|  |  |
| --- | --- |
|  | **Эта статья предлагается для** [**быстрого удаления**](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D0%B8%D0%B8_%D0%B1%D1%8B%D1%81%D1%82%D1%80%D0%BE%D0%B3%D0%BE_%D1%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F)**.**  *Причина*: [С5](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%9A%D0%91%D0%A3#%D0%A15): из статьи явно не следует важность, известность или значительность её объекта.  **Выявившему нарушение**: пожалуйста, поместите сообщение  {{subst:СпасибоНезначимо|Hidden Lake Messenger}} ~~~~  на страницу обсуждения участника, [создавшего статью](https://ru.wikipedia.org/w/index.php?title=Hidden_Lake_Messenger&action=history&dir=prev&limit=1).   * [Автоподтверждённые участники](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%90%D0%B2%D1%82%D0%BE%D0%BF%D0%BE%D0%B4%D1%82%D0%B2%D0%B5%D1%80%D0%B6%D0%B4%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D1%83%D1%87%D0%B0%D1%81%D1%82%D0%BD%D0%B8%D0%BA%D0%B8) имеют право снять или заменить этот шаблон в [случаях, оговорённых в правилах](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%A3%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86#%D0%91%D1%8B%D1%81%D1%82%D1%80%D0%BE%D0%B5_%D1%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5). * Если вы не согласны с необходимостью быстрого удаления, [поставьте](https://ru.wikipedia.org/w/index.php?title=Hidden_Lake_Messenger&action=edit) шаблон {{[hangon](https://ru.wikipedia.org/wiki/%D0%A8%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD:Hangon)}}*прямо под этим сообщением* и **сразу же объясните** необходимость оставления на [странице обсуждения](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%81%D1%83%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5:Hidden_Lake_Messenger?action=edit&redlink=1).   [*Последнее изменение*](https://ru.wikipedia.org/w/index.php?title=Hidden_Lake_Messenger&diff=cur) *сделано участником* [*Владлен Манилов*](https://ru.wikipedia.org/wiki/%D0%A3%D1%87%D0%B0%D1%81%D1%82%D0%BD%D0%B8%D0%BA:%D0%92%D0%BB%D0%B0%D0%B4%D0%BB%D0%B5%D0%BD_%D0%9C%D0%B0%D0%BD%D0%B8%D0%BB%D0%BE%D0%B2) *(*[*вклад*](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%92%D0%BA%D0%BB%D0%B0%D0%B4/%D0%92%D0%BB%D0%B0%D0%B4%D0%BB%D0%B5%D0%BD_%D0%9C%D0%B0%D0%BD%D0%B8%D0%BB%D0%BE%D0%B2)*•* [*журналы*](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%96%D1%83%D1%80%D0%BD%D0%B0%D0%BB%D1%8B/%D0%92%D0%BB%D0%B0%D0%B4%D0%BB%D0%B5%D0%BD_%D0%9C%D0%B0%D0%BD%D0%B8%D0%BB%D0%BE%D0%B2)*) в 10:10, 15 февраля 2023 (UTC; менее 2 часов назад).* [*Ссылки сюда*](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%A1%D1%81%D1%8B%D0%BB%D0%BA%D0%B8_%D1%81%D1%8E%D0%B4%D0%B0/Hidden_Lake_Messenger)*,* [*история*](https://ru.wikipedia.org/w/index.php?title=Hidden_Lake_Messenger&action=history)*,* [*журналы*](https://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:Log&page=Hidden_Lake_Messenger)*. Администраторам и подводящим итоги:* [*удалить*](https://ru.wikipedia.org/w/index.php?title=Hidden_Lake_Messenger&action=delete&wpReason=%5B%5B%D0%92%D0%9F%3A%D0%9A%D0%91%D0%A3%23%D0%A15%7C%D0%A15%5D%5D%3A+%D0%B8%D0%B7+%D1%81%D1%82%D0%B0%D1%82%D1%8C%D0%B8+%D1%8F%D0%B2%D0%BD%D0%BE+%D0%BD%D0%B5+%D1%81%D0%BB%D0%B5%D0%B4%D1%83%D0%B5%D1%82+%D0%B2%D0%B0%D0%B6%D0%BD%D0%BE%D1%81%D1%82%D1%8C%2C+%D0%B8%D0%B7%D0%B2%D0%B5%D1%81%D1%82%D0%BD%D0%BE%D1%81%D1%82%D1%8C+%D0%B8%D0%BB%D0%B8+%D0%B7%D0%BD%D0%B0%D1%87%D0%B8%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C+%D0%B5%D1%91+%D0%BE%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%B0)*.* |

|  |  |
| --- | --- |
|  | **Быстрое удаление этой статьи оспаривается.**  Указана следующая причина: **HLM базируется на теоретически доказуемой анонимности, отличной от DC-сетей, поэтому присутствует значимость объекта**. Участник, поставивший это уведомление, сомневается в необходимости быстрого удаления этой статьи. Комментарии — на [**странице обсуждения**](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%81%D1%83%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D0%B5:Hidden_Lake_Messenger?action=edit&redlink=1). Несмотря на это, администраторы всё равно могут выполнить удаление при соответствии этой статьи [критериям быстрого удаления](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D0%B8%D0%B8_%D0%B1%D1%8B%D1%81%D1%82%D1%80%D0%BE%D0%B3%D0%BE_%D1%83%D0%B4%D0%B0%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F). |

**Hidden Lake Messenger (HLM)** — [анонимный](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%BE%D0%BD%D0%B8%D0%BC%D0%BD%D1%8B%D0%B5_%D1%81%D0%B5%D1%82%D0%B8) мессенджер с [открытым исходным кодом](https://github.com/number571/go-peer/tree/master/cmd/hidden_lake/messenger) безопасность которого базируется на [сквозном шифровании](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D0%B2%D0%BE%D0%B7%D0%BD%D0%BE%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) и [friend-to-friend](https://ru.wikipedia.org/wiki/Friend-to-friend) коммуникации. Связывается с приложением [Hidden Lake Service](https://github.com/number571/go-peer/tree/master/cmd/hidden_lake/service) (HLS) посредством которого происходит дальнейшая анонимизация трафика.

## **Особенности**

HLM позволяет достигать теоретически доказуемой анонимности от пассивных наблюдателей за счёт задачи (модели) на базе очередей.

#### **Модель на базе очередей**

Предположим, что в сети существует три узла (пользователя): {*A, B, C*}. Если у каждого узла выставлена очередь генерации сообщений с периодом равным *N*, то это говорит о том, что каждый пользователь обязан ровно один раз в период *N* генерировать информацию и отправлять её в сеть всем узлам. Если истинной информации не существует, то отправляется ложная информация. Каждая информация, будь то ложная или истинная, зашифровывается, тем самым для внешнего наблюдателя ложная информация становится неотличимой от истинной. Зашифрованное сообщение не указывает кому оно адресовано, а информация об отправителе находится внутри шифрованной оболочки. Единственный способ получить информацию — обладать нужным приватным ключом. Как только один узел получает зашифрованную информацию — он отсылает её всем своим соединениям и пытается её расшифровать. Таким образом, сетевая идентификация (IP адреса) в HLM не играет роли, потому как вся действительная маршрутизация базируется на криптографической идентификации (публичные ключи).

Алгоритм каждого узла может быть представлен следующим образом.

1. Если существует сообщение для отправления, то оно шифруется публичным ключом получателя и вставляется в очередь сообщений. Каждая очередь локальна, в отличие от сетей типа DC ([проблема обедающих криптографов](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B1%D0%BB%D0%B5%D0%BC%D0%B0_%D0%BE%D0%B1%D0%B5%D0%B4%D0%B0%D1%8E%D1%89%D0%B8%D1%85_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%BE%D0%B2)).
2. Если достигается время периода равное N, то из очереди берётся зашифрованное сообщение и отправляется всем текущим соединениям. Если очередь пуста, то генерируется ложное сообщение, шифруется и отправляется в сеть.
3. Если узел получает сообщение из сети, то он транслирует данное сообщение дальше по сети, а после пытается его расшифровать. Если сообщение расшифровывается, то узел является истинным получателем.
4. У каждого сообщения существует свой хеш, благодаря которому узлы запоминают сообщение и не позволяют более одного раза транслировать его в сеть. За счёт этого критерия не образуется зацикливание информации.
5. Если узел смог расшифровать сообщение, то он проверяет отправителя и удостоверяется в том, что он находится в белом списке (в списке друзей). Иначе сообщение игнорируется.

