#p_1$. Композиция представляет собой объединение нескольких конструктов под одно свойство. Иными словами, аргументом свойства становятся последовательные действия конструктов $\#p_1(\#c_2\#c_1)$. Операция коммутативна, то есть $\#c_2(\#c_1\#p_1) = (\#c_1\#p_1)\#c_2$. Исполнение конструктов внутри блока свойства происходит справа-налево.

5.4. Анонимизирующие схемы

На основе вышеприведённых конструктов, а также их свойств, становится возможным формирование анонимизирующих схем. Результатом таких схем является возможность выстраивания любых типов анонизирующих связей: 1) анонимность отправителя или получателя, 2) анонимность отправителя и получателя, 3) анонимность связи между отправителем и получателем. Это можно продемонстрировать на следующих примерах.

1. Пример схемы сетевой коммуникации с анонимностью связи между отправителем и получателем на базе конструктов «следование» и «перемешивание». Представителями такого вида коммуникаций можно считать сети Tor, I2P. Если изменить свойство «поточность» на «аккумулятивность», то конструкт «перемешивание» станет статичным и основополагающим конструктом. Представителем уже такого усовершенствованного вида сетей становится сеть Mixminion.

$$n(F_cS_p)$$

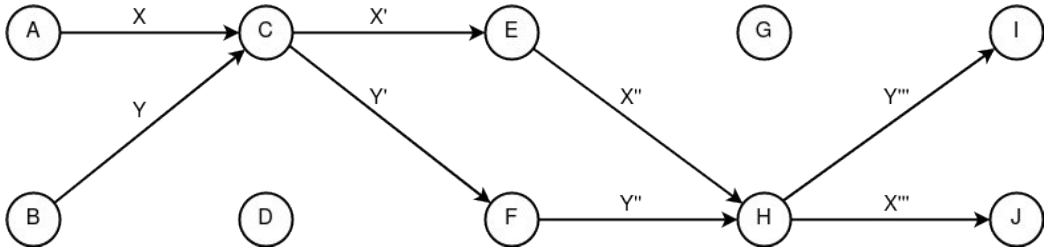

Рисунок 32. Применение конструктов «следование» и «перемешивание», где {*A, B*} – отправители запакованной информации {*X, Y*}, {*I, J*} – получатели информации {*X’’’, Y’’’*}

2. Пример схемы сетевой коммуникации с анонимностью отправителя на базе конструктов «запутывание», «следование», «сведение» и «распространение». Безопасность приведённой концепции держится на узле «сведения» *E*, который должен обладать свойством «аккумулятивности» и на узлах {*A, B, C*}, которые должны обладать свойством «периодичности».

$$(F_cT_p;F_cE_cT_p)+(M_cA_p)+(D_cS_p)$$

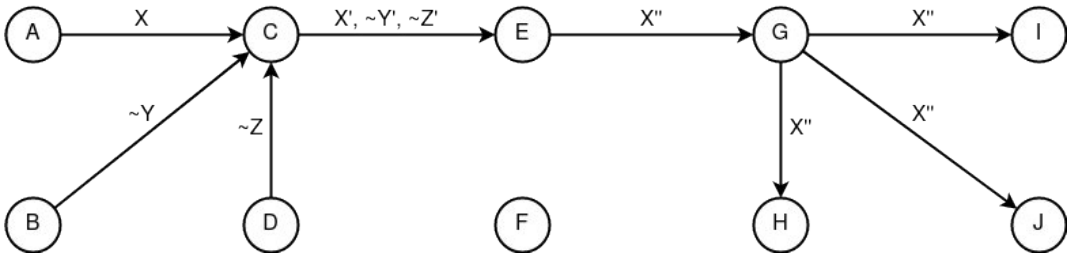

Рисунок 33. Применение конструктов «запутывание», «перемешивание», «сведение», «следование» и «распространение», где *A* – отправитель запакованной информации *X*, *C* – узел «перемешивания», *E* – узел «сведения», {*G, H, I, J*} – получатели информации *X’’’*

3. Пример схемы сетевой коммуникации с анонимностью получателя на базе конструктов «следование», «расщепление», «сведение» и «распространение». Безопасность приведённой концепции держится на узле «сведения» *H*, который должен обладать свойством «аккумулятивности».

$$(S_cF_cS_p)+(D_cM_cA_p)$$

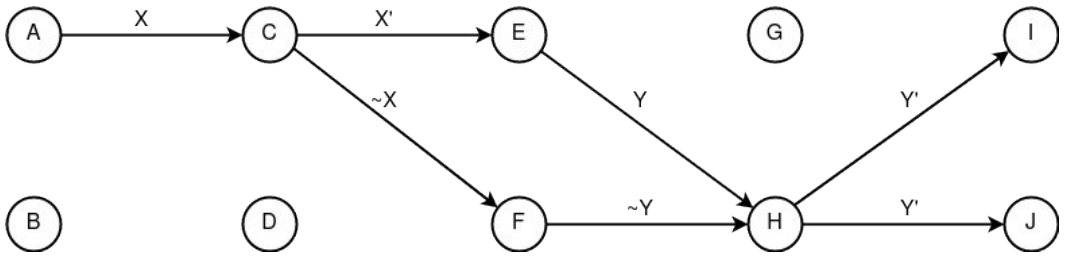

Рисунок 34. Применение конструктов «следование», «расщепление», «сведение» и «распространение», где *A* – отправитель запакованной информации *X*, *E* – получатель информации *X'*, *C* – узел «расщепления», *H* – узел «сведения», *Y* – сгенерированный ответ

4. Пример схемы сетевой коммуникации с анонимностью отправителя и получателя на базе конструктов «распространение», «запутывание» и «сведение». Безопасность приведённой концепции держится на всех узлах сети, которые должны обладать свойством «периодичности».

$$(D_cT_p;D_cE_cT_p)+(M_cS_p)$$

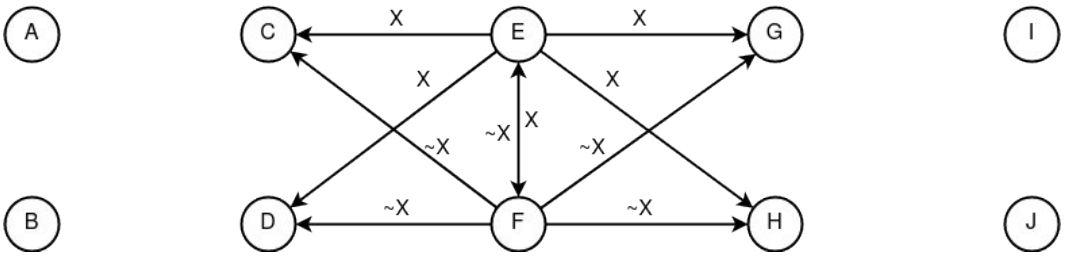

Рисунок 35. Применение конструктов «распространение» и «запутывание», где *E* – отправитель информации *X*, *F* – отправитель ложной информации *~X*.

Таким образом, любой механизм анонимной сети строится во-первых, на примитивах проектирования (конструктах), во-вторых, на определяемых ими свойствах. За счёт приведённых композиций приобретаются соответствующие уровни анонимности, производительности или применимости в лице выстраиваемых схем.

6. Заключение

Актуальность данной работы прямолинейно зависит от повсеместной активности использования монополистических централизованных систем, когда таковые становятся фундаментом, основой всех дальнейших сетевых коммуникаций. Таким образом, представленное исследование неразрывно связано с иерархическими системами, потому как является их описанием и отрицанием, формой их деструктуризации, выявляющей противоречия, особенности, факторы непосредственного развития и отмирания. По этой причине становится возможным выявление более качественных систем, приходящих на смену централизованным, как со стороны анонимности субъектов, так и со стороны безопасности передаваемых / сохраняемых объектов.

6.1. Основные выводы

Ключевым аспектом данной работы стал анализ развития сетевых коммуникаций, сетевых архитектур и, как следствие, сетевой анонимности. Было дано определение анонимности и стадий её становления, каждая из которых формировалась посредством двух составляющих – мощности доверия и мощности анонимности. Было выявлено шесть основных стадий анонимности и две противоречивые формы базового вектора развития: первая^ и пятая^ стадии. Также было выявлено противоречие, при котором стремление к уменьшению мощности доверия становилось второстепенным свойством, как только достигался этап формирования анонимной сети. Решением проблемы стало объединение пятой стадии анонимности со стадией скрытой сети, тем самым образовав полные скрытые системы. Далее в работе были приведены основные и составные конструкты (шаблоны) проектирования анонимных сетей с различными свойствами. Шаблоны проектирования, в совокупности с их свойствами, позволяют анализировать уровень анонимности и выстраивать за счёт этого модели будущих или текущих анонимных сетей. В качестве завершения работы была приведена проблема использования полиморфизма информации в лице множественного шифрования, как основного способа анонимизации трафика. Проблемой становилось изменение размера полиморфной информации при её маршрутизации от одного узла к другому. Было предложено несколько возможных способов исключения данной проблемы. У каждого способа были выявлены как положительные, так и отрицательные качества.

