Геннадий Александрович
Коваленко

Общая теория анонимных коммуникаций

Второе издание

Геннадий Александрович Коваленко

Общая теория анонимных коммуникаций

Второе издание

Издательские решения
По лицензии Ridero
2023

УДК 60
ББК 3
К56

Шрифты предоставлены компанией «ПараТайп»

Коваленко Геннадий Александрович

К56 Общая теория анонимных коммуникаций : Второе издание / Геннадий Александрович Коваленко. — [б. м.] : Издательские решения, 2023. — 208 с.
ISBN 978-5-0060-5715-9

Существующие определения анонимности и безопасности конечных пользователей в сетевых коммуникациях часто являются расплывчатыми, неясными и противоречащими друг другу. Такая реальность восприятия стала следствием недостающей теоретической основы, которая могла бы структурировать основные подходы к построению или использованию скрытых систем. Понимание термина «анонимность» посредством декомпозиции его составляющих способно дать оценку дальнейшего вектора развития анонимных / безопасных систем.

УДК 60
ББК 3

12+ В соответствии с ФЗ от 29.12.2010 №436-ФЗ

ISBN 978-5-0060-5715-9

ПРЕДИСЛОВИЕ

Книга, которую сейчас вы держите в руках, состоит из научно-теоретических, а также научно-исследовательских работ, основным направлением которых является анализ анонимных коммуникаций в сетевом пространстве. Книга состоит из четырёх глав:

1. «Теория строения скрытых систем»,
2. «Монолитный криптографический протокол»,
3. «Абстрактные анонимные сети»,
4. «Децентрализованный протокол обмена ключами».

Каждая глава разбирает определенную сторону вопроса анонимных коммуникаций. Так в первой главе даются общие понятия об анонимности, такие как — определение, развитие и моделирование. Во второй главе даются более конкретные аспекты проектирования анонимных и безопасных систем, в основе которых закладывается разработка криптографического протокола. В третьей главе даётся определение узкого класса анонимных сетей с возможностью своего функционирования в замкнутых пространствах централизованных систем. В четвертой главе на рассмотрение даётся проблема обмена ключами в децентрализованных системах, а также её возможные сопутствующие решения.

Книга может быть полезна программистам, собравшимся проектировать и разрабатывать собственные анонимные / безопасные системы, криптографам, предлагая ко вниманию новые направления в анонимных коммуникациях (абстрактные анонимные сети, криптографические протоколы), преподавателям и студентам предметов КСЗИ (криптографические средства защиты информации), СиСПИ (сети и системы передачи информа-

ции), КС (компьютерные сети), за счёт структурированного материала по терминологии «анонимность».

На базе приведённой теории была разработана теоретически доказуемая анонимная сеть «Hidden Lake», исходные коды которой находятся в открытом доступе по ссылке: https://github.com/number571/go-peer/tree/master/cmd/hidden_lake.
Дополнительный материал, программные коды, а также дальнейшее развитие теории вы можете найти на страницах GitHub профиля: https://github.com/number571, и в частности на страницах проекта «go-peer»: https://github.com/number571/go-peer.

Теория строения скрытых систем

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

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

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

1. ВВЕДЕНИЕ

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

Если брать во внимание криптографию как основной и базовый ориентир методов и средств защиты информации, то можно с уверенностью говорить об абсолютном опережении защищающей стороны над атакующей. Во второй половине XX века криптография вышла из составляющей искусства (своей классической формы) и переродилась в полноценную науку

(современную криптографию) благодаря работам Клода Шеннона, стандартизации шифра DES, открытию асимметричной криптографии, хеш-функциям и цифровым подписям. Все данные явления положительно сказались на разработке и переустройстве схем безопасности, когда в аналогичном всплеске начали зарождаться криптографические протоколы, пригодные для обширного множества частных и общих задач. Постепенно и поэтапно появлялись алгоритмы, такие как RSA, Elgamal, Serpent, AES, SHA256, Keccak, и протоколы, такие как Diffie-Hellman, Messi-Omura, Kerberos, TLS и т. д., эффективных способов взлома которых в настоящее время так и не было найдено, даже спустя десятилетия их открытого криптоанализа с присущими вознаграждениями.

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

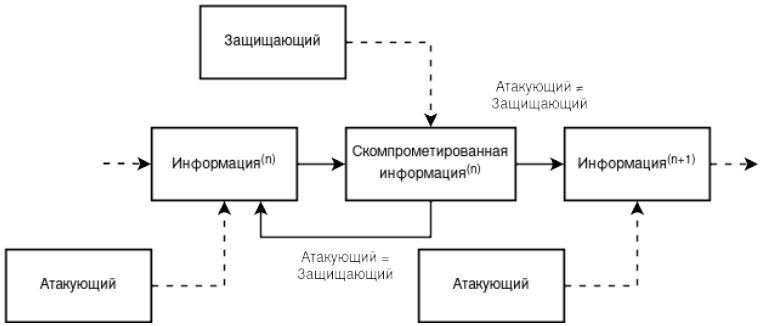

Рисунок 1. Развитие средств защиты информации (n) посредством действий атакующих и защищающих сторон. Слияние атакующих и защищающих способно порождать стагнацию в развитии средств защиты информации

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

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

Изложение данной работы направлено на анализ становления таковых систем и на отличительные их особенности со стороны безопасности объекта (информации) и субъекта (пользователя, клиента системы). Из первичного анализа становится возможным выявление вектора развития последующих, более качественных сетевых коммуникаций. Большинство нижеизложенного материала проходит сквозь призму диалектической триады «тезис — антитезис — синтез». Таковой подход позволяет выявлять не только лишь основные векторы развития будущих систем, но и их последующие качества, характеристики как сочетания *N*-го количества бывших парадигм. Помимо про-

чего, такой подход позволяет более детально рассматривать и ныне существующие системы, выявлять их недостатки, противоречия, способные играть роль в последующих деконструкциях и фазах отрицания. Поэтому само введение становится истоком и началом зарождения проблемы.

1.1. СЕТЕВЫЕ КОММУНИКАЦИИ

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

Децентрализация как первичная форма Интернет-коммуникаций в целом появляется на фоне академических исследований [4, с. 70], повлекших за собой глобальное развитие информационных технологий. Первичная система представляла собой не только внешний прогресс относительно себя, но и имманентную эволюцию, выявляя в своей реализации отрицательные стороны и внутренние противоречия. Фактором дальнейшего развития и одновременно гибели стала проблема масштабируемости связей типа «клиент-клиент». Сложность в построении широковещательных и широкомасштабных соединений постепенно влекла за собой потребность в промежуточных узлах, основаниях концентрации линий связи типа «клиент-сервер», тем самым зарождая ядро централизации как основную точку отчёта всей дальнейшей проблематики.

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

Централизация как вторая форма развития Интернет-коммуникаций появляется на фоне разложения и отмирания первичной децентрализованной оболочки [5]. Представляя свои плюсы масштабируемости, централизация начинает претерпевать внутренние этапы развития как итерации наложения слоёв абстракций и отрицания децентрализации, противоречиво становясь для последней фазой её собственной эволюции. При каждой новой итерации своего прогресса централизованная система всё сильнее масштабируется, всё более углубляется корнями, всё чаще репрезентирует себя, образовывая тем самым симулякры [6, с. 151] второго порядка. Одновременно с этим система постоянно и планомерно нейтрализует внешние атаки, ранее являвшимися губительными для её ядра, но ныне безвредными для её функционирования, подобно атакам в обслуживании [4, с. 869] (DDoS) или эксплуатации уязвимостей с учётом изъятия внутренней информации сторонними лицами. С течением времени, продолжая развиваться и масштабироваться, система постепенно начинает порождать общество всё более абстрагируемое от понимания её первичного механизма, всё более догматичное и фрагментированное. Инициатор системы становится её созерцателем, система становится воспроизводством созерцателей. В итоге централизованная структура запускает инициализацию

своих внутренних интересов, инвертированно направленных на пользователей, тем самым кардинально изменяя способ взаимодействия с ними. При выстроенном императиве система начинает образовывать множество симулякров третьего порядка, ориентируемых на незначимость или скрытность истинного уровня безопасности, подменяя реальность иллюзорностью происходящего в своём внутреннем слое за полями «сконфигурированных» абстракций. Итогом таковых ложных представлений становится «театр безопасности» [7], направленный на поддержание имеющегося порядка вещей (системы), с целью сокрытия реального уровня соблюдаемой конфиденциальности.

Внешние угрозы информационной безопасности хоть и становятся полностью безвредными для централизованных систем в ходе их постоянной, постепенной и планомерной эволюции, но такое утверждение ничего не может говорить об отсутствии внутренних угроз. Само масштабирование начинает порождать внутренние угрозы, быть противоречием системы, её развитием и конечным отмиранием. Всё большее расширение, продолжительная концентрация связей, неостановимая монополия соединений вызывают аккумулятивную реакцию внутренних интересов её же участников. Внутреннему сотруднику компании теперь становится выгодно продавать информацию об её пользователях при всё большем расширении системы; государству становится выгодно концентрировать линии связи в одном сингулярном пространстве, открывая более удобный спектр возможностей контроля за обществом и его деятельностью; рекламодателю становится выгодно вкладывать свои средства в массовую систему с наиболее релевантным алгоритмом выдачи рекламы на базе конфиденциальной информации клиентов, повышая тем самым свою прибыль [8], [9]. В результате вышеприведённые проблемы информационной безопасности становятся неразрешимыми централизованными системами, потому как последние продолжают руководствоваться исключительно механизмом неостановимого стремления к собственной масштабируемости и постоянной репрезентации, за счёт чего самолично, неосознанно и планомерно

продолжают возобновлять эти же самые проблемы. Таким образом, жизнь централизованных систем начинает постепенно и прямо пропорционально зависеть от количества и качества выстроенных слоёв абстракций, от форм без содержания, от копий без собственных оригиналов, направленных на единственного созерцателя и зрителя данного спектакля — клиента системы, лишь с той единственной целью, чтобы доказать своим «совершенным» существованием финальность и фатальность централизации.

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

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

1.2. ВЛИЯНИЕ ЦЕНТРАЛИЗАЦИИ

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

В отличие от других систем, в централизованных открыто прослеживаются два вида дифференцированных интересов, где с одной стороны находятся обладатели сервисов связи, с другой — пользователи этой системы. Первым становится выгодна такая парадигма вещей, потому как они овладевают всей ин-

формацией, проходимой через них и хранимой у них. Это выгодно не только со стороны экономического влияния (реклама, продажа конфиденциальной информации, явные и неявные подкупы и т. д.), но и со стороны политического контроля (пропаганда государственной или маркетинговой позиции, блокирование оппозиционных или «неправильных» мнений, явные и неявные шантажи, лоббирование интересов и т. д.). Само влияние, как тень, накладывается на субъектов подобных сервисов, поэтапно переводя их в категорию типичных объектов исследования рынка. Вторым становится выгодна парадигма использования сервиса без какой-либо нагрузки на своей стороне, с условиями хорошего соединения, большого хранилища и качественного дизайна UX/UI (user experience / user interface). Внешнее представление таковых действий становится с одной стороны неким описанием симбиоза, когда сервисы создают всю инфраструктуру для клиентов с целью своего будущего экономического и/или политического влияния, в то время как пользователи начинают использовать данную систему для комфортной взаимосвязи с другими её участниками. С другой стороны эти же действия становятся последующей формой паразитизма сервисов над её участниками, потому как вектор развития сервисов при достижении *N*-го количества клиентов, при достижении некой критической массы, перевоплощается, инвертируется и становится в конечном итоге платформой связи, живущей не для клиентов, а за счёт них. Теряя из виду причинно-следственную связь жизнеспособности централизованного механизма, пользователи перестают осознавать, насколько масштабной начинает быть развивающаяся система сбора личной и конфиденциальной информации. Если таковые субъекты смогут не только осознать весь масштаб происходящего и не только найти альтернативу происходящему, но и успешно перевести все свои интересы на безопасные системы, представляющие близкие к ним стремления — интересы большинства, то централизованные механизмы постепенно и поэтапно начнут замещаться гибридными, децентрализованными альтер-

нативами, начнут отмирать и в конечном счёте станут формой остатка всего множества сетевых коммуникаций.

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

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

2. Комфортность использования сервисов начинает постепенно и неявно накладываться на текущий уровень безопасности, в некой степени отодвигая его на второй план, потому как конечные клиенты с большей долей вероятности начинают вы-

бирать более производительную систему, чем безопасную и медленную [13, с. 239]. Со стороны компаний и корпораций дизайн может диктоваться, видоизменяться, подвергаться моде, тем временем как безопасность остаётся всегда процессом без окончания, сложным, невидимым и, как следствие, менее значимым для обычных пользователей. Подобная дифферентная реакция клиентов на комфортность и безопасность становится в определённой степени выгодна производителю за счёт снижения затрат на реальную безопасность разрабатываемых или поддерживаемых систем.

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

4. Экономический базис существования централизованных систем не позволяет выйти из существующего императива ве-

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

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

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

Таким образом, развитие постцентрализованных сетевых коммуникаций становится делом далёкого будущего. Противоречий накапливается с каждым разом всё больше, что продолжает играть двоякую роль. С одной стороны, противоречия приводят систему к собственному отмиранию за счёт выявления явных недостатков, которые приходится постепенно решать и исправлять. С другой стороны, большое количество накопленных противоречий также становится и фактором сдерживания к отмиранию

системы за счёт необходимости в более длительном анализе её составляющих. В любом случае на гниющей, разлагающейся и репрезентируемой, самовосстанавливающейся почве уже виднеются малые ростки будущих сетевых коммуникаций, способных обеспечивать настоящий, а не фиктивный уровень безопасности конечных пользователей, защищающий их личную и конфиденциальную информацию. Всё дальнейшее изложение нашей статьи будет акцентировано на анализе подобных систем.

1.3. ОСНОВНАЯ ПРОБЛЕМАТИКА

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

Приведённая атака ссылается на нерешённую проблему доверия[1], разрушительную и губительную по своей сути, но при этом затмевающую более скрытую и деструктивную, мощь которой в современном мире превосходит прямолинейные MITM-

[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 сто-

атаки. Одной из задач нашей статьи является выявление данного метода нападения, его анализ и последующие решения.

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

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

ронних каналов связи, то есть прямого доверия, через которое уже может образовываться сеть доверия.

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

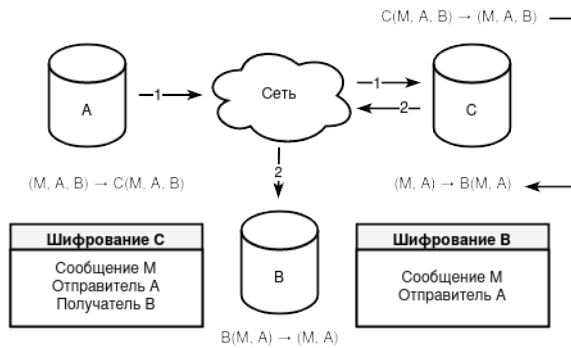

Рисунок 3. Коммуникация субъектов *A*,*B* посредством общего сервиса *C*

Таковое развитие инициализирует возникновение систем доверия, где не только сами доверительные узлы становятся

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

Тем не менее безоговорочно аннигилировать такую систему доверия не представляется возможным из-за реального ухудшения оптимизации и производительности программ, последующих трудностей построения архитектуры приложений и в конечном счёте из-за невозможности полного искоренения доверия как такового [23, с. 267]. Таким образом, необходимо не уничтожать, а заменять данную систему более безопасной, отодвигать её на второй план, в нишу, в которой только она способна быть полезной. Во всех других случаях необходимо строить и разрабатывать иные системы, механизм которых стремился бы к уменьшению мощности доверия[1], в которых собственная структура представляла бы защиту объектов и анонимат субъектов. К системам подобного рода уже частично относятся ано-

[1] Мощность доверия — количество узлов, участвующих в хранении или передаче информации, представленной дли них в открытом описании. Иными словами, такие узлы способны читать, подменять и видоизменять информацию, т. к. для них она находится в предельно чистом, прозрачном, транспарентном состоянии. Чем больше мощность доверия, тем выше предполагаемый шанс компрометации отдельных узлов, а, следовательно, и хранимой на них информации. Принято считать одним из узлов получателя. Таким образом, нулевая мощность доверия $|T| = 0$ будет возникать лишь в моменты отсутствия каких-ли-

нимные сети, клиент-безопасные приложения и тайные каналы связи, анализ и развитие которых представлено в последующих разделах и подразделах.

1.4. ЭКОНОМИЧЕСКИЕ ПРИЧИНЫ

На основе технической проблематики становится возможным выявление репродукции экономических причин [24]. В то время как техническое описание проблематики даёт лишь ответы на вопросы типа: «как централизованные сервисы могут получать конфиденциальную информацию клиентов?» или «как можно улучшить систему таким образом, чтобы сервисы не получали конфиденциальную информацию?», экономическое описание проблематики даёт более общие ответы на вопросы типа: «почему сервисам выгодно получать конфиденциальную информацию клиентов?» и «какова модель жизненного цикла конфиденциальной информации клиентов в кругу множества централизованных сервисов?».

В проблематике экономического толка необходимым становится выявление участников (сервисов) с точки зрения максимизации их прибыли от получаемой конфиденциальной информации. С такой стороны можно выявить несколько участников, потребляющих информацию, но при этом каждый из которых исполняет свою одностороннюю, узконаправленную роль.

1. «*Сервис-считыватель*». В общей основе — это есть сервис, получающий всю вводимую информацию и метаданные

бо связей и соединений. Если $|T| = 1$, это говорит о том, что связь защищена, иными словами, никто кроме отправителя и получателя информацией не владеют. Во всех других случаях $|T| > 1$, что говорит о групповой связи (то есть о существовании нескольких получателей), либо о промежуточных узлах, способных читать информацию в открытом виде.

клиентов. Его действия сводятся лишь к простому алгоритму: 1) принять сырую информацию и метаданные от клиентов своей системы; 2) обработать сырую информацию, переведя её в нормализованный вид; 3) положить обработанную информацию в хранилище.

2. «*Сервис-распределитель*». Является посредником между сервисами-считывателями и сервисами-потребителями. Считывает обработанную информацию из хранилищ сервисов-считывателей и перекладывает в своё хранилище. В итоге хранилище сервиса-распределителя становится суммой хранилищ сервисов-считывателей.

3. «*Сервис-потребитель*». В общей основе — это есть сервис, выдающий таргетированную рекламу своим клиентам на основе суммы обработанной информации, складируемой в хранилище сервиса-распределителя.

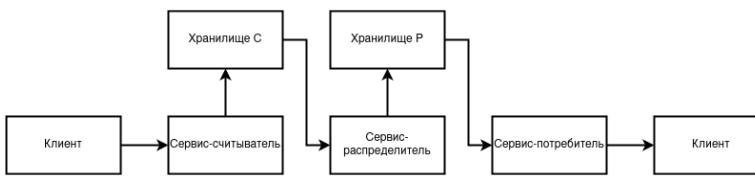

Рисунок 4. Общая модель связи между разными сервисами

На *Рисунке 4* изображена общая модель взаимодействия сервисов между собой. При этом стоит сказать, или вернее уточнить тот факт, что один и тот же централизованный сервис может быть как сервисом-считывателем, так и сервисом-потребителем, за счёт чего таковой сервис может полноценно существовать без сервиса-распределителя, основываясь исключительно и только на своей имманентно получаемой ин-

формации. Тем не менее получаемый результат становится всегда хуже первоначально ожидаемого, потому как таковой композитный сервис не может охватить всей области жизни своих клиентов, весь их спектр увлечений, начиная с чтения научной литературы, продолжая спецификой выполняемой работы и заканчивая просмотром порнографии в свободное время.

Рисунок 5. Частная модель самостоятельного сервиса без участия сервиса-распределителя

Также стоит сказать, что не все сервисы способны быть эффективными считывателями, ровно так же и не все сервисы способны быть эффективными потребителями. Связано это в первую очередь с тем обстоятельством, что имея один сервис — невозможно охватить все возможные области жизни, как производство контента (социальные сети, мессенджеры, форумы), так и его потребление (маркетплейсы). На основе этого и рождается более общая модель взаимодействия нескольких сервисов между собой. Так например.

1. Маркетплейсы не могут эффективно считывать конфиденциальную информацию клиента, как его предпочтения, хобби, список знакомых и родственников, предпочтения в еде, музыке, спорте и т. д., потому что они лишь предоставляют уже готовые

имеющиеся у них товары как некое ограниченное множество элементов, из которого клиент и выбирает всё ему необходимое. Это, конечно, свидетельствует об интересах клиента, но охватываемый сбор конфиденциальной информации начинает исходить лишь из его покупок и действий, направленных на определённые виды и категории товаров.

2. Мессенджеры, форумы, поисковые системы не могут эффективно потреблять конфиденциальную информацию клиента, потому как таковые не представляют собой конечную цепочку жизненного цикла конфиденциальной информации в лице продажи товаров, и, как следствие, становятся способными лишь продавать конфиденциальную информацию пользователей. На этом простом факте начинает строиться их основная выгода. Интересной особенностью сервисов-считывателей является также их возможность к прямой/косвенной кооперации с сервисами-потребителями за счёт делегирования таргетированной рекламы с последних на первых. В таком контексте происходит не только лишь рекламирование сервисов-потребителей, но и также релевантный подбор/показ товаров на основе ранее полученной конфиденциальной информации.

3. Социальные сети представляют собой более гибридную модель поведения, потому как таковые сервисы способны предоставлять не только возможность коммуникации клиентов между собой, но и возможность коммуникации клиентов с товарами, формируя собственноручно торговые площадки. В результате становится возможным единовременное формирование как эффективного считывания, так и эффективного потребления конфиденциальной информации клиентов.

В теории, социальные сети способны существовать и без промежуточных сервисов-распределителей, но на практике этого они не делают, потому как основной их двигатель всегда остаётся статичным — максимизация прибыли. Выгодным становится не только использование полученной информации внутри своей

«экосистемы», но и также её продажа вовне и потребление извне.

В итоге всего вышеперечисленного остаётся лишь один единственный вопрос — как разрозненные сервисы способны с лёгкостью идентифицировать одного и того же клиента? Если бы это являлось сложной или невозможной задачей, то и сформировавшаяся цепочка сервисов становилась бы затруднительной или бессмысленной. Связано это, в первую очередь, с тем фактом, что получение максимальной прибыли с клиента неразрывно связано с качеством привязанной к нему конфиденциальной информации. Это, в свою очередь, становится возможным лишь за счёт формирования таргетированной рекламы, в основе которой заложена стабильная идентификация клиента.

Ответ на этот вопрос с постоянным развитием информационных технологий становится всё нагляднее и прямолинейнее. Большинство современных централизованных сервисов начинают проводить авторизацию клиентов исключительно за счёт его «привязки» к номеру телефона, ограничивая иные способы авторизации, которые ранее являлись оправданными и достаточными, как например использование электронной почты. Такая наращивающаяся стандартизация становится планомерной, потому как облегчает способы идентификации клиентов и, как следствие, облегчает связывание сервисов-считывателей и сервисов-потребителей с сервисами-распространителями. В итоге упрощение всей системы приводит лишь к тому, что хранилище сервиса-распределителя начинает представлять собой упрощённую базу данных по типу ключ-значение, где ключом становится номер телефона, а значением — вся обработанная информация, полученная от сервисов-считывателей.

2. ПАРАДИГМЫ СЕТЕВЫХ КОММУНИКАЦИЙ

Все сетевые коммуникации строятся на определённых топологиях, архитектурах, задающих последующее их применение. Топологию можно рассматривать как со стороны более низкого уровня, вида «звезда», «ячеистая», «шина», «кольцо» и т. п. [25], [26], так и со стороны более прикладного уровня, как «многоранговая», «одноранговая», «гибридная» [27]. На первый взгляд, таковые определения дают однозначные соответствия: «многоранговая» = «звезда» ИЛИ «звезда + иерархическая» ИЛИ «иерархическая», «одноранговая» = «ячеистая» ИЛИ «полносвязная», «гибридная» = «иерархическая + полносвязная» ИЛИ «звезда + ячеистая» и т. д. Но по мере изучения будут явно прослеживаться противоречия таковых суждений, при которых «одноранговая» архитектура может становиться «звездой», «гибридная» — «иерархической» и прочее.

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

2.1. СЕТЕВЫЕ АРХИТЕКТУРЫ

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

В одноранговых (peer-to-peer) системах все пользователи однородны, имеют одинаковые возможности, могут представлять одни и те же услуги маршрутизации [4, с. 792]. Сами одноранговые сети могут быть разделены на три модели: централизованные, децентрализованные и распределённые (последняя — условно). Централизованные одноранговые сети представляют собой соединения на базе одного или нескольких заранее выделенных или динамически выделяемых серверов-ретрансляторов, исключение которых приводит к блокированию всей сети. Отсутствие прав серверов в такой модели начинает порождать равноправность их клиентов. Распределённые сети не выделяют какой-либо центр или узел связи, сохраняя факт одновременной и полной коммуникации узла со всеми другими узлами, иными словами, со всей сетью. Иногда под распределённой связью подразумевают также необходимое *N*-е количество соединений, необязательно со всей сетью. В децентрализованных сетях становится возможным образование неравномерного распределе-

ния соединений и появление «неофициальных» узлов-серверов, часто используемых другими узлами в качестве последующей маршрутизации. Таким образом, децентрализованная модель в своём определении начинает быть более подверженной концентрированию линий связи, чем распределённая модель. Тем не менее распределённая модель является лишь конфигурацией децентрализованной и полноценно, в отрыве от последней, рассматриваться не может. Сети на основе одноранговой архитектуры расширяются извне, за исключением начальной фазы одноранговой централизации.

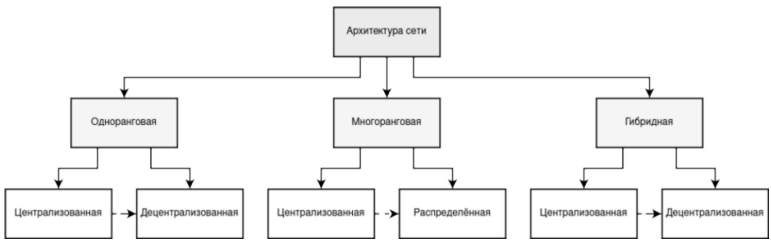

Рисунок 6. Сетевые архитектуры и их декомпозиция в моделях

Гибридная система объединяет свойства многоранговых и одноранговых архитектур, пытаясь взять и удержать как можно больше положительных и меньше отрицательных качеств. Сама гибридность системы может рассматриваться в разных значениях и проявлениях, как пример на уровне топологий: «шина + кольцо», «кольцо + полносвязная», «звезда + ячеистая» и т. д., или на уровне прикладного рассмотрения: «одноранговая + многоранговая». Плюсом многоранговых архитектур становится возможность разделения логики на серверную и клиентскую, а также более быстрая и/или статичная скорость маршрутизации. Плюсом одноранговых архитектур становится высокая отказоустойчивость за счёт внешнего расширения сети и возможность построения безопасной, а также масштабируемой «клиент-клиент» связи. Минусом гибридных архитектур

на ранних стадиях развития является их возможный, осуществимый и более вероятностный переход в многоранговые системы (по сравнению с одноранговыми) за счёт большого уплотнения серверов, принадлежащих одному лицу либо группе лиц с общими интересами.

2.2. АРХИТЕКТУРНЫЕ МОДЕЛИ

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

распределённой модели, потому как таковая в своей совокупности начинает уже содержаться в гибридных архитектурах, которые и становятся способными самостоятельно воссоздавать первично качественную анонимность, что является непосредственным противоречием. Таким образом, весь нижеизложенный материал необходимо пропускать через призму развития безопасности и анонимности как единого неразрывного целого.

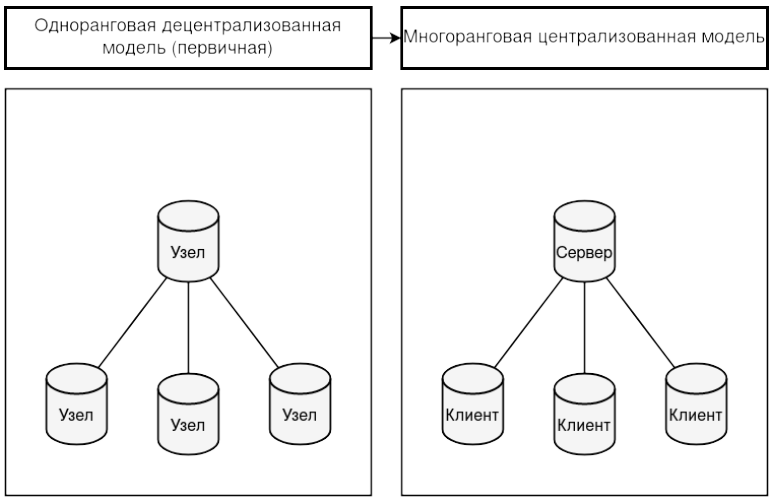

Рисунок 7. Становление многоранговой архитектуры из первичной одноранговой децентрализованной модели

Становление многоранговой централизованной (классической) системы является следствием отрицания одноранговой начальной децентрализованной модели как формы, нежизнеспособной к нарастающим реалиям масштабируемости. На данном этапе одноранговый узел, словно единая личность, расщепляется, чтобы собраться вновь, на два субъекта — клиента и сервера. Таковое разделение предполагает разграничение прав между обработкой информации со стороны сервера и её инициализаци-

ей со стороны клиента. В подобной системе информация становится отчуждённой от её первичного создателя и переданной в «руки» сервиса хранения. Клиентам в такой парадигме становится избыточно, проблематично и даже архаично создавать прямолинейные связи между друг другом, потому как их информация благоприятно начинает переходить в удобочитаемое и отсортированное состояние без добавочных проблем и трудностей в плане ручной настройки соединений и способа хранения данных. Инициализация единой точки отказа становится главным фактором развития иерархичности, но никак не точкой сопутствующего разрушения, как это было с первичной децентрализацией, когда таковая не могла эволюционировать без собственной деструктуризации. Когда многоранговая классическая централизованная система начинает нести бремя значительных рисков компрометации всей хранимой информации, она прогрессирует, вбирая в себя частично свойства первичной децентрализации и подстраивая их под собственный императив. Таким образом начинают зарождаться многоранговые распределённые системы.

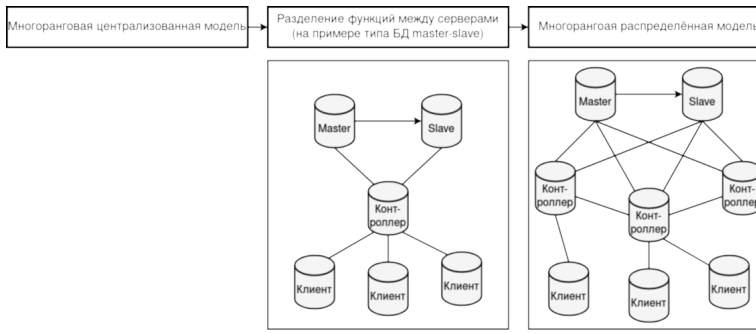

Рисунок 8. Развитие многоранговой архитектуры на примере типа БД «master-slave»

Становление многоранговой распределённой системы из классической централизованной является важным составляю-

щим фактором эволюции существующих иерархических сетей. Данное «разложение» как отрицание явной централизации начинается на этапе разделения функций, приравнивая сервер к определённому действию, как это изображено на *Рисунке 8*. 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 вследствие внутреннего алгоритма расширения системы, доступ к которому осуществляется наиболее высшими звеньями уже существующей и выстроенной иерархической цепи, а также вследствие бессмысленности существования узкоспециализированных одноранговых узлов вне всей системы. Поэтому, даже если внутри централизованных систем будет существовать *N*-е количество одноранговых, сама сеть не перестанет быть многоранговой до тех самых пор, пока будет существовать механизм восстановления и удержания иерархичности, а также до тех пор, пока одноранговые узлы будут оставаться специализированными конкретным задачам. Т. к. иерархичность в любом своём проявлении является следствием централизации, её закономерным развитием, то во всех последующих упоминаниях под термином «централизация» будет пониматься именно конечная фаза эволюции многоранговой архитектуры — распределённая модель.

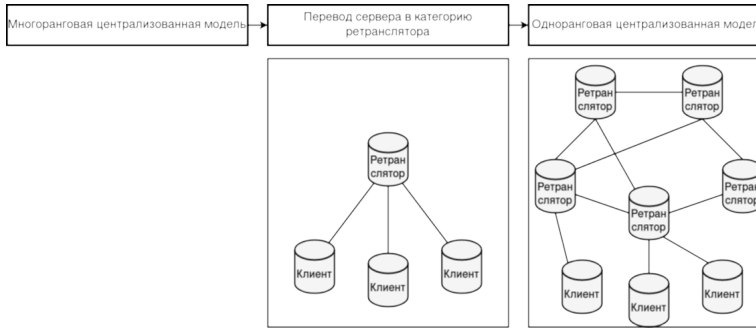

Рисунок 9. Становление одноранговой централизованной модели на примере перевода категории сервера в категорию ретранслятора

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

многоранговой распределённости, но также и расширяться извне, что присуще более одноранговым архитектурам. Таким образом, можно утверждать, что одноранговая централизация[1] становится в некой степени альтернативным вектором развития многоранговой централизации.

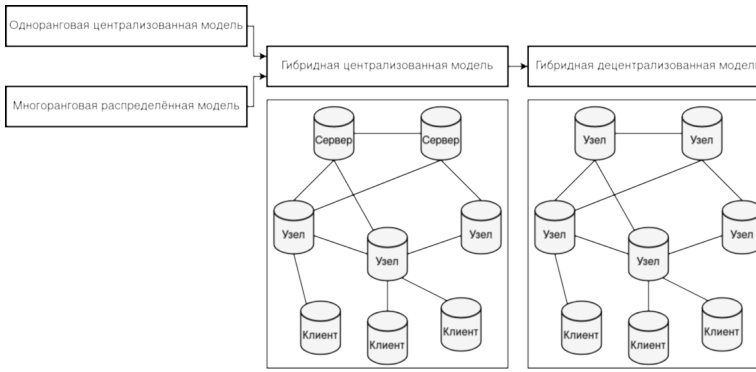

Рисунок 10. Развитие гибридной архитектуры на базе синтеза одноранговой централизованной и многоранговой распределённой моделей

[1] Одноранговая централизованная модель в своём финальном проявлении является достаточно отказоустойчивой системой, потому как позволяет ретрансляторам расширяться извне, тем самым ликвидируя потенциальную зависимость и уязвимость от многоранговых систем. Во внутреннем своём содержании финальная одноранговая централизация уже содержит зачаток образования финальной децентрализации, вобрав в себя децентрализацию бесправных ретрансляторов. Примером начальной формы одноранговой централизации может являться сеть Napster, а примерами финальной формы могут выступать такие системы, как протокол BitTorrent, в котором под ретрансляторами понимаются трекеры, а также сеть Gnutella2, где под ретрансляторами понимаются хабы (в терминологии данных сетей).

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

бридности), а Bitcoin к децентрализованной модели одноранговой архитектуры (децентрализованной модели гибридности).

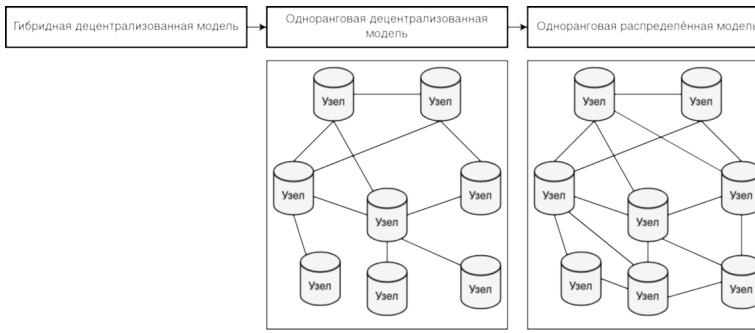

Рисунок 11. Развитие одноранговой децентрализованной модели на примере дальнейшей эволюции в лице распределённой модели

Становление одноранговой (финальной) децентрализованной системы не является прямым следствием развития централизованной модели. Централизация одноранговая по историческим причинам способствовала инициализации децентрализованной философии, но не за счёт последовательных этапов улучшения, а за счёт фактора нежизнеспособности, слабости в «сожительстве» с многоранговой системой [28] в начальной фазе своего существования. Последняя в буквальном смысле «поглотила» примитивную одноранговую централизацию, прервала этап её эволюции, привела к концентрированному методу выстраивания связей и иерархическому способу существования системы. Таким образом, децентрализованная модель должна была стать более качественным выражением и проявлением одноранговой архитектуры, чем централизованная. Итогом такого процесса стало объединение клиентской составляющей с серверной частью, породив тем самым узлы связи как отдельные сетевые единицы коммуникации, возникшие из эволюции ги-

бридных архитектур. Частным случаем продолжительного развития одноранговой децентрализации является становление распределённой системы как следствия нарастающей концентрации линий связи со стороны децентрализованной модели, претерпевающей этапы «коррозии» централизацией и приводимой к возникновению «узких» мест среди нескольких сетевых множеств. Противоречием децентрализованных моделей является их постоянное движение к сосредоточению соединений, от хаотичности к порядку, от безопасности к отказоустойчивости, — таковыми становятся основные векторы регресса децентрализации, основанные на выборе наиболее стабильных узлов. Решением становится иная и более качественная концентрация линий связи, основанная на объединении узлов посредством многочисленных соединений, в противовес единому центру коммуникаций, и, как следствие, фактор стабильности возобновляется, но в уже количественном выражении узлов.

2.3. ЗАМКНУТОСТЬ МОДЕЛЕЙ

Метаморфозы сетевых моделей кратко представляются через призму детерминированного конечного автомата, изображённого на *Рисунке 12*, состояния которого изменяются по мере исторической на то необходимости и направленности. Так, например, действия (*a, d, g*) можно рассматривать как необходимость в переосмыслении, во внешнем отрицании, (*b*, *f*) — необходимость в развитии, во внутреннем отрицании, (*c+e*) — необходимость в объединении, в синтезе отрицаний. Из всего вышеприведённого возможно составить выражения, относящиеся к развитию каждой определённой модели, где многоранговая централизация = (*a*), многоранговая распределённость = (*ab*), одноранговая централизация = (*ad*), гибридная централизация = (*abc+ade*), гибридная децентрализация = (*abc+ade*) (*f*) и в конечном итоге одноранговая децентрализация = (*abc+ade*) (*fg*).

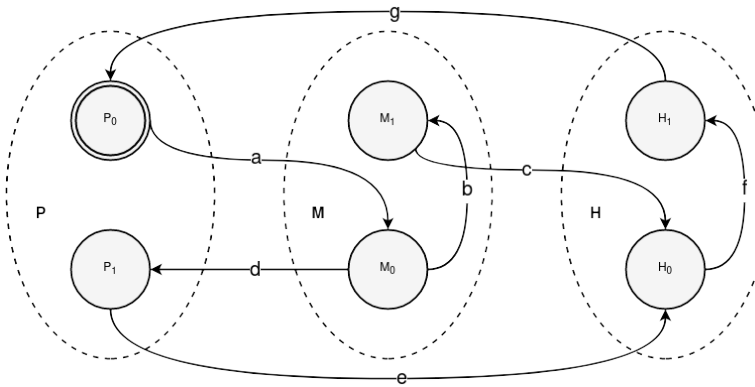

Рисунок 12. Конечный автомат развития сетевых архитектур посредством движения их моделей, где {P, M, H} — сетевые архитектуры: P — одноранговая, M — многоранговая, H — гибридная

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

3. ОПРЕДЕЛЕНИЕ СКРЫТЫХ СИСТЕМ

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

3.1. АНОНИМНЫЕ СЕТИ

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

или оставаться скрытой [29], [30].

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 [31]. Именно по историческим причинам современные скрытые сети имеют оверлейные уровни безопасности.

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

По скорости и способу распространения информации выделяют два вида анонимных сетей — с низкими и высокими задержками [32]. Системы с низкими задержками ставят в качестве базовой необходимости скорость, эффективность транспортирования информации между истинными её субъектами, при этом уровень анонимности таковых сетей недостаточен для противодействия атакам со стороны внешних глобальных наблюдателей (как доказательство фактора существования сильной анонимности). Системы с высокими задержками ставят в качестве базовой необходимости высокий уровень анонимности, в том числе и направленный на противодействие глобальным наблюдателям, но при этом скорость передачи становится в таковых сетях самым главным недостатком. Из вышеописанного следует классическая проблема проектирования безопасных систем — выбор компромисса между производительностью и безопасностью.

В качестве примеров систем с низкими задержками выделяют Tor, I2P, Tarzan и т. д., а с высокими задержками — Mixminion, Herbivore, Dissent и т. п.

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

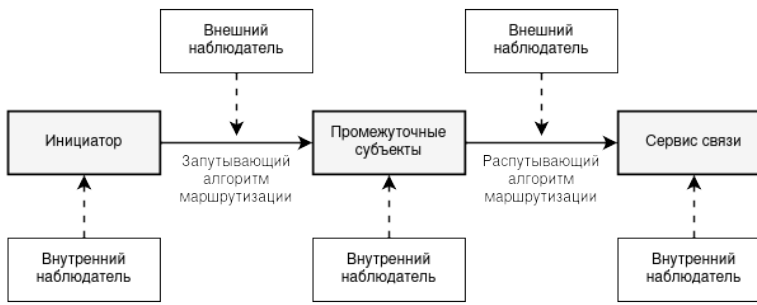

Рисунок 13. Внешние и внутренние наблюдатели (атакующие) в критериях запутывающего алгоритма маршрутизации

Запутывающий алгоритм определяется дополнительной нагрузкой к нагрузке распространения/транспортирования информации относительно базового алгоритма маршрутизации. В отличие от основной нагрузки базового алгоритма, стремящегося наиболее быстро и/или доказуемо передать информацию от одной точки к другой (или ко множеству других), дополнительная

нагрузка сводится, в той или иной мере, к отрицанию базовой, ухудшая её скорость и/или корректность доставки с целью сопутствующего ухудшения внешнего и/или внутреннего анализа: либо связей между точками, либо непосредственно их активности.

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

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

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

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

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

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

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

Примером таковых сетей может являться сеть, где отправитель транспортирует полностью зашифрованное сообщение всем

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

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

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

Первый пункт относится к критерию несвязываемости, в то время как второй и третий пункты к критерию ненаблюдаемости [32]. Критерий ненаблюдаемости уже включает в себя критерий несвязываемости. Если пойти от обратного и предположить лож-

ность данного суждения (то есть отсутствие несвязываемости в ненаблюдаемости), тогда можно было бы при помощи несвязываемости определить существование субъектов информации и тем самым допустить нарушение ненаблюдаемости, что является противоречием для последнего.

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

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

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

Скрытыми сетями с теоретически доказуемой анонимностью принято считать замкнутые, полностью прослушиваемые системы, в которых становится невозможным осуществление любых

пассивных атак (в том числе и при существовании глобального наблюдателя), направленных на деанонимизацию факта отправления и/или получения информации, или на деанонимизацию связи между отправителем и получателем с минимальными условностями по количеству узлов, не подчинённых сговору. Говоря иначе, с точки зрения пассивного атакующего, апостериорные знания, полученные вследствие наблюдений, должны оставаться равными априорным, до наблюдений, тем самым сохраняя равновероятность деанонимизации по *N*-му множеству субъектов сети.

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

3.2. КЛИЕНТ-БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ

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

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

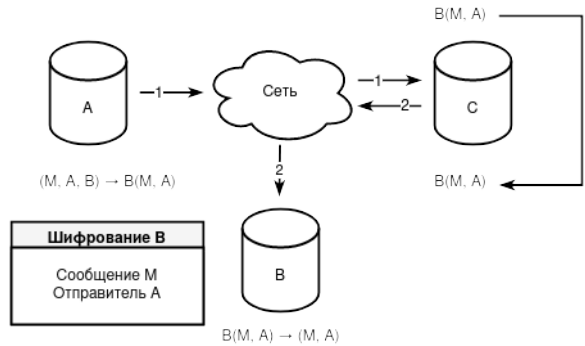

Рисунок 14. Общая схема клиент-безопасных приложений

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

аутентифицируя инициатора связи. Схема «логин/пароль» способна применяться в таких системах, но уже локально, для защиты приватного ключа конкретно выбранного участника сети.

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

3.3. ТАЙНЫЕ КАНАЛЫ СВЯЗИ

Секретные, тайные, эзотерические каналы связи — есть соединения, располагаемые в заведомо замкнутом, незащищённом, враждебном окружении и имеющие характеристики безопасной передачи информации. В отличие от определения [33, с. 147], в нашем случае под тайными каналами будут пониматься системы «неорганически вживляющиеся» в уже существующие сети. При этом анонимность, родственная скрытым сетям, не является базисом секретных каналов связи и, следовательно, может быть отброшена из-за ненадобности или по необходимости. Из такого краткого определения можно выделить две формы тайных каналов связи:

1. Первой формой тайных каналов связи можно считать сохранение экзотеричности субъекта и эзотеричности объекта, благодаря использованию криптографических методов преобразования информации. Но стоит также заметить, что такой принцип сохраняется и при использовании стеганографических методов [34], поскольку субъект остаётся открытым, а объект продолжает быть закрытым (только вместо сокрытия информа-

ции скрывается сам факт её существования). При этом, если в секретных каналах связи используются именно криптографические методы, то они не ограничиваются только идентификацией субъектов (целостностью, аутентификацией), но также и применяют практику шифрования объектов (конфиденциальность). Примером такого поведения может служить использование программ типа PGP [33, с. 785], [35] на форумах, в мессенджерах, социальных сетях.

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

Тайные каналы связи не стоит считать отдельным видом скрытых систем, потому как таковые являются лишь и только способом применения клиент-безопасных приложений или анонимных сетей на специфичном уровне. Тем не менее всё становится не таким простым и очевидным, как только начинает происходить анализ становления тайных каналов связи. Вкратце секретные каналы связи представляют собой сетевую абстракцию, которая может рассматриваться как способ инициализации безопасных оверлейных систем. Такое суждение неминуемо приводит к противоречию, потому как начинает инверсивно и рекурсивно указывать иное место в иерархии связей становления скрытых систем, представляя тайные каналы связи инициатором развития анонимных сетей и клиент-безопасных прило-

жений, а не наоборот, как это было описано ранее. Но именно свойство «неорганической вживляемости» является решающим фактором, по которому становится невозможным считать тайными каналами связи большинство безопасных оверлейных соединений. Под «неорганической вживляемостью» понимается использование оверлейного соединения поверх прикладного уровня связи, когда первичная система уже полностью выстроилась и функционирует с определённой целью. Поэтому, как пример, нельзя полноценно считать тайными каналами связи безопасные или анонимные сети, базируемые на сети Интернет. Но это не говорит о том, что сама сеть Интернет не может содержать тайных каналов связи на своём функционируемом уровне. Как пример, определённые поля в протоколе IP (адрес источника = *N*-бит при существовании нескольких принимающих узлов с разными адресами, контрольная сумма = *N*-младших подобранных бит и т. д.) или TCP (порт источника = *N*-бит при существовании нескольких принимающих процессов с разными портами, опции = 2 байта, контрольная сумма подобно примеру из IP и т. д.) могут содержать изменяемые по мере необходимости биты, что способно приводить к распространению (утечке) информации на специфичном уровне работы самой сети. Это как раз и указывает на эзотерический способ применения тайных каналов связи, и подтверждает тот факт, что таковые не образуют соединений и не являются инициализаторами связей, потому как лишь внедряются, на своей «паразитической» основе, в уже существующие сети. Можно также сказать, что тайные каналы связи представляют собой свойство гипертелии (сверхокончания), когда дополняют базовую систему вспомогательными, второстепенными функциями, которыми таковая ранее не обладала.

Тайные каналы связи, использующие стеганографию, всегда имеют некий контейнер, в который помещается истинное сообщение [34, с. 8]. Под контейнером может пониматься ложное, неявное, сбивающее с пути сообщение, которое чаще всего носит нейтральный характер. Из этого также следует, что в зави-

симости 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, аудиозапись, видеофайл, то есть всё, что может хранить дополнительную или избыточную информацию, которая останется незаметной для человеческих глаз и ушей. Одним из примеров сокрытия информации может служить замена каждого старшего бита в изображении битами исходного сообщения. Таким образом, если размер изображения (то есть контейнера) будет равен 2MiB (без учёта метаданных), то максимальный размер исходного сообщения (в лучшем случае) не будет превышать 256KiB.

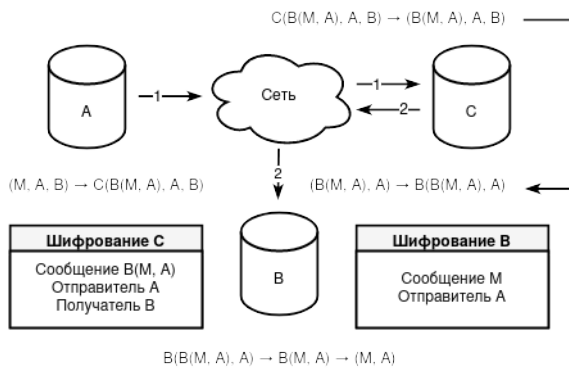

Рисунок 15. Общая схема тайных каналов связи

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

текст дополняется до блока), а из этого уже следует, что максимальный размер исходного сообщения уменьшается.

Существует ещё один, третий способ сокрытия информации, относящийся к криптографическим, но при этом обладающий некоторыми стеганографическими свойствами, качествами, особенностями [33, с. 720]. Это не является последовательным объединением, использованием методов, как это было описано выше, а скорее оказывается их слиянием, синтезом и симбиозом. В таком методе истинная информация скрывается в цифровой подписи ложного сообщения на основе общего согласованного ключа, где главной чертой и исключительностью является стойкость ко взлому, сродни сложности взлома цифровой подписи. При этом сама подпись — есть контейнер, скрывающий существование сообщения методом аутентификации ложной информации.

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

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

4. АНАЛИЗ СЕТЕВОЙ АНОНИМНОСТИ

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

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

4.1. СТАДИИ АНОНИМНОСТИ

Потому как сетевая анонимность есть объект фрагментированный со стороны определений и терминологий, то можно предположить неоднородность и факт становления, развития в определённых этапах. Вкратце анонимность становится возможным трактовать как некую градацию, поэтапность, которой

присуще шесть стадий, выявляющих процесс её формирования посредством фаз отрицаний и внутренних противоречий.

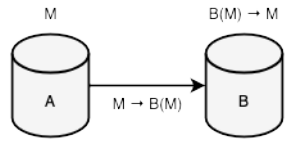

Рисунок 16. Первая стадия анонимности (прямое соединение)

1. Первая стадия является исходной точкой анонимности, тезисом, монадой, примитивно не представляющей анонимность, пустотой, инициализирующей мощность анонимности[1] *|A| = 0*. Примером является существование только прямого, прямолинейного, примитивного соединения «клиент-клиент» между дву-

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

|A| = |Q (R) |, *где*
R — множество узлов, участвующих в маршрутизации,
Q — функция выборки списка подмножеств узлов, подчиняющихся од-

мя одноранговыми субъектами, что равносильно их стазисному состоянию. По причине отсутствия промежуточных субъектов мощность доверия на данном этапе представляет минимально возможную величину.

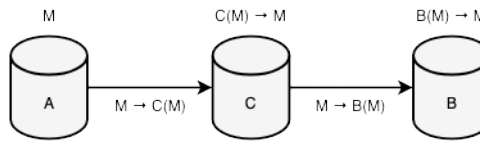

Рисунок 17. Вторая стадия анонимности (соединение посредством сервиса)

2. Вторая стадия, становясь антитезисом, начинает отрицать первый этап, приводить систему к первичному метастазису, изменять собственным преобразованием способ взаимодействия

ному лицу или группе лиц с общими интересами.

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

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

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

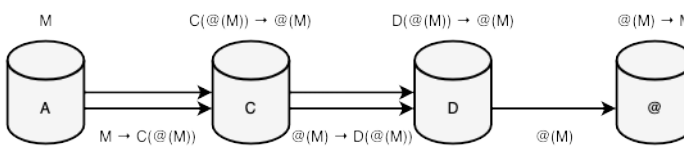

Рисунок 18. Третья стадия анонимности (proxy-транслирование)

3. Третья стадия, являясь синтезом предыдущих стадий, представляет примитивную маршрутизацию, а следовательно и примитивную анонимность нескольких прокси-серверов, не связанных между собой. Именно на данном этапе сеть становится раздробленной, неопределённой, гибридной за счёт чего и повышается мощность анонимности методом стремления к статичному значению $lim_{|A|\to C}$, где C — количество прокси-серверов. Данный метод предполагает выстраивание цепочки узлов, через которые будет проходить информация. Мощность анонимности на данном этапе действительно повышается, но и безопасность самих субъектов ещё никак не обеспечивается. Связано это всё потому, что шифрование на данном этапе есть свойство добавочное (сродни второй стадии), не обеспечивающее защиту связи «клиент-клиент», а следовательно, и не приводящее к уменьшению мощности доверия. На *Рисунках 18, 19, 21* изображён абстрактный субъект @, способный быть как настоящим получателем, так и промежуточным субъектом — сервисом.

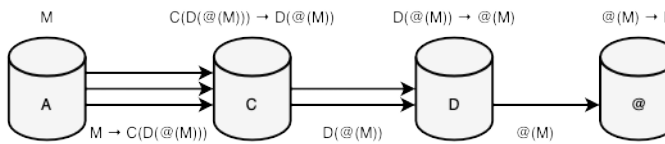

Рисунок 19. Четвёртая стадия анонимности (VPN-туннелирование)

4. Четвёртая стадия, как развитие третьего этапа, инициализирует способ изменчивости, полиморфизма информации[1] посредством её множественного шифрования, туннелирования.

К такому этапу относятся VPN-сервисы (виртуальные частные сети) как *N*-е сочетание прокси-серверов со внутренними слоями шифрования [36], где мощность доверия и мощность анонимности эквивалентно третьей стадии. Отличительной особенностью четвёртого этапа является существование выходных узлов, постепенно «раскрывающих» истинную информацию, созданную до первичного туннелирования на отправляющей стороне, из-за чего и появляется возможность к сокрытию метаданных, связующих инициатора сообщения и сервер назначения. В связи с этим данный этап изменяет способ маршрутизации, придаёт ему свойство полиморфизма как изменчивости закрытой информации по мере перехода от одного узла к другому и отстраняет промежуточные узлы к анализу и сравниванию шифрованной информации. Таким методом скрывается настоящая связь между субъектами посредством их объекта, а следовательно, и анонимат начинает обретать более истинный характер, при котором стремление системы к увеличению и сдерживанию мощности анонимности становится более качественным в сравнении с третьей стадией.

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

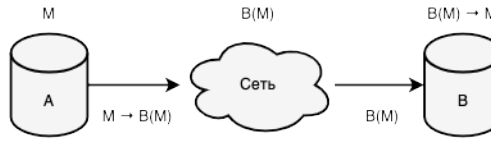

Рисунок 20. Пятая стадия анонимности (соединение посредством абстрактной сети)

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. [37], [38], где главным фактором идентификации клиентов становятся криптографические адреса (публичные ключи, хеши публичных ключей). Сеть начинает представлять собой не только гибридный, но и одноранговый характер поведения узлов с возможным и дополнительным динамическим способом определения мощности анонимности, как $0 < |A| \leqslant N$, где N — количество узлов в сети, обуславливаемым слепой заливочной маршрутиза-

цией [4, с. 398] и криптографической идентификацией. При этом стоит заметить, что на данном этапе не существует какого бы то ни было полиморфизма информации (как это было в четвёртой стадии), что приводит к внутренним противоречиям одновременного прогресса и регресса анонимности. Поэтому пятую стадию можно вкратце охарактеризовать игнорированием анонимности (экзотеричностью) со стороны субъекта и её сохранением (эзотеричностью) в передаваемом объекте. На *Рисунке 20* под сетью понимается переключение системы из состояния сетевой идентификации к идентификации криптографической, вследствие чего происходит абстрагирование информации об отправителе для получателя и о получателе для отправителя непосредственно.

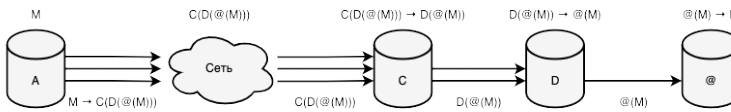

Рисунок 21. Шестая стадия анонимности (абстрактная сеть + тунелирование)

6. Шестая стадия приводит к единовременному отрицанию и синтезу четвёртой стадии как системы, не ориентированной на анонимную идентификацию субъектов, и пятой стадии как системы, не направленной 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. Примером шестой стадии является большинство скрытых сетей, наподобие Tor (onion routing) [39], I2P (garlic routing) [40], Mixminion (mix network) [41] и т. д. На *Рисунке 21* изображён прототип функционирования системы Tor с запросом, ориентированным на внутренний ресурс (в качестве упрощения показана схема с двумя промежуточными узлами).

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

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

руются от конечного потребителя информации и акцентируют внимание только на сам способ передачи. Исключением всего вышесказанного является лишь первая стадия анонимности, где сам факт передачи является одновременно и способом финального получения информации.

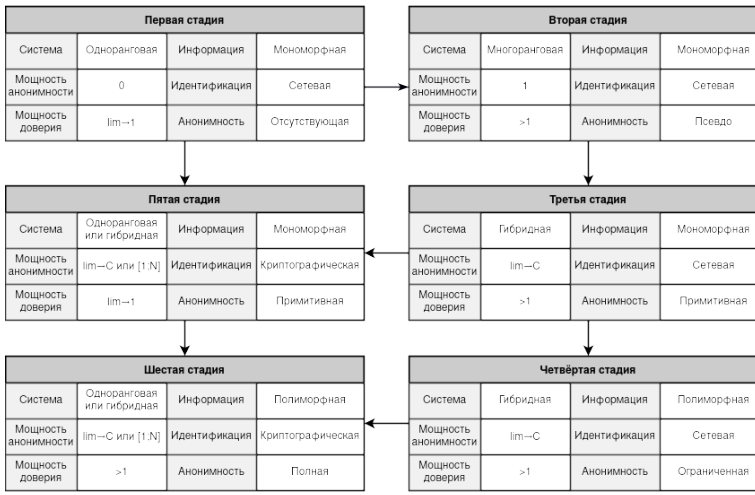

Рисунок 22. Развитие анонимности как процесс формирования стадий

Защита, определяемая связью «клиент-клиент», зарождается на моменте первой стадии анонимности и впоследствии 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 пя-

том этапе и ровно там же заканчивается, потому как целью всех последующих стадий уже является сокрытие субъектов информации посредством методов транспортирования объекта на базе криптографических адресов, где более не ставится вопрос истинности принимающей стороны.

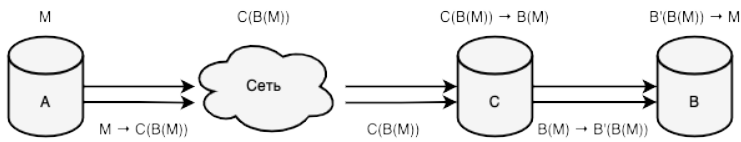

Рисунок 23. Тайный канал связи на базе пятой стадии анонимности, где A, B — отправитель/получатель, C — сервис связи

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 [42, с. 223]. Дополнительно может появляться свойство конфиденциальности, где информация начинает представлять собой суть секретного, тайного, шифрованного, а не открытого и общего объекта. Но и само свойство конфиденциальности на данном этапе — есть дополнительный критерий, а следовательно, может быть удалён, если таковой является избыточным для самой системы. Как пример, в криптовалютах имеются свойства целостности и аутентификации, но не всегда конфиденциальности.

На основе четвёртой стадии анонимности становится возможным формирование принципа федеративности, который более качественно выражается уже непосредственно на шестой

стадии анонимности. Принцип федеративности сводится к двум нижеприведённым критериям и базируется на количественных характеристиках мощности федеративности[1].

1. Необходимо 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. Необходимо использовать изменения информации в процессе её маршрутизации. При таком способе информация будет представлена в полиморфной и самоизменяющейся оболочке. 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.

[1] Мощность федеративности — количество государств, не связанных между собой общими политическими интересами, 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. Также из этого следует, что обычная неполиморфная маршрутизация не будет повышать мощность федеративности, даже при учёте существования нескольких несвязанных государств.

На основе пятой стадии анонимности становится возможным формирование тайных каналов связи первой формы, как это представлено на *Рисунке 23*. Такое свойство достигается появлением криптографической идентификации субъектов, благодаря которому становится возможным абстрагироваться от сетевой идентификации.

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

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

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

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

Второй пункт является в определённой степени упрощением, потому как разрыв связи должен происходить также и между двумя криптографическими идентификациями разнородных систем, сливаемых между собой в одну цельную, а не только между сетевой и криптографической идентификациями. Так, например, если объединяется пятая и шестая стадии между собой,

то криптографическая идентификация одного и того же субъекта должна «раздваиваться» под пятую и шестую стадии соответственно. Таким образом, в подобном синтезе идентификация субъекта должна быть выражена как последовательность идентификаций вида «сетевая → криптографическая (шестая стадия) → криптографическая (пятая стадия)».

Скрытая система, наделённая только первыми двумя пунктами, является анонимной сетью. Скрытая система, наделённая только последними двумя пунктами, является клиент-безопасным приложением. Скрытая система, наделённая сразу тремя критериями анонимности, является полной и принадлежит не отдельной стадии анонимности, а их комбинациям. Система, наделённая только одним пунктом из трёх, не является скрытой. Под системой с первым пунктом может пониматься VPN-туннелирование, а под вторым — централизованные сервисы связи. Не существует систем исключительно с третьим пунктом, равно как и комбинации третьего пункта с первым, потому как третий критерий является лишь следствием второго (обратное суждение неверно). Все вышеприведённые дескрипции можно представить в более кратком списке описания примеров:

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

Таким образом, на основании вышеприведённых критериев обязанностей вида «быть, иметь, предотвращать» можно выявить базовое определение анонимности относительно общего типа скрытых систем, где под сетевой анонимностью будет пониматься разрыв большинства логических связей между транс-

портируемым/хранимым объектом и его субъектами, а также между сетевой и криптографической идентификациями.

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

4.2. ВТОРОЙ ВЕКТОР РАЗВИТИЯ

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

1. Первая стадия анонимности исключает из своего рассмотрения промежуточные субъекты. Если данная стадия переходит

в состояние анонимной сети, то внутри неё способны зарождаться сервисы связи, основанные либо на второй, либо на пятой стадиях анонимности. Таким образом, получатель в анонимной сети становится не равен конечному получателю в условиях прямого соединения, что противоречит определению первой стадии анонимности.

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

Все парадоксы базируются на самой двойственной форме первой стадии, когда таковая одновременно вбирает в себя и выраженное транспортирование объекта, и конечное его хранение. Парадоксы своим существованием фактически расщепляют двойственность и образуют новое подмножество как неявную градацию первой стадии анонимности. Во всех последующих упоминаниях вышеописанный этап с присущими парадоксами будет отображаться как «первая^ стадия анонимности», со знаком циркумфлекса. В качестве примера существования первой^ стадии анонимности выделяют скрытые сети, базируемые на проблеме обедающих криптографов [43] (DC-сети), такие, как Dissent [44] и Herbivore [45]. Чистая форма первой^ стадии анонимности (выраженная в DC-сетях) приводит к следующим недостаткам.

1. Масштабируемость. Первая^ стадия анонимности приводит к необходимости выстраивания большого количества прямых соединений, что приводит к проблеме масштабируемости, где каждый новый пользователь обязан подключаться ко всем

существующим участникам сети. Проблема решается переводом первой^ стадии анонимности на градации высшего порядка, образуя промежуточные узлы, полностью не влияющие на уровень анонимности в сети. Dissent переводит систему на третью стадию анонимности, Herbivore на третью при локальной топологии и на пятую при глобальной.

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

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

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

и доказуемую анонимность субъектов без безопасности объектов (первая стадия с противоречиями или неклассическая форма первой стадии).

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

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

1. Маршрутизация. Первая^ стадия анонимности в своей минимальной реализации не предполагает промежуточных субъектов, что может приводить к ошибочным суждениям об отсутствии маршрутизации, и в частности — запутывающей маршрутизации. Ложность тезиса можно доказать тем фактом, что участники сети на базе первой^ стадии анонимности кооперируют и объединяют информацию в одну выходную последовательность бит, где даже при связи «*все-ко-всем*» передаётся уже «скрещиваемая» информация, что, в свою очередь, становится запутывающим алгоритмом маршрутизации. В отличие от множественного шифрования, при котором информация распространяется посредством системы, в первой^ стадии анонимности сама система изнутри начинает генерировать полиморфную информацию. Поэтому ложность тезиса базируется исключительно на предположении того, что «полиморфизм информации = множественное шифрование», что не есть верно, потому как «множественное шифрование $\in$

полиморфизму информации», равно как и «алгоритм запутывающей маршрутизации первой^ стадии анонимности ∈ полиморфизму информации».

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

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

Из всего вышеописанного мощность доверия $|T|$ первой^ стадии анонимности становится эквивалентна количеству её участников = N без инициатора связи $|T| = N-1$, а мощность анонимности $|A|$ начинает стремиться к количеству участников сети без инициатора связи $lim_{|A|\to N-1}$. Это является хорошим показателем противоречия между безопасностью передаваемых объек-

тов и анонимностью субъектов, потому как первая стадия как оригинальный классический вектор развития скрытых систем обладает полностью инверсивным определением равным $lim_{|T| \to 1}$, $|A| = 0$.

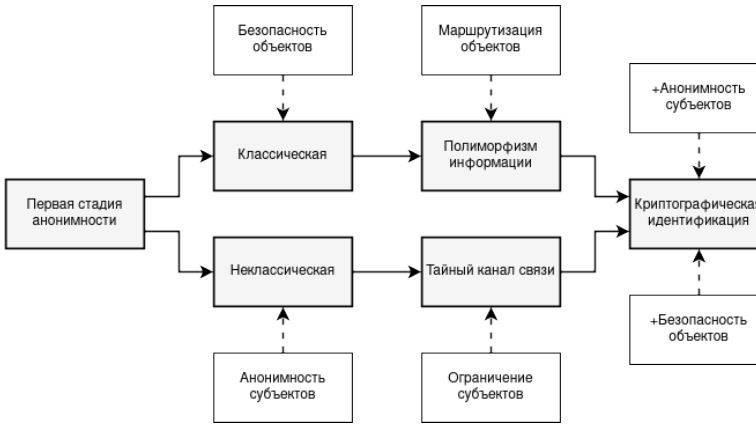

Рисунок 24. Двойственный вектор развития скрытых сетей относительно первой стадии анонимности для нешироковещательных коммуникаций

Далее, если начать анализировать подобным же методом оставшиеся стадии анонимности, то можно заметить явным образом схожие противоречия и на стороне пятой стадии, при условии, что таковая система становится скрытой сетью, нацеленной на реализацию запутывающей маршрутизации отличной от множественного шифрования. Так, например, если трактовать пятую стадию анонимности как первую стадию с задержками связи, иными словами, абстрагироваться от существования промежуточных субъектов (т. к. таковые не нарушают безопасность связи типа «клиент-клиент»), то можно свести второе противоречие первой стадии к пятой. И действительно, если пятая стадия анонимности также является платформой связи с постоянным стремлением

к уменьшению мощности доверия, как и первая, то в таком случае становится возможным порождение анонимных сетей, неминуемо приводящих к аналогичным противоречиям в существовании промежуточных субъектов с повышенной мощностью доверия. Таким образом, ответвление оригинальной формы пятой стадии анонимности, с присущей ей противоречивостью, будет называться далее пятой^ стадией анонимности.

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

4.3. РЕГРЕСС МОЩНОСТИ ДОВЕРИЯ

При существовании и полной реализации, а также доступности скрытых сетей проблема, связанная с мощностью доверия, возвращается. Это кажется парадоксальным, ведь сама задача ещё решилась на пятой стадии анонимности, когда мощность доверия становилась минимально возможной величиной. Сложность заключается именно в том, что при достижении анонимности стремление к уменьшению мощности доверия начинает игнорироваться, становиться второстепенным и добавочным критерием, в то время как стремление к увеличению мощности анонимности начинает переходить в 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.

Сутью проблемы становится возможность создания сервисов связи внутри скрытых сетей, не основанных на пятой стадии анонимности (*Рисунок 25*), что приводит к возникновению приложений на базе второй стадии, представляющих угрозу информационной безопасности. Это связано с тем фактом, что анонимные сети в массе своей базируются на принципах третьей стадии анонимности, в которой игнорируется истинность получаемой стороны. Подобная абстрагируемость неявно порождает возможность централизации внутри ризоморфных систем, тем самым косвенно приводя к потере настоящей безопасности транспортируемых объектов.

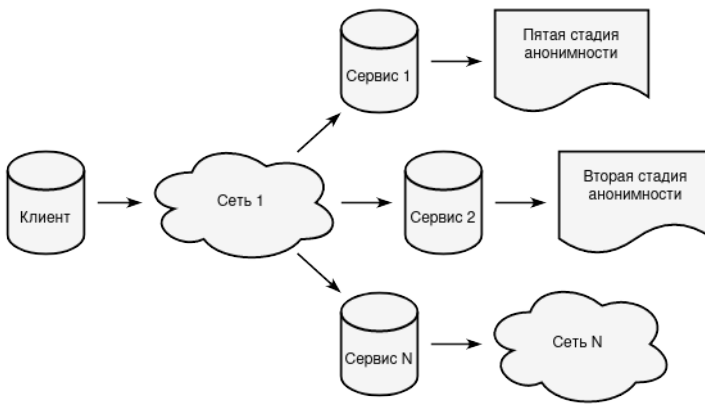

Рисунок 25. Взаимодействие скрытых сетей со внутренними сервисами

В качестве примера можно привести сеть Tor. Доступ к сервису осуществляется вполне анонимно, но при этом сам способ хранения информации в данном приложении полностью зависит от его владельца. Это приводит к тому, что мощность доверия будет приближаться к обычному среднестатистическому сервису, построенному на мощности анонимности равной единице. В итоге становится безразличным сама среда работающе-

го приложения, т. к. первоначальная проблема доверия будет оставаться в неизменно исходной форме со стороны второй стадии анонимности.

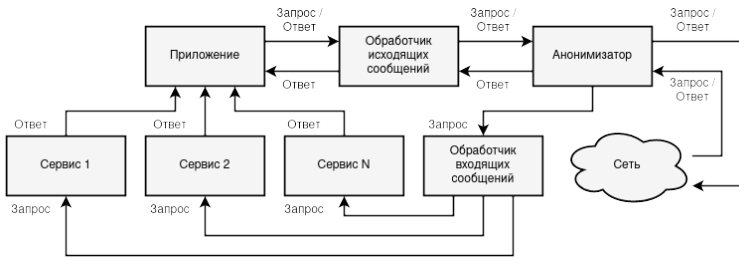

Рисунок 26. Пример архитектуры приложения анонимной сети с несколькими принимающими сервисами

Решить данный вопрос возможно лишь ограничением допустимых сервисов со стороны самой скрытой сети. Таким образом, анонимная сеть в своей базе и основе должна быть имманентной и имплозивной, содержать *N*-е количество приложений, построенных только на пятой стадии анонимности. Доступ к любым другим сервисам, не имеющим пятую стадию анонимности, или скрытым сетям, не реализующим безопасную архитектуру, должен быть закрыт и ликвидирован. Только методом ограничений и соединений будет возможна синергия свойств анонимности и безопасности. Примером таких сочетаний могут служить связи Tor+Bitcoin, I2P+Filetopia и т. п., или более монолитные технологии Monero [46], Dash [47] и т. д. Только на данном основании скрытые системы становятся полными.

4.4. АЛГЕБРАИЧЕСКИЕ МОДЕЛИ

Анонимные сети базируются на определённых шаблонах, конструктах или примитивах проектирования, в которых учитываются роли субъектов и конструируемые модели угроз. В наи-

более простых случаях используется только один шаблон проектирования, в других используются уже комбинации подобных паттернов, что может приводить к некоторым улучшениям, новым возможностям и параллельно к усложнению итоговой логики приложения.

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

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

2. «*Периодичность*» $T_p\ (f,\ X,\ t) = t \rightarrow f\ (X)$. Если на вход алгоритму поступает информация *X*, тогда необходимое действие *f* как ответ должно выполняться только после совершения периода равного *t,* зависимого или независимого от времени поступающей информации *X*. Может представлять высокое качество анонимности за счёт уменьшения качества производительности вычислений. Имеет самое малое количество способов применения из-за своих накладных расходов. В качестве примера можно привести сеть Herbivore и устанавливаемое расписание генерации.

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

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

I. *Генезис конструкт*

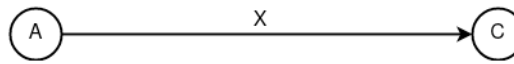

Рисунок 27. Генезис конструкт «генерирование»

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

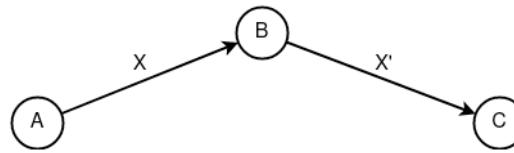

Рисунок 28. Базовый конструкт «следование»

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

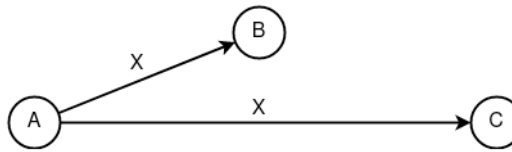

Рисунок 29. Базовый конструкт «распространение»

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

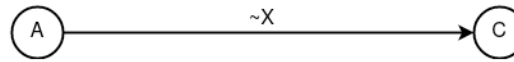

Рисунок 30. Базовый конструкт «запутывание»

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

III. *Составные конструкты*

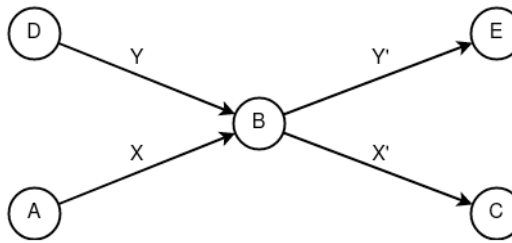

Рисунок 31. Составной конструкт «перемешивание»

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

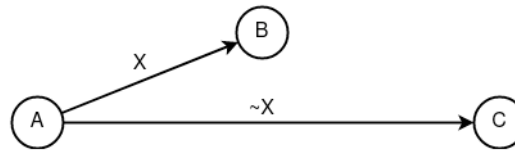

Рисунок 32. Составной конструкт «расщепление»

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

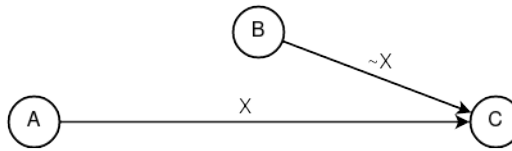

Рисунок 33. Составной конструкт «сведение»

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

Теперь в качестве примера становится возможным формирование связи между конструктом «Генерирование» и свойством «Периодичность» следующим образом: $G_cT_p = T_p\ (G_c, X, t)$. В таком случае само отправление информации X (а точнее множества информаций вида X_i) от одного абонента к другому будет периодичным по времени t.

Свойства, в отличие от конструктов, не имеют возможности накладываться друг на друга или формировать определённые композиции своих функций. Так, например, если существует некий абстрактный конструкт A_c, то становится невозможным применение операций типа $A_cS_pT_p$, $A_cT_pA_p$, $A_cA_pS_p$ и т. д. Тем не менее за счёт возможности комбинирования конструктов появляется возможность и комбинирования свойств, на примере суммирования их связей: $A_cS_p+A_cT_p$. Плюс к этому появляется возможность и комбинировать конструкты с одним лишь свойством по типу $A_{c1}A_{c2}T_p$.

Вследствие этих наблюдений можно заметить, что конструкты и свойства зависимы друг от друга, но имеют разные пропорции зависимостей, что легко наблюдается в возможности создавать N-е количество конструктов с одним лишь свойством, но в невозможности создавать N-е количество свойств с одним конструктом. Связано это в первую очередь с тем, что конструкты определяются наследованием предыдущих, более базисных конструктов, в то время как свойства определяются своеобразным методом соединения таковых наследований.

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

следствием свойства «поточность» конструкта «следование», в то время как статичный конструкт «перемешивание» обуславливается свойством «аккумулятивность».

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

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

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

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

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

На основе вышеприведённых конструктов, а также их свойств, становится возможным формирование анонимизирующих схем. Результатом таких схем становится возможность вы-

страивания любых типов анонимизирующих связей: 1) анонимность отправителя или получателя, 2) анонимность отправителя и получателя, 3) анонимность связи между отправителем и получателем. Это можно продемонстрировать на следующих примерах.

I. Анонимность связи между отправителем и получателем

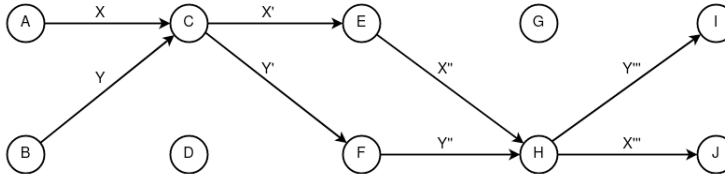

Рисунок 34. Применение конструктов «следование» и «перемешивание», где {*A, B*} — отправители запакованной информации {*X, Y*}, {*I, J*} — получатели информации {X^{III}, Y^{III}}

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

Алгебраическая модель

$n\ (F_c S_p)$ [пример: Tor, I2P]
ИЛИ
$n\ (F_c A_p)$ [пример: Mixminion]

II. Анонимность отправителя

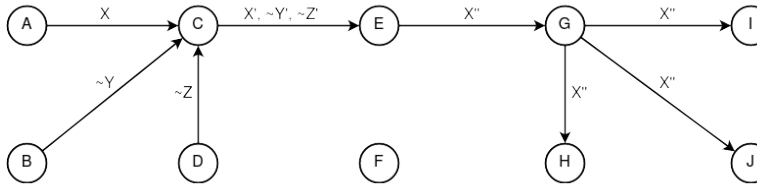

Рисунок 35. Применение конструктов «запутывание», «перемешивание», «сведение», «следование» и «распространение», где *A* — отправитель запакованной информации *X*,*C* — узел «перемешивания»,*E* — узел «сведения», {*G, H, I, J*} — получатели информации X^{II}

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

Алгебраическая модель

$(F_cT_p;\ {}_Fc_Ec_{Tp}) + (G_cA_p) + (M_cS_p) + (D_cS_p)$
[безопасность на узле *C*]
ИЛИ
$(F_cT_p;\ {}_Fc_Ec_{Tp}) + (M_cA_p) + (D_cS_p)$
[безопасность на узле *E*]

III. Анонимность получателя

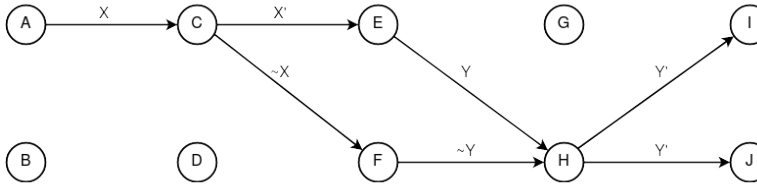

Рисунок 36. Применение конструктов «следование», «расщепление», «сведение» и «распространение», где *A* — отправитель запакованной информации *X*,*E* — получатель информации $X^{|}$,*C* — узел «расщепления»,*H* — узел «сведения»,*Y* — сгенерированный ответ

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

Алгебраическая модель

$$(S_c F_c S_p) + (D_c M_c A_p)$$

IV. Анонимность отправителя и получателя

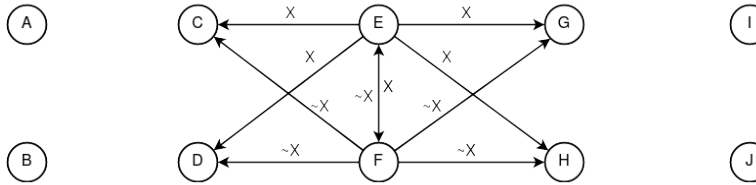

Рисунок 37. Применение конструктов «распространение» и «запутывание», где *E* — отправитель информации *X*,*F* — отправитель ложной информации *~X*

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

Алгебраическая модель

$$(D_c T_p;\ {}_D c_E c_{Tp}) + (M_c S_p)$$

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

4.5. МНОЖЕСТВЕННОЕ ШИФРОВАНИЕ

Если анализировать непосредственно саму полиморфную информацию в момент её маршрутизирующего перемещения по сети как этап наложенных итераций шифрования, то можно наблюдать точно заданную тенденцию, при которой размер информации будет стремиться к собственному уменьшению. Связано это с тем фактом, что подобная информация инициализируется на отправляющей стороне и постепенно финализируется на пути к принимающей. Такая закономерность способна выявлять роль субъектов информации, при которой достаточно проанализировать лишь размер информации с позиции двух отправлений $(A \rightarrow B) \rightarrow (B \rightarrow C)$, и если информация в таком случае уменьшается на заведомо известную величину D[1], то это свидетельствует о крайне высокой вероятности, что сам узел B является только промежуточным получателем. Чтобы решить данную

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

проблему, необходимо рассматривать структуру информации со стороны её размерности. Так, например, если сообщение размером $S(P)$ создаётся на отправителе и сразу же шифруется всеми слоями размером равным $S(E)$, то результатом такой функции является размер полиморфной информации $S(P) + S(E) = S(E(P))$. При этом т. к. $S(E)$ предполагает собой все слои шифрования, то данный размер можно представить в виде суммы каждого отдельного шифрования, где $S(E) = \Sigma S(E_i) = S(E_1) + S(E_2) + \ldots + S(E_n) \rightarrow S(E_n(\ldots(E_2(E_1(P)))\ldots)) = S(E(P))$. При этом каждый отдельный слой шифрования $S(E_i)$ равен любому другому слою $S(E_j)$, что даёт тождество вида $S(E_1) + S(E_2) + \ldots + S(E_n) = nS(E_1) = S(E)$. 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 $S(V_i \parallel E_i) \neq S(V_j \parallel E_j)$ и к невозможности представления размера $S(V \parallel E)$ через выражение $nS(V_1 \parallel E_1)$.

Хоть на данном этапе и невозможно определить число D, т. к. оно уже становится случайным, исходя из выражения $S(V_i \parallel E_i)$, тем не менее стремление полиморфной информации к своему собственному разложению остаётся, а это говорит, что остаётся возможным вероятностный анализ его размерности. Также, если идти от обратного и предположить, что существует отправление вида $(A \rightarrow B) \rightarrow (B \rightarrow C)$ и при этом первая информация оказывается меньше последующей, то данный факт говорит

$D = S(E(P)) - S(P)$, *где*

S — функция вычисления размера информации,

E — функция шифрования информации,

P — первоначальная информация.

только о том, что вторая информация является самостоятельно сгенерированной и считается либо запросом, либо ответом, а узел *B* либо отправителем, либо получателем. Одним из решений данной проблемы может являться создание отдельного поля в отправляемой информации, указывающего на следующего получателя (будь то истинного или промежуточного) с той лишь целью, чтобы маршрутизатор мог дополнять информацию на некую величину размера M[1], приводящую к константному размеру K[2] [29, с. 6]. Данный способ удаляет вышеописанные проблемы полностью, но выдаёт промежуточным узлам дополнительную информацию о последующих получателях информации, одним из которых станет истинный получатель. Критичный характер данной проблемы приведёт к негэнтропии, автоматической деградации скрытой системы, где будет существовать

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

$M_n = \Sigma\ S\ (V_i \parallel E_i)$, *где*
$S\ (V_i)$ — размер случайной информации для каждого слоя шифрования,
$S\ (E_i)$ — размер отдельного слоя шифрования,
n — количество удалённых слоёв шифрования.

———

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

$K_j = S\ (P) + \Sigma\ S\ (V_i \parallel E_i) + M_{j-1}$, *где*
j — стадия полиморфной информации,
n — количество слоёв шифрования.

возможность формирования списка потенциальных получателей на основе ограничения диапазона множества узлов всей сети и приводящий к зарождению выходных нод, определённо знающих (или вероятностно распознающих) истинных получателей.

Ещё одним и более радикальным способом решения проблемы является использование случайной величины R[1] вместо константной величины K. В то время как сама уязвимость и проблема образуется и воссоздаётся из детерминированности полиморфизма, то и константная величина *K,* порождённая ей же, не способна в корне предотвращать схожие проблемы. На место величины K встаёт величина R, приводящая к хаотичности размерности информации, к диффузии детерминированных качеств и к неопределённому выявлению субъектов информации. Такой подход базируется на необходимости генерации вероятностной псевдоинформации случайного и большего размера (чем истинная) на маршрутизирующей или принимающей стороне. Таким образом, промежуточный/принимающий узел начинает становиться одновременно и псевдополучателем для всех остальных участников сети.

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

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

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

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

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

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

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

Ложно, т. к. маршрутизатор может сгенерировать псевдоинформацию большего размера.

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

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

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

В результате всего вышеописанного нельзя однозначно ответить, что какое-то решение является наилучшим при использовании в анонимных сетях. В некоторых случаях становится невозможным использование константной величины K, как пример, в анонимизации сетевого трафика при соблюдении критериев ненаблюдаемости. В большинстве других случаев становится проблематичным правильное использование случайной величины R, т. к. сложность реализации будет приводить ко множеству «подводных камней» и, как следствие, к более затруднительному анализу безопасности итоговых систем.

Ещё одним ответом на данный вопрос может становиться создание анонимных сетей либо с отсутствующим полиморфизмом информации, либо с отсутствующим множественным шифрованием как частным случаем полиморфизма информации. Взамен отсутствия полиморфизма, будь то в общем случае или только в его частной реализации, будет теряться множество прикладных применений.

5. ЗАКЛЮЧЕНИЕ

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

5.1. ОСНОВНЫЕ ВЫВОДЫ

Ключевым аспектом данной работы стал анализ развития сетевых коммуникаций, сетевых архитектур и, как следствие, сетевой анонимности. Было дано определение анонимности и стадий её становления, каждая из которых формировалась посредством двух составляющих — мощности доверия и мощности анонимности. Было выявлено шесть основных стадий анонимности и две противоречивые формы базового вектора развития: первая^ и пятая^ стадии. Также было выявлено противоречие, при котором стремление к уменьшению мощности доверия становилось второстепенным свойством, как только достигался этап формирования анонимной сети. Решением проблемы стало объединение пятой стадии анонимности со стадией скрытой сети, тем самым образовав полные скрытые системы. Далее в работе были

приведены основные и составные конструкты (шаблоны) проектирования анонимных сетей с различными свойствами. Шаблоны проектирования, в совокупности с их свойствами, позволяют анализировать уровень анонимности и выстраивать за счёт этого модели будущих и текущих анонимных сетей. В качестве завершения раздела была приведена проблема использования полиморфизма информации в лице множественного шифрования как основного способа анонимизации трафика. Проблемой становилось изменение размера полиморфной информации при её маршрутизации от одного узла к другому. Было предложено несколько возможных способов исключения данной проблемы. У каждого способа были выявлены как положительные, так и отрицательные качества.

5.2. ТЕРМИНОЛОГИЯ DARKNET

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

В разных ситуациях данную сущность рассматривают то как анонимные сети, то как безопасные системы, а иногда и вовсе не анонимные и не безопасные, вбирая в себя множество противоречий в качестве размытия терминологий. Например, Darknet'ом могут называть friend-to-friend сети, рассчитанные на обмен файлами, RetroShare, GNUnet, FreeNet (клиент-безопасные) приложения, Tor, I2P (анонимные) сети, Proxy и VPN-сервисы (качество анонимности которых уступает скрытым сетям), социальные сети с уникально настроенным протоколом связи, TON (Telegram Open Network), что является криптовалютой и одной из вариаций представления Web3 (тогда Bitcoin и Ethereum должны также считаться Darknet-системами?), Telegram (централизованный сервис связи с возможной

и неоднозначной опцией сквозного шифрования, тогда WhatsApp также может стать Darknet'ом?), BitTorrent (протокол, не предоставляющий анонимность субъектов и конфиденциальность объектов) и т. п. Такой список можно продолжать и дополнять ещё десятками разнообразных технологий[1], поэтому из-за своей противоречивости в данной работе намеренно не использовался термин Darknet[2], чтобы не добавлять ещё одно возможное запутывающее значение к такому определению.

В литературе [48] указывается, что Darknet'ом можно назвать буквально всё что угодно, что связано так или иначе с фактом сокрытия информации либо личности от глобальных наблюдателей (будь то государства или монополистические корпорации) вне зависимости от способов достижения такого сокрытия. Данное суждение приводит одновременно к следующим противоречиям.

1. Если не ставится различий между неиндексируемыми запароленными страницами сайтов в сети Интернет и скрытой

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

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

сетью Tor, то это приводит к фактическому отрицанию анонимности Darknet за счёт второстепенности и незначимости её запутывающей маршрутизации (как главного критерия сетевой анонимности). Тем не менее в терминологии Darknet анонимность считается одной из базовых характеристик, присущих данной системе, что несомненно является противоречием.

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

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

Термин Darknet также подкрепляется и современными научными материалами, такими, как [49], [50], которые, в отличие от вышеописанных определений, всё же не настолько противо-

речивы, но непротиворечивы они лишь потому, что акцентируют внимание исключительно на частных случаях и не пытаются углубляться в структурный анализ рассматриваемых систем. Данные работы, как чаще всего бывает, приводят в качестве Darknet-составляющих Tor (и реже I2P) сети, которые были описаны и проанализированы в разных публикациях уже достаточное количество раз, из-за чего такие исследования становятся лишь дубликатами других.

Базовые же, фундаментальные работы в направлении анализа и разработки новых скрытых систем датировались в массе своей лишь 1980-2000-ми годами исследователями, из которых можно выделить Дэвида Чаума (DC-сети и Mix-сети) [29], [43], Андреаса Пфицмана и Марита Хансена (терминология анонимности) [51], Михаила Рейтера и Авиеля Рубина (системы измерения уровня анонимности) [52]. В настоящем же времени данные работы становятся забываемыми и включаются в источники лишь посредством других источников, где неявным образом создаются и реконструируются симулякры третьего порядка, интерпретирующиеся на базе выдвинутых тезисов из последующих производных исследований.

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

5.3. ПРОТИВОРЕЧИВОСТЬ WEB3

Всё вышеописанное исследование является в первую очередь анализом развития безопасных и анонимных систем, становление которых проходит через внутренние этапы противоречий на уровне их технического описания. Тем не менее, как было сказано в разделе «Введение», все системы не так просты, и их

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

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

иерархических коммуникаций. Экономическая целесообразность становится вполне разумной, потому как направляется на перманентное повышение своей отказоустойчивости и свойств заменяемости за счёт разделения и дублирования функций узлов системы. Тем не менее таковой исход приводит одновременно к двум противоречиям:

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

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

а долгосрочными — экономические, но в любом случае, какой бы исход централизация не выбрала, она самолично придёт к своему фатальному расщеплению.

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

Идея Web3[1] становится продолжением, эволюцией Web 1.0 и Web 2.0, которые, являясь централизованными системами, представляют разные методы управления содержанием. Так, на-

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

пример, сутью Web 1.0 являлось создание базовой информации (контента) на стороне самого сервиса. Иными словами, сам сервис и производил весь основной контент, а клиенты лишь были его потребителями. Концепция Web 2.0 сменила данный механизм посредством смешивания функций. Теперь клиенты могут не только вбирать в себя контент, но и создавать его, в то время как функциями сервиса становится лишь редактирование уже существующего содержания, как форма остаточных действий. Web3 исключает данный остаток, переводя все действия исключительно клиентской стороне. Существует два основных противоположных мнения насчёт концепции Web3 [53].

1. Термин Web3 представляет собой проект при котором пользователи вернут контроль над своими данными и генерируемым контентом, тем самым сделав децентрализацию доминируемой формой выражения сетевых коммуникаций над централизованной экономической составляющей. Более не будет монополистических корпораций, желающих на базе конфиденциальной информации, посредством её продажи, увеличивать свой капитал. Плюс к этому открываются рынки для обычных пользователей, способных обменивать свой контент на денежную составляющую без непосредственных централизованных посредников [54], [55].

2. Термин Web3 представляет собой просто маркетинговый ход, который играет на проекте децентрализованного будущего без корпораций и монополий. За счёт данной составляющей выгоду получают исключительно (или в большей мере) те, кто разрабатывает, спонсирует или инвестирует в подобные приложения. При этом экономическая составляющая Web3-технологий, на первых порах являющаяся либертарианской, будет постепенно стремиться по рыночным законам к концентрации капитала

речат друг другу.

и, как следствие, вновь к централизации всех возможных ресурсов (денежных, информационных, коммуникационных) [56]. Также предполагается, что таковой Web3 может быть крайне проблематичен и сомнителен в своих реализациях [57].

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

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

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

5.4. ИНТЕРНЕТ-«АНОНИМНОСТЬ»

В данной работе не был представлен период существования анонимности в сети Интернет до монополизации сетевых коммуникаций. На первый взгляд кажется, что такой период являлся бы интересным не только по причине более детального анализа исторических причин становления централизации, но и по причине «ретроспективы», в которую общество с периодической ностальгией углубляется, сравнивая прошлый и настоящий уровни централизации. Тем не менее такой промежуток времени является не более чем логическим продолжением становления централизации (хоть и наиболее запоминающимся вследствие своей массовости), начало которого было положено ещё переходом первой стадии анонимности ко второй посредством появления промежуточных узлов.

При зарождении и бурном развитии сети Интернет зарождался параллельным образом и симулякр третьего порядка как видимость существования анонимности. Это был чистый симулякр в том лишь простом смысле этого слова, что он не навязывался кем-либо извне в целях своих или чужих интересов, а был сформирован самим обществом лишь и только посредством своего незнания и своей наивности.

В данную эпоху царило массовое убеждение, что любое действие в сети Интернет является безнаказанным, будь то оскорбления или угрозы в чей-либо адрес, мошенничества, открытые высказывания своих политических убеждений и прочее. Симулякр казался реальностью, был даже в некоем роде гиперреальностью, потому как в действительности любые действия, даже противоправные и противозаконные, приводили только к пассивной агрессии и к отсутствию каких-либо принимаемых мер, даже со стороны государств и правоохранительных органов. Это было единственное время, когда анонимность, хоть и в своей форме видимости, являлась массовой.

Но симулякр анонимности никогда не был абсолютен в своём проявлении — он всегда выражался пропорцией к уровню

централизации, в которой масштабность симулякра определялась слабостью и неразвитостью самой централизации. Чем слабее была централизация, тем сильнее становилась видимость анонимности. Слабость централизации выражалась своей децентрализованностью как отсутствием монополизации в сфере сетевых коммуникаций. Иными словами, вся сеть Интернет в приведённое время состояла из множеств разрозненных централизованных сервисов между собой, но и в этот же самый период, в общих своих чертах, сеть всегда оставалась выражением второй стадии анонимности, то есть псевдоанонимностью.

С постоянным усилением централизации, как со стороны государств, так и со стороны компаний, с увеличением её масштабов посредством образования транснациональных корпораций, с образованием монопольных картелей, за счёт подавления конкуренции, с переходом коммуникаций от Web 1.0 к Web 2.0, при массовом производстве контента, закономерно исчезала, растворялась и уничтожалась видимость анонимности. Интернет становился всё более монолитным, всё более подконтрольным, а надвигающаяся реальность самим своим существованием безвозвратно сжигала и «втаптывала в грязь» наивные представления об анонимности.

Лишь и только посредством такого давления, посредством безжалостного искоренения видимости начинали зарождаться действительно анонимные коммуникации, но уже не как общее явление и движение всего множества сетевых коммуникаций, а как придаток, остаток такого множества, обуславливаемый исторически закономерным развитием.

СПИСОК ЛИТЕРАТУРЫ

1. Кан, Д. Взломщики кодов / Д. Кан. — М.: ЗАО Изд-во Центрполиграф, 2000. — 473 с.

2. Сингх, С. Тайная история шифров и их расшифровки / С. Сингх. — М.: АСТ: Астрель, 2009. — 447 с.

3. Граймс, Р. Апокалипсис криптографии / Р. Граймс. — М.: ДМК Пресс, 2020. — 290 с.

4. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. — СПб.: Питер, 2017. — 960 с.

5. Попова, А. Интернет как сетевая или иерархическая структура: концепция сети в постмодернистской философии и социальных науках конца XX-го и начала XXI-го вв. [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/internet-kak-setevaya-ili-ierarhicheskaya-struktura-kontseptsiya-seti-v-postmodernistskoy-filosofii-i-sotsialnyh-naukah-kontsa-xx-go-i (дата обращения: 02.01.2022).

6. Бодрийяр, Ж. Символический обмен и смерть / Ж. Бодрийяр. — М.: РИПОЛ классик, 2021. — 512 с.

7. Шнайер, Б. Beyond Security Theater [Электронный ресурс]. — Режим доступа: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html (дата обращения: 16.03.2022).

8. Меньшиков, Я., Беляев, Д. Утрата анонимности в век развития цифровых технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/utrata-anonimnosti-v-vek-razvitiya-tsifrovyh-tehnologiy (дата обращения: 04.01.2022).

9. Молчанов, А. Парадокс анонимности в Интернете и проблемы ее правового регулирования [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/paradoks-anonimnosti-v-internete-i-problemy-ee-pravovogo-regulirovaniya (дата обращения: 12.07.2022).

10. Симаков, А. Анонимность в глобальных сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/anonimnost-v-globalnyh-setyah (дата обращения: 04.01.2022).

11. Рабинович, Е., Шестаков, А. Способ управления трафиком в BitTorrent-сетях с помощью протокола DHT [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/sposob-upravleniya-trafikom-v-bittorrent-setyah-s-pomoschyu-protokola-dht (дата обращения: 26.09.2022).

12. Зденек, Ш. Международная реакция на действия Эдварда Сноудена [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/mezhdunarodnaya-reaktsiya-na-deystviya-edvarda-snoudena (дата обращения: 26.09.2022).

13. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. — СПб.: Питер, 2003. — 368 с.

14. Спраул, М. Антимонопольная практика и цены [Электронный ресурс]. — Режим доступа: https://prompolit.ru/files/560276/sproul.pdf (дата обращения: 26.09.2022).

15. Иванов, А. Мифы о легальной монополии, или Сказ о том, почему в России не развиваются инновации при упорной охране интеллектуальной собственности [Электронный ресурс]. — Режим доступа: https://www.hse.ru/data/2020/03/16/1565183163/086-102_иванов.pdf (дата обращения: 26.09.2022).

16. Смыгин, К. Тайные сговоры, повышение цен, рост безработицы и другие риски, которые таят в себе монополии. Ключевые идеи из бестселлера «Миф о капитализме» [Электронный ресурс]. — Режим доступа: https://rb.ru/opinion/mif-o-kapitalizme/?ysclid=l8ii06vu6s628640881 (дата обращения: 26.09.2022).

17. 5-5-3-5: проще штрафы платить, чем ИБ внедрять [Электронный ресурс]. — Режим доступа: https://habr.com/ru/company/dsec/blog/677204/?ysclid=l8iii2g114542316743 (дата обращения: 26.09.2022).

18. Иванович, Я. Может ли быть «монополия без монополиста»? [Электронный ресурс]. — Режим доступа: https://

cyberleninka.ru/article/n/mozhet-li-byt-monopoliya-bez-monopolista (дата обращения: 26.09.2022).

19. Анохин, Ю., Янгаева, М. К вопросу о MITM-атаке как способе совершения преступлений в сфере компьютерной информации [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-mitm-atake-kak-sposobe-soversheniya-prestupleniy-v-sfere-kompyuternoy-informatsii (дата обращения: 04.01.2022).

20. Молоков, В. К вопросу о безопасном шифровании в интернет-мессенджерах [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/k-voprosu-o-bezopasnom-shifrovanii-v-internet-messendzherah (дата обращения: 04.01.2022).

21. Вишневская, Ю, Коваленко, М. Анализ способов и методов незаконного распространения личных данных пользователей мессенджеров, социальных сетей и поисковых систем [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/analiz-sposobov-i-metodov-nezakonnogo-rasprostraneniya-lichnyh-dannyh-polzovateley-messendzherov-sotsialnyh-setey-i-poiskovyh-sistem (дата обращения: 30.12.2021).

22. Diffie, W., Hellman, M. New Directions in Cryptography [Электронный ресурс]. — Режим доступа: https://ee.stanford.edu/~hellman/publications/24.pdf (дата обращения: 19.12.2020).

23. Шнайер, Б., Фергюсон, Н. Практическая криптография / Б. Шнайер, Н. Фергюсон. — М.: Издательский дом «Вильямс, 2005. — 420 с.

24. Мавринская, Т., Лошкарёв, А., Чуракова, Е. Обезличивание персональных данных и технологии «Больших данных» (bigdata) [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/obezlichivanie-personalnyh-dannyh-i-tehnologii-bolshih-dannyh-bigdata (дата обращения: 13.07.2023).

25. Соснин, М. Реализация оптимальной архитектуры и обеспечение безопасного функционирования сети ЭВМ [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/

article/n/realizatsiya-optimalnoy-arhitektury-i-obespechenie-bezopasnogo-funktsionirovaniya-seti-evm (дата обращения: 26.09.2022).

26. Dwivedy, A. Secure File Sharing in Darknet [Электронный ресурс]. — Режим доступа: https://www.ijert.org/research/secure-file-sharing-in-darknet-IJERTV3IS10878.pdf (дата обращения: 06.11.2022).

27. Михайленко, Н., Мурадян, С., Вихляев, А. Актуальные вопросы мониторинга и противодействия киберугрозам в одноранговых сетях [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/aktualnye-voprosy-monitoringa-i-protivodeystviya-kiberugrozam-v-odnorangovyh-setyah (дата обращения: 26.09.2022).

28. 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).

29. Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms [Электронный ресурс]. — Режим доступа:https://www.lix.polytechnique.fr/~tomc/P2P/Papers/Theory/MIXes.pdf (дата обращения: 16.08.2022).

30. 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).

31. NETSUKUKU RFC документация [Электронный ресурс]. — Режим доступа: http://netsukuku.freaknet.org/sourcedocs/main_doc/ntk_rfc/ (дата обращения: 31.12.2021).

32. Danezis, G., Diaz, C., Syverson, P. Systems for Anonymous Communication [Электронный ресурс]. — Режим доступа: https://www.esat.kuleuven.be/cosic/publications/article-1335.pdf (дата обращения: 27.09.2022).

33. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы и исходные коды на языке С / Б. Шнайер. — СпБ.: ООО «Альфа-книга», 2018. — 1040 с.

34. Шелухин, О., Канаев, С. Стеганография. Алгоритмы и программная реализация / О. Шелухин, С. Канаев. — М.: Горячая линия — Телеком, 2018. — 592 с.

35. Карпов, Д., Ибрагимова, З. Способы и средства обеспечения анонимности в глобальной сети Интернет [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/sposoby-i-sredstva-obespecheniya-anonimnosti-v-globalnoy-seti-internet (дата обращения: 15.07.2022).

36. Рябко, Е. Калейдоскоп vpn-технологий [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/kaleydoskop-vpn-tehnologiy (дата обращения: 02.01.2022).

37. 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).

38. 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).

39. 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).

40. 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).

41. 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).

42. Рябко, Б., Фионов, А. Криптография в информационном мире / Б. Рябко, А. Фионов. — М.: Горячая линия — Телеком, 2019. — 300 с.

43. Chaum, D. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability [Электронный ресурс]. — Режим доступа: https://www.cs.cornell.edu/people/egs/herbivore/dcnets.html (дата обращения: 24.07.2022).

44. Goel, S., Robson, M., Polte, M., Gun Sirer, E. Dissent in Numbers: Making Strong Anonymity Scale [Электронный ресурс]. — Режим доступа: https://dedis.cs.yale.edu/dissent/papers/osdi12.pdf (дата обращения: 24.07.2022).

45. Corrigan-Gibbs, H., Wolinsky, D., Ford, B. Proactively Accountable Anonymous Messaging in Verdict [Электронный ресурс]. — Режим доступа: https://dedis.cs.yale.edu/dissent/papers/verdict.pdf (дата обращения: 24.07.2022).

46. 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).

47. 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).

48. Бартлетт, Д., Подпольный интернет: темная сторона мировой паутины / Д. Бартлетт. — М.: Эксмо, 2017. — 352 с.

49. Бондаренко, Ю., Кизилов, Г. Проблемы выявления и использования следов преступлений, оставляемых в сети «Darknet» [Электронный ресурс]. — Режим доступа: https://cyberleninka.ru/article/n/problemy-vyyavleniya-i-ispolzovaniya-sledov-prestupleniy-ostavlyaemyh-v-seti-darknet (дата обращения: 20.10.2022).

50. Гонов, Ш., Милованов, А. Актуальные вопросы противодействия преступности в сети Даркнет [Электронный ресурс]. —

Режим доступа: https://cyberleninka.ru/article/n/aktualnye-voprosy-protivodeystviya-prestupnosti-v-seti-darknet (дата обращения: 20.10.2022).

51. Pfitzmann, A., Hansen, M. Anon Terminology [Электронный ресурс]. — Режим доступа: http://dud.inf.tu-dresden.de/Anon_Terminology.shtml (дата обращения: 20.10.2022).

52. Reiter, M., Rubin, A. Crowds: Anonimity for Web Transactions [Электронный ресурс]. — Режим доступа: https://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/crowds.pdf (дата обращения: 20.10.2022).

53. Взлетит или нет — две разные точки зрения на Web3 [Электронный ресурс]. — Режим доступа: https://habr.com/ru/company/vasexperts/blog/670964/ (дата обращения: 30.10.2022).

54. Dabit, N. What is Web3? The Decentralized Internet of the Future Explained [Электронный ресурс]. — Режим доступа: https://www.freecodecamp.org/news/what-is-web3/ (дата обращения: 30.10.2022).

55. Решетникова, М. Без владельцев и цензуры: каким будет интернет эпохи Web3 [Электронный ресурс]. — Режим доступа: https://trends.rbc.ru/trends/industry/629070a99a79470ec4bdb673 (дата обращения: 30.10.2022).

56. Ingram, D. What is web3? It's Silicon Valley's latest identity crisis [Электронный ресурс]. — Режим доступа: https://www.nbcnews.com/science/science-news/web3-s-silicon-valleys-latest-identity-crisis-rcna9846 (дата обращения: 30.10.2022).

57. Marklinkspike, M. My first impressions of Web3 [Электронный ресурс]. — Режим доступа: https://moxie.org/2022/01/07/web3-first-impressions.html (дата обращения: 30.10.2022).

Монолитный криптографический протокол

Аннотация. Монолитность протокола, определяемая в первую очередь его самодостаточностью, сводится также к его имманентности. Последнее свойство является уникальным качеством класса подобных протоколов, потому как содержит всю информацию внутри шифрованной оболочки. Чтобы иметь представление маршрута передаваемой информации, каждый субъект самолично пытается её расшифровать. Безуспешность расшифрования лишь свидетельствует о факте непричастности данного объекта к текущему субъекту получателю. Таким образом, на уровне протокола автоматически производится постоянная авторизация субъектов к хранимой либо передаваемой информации.

Ключевые слова: монолитный криптографический протокол; протокол Bitmessage; скрытые системы; программная реализация.

1. ВВЕДЕНИЕ

Ядром всех скрытых систем [1] являются криптографические протоколы. Наиболее приоритетными протоколами в конечном счёте становятся простые, легкочитаемые и легкореализуемые. В массе своей практические составляющие реального мира часто приводят к необходимости выбирать компромиссы между теоретической безопасностью и практической производительностью. Тем не менее существуют протоколы, стремящиеся к теоретической безопасности, но при этом не исключающие практическую производительность для малых групп участников. К такому виду протоколов может относиться монолитный криптографический протокол, являющийся одновременно наследником протокола Bitmessage [2] и классом его выражения. Главной особенностью протокола становится его самодостаточность [3, с. 80] и простота [3, с. 58], а также абстрактность, за счёт которой появляется возможность применять данный протокол в тайных каналах связи и во множестве анонимных сетей.

2. ОПРЕДЕЛЕНИЕ

Протокол определяется восьмью шагами, где три шага на стороне отправителя и пять шагов на стороне получателя. Для работы протокола необходимы алгоритмы КСГПСЧ (криптографически стойкого генератора псевдослучайных чисел), ЭЦП (электронной цифровой подписи), криптографической хеш-функции, установки/подтверждения работы, симметричного и асимметричного шифров.

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.

Монолитный криптографический протокол игнорирует способ получения публичного ключа от точки назначения, чтобы та-

ковой оставался встраиваемым и мог внедряться во множество систем, включая одноранговые сети, не имеющие центров сертификации, и тайные каналы связи, имеющие уже установленную сеть по умолчанию.

Протокол способен также 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 заменяться криптографическим слоем по способу обнаружения отправителя и получателя, как это показано на *Рисунках 2, 3*. Из вышеописанного также справедливо следует, что для построения полноценной коммуникационной системы необходимым является симулятивная замена транспортного и прикладного уровня последующими криптографическими абстракциями. Под транспортным уровнем может пониматься способ передачи сообщений из внешней (анонимной сети) во внутреннюю (локальную), под прикладным — взаимодействие со внутренними сервисами.

Сеанс связи в приведённом протоколе определяется самим пакетом, 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.

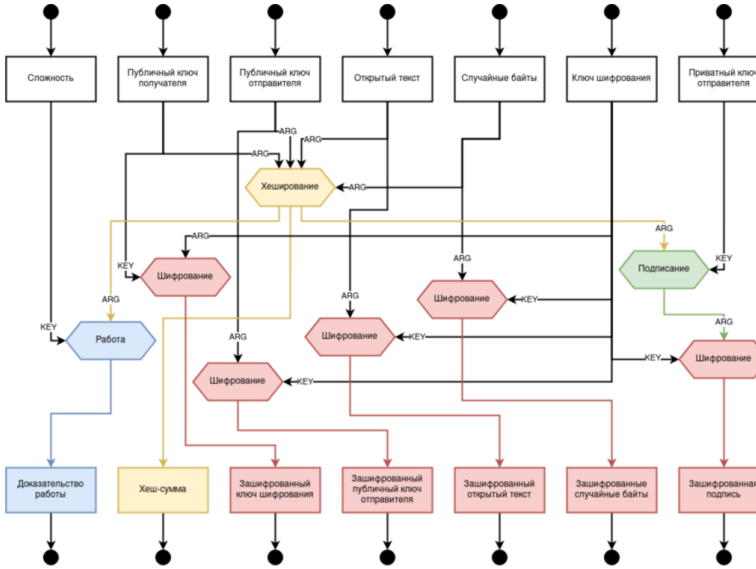

Рисунок 1. Схема монолитного криптографического протокола на инициирующей стороне

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.

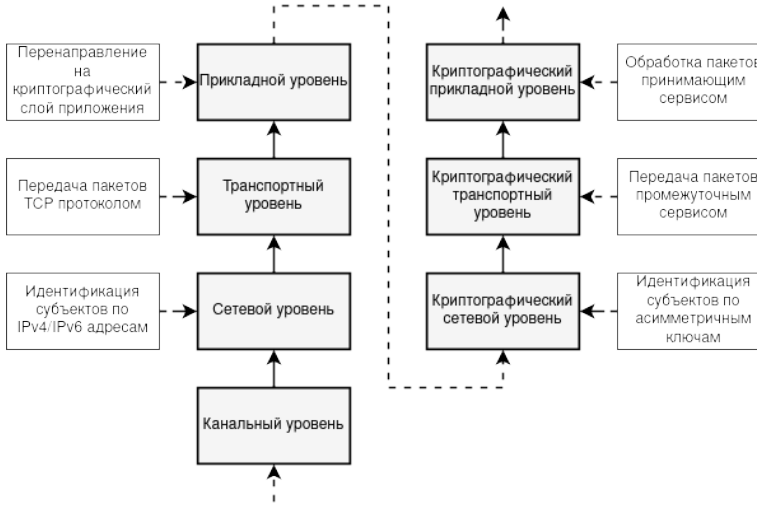

Рисунок 2. Расширение стека протоколов TCP/IP на базе криптографических абстракций

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.

Использование одной и той же пары асимметричных ключей для шифрования и подписания не является уязвимостью, если применяются разные алгоритмы кодирования [3, с. 257] или сама структура алгоритма представляет различные способы реализации. Так, например, при алгоритме RSA для шиф-

рования может использоваться алгоритм OAEP, а для подписания — PSS. В таком случае не возникает «подводных камней», связанных с возможным чередованием «шифрование-подписание». Тем не менее остаются риски, связанные с компрометацией единственной пары ключей, при которой злоумышленник сможет не только расшифровывать все получаемые сообщения, но и подписывать отправляемые [3, с. 99], [3, с. 291]. Но этот критерий также является и относительным плюсом, когда личность субъекта не раздваивается, и, как следствие, данный факт не приводит к запутанным ситуациям чистого отправления и скомпрометированного получения (и наоборот).

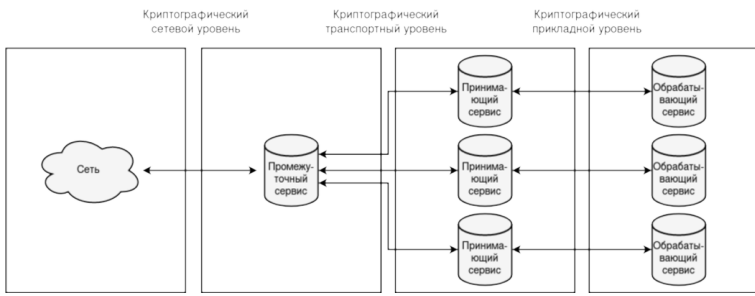

Рисунок 3. Расширенный стек протоколов на примере сервисов в анонимной сети

Протокол пригоден для многих задач, включая передачу сообщений, запросов, файлов, но не пригоден для передачи поточной информации, подобия аудиозвонков и видеотрансляций, из-за необходимости подписывать и подтверждать работу, на что может уходить продолжительное количество 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.

Недостатком протокола является отсутствие последовательности между несколькими пакетами. Иными словами, невозможно определить нумерацию, что в некой степени переводит часть полноценного протокола на логику приложения, как, например, передача файлов. Это, в свою очередь, обосновывается упрощением протокола, где не требуются хранилище или база данных для хранения последовательности пакетов со стороны каждого входящего объекта. Также в некоторых приложениях последовательность сообщений не критична, как, например, в электронной почте или мессенджерах, где необходим лишь сам факт уже существующего дубликата (данный момент можно проверять хешем пакета).

Другим недостатком является постоянное применение функции подписания, которая считается одной из наиболее ресурсозатратных, с практической точки зрения, операций. При большом количестве поступающих сообщений возникнет и необходимость в большом количестве проверок подписания. При этом использование MAC взамен ЭЦП является недопустимым, потому как таковая имитовставка создаст буквально поточную связь между субъектами информации (создаст дополнительные связи между субъектами и генерируемым объектом), усложнит протокол и может привести теоретически к более чем одному возможному вектору нападения на протокол.

Протокол можно также расширить и под широковещательную передачу сообщений, где необходимым действием будет являться шифрование одного и того же сеансового ключа пакета несколькими публичными ключами. В итоге для того, чтобы получить сообщение, получатель должен будет перебрать список зашифрованных экземпляров одного и того же ключа. Расшифровав один из множества ключей, конечный абонент сможет расшифровать и всё сообщение. Недостатком такого подхода является линейное увеличение основной нагрузки на попытки расшифрования сеансового ключа приватным.

Протокол не подвержен timing-атакам (по времени) [4] (не стоит путать данную атаку с timing-атаками по анализу

трафика в анонимных сетях), если таковой не участвует в генерации ответа при наступлении стадии прерывания действий принимающей стороной. Иначе, если будет постоянно генерироваться ответ определённым сервисом «принятия всех сообщений», тогда злоумышленник сможет собрать *N*-е количество пакетов из сети и постепенно отправлять их предполагаемому получателю с постоянным фиксированием времени. Если ответ будет генерироваться дольше среднего значения, то это будет означать повышенную вероятность того, что запрос был отправлен настоящему получателю. Различное время генерации ответа связано с расшифрованием сообщения на уровне протокола, где получатель своевременно проверяет корректность пакета, что может приводить к исключению действий 6, 7 и 8-го протокола. Предотвратить timing-атаку можно сохранением всех принимаемых хеш-значений на стороне сервиса, что приведёт к невозможности повторного использования пакета. Другим решением может являться выставление случайной или статичной задержки при ответе, если возможны случаи отключения определённых участников сети с целью их коммуникационного абстрагирования друг от друга.

Также протокол не подвержен атакам дополнения (padding oracle) [5] при использовании блочных симметричных алгоритмов с режимом шифрования CBC. Невозможность применения данной атаки сводится к вычислению хеш-функции по открытому сообщению. Если злоумышленник будет изменять побайтово данные, стремясь найти правильное значение в шифрованном блоке, таковое действие не будет иметь положительного результата до тех пор, пока все байты не приведут к аналогичному сопоставлению с хеш-значением. По этой причине злоумышленник самостоятельно не сможет выставлять и эффективно проверять корректность промежуточных значений по ответам принимающей стороны.

Протокол способен обеспечивать полиморфизм информации методом установки промежуточных получателей (маршрутизаторов) и созданием транспортировочных пакетов, пред-

ставленных 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. 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 псевдоадреса отправителя.

3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ

Монолитный криптографический протокол удобен в программной реализации за счёт своей абстрактности, при которой сами алгоритмы шифрования не имеют решающего значения. Таким образом, если один из алгоритмов окажется уязвимым — его можно будет заменить на другой, не изменяя при этом сам протокол.

Для улучшения эффективности, допустим при передаче файлов, 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*-й проверки. Таким образом, минимальный контроль работы будет осуществляться лишь *[M/nN] +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[1] [6] для шифрования информации:

```
import (
	"bytes"
)
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),
		},
	}
}
```

[1] Программная реализация протокола go-peer [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer (дата обращения: 20.03.2022).