#### **Программная реализация**

Мессенджер написан на языке [Go](https://ru.wikipedia.org/wiki/Go). Используется фреймфорк [Bootstrap](https://ru.wikipedia.org/wiki/Bootstrap_(%D1%84%D1%80%D0%B5%D0%B9%D0%BC%D0%B2%D0%BE%D1%80%D0%BA)) для отображения интерфейсной составляющей. Может быть портирован на [Windows](https://ru.wikipedia.org/wiki/Windows), [Linux](https://ru.wikipedia.org/wiki/Linux), [Mac OS](https://ru.wikipedia.org/wiki/MacOS), [Android](https://ru.wikipedia.org/wiki/Android) за счёт специфики исполнения (локальный [HTTP](https://ru.wikipedia.org/wiki/HTTP)-сервер) и отображения ([GUI](https://ru.wikipedia.org/wiki/%D0%93%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8F) в браузере).

## **Недостатки**

HLM обладает рядом недостатков из-за чего его применение становится ограниченным.

1. Увеличение количества участников сети приводит линейно к нагрузке всей системы. Если количество пользователей равно *Q*, то каждый узел должен будет расшифровывать *Q-1* информации в период равный *N*. Расшифрование является ресурсозатрачиваемой операцией, а потому может приводить к большим нагрузкам на ПК. Таким образом, HLM становится применим лишь в малых группах участников.
2. Модель на базе очередей приводит к последовательным действиям исключающим параллельность. Если *X* участников одновременно отправят одному участнику сообщение, то все гарантировано получат ответ минимум за *XN* времени, где *N* — время периода. Увеличение количества возможных отправлений за указанный период, ровно как и уменьшение времени периода, не решит проблемы, так как это лишь приведёт к линейному увеличению нагрузки на каждого участника сети.
3. Модель на базе очередей делает проблематичным реализацию некоторых сервисов, как например файловых серверов. Связано это с тем, что загрузка файла должна осуществляться порциями по 1MiB (лимит установленный в HLS). Следовательно, если файл равен 1GiB, то требуется *1000* запросов и минимум (в лучшем случае) *1000N* времени ожидания, где *N* — время периода. Тем не менее, для функций типа мессенджеров с малым размером сообщений, модель на базе очередей может быть хорошо использована.

|  |  |
| --- | --- |
|  | В статье **не хватает** [**ссылок на источники**](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%A1%D1%81%D1%8B%D0%BB%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8) (см. также [рекомендации по поиску](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%9F%D0%BE%D0%B8%D1%81%D0%BA_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2)).  Информация должна быть [проверяема](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%9F%D1%80%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D0%B5%D0%BC%D0%BE%D1%81%D1%82%D1%8C), иначе она может быть удалена. Вы можете [отредактировать](https://ru.wikipedia.org/w/index.php?title=Hidden_Lake_Messenger&action=edit) статью, добавив ссылки на [авторитетные источники](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D1%82%D0%B5%D1%82%D0%BD%D1%8B%D0%B5_%D0%B8%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8) в виде [сносок](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%A1%D0%BD%D0%BE%D1%81%D0%BA%D0%B8).*(15 февраля 2023)* |

|  |  |
| --- | --- |
|  | В этой статье **не проставлены** [**тематические категории**](https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D0%BA%D0%B8%D0%BF%D0%B5%D0%B4%D0%B8%D1%8F:%D0%9A%D0%B0%D1%82%D0%B5%D0%B3%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F).  Вы можете помочь проекту, найдя их или создав новые, а потом добавив их в статью. |