Теория строения скрытых систем

Коваленко Геннадий Александрович

1. Введение

Децентрализация, как первичная форма Интернет-коммуникаций в целом, появлялась на фоне академических исследований [1, 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 децентрализации стала проблема масштабируемости связей. Невозможность в построении широковещательных и широкомасштабных соединений повлекли за собой потребность в промежуточных узлах, основаниях концентрации линий связи, тем самым, зародив ядро централизации, как точку отчёта дальнейшей проблематики.

Централизация, как вторая форма развития Интернет-коммуникаций, появилась на фоне разложения и отмирания первичной, децентрализованной оболочки [2]. Представляя свои плюсы масштабируемости, централизация начала претерпевать внутренние этапы развития, как итерации наложения слоёв абстракций и отрицания децентрализации, противоречиво став для последней фазой её собственной эволюции. При каждой новой итерации своего прогресса, централизованная система всё больше масштабируется, всё сильнее углубляется корнями, всё чаще репрезентует себя, образуя тем самым симулякры [3, с.111] второго порядка. Одновременно с этим, система нейтрализует внешние атаки, ранее губительные для её ядра, но ныне безвредные для её функционирования, как пример атаки в обслуживании [1, с.869] (DDoS) или внешние хакерские нападения с учётом изъятия внутренней информации. В следствие такого развития, система начинает порождать общество всё более абстрагируемое от её механизма, всё более спящее, и напоминающее больше зрителя, чем инициатора. В итоге система запускает собственную инициализацию своих внутренних интересов, направленных на пользователей, тем самым инвертируя способ взаимодействия с ними. При выстроенном императиве, система образовывает множество симулякров третьего порядка, подменяя реальность иллюзорностью происходящего в своём внутреннем слое, за полями созданных абстракций и закрытого исходного кода. Примером ложного представления становится «театр безопасности» [4], направленный на поддержание имеющегося порядка вещей, спокойствия и веру в сохранность личной информации.

Внешние угрозы информационной безопасности хоть и становятся полностью безвредными для централизованной системы в ходе её эволюции, но такое утверждение ничего не говорит 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 вызывает аккумулятивную реакцию внутренних интересов её же участников. Внутреннему сотруднику компании становится выгодно продавать информацию об её пользователях при расширении системы; государству становится выгодно концентрировать линии связи в одном сингулярном пространстве, в следствие возможности массового слежения и контроля общественным мнением; рекламодателю становится выгодно вкладывать свои средства в массовую систему с наиболее релевантным алгоритмом выдачи реклам на базе конфиденциальной информации клиентов, тем самым повышая свою прибыль [5]. И данная проблема информационной безопасности со стороны

централизованных систем не может быть решена ей же, потому как она в самом базисе и своём ядре рассчитана на собственную масштабируемость и репрезентацию. Именно поэтому, жизнь централизованной системы прямо пропорционально зависит от количества слоёв абстракций, от количества копий без собственных оригиналов.

Гибридность, как третья форма развития Интернет-коммуникаций, отрицает централизацию, и в то же время, синтезирует её с децентрализацией. Оставляя масштабируемость, но отрицая внутреннее развитие централизации, происходит синтез внешнего развития децентрализации, как способа транспарентного доказательства функционирования без слоёв абстракций и симулякров третьего порядка. Такая система более невосприимчива к внутренним и внешним атакам, более нет внутреннего сотрудника, разглашающего информацию; государству становится не под силу эффективно собирать информацию; рекламодателю становится невыгодно вкладывать свои финансы. Подобный прогресс также несёт за собой и относительный регресс, потому как сама жизнеспособность системы начинает зависеть от её же участников и их энтузиазма. Более нет постоянного финансирования, а централизованные системы (в частности и само государство) являются враждебными к её существованию [6]. Порождённость централизацией и враждебность к ней является важным фактом противоречия и главным фактором разложения гибридности, посредством её будущего разделения и расщепления.

Децентрализация, как четвёртая форма развития Интернет-коммуникаций, становится масштабируемой и одновременно безопасной средой пользователей. Более не существует проблем гибридности, потому как ликвидировать систему централизацией более становится невозможным из-за её ризоморфного характера, как отрицания иерархического. Любой пользователь становится в конечном счёте олицетворением самой системы. На данном этапе безопасность информации начинает эволюционировать и переходить на безопасность её субъектов более качественном, тем самым образуя, в своём финальном проявлении, полную и абсолютную анонимность. Система децентрализованная лишается всех своих первичных недостатков начальной формы и становится в конечном счёте снятием итераций отрицания.

2. Первичная проблематика

При рассмотрении вопросов, базируемых на безопасности каналов связи, использующих криптографические протоколы с участниками *A* и *B*, 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 [7]. Приведённая атака ссылается на нерешённую проблему доверия[1], разрушительную и губительную по своей сути, но при этом затмевающую более скрытую и деструктивную, мощь которой в современном мире превосходит прямолинейные MITM атаки. Целью нашей статьи является выявление данного метода нападения, его анализ и последующие решения.

---

[1]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.

Возможность атаки со стороны принимающей стороны 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, 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 [8][9]. Примером такого явления служат современные мессенджеры, социальные сети, форумы, чаты, файловые сервисы и т.д., где общение не происходит напрямую (как это предполагается в криптографических протоколах), а всегда проходит сквозь стороннюю точку, представляющую собой сервис или платформу связи.

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 [10]. Данная апория куда серьёзнее и значимее, нежели классическая MITM атака и требует куда меньшее количество затрат атакующего для слежки большего количества атакуемых. Это есть паноптикум 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, оболочку воображаемого величия, 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».

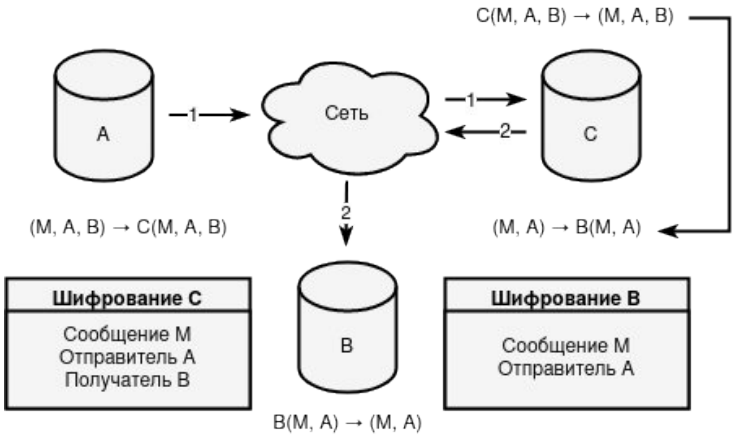

Рис. 1. Коммуникация субъектов *A*, *B* посредством общего сервиса *C*

Итогом такого развития считается возникновение систем доверия, где не только сами доверительные узлы становятся атакующими, но и промежуточные получатели, что приводит к

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 маркетинга, продажи релевантной рекламы.

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 [11, 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 иную систему, механизм которой стремился бы к уменьшению мощности доверия[2], в которой собственная её структура представляла бы защиту объектов и анонимат субъектов. К системам подобного рода уже относятся анонимные сети и тайные каналы связи, анализ и развитие которых представлен в последующих разделах.

3. Определение скрытых сетей

Скрытые, тёмные, анонимные сети — есть сети, соединяющие и объединяющие маршрутизацию вместе с шифрованием. Маршрутизация обеспечивает критерий анонимности, направленный на субъект, шифрование — критерии конфиденциальности, целостности, аутентификации, направленные на объект. Без маршрутизации легко определяются отправитель/получатель, без шифрования легко определяется передаваемое сообщение. Таким образом, только в совокупности этих двух свойств сеть может являться скрытой [12][1, с.912].

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 [13]. Именно по историческим причинам, современные сети имеют оверлейные уровни безопасности.

Любая анонимная сеть основывается либо на одноранговой (ризоморфной), либо на гибридной архитектуре сети, исключая при этом многоранговую (иерархическую). Последняя в свою очередь не способна к анонимности, потому как всегда представляется константной величиной мощности анонимности[3].

---

[2]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 будет возникать лишь в моменты отсутствия каких-либо связей и соединений. Если мощность доверия равна единице, это говорит о том, что связь защищена, иными словами, никто кроме отправителя и получателя информацией не владеют. Во всех других случаях мощность доверия будет больше единицы, что говорит о групповой связи (то-есть, о существовании нескольких получателей), либо о промежуточных узлах, способных читать информацию в открытом виде.

[3]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 равной единице (вне зависимости от количества серверов). Нулевая мощность

Многоранговые сети разделяются 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. Сеть на основе многоранговой архитектуры расширяется изнутри, относительно своего ядра, и не допускает расширения извне. Из вышеописанного также следует, что классическая централизованная структура является лишь частным случаем более общей распределённой структуры, или иными словами, сам факт распределённости становится следствием централизации.

В одноранговых (peer-to-peer) системах все пользователи однородны, имеют одинаковые возможности, могут представлять одни и те же услуги маршрутизации [1, с.792]. Сами одноранговые сети могут быть разделены на три модели: централизованные, децентрализованные и распределённые. Централизованные одноранговые сети представляют собой соединения на базе одного или нескольких заранее выделенных серверов-ретрансляторов, исключение которых приводит к блокированию всей сети, тем самым отсутствие прав серверов 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 нодами, иными словами, со всей сетью (иногда под распределённой связью подразумевают необходимое *N*-ое количество соединений, не обязательно со всей сетью). В децентрализованных же сетях возможно образование неравномерного распределения соединений и появление «неофициальных» узлов-серверов, часто используемых другими нодами в качестве последующей маршрутизации. Таким образом, децентрализованная модель в своём определении куда сильнее подвержена концентрированию линий связи, чем модель распределённая. Сеть на основе одноранговой архитектуры расширяется извне, не образуя тем самым статичное ядро даже в своей централизованной модели.

