## **Симметричные протоколы[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=1)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=1)**]**

|  |  |
| --- | --- |
| **Криптографические обозначения, используемые в протоколах проверки подлинности и обмена ключами** | |
| {\displaystyle A} | Идентификаторы Алисы (*Alice*), инициатора сессии |
| {\displaystyle B} | Идентификатор Боба (*Bob*), стороны, с которой устанавливается сессия |
| {\displaystyle T} | Идентификатор Трента (*Trent*), доверенной промежуточной стороны |
| {\displaystyle K\_{A},K\_{B},K\_{T}} | Открытые ключи Алисы, Боба и Трента |
| {\displaystyle K\_{A}^{-1},K\_{B}^{-1},K\_{T}^{-1}} | Секретные ключи Алисы, Боба и Трента |
| {\displaystyle E\_{A},\left\{...\right\}\_{K\_{A}}} | Шифрование данных ключом Алисы, либо совместным ключом Алисы и Трента |
| {\displaystyle E\_{B},\left\{...\right\}\_{K\_{B}}} | Шифрование данных ключом Боба, либо совместным ключом Боба и Трента |
| {\displaystyle \left\{...\right\}\_{K\_{B}^{-1}},\left\{...\right\}\_{K\_{A}^{-1}}} | Шифрование данных секретными ключами Алисы, Боба (цифровая подпись) |
| {\displaystyle I} | Порядковый номер сессии (для предотвращения атаки с повтором) |
| {\displaystyle K} | Случайный сеансовый ключ, который будет использоваться для симметричного шифрования данных |
| {\displaystyle E\_{K},\left\{...\right\}\_{K}} | Шифрование данных временным сеансовым ключом |
| {\displaystyle T\_{A},T\_{B}} | Метки времени, добавляемые в сообщения Алисой и Бобом соответственно |
| {\displaystyle R\_{A},R\_{B}} | Случайные числа (*[nonce](https://ru.wikipedia.org/wiki/Nonce" \o "Nonce)*), которые были выбраны Алисой и Бобом соответственно |

основная статья: [**Симметричные криптосистемы**](https://ru.wikipedia.org/wiki/%D0%A1%D0%B8%D0%BC%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%8B%D0%B5_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B)

### Лягушка с открытым ртом [[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=2) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=2)]

Протокол "Лягушка с открытым ртом" (Wide-Mouth Frog англ.), оригинальная статья [Wide-Mouth Frog](https://ru.wikipedia.org/wiki/Wide-Mouth_Frog" \o "Wide-Mouth Frog) — простейший протокол управления ключами. Он позволяет двум абонентам установить общий сессионный ключ для защищенного общения между собой.[[1]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-1) В протоколе принимает участие [доверенный центр](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8).

#### Описание работы протокола [**[2]**](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-2)**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=3)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=3)**]**

* Алиса хочет установить сессионный ключ с Бобом. Она начинает, формируя:

1. K — случайный сеансовый ключ

2. TA — метку времени

и отправляет Тренту (доверенному центру), добавив своё имя:

M0 = A, EA(TA, B, K).

* Трент, используя общий с Алисой секретный ключ, расшифровывает сообщение и проверяет правильность метки времени TAи идентификатора Боба. Если все хорошо, он формирует:

TB — новую метку времени (которая может отличаться от TA) и отправляет Бобу

M1 = EB (TB, A, K).

* Боб получает сообщение, расшифровывает его общим с Трентом ключом и проверяет метку времени TA и идентификатор Алисы. Если сообщение прошло проверку, то теперь Боб имеет общий с Алисой ключ.

### Протокол Нидхема-Шрёдера[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=4) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=4)]

[Протокол Нидхема-Шрёдера на симметричных ключах](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%9D%D0%B8%D0%B4%D1%85%D0%B5%D0%BC%D0%B0_%E2%80%94_%D0%A8%D1%80%D1%91%D0%B4%D0%B5%D1%80%D0%B0#.D0.9F.D1.80.D0.BE.D1.82.D0.BE.D0.BA.D0.BE.D0.BB_.D0.9D.D0.B8.D0.B4.D1.85.D0.B5.D0.BC.D0.B0-.D0.A8.D1.80.D1.91.D0.B4.D0.B5.D1.80.D0.B0_.D0.B4.D0.BB.D1.8F_.D0.B0.D1.83.D1.82.D0.B5.D0.BD.D1.82.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.86.D0.B8.D0.B8_.D1.81_.D1.81.D0.B8.D0.BC.D0.BC.D0.B5.D1.82.D1.80.D0.B8.D1.87.D0.BD.D1.8B.D0.BC_.D0.BA.D0.BB.D1.8E.D1.87.D0.BE.D0.BC) (англ. The Needham-Schroeder shared-key protocol) важен, в первую очередь, по историческим причинам. Он является основой для многих протоколов распространения ключей, использующих доверенный центр, начиная с 1978 года. В том числе протоколы Kerberos и Otway-Rees (описанные ниже) берут своё начало в этом протоколе.