6.2. Терминология «Darknet»

На основе всего вышесказанного и проанализированного, скрытые системы, как множество клиент-безопасных приложений, анонимных сетей и, в частности, тайных каналов связи, перестают являться чем-то мистическим, скрытным, транзитивным, как того чаще общество, не понимая их «внутренностей», обрекает данные механизмы метафизическим термином «Darknet».

В разных ситуациях данную сущность рассматривают то как анонимные сети, то как безопасные системы, а иногда и вовсе не анонимные и не безопасные, вбирая в себя множество противоречий в качестве размытия терминологий. Например, «Darknet»’ом могут называть friend-to-friend сети расчитанные на обмен файлами, RetroShare, GNUnet, FreeNet (клиент-безопасные) приложения, Tor, I2P (анонимные) сети, Proxy и VPN сервисы (качество анонимности которых уступает скрытым сетям), социальные сети с уникально настроенным протоколом связи, TON (Telegram Open Network) (что является криптовалютой и одной из вариаций представления Web3, тогда Bitcoin и Ethereum должны также считаться «Darknet» системами?), Telegram (централизованный сервис связи с возможной и неоднозначной опцией сквозного шифрования, тогда WhatsApp также может стать «Darknet»’ом?), BitTorrent (протокол не предоставляющий анонимность субъектов и конфиденциальность объектов) и т.п. Такой список можно продолжать и дополнять ещё десятками разнообразных технологий[11], поэтому из-за своей противоречивости в данной работе намеренно не

[11]Википедия «Даркнет» [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82 (дата обращения: 20.10.2022). Википедия «Darknet» [Электронный ресурс]. — Режим доступа: https://en.wikipedia.org/wiki/Darknet (дата обращения: 20.10.2022).

использовался термин «Darknet»[12], чтобы не добавлять ещё одно возможное запутывающее значение к такому определению.

В литературе [47] указывается, что «Darknet»'ом можно назвать буквально всё что угодно, что связано так или иначе с фактом скрытия информации, либо личности от глобальных наблюдателей (будь то это государства или монополистические корпорации) вне зависимости от способов достижения такого сокрытия. Данное суждение приводит одновременно к следующим противоречиям.

1. Если не ставится различий между неиндексируемыми запароленными страницами сайтов в сети Интернет и скрытой сетью Tor, то это приводит к фактическому отрицанию анонимности «Darknet» за счёт второстепенности и незначимости её запутывающей маршрутизации (как главного критерия сетевой анонимности). Тем не менее, в терминологии «Darknet» анонимность считается одной из базовых характеристик присущих данной системе, что несомненно является противоречием.

2. Если предположить, что под анонимностью понимается безопасность передаваемых объектов, где нельзя узнать что конкретно передаётся, иными словами понимать под «Darknet» клиент-безопасные приложения с характеристикой конфиденциальности, то это противоречит «Darknet» системам связанных с неиндексируемыми запароленными страницами сайтов в сети Интернет, принадлежащими второй стадии анонимности, с присущей пседоанонимностью и отсутствием безопасности передаваемой / хранимой информации.

В то время как первое противоречие выдаёт фактор неанонимности «Darknet» сетей, что отчасти может всё равно коррелировать с другими определениями в плане практического использования (F2F-сети, клиент-безопасные приложения и т.п.), исключая лишь и только применение анонимных сетей (подобия Tor, I2P и т.д.), второе же противоречие начинает вступать в открытый конфликт со множеством других терминологий «Darknet» сетей, как на практическом, так и на теоретическом уровнях, даже учитывая наиболее общий и абстрактный характер термина приведённого в рассматриваемой литературе. Иными словами, такие противоречия приводят одновременно к пониженной мощности анонимности $|A| = 1$ и к повышенной мощности доверия $|T| > 1$, что является абсолютным и негативным отражением реальной анонимности субъектов и безопасности объектов в «Darknet» сетях.

Термин «Darknet» также подкрепляется и современными научными материалами, такими как [48][49], которые в отличие от вышеописанных определений всё же не настолько противоречивы, но непротиворечивы они лишь потому, что акцентируют внимание исключительно на частных случаях и не пытаются углубляться в структурный анализ рассматриваемых систем. Данные работы, как чаще всего бывает, приводят в качестве «Darknet» составляющих Tor (и реже I2P) сети, которые были описаны и проанализированы в разных публикациях уже достаточное количество раз, из-за чего такие исследования становятся лишь дубликатами других.

---

[12]Термин «Darknet» хоть и переводится дословно как «тёмная сеть», но смысл вложенный в таковой термин на уровне данной работы часто не коррелирует со множеством сторонних определений, потому как сводится исключительно к синониму анонимных сетей. Если исходить из нашего исследования, то наиболее близким термином к «Darknet» становится «скрытая система», хоть и со множеством противоречий, потому как скрытые системы куда менее абстрактны и куда более конкретны в сравнении с «Darknet»'ом.

Базовые же, фундаментальные работы в направлении анализа и разработки новых скрытых систем датировались, в массе своей, лишь 19(80)-20(00)-ыми годами исследователями, из которых можно выделить Дэвида Чаума (DC-сети и Mix-сети) [28][42], Андреаса Пфицмана и Марита Хансена (терминология анонимности) [50], Михаила Рейтера и Авиеля Рубина (системы измерения уровня анонимности) [51]. В настоящем же времени данные работы становятся забываемыми и включаются в источники лишь посредством других источников, где неявным образом создаются и реконструируются симулякры третьего порядка, интерпретирующиеся на базе выдвинутых тезисов из последующих, производных исследований.

Являясь так или иначе суммирующей работой, данная статья отличается от множества остальных тем, что ставит проблему репрезентации и стандартизации «старых» исследований в совокупности с текущими реалиями повсеместной монополистической централизации, следствием которой становится отсутствие фактической анонимности субъектов и безопасности передаваемых ими объектов.

6.3. Противоречивость «Web3»

Всё вышеописанное исследование является в первую очередь анализом развития безопасных и анонимных систем, становление которых проходит через внутренние этапы противоречий на уровне их технического описания. Тем не менее, как было сказано в подразделе «Централизация как фактор продолжительной стагнации» раздела «Введение», все системы не так просты и их развитие, или вернее сказать их стагнацию, невозможно описать исключительно техническим языком, потому как фактор сдерживания, удержания системы начинает зависеть уже непосредственно от экономических и политических причин. Если бы все системы развивались лишь и только технической на то необходимостью, в том числе ориентируясь на безопасность и анонимность обычных пользователей, то сеть Интернет (или какая-либо другая сеть, подобия NETSUKUKU) стала бы уже сегодня выражением реальной защиты конфиденциальной информации без значимых централизованных механизмов. Но именно экономические факторы начинают диктовать нецелесообразность мер, не позволяют эволюционировать на почве векторов скрытых систем, потому как само развитие становится невыгодным излишком иерархических структур. Централизация, как доминирующая система, в буквальном смысле, понесёт огромные убытки с многократным ухудшением качества сбора информации о рядовых пользователях, что также кардинально сузит рынки сбыта конфиденциальной информации со стороны рекламодателей, а также многократно понизит контроль за таковой информацией со стороны государств. Поэтому транспарентно и явственно наблюдаются случаи, когда государства пытаются из-за всех сил запрещать децентрализованные системы, а монополистические корпорации, с их значительными экономическими ресурсами, не стремятся переводить свои системы на базу клиент-безопасных приложений.

Из вышеописанного также следует, что моментальная техническая революция нацеленная на безопасность и анонимность пользователей, и при этом находящаяся на почве синтеза политических и экономических интересов, становится лишь идеалистическим представлением прогресса. Экономическая рационализация централизованных систем становится главной и непреодолимой преградой идеалистических взглядов на развитие скрытых систем. С другой стороны, сама централизация, по мере своей имманентной эволюции, начинает с каждой итерацией прогресса вбирать в себя всё больше одноранговых соединений, постепенно встраивая, «вживляя» их в парадигму иерархических коммуникаций. Экономическая целесообразность становится вполне разумной, потому как

направляется на перманентное повышение своей отказоустойчивости и свойств заменяемости за счёт разделения и дублирования функций узлов системы. Тем не менее таковой исход приводит одновременно к двум противоречиям:

1. Внутренние сотрудники корпораций, представляя сам масштаб иерархической монополизации, всё чаще и интенсивнее будут предпринимать меры нацеленные на утечку информации ради собственной выгоды. Данное суждение связано не только с увеличивающимся интересом сотрудников, но также и с увеличением количества таковых сотрудников, потому как масштаб компании начинает прямолинейно определяться количеством её служащих, ровно как и вероятность сопутствующего риска. Иерархическими системами, с каждым новым вживлённым одноранговым механизмом, становится всё сложнее управлять, что постепенно и планомерно начинает приводить к более частым нарушениям политик безопасности её сотрудниками, и как следствие, снова к увеличению рисков.

2. Новые участники рынка, не представляющие монополию, могут «отыграться», создавая сразу одноранговые системы с экономическими механизмами, тем самым инициализируя конкуренцию на рынке неоднородных систем, и в конечном счёте реконструируя «монополию в децентрализованном представлении». Корпорации же начинают понимать, что если не подавлять такие новые системы, либо экономическим путём (опережение, покупка), либо политическим (запреты), то таковые системы рано или поздно начнут формировать новые экономические рынки, на которых у таковых компаний уже не будет власти. Поэтому сами монополии продолжают общее движение к новым рынкам самоличной деструктуризации, ризоморфности, разложению централизации. При этом стоит заметить, что краткосрочными интересами являются политические подавления, а долгосрочными – экономические, но в любом случае, какой бы исход централизация не выбрала, она самолично придёт к своему фатальному расщеплению.

На основе данных противоречий начинают зарождаться ростки, приводящие к началу развития скрытых систем, когда компаниям и корпорациям становится выгоднее управлять гибридными или децентрализованными системами, нежели сложными иерархическими структурами. При этом таковые корпорации не ставят целью полное и окончательное искоренение централизованных механизмов, потому как финальная замена приведёт к моментальному банкротству, что стало бы явным противоречием экономической рациональности на основе которой зарождались два вышеописанных противоречия. Такие ростки, отмирающей иерархичности и отрывающейся децентрализации, становятся связывающими, интерстициальными узлами между централизованными и скрытыми системами посредством экономической целесообразности. Результатом подобных действий становятся концепты технологий «Web3»[13].

[13] Помимо термина «Web3» существует также термин «Web 3.0». Данные термины не являются синонимами, потому как под первым преимущественно понимаются концепты построения клиент-безопасных приложений с экономической моделью, в то время как под вторым понимается взаимосвязанность разнородных сетей для возможности автоматического чтения и/или обмена информацией (семантическая паутина). Последний концепт в прямом смысле этого слова также не реализован как и первый, но противоречиво и через своё отрицание воссоздаётся в парсинге открытой WEB информации, полностью нестандартизированной, но повсеместно практикуемой. Оба концепта являются параллельным следствием развития этапов «Web 1.0» и «Web 2.0», и не противоречат друг другу.

Идея «Web3» становится продолжением, эволюцией «Web 1.0» и «Web 2.0», которые являясь централизованными системами, представляют разные методы управления содержанием. Так например, сутью «Web 1.0» являлось создание базовой информации (контента) на стороне самого сервиса. Иными словами, сам сервис и производил весь основной контент, а клиенты лишь были его потребителями. Концепция «Web 2.0» сменила данный механизм, посредством смешивания функций. Теперь клиенты могут не только вбирать в себя контент, но и создавать его, в то время как функциями сервиса становится лишь редактирование уже существующего содержания, как форма остаточных действий. «Web3» исключает данный остаток, переводя все действия исключительно клиентской стороне. Существует два основных противоположных мнения насчёт концепции «Web3» [52].

1. Термин «Web3» представляет собой проект при котором пользователи вернут контроль над своими данными и генерируемым контентом, тем самым сделав децентрализацию доминируемой формой выражения сетевых коммуникаций над централизованной экономической составляющей. Более не будет монополистических корпораций, желающих на базе конфиденциальной информации, посредством её продажи, увеличивать свой капитал. Плюс к этому открываются рынки для обычных пользователей, способных обменивать свой контент на денежную составляющую без непосредственных централизованных посредников [53][54].

2. Термин «Web3» представляет собой просто маркетинговый ход, который играет на проекте децентрализованного будущего без корпораций и монополий. За счёт данной составляющей, выгоду получают исключительно (или в большей мере) те, кто разрабатывает, спонсирует или инвестирует в подобные приложения. При этом экономическая составляющая «Web3» технологий, на первых порах являющиеся либертарианской, будет постепенно стремиться по рыночным законам к концентрации капитала, и как следствие, вновь к централизации всех возможных ресурсов (денежных, информационных, коммуникационных) [55]. Также предполагается, что таковой «Web3» может быть крайне проблематичен и сомнителен в своих реализациях [56].

Нельзя однозначно сказать, что какое-то из этих мнений неправильно или полностью правильно. В своей совокупности таковые суждения придерживаются крайних позиций, в то время как сущность «Web3» более гибридна по своему содержанию. Именно поэтому правильность или неправильность двух суждений становится одним содержательным синтезом, в котором проявляются одновременно первые ростки децентрализации со свойством клиент-безопасных приложений и повсеместная монополизация капитала с привязкой иерархических систем.

Противоречие свидетельствует о недостаточной зрелости скрытых систем, но и в это же самое время, указывает на фактор эволюции централизованных структур, переходящих в децентрализованные вычисления. Таким образом, сам вектор развития подобных концепций и технологий постепенно направляется на безопасность клиентской стороны и на «разложение» централизованных соединений (что противоречит второму суждению на счёт постоянной монополизации), но при этом выстраивание такого вектора является лишь второстепенной задачей, потому как первоочередной целью становится несомненно выгода, увеличение капитала монополистическими корпорациями (что противоречит первому суждению на счёт самоцели в децентрализованных формах).

В результате, множество технологий «Web3» становится лишь способом, своеобразным механизмом перехода от централизованных монополистических форм к скрытым системам, посредством видоизменения и смешивания разных, чуждых, противоречивых друг к другу целей – необходимости в информационной безопасности и экономической рационализации.

Список литературы

1. Кан, Д. Взломщики кодов / Д. Кан. — М.: ЗАО Изд-во Центрполиграф, 2000. - 473 с.
2. Сингх, С. Тайная история шифров и их расшифровки / С. Сингх. — М.: АСТ: Астрель, 2009. - 447 с.
3. Граймс, Р. Апокалипсис криптографии / Р. Граймс. — М.: ДМК Пресс, 2020. - 290 с.
4. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. - 960 с.
5. Попова, А. Интернет как сетевая или иерархическая структура: концепция сети в постмодернистской философии и социальных науках конца XX-го и начала XXI-го вв. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/internet-kak-setevaya-ili-ierarhicheskaya-struktura-kontseptsiya-seti-v-postmodernistskoy-filosofii-i-sotsialnyh-naukah-kontsa-xx-go-i (дата обращения: 02.01.2022).
6. Бодрийяр, Ж. Символический обмен и смерть / Ж. Бодрийяр. — М.: РИПОЛ классик, 2021. – 512 с.
7. Шнайер, Б. Beyond Security Theater [Электронный ресурс]. — Режим доступа: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html (дата обращения: 16.03.2022).
8. Меньшиков, Я., Беляев, Д. Утрата анонимности в век развития цифровых технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/utrata-anonimnosti-v-vek-razvitiya-tsifrovyh-tehnologiy (дата обращения: 04.01.2022).
9. Молчанов, А. Парадокс анонимности в Интернете и проблемы ее правового регулирования [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/paradoks-anonimnosti-v-internete-i-problemy-ee-pravovogo-regulirovaniya (дата обращения: 12.07.2022).
10. Симаков, А. Анонимность в глобальных сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/anonimnost-v-globalnyh-setyah (дата обращения: 04.01.2022).
11. Рабинович, Е., Шестаков, А. Способ управления трафиком в BitTorrent-сетях с помощью протокола DHT [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodnaya-reaktsiya-na-deystviya-edvarda-snoudena (дата обращения: 26.09.2022).
12. Зденек, Ш. Международная реакция на действия Эдварда Сноудена [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodnaya-reaktsiya-na-deystviya-edvarda-snoudena (дата обращения: 26.09.2022).
13. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. - СПб.: Питер, 2003. - 368 с.
14. Спраул, М. Антимонопольная практика и цены [Электронный ресурс]. — Режим доступа: https://prompolit.ru/files/560276/sproul.pdf (дата обращения: 26.09.2022).
15. Иванов, А. Мифы о легальной монополии, или сказ о том, почему в России не развиваются инновации при упорной охране интеллектуальной собственности [Электронный ресурс]. — Режим доступа:

https://www.hse.ru/data/2020/03/16/1565183163/086-102_%D0%B8%D0%B2%D0%B0%D0%BD%D0%BE%D0%B2.pdf?ysclid=l8ihr02tc6145956359 (дата обращения: 26.09.2022).
16. Смыгин, К. Тайные сговоры, повышение цен, рост безработицы и другие риски, которые таят в себе монополии. Ключевые идеи из бестселлера «Миф о капитализме» [Электронный ресурс]. — Режим доступа: https://rb.ru/opinion/mif-o-kapitalizme/?ysclid=l8ii06vu6s628640881 (дата обращения: 26.09.2022).
17. 5-5-3-5: проще штрафы платить, чем ИБ внедрять [Электронный ресурс]. — Режим доступа: https://habr.com/ru/company/dsec/blog/677204/?ysclid=l8iii2g114542316743 (дата обращения: 26.09.2022).
18. Иванович, Я. Может ли быть "монополия без монополиста"? [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mozhet-li-byt-monopoliya-bez-monopolista (дата обращения: 26.09.2022).
19. Анохин, Ю., Янгаева, М. К вопросу о MITM-атаке как способе совершения преступлений в сфере компьютерной информации [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-mitm-atake-kak-sposobe-soversheniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 04.01.2022).
20. Молоков, В. К вопросу о безопасном шифровании в интернет-мессенджерах [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-bezopasnom-shifrovanii-v-internet-messendzherah (дата обращения: 04.01.2022).
21. Вишневская, Ю, Коваленко, М. Анализ способов и методов незаконного распространения личных данных пользователей мессенджеров, социальных сетей и поисковых систем [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/analiz-sposobov-i-metodov-nezakonnogo-rasprostraneniya-lichnyh-dannyh-polzovateley-messendzherov-sotsialnyh-setey-i-poiskovyh-sistem (дата обращения: 30.12.2021).
22. Diffie, W., Hellman, M. New Directions in Cryptography [Электронный ресурс]. — Режим доступа: https://ee.stanford.edu/~hellman/publications/24.pdf (дата обращения: 19.12.2020).
23. Шнайер, Б., Фергюсон, Н. Практическая криптография / Б. Шнайер, Н. Фергюсон. - М.: Издательский дом «Вильямс, 2005. - 420 с.
24. Соснин, М. Реализация оптимальной архитектуры и Обеспечение безопасного функционирования сети ЭВМ [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/realizatsiya-optimalnoy-arhitektury-i-obespechenie-bezopasnogo-funktsionirovaniya-seti-evm (дата обращения: 26.09.2022).
25. Dwivedy, A. Secure File Sharing in Darknet [Электронный ресурс]. — Режим доступа: https://www.ijert.org/research/secure-file-sharing-in-darknet-IJERTV3IS10878.pdf (дата обращения: 06.11.2022).
26. Михайленко, Н., Мурадян, С., Вихляев, А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/aktualnye-voprosy-monitoringa-i-protivodeystviya-kiberugrozam-v-odnorangovyh-setyah (дата обращения: 26.09.2022).
27. Садаков, Д., Сараджишвили, С. Рекомендательный протокол децентрализованной файлообменной сети [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/rekomendatelnyy-protokol-detsentralizovannoy-fayloobmennoy-seti (дата обращения: 29.03.2022).

28. Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [Электронный ресурс]. — Режим доступа: https://www.lix.polytechnique.fr/~tomc/P2P/Papers/Theory/MIXes.pdf (дата обращения: 16.08.2022).
29. Ершов, Н., Рязанова, Н. Проблемы сокрытия трафика в анонимной сети и факторы, влияющие на анонимность [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/problemy-sokrytiya-trafika-v-anonimnoy-seti-i-faktory-vliyayuschie-na-anonimnost (дата обращения: 02.01.2022).
30. NETSUKUKU RFC документация [Электронный ресурс]. — Режим доступа: http://netsukuku.freaknet.org/sourcedocs/main_doc/ntk_rfc/ (дата обращения: 31.12.2021).
31. Danezis, G., Diaz, C., Syverson, P. Systems for Anonymous Communication [Электронный ресурс]. — Режим доступа: https://www.esat.kuleuven.be/cosic/publications/article-1335.pdf (дата обращения: 27.09.2022).
32. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные коды на языке С / Б. Шнайер. — СпБ.: ООО «Альфа-книга», 2018. - 1040 с.
33. Шелухин, О., Канаев, С. Стеганография. Алгоритмы и программная реализация / О. Шелухин, С. Канаев. — М.: Горячая линия - Телеком, 2018. - 592 с.
34. Карпов, Д., Ибрагимова, З. Способы и средства обеспечения анонимности в глобальной сети Интернет [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/sposoby-i-sredstva-obespecheniya-anonimnosti-v-globalnoy-seti-internet (дата обращения: 15.07.2022).
35. Рябко, Е. Калейдоскоп vpn технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kaleydoskop-vpn-tehnologiy (дата обращения: 02.01.2022).
36. Накамото, С. Биткойн: система цифровой пиринговой наличности [Электронный ресурс]. — Режим доступа: https://bitcoin.org/files/bitcoin-paper/bitcoin_ru.pdf (дата обращения: 19.12.2020).
37. Warren, J. Bitmessage: A Peer-to-Peer Message Authentication and Delivery System [Электронный ресурс]. — Режим доступа: https://bitmessage.org/bitmessage.pdf (дата обращения: 31.12.2021).
38. Perry, M. Securing the Tor Network [Электронный ресурс]. — Режим доступа: https://www.blackhat.com/presentations/bh-usa-07/Perry/Whitepaper/bh-usa-07-perry-WP.pdf (дата обращения: 03.01.2022).
39. Astolfi, F., Kroese, J., Oorschot, J. I2P - Invisible Internet Project [Электронный ресурс]. — Режим доступа: https://staas.home.xs4all.nl/t/swtr/documents/wt2015_i2p.pdf (дата обращения: 03.01.2022).
40. Danezis, G., Dingledine, R., Mathewson, N. Mixminion: Design of a Type III Anonymous Remailer Protocol [Электронный ресурс]. — Режим доступа: https://web.archive.org/web/20170312061708/https://gnunet.org/sites/default/files/minion-design.pdf (дата обращения: 03.01.2022).
41. Рябко, Б., Фионов, А. Криптография в информационном мире / Б. Рябко, А. Фионов. - М.: Горячая линия - Телеком, 2019. - 300 с.
42. Chaum, D. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability [Электронный ресурс]. — Режим доступа: https://www.cs.cornell.edu/people/egs/herbivore/dcnets.html (дата обращения: 24.07.2022).
43. Goel, S., Robson, M., Polte, M., Gun Sirer, E. Dissent in Numbers: Making Strong Anonymity Scale [Электронный ресурс]. — Режим доступа: https://dedis.cs.yale.edu/dissent/papers/osdi12.pdf (дата обращения: 24.07.2022).

44. Corrigan-Gibbs, H., Wolinsky, D., Ford, B. Proactively Accountable Anonymous Messaging in Verdict [Электронный ресурс]. — Режим доступа: https://dedis.cs.yale.edu/dissent/papers/verdict.pdf (дата обращения: 24.07.2022).
45. Alonso, K., KOE. Zero to Monero: First Edition A technical guide to a private digital currency; for beginners, amateurs, and experts [Электронный ресурс]. — Режим доступа: https://www.getmonero.org/library/Zero-to-Monero-1-0-0.pdf (дата обращения: 28.12.2021).
46. Duffield, E., Diaz, D. Dash: Privacy-Centric Crypto-Currency [Электронный ресурс]. — Режим доступа: https://web.archive.org/web/20150514080026/https://www.dashpay.io/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf (дата обращения: 28.12.2021).
47. Бартлетт, Д., Подпольный интернет: Темная сторона мировой паутины / Д. Бартлетт. – М.: Эксмо, 2017. - 352 с.
48. Бондаренко, Ю., Кизилов, Г. Проблемы выявления и использования следов преступлений, оставляемых в сети «Darknet» [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/problemy-vyyavleniya-i-ispolzovaniya-sledov-prestupleniy-ostavlyaemyh-v-seti-darknet (дата обращения: 20.10.2022).
49. Гонов, Ш., Милованов, А. Актуальные вопросы противодействия преступности в сети Даркнет [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/aktualnye-voprosy-protivodeystviya-prestupnosti-v-seti-darknet (дата обращения: 20.10.2022).
50. Pfitzmann, A., Hansen, M. Anon Terminology [Электронный ресурс]. — Режим доступа: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (дата обращения: 20.10.2022).
51. Reiter, M., Rubin, A. Crowds: Anonimity for Web Transactions [Электронный ресурс]. — Режим доступа: https://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/crowds.pdf (дата обращения: 20.10.2022).
52. Взлетит или нет – две разные точки зрения на Web3 [Электронный ресурс]. — Режим доступа: https://habr.com/ru/company/vasexperts/blog/670964/ (дата обращения: 30.10.2022).
53. Dabit, N. What is Web3? The Decentralized Internet of the Future Explained [Электронный ресурс]. — Режим доступа: https://www.freecodecamp.org/news/what-is-web3/ (дата обращения: 30.10.2022).
54. Решетникова, М. Без владельцев и цензуры: каким будет интернет эпохи Web3 [Электронный ресурс]. — Режим доступа: https://trends.rbc.ru/trends/industry/629070a99a79470ec4bdb673 (дата обращения: 30.10.2022).
55. Ingram, D. What is web3? It’s Silicon Valley’s latest identity crisis [Электронный ресурс]. — Режим доступа: https://www.nbcnews.com/science/science-news/web3-s-silicon-valleys-latest-identity-crisis-rcna9846 (дата обращения: 30.10.2022).
56. Marklinkspike, M. My first impressions of web3 [Электронный ресурс]. — Режим доступа: https://moxie.org/2022/01/07/web3-first-impressions.html (дата обращения: 30.10.2022).