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 является возможность разделения логики на серверную и клиентскую, а также более быстрая и/или статичная скорость маршрутизации. Плюсом одноранговых архитектур является высокая отказоустойчивость за счёт внешнего расширения сети и возможность построения безопасной «клиент-клиент» связи. Минусом гибридных архитектур является их возможный, осуществимый и более вероятностный переход в многоранговые системы (по сравнению с одноранговыми) за

анонимности возникает либо при отсутствии связей, либо при существовании прямого соединения между субъектами (иными словами при отсутствии какой бы то ни было маршрутизации).

$$|A| = |F(N)| - \sum_{i=1}^{|W|} \begin{cases} 0, W_i = \varnothing \\ |W_i| - 1, W_i \neq \varnothing \end{cases},$$

где $W = E(F(N))$,

N - множество узлов, расположенных в сети,

F - функция выборки множества узлов, участвующих в маршрутизации,

E - функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами.

счёт большого уплотнения серверов принадлежащих одному лицу, либо группе лиц с общими интересами.

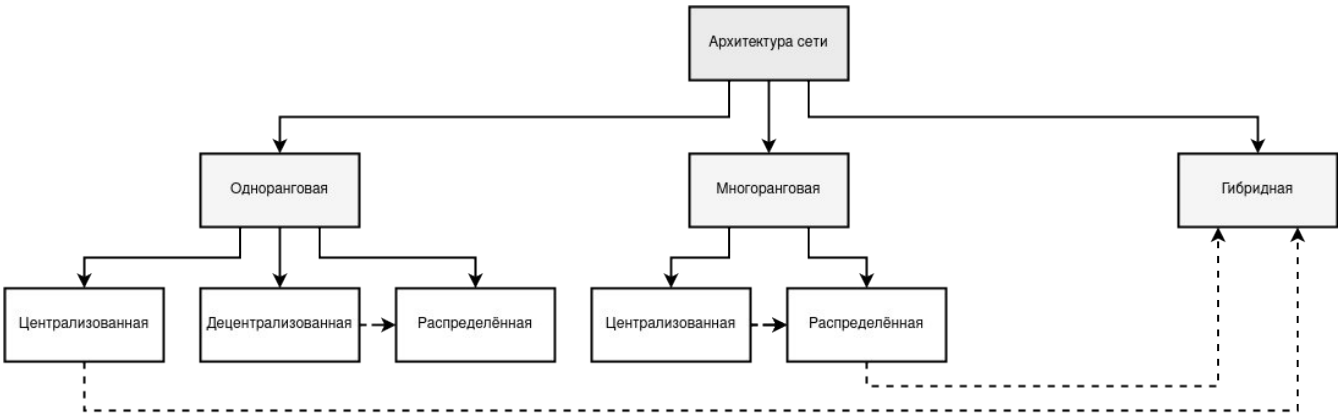

Рис. 2. Архитектуры построения сетей с прилагаемыми моделями

Становление одноранговой 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 в «сожительстве» с многоранговой системой [14]. Последняя в буквальном смысле «поглотила» примитивную одноранговую централизацию, 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, но не за счёт её эволюции, как постепенного и планомерного развития, а уже за счёт революции, как скачкообразного и моментального прогресса. Итогом такого процесса стало объединение клиентской составляющей с серверной частью, породив тем самым узлы связи, как отдельные сетевые единицы коммуникации.

Становление одноранговой распределённой системы является следствием 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 устойчивости, — 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 уже в лице количества узлов, а не их качества.

Становление многоранговой распределённой системы из классической централизованной является важным составляющим фактором эволюции существующих иерархических сетей. Данное «разложение» начинается на этапе разделения функций, приравнивая сервер к определённому действию. 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. 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. Во всех последующих упоминаниях под термином «централизация» будет пониматься именно конечная фаза эволюции многоранговой архитектуры.

Становление гибридной системы проходит в следствие синтеза одноранговой централизации и многоранговой распределённости. С одной стороны, одноранговая архитектура избавляет систему частично или полностью от ядра внутренней иерархии, разбавляя систему внешними одноранговыми связями. С другой стороны, многоранговая архитектура преобразует примитивные редирект-функции, изменяя форму передачи информации и сохраняя иерархию между сервером-клиентом. Внешним противоречием гибридности является сильная схожесть с «классическими» (децентрализованными, распределёнными) моделями одноранговой архитектуры, при этом не являясь их прямым вырождением. Иными словами, при рассмотрении внутреннего фрагмента системы, сама сеть начинает анализироваться как прозрачно одноранговая, но при целостном осмотре системы, а не только её составной части, она начинает обретать «краски» иерархичности и быть зависимой от действий клиентов, тем самым становясь несамостоятельной в своих функциях исполнения, и как следствие не одноранговой в своём проявлении. Таким образом, противоречием системы является симуляция одноранговой распределённости её многоранговым аналогом, и многоранговой централизации её одноранговым дженериком.

4. Развитие сетевой анонимности

Анализируя сетевую анонимность как объект, стоит сразу отметить её фрагментированность со стороны определений и терминологий, что предполагает также её неоднородность, а следовательно и становление как таковое. В кратце, анонимность можно трактовать как некую градацию, поэтапность, которой присуще семь стадий, выявляющих процесс её формирования посредством фаз отрицаний и внутренних противоречий.

1. Первая стадия является исходной точкой анонимности, тезисом, монадой не представляющей анонимность, пустотой инициализирующей мощность анонимности $|A| = 0$. Примером является отсутствие связи как таковой или 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.

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) не является случайным, а представляет собой правило и закономерность, в чём можно будет убедиться далее. Описанную стадию вкратце именуют псевдо-анонимностью, а клиентов — анонимами.

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 пакет. 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.

4. Четвёртая стадия, как развитие третьего этапа, инициализирует способ изменчивости, множественного шифрования, полиморфизма информации посредством её туннелирования. К такому этапу относятся L4 VPN сервисы (виртуальные частные сети) как N-ое сочетание прокси-серверов со внутренними слоями шифрования [15], где мощность доверия и мощность анонимности эквивалентно третьей стадии. Отличительной особенностью четвёртого этапа является существование выходных узлов, постепенно «раскрывающих» истинный пакет, созданный до первичного туннелирования на 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, относительно третьей стадии.

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. [16][17], где главным фактором идентификации клиентов являются криптографические адреса (публичные ключи, хеши публичных ключей). Сеть представляет собой также, как и в третьей стадии, гибридный, разрозненный 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 маршрутизацией [1, 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.

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 шестом разделе «Проблематика анонимных сетей»). Примером шестой стадии является большинство скрытых сетей, наподобие Tor (onion routing) [18], I2P (garlic routing) [19], Mixminion (mix network) [20] и т.д.

7. Седьмая стадия повышает анонимность до абсолюта, теоретического максимума за счёт объединения свойств полиморфной и слепой маршрутизации, образовывая новую, виртуальную маршрутизацию. Данный этап применяет конъюнкцию на основные характеристики пятой и шестой стадий, иными словами, предполагает распространение объекта по всем узлам с вероятностной возможностью его полиморфизма. Мощность анонимности определяется следующим методом — $lim_{|A|' \to C} \leq |A| \leq N$, где N — количество узлов в сети, C — количество узлов участвующих в маршрутизации из всего множества сети. Двойственная мощность, с неравенством и пределом, обуславливается двойным способом маршрутизации. Данный этап может быть основой, ядром скрытых сетей, а также тайных каналов связи. В отличие от шестой стадии анонимности, где скрытые сети могут быть как одноранговыми, так и гибридными, сеть на основе седьмой стадии может быть только одноранговой (дальнейшее изложение более подробно акцентирует внимание на анализе седьмой стадии, доказывает и подтверждает выдвинутые тезисы).

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 поддержка одноранговых соединений. С другой стороны, пятая стадия также справедливо могла стать четвёртой, базируясь не на развитие анонимности субъектов, а на развитие 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 распространение 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.

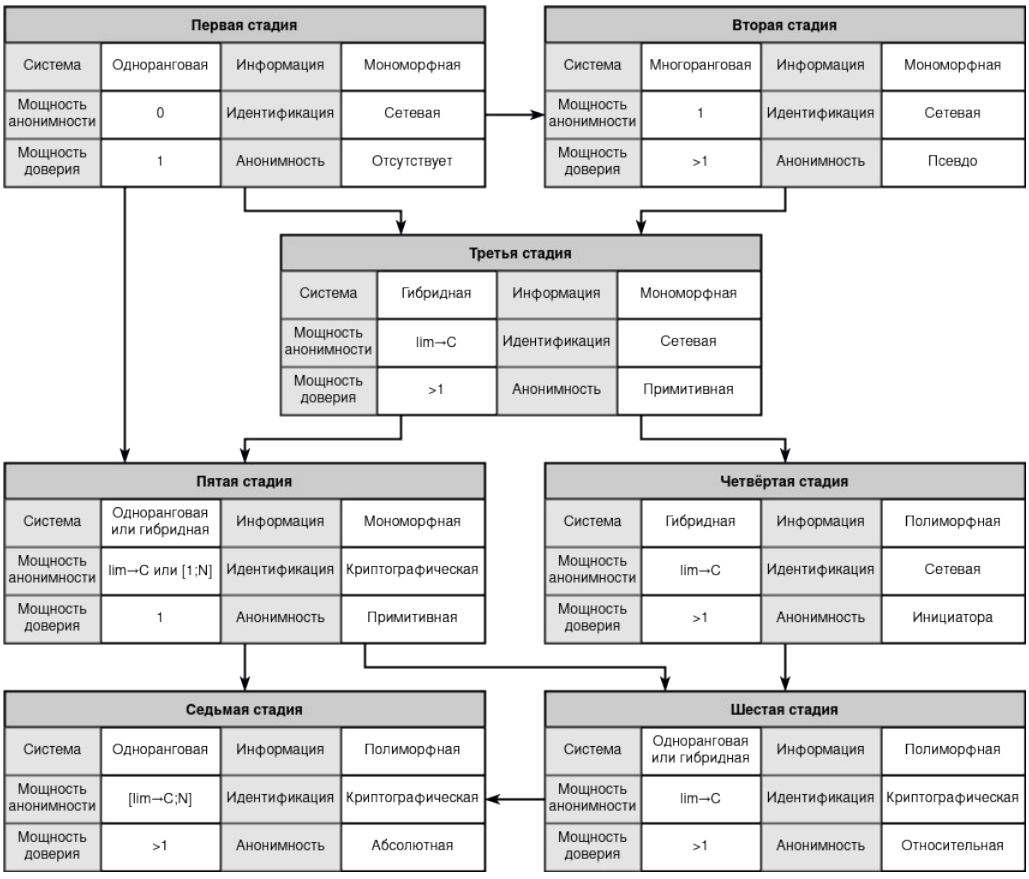

Рис. 3. Развитие анонимности как процесс формирования стадий

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.

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 [21, 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.

Из всего вышесказанного можно вывести основные критерии анонимности на базе которых будет доступно формирование скрытых сетей с повышенным уровнем безопасности.

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 полиморфизма информации.

2. Анонимность обязана быть двунаправленной относительно субъектов информации и применяться как к отправителю — инициатору связи, так и к получателю — платформе связи. 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.

4. Анонимность абсолютная обязана существовать даже в заведомо враждебной, замкнутой и полностью прослушиваемой системе. Данный критерий должен обуславливаться модификацией первого критерия, а именно заменой полиморфизма на вероятностный полиморфизм.

На базе всего вышесказанного можно выявить определение анонимности относительно общего вида скрытых сетей, на основании её первых трёх пунктов. Таким образом, под сетевой анонимностью будет пониматься разрыв большинства логических связей между транспортируемым/хранимым объектом и его субъектами, а также между идентификацией сетевой и криптографической.

5. Становление седьмой стадии анонимности

Продолжая анализ развития анонимных сетей, можно ссылаться на методы нападений, которые в своей совокупности являются способами совершенствования последующих сетевых формаций. Так, например, большинство атак, направленных на скрытые сети, представляют способы деанонимизации субъектов (как наиболее лёгкий способ), нежели попытки раскрытия, взлома, дешифрования объектов (как наиболее сложный).

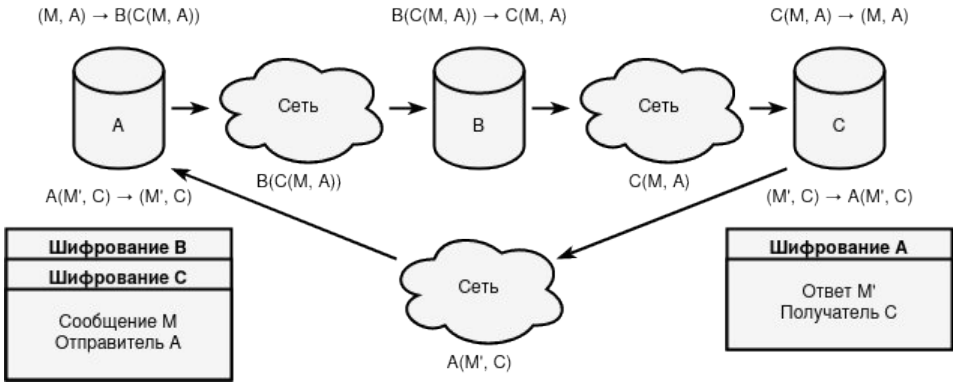

Рис. 4. Обобщённая схема полиморфизма информации на базе седьмой стадии анонимности

Одной из достаточно сильных и сложно искоренимых атак на одноранговые (а следовательно, и на гибридные) сети является атака Сивиллы [22]. Она базируется на том факте, что главным способом анонимности является элемент маршрутизации, который обеспечивается за счёт передачи информации посредством нескольких узлов. С одной стороны, сутью атаки является замена несвязанных между собой узлов, на узлы подчинённые одному лицу, либо группе лиц с общими интересами, тем самым, атака ориентируется на ($lim_{|A|\to 1}$) уменьшение мощности анонимности до единицы. С другой стороны, в некоторых видах сетей с увеличенной мощностью доверия, атака может вредить и целостности передаваемой информации, иными словами, подменять и видоизменять её. При повышении количества узлов несвязанных между собой в сети, повышается и сложность реализации атаки Сивиллы, за счёт более равномерного распределения узлов. Из этого также следует, что мощность анонимности будет стремиться к своим теоретически заданным значениям. Всё это связано с тем, что атакующие узлы будут конкурировать с обычными узлами за возможность быть посредниками между субъектами передаваемой информации. Чем больше несвязанных узлов и лучше алгоритм распределения, тем меньше вероятность осуществления данной атаки. Тем не менее атака Сивиллы особо опасна на этапе зарождения скрытых сетей, когда количество узлов минимально. Решений данной проблемы несколько:

1. Обеспечить замкнутость и сложность встраивания узлов в сеть. Иными словами, использовать фактор доверия или параметр дружбы. Узлы в таких сетях должны выстраивать связи между собой, основываясь на субъективности к уровню доверия. Выстраивая связи друг к другу [23] (или friend-to-friend), узлы также начинают выстраивать связи друг моего друга — это мой скрытый друг. Таким образом, друзья друзей не подключаются напрямую и не знают друг друга, но при этом вполне могут обмениваться информацией между собой, что является показателем увеличения размеров сети. Чтобы успешно подключиться к такой сети, необходимо самому стать доверенным узлом, то есть пользователем, которому кто-либо доверяет. Сложность исполнения атаки, на такой род сети, сводится к сложности встраивания в сеть подчиняемых узлов, как того требует атака Сивиллы, а это, как было описано выше, является проблематичным действием.
Единственная проблема friend-to-friend сетей заключается в их малой эксплозии, расширении, увеличении масштаба, являясь тем самым следствием причины ручной настройки и установки списка доверенных узлов.

2. Осуществить переход к седьмой стадии — крайней форме анонимности. В таком случае, целью является сокрытие, удаление, исключение всех возможных связей между отправляемой информацией (объектом) и самим отправителем/получателем (субъектом).

После исчезновения всех связей, сама маршрутизация перестаёт являться чем-то реальным и настоящим, перерастая тем самым в этап условного и виртуального, где раскрытие даже одного из субъектов начинает быть сложной задачей. Сивилле потребуется, чтобы сеть содержала менее трёх узлов несвязанных между собой общими целями и интересами, иными словами атака базируется на формуле, результат которой должен быть равен двум, $a = N - d$, где N — количество всех узлов в сети, d — количество деанонимизирующих узлов. Для осуществления подобной атаки потребуется примерно $\frac{a\,(a-1)}{2}$ итеративных блокировок всей сети, базируемой на связи *все-ко-всем*, при выдаваемом результате $a > 2$.

Основным и пожалуй главным отрицательным свойством седьмой стадии анонимности является линейное увеличение нагрузки на сеть $O(N)$ со стороны всех пользователей в ней участвующих. Так, например, если сеть состоит из N узлов, то каждый узел должен будет обрабатывать $N - 1$ запросов от других узлов. Время жизни пакета (TTL) на седьмой стадии не является решением данной проблемы, по причине появления новых связей между отправителем и передаваемой информацией, что, следовательно, приведёт к деструктуризации базиса, к дисфункции сокрытия связей, к деградации виртуальной маршрутизации, и как итог, к переходу на шестую стадию анонимности.

Атака Сивиллы может быть рассмотрена и более обще, где вместо встраивания узлов в скрытую сеть, сначала происходит образование подконтрольной первичной сети, на основе которой будет существовать уже последующая тёмная сеть. Такой вид атаки может существовать лишь при оверлейных соединениях, коим и является сеть Интернет для провайдеров связи. Если вся тёмная сеть будет воссоздана в первичной сети, управляемой одним лицом или группой лиц с общими интересами, то, следовательно, и весь трафик скрытой сети возможно будет анализировать, с момента её появления и до момента её гибели. Подобная атака требует огромных ресурсов и первоначально настроенной инфраструктуры, что в современных реалиях под силу лишь государствам. Предотвратить такой вид атаки сложно, но вполне возможно, если соблюдать два правила:

1. Использовать противоречия государств — вариативные и несогласованные законы, политические и империалистические интересы. Всё это есть моменты, при которых одно государство не будет выдавать информацию о своей сети другому государству. И чем более агрессивно настроены страны по отношению друг к другу, тем менее успешно они могут контролировать свои собственные ресурсы. В таком случае, необходимо строить сеть по федеративному принципу, чтобы узлы располагались на разных континентах мира, странах и государствах.

2. Использовать изменения информации в процессе её маршрутизации. При таком способе информация будет представлена в полиморфной и самоизменяющейся оболочке, то есть оболочке шифрованной. Такой подход необходим в моменты, когда информация, приходящая из государства *A* в государство *B*, будет снова возвращаться на свою родину *A*. В качестве примера можно привести луковую маршрутизацию сети Tor, где само шифрование представлено в виде слоёв, которые каждый раз «сдирают», снимают при передаче от одного узла к другому[4].

[4]Мощность федеративности — количество государств, не связанных общей военной силой, через территорию которых проходит маршрутизация полиморфной информации. Из этого следует, что если сеть разворачивается лишь в пределах одного государства, то мощность федеративности по умолчанию будет равна единице. Нулевой мощности федеративности не существует.

Существует также и альтернативный вариант противодействия подобной атаке. Он в отличие от вышеописанного не требует этапа с федеративностью, но взамен требует огромное количество информации, приводящей к спаму. Плюсом такого подхода является возможность использовать его в тайных каналах связи как единственно возможный элемент анонимизации субъектов. Для осуществления такого метода применяются сети основанные на седьмой стадии анонимности, т.к. они распространяют информацию методом вероятностной маршрутизации, что априори ведёт к множественному дублированию, пролиферации объектов. Полиморфизм информации осуществляется способом установки промежуточных получателей (маршрутизаторов) и созданием транспортировочных пакетов, представленных в форме множественного шифрования. Как только узел сети принимает пакет, он начинает его расшифровывать. Если пакет успешно расшифровывается, но при этом сама расшифрованная версия является шифрованным экземпляром, то это говорит о том, что данный принимающий узел — это промежуточный получатель, целью которого является последующее распространение «расшифрованной» версии пакета по сети. Базовый механизм распространения и получения объектов схож с Bitmessage, но в отличие от него, здесь существует свойство полиморфизма, которое образуется методом дополнительной цепной маршрутизации, скрывающей субъектов информации. Рекуперация, в совокупности с конечной рекурсией, будет происходить до тех пор, пока не будет расшифрован последний пакет, предполагающий существование истинного получателя, либо до тех пор, пока пакет не распространится по всей сети и не окажется забытым, по причине отсутствия получателя (будь то истинного или промежуточного). Стоит также заметить, что маршрутизаторы при расшифровании пакета могут узнавать криптографический адрес отправителя, именно поэтому стоит отправлять транспортировочные пакеты из-под криптографического псевдо-адреса отправителя.

Пример программного кода [24][25] для создания транспортировочного пакета:

```
import (
	"bytes"
)
func RoutePackage(sender *PrivateKey, receiver *PublicKey, data []byte, route []*PublicKey) *Package {
	var (
		rpack   = Encrypt(sender, receiver, data)
		psender = GenerateKey(N)
	)
	for _, pub := range route {
		rpack = Encrypt(
			psender,
			pub,
			bytes.Join(
				[][]byte{
					ROUTE_MODE,
					SerializePackage(rpack),
				},
				[]byte{},
			),
		)
	}
	return rpack
}
```

Теперь, если предположить, что в сети существует всего три узла $\{A, B, C\}$ (где один из них является отправителем — A) и сама сеть основывается на седьмой стадии анонимности без полиморфизма информации, то в таком случае и при таком условии крайне проблематично

определить истинного получателя, пока он сам себя не выдаст ответом на запрос (т.к. ответом будет являться совершенно новый пакет, отличный от всех остальных). Иначе, если предположить, что существует возможность полиморфизма информации, то есть вероятность её маршрутизации, то начинается этап слияния свойств получения и отправления, образуя антиципацию. Так, например, если полиморфизм существует, значит будет существовать три этапа: (*A → B ИЛИ A → C*) → (*B → C ИЛИ C → B*) → (*B → A ИЛИ C → A*), но если полиморфизма не существует, то будет два этапа: (*A → B ИЛИ A → C*) → (*B → A ИЛИ C → A*)[5]. При этом предполагается, что системе известен лишь отправитель информации (инициатор), в то время как получатель не определён. Из этого следует, что если полиморфизм будет являться статичной величиной (то есть, будет всегда существовать или не существовать вовсе), то определение получателя будет являться лёгкой задачей (при условии, что он всегда отвечает инициатору). Но, если полиморфизм будет иметь вероятностную величину, то грань между отправлением и получением будет стираться, сливаться, инвертироваться, что приведёт к неоднородному трактованию анализируемых действий: запрос(1) - ответ(1) - запрос(2) или запрос(1) - маршрутизация(1) - ответ(1). Но в таком случае, возникает свойство гипертелии (сверх окончания), где запрос(2) не получает своего ответа(2), что снова приводит к возможности детерминированного определения субъектов. Теперь, если выровнять количество действий полиморфизма (количество маршрутизации пакета) *k* и количество действий без него *n* (что представляет собой всегда константу *n = 2*), иными словами придерживаться формулы *НОД(k, 2) = 2*, где *НОД* — наибольший общий делитель, то получим максимальную неопределённость, алеаторность при константе *k = 2*, которую можно свести к следующему минимальному набору действий полиморфизма: (*A → B ИЛИ A → C*) → (*B → C ИЛИ C → B*) → (*B → C ИЛИ C → B*) → (*B → A ИЛИ C → A*). В итоге все действия начинают трактоваться двумя полностью самодостаточными процессами: запрос(1) - ответ(1) - запрос(2) - ответ(2) или запрос(1) - маршрутизация(1) - маршрутизация(~1) - ответ(1), что в свою очередь приводит к неопределённости отправления и получения информации со стороны анализа трафика всей сети. И потому, ответ(1) = маршрутизация(1), запрос(2) = маршрутизация(~1), а также ответ(2) = ответ(1) = маршрутизация(2), где последняя добавочная маршрутизация(2) получается из запроса(2). Проблемой, в таком случае, является лишь запрос(1), созданный генезис-инициатором связи, который будет трактоваться всегда детерминировано. Но и здесь, в первую очередь, стоит заметить, что при последующих запросах данная проблема всегда будет угасать из-за увеличивающейся энтропии [26], приводящей к хаотичности действий посредством метаморфозов вероятностного полиморфизма. Так например, на следующем шаге появится неопределённость вида запрос(3) = запрос(2) = маршрутизация(~2), означающая неоднозначность выявления отправителя. Итоговую модель можно представить следующим способом:

Метаморфозы вероятностного полиморфизма	Расширение энтропии
1. (*A → B ИЛИ A → C*) [# *A* - инициатор] [# *B или C* - получатель или маршрутизатор]	1, 2. [запрос(1)] → | 0 бит |
2. (*B → C ИЛИ C → B*) [# *B или C* - маршрутизатор] *ИЛИ* (*B → A ИЛИ C → A*)	1. [маршрутизация(1)] = 2. [ответ(1)] →

[5]Стрелка в скобках указывает отправителя слева и получателя справа, вне скобок стрелка указывает на изменение структуры пакета, сами же скобки предполагают существование одинакового пакета, операция *ИЛИ* указывает вариативность и параллельность отправления.

	[# *A* - инициатор]	| 1 бит |
	[# *B или C* - получатель]	
3.	(*B → C ИЛИ C → B*)	1. [маршрутизация(~1)]
	[# *B или C* - маршрутизатор]	
	ИЛИ	=
	(*B → A ИЛИ B → C*)	2, 3. [запрос(2)] →
	[# *B* - инициатор]	| 1 бит |
	[# *A или C* - получатель или маршрутизатор]	
4.	(*B → A ИЛИ C → A*)	1. [ответ(1)]
	[# *A* - инициатор]	
	[# *B или C* - получатель]	
	ИЛИ	=
	(*A → B ИЛИ C → B*)	2. [ответ(2)]
	[# *B* - инициатор]	
	[# *A или C* - получатель]	
	ИЛИ	=
	(*A → C ИЛИ C → A*)	3. [маршрутизация(2)] →
	[# *A или C* - маршрутизатор]	| 2 бита |
5.	…	…

Таким образом, задача седьмой стадии анонимности формируется сложностью нахождения истинных субъектов информации при трёх и более пользователях не связанных между собой общими целями и интересами. Это возможно при использовании слепой маршрутизации в совокупности с вероятностным полиморфизмом пакета, где слепая маршрутизация обеспечивает диффузию пакета, распространяет его и делает каждого узла в сети потенциальным получателем, а вероятностный полиморфизм обеспечивает конфузию пакета, приводит к размытию роли субъектов информации, стирает грань между отправлением и получением. На основе вышеприведённых критериев уже образуется виртуальная маршрутизация, которая скрывает и разрывает связь объекта с его субъектами, приводит к зарождению седьмой стадии анонимности.

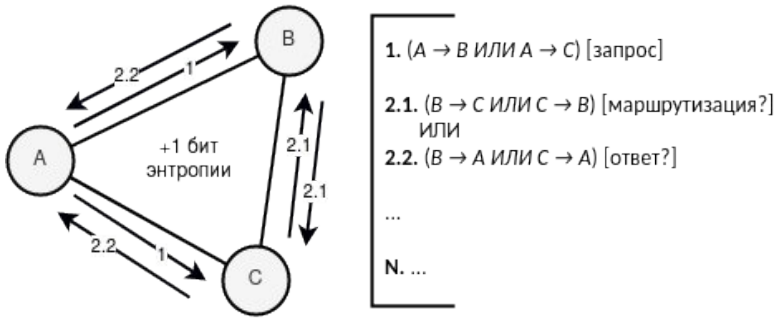

Рис. 5. Зарождение неопределённости при вероятностном полиморфизме

При этом, стоит заметить, что в самой седьмой стадии анонимности, на уровне ядра, заложен механизм постоянного умножения, приумножения энтропии, вследствие чего зарождаются и усваиваются одни лишь ложные логические суждения. Если таковые суждения априори представляют ложные выводы на любые выражения, то это эквивалентно полному доминированию энтропии над системой, в которой становится невозможным выявление закономерностей посредством декомпозиции её составляющих (данный момент будет

проанализирован более подробно при рассмотрении «подводных камней» седьмой стадии анонимности).

6. «Подводные камни» седьмой стадии анонимности

Анализируя сеть, базирующуюся на седьмой стадии анонимности, можно выявить, что маршрутизация и ответ в ней, являются этапами полностью автоматизированными, в то время как запрос является этапом ручным. Такой момент приводит к явлению, что между ответом и последующим запросом интервал времени ожидания больше, нежели между запросом - ответом, запросом - маршрутизацией, маршрутизацией - маршрутизацией и маршрутизацией - ответом. Это приводит к возможности осуществления атаки методом учёта времени с последующим расщеплением хаотичности, тем самым приводя к однозначности маршрутизации и к возможному выявлению субъектов информации. Предотвратить подобную уязвимость можно двумя противоположными, дифференциальными, амбивалентными способами:

1. Симуляция времени запроса. Иными словами, маршрутизация и ответ будут подстраиваться под примерное время генерации пакета в сети, способом установления задержки. Чем больше узлов в сети, тем меньше время задержки. Подобный метод следует использовать только в системах с большим количеством узлов, т.к. с малым количеством время ожидания маршрутизации или ответа будет достаточно долгим.

2. Симуляция времени маршрутизации и ответа. Иными словами, запрос будет подразумевать не только передачу истинной информации, но и передачу ложной, незначимой, пустой информации, в моменты отсутствия настоящего запроса. Подобный метод следует использовать только в системах с малым количеством узлов, т.к. производится огромное количество спама.

Продолжая анализ, можно заметить некоторые закономерности, приводящие к более точному обнаружению состояния пакета, а именно, является ли он запросом или ответом с вероятностью $\frac{2}{3}$, что эквивалентно более точному определению состояния субъекта информации.

Исходя из периода *T*, который вычисляется по формуле *НОК(2+k, 2)*, где *НОК* — наименьшее общее кратное, несложно узнать, что период при $k = 2$ будет равен 4. Это в свою очередь говорит о том, что каждое четвёртое действие, начиная с предыдущего запроса, будет с вероятностью $\frac{2}{3}$ также являться запросом (аналогична ситуация с ответом). Проблема не приводит к выявлению сеанса связи или сессии (потому как данная величина является алеаторной и неопределённой), но при этом делает более транспарентным сам факт существующего отправления/получения. В момент повышения энтропии, когда создаётся коллизия состояний, одновременно зарождается и период, как побочный эффект, противопоставляющий себя непредсказуемости, индетерминированности и дифферентности.

Проблема периода представляет собой лишь более вероятностный способ определения состояния, для решения которой будет достаточным повышение периода двумя возможными способами:

1. Повысить *k*. Тогда период $T = \begin{cases} 2 + k, k \bmod 2 = 0 \\ 2(2 + k), k \bmod 2 \neq 0 \end{cases}$ (не стоит забывать о свойстве гипертелии, если выбор падает на нечётное число).

2. Сделать *k* случайной переменной диапазона *[1;n]*, где *n* — максимальное количество маршрутизаций. Тогда период $T = HOK(2, 1+2, 2+2, ..., n+2)$.

Теперь, если анализировать непосредственно сами пакеты, в моменты их перемещения по сети, то можно наблюдать точно заданную тенденцию при которой их размер стремится к уменьшению. Это связано с тем фактом, что сам пакет имеет свойство полиморфизма, которое инициализируется на отправляющей стороне и постепенно финализируется на пути к принимающей. Такая закономерность способна выявлять роль субъектов информации, при которой достаточно проанализировать лишь размер пакета с позиции двух отправлений $(A \to B) \to (B \to C)$ и если пакет, в таком случае, уменьшается на заведомо известную величину D[6], то это свидетельствует о крайне высокой вероятности, что сам узел B является только промежуточным получателем.

Чтобы решить данную проблему, необходимо рассматривать структуру пакета 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 полиморфного пакета $S(P) + S(E) = S(E(P))$. При этом, т.к. $S(E)$ предполагает собой все слои шифрования, то данный размер можно представить в виде суммы каждого отдельного шифрования, где $S(E) = S(E_1) + S(E_2) + ... + S(E_n) \to S(E_n(...(E_2(E_1(P)))...)) = S(E(P))$. 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 полиморфного пакета 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 $(A \to B) \to (B \to C)$ и при этом, первый пакет оказывается меньше последующего, то данный факт говорит только о том, что второй пакет является самостоятельно сгенерированным и считается либо запросом, либо ответом, а узел B либо отправителем, либо получателем. Одним из решений данной проблемы может являться создание отдельного поля в

---

[6]Детерминированная разница размеров пакета между шифрованной и открытой версией, имеющая единственный слой шифрования. Шифрованный пакет 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 пакета по динамике постоянного стремления к уменьшению, исходя из его константной дифференции.

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

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

пакете, указывающего на следующего получателя (будь то истинного или промежуточного) с той лишь целью, чтобы маршрутизатор мог дополнять пакет на некую величину размера M[7], приводящую к константному размеру K[8]. Данный способ удаляет вышеописанные проблемы полностью, но выдаёт промежуточным узлам дополнительную информацию о последующих получателях пакета, одним из которых станет истинный получатель. Критичный характер данной проблемы приведёт к негэнтропии, автоматической деградации седьмой стадии, 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.

Другим решением данной проблемы является постоянное перенаправление пакета на псевдо-адрес отправителя, который вследствие всех процессов будет постоянно уменьшать размер пакета, добавляя при этом величину M, тем самым, приводя пакет к константной величине K. Так как адрес отправителя является симулятивным, то он никак не выдаст адрес настоящий. Теперь предположим, что существует три узла $\{A, B, C\}$, где A является отправителем, а B или C — получателем, то вся концепция полиморфных действий приводится в следующем акте: $(A \to B$ *ИЛИ* $A \to C) \to (B \to A$ *ИЛИ* $C \to A) \to (A \to B$ *ИЛИ* $A \to C) \to (B \to A$ *ИЛИ* $C \to A)$ вместо $(A \to B$ *ИЛИ* $A \to C) \to (B \to C$ *ИЛИ* $C \to B) \to (B \to C$ *ИЛИ* $C \to B) \to (B \to A$ *ИЛИ* $C \to A)$. Проблемой такого подхода является отсутствие увеличения энтропии, т.к. само полиморфное состояние равновероятно и эквивалентно разбивается на два неполиморфных положения, которые в свою очередь полностью и однозначно выявляют истинного отправителя информации вне зависимости от количества этапов полиморфизма и вне зависимости от псевдо-адреса отправителя.

Ещё одним и более корректным способом решения проблемы является использование случайной величины R[9], вместо константной величины K. В то время как сама уязвимость и проблема образуется и воссоздаётся из детерминированности, 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 пакетов, к диффузии

---

[7]Переменная величина M применяется для замещения удалённых слоёв шифрования, сохраняя размер любой стадии полиморфного пакета на уровне константной величины K.

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

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

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

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

где j - стадия полиморфного пакета,
n - количество слоёв шифрования.

[9]Случайная величина R является противоположной концепцией константной величины K и представляет неопределённость отправления пакета со стороны маршрутизирующей стороны, где с вероятностью $\frac{1}{2}$ может быть создан и отправлен новый, «пустой» псевдо-пакет случайного и большего размера, скрывающий, посредством алеаторности, дальнейший анализ динамики истинного пакета.

детерминированных качеств и к неопределённому выявлению субъектов информации. Такой подход базируется на необходимости генерации вероятностного псевдо-пакета случайного и большего размера (чем истинный пакет) 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 $X \in \{$*пакет меньшего размера, пакет 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 новый пакет меньше предыдущего, то субъектом данного объекта является истинный отправитель, либо получатель.
Ложно, т.к. маршрутизатор может «раскрыть» пакет, тем самым уменьшив его размер.

2. Если новый пакет меньше предыдущего, то субъектом данного объекта является маршрутизатор.
Ложно, т.к. ответ может быть меньше запроса.

3. Если новый пакет больше предыдущего, то субъектом данного объекта является истинный отправитель, либо получатель.
Ложно, т.к. маршрутизатор может сгенерировать псевдо-пакет большего размера.

4. Если новый пакет больше предыдущего, 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 $\{V_1, V_2, ..., V_n\}$.

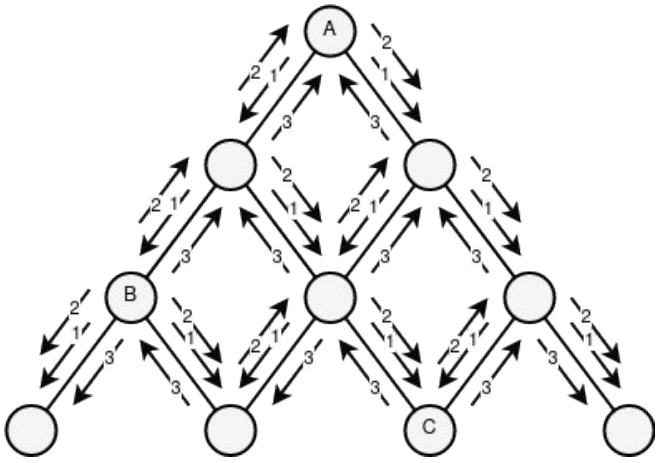

Рис. 6. Маршрутизация пакета на базе седьмой стадии анонимности из 10 узлов, где A - отправитель, B - маршрутизатор, C - получатель

Побочным эффектом такого решения, является возможность одновременного появления сразу двух пакетов от одного узла в сети, что будет говорить только о факте маршрутизации или получения. Но данная проблема перестаёт таковой являться, если истинный/псевдо пакет будет отправляться спустя случайное количество времени после псевдо/истинного пакета.

В результате, стоит учесть, что каждое решение проблемы либо увеличивает уровень спама (посредством симуляции времени маршрутизации и ответа, отправления псевдо-пакета), либо уменьшает производительность (посредством симуляции времени запроса, изменения переменной *k* для периода *T*) всей сети. Линейно увеличивающаяся нагрузка *O(N)*, зависимая от количества участников сети, представляет собой главную проблему седьмой стадии анонимности.

7. Анализ сетевых связей при седьмой стадии анонимности

При анализе седьмой стадии анонимности, при выявлении её «подводных камней» и способов их решения, во всех случаях в качестве базиса использовалась связь *«все-ко-всем»*, предполагающая, что исследуемые субъекты данной сети будут заведомо соединены друг с другом. Это в свою очередь приводит к игнорированию и абстрагированию иных возможных связей, способных существовать в реальности. Чтобы доказать безопасность оставшихся соединений, необходимо свести их ко связи *«все-ко-всем»*, тем самым, инкапсулировать множество свойств и неопределённостей в одно сингулярное, подвергаемое анализу состояние.

В общем случае существует всего три основных вида связи, в то время как все остальные соединения являются лишь побочными гибридами нижеприведённых моделей.

1. *«все-ко-всем»* ($A \leftrightarrow B, B \leftrightarrow C, C \leftrightarrow A$) [распределённая],
2. «*все-к-одному*» ($A \leftrightarrow D, B \leftrightarrow D, C \leftrightarrow D$) [централизованная],
3. *«один-к-одному»* ($A \leftrightarrow B, B \leftrightarrow C, C \leftrightarrow D$) [децентрализованная].

Во-первых, стоит сказать, что все приведённые выше связи являются одноранговыми, в том числе и связь централизованная. Данные соединения рассматриваются в вакууме седьмой стадии анонимности, а следовательно, все они априори предполагают одноранговую, peer-to-peer модель. Разделение связей рассматривает лишь расположение и сочетание субъектов относительно друг друга, а не дополнительную нагрузку, повышение прав или разделение полномочий.

Во-вторых, стоит заметить, что связи *«все-к-одному»* и «*один-к-одному*» схожи между собой куда больше, чем отдельно каждое из представленных со связью «*все-ко-всем*». Для полного представления распределённой связи достаточно трёх узлов, в то время как для двух оставшихся необходимо уже четыре узла. Связано это с тем, что если представить децентрализованную связь при помощи трёх субъектов, то результатом такого преобразования станет связь централизованная, и наоборот, что говорит об их родстве, сходстве и слиянии более близком, нежели со связью распределённой.

В-третьих, централизованная связь по своей концепции распространения информации стоит ближе к связи распределённой, нежели связь децентрализованная. Сложность распространения объекта между истинными субъектами информации в распределённых и централизованных системах равна *O(1)*, в то время как в децентрализованных сложность равна *O(N)*.

В-четвёртых, по критериям отказоустойчивости децентрализованная связь стоит ближе к распределённой, нежели связь централизованная. В связи *«все-ко-всем»*, при удалении одного субъекта, сеть остаётся целостной и единой. В связи «*один-к-одному*», при удалении одного

субъекта, сеть может разделиться на *N* децентрализованных сетей. В связи «*все-к-одному*», при удалении одного субъекта, сеть может прекратить своё существование вовсе.

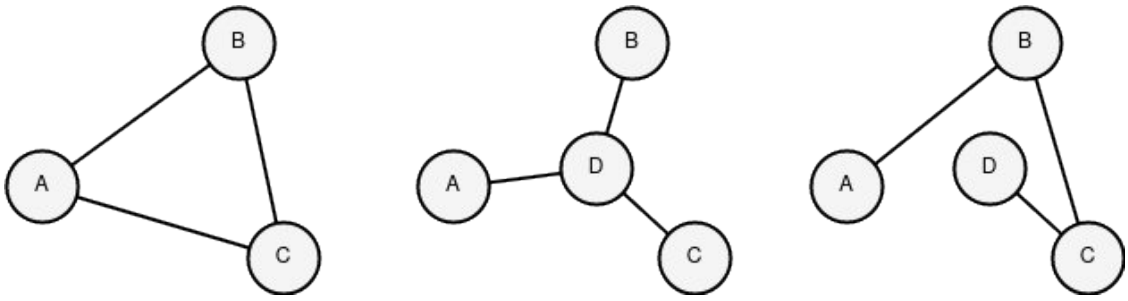

Рис. 7. Связи: «*все-ко-всем*», «*все-к-одному*», «*один-к-одному*» (слева направо)

Таким образом, схожесть и однородность связей можно представить как (децентрализованная ↔ централизованная) ↔ (централизованная ↔ распределённая) ↔ (распределённая ↔ децентрализованная). При цикличности трёх элементов, инициализируется общий эквивалент представленный в формации соединений *«все-ко-всем»*.

Далее, если предположить, что существует четыре субъекта {*A, B, C, D*} со связью *«все-к-одному»*, где центральным узлом является точка *D*, то анализ безопасности седьмой стадии анонимности будет сводиться к осмотру действий от узла *D* ко всем остальным субъектам и от любого другого узла к субъекту *D*. В одном случае будет происходить прямая широковещательная связь, в другом же случае, будет происходить передача сообщения для последующей множественной репликации.

Если предположить, что субъект *D* не способен генерировать информацию, а создан только для её ретранслирования, то это эквивалентно его отсутствию как таковому. Действительно, если пакет имманентен в своём проявлении (не выдаёт никакую информацию о субъектах), то все действия внутреннего узла *D* тождественны внешнему наблюдателю, а как было доказано ранее, седьмая стадия невосприимчива к такому виду деанонимизации. Следовательно, узел *D* становится словно фантомом, несущественным прозрачным субъектом, не влияющим на безопасность и анонимность сети, базируемой на связи *«все-к-одному»*. Из этого также следует, что седьмая стадия анонимности может применяться и в тайных каналах связи, где безопасность приложения выстраивается в заведомо подконтрольной, враждебной и централизованной инфраструктуре.

Теперь, если субъект *D* способен генерировать информацию, то создавая сеть и имплозируя её в себя, субъект сам становится сетью, в которой он априори соединён со всеми, что приводит это суждение ко связи «*один-ко-всем*». Связь же «*все-ко-всем*», состоит из множества связующих *«один-ко-всем»* для каждого отдельного субъекта, коим и является узел *D*, а это, в свою очередь приводит к классическому (ранее заданному) определению седьмой стадии анонимности. Таким образом, связь «*все-к-одному*» внутри себя уже содержит логическую составляющую связи *все-ко-всем* через которую и доказывается её безопасность.

Доказать безопасность связи «*один-к-одному*» возможно через неопределённость посредством её слияния со связью «*все-к-одному*», которое определяется при трёх участниках сети. Такое свойство неоднородности и неоднозначности предполагает, что сеть становится одновременно и централизованной, и децентрализованной. Следовательно, доказав ранее безопасность связи «*все-к-одному*», автоматически доказывается и безопасность связи *«один-к-одному»* для конкретно заданного случая.

Далее, если предположить, что существует четыре субъекта {*A, B, C, D*} со связью *«один-к-одному»*, то базируясь на итеративности передачи информации в децентрализованных системах,

можно декомпозировать любую модель в более замкнутую. Таким образом, сеть {*A, B, C, D*} фактически может расщепиться на две подсети {*A, B, C*} и {*B, C, D*}, мостом которой являются субъекты {*B, C*}. Каждая отдельная подсеть представляет собой ту же неопределённость, внутри которой присутствует централизованная система. В результате, безопасность связи *«один-к-одному»* сводится ко связи «*все-к-одному*», и как следствие, ко связи *«все-ко-всем»*.

Таким образом, вне зависимости от типа соединений, сеть на базе седьмой стадии анонимности будет оставаться безопасной, даже при условии существования единственного сингулярного сервера, связывающего всех клиентов между собой. Простота построения централизованной сети в седьмой стадии анонимности приводит противоречиво к выражению истинной отказоустойчивости, а также к живучести подобных систем, регенерирующих лишь от одной сетевой единицы. Данное свойство (в большей мере) отличает седьмую стадию анонимности от всех других скрытых сетей.

8. Проблематика анонимных сетей

При существовании и полной реализации, а также доступности скрытых сетей, будь то основанных на шестой или седьмой стадиях анонимности, 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 шестой стадии 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 доминирующее 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.

Не стоит также считать, что седьмая стадия анонимности, объединяя два разных способа маршрутизации из двух стадий, сама по себе будет решать данную проблему. Это является ошибочной гипотезой, т.к. данная стадия напрямую наследует задачи и методы их решения от шестого этапа.

Сутью проблемы является возможность создания сервисов внутри скрытых сетей не основанных на пятой стадии анонимности, что приводит к возникновению приложений, представляющих угрозу информационной безопасности. Это связано с тем фактом, что анонимные сети являются лишь способом маршрутизации к конечному субъекту, представляют собой некую платформу сервисов и позволяют размещать внутри себя приложения базируемые на клиент-серверной, многоранговой архитектуре, тем самым откатывая, регрессируя структуру защиты информации до второй стадии анонимности, делая её защиту централизованной, примитивной, а саму информацию транспарентной к серверному приложению.

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. Иначе говоря, нет разницы, где приложение будет воссоздано, т.к. первоначальная проблема доверия будет оставаться в неизменно исходной форме.

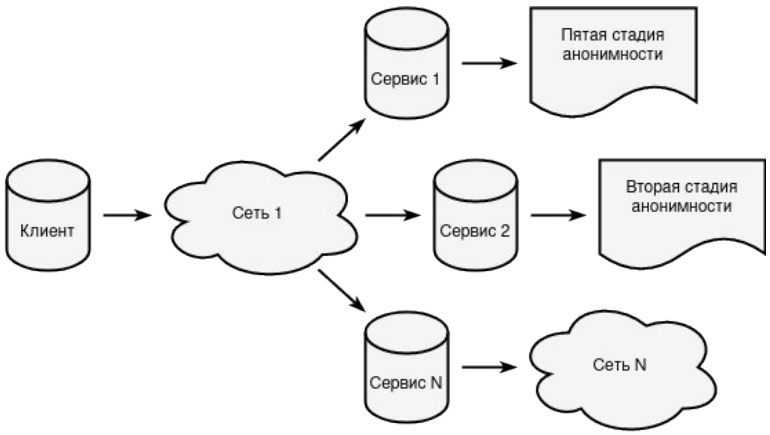

Рис. 8. Взаимодействие скрытых сетей со внутренними сервисами

Решить данный вопрос можно 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 агглютинации и интерференции, будет возможна синергия свойств анонимности и безопасности. Примером таких сочетаний могут служить связи Tor+Bitcoin, I2P+Filetopia и т.п., или монолитные технологии Monero [27], Dash [28] и т.д.

9. Тайные каналы связи

Секретные, тайные, эзотерические каналы связи — есть соединения, располагаемые в заведомо замкнутом, незащищённом, враждебном окружении и имеющие характеристики безопасной передачи информации [29, с.147]. При этом анонимность, родственная скрытым сетям, не является базисом секретных каналов связи и, следовательно, может быть отброшена из-за ненадобности или по необходимости. Так, например:

1. Первым, минимальным видом анонимности в тайных каналах связи принято считать пятую стадию, то есть 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 [30], поскольку субъект остаётся открытым, а объект остаётся закрытым (только вместо сокрытия информации, скрывается сам факт её существования). Поэтому данный способ вполне корректно относить точно равным образом и к пятой стадии анонимности. 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). И так как тайные каналы связи разворачиваются в заведомо замкнутой системе (многоранговой), то и мощность анонимности в таком случае равна единице.

2. Вторым, максимальным видом анонимности в тайных каналах связи принято считать седьмую стадию, при этом пропуская, игнорируя, импутируя шестую. Вся особенность такого подхода заключается в невозможности использовать фактическую, реальную маршрутизацию, которую предполагает шестая стадия анонимности. Тем самым

реальная маршрутизация отдаётся на откуп виртуальной, существование которой возможно лишь и только на седьмой стадии анонимности. Виртуальная маршрутизация имманентна, способна сводиться к передаче объекта внутри единого, сингулярного приложения, связывающего всех субъектов изнутри. Таким приложением является сервер (или группа серверов с $|A| = 1$), при помощи которого клиенты передают друг другу и принимают друг от друга информацию. Так как приложение располагает полным знанием того, кто является отправителем и кто является получателем, то сам сервер становится создателем сети на основе которой располагается тайный канал связи. При всём этом, такое приложение, в задаче о тайных каналах связи, аналогично и равносильно государству, в задаче о построении анонимных сетей. Всё это ведёт лишь к единственно возможной борьбе за анонимность с приложением-создателем — методом спама (способ с федеративностью недейственный в замкнутом и враждебном окружении одной линии связи).

Тайные каналы связи, использующие стеганографию, всегда имеют некий контейнер, в который помещается истинное сообщение [30, 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 не будет превышать 256KiB.

Тайные каналы связи, использующие криптографию, по умолчанию можно охарактеризовать пятой стадией анонимности. Если тайный канал разворачивается в заведомо замкнутой и незащищённой, но всё же сети, то это говорит о том, что стадия анонимности не меньше второй. Сами же секретные каналы данного вида используют идентификацию по криптографическим адресам, а не адресам, заданными системой по умолчанию (никнеймом, телефоном и т.д.), следовательно, стадия анонимности таких каналов определяется пятым этапом. Далее, если возникает виртуальная маршрутизация между субъектами, то пятая стадия начинает переходить в седьмую, минуя при этом шестую. Таким образом, секретные каналы способны улучшать безопасность уже выстроенной и существующей системы в неизменном для неё состоянии, используя лишь и только её базис в качестве фундамента.

Использование стеганографии, вместе с криптографией, может помочь в случаях, когда имеется вероятность или возможность нахождения скрытого сообщения в контейнере. 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 [29, 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 могут быть воссозданы совершенно в разных 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).

10. Монолитный криптографический протокол

Из всего вышесказанного можно создать простой, легковесный, но при этом и безопасный протокол передачи информации, являющийся самодостаточным, цельным и монолитным. Может быть применим к анонимным сетям и тайным каналам связи [11, с.58][29, с.80].

Участники протокола:

A - отправитель,

B - получатель.

Шаги участника A:

1. $K = G(N), R = G(N)$,

где G - функция-генератор случайных байт,
N - количество байт для генерации,
K - сеансовый ключ шифрования,
R - случайный набор байт.

2. $H_P = H(R \,||\, P \,||\, PubK_A \,||\, PubK_B)$,

где H_P - хеш сообщения,
H - функция хеширования,
P - исходное сообщение,
$PubK_X$ - публичный ключ.

3. $C_P = [E(PubK_B, K), E(K, PubK_A), E(K, R), E(K, P), H_P, E(K, S(PrivK_A, H_P)), W(C, H_P)]$,

где C_P - зашифрованное сообщение,
E - функция шифрования,
S - функция подписания,
W - функция подтверждения работы,
C - сложность работы,
$PrivK_X$ - приватный ключ.

Шаги участника B:

4. $W(C, H_P) = P_W(C, W(C, H_P))$,

где P_W - функция проверки работы.
Если ≠, то протокол прерывается.

5. $K = D(PrivK_B, E(PubK_B, K))$,

где D - функция расшифрования.
Если ≠, то протокол прерывается.

6. $PubK_A = D(K, E(K, PubK_A))$.

Если ≠, то протокол прерывается.

7. $H_P = V(PubK_A, D(K, E(K, S(PrivK_A, H_P))))$,

где V - функция проверки подписи.
Если ≠, то протокол прерывается.

8. $H_P = H(D(K, E(K, R)) \,||\, D(K, E(K, P)) \,||\, PubK_A \,||\, PubK_B)$,

Если ≠, то протокол прерывается.

Данный протокол игнорирует способ получения публичного ключа от точки назначения. Это необходимо по причине того, чтобы протокол был встраиваемым и мог внедряться во множество систем, включая одноранговые сети, не имеющие центров сертификации, и тайные каналы связи, имеющие уже установленную сеть по умолчанию.

Также протокол способен игнорировать сетевую идентификацию субъектов информации, замещая её идентификацией криптографической. При таком подходе аутентификация субъектов начинает становиться сингулярной функцией, относящейся лишь и только к асимметричной криптографии, и как следствие, прикладной уровень стека TCP/IP начинает симулятивно заменять сетевой по способу обнаружения отправителя и получателя. Из вышеописанного также справедливо следует, что для построения полноценной информационной системы необходимым является симулятивная замена транспортного и прикладного уровня последующими криптографическими абстракциями. Под транспортным уровнем может пониматься способ передачи сообщений, под прикладным — взаимодействие со внутренними сервисами анонимной сети.

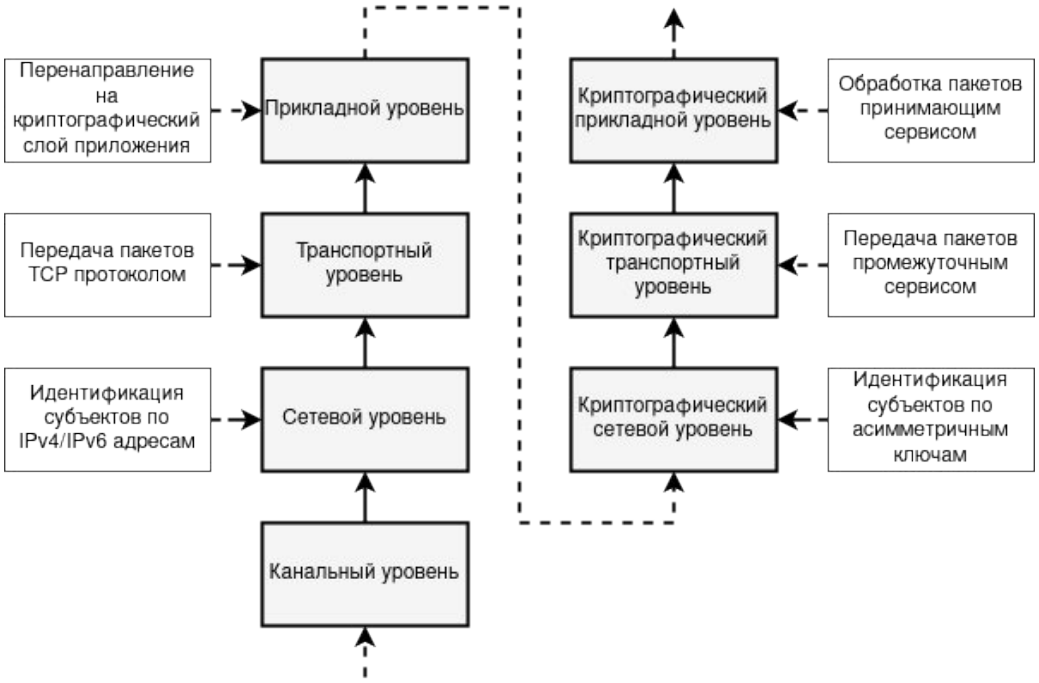

Рис. 9. Расширение стека протоколов TCP/IP на базе криптографических абстракций

Сеанс связи в приведённом протоколе определяется номером пакета, или иными словами один пакет становится равен одному сеансу за счёт генерации случайного сеансового ключа. Описанный подход приводит к ненадобности сохранения фактического сеанса связи, исключает внешние долговременные связи между субъектами посредством имманентности и абстрагирования объектов, что приводит к невозможности рассекречивания всей информации, даже при компрометации одного или нескольких сеансовых ключей.