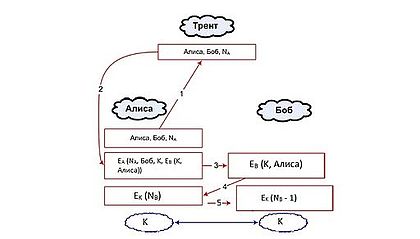
Данный протокол является примером протокола, не зависящего от меток времени и при этом обеспечивающего выработку и подтверждение ключа.

#### Описание работы протокола Нидхема-Шрёдера**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=5)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=5)**]**

##### Ситуация перед началом работы протокола**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=6)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=6)**]**

* 3 действующих лица: клиенты Алиса и Боб, которые хотят получить ключ для общения между собой, Трент — доверенный центр.
* У Алисы и Боба есть секретные ключи EA и EB соответственно для общения с Трентом.
* Алиса выбирает [число NA](https://ru.wikipedia.org/wiki/Nonce),Боб выбирает число NB.

##### Период работы протокола**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=7)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=7)**]**

* [](https://commons.wikimedia.org/wiki/File:NSSK_forwiki.jpg?uselang=ru)

Графическое описание работы протокола Нидхема-Шредера на симметричных ключах

Итак, Алиса запускает протокол, формирует сообщение, состоящее из своего и Боба идентификаторов, а так же выбранного числа [NAи](https://ru.wikipedia.org/wiki/Nonce) отправляет его Тренту.

M0 = A, B, NA.

* Получив сообщение от Алисы, Трент формирует сообщение, состоящее из двух частей. В первую часть он кладет NA, идентификатор Боба, а также новый ключ K, который и хотят получить Алиса и Боб. Вторая часть сообщения так же содержит новый ключ K и еще идентификатор Алисы, но при этом она зашифрована секретным ключом Трента и Боба EB. Все сообщение шифруется секретным ключом Алисы и Трента EA. и отправляется Алисе.

M1 = EA (NA, B, K, EB (K, A)).

* Алиса расшифровывает сообщение. Найдя в сообщении NA, она убеждается, что поговорила с Трентом. Вторую часть, зашифрованную EB она прочитать совершенно не способна, пересылает её Бобу.

M2 = EB(K, A).

* Боб получает и расшифровывает сообщение, достает оттуда новый ключ K и формирует сообщение для Алисы, в котором сообщает ей своё число NB, шифрованное новым ключом.

M3 = EK (NB).

* Алиса получает сообщение, достает оттуда NB, меняет его и отправляет обратно Бобу.

M4 = EK (NB- 1).[[3]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-3)

* Алиса и Боб владеют общим ключом K.

|  |  |
| --- | --- |
| [Ссылки 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) | **В этой статье не хватает**[**ссылок на источники информации**](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)**.**  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 поставлена под сомнение и удалена. Вы можете [отредактировать](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit) эту 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). Эта отметка установлена **28 февраля 2014 года**. |

### Протокол Kerberos[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=8) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=8)]

[Протокол Kerberos](https://ru.wikipedia.org/wiki/Kerberos) (англ. Kerberos Protocol) — это распределенная система [аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) (проверки подлинности), которая позволяет процессу (клиенту), запущенному от имени пользователя, доказать свою личность серверу без отправления данных по [сети](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D1%81%D0%B5%D1%82%D1%8C), которое может позволить злоумышленнику впоследствии выдавать себя за пользователя. Kerberos при необходимости обеспечивает целостность и конфиденциальность данных, передаваемых между клиентом и сервером.

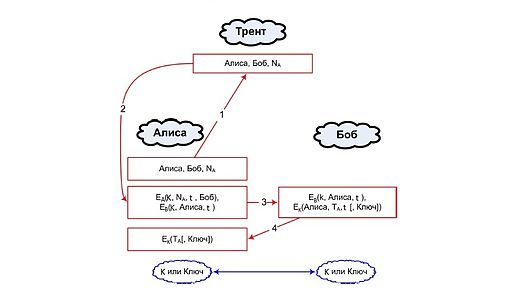
Kerberos был разработан в середине 80-х в рамках проекта [Athena](https://en.wikipedia.org/wