

Грокаем анонимность



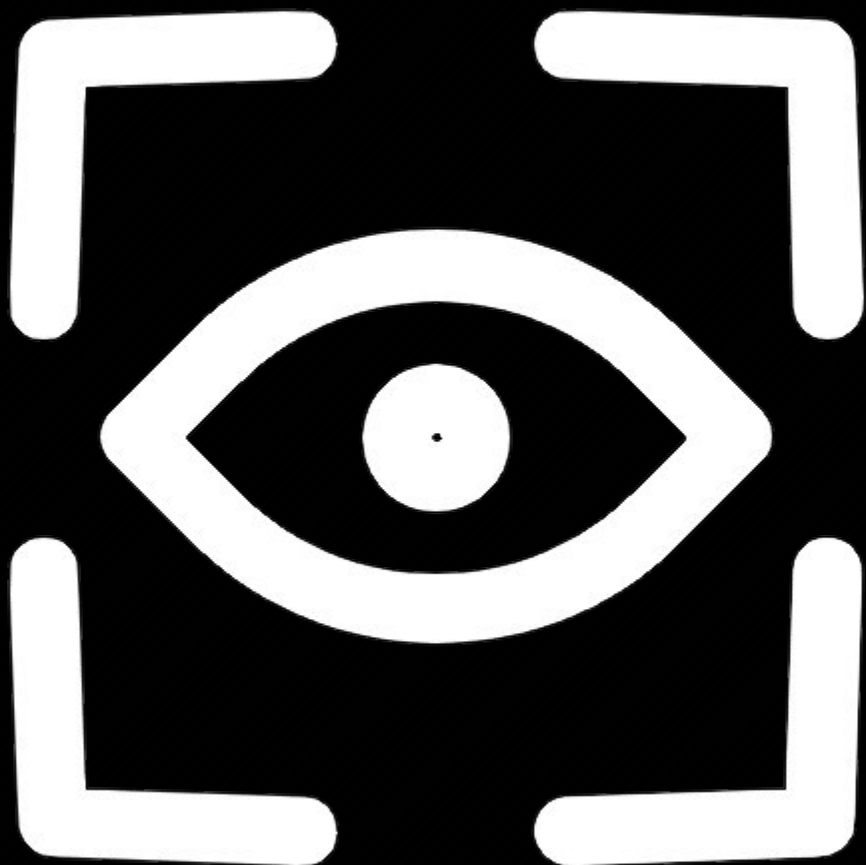
Коваленко Геннадий Александрович

Анонимность во многом пересекается с
безопасностью данных, потому как это есть
безопасность метаданных — связей между
отправлением и получением

Определение

- Любая анонимность сводится к **сокрытию связей** между отправителем и получателем
- Отправитель и получатель **не всегда обязаны** быть анонимны друг к другу
- Анонимность может существовать в любой среде, где **больше чем одна** связь





- Под связью следует понимать не только явные случаи отправления информации, но также и **неявные случаи** её получения
- **Наблюдатели трафика** аналогично начинают формировать связь с отправителем, становясь получателями факта появления информации

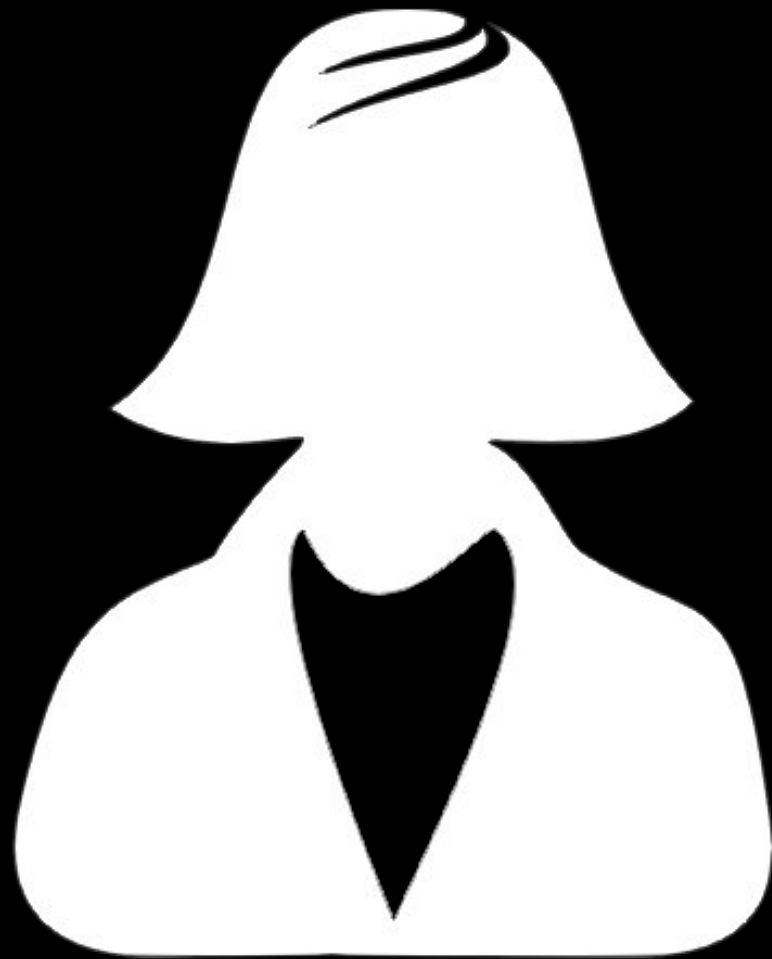
- В некоторых системах для формирования анонимности становится необходимым фактор **относительной деанонимизации**
- Данный фактор носит **роль доверия**, где все связи, или только их часть, перестают быть анонимными для ограниченного круга лиц
- **Рамки заданного круга лиц** определяют различие между относительной и **абсолютной деанонимизацией**



Примеры

- Преступник, совершивший своё действие, становится **анонимным отправителем** информации
- Общество в таком случае становится **получателем** данной информации
- Сам факт получения информации может быть **побочным эффектом** действия преступника, что не отменяет наличие получателей



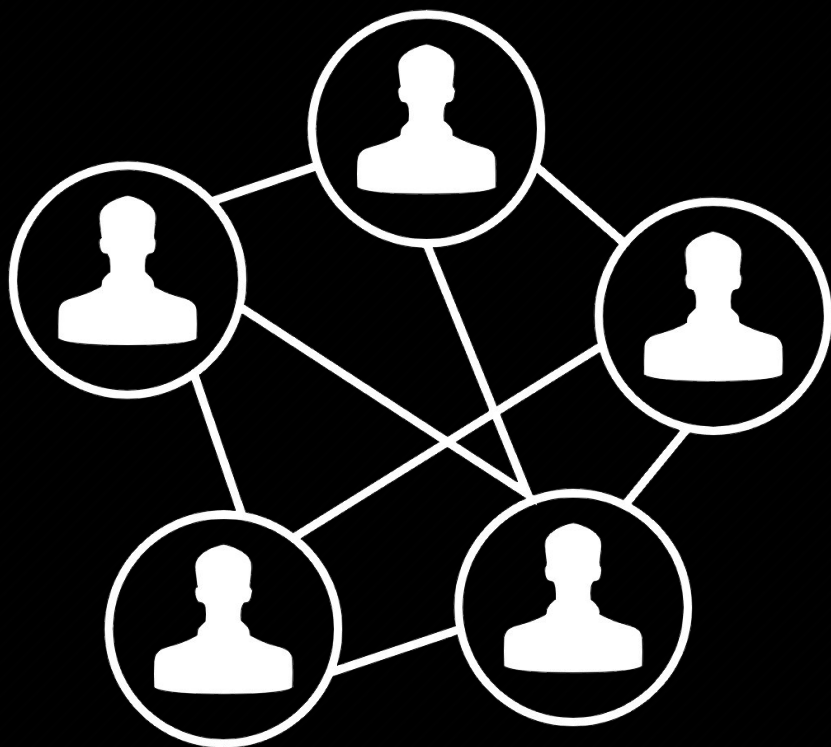


- У преступника мог быть **сообщник**, являющийся одним из получателей в обществе
- Целью сообщника становится **ретрансляция** истинных целей (сообщений) преступника
- Преступник не анонимен для сообщника, что свидетельствует об **относительной** его деанонимизации, предотвращающей деанонимизацию **абсолютную**

Сетевая анонимность

- Сетевая анонимность базируется преимущественно на **криптографических** примитивах
- Чаще всего риск перехода относительной деанонимизации в абсолютную **может контролироваться** за счёт выстраивания N -ого количества промежуточных узлов в цепочке маршрутизации

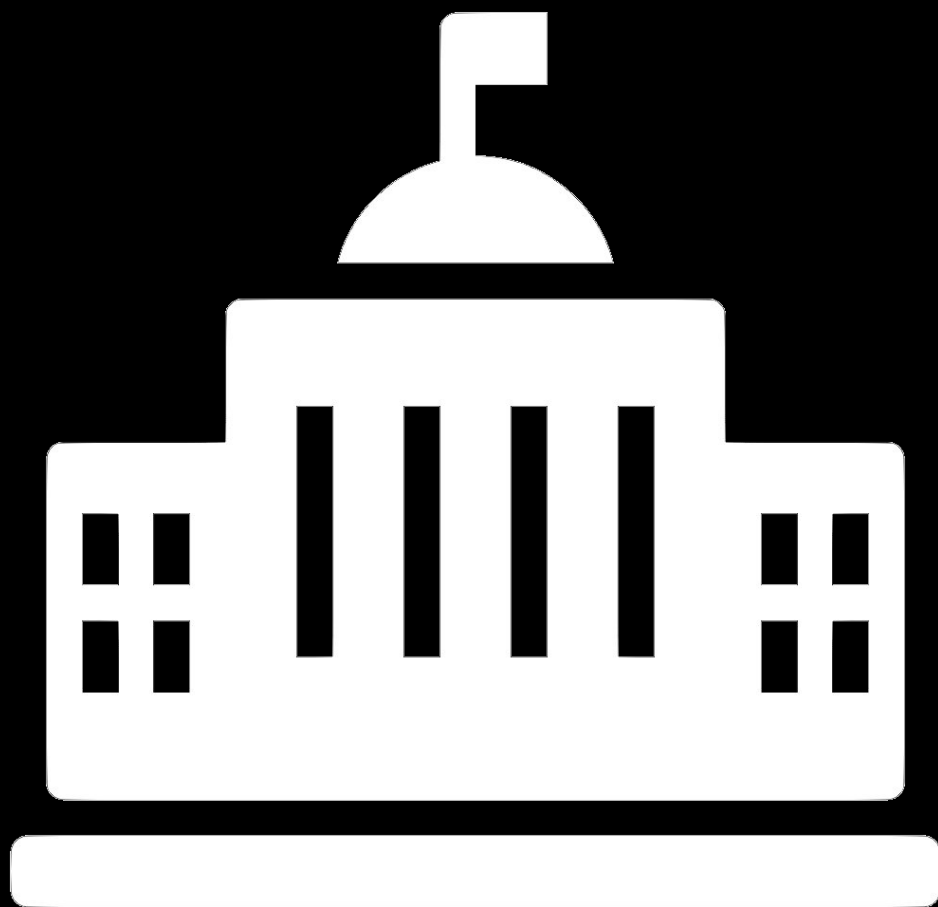




- Сетевая анонимность, являясь подмножеством анонимности, приводит к появлению более **конкретных моделей угроз и задач**
- В отличие от классической анонимности, сетевая анонимность способна **формировать скрытые (анонимные) сети**
- Анонимные сети создают **благоприятные условия** для формирования и удержания определённо заданного уровня анонимата

- **Скрытие сетевого адреса (IP) получателя часто является одной из форм анонимности для сопутствующего обхода блокировок со стороны провайдера связи**
- **Скрытие сетевого адреса (IP) отправителя часто является одной из форм анонимности для сопутствующего обхода блокировок со стороны сервиса связи**





- Государства становятся **внешними**, и зачастую **глобальными** наблюдателями (получателями) всего генерируемого трафика
- С целью противодействия глобальным наблюдателям создаются анонимные сети с **теоретически доказуемой** моделью
- При отсутствии глобальных наблюдателей применяются сети с более слабой моделью угроз на базе **принципа федеративности**

Термины

- **Мощность анонимности**
 $|A|$ — 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



|T|

- **Мощность доверия $|T|$ —** количество узлов, участвующих в хранении или передаче информации, представленной для них в открытом виде

- **Вид данных $\{D\} = M$ (мономорфный) | P (полиморфный)**
- **Полиморфизм информации** — свойство изменчивости передаваемого объекта при множественной маршрутизации несколькими субъектами сети, разграничивающее связь субъектов посредством анализа объекта
- **Мономорфизм информации** — свойство неизменчивости передаваемого объекта

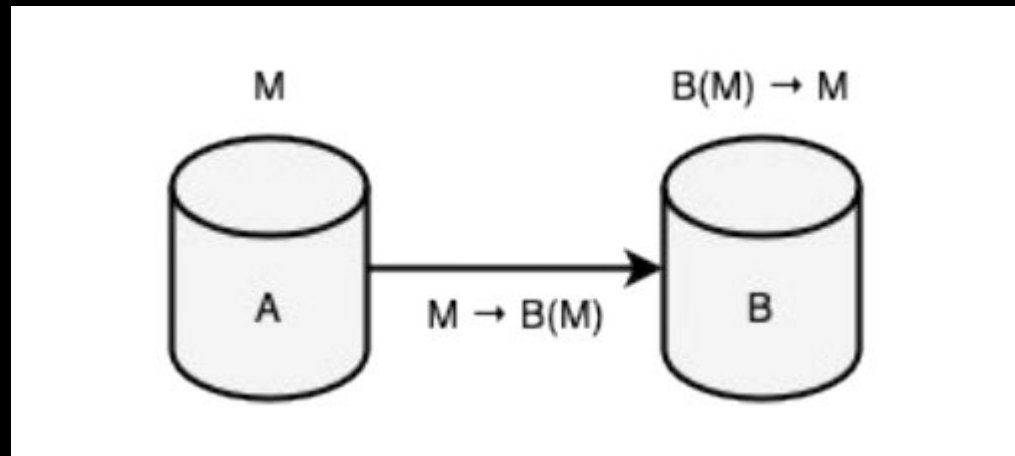
- Система $\{S\} = P$ (одноранговая) | M (многогранговая) | H (гибридная)
- **Одноранговая** — равноправные системы
- **Многогранговая** — централизованные сервисы
- **Гибридные** — системы, сочетающие в себе качества одноранговых и многогранговых систем

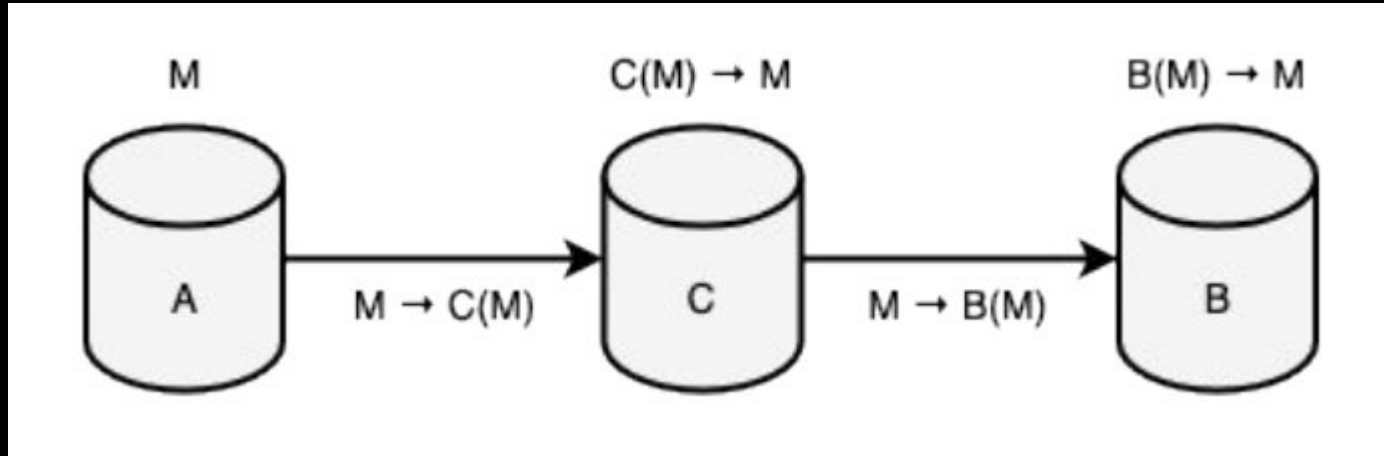
- **Идентификация** $\{I\} = N$ (сетевая) | C (криптографическая)
- Криптографическая идентификация выстраивается **поверх сетевой** и способна моделировать **собственную логику** маршрутизации поверх последней

- Система коммуникации $\{C\} = R$
(маршрутизация) | P (платформа)
- Платформа связи определяется **конечной логикой** сети / приложения, логикой исполнения итоговых целей
- Маршрутизация определяется способом транспортировки информации от субъекта к платформе связи

Развитие анонимности *v1*

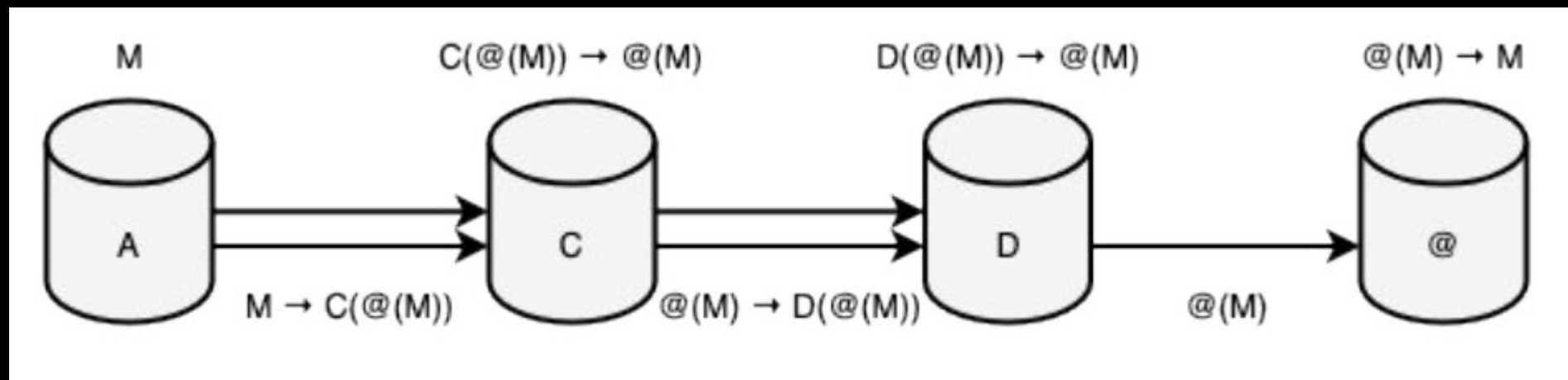
- **Первая стадия анонимности** — её отсутствие в лице прямой связи между отправителем и получателем
 - $|A|=0, \lim|T|\rightarrow 1, \{D\}=M, \{S\}=P, \{I\}=N, \{C\}=P$

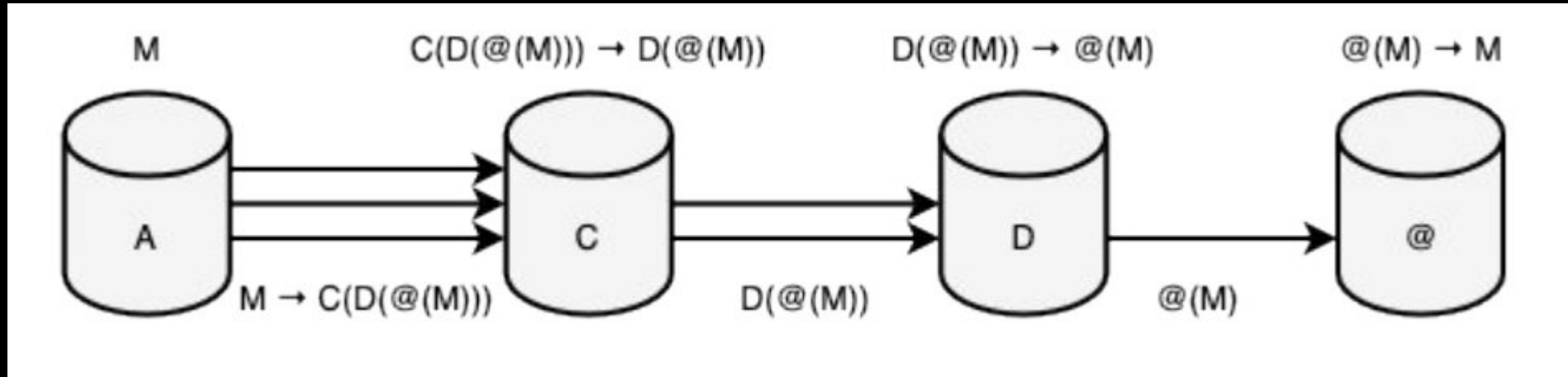




- **Вторая стадия анонимности** — формирование централизованного / промежуточного узла, устанавливающего связь между отправителем и получателем
 - $|A|=1$, $|T| \geq 2$, $\{D\}=M$, $\{S\}=M$, $\{I\}=N$, $\{C\}=P$

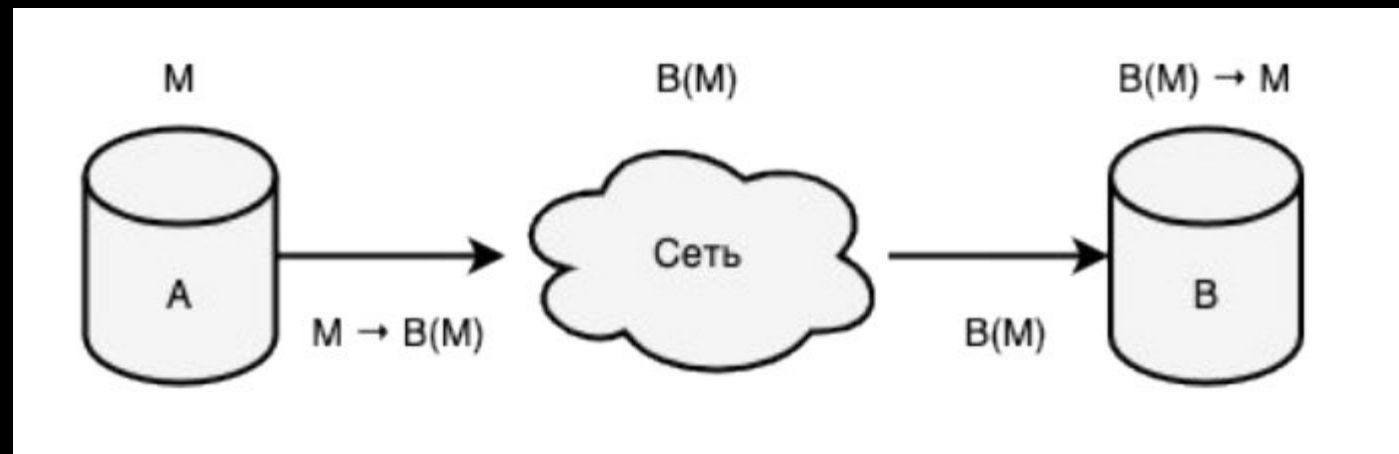
- **Третья стадия анонимности** — использование ретрансляторов (проxy серверов) в C -ом количестве между отправителем и получателем
 - $\lim |A| \rightarrow C, |T| \geq 1, \{D\} = M, \{S\} = H, \{I\} = N, \{C\} = R$

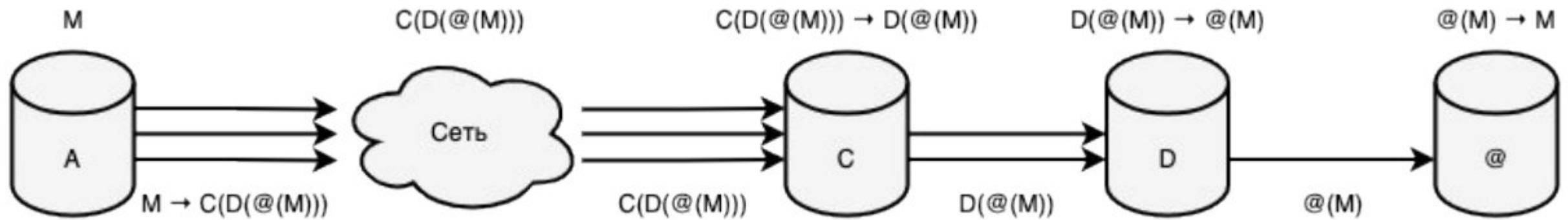




- **Четвёртая стадия анонимности** — использование туннелирования (VPN сервисов) в C -ом количестве между отправителем и получателем
 - $\lim |A| \rightarrow C, |T| \geq 1, \{D\} = P, \{S\} = H, \{I\} = N, \{C\} = R$

- **Пятая стадия анонимности** — замена сетевой идентификации криптографической с динамичным количеством маршрутизирующих узлов = N
- $0 \leq |A| < N$, $\lim |T| \rightarrow 1$, $\{D\} = M$, $\{S\} = (P|H)$, $\{I\} = C$, $\{C\} = P$





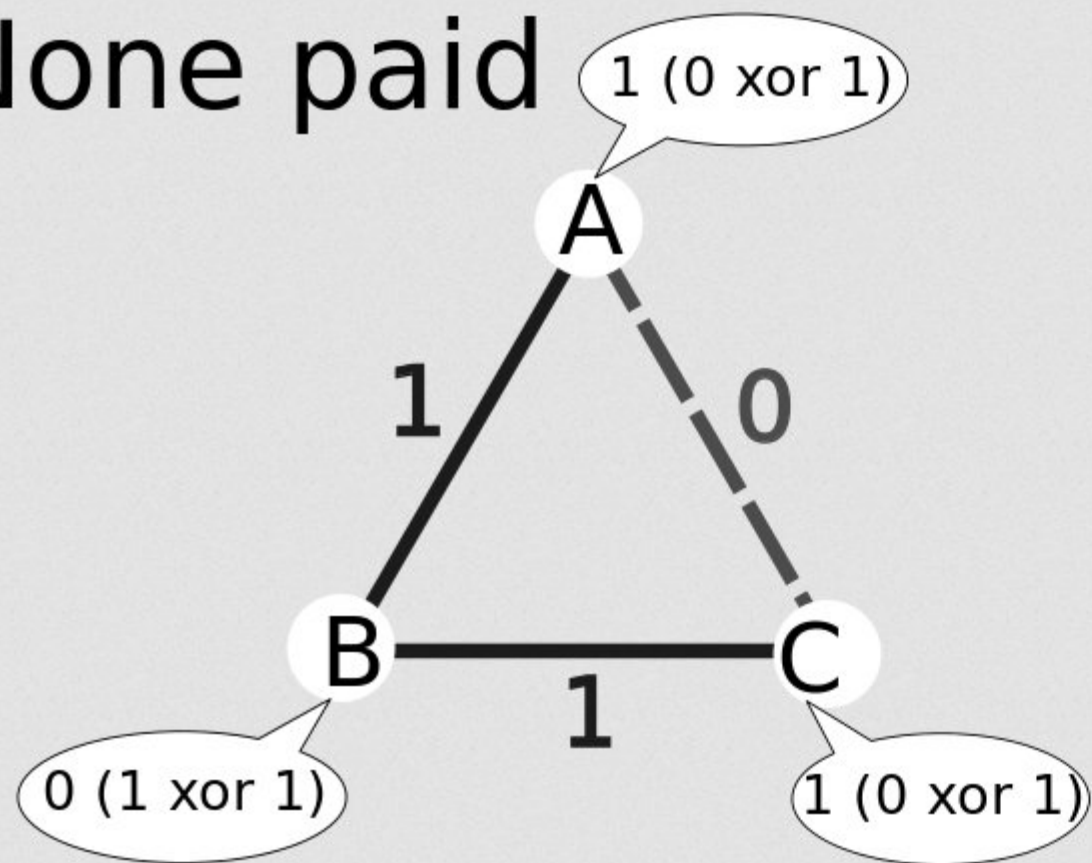
- **Шестая стадия анонимности** — композиция четвёртой (множественное шифрование) и пятой (криптографическая идентификация) стадий
- $(1 \leq |A| < N \mid \lim |A| \rightarrow C), |T| > 1, \{D\} = P, \{S\} = (P|H), \{I\} = C, \{C\} = R$

Развитие анонимности v2

- Второй вектор развития определяется **переходом** децентрализованных систем с платформ связи на маршрутизирующий характер

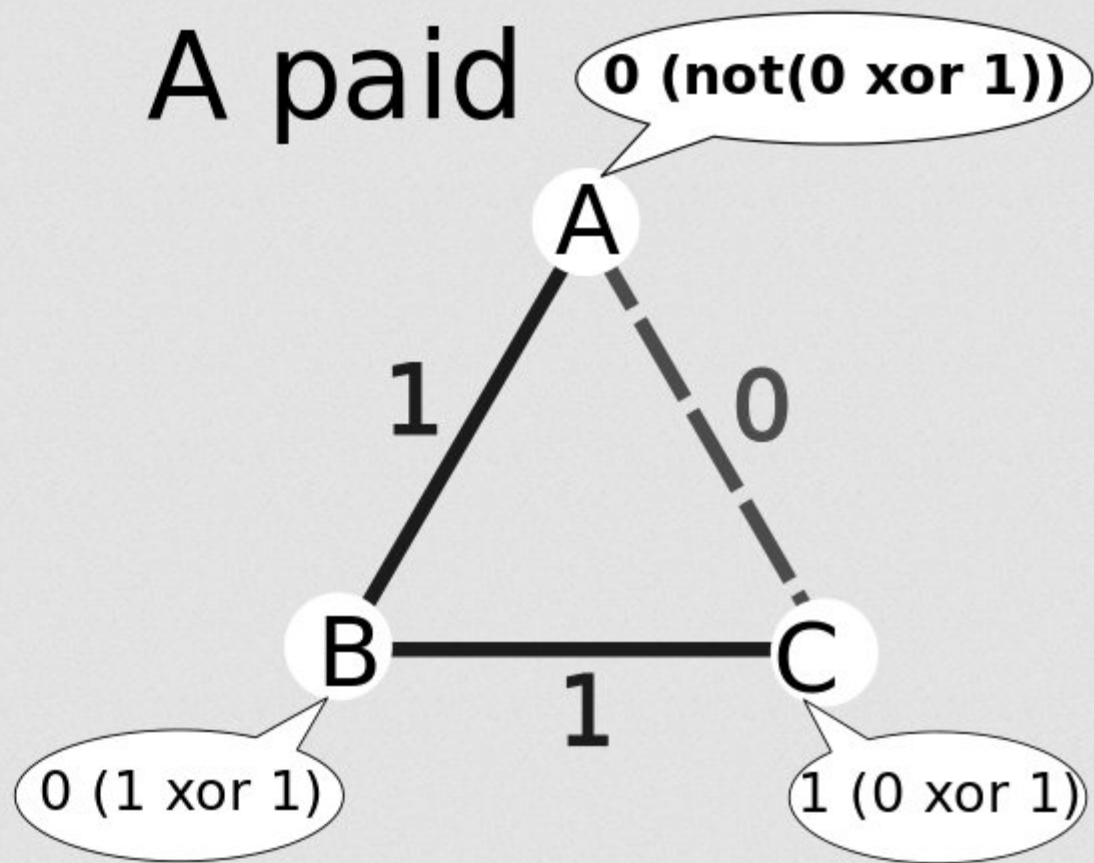
- **Первая^ стадия анонимности** — формирование сети без промежуточных узлов с сильной зависимостью к создаваемому трафику
 - $\lim |A| \rightarrow N-1, |T|=N-1, \{D\}=P, \{S\}=P, \{I\}=N, \{C\}=R$
- К первой^ стадии анонимности могут быть отнесены **ДС-сети** (dining cryptographers) — сети на базе проблемы **обедающих криптографов**

None paid



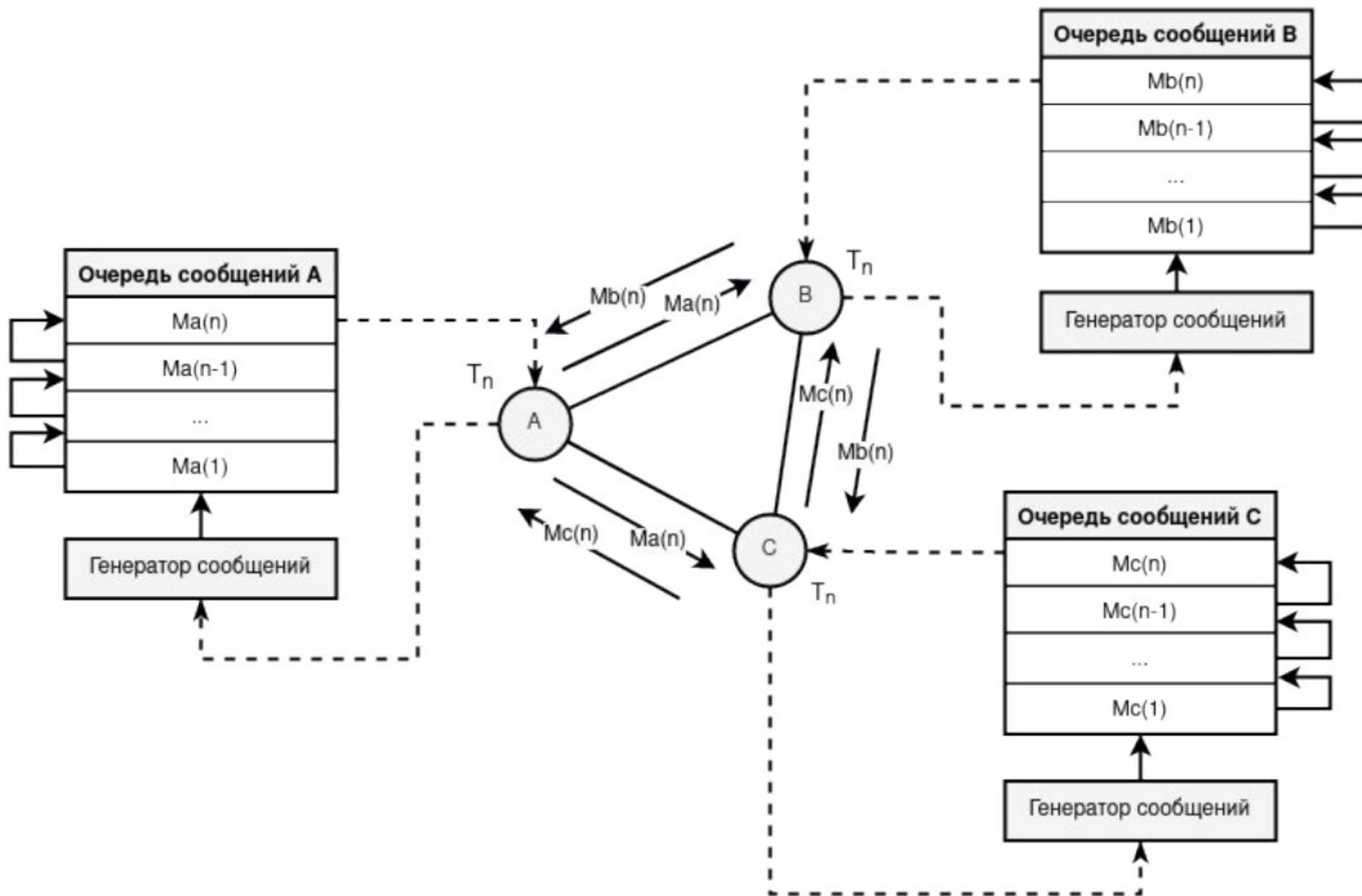
$$1 \text{ xor } 1 \text{ xor } 0 = 0$$

A paid

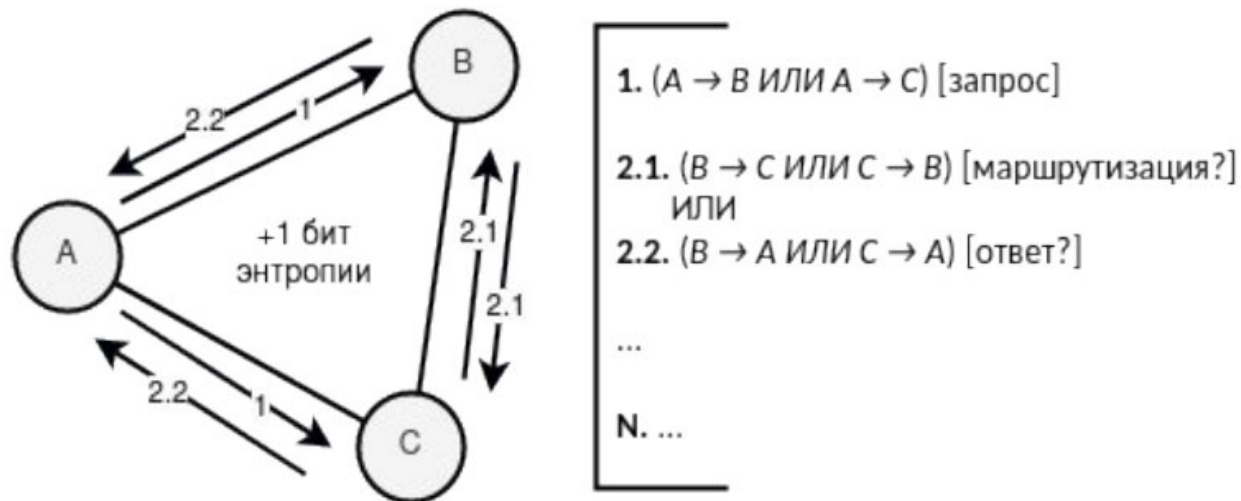


$$1 \text{ xor } 0 \text{ xor } 0 = 1$$

- **Пятая^ стадия анонимности** — формирование сети с локальным свойством генерации трафика по периоду
 - $0 \leq |A| < N$, $|T| > 1$, $\{D\} = M$, $\{S\} = P$, $\{I\} = C$, $\{C\} = R$
- К пятой^ стадии анонимности могут быть отнесены **QB-сети** (queue based) — сети на базе проблемы очередей



- В классическом (первом) векторе развития на шестой стадии анонимности также **могут существовать** сети с теоретически доказуемой моделью
- К таким представителям относятся **ЕІ-сети** (entropy increase) — сети на базе проблемы **увеличения энтропии**



Заключение

Литература

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