Безопасность протокола определяется в большей мере безопасностью асимметричной функции шифрования, т.к. все действия сводятся к расшифрованию сеансового ключа приватным ключом. Если приватный ключ не может расшифровать сеансовый, то это говорит о том факте, что само сообщение было зашифровано другим публичным ключом и потому получатель также есть другой субъект. Функция хеширования необходима для проверки целостности отправленных данных. Функция проверки подписи необходима для аутентификации отправителя. Функция проверки доказательства работы необходима для предотвращения спама.

Шифрование подписи сеансовым ключом является необходимым, т.к. взломщик протокола, для определения отправителя (а именно его публичного ключа) может составить список уже известных ему публичных ключей и проверять каждый на правильность подписи. Если проверка приводит к безошибочному результату, то это говорит об обнаружении отправителя.

Шифрование случайного числа (соли) также есть необходимость, потому как, если злоумышленник знает его и субъектов передаваемой информации, то он способен пройтись методом «грубой силы» по словарю часто встречаемых и распространённых текстов для выявления исходного сообщения.

Пример программного кода для шифрования информации:

```
import (
	"bytes"
	"encoding/hex"
)
func Encrypt(sender *PrivateKey, receiver *PublicKey, data []byte) *Package {
	var (
		pubsend		= PublicKeyToBytes(&sender.PublicKey)
		session		= GenerateBytes(N)
		randBytes	= GenerateBytes(N)
	)

	hash := HashSum(bytes.Join(
		[][]byte{
			randBytes,
			data,
			pubsend,
			PublicKeyToBytes(receiver),
		},
		[]byte{},
	))

	return &Package{
		Head: HeadPackage{
			Sender:		EncryptS(session, pubsend),
			Session:	EncryptA(receiver, session),
			RandBytes:	EncryptS(session, randBytes),
		},
		Body: BodyPackage{
			Data:	EncryptS(session, data),
			Hash:	hash,
			Sign:	EncryptS(session, Sign(sender, hash)),
			Proof:	ProofOfWork(hash, C),
		},
	}
}
```

Протокол пригоден для многих задач, включая передачу сообщений, запросов, файлов, но не пригоден для передачи поточной информации, подобия аудио звонков и видео трансляций, из-за необходимости подписывать и подтверждать работу, на что уходит много времени. Иными словами, протокол работает с конечным количеством данных, размер которых заведомо известен и обработка которых (то есть, их использование) начинается с момента завершения полной проверки.

Для улучшения эффективности, допустим при передаче файла, программный код можно изменить так, чтобы снизить количество проверок работы в процессе передачи, но с первоначальным доказательством работы на основе случайной строки (полученной от точки назначения), а потом и с накопленным хеш-значением из n-блоков файла, для i-ой проверки. Таким

образом, минимальный контроль работы будет осуществляться лишь $\lceil M/nN \rceil+1$ раз, где M — размер файла, N — размер одного блока. Если доказательство не поступило или оно является неверным, то нужно считать, что файл был передан с ошибкой и тем самым запросить повреждённый или непроверенный блок заново.

Пример программного кода для расшифрования информации:

```
import (
	"bytes"
	"encoding/hex"
)
func Decrypt(receiver *PrivateKey, pack *Package) (*PublicKey, []byte) {
	// Check hash size.
	If len(pack.Body.Hash) != HashSize {
		return nil, nil
	}

	// Check proof of work.
	if !ProofIsValid(pack.Body.Hash, C, pack.Body.Proof) {
		return nil, nil
	}

	// Decrypt session key.
	session := DecryptA(receiver, pack.Head.Session)
	if session == nil {
		return nil, nil
	}

	// Decrypt public key.
	bpubsend := DecryptS(session, pack.Head.Sender)
	if bpubsend == nil {
		return nil, nil
	}
	pubsend := BytesToPublicKey(bpubsend)
	if pubsend == nil {
		return nil, nil
	}
	pubsize := PublicKeySize(pubsend)
	if pubsize  != KeySize {
		return nil, nil
	}

	// Decrypt rand bytes.
	randBytes := DecryptS(session, pack.Head.RandBytes)
	if randBytes == nil {
		return nil, nil
	}

	// Decrypt data.
	data := DecryptS(session, pack.Body.Data)
	if data == nil {
		return nil, nil
	}

	// Check hash.
	check := HashSum(bytes.Join(
		[][]byte{
			randBytes,
			data,
			PublicKeyToBytes(pubsend),
			PublicKeyToBytes(&receiver.PublicKey),
		},
```

```
                []byte{},
        ))
        if !bytes.Equal(pack.Body.Hash, check) {
                return nil, nil
        }

        // Decrypt signature.
        sign := DecryptS(session, pack.Body.Sign)
        if sign == nil {
                return nil, nil
        }

        // Check signature.
        if !Verify(pubsend, pack.Body.Hash, sign) {
                return nil, nil
        }

        return pubsend, data
}
```

Представленный программный код на языке Go представлен только как шаблон, показывающий способ шифрования и расшифрования непосредственно. Проблемой здесь является простота и примитивность анализа сетевого трафика по JSON-формату, что может привести к последующим блокировкам всех сетевых построений на основе данного кода. Необходимым решением должно служить вынесение сеансового ключа за пакет JSON-формата, последующее шифрование им пакета и конкатенация зашифрованного пакета с шифрованным сеансовым ключом. Если размер асимметричного ключа заведомо известен, то будет известен и размер зашифрованного сеансового ключа, что не приведёт к каким-либо проблемам расшифрования информации. Другая проблема заключается в отсутствии каких бы то ни было видимых метаданных (хеш-значения, доказательства работы), которые бы помогли в борьбе со спамом, что в свою очередь является крайне важным критерием для большинства децентрализованных систем. Таким образом, отсутствие метаданных равносильно отсутствию отказоустойчивости, что отсылает на противоречие эквивалентности полностью анализируемого и неподверженного анализу пакетам. В связи с этим, вопрос об отказоустойчивости скрытых сервисов в замкнутой системе посредством блокировок остаётся открытым.

11. Заключение

В данной работе были проанализированы скрытые системы, представляющие безопасность и безымянность пользователей — анонимные сети и тайные каналы связи. Была приведена градация анонимности в компьютерных сетях, базируемая на её мощности. На основе же градации было выявлено само развитие анонимности и необходимые условия для её существования. Основным, и пожалуй главным, моментом данной статьи является определение теоретической, абсолютной анонимности, базируемой на седьмой стадии. Было найдено противоречие, при котором стремление к уменьшению мощности доверия становится второстепенным свойством, как только достигалась шестая стадия анонимности. Решением проблемы является объединение пятой стадии анонимности со стадиями высшего порядка. Из определения абсолютного анонимата была также выявлена возможность создания тайных каналов связи на базе седьмой стадии анонимности, за счёт осуществимости применения виртуальной маршрутизации в замкнутых системах. В части о тайных каналах связи было расширено определение пятой стадии анонимности, за счёт внесения стеганографических методов как возможной альтернативы криптографическим. Был представлен протокол безопасной передачи информации, вместе с

примерами программного кода, на основе которого могут базироваться в последующем анонимные сети и тайные каналы связи.

Список литературы

1. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. - 960 с.
2. 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).
3. Бодрийяр, Ж. Символический обмен и смерть / Ж. Бодрийяр. — М.: «Добросвет» 2000. - 387 с.
4. 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).
5. 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).
6. Симаков, А. Анонимность в глобальных сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/anonimnost-v-globalnyh-setyah (дата обращения: 04.01.2022).
7. 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-sovershenia-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 04.01.2022).
8. 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).
9. 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).
10. 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).
11. Шнайер, Б., Фергюсон, Н. Практическая криптография / Б. Шнайер, Н. Фергюсон. - М.: Издательский дом «Вильямс, 2005. - 420 с.
12. 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).
13. NETSUKUKU RFC документация [Электронный ресурс]. — Режим доступа: http://netsukuku.freaknet.org/sourcedocs/main_doc/ntk_rfc/ (дата обращения: 31.12.2021).
14. 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).

15. Рябко, Е. Калейдоскоп vpn технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kaleydoskop-vpn-tehnologiy (дата обращения: 02.01.2022).
16. 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).
17. 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).
18. 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).
19. 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).
20. 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).
21. Рябко, Б., Фионов, А. Криптография в информационном мире / Б. Рябко, А. Фионов. - М.: Горячая линия - Телеком, 2019. - 300 с.
22. Douceur, J. The Sybil Attack [Электронный ресурс]. — Режим доступа: https://www.microsoft.com/en-us/research/wp-content/uploads/2002/01/IPTPS2002.pdf (дата обращения: 29.12.2021).
23. Popescu, B., Crispo, B., Tanenbaum, A. Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System [Электронный ресурс]. — Режим доступа: http://turtle-p2p.sourceforge.net/turtleinitial.pdf (дата обращения: 29.12.2021).
24. Донован, А., Керниган, Б. Язык программирования Go / А.А. Донован, Б.У. Керниган. — М.: ООО «И.Д. Вильямс», 2018. - 432 с.
25. Программная реализация протокола go-peer [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer (дата обращения: 20.03.2022).
26. Шеннон, К. Теория связи в секретных системах [Электронный ресурс]. — Режим доступа: https://web.archive.org/web/20141222030352/http://pv.bstu.ru/crypto/shannon.pdf (дата обращения: 02.01.2022).
27. 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).
28. 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).
29. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные коды на языке С / Б. Шнайер. — СпБ.: ООО «Альфа-книга», 2018. - 1040 с.
30. Шелухин, О., Канаев, С. Стеганография. Алгоритмы и программная реализация / О. Шелухин, С. Канаев. — М.: Горячая линия - Телеком, 2018. - 592 с.