Пример программного кода 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
}
```

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 пакета. Одним из возможных решений данной проблемы может служить использование общепринятого и стандартизированного протокола типа SSL/TLS с целью сокрытия факта использования монолитного протокола. Другим решением может стать создание отдельного слоя преобразования информации в котором вся сеть будет обладать дополнительным секретом — ключом сети, посредством которого будет происходить дальнейшая аутентификация и шифрование передаваемых сообщений.

4. ЗАКЛЮЧЕНИЕ

Монолитный криптографический протокол является наследником протокола Bitmessage, потому как скрывает внутри шифрованной оболочки сообщения не только маршрутизирующую информацию о её субъектах (отправителе и получателе), но также и всю возможную информацию (криптографическую соль, подписи, версии, расширения), которая так или иначе могла бы выдавать субъектов информации сторонними способами. Монолитный криптографический протокол одновременно является абстрактным, потому как для его функционирования алгоритмы кодирования, шифрования, подписания, хеширования и т. д. не играют решающей роли, и сложно расширяемым, потому как большинство возможных дополнений будет проходить лишь через его более прикладные уровни реализации, но не через модификацию самого протокола. Простота монолитного криптографического протокола становится наиболее выраженным свойством, порождающим его абстрактность, за счёт которой протокол обретает вид класса, соблюдающего основные характеристики монолитности — сокрытие идентификации внутри шифрованной оболочки сообщений.

СПИСОК ЛИТЕРАТУРЫ

1. Коваленко, Г. Теория строения скрытых систем [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer/blob/master/docs/hidden_systems.pdf (дата обращения: 04.01.2023).

2. 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).

3. Шнайер, Б., Фергюсон, Н. Практическая криптография / Б. Шнайер, Н. Фергюсон. — М.: Издательский дом «Вильямс», 2005. — 420 с.

4. Атака по времени — сказка или реальная угроза? [Электронный ресурс]. — Режим доступа: https://habr.com/ru/post/217327/ (дата обращения: 08.12.2022).

5. Heaton, R. The Padding Oracle Attack [Электронный ресурс]. — Режим доступа: https://robertheaton.com/2013/07/29/padding-oracle-attack/ (дата обращения: 08.12.2022).

6. Донован, А., Керниган, Б. Язык программирования Go / А. А. Донован, Б. У. Керниган. — М.: ООО «И. Д. Вильямс», 2018. — 432 с.

Абстрактные анонимные сети

Аннотация. Разработка абстрактных анонимных сетей, которым не важно расположение узлов, их количество, факт сокрытия IP-адресов и уровень централизованности системы, является новой и важной формой развития анонимизации трафика, которая позволяет внедряться в уже готовые замкнутые и враждебные коммуникационные среды, оставляя при этом теоретически доказуемую анонимность. Подобные системы способны быстро восстанавливаться при массовых блокировках за счёт простоты возобновления своей работоспособности от одной лишь сетевой единицы. Свойство невосприимчивости к централизации способно порождать приложения, защищающие конфиденциальную информацию пользователей и анонимность их действий даже в полностью подконтрольных средах.

Ключевые слова: абстрактные анонимные сети; тайные каналы связи; децентрализованные сети; модель на базе проблемы обедающих криптографов; модель на базе очередей; модель на базе увеличения энтропии; мощность спама;

1. ВВЕДЕНИЕ

Все анонимные сети базируются на двух идентифицирующих уровнях — сетевом и криптографическом. Сетевой уровень позволяет выстраивать маршрутизацию между узлами, более эффективно расходовать ресурсы частных ЭВМ и всей системы в целом. Криптографический уровень позволяет осуществлять анонимизацию субъектов посредством алгоритма запутывающей маршрутизации. Данный алгоритм часто становится связанным с сетевым уровнем непосредственно. Тем не менее существует класс анонимных сетей, запутывающая маршрутизация которых позволяет полноценно отделяться от сетевых протоколов. Сама сетевая связь в конечном итоге становится лишь придатком общих коммуникаций, где все базовые функции идентификации и маршрутизации вбирает в себя криптографический уровень. При таком сценарии становятся незначимы такие факторы, как расположение узлов в сети, сокрытие IP-адресов, число участников и уровень централизованности системы. Данным сетям становится неважна как таковая коммуникационная среда, вследствие чего их анонимность может быть распространена далее на тайные каналы связи, располагаемые в заведомо враждебных и замкнутых системах. Во всей работе вышеописанные системы будут именоваться абстрактными анонимными сетями.

Рисунок 1. Абстрактные анонимные сети являются подмножеством класса теоретически доказуемой анонимности

Абстрактные анонимные сети не могут не принадлежать сетям с теоретически доказуемой анонимностью [1]. Если взять обратное и предположить, что абстрактными могут быть скрытые сети без теоретически доказуемой анонимности, тогда они также должны уметь противостоять внешним и внутренним пассивным наблюдателям в замкнутом, незащищённом и враждебном окружении, как того предполагают тайные каналы связи. В таком пространстве внешний пассивный наблюдатель становится глобальным, а внутренний становится слиянием с глобальным, т. е. все функции отправления и получения информации будут проходить через единую централизованную структуру (если брать самый худший и более вероятный сценарий образования тайных каналов связи). Такие суждения приводят к воссозданию теоретически доказуемой анонимности и к явному противоречию существования абстрактных скрытых сетей без теоретически доказуемой анонимности.

2. АБСТРАКТНОСТЬ СЕТЕВЫХ КОММУНИКАЦИЙ

По умолчанию способ распространения всех абстрактных скрытых сетей сходится к связи «*все-ко-всем*», то есть когда каждый пользователь при генерации запроса отправляет свой пакет всем своим соединениям. Данное свойство связано с необходимостью минимального количества субъектов в системе для достижения анонимности с отсутствием противоречивости связей. Допустим, связь «*один-к-одному*» с двумя субъектами, заданная как (*A* ↔ *B*), также является и фактической связью «*все-ко-всем*» и «*все-к-одному*», что приводит к противоречивой определённости. Такая же ситуация с возможностью представления связей «*один-к-одному*» и «*все-к-одному*» при помощи трёх субъектов. Поэтому минимальной структурой представления сетевых коммуникаций является связь «*все-ко-всем*» с тремя участниками сети.

В общем виде существует всего три основных типа связей, как это представлено на *Рисунке 26*, в то время как все остальные соединения являются лишь их побочными гибридами.

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

Во-первых, стоит сказать, что все приведённые выше связи являются одноранговыми, в том числе и связь централизованная. Данные соединения рассматриваются в вакууме абстрактной сети, 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.

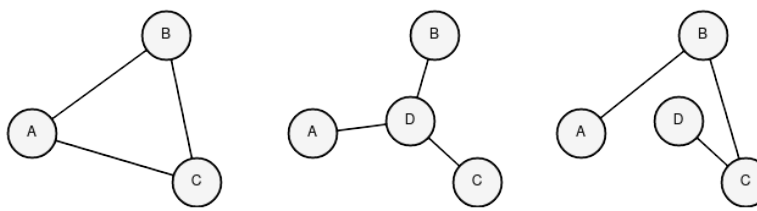

Рисунок 2. Связи: «*все-ко-всем»*, «*все-к-одному»*, «*один-к-одному»* (слева направо)

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.

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 абстрактной анонимной сети 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.

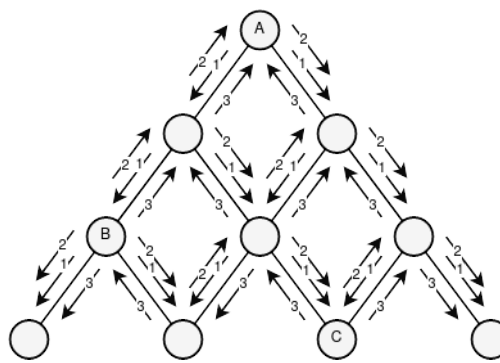

Рисунок 3. Маршрутизация пакета на базе абстрактной анонимной сети из 10 узлов, где *A* — отправитель,*B* — маршрутизатор,*C* — получатель

Если предположить, что субъект *D* не способен генерировать информацию, а создан исключительно 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 утверждено ранее, абстрактная сеть невосприимчива к такому виду деанонимизации. Следовательно, узел *D* становится словно фантомом, ретранслирующим субъектом, не влияющим на безопасность и анонимность сети, базируемой на связи *«все-к-одному»*. Из этого также следует, что абстрактная система 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 к связи «*один-ко-всем»*. Связь же «*все-ко-всем»* состоит из множества связующих *«один-ко-всем»* относительно каждого отдельного субъекта, коим и является узел *D*, а это в свою очередь приводит к классическому (ранее заданному) определению абстрактной анонимной сети. 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 итератив-

ности 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 которых 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 к связи «*все-к-одному»*, и как следствие, к связи *«все-ко-всем»*.

Таким образом, вне зависимости от типа соединений, абстрактная скрытая сеть будет оставаться безопасной даже при условии существования единственного сингулярного сервера, связывающего всех клиентов между собой. Простота построения централизованной системы в абстрактной анонимной сети приводит противоречиво к выражению истинной отказоустойчивости, а также к живучести подобных коммуникаций, регенерирующих лишь от одной сетевой единицы. Данное свойство в большей мере отличает абстрактные анонимные сети от всех других скрытых сетей.

3. ПРИМЕРЫ АБСТРАКТНЫХ АНОНИМНЫХ СЕТЕЙ

Одним из возможных способов (как шагов) построения таковых систем является необходимость в доказуемой устойчивости системы по отношению хотя бы к одному из наблюдателей, будь то внешнему или внутреннему. При этом в качестве внешнего берётся наивысшая форма в лице глобального наблюдателя, а в качестве внутреннего берутся узлы, заполняющие всю сеть с определённой минимальной условностью по количеству не связанных между собой узлов.

Простота системы является также важным качеством теоретически доказуемой анонимности. Если система будет иметь массу условностей, то даже при теоретической её доказуемости практическая реализация может составить огромное количество трудностей, ошибок или неправильных использований, что приведёт к фактической дискредитации самой теории, и таковая анонимность в конечном счёте останется лишь теоретической.

3.1. МОДЕЛЬ НА БАЗЕ ОЧЕРЕДЕЙ

Одной из самых простых возможных реализаций абстрактной системы является использование очередей генерации пакетов в сети. Для начала предположим, что необходимо защититься от внешнего глобального наблюдателя. Также предположим, что существует три узла в сети {*A, B, C*}, где один из них отправитель информации, а другой — получатель. Целью атакующего становится сопоставление факта отправления с инициатором и/или получения с сервисом связи (получателем). В идеальной системе (теоретически доказуемой) вероятность обнаружения правильного запроса составит 1/3. Ровно такая же картина должна

быть с фактом ответа на запрос. В сумме при трёх участниках и при условии ИЛИ факт обнаружения должен быть равен 2/3 (не имеет значения, запрос это или ответ). При существовании *N* узлов, не связанных между собой общими целями и интересами, вероятность становится равной 2/N. Итоговая система должна удовлетворять данным свойствам.

Предположим далее, что необходимо защититься от *q*-го количества внутренних наблюдателей системы из количества *q*+| {*A, B, C*} | узлов, где известно, что узел *C* — не связанный в сговоре маршрутизатор для одного из узлов *A* или *B*. Если внутренний наблюдатель становится пассивным, то спектр его действий ограничивается внешним наблюдением с *q*-м охватом сети, при условии, что пакет не выдаёт никакой информации об отправителе или получателе. Таким образом, в данном контексте необходимым является рассмотрение активных внутренних нападений, где субъект-атакующий становится способным генерировать самостоятельно пакеты и быть отправителем информации к определённой точке назначения. Целью атакующего становится сопоставление факта отправления ответа из множества {*A, B*} с конкретным его элементом. В идеальной системе (теоретически доказуемой) вероятность обнаружения правильного ответа составит 1/2. При существовании *N* узлов, не связанных между собой общими целями и интересами, вероятность становится равной 1/N. Итоговая система должна удовлетворять данным свойствам.

Если предположить, что существует сговор пассивного внешнего и активного внутреннего наблюдателей, то условие и цель атакующих полностью становится аналогична цели внутреннего наблюдателя, где в идеальной системе (теоретически доказуемой) ровно так же вероятность обнаружения ответа должна составить 1/2. При существовании *N* узлов, не связанных между собой общими целями и интересами, вероятность должна становиться равной 1/N. Итоговая система должна удовлетворять данным свойствам.

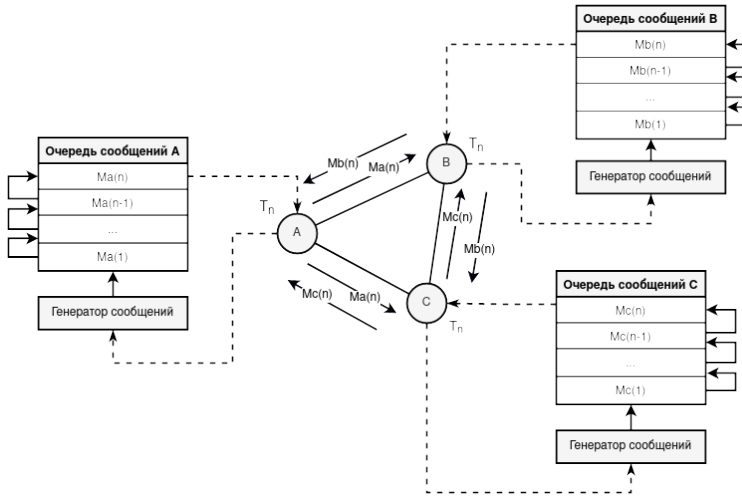

Рисунок 4. Схема абстрактной анонимной сети на базе очередей со стороны внешнего глобального наблюдателя

Работа системы на базе очередей может сводиться к следующему протоколу на основе 10 пунктов, которые полностью (за исключением сговора активных наблюдателей) обеспечивают замкнутость и безопасность системы:

1. Каждый субъект сети должен выстроить период генерации пакета равный T_n, где $n \in Q$, n — статичная величина периода. Иначе становится эффективна атака со стороны внутреннего наблюдателя. Несогласованность константного числа T_n с другими участниками сети приведёт к возможности разграничения субъектов по подмножествам с разными периодами генераций.

2. Каждый субъект сети выстраивает период равный T_n полностью локально, без кооперирования с другими субъектами сети. Это условие является лишь упрощением системы, само кооперирование или его отсутствие не приведёт к нарушению

протокола, потому как предполагается, что сама генерация пакетов, а конкретно — время начала генерации, не является секретом.

3. Каждый действующий субъект сети выставляет минимум одного существующего пользователя в роли маршрутизирующего узла для поддержания анонимности. Причисление маршрутизатора в сговор атакующих приведёт к деанонимизации субъектов, использующих данного промежуточного участника. Поэтому в практическом применении для снижения рисков, связанных с деанонимизацией субъектов посредством контроля ретранслятора, необходимо выбирать сразу несколько маршрутизирующих узлов, формируя тем самым цепочку нод и повышая мощность анонимности.

4. Каждый действующий субъект сети знает период и время генерации нового пакета на маршрутизирующем узле. Такое условие необходимо для предотвращения атак, направленных на нестабильные системы (как будет показано далее), с учётом существующего сговора внешних и внутренних наблюдателей.

5. Каждое сообщение зашифровывается монолитным криптографическим протоколом [2] с множественным туннелированием и проходит сквозь маршрутизирующие узлы. Такое свойство приведёт к сильному разрыву связей между объектом и его субъектами, а также между идентификацией сетевой и криптографической.

6. Каждый субъект хранит все свои сообщения, готовые к отправлению по сети, в очереди. Помимо очереди субъект должен содержать автодополняющийся пул ложных сообщений. Данное свойство необходимо для пункта 7.

7. Если на момент T_{ni} очередь пуста, где $i \in N$, i — номер периода, то есть не существует ни запроса, ни ответа, ни маршру-

тизации, то отправляется сообщение из пула ложных сообщений. При таком случае данное сообщение фактически никто не получает.

8. Если приходит сообщение, представляющее собой маршрутизацию, то оно ложится в очередь и при наступлении локального времени T_{ni} отправляется по сети. Пункт 5 обеспечивает несвязность объекта с его субъектами, поэтому при получении сообщения-маршрутизации промежуточный принимающий узел увидит только факт маршрутизации.

9. При необходимости отправить запрос субъект сначала анализирует текущее время с периодом маршрутизатора с целью отправить сообщение на второй итерации периода маршрутизирующего узла. Если ещё не прошла собственная итерация периода, то перед запросом в очередь вставляется ложное сообщение, данный запрос отправляется по сети. Пункт 3 обеспечивает несвязность идентификации сетевой и криптографической, что не даёт отправителю никакой информации о получателе, кроме его публичного ключа.

10. При необходимости отправить ответ субъект сначала анализирует текущее время с периодом маршрутизатора с целью отправить сообщение на второй итерации периода маршрутизирующего узла. Если ещё не прошла собственная итерация периода, то перед ответом в очередь вставляется ложное сообщение, данный ответ отправляется по сети. Пункт 3 обеспечивает несвязность идентификации сетевой и криптографической, что не даёт получателю никакой информации об отправителе, кроме его публичного ключа.

Явным недостатком данной архитектуры становится подверженность атакам отказа в обслуживании (DDoS), как для конкретного субъекта, перегружая его очередь сообщениями, так и для всей сети. Связано это с тем, что в основе системы исполь-

зуются очереди, сохраняющие и накапливающие сообщения, а также слепая маршрутизация, порождающая наибольшую несвязанность объекта с его субъектами за счёт полного распространения информации по всем участникам сети.

В любом случае преднамеренные атаки на сеть с целью отказа в обслуживании можно предотвратить проверяемостью на принадлежность субъектов к периоду генерации сообщений, но при всё большем расширении сети сами её участники станут давлением и причиной ухудшения производительности. Причиной такого исхода становится линейная увеличивающаяся нагрузка на сеть *O (N)* прямо пропорционально количеству действующих узлов *N* в сети. Иными словами, каждый субъект должен будет обрабатывать в T_n период *N-1* пакетов, постоянно расшифровывая их, что и становится достаточно ресурсозатратной операцией.

Тем не менее в выстроенной системе становится достаточно легко доказать невозможность атаки со стороны внешнего наблюдателя, анализирующего дифференцность сети. Если каждый субъект соблюдает генерацию пакета по локальному периоду (даже гипотетически с разными значениями T_n), то становится невозможным установление факта отправления, получения, маршрутизации или ложной генерации, потому как наблюдатель в конечном счёте способен лишь видеть определённые шифрованные сообщения, генерируемые каждый промежуток времени равный T_n. Также если внешним наблюдателем будут блокироваться определённые субъекты информации без непосредственного кооперирования со внутренним атакующим, то кардинально данный подход ситуации не изменит.

Атака внутренних наблюдателей с приведённым выше условием является качественно более сложной и мощной (даже относительно большинства внутренних нападений на практике), потому как *q* субъектов контролируют всю сеть за исключением трёх субъектов, а следовательно атакующие фактически являются не только внутренними наблюдателями, но и в массе своей монолитным глобальным наблюдателем. В качестве упрощения

доведём нападения до теоретически возможной комбинации в отображении сговора внешних и внутренних наблюдателей. Аудит будет базироваться на 10-м пункте, когда субъекту должен сгенерироваться ответ на отправленный запрос. При анализе системы может встретиться два разных случая — частный (a), наиболее благоприятный в определении анонимности, и общий (b), дающий больший простор действий для нападающих.

Частный случай удобно рассматривать на примере основных подходов к деанонимизации и методов их предотвращения. Общий же случай более реален в настоящем мире, потому как частный неустойчив к отказам в обслуживании (если субъект переподключится, то изменится сдвиг периода) и требует из-за этого постоянного кооперирования субъектов между собой по времени (чтобы сама генерация информации была одновременной). Таковые условия поведения частного случая делают общий более приоритетным в анализе практической анонимности, потому как он становится «стабильным» за счёт невозможности своего дальнейшего ухудшения.

а) Частный случай. Предположим, что существует крайне стабильная система, при которой каждый узел из множества {*A, B, C*} выставил в один и тот же промежуток времени значение равное T_n без отставания по времени относительно всех остальных участников сети. Все участники генерируют запрос секунда в секунду каждые T_{ni} по периоду. Предположим, что $T_n = 3$, тогда генерацию можно представить в виде *Таблицы 1*.

	$T_{n1-2}=t_1$	$T_{n1-1}=t_2$	$T_{n1}=t_3$	$T_{n2-2}=t_4$	$T_{n2-1}=t_5$	$T_{n2}=t_6$	$T_{n3-2}=t_7$	$T_{n3-1}=t_8$	$T_{n3}=t_9$
A			+			+			+
B			+			+			+
C			+			+			+

Таблица 1. Стабильная система со множеством участников {*A, B, C*} и $T_n = 3$

Если отсутствует маршрутизация от субъекта *C*, то легко определимым становится вычисление истинного субъекта, генерирующего настоящее сообщение. И действительно, если существует сговор внутреннего и внешнего наблюдателей, то возможен сценарий, при котором внутренний наблюдатель в роли инициатора генерирует сообщение и отправляет его одному из участников {*A, B*}. Спустя период T_n (при условии, что у получателя не существует сообщений в очереди) инициатор получает ответ, предварительно сохраняя его шифрованную версию. Далее внутренний наблюдатель обращается к внешнему с шифрованной версией сообщения, тот в свою очередь по своим записям проверяет, где впервые был создан таковой пакет. Узел, на котором появилось впервые подобное сообщение, и является истинным субъектом информации в лице получателя.

Теперь предположим, что маршрутизация субъекта C существует. Если внутренний наблюдатель хочет раскрыть субъектов {*A, B*}, то можно предположить, что ему необходимо каким-либо образом обойти ретрансляцию субъекта *C*. Но исключение узла *C* из сети не является решением, потому как прекратится вся последующая связь с субъектом *A* или *B*. Другим способом раскрытия (и куда более продуктивным) является уже исключение одного субъекта из множества {*A, B*}, иными словами, блокировка участника сети на определённый период времени mT_n. Тогда в таком случае активный внешний наблюдатель блокирует одного из субъектов {*A, B*}, после этого активный внутренний наблюдатель посылает запрос на одного из субъектов множества {*A, B*}. Если отправитель получает ответ, значит истинным получателем информации является не исключённый участник, в противном случае — исключённый.

Для предотвращения активных атак со стороны сговора внешних и внутренних наблюдателей необходимо добавить дополнительный (но не единственно возможный) 11_1 пункт, который представляет новую псевдороль субъектов в качестве контролирующих узлов. Такая атака приводит к невозможности деанонимизации субъектов посредством частичного блокирова-

ния, потому как её следствием станет взаимоблокировка субъектов. Тем не менее добавление данного пункта скажется на том, что сама сеть выйдет из класса абстрактных анонимных сетей, потому как добавится необходимость в поточном распространении информации на базе прямых соединений.

11_1. Каждый действующий субъект сети выставляет минимум одного существующего пользователя в роли контролирующего узла для предотвращения от активных атак методом исключения участников системы. Суть такого пользователя в понимании его существования. Если связь с подобным субъектом будет разорвана, то все последующие действия автоматически прекращаются. Само соединение функционирует за пределами механизма очередей, что тем не менее не приводит к снижению уровня анонимности, потому как все субъекты начинают подчиняться этому правилу однонаправленно (в такой концепции не существует функций типа запрос/ответ, существуют только поточные уведомления своего присутствия).

Хоть теоретически сама атака становится невозможной, но в практическом смысле и в долгосрочном наблюдении она более чем реальна. Связано это с тем, что одноранговая архитектура как таковая приводит к постоянному и динамичному изменению связей между субъектами. Это в свою очередь может приводить к исключениям групп субъектов, связанных контролирующими узлами, потому как последние обязаны быть действующими и настоящими участниками системы, в отличие от маршрутизирующих узлов.

Ещё одним возможным решением вышеописанной проблемы может стать использование доверенных соединений между участниками сети. Такой подход ограничивает действия активных внутренних наблюдателей и за счёт данного свойства позволяет снизить риски деанонимизации, а также сохранить абстрактность системы (по сравнению с пунктом 11_1).

11_2. Каждый действующий субъект сети выстраивает связи с другими участниками, основываясь на субъективности к уровню доверия, устанавливая и редактируя белый список на своей стороне. Чтобы успешно подключиться к сети такого рода, субъекту необходимо стать доверенным узлом, то есть пользователем, которому кто-либо доверяет. Сложность исполнения атаки на подобную сеть будет сводиться к сложности встраивания подчиняемых узлов, потому как каждый получатель информации в конечном итоге должен будет заранее устанавливать список возможных отправителей.

Сети с таким свойством именуются friend-to-friend (F2F) сетями [3]. Естественным недостатком является малая экспансия как возможность масштабирования системы. С другой стороны, как раз такое качество позволяет дополнительно (и довольно эффективно) сдерживать недостатки самой структуры, когда увеличивающееся количество субъектов приводит линейно к регрессу производительности системы. В общем представлении такой метод защиты достаточно эффективен против внутренних активных наблюдателей (особенно с практической точки зрения), но теоретически является более сложной моделью. Анонимность такого случая начинает базироваться на гипотетически большем количестве связей между участниками, чем при выстраивании константно заданного количества маршрутизирующих узлов, что и приводит к дополнительным рискам деанонимизации субъектов.

Также ещё одним возможным решением может стать синтез подходов, что закономерно объединит не только положительные, но и отрицательные стороны этапов 11_1 и 11_2. Вследствие такого соединения система перестанет быть абстрактной (за счёт необходимости в поточном поддержании соединений), появится свойство малой экспансии (за счёт принадлежности к F2F-сети) и увеличится сложность практической реализации (за счёт, соответственно, синтеза двух подходов). Тем не менее теоретическая безопасность выйдет на более высокий уровень,

потому как если один из доверенных субъектов станет скомпрометированным, то останется дополнительный слой защиты в лице маршрутизаторов, и наоборот.

b) Общий случай. Предположим, что существует нестабильная система, при которой каждый узел из множества {*A, B, C*} выставил в разный промежуток времени значение равное T_n с отставанием по времени относительно всех остальных участников сети. Все участники генерируют запрос в разные секунды, но также сохраняя локальный период равный T_n. Предположим, что $T_n = 3$, тогда генерацию можно представить в виде *Таблиц 2, 3, 4* относительно расположения субъекта *C* к другим участникам.

	$T_{n\text{-}2}=t_1$	$T_{n\text{-}1}=t_2$	$T_{n1}=t_3$	$T_{n2\text{-}2}=t_4$	$T_{n2\text{-}1}=t_5$	$T_{n2}=t_6$	$T_{n3\text{-}2}=t_7$	$T_{n3\text{-}1}=t_8$	$T_{n3}=t_9$
A		+			+			+	
B			+			+			+
C	+			+			+		

Таблица 2. Нестабильная система со множеством участников {*A, B, C*} и $T_n = 3$, где узел *C* находится в начале генерации

	$T_{n\text{-}2}=t_1$	$T_{n\text{-}1}=t_2$	$T_{n1}=t_3$	$T_{n2\text{-}2}=t_4$	$T_{n2\text{-}1}=t_5$	$T_{n2}=t_6$	$T_{n3\text{-}2}=t_7$	$T_{n3\text{-}1}=t_8$	$T_{n3}=t_9$
A	+			+			+		
B			+			+			+
C		+			+			+	

Таблица 3. Нестабильная система со множеством участников {*A, B, C*} и $T_n = 3$, где узел *C* находится в середине генерации

	$T_{n\text{-}2}=t_1$	$T_{n\text{-}1}=t_2$	$T_{n1}=t_3$	$T_{n2\text{-}2}=t_4$	$T_{n2\text{-}1}=t_5$	$T_{n2}=t_6$	$T_{n3\text{-}2}=t_7$	$T_{n3\text{-}1}=t_8$	$T_{n3}=t_9$
A		+			+			+	
B	+			+			+		
C			+			+			+

Таблица 4. Нестабильная система со множеством участников {*A, B, C*} и $T_n = 3$, где узел *C* находится в конце генерации

В качестве упрощения и абстрагирования предположим, что ни для какого субъекта не существует контролирующего участника или F2F-соединений, а следовательно и пунктов 11_1 и 11_2 как таковых. Существуют только субъекты {*A, B*}, один из которых является настоящим получателем, и постоянный маршрутизатор *C*. Основной целью анонимизации в нестабильных коммуникациях становится сведение действий субъекта *A* к аналогичным действиям субъекта *B*, и наоборот, посредством маршрутизатора *C*. Действительно, если *C* станет замыкающим узлом в момент времени T_{ni} при ответе любого субъекта множества *X*, то возникнет максимальная неопределённость равная $1/|X|$.

Анализируя сетевые коммуникации в нестабильных системах внешний наблюдатель способен сопоставлять для каждого субъекта его период равный T_n и сдвиг относительно определённого субъекта. В сговоре со внутренним наблюдателем появляется возможность деанонимизации субъекта на базе приведённого сдвига. Предположим, что игнорируется условие пунктов 9 и 10 с необходимостью генерировать пустое сообщение на основе периодов маршрутизирующего узла. Далее, пусть существует сеть на базе *Таблицы 2*, где внутренний наблюдатель располагает всеми сведениями, полученными от внешнего атакующего, и на основе этого генерирует сообщение в момент времени T_{n1} и отправляет его по сети. Если будет получен ответ в момент $T_{n1+1} = T_{n2-2}$ от маршрутизатора *C*, то это говорит только о том, что получателем сообщения является участник *B*, потому как субъект *A* становится способным выдать ответ маршрутизирующему узлу только в период $T_{n1+2} = T_{n2-1}$ по причине его умышленного пропуска в момент T_{n1-1} атакующей стороной. Такой вид атаки приводит к полной деанонимизации субъектов.

Предотвращением атаки является отправление истинного пакета на вторую итерацию периода маршрутизирующей стороны (относительно текущего времени). Теперь репродуцируем вышеописанную атаку на систему с таким условием. Также предположим, что сетью является система на базе *Таблицы 2*. Если

атакующий сгенерирует сообщение в момент времени T_{n1}, то получит ответ только в момент T_{n3-2}. Получателем в такой системе может оказаться любой из множества {*A, B*}, потому как ответ может быть отправлен как в момент времени T_{n2-1} (субъект *A*), так и в T_{n2} (субъект *B*). Чтобы субъект *B* отправил ответ именно в T_{n2}, то перед ним он помещает в очередь ложное сообщение, тем самым отодвигая отправление истинного сообщения по сети на одну итерацию. Аналогичные ситуации распространяются и на *Таблицы 3, 4*.

Таким образом, на основе всего вышеописанного наиболее сильной атакой является сговор внешних и внутренних активных атакующих, при которой необходимым условием противодействия становится либо существование постоянной поточной линии связи, что, в свою очередь, приводит к негации абстрактности и к невозможности применения данной системы в тайных каналах связи, либо принадлежность системы к классу F2F-сетей, что, в свою очередь, приведёт к малым возможностям экспансии.

В результате, если исходить из необходимости синтеза простоты и безопасности системы, то наилучшим вариантом становится выбор F2F-сетей. Это также способно привести к ещё бо́льшему упрощению структуры скрытой сети за счёт исключения полиморфизма информации как явления, то есть пункта 3, связанного с маршрутизацией посредством множественного шифрования. Такое действие приведёт к следующим выводам:

1. Исчезнет необходимость в промежуточных узлах и кооперировании с ними для установления периодов. Как следствие, не будет надобности в условностях отправления сообщений на конкретной итерации периода маршрутизирующего узла.

2. Исчезнет необходимость в использовании механизмов несвязываемости размеров сообщений при множественном шифровании [1].

3. Исчезнет необходимость в анализе частного и общего случаев, потому как таковые являются лишь следствием существования маршрутизирующих узлов и полиморфизма информации. И как следствие, пункт 3 заменится пунктом 11_2.

Вышеописанные действия переводят шестую стадию анонимности на противоречие пятой градации, аналогично первой^ стадии анонимности. И действительно, если происходит образование анонимной сети на базе пятой стадии анонимности, где перестаёт существовать полиморфизм информации, то подобная система должна будет вбирать основной критерий скрытых сетей, а именно — возможность создавать сервисы связи. Сервисы связи, выстроенные в анонимной сети, могут быть основаны на второй стадии, что приводит к увеличению $|T|$ мощности доверия. Это в свою очередь противоречит пятой стадии анонимности по причине её принадлежности к сервисам с теоретически минимальной мощностью доверия. Данный парадокс базируется на специфике запутывающего алгоритма, не принадлежащего классу полиморфной маршрутизации. Таким образом, данную стадию нельзя полноценно считать пятой стадией анонимности (по природе своего транслирования информации, а не хранения в роли сервиса связи) и шестой градацией (по причине отсутствия полиморфизма информации). По этой причине и вполне корректно можно считать данный этап пятой^ стадией анонимности, как это было выявлено и сделано ранее (в работе [1]) с первой^ стадией анонимности. Этим также доказывается не обязательная принадлежность скрытых сетей к последнему этапу анонимата при первом векторе развития анонимности (ориентированном на безопасность объектов), потому как запутывающим алгоритмом становится «очередь», скрывающая факт истинной передачи информации между субъектами, взамен комбинации «очередь+полиморфизм».

Теоретически основным отличием таковых подходов становятся иные векторы нападения, где при алгоритме «очередь»

атаки начинают принадлежать способам компрометации доверенных узлов, а при алгоритме «очередь+полиморфизм» — компрометациям маршрутизирующих узлов. В обоих случаях требуется сговор скомпрометированного узла с внешним глобальным наблюдателем. При удовлетворении условия нескомпрометированности ключевых субъектов, анонимность двух алгоритмов будет удерживаться на определённо заданном уровне.

Практически же основным отличием доверенной сети от маршрутизирующей становится существование прямой криптографической связи между отправителем и получателем, что приводит к фактически взаимной деанонимизации субъектов, при условии, что один из них становится скомпрометированным узлом. При увеличении участников сети, связанных между собой одной группой, возрастает соответственно и риск деанонимизации. Таким образом, в доверенных системах предполагается, что сами субъекты не защищаются и не скрывают свою идентификацию друг от друга. В то время как маршрутизирующие системы наоборот, с присущим им полиморфизмом информации, предполагают, что все субъекты, включая отправителя или получателя, могут быть атакующими, и следовательно сводят все свои векторы нападения на третью, незаинтересованную сторону.

Поэтому способы применения чистых F2F-сетей (без полиморфизма информации) становятся отличными от других анонимных сетей. Так, например, пятую^ стадию анонимности можно корректно применять лишь при условиях, когда все участники системы способны идентифицировать своих друзей как по сетевому критерию, так и по криптографическому, со знанием их взаимосвязей. Таковой критерий сужает способ применения подобных сетей, т. к. не позволяет применять их в системах, где требуется разграничение анонимности отправителя и получателя между собой.

Помимо прочего, если доверенный узел становится скомпрометированным, то у него появляется возможность узнать, общается ли собеседник ещё с кем-либо в определённый про-

межуток времени, просто отправляя запросы в его сторону. Если по прошествии T_n времени ответ не был получен, то это говорит о том, что в очереди получателя хранилось как минимум одно сообщение в данный промежуток времени, которое было настоящим запросом или ответом. Подключая внешнего активного глобального атакующего, можно достичь деанонимизации отправителя и получателя, если итеративно блокировать участников и постоянно проверять, занята ли очередь. Тем не менее такая атака может занять очень много времени, если у субъекта уже была загружена очередь сообщений, что в теории может достигать её константного пика, либо если он вставляет случайным образом в очередь «пустые» пакеты, что ещё сильнее может затруднять связность настоящего отправления либо получения. Также данную проблему можно искоренить внедрением поточного поддержания связи с одним или несколькими субъектами сети, приводящего к взаимоблокировке при отключении, но данное свойство автоматически исключит фактор абстрактности системы.

Также, из-за специфичности очередей, сети такого рода не могут выстраивать сильную концентрацию любых сервисов связи, потому как запрос-ответ со стороны разных субъектов становится единым последовательным действием, из-за чего становится невозможным эффективно создавать общий сервис на множество клиентов в один промежуток времени. Как пример, пятая^ стадия анонимности на базе очередей может эффективно быть применима при построении мессенджеров с неотслеживаемостью факта переписки (дополнительно с E2E-шифрованием), но не может использоваться при построении файловых сервисов, рассчитанных на множество клиентов. Если существует *N*-е количество субъектов, взаимодействующих с файловым сервисом в один промежуток времени, и каждый пытается скачать файл размером в *X*, то при размере пакета в *Y* (где *X*> *Y*) с конфигурационным периодом равным T_n все участники гарантированно смогут скачать данный файл только спустя $M = T_n N\ [X/Y]$. При увеличении *N*, конечная скорость ска-

чивания будет линейно регрессировать, при уменьшении T_n будет производиться большое количество спама, при котором стабильность работы узлов станет ухудшаться, при увеличении *Y* очередь будет содержать меньшее количество объектов для сохранения памяти устройства, тем самым приводя к игнорированию некоторого количества запросов от клиентов. Таким образом, эффективность использования пятой^ стадии анонимности на базе очередей зависит от конкретных типов задач.

3.2. МОДЕЛЬ НА БАЗЕ УВЕЛИЧЕНИЯ ЭНТРОПИИ

Другой абстрактной анонимной сетью может быть система на базе увеличения энтропии. Со стороны теоретического доказательства анонимности она более трудоёмкая и в некой степени более «хрупкая» (чем сеть на основе очередей), потому как большинство действий сводит к вероятностям конкретно выбранного субъекта, а не к действиям всей группы. Чтобы правильно доказать существование теоретической анонимности в таких условиях, необходимо рассматривать факт связывания субъектов между собой, анализируя при этом постоянный прирост энтропии.

Предположим, что существует всего три узла {*A, B, C*} и сама сеть работает по принципу вероятностного полиморфизма с множественным шифрованием, где каждый субъект может с вероятностью 1/2 выстроить маршрут с промежуточным узлом или без него соответственно. Предполагается, что вся генерируемая информация в такой системе принадлежит монолитному криптографическому протоколу [2], из чего следует, что транспортируемый пакет не хранит в открытом виде идентификацию абонентов. В конечном итоге будет образовано два разных и равновероятно возможных действия.

1. При полиморфизме информации будет существовать три этапа транспортирования информации: (*A* → *B ИЛИ A* → *C*) → (*B* → *C ИЛИ C* → *B*) → (*B* → *A ИЛИ C* → *A*)[1].

2. При отсутствии полиморфизма информации будет существовать всего два этапа транспортирования информации: (*A* → *B ИЛИ A* → *C*) → (*B* → *A ИЛИ C* → *A*).

В данном концепте временно предполагается, что системе известен лишь отправитель информации (инициатор), в то время как получатель не определён. Из вышеописанного также следует, что если полиморфизм будет являться статичной величиной (то есть будет всегда существовать или не существовать вовсе), то определение получателя станет лёгкой задачей по причине необходимости в генерации обязательного ответа инициатору.

Тем не менее если полиморфизм будет иметь вероятностную величину, то грань между отправлением и получением будет постоянно и постепенно стираться, сливаться, инвертироваться, что приведёт к неоднородному трактованию анализируемых действий: запрос (1) — ответ (1) — запрос (2) может стать равным запросу (1) — маршрутизации (1) — ответу (1). Но в таком случае возникает свойство гипертелии (сверхокончания), где запрос (2) не получает своего ответа (2), что снова приводит к возможности детерминированного определения субъектов на основании данного анализа.

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 минимальной константе *k = 2*, которую можно свести к следующему набору действий полиморфизма: (*A* → *B ИЛИ A* → *C*) → (*B* → *C ИЛИ C* → *B*) → (*B* → *C ИЛИ*

[1] 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.

C → *B*) → (*B* → *A ИЛИ C* → *A*). В итоге все действия начнут 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 приведёт 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 детерминированно. Но и здесь, в первую очередь, стоит заметить, что при последующих запросах данная проблема всегда будет угасать из-за увеличивающейся энтропии [4], 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 и расширение энтропии

1. (*A* → *B ИЛИ A* → *C*)

1, 2. [запрос (1)] →
| *0 бит* |

[# *A* — инициатор]
[# *B или C* — получатель или маршрутизатор]

2. (*B* → *C ИЛИ C* → *B*)

1. [маршрутизация (1)]
=

2. [ответ (1)] →
| 1 бит |

[# *B или C* — маршрутизатор]
ИЛИ
(*B* → *A ИЛИ C* → *A*)
[# *A* — инициатор]
[# *B или C* — получатель]

3. (*B* → *C ИЛИ C* → *B*)

1. [маршрутизация (~1)]
=
2, 3. [запрос (2)] →
| 1 бит |

[# *B или C* — маршрутизатор]
ИЛИ
(*B* → *A ИЛИ B* → *C*)
[# *B* — инициатор]
[# *A или C* — получатель или маршрутизатор]

4. (*B* → *A ИЛИ C* → *A*)

1. [ответ (1)]
=
2. [ответ (2)]
=
3. [маршрутизация (2)] →
| 2 бита |

[# *A* — инициатор]
[# *B или C* — получатель]
ИЛИ

(*A* → *B ИЛИ C* → *B*)
[# *B* — инициатор]
[# *A или C* — получатель]
ИЛИ
(*A* → *C ИЛИ C* → *A*)
[# *A или C* — маршрутизатор]

5. .....

Таким образом, задача анонимной сети на базе увеличения энтропии формируется сложностью нахождения истинных субъектов информации при трёх и более пользователях, не связанных между собой общими целями и интересами для внешнего глобального и внутреннего наблюдателей. Это возможно при использовании слепой маршрутизации в совокупности с вероятностным полиморфизмом пакета, где слепая маршрутизация обеспечивает диффузию пакета, распространяет его и делает каждый узел 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 абстрактной анонимной сети.

При этом стоит заметить, что в сети на базе увеличения энтропии, на уровне ядра, заложен механизм постоянного умножения, увеличения энтропии, как это представлено на *Рисунке 5*, 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.

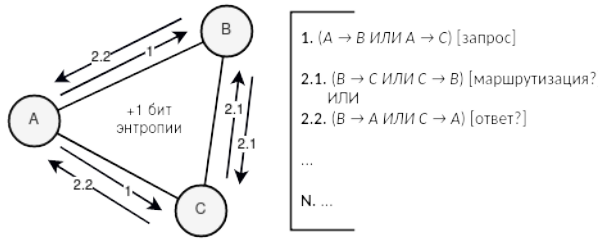

Рисунок 5. Зарождение неопределённости при вероятностном полиморфизме

Продолжая анализ абстрактной анонимной сети на базе увеличения энтропии, 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 или 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 и 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 при последовательных итерациях запрос — ответ или запрос — маршрутизация — ответ, а именно, является ли он (пакет) запросом или ответом с вероятностью 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 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 $T = 2+k$ при $k \bmod 2 = 0$ *ИЛИ* $T = 2(2+k)$ при $k \bmod 2 \neq 0$ (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 = НОК (2, 1+2, 2+2, ..., n+2)*.

Далее, если предположить, что существует сговор активного внутреннего наблюдателя и пассивного глобального наблюдателя, то вырисовывается картина, неблагоприятная для получателя, т. к. она в конечном счёте будет представлять его деанонимизацию. И правда, если отправитель становится способным формировать собственный маршрут, а также следить за сценарием работы сети посредством знания всех полиморфных состояний своего пакета, то последний узел из списка маршрутизации станет тем, кто выдаст детерминированно ответ на поставленный запрос, и, как следствие, самостоятельно создаст изоморфную связь между сетевой и криптографической идентификациями путём выдачи состояния объекта.

Решением должно стать отнесение отправителя ко множеству внешних атакующих, сделать его пассивным анализатором, прослушивателем системы на моменте получения пакета принимающей стороной и последующим транспортированием объекта до инициирующей стороны. Дополнительное формирование собственных маршрутов на принимающих узлах может стать частичным или составным решением проблемы, как это изображено на *Рисунке 6*, и привести к полиморфизму вида [(*A → B ИЛИ A → C*) → (*B → C ИЛИ C → B*)] → [(*B → C ИЛИ C → B*) → (*B → A ИЛИ C → A*)], где [] представляет раздельную генерацию маршрутизации пакета. Следовательно, вероятностный полиморфизм станет определением совокупной возможности существования промежуточных субъектов 3/4 = 1/4 (со стороны отправителя) +1/4 (со стороны получателя) +1/4 (со стороны обоих узлов) и их отсутствия 1/4. Таким образом, инициатор связи в конечном счёте станет неспособным со 100% уверенностью определить, что последний узел, отправляющий пакет, станет тем самым истинным получателем сообщения.

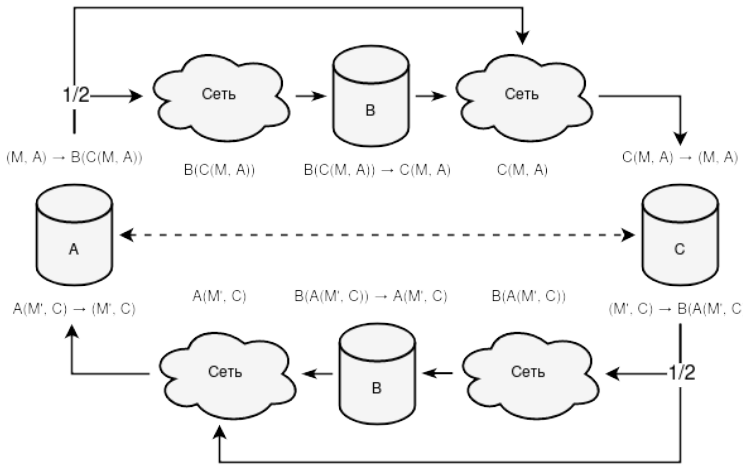

Рисунок 6. Обобщённая схема передачи информации в анонимной сети на базе увеличения энтропии

Но даже в вышеописанном случае остаётся связь, при которой получатель должен будет первым формировать всю последующую маршрутизацию, а следовательно и первым, кто будет генерировать новый полиморфный пакет. И т. к. инициатор способен анализировать всю сеть, то выявить субъекта, генерирующего пакет отличный от маршрутизирующего первоначально, на первый взгляд, не составит больших проблем. Но данная задача лежит в плоскости долгосрочного наблюдения за субъектами, а не краткосрочного. Проблематика деанонимизации такого случая усложняется алеаторными факторами (каждый промежуточный узел имеет вероятность генерировать псевдопакет, симуляция времени маршрутизации и ответа будет постоянно приводить к спаму, получатель способен самолично выставлять задержки отклика), порождающими и накапливающими энтропию, которая, как следствие, накладываясь на данную задачу, делает её анализ не таким примитивным и тривиальным — *Рисунок 7*.

Пример предотвращения выявления связи между сетевой и криптографической идентификациями получателя можно представить также на базе метаморфозов вероятностного полиморфизма со стороны инициирующей (атакующей) стороны.

Метаморфозы вероятностного полиморфизма и расширение энтропии

1. (*A* → *B ИЛИ A* → *C*)

1. [запрос (1)] →
| *0 бит* |

[# *A* — инициатор]
[# *B или C* — получатель]

2. (*B* → *C ИЛИ C* → *B*) [# $T_{[0;N]}$]

1. [маршрутизация (1)]
=
2. [запрос (2)] →
| 1 бит |

[# *B или C* — маршрутизатор]
ИЛИ =
(*B* → *C ИЛИ C* → *B*)
[# *B или C* — отправитель]

3. (*B* → *A ИЛИ C* → *A*) [# $T_{[0;N]}$]

3. [ответ (1)] →
| *1 бит* |

[# *B или C* — получатель]

В такой концепции свойство задержки $T_{[0;N]}$ применяется для аккумулирования энтропии. Чем больше участников сети становится, тем бо́льший прирост энтропии способен обеспечиваться в интервале $T_{[0;N]}$. При отсутствии данного параметра вероятность нулевого прироста энтропии увеличивается прямо пропорционально уменьшению мощности спама[1] (активности) сети. Таким образом, максимальный диапазон задержки N должен устанавливаться не меньше среднего времени генерации нового

[1] Мощность спама — количество сгенерированных уникальных пакетов в системе за определённый период времени *t*, совершённый разнородными (никак не связанными между собой общими целями и интересами) участниками сети. Из данного определения мощность спама не может превышать количество её участников ни в какой выбранный промежуток времени, потому как два и более сгенерированных пакета одним пользователем будут считаться за один по причине однородности узла к самому себе. Уровень заспамленности становится в некой мере ключевым фактором безопасности большинства анонимных сетей, т. к. «размывает» связь между истинными субъектами посредством перемешивания множества объектов в сети.

$|St| = \Sigma_{i=1}^{|L|} F\ (\Sigma_{j=1}^{|Li|}\ ((F*G)\ (t \bmod P\ (L_{ij}))))$, *где*
F: $N \cup \{0\} \rightarrow \{0, 1\} = [x/1+x] \Rightarrow 0 \rightarrow 0;\ x \neq 0 \rightarrow 1$,
G: $\{0, 1\} \rightarrow \{0, 1\} = x + 1 \pmod 2 \Rightarrow 0 \rightarrow 1;\ 1 \rightarrow 0$,
$L = Q\ (M)$,
M — множество всех узлов в сети,
Q — функция выборки списка подмножеств узлов, подчиняющихся одному лицу или группе лиц с общими интересами,
P — период генерации пакета на базе выбранного узла.

Если t представлено как *НОК* от всех $P\ (L_{ij}) \rightarrow НОК\ (P\ (L_{11}), P\ (L_{12}), \ldots, P\ (L_{21}), P\ (L_{22}), \ldots, P\ (L_{nm}))$, то в заданный промежуток времени мощность спама обретает своё максимальное значение $|S_t| = |L|$. Примером могут служить значения $L = [\{A, B\}, \{C\}, \{D\}]$, $(A) = 1$, $(B) = 2$, $(C) = 3$, $P\ (D) = 2$, где $НОК\ (P\ (A), P\ (B), P\ (C), P\ (D)) = 6$.

пакета в системе.

Защита от сговора активных внутренних и внешних наблюдателей схожа с анонимной сетью на базе очередей, где становится возможным создание поточной связи с целью взаимоблокировки субъектов, либо создание доверенных соединений с целью установки сложности встраивания в сеть зловредных узлов.

Принципиальное отличие сети на базе очередей от увеличивающей энтропию сводится к способу сдерживания мощности спама. В первом случае мощность спама разбивается по периодам (очередям), заданным самой системой, а потому и активность становится статичной, постоянной и определяемой величиной. Если периоды генерации будут сильно различаться между собой, то начнётся образование новых и дополнительных векторов нападения на систему. Во втором случае сдерживание мощности спама становится следствием алеаторного характера функционирования сети, удерживающего анализ поведения субъектов на базе накапливающейся меры неопределённости — энтропии. Таким образом периоды T_n и $T_{[0;N]}$ являются родственными явлениями, объединёнными принципом мощности спама.

В сравнении с абстрактной анонимной сетью на базе очередей, сеть на базе увеличения энтропии имеет свои положительные стороны. Во-первых, нет необходимости в ожидании очередей, что приводит к относительно быстрым откликам субъектов информации за счёт возможности параллельных действий. Во-вторых, из-за данного аспекта сеть на базе очередей становится неэффективной в удержании сервисов связи, потому как таковым жизненно необходимо иметь свойство параллельности. Тем самым, сети на базе очередей работают наиболее эффективно лишь и только в полностью децентрализованных системах, гибридность напротив будет приводить к большим задержкам отклика, что нельзя сказать о сетях на базе увеличения энтропии.

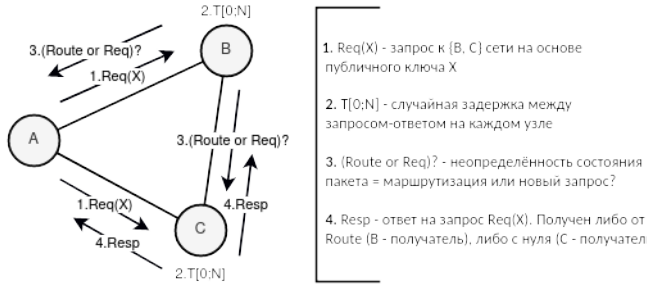

Рисунок 7. Неопределённость выявления получателя при атаке сопоставления связей между сетевой и криптографической идентификациями на инициирующей стороне

Отрицательными характеристиками сети на базе увеличения энтропии, в сравнении с сетью на базе очередей, являются необходимость в полиморфной маршрутизации (в том числе и при доверенных соединениях), а также необходимость в контроле накапливания энтропии. Данные случаи могут достаточно сильно усложнять систему и приводить к неправильным программным реализациям.

3.3. МОДЕЛЬ НА БАЗЕ ОБЕДАЮЩИХ КРИПТОГРАФОВ

Ещё одну из множества возможных моделей можно построить на базе существующих скрытых систем вида DC-сетей с присущей им теоретически доказуемой анонимностью. По умолчанию сети на базе «проблемы обедающих криптографов» не являются абстрактными, потому как привязаны к своей сетевой топологии типа «полносвязная». В такой архитектуре исключается возможность вариативного расположения узлов по всему множеству сетевых коммуникаций. Допустим, в чистом виде DC-сети нельзя применять так, чтобы вычисление результата проходило только через одного участника, потому как

таковой впоследствии будет способен деанонимизировать всех остальных субъектов и переведёт анонимную сеть в этап второй стадии анонимности.

Возможным решением перевода DC-сетей в модель абстрактности становится использование комбинации первой^ стадии анонимности с пятой, посредством которой информация сможет распространяться по сети без увеличения мощности доверия. В такой системе сетевая идентификация окончательно заменяется криптографическим аналогом, а композиция приобретает вид «пятая стадия анонимности + первая^ стадия анонимности + тайный канал связи». Комбинация «первая^ стадия анонимности + тайный канал связи» является классическим определением анонимной сети на базе DC-сетей, необходимой для ограничения получателей информации в широковещательной линии связи. Прибавочная «пятая стадия анонимности» становится следствием в необходимости иного распространения информации по широковещательной линии связи таким образом, чтобы промежуточный субъект легко мог транслировать и маршрутизировать поступающие ему пакеты, но не мог их читать в открытом виде или редактировать содержание.

Таким образом, заменив сетевой способ широковещательной связи на криптографический, становится возможным использование абстрактных DC-сетей в качестве второй формы тайных каналов связи. Также плюсом такого подхода композиций с заранее существующими скрытыми сетями и их преобразованием в абстрактные сети становится наследственность в доказуемости уровня анонимности. Иными словами, если анонимная сеть до преобразования в абстрактную являлась теоретически доказуемой, то и после такого изменения она в равной степени останется теоретически доказуемой, потому как сам внутренний механизм функционирования не изменится, изменится лишь внешний способ идентификации субъектов между собой.

4. ЗАКЛЮЧЕНИЕ

Абстрактные анонимные сети представляют собой достаточно большой интерес для последующих изучений, потому как позволяют поддерживать теоретически доказуемую анонимность в уже существующих подконтрольных централизованных системах. В сравнении с другими анонимными сетями, абстрактные сети наиболее эффективно разделяют сетевые и криптографические коммуникации, за счёт чего становится неважным факт существования «цепочек» маршрутизаций для сохранения анонимата субъектов. С другой стороны, на базе приведённых моделей абстрактных анонимных сетей, проблемой таковых систем становится свойство масштабируемости, которое не позволяет принимать большое количество соединений. Таким образом, абстрактные анонимные сети становятся способными обеспечивать анонимизацию трафика лишь для малого круга лиц.

СПИСОК ЛИТЕРАТУРЫ

1. Коваленко, Г. Теория строения скрытых систем [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer/blob/master/docs/theory_of_the_structure_of_hidden_systems.pdf (дата обращения: 04.01.2023).

2. Коваленко, Г. Монолитный криптографический протокол [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer/blob/master/docs/monolithic_cryptographic_protocol.pdf (дата обращения: 04.01.2023).

3. 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).

4. 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).

Децентрализованный протокол обмена ключами

Аннотация. Разработка протоколов обмена ключами между собеседниками/узлами в сети всегда является крайне важной и сложной задачей в проблематике безопасных коммуникаций, потому как исходит из возможных нападений и специфики самой системы, в которой обмен должен корректно происходить. Централизованные и децентрализованные способы обмена ключами представляют собой два разнородных способа функционирования таковых механизмов. В то время как централизованные механизмы уже действуют и функционируют в повседневности, децентрализованные механизмы за счёт этого кажутся более эзотерическими и мало изученными, что не всегда является таковым. Децентрализованные системы также имеют возможность обмениваться ключами, но исходя лишь из своей ризоморфной парадигмы.

Ключевые слова: протокол обмена ключами; криптографический протокол; децентрализованные сети; централизованные системы; сеть доверия; MITM-атака.

1. ВВЕДЕНИЕ

При разработке децентрализованных систем всегда остро стоит проблема аутентификации субъектов при обмене публичными ключами как между непосредственными собеседниками, так и между узлами в самой сети. Проблема исходит из атак типа MITM (man in the middle), осуществление которых приводит не только к череде пассивных нападений в лице прослушивания транслируемого трафика, но и к активным нападениям в лице его подмены. Такой исход вызывает сопутствующие проблемы доверия безопасности всех накладываемых коммуникаций.

2. ПРОБЛЕМАТИКА

Проблема обмена ключами исходит из классической криптографии, когда не существовало какого бы то ни было раздела асимметричной криптографии. Проблема звучала достаточно просто: возможно ли передать симметричный ключ шифрования безопасно так, чтобы третья сторона не смогла его перехватить и прочитать?

Рисунок 1. Использование небезопасного канала связи при передаче ключа

За четыре тысячелетия классической криптографии так и не был дан корректный ответ на поставленный вопрос. Лишь с приходом современной криптографии, когда классическая форма постепенно приобретала новый облик науки, появлялся и новый раздел криптографии — асимметричная криптография [1], сутью которой стала возможность безопасной передачи симметричного ключа, использовав при этом небезопасный канал связи.

Головоломки Меркла (1974), протокол Диффи-Хеллмана [DH] (1976), алгоритм RSA (1976), протокол Месси-Омуры [MO]

(1978), ранцевая криптосистема Меркла-Хеллмана (1978), криптосистема Рабина (1979), схема Эль-Гамаля [EG] (1985) и последующие вариации DH, EG, MO на эллиптических кривых породили возможность решения огромного спектра прикладных задач, которым важна была безопасность коммуникаций, начиная с обычной потребности в общении и заканчивая банковскими транзакциями.

Внешне может показаться, что при таком развитии криптографии, и в частности её асимметричного раздела, ранее существовавшая и старая проблема классической криптографии более становится неактуальной. Но на самом деле асимметричная криптография не решает окончательно первоначальную проблему, а лишь сдвигает «ареал обитания атакующих» с пассивных до активных нападений, заменяя проблему передачи симметричного ключа на проблему передачи публичного ключа.

Тем не менее даже такой результат уже является достаточно позитивным, потому как злоумышленнику становится необходимо совершать дополнительные действия и трудозатраты, которые по истечению времени могут ещё и выдать факт его существования субъектам коммуникации (если таковые смогут лично встретиться и проверить передаваемые значения), но лишь постфактум.

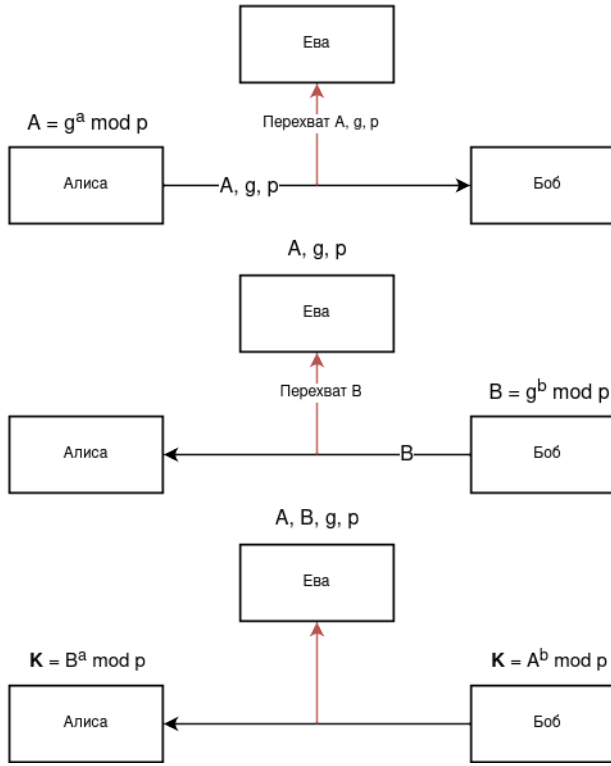

Рисунок 2. Использование небезопасного канала связи при генерации ключа (протокол Диффи-Хеллмана)

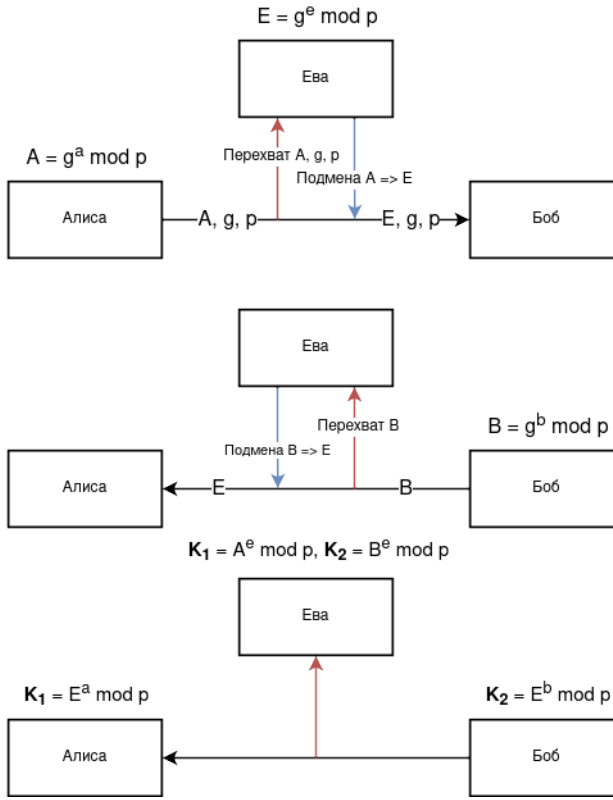

Рисунок 3. Атака MITM на примере протокола Диффи-Хеллмана

3. РЕШЕНИЯ ЦЕНТРАЛИЗАЦИИ

Современный Интернет со всей текущей рекламой, коммерцией, онлайн-покупками и продажей просто не мог бы адекватно существовать, если бы постоянно совершались злоумышленниками сопутствующие MITM-атаки. И действительно, если бы такое существовало в реальности, то можно было бы пересчитать на пальцах компании, которые были бы готовы смириться с рисками кражи передаваемых финансов и с постоянным снижением уровня доверия их же клиентов. Да и сами клиенты, принимая отрицательную сторону платежей через Интернет, просто бы продолжали пользоваться наличными деньгами. В итоге единственной безотказно рабочей бизнес-моделью в Интернете оставались бы сами MITM-атаки.

Тем не менее настоящая реальность показывает нам, что проблема MITM как-то решается и по ощущениям довольно успешно. Когда мы пользуемся браузером, то он нам может показывать три возможных состояния коммуникаций: небезопасно (http://), безопасно (https://) и ещё раз небезопасно (~~https://~~). Первое говорит просто о том, что не существует вовсе шифрования. Второе утверждает, что всё безопасно шифруется и подтверждается. И как раз последнее свидетельствует о том, что возможно осуществление MITM-атаки.

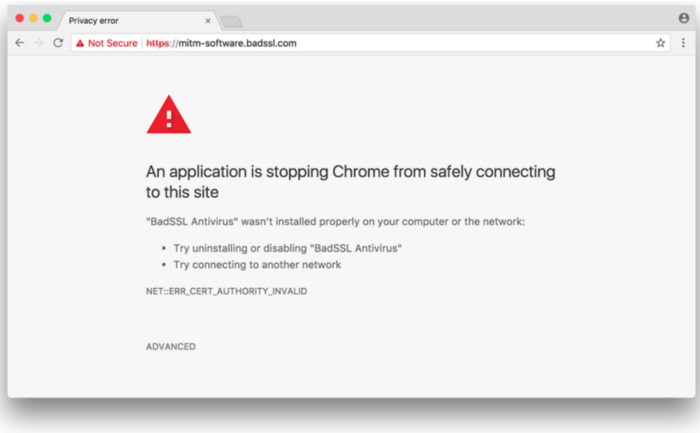

Рисунок 4. Атака MITM на примере протокола Диффи-Хеллмана

Так в итоге, как современный мир смог решить проблему MITM? Ответ: достаточно просто — делегировав возможность совершения MITM-атаки ограниченному кругу сервисов, выдвигаемых в роли центров сертификации (доверенных узлов). Схема крайне проста, но на своих первоначальных этапах она была также уязвима к MITM со стороны сторонних злоумышленников.

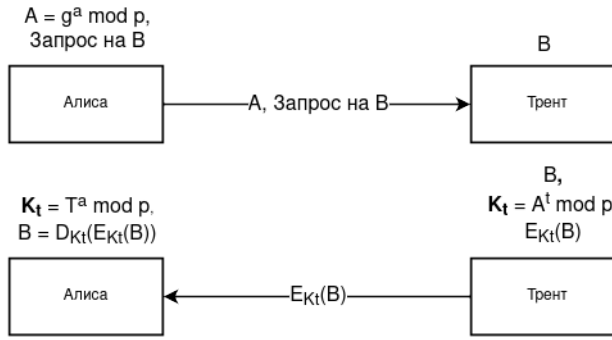

Рисунок 5. Трент — доверенный узел. Предполагается, что Алиса уже знает Трента, а потому и знает T. Доверие абсолютно, и Алиса предполагает, что Трент не будет совершать MITM. Под E_{Kt} понимается алгоритм, способный доказать Алисе, что само сообщение отправил и подтвердил именно Трент

Иными словами, при работе за компьютером с доступом в Интернет уже предполагается, что на таковом компьютере на уровне ОС, браузера или конкретного приложения установлены сертификаты (публичные ключи) центров сертификации, за счёт которых и совершаются дальнейшие безопасные коммуникации. Но стоит понимать, что как-то ОС, браузер, приложение должны были попасть на итоговый компьютер без доверенного узла. Здесь может быть несколько ветвлений развития со стороны централизации.

1. Первый и самый очевидный вектор — просто плыть по течению, и рано или поздно, даже с учётом жертв MITM, б*о*льшая часть пользователей наконец установит обновлённую ОС, браузер или приложение с вложенными в них публичными ключами центров сертификации.

2. Второй вектор — использовать кооперацию с производителями устройств, чтобы таковые устанавливали ОС с уже вло-

женными публичными ключами центров сертификации. Таковой способ вполне удовлетворителен, но не действителен для клиентов, у которых уже присутствуют устройства.

Как только информация о центрах сертификации будет установлена на клиентском устройстве, то все дальнейшие MITM-атаки начинают делегироваться. Общий вид MITM со сторонними злоумышленниками теряет свой первоначальный смысл. Теперь MITM могут совершать лишь «законно установленные» злоумышленники в роли ЦС.

4. РЕШЕНИЯ ДЕЦЕНТРАЛИЗАЦИИ

Децентрализованные системы часто решают проблемы MITM-атак более изощрёнными, эзотерическими способами за счёт невозможности создания центров сертификации, которые бы явно противоречили ризоморфной структуре. Тем не менее, как далее мы опишем, децентрализованные сети часто на своих первоначальных стадиях запуска будут использовать централизованные системы, как и до этого сами централизованные системы использовали небезопасные каналы связи при установке ЦС.

1. Первый метод обмена ключами в децентрализованных сетях — это обмен ключами лично в оффлайне. Иными словами, метод сводится к использованию простого, старого, надёжного и проверенного временем в тысячелетия способа обмена. Безусловно, это не самый удобный способ, потому как может существовать большое количество его ограничений — невозможность передачи ключа явно, географическое расположение, не позволяющее осуществить передачу, небезопасность использования посредника при транспортировании и прочее. В любом случае такой способ хоть и не имеет технической базы, но при этом является одним из самых надёжных методов передачи.

2. Второй метод сводится к использованию централизованных сервисов в роли площадок для размещения публичных ключей. Часто создатели децентрализованных систем сами создают сервер, на котором выкладывают и постоянно редактируют список публичных ключей, выступая тем самым в роли некого ЦС, хоть и на более низком уровне по иерархии доверия. Как только первоначальная децентрализованная сеть была построена и сервер в роли ЦС сыграл свою основную роль *корректно*,

сами участники могут обмениваться внутри сети публичными ключами, в некой степени эмулируя применение *первого* способа обмена. Подменить публичные ключи становится возможным на трёх уровнях: 1) на уровне оригинального ЦС, где таковой должен сотрудничать с провайдерами связи для успешных редиректов на копию сервера с другими публичными ключами, 2) на уровне выдвигаемого сервера в роли ЦС, где таковой может самолично изменять публичные ключи, 3) на уровне децентрализованной сети, если произошёл либо первый, либо второй пункт, либо если сам узел является злоумышленником, выдающим ложные ключи.

3. Третий метод сводится к использованию сети доверия [2]. Данный способ успешно может функционировать в роли продолжения второго, после того как клиенты получили первоначальные публичные ключи от сервера. Каждый указанный публичный ключ на сервере сам становится своеобразным ЦС, который перенаправляет публичные ключи от одного узла к другому. Далее, как только сами клиенты начинают обладать определённым количеством ключей, они также автоматически становятся ЦС, устанавливающими и выстраивающими на своей стороне дальнейшие коммуникации. Указанный механизм интересен тем, что уровень централизованного доверия к узлам постоянно «разлагается». Изначально существовавший один сервер обладает *100%* уровнем доверия, далее список публичных ключей в *N* уменьшает, в лучшем случае, первоначальное доверие до *100%/N*, и далее сами клиенты, подключившись к узлам в *Q-м* количестве, продолжают уменьшать необходимый уровень доверия, в лучшем случае, до *100%/N/Q* и т. д. Сеть доверия будет работать лишь при условии, что *N* и *Q* не приводят всё к тому же *100%* уровню доверия, иначе говоря, если *N* и *Q* не равны единице. Поэтому следует понимать под *N и Q* не просто количество узлов, а количество узлов, не подменяющих информацию. Если количество узлов, не подменяющих информацию, равно нулю, то следует установить *N или Q = 1*.

4. Четвёртый метод сводится к использованию уже существующих децентрализованных сервисов в роли площадок для размещения публичных ключей. Как пример, используя некий блокчейн *X*, мы можем внести криптовалюту в свой аккаунт, вставив публичный ключ в определённо договорённый (с абонентом) интервал времени *T* или блок *B*. Далее мы ссылаемся на конкретный блок *B* и интервал времени *T* для идентификации своего публичного ключа. Злоумышленнику в таком сценарии становится необходимо успеть поместить публичный ключ в интервал *T* или блок *B*, заменив до этого сообщение о публичном ключе на стороне абонента.

5. Пятый метод сводится к использованию уже существующих централизованных сервисов как ретрансляторов публичных ключей от точки *A* до точки *B*. Внешне пятый способ может быть схож со вторым по причине использования централизованных механизмов, но внутренне он отличается достаточно сильно. Так, например, во втором способе публичные ключи размещаются на централизованном сервисе, а далее по запросу таковой список просто выгружается уже в качестве ответа. В пятом же способе передача публичных ключей связана непосредственно с криптографическим протоколом, позволяющим с определённой степенью регулируемой вероятности передать публичный ключ не только без последующей подмены централизованными сервисами, но и при этом не раскрывая сам передаваемый публичный ключ, что может быть необходимо/полезно при условии, что децентрализованная сеть является анонимной [3].

4.1. ПРОТОКОЛ ПЯТОГО МЕТОДА

Использование централизованных сервисов при обмене публичными ключами звучит противоречиво, потому что сами же централизованные сервисы могут с бо́льшим шансом/успехом подменять публичные ключи. Поэтому, чтобы снизить риски подмены, разработчики децентрализованных систем со-

здают собственные серверы, как это было описано во *втором* методе. Тем не менее весь подход сводится к двум моментам.

1. Во-первых, связь с централизованными сервисами уже по умолчанию защищена ЦС, иными словами, мы начинаем искоренять всевозможных злоумышленников, стоящих между отправителем и получателем в децентрализованных сетях. В таком случае мы просто сужаем спектр всех возможных атакующих до централизованных сервисов.

2. Во-вторых, должно быть выбрано несколько централизованных сервисов, наиболее несвязанных между собой. Например, facebook[1] и vkontakte, telegram и signal, и т. д. Иными словами, необходимо «разложить» централизацию индивидуальных сервисов на децентрализацию множества сервисов.

Далее механизм связи сводится к передаче одного публичного ключа сразу по нескольким централизованным сервисам. Если ключи все пришли одинаковые, то велика вероятность того, что ключ не был подменён. Если малая часть ключей была подменена, то можно взять в качестве правды ключ с бо́льшим процентом однотипности либо совершить вновь процедуру отправления ключа, но исключая предыдущие сервисы (которые выдали ключ в ме́ньшей пропорции) и заменяя их другими сервисами.

Плюс такой схемы в том, что мы используем уже готовую (централизованную) инфраструктуру для обмена ключами, в отличие от Web of Trust, требующей создавать собственную инфраструктуру открытых ключей.

Предполагается, что у *A* и *B* есть своя пара открытый/закрытый ключ. Для *A* — это (*PubA/PrivA*), для *B* — это (*PubB/PrivB*).

[1] Продукт компании Meta, которая признана экстремистской организацией в Российской Федерации.

1. Пользователь *B* генерирует временную пару открытый/закрытый ключ (*PubT/PrivT*) и отправляет открытый ключ *PubT* пользователю *A* через *N* централизованных сервисов, прямо не связанных[1] между собой.

2. Пользователь *A* получает открытые ключи $PubT_1$, $PubT_2$, $PubT_3$, ..., $PubT_N$ с централизованных сервисов соответственно *1, 2, 3, ..., N* и сравнивает, все ли они одинаковые. Если больше половины ключей расходится ($\lim_{C \to N/2}$) — пользователи *A* и *B* выбирают совершенно новые *N* централизованных сервисов и начинают процедуру заново.

3. Если меньше половины ключей расходится ($\lim_{C \to N}$) — пользователи *A* и *B* выбирают под несогласованный публичный ключ новые сервисы связи и повторяют процедуру конкретно с ними.

4. Если результат выбранных сервисов расходится с результатом предыдущего большинства, то следует вновь поменять сервисы. Если ряд выбираемых сервисов выдают результат, отличный от предыдущего большинства, и в количестве данный ряд превышает предыдущее большинство, то следует вернуться на условие *процедуры 2*.

[1] Под несвязанностью понимается отсутствие общих директоров, инфраструктуры, кооперации. Например, vk.com и mail.ru являются связанными между собой сервисами, потому как располагают непосредственной коммуникацией, как на уровне общих директоров, так и на уровне инфраструктуры. С другой стороны vk.com и signal.org считаются несвязанными, потому как их модель взаимодействия либо отсутствует, либо неизвестна.

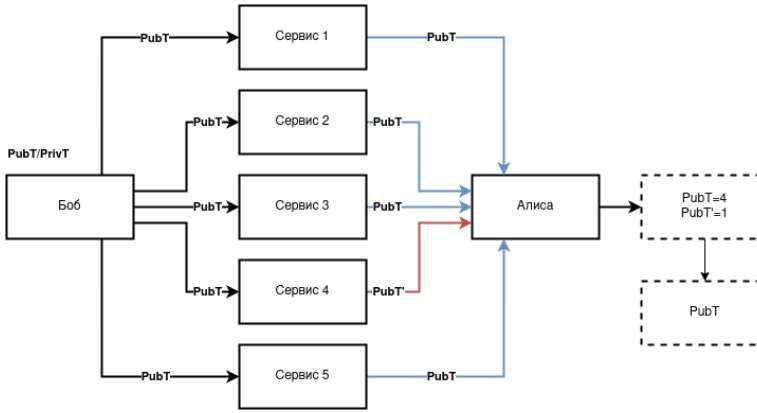

Рисунок 6. Схема получения временного публичного ключа PubT

5. Далее пользователь *A* зашифровывает открытым ключом *PubT* свой открытый ключ *PubA* и отправляет полученный результат также на выбранные ранее *N* сервисов:

CPubA = E (PubT, PubA)

6. Пользователь *B* просматривает корректность получения *CPubA*. Если шифрованные ключи расходятся, то применяются процедуры *2, 3, 4,* направленные на уже шифрованную версию ключей.

7. При успешном получении шифрованного публичного ключа *CPubA* пользователь *B* применяет временный закрытый ключ *PrivT* и расшифровывает *CPubA*, получая тем самым публичный ключ *PubA*:

PubA = D (PrivT, CPubA)

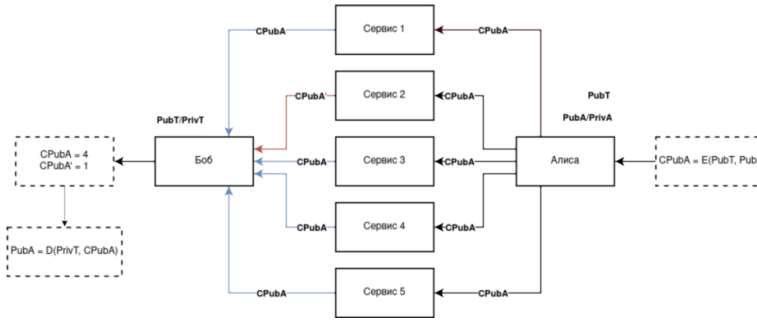

Рисунок 7. Схема получения публичного ключа PubA

8. Далее пользователь *B* подписывает свой публичный ключ *PubB* временным закрытым ключом *PrivT* и шифрует результат ранее полученным публичным ключом *PubA*. Результат подписания и шифрования пользователь *B* отправляет пользователю *A*. Пользователь *B* может использовать любой сервис связи, т. к. в данном случае уже нельзя будет корректно подменить информацию за счёт необходимости нарушения подписи для *PrivT*:

SPubB = S (PrivT, PubB),
CSPubB = E (PubA, SPubB).

9. Пользователь *A* принимает *CSPubB*, расшифровывает его своим публичным ключом *PubA*, получая тем самым *SPubB*. Далее пользователь *A* проверяет подпись, используя временный публичный ключ *PubT*, получая тем самым истинность публичного ключа *PubB*:

SPubB = D (PubA, CSPubB),
PubB = V (PubT, SPubB).

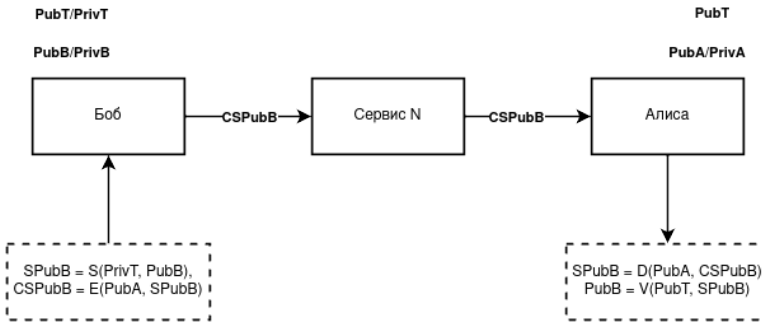

Рисунок 8. Схема получения публичного ключа PubB

Таким образом, пользователи *A* и *B* обменялись своими публичными ключами, воспользовавшись сторонними централизованными сервисами связи. При этом в вышеописанном протоколе централизованные сервисы так и не узнали истинные публичные ключи, которые будут применяться в качестве дальнейших идентификаторов *ID* в децентрализованной сети, а потому и не смогут их использовать для связывания с сетевым адресом *IP* (анонимные сети).

У централизованных сервисов в полномочии остались только *PubT, CPubA, CSPubB*. Этапы 2*, 3, 4* защищают от активных атак за счёт однотипных действий на не связанных между собой сервисах.

Несмотря на вышеописанные положительные стороны и финальную успешность передачи ключа, протокол всё же обладает рядом недостатков:

1. Протокол является *вероятностным*. Существует вероятность, что централизованные сервисы смогут связаться и успешно подменять публичные ключи хотя бы для *1/4* сервисов, что будет достаточно, т. к. последний сервис будет считаться уже некорректным.

2. Если *A* или *B* является злоумышленником, а децентрализованная сеть является анонимной и чувствительной к связи *ID=IP*, то злоумышленник, получив публичный ключ своего абонента, получит тем самыми и его идентификатор *ID* в сети. При сотрудничестве с сервисами связи он сможет легко узнать и *IP* абонента. Таким образом, легко свяжет полученный публичный ключ с сетевым адресом.

3. Предполагается, что пользователи *A* и *B* уже друг друга идентифицируют на выбираемых ими централизованных сервисах. В противном случае пользователи *A* и *B* не будут знать, кому отправляют и от кого получают ключи.

5. ЗАКЛЮЧЕНИЕ

В работе были представлены способы обмена ключами как в централизованных системах, так и в децентрализованных. При разборе децентрализованных систем был подробно описан криптографический протокол, позволяющий обмениваться публичными ключами за счёт использования множества централизованных сервисов. Протокол может применяться при обмене ключами для последующего их использования в анонимных сетях за счёт сокрытия истинного публичного ключа при передаче. Недостатком протокола является его вероятностная структура, успешность результата которой зависит от количества централизованных сервисов связи и их несвязываемости между собой.

СПИСОК ЛИТЕРАТУРЫ

1. 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).

2. Hung-Yu C., Dynamic Public Key Certificates with Forward Secrecy [Электронный ресурс]. — Режим доступа: https://www.mdpi.com/2079-9292/10/16/2009 (дата обращения: 01.08.2023).

3. Коваленко, Г. Теория строения скрытых систем [Электронный ресурс]. — Режим доступа: https://github.com/number571/go-peer/blob/master/docs/theory_of_the_structure_of_hidden_systems.pdf (дата обращения: 26.09.2023).

ОГЛАВЛЕНИЕ

Геннадий Александрович Коваленко

Общая теория анонимных коммуникаций

Второе издание

Создано в интеллектуальной издательской системе Ridero

Геннадий Александрович Коваленко — преподаватель предмета КСЗИ (криптографические средства защиты информации), разработчик информационных систем. Занимается открытой разработкой криптографических приложений, анонимных сетей, блокчейн систем. Github: https://github.com/number571

Существующие определения анонимности и безопасности конечных пользователей в сетевых коммуникациях часто являются расплывчатыми, неясными и противоречащими друг другу. Такая реальность восприятия стала следствием недостающей теоретической основы, которая могла бы структурировать основные подходы к построению или использованию скрытых систем. Понимание термина «анонимность» посредством декомпозиции его составляющих способно дать оценку дальнейшего вектора развития анонимных/безопасных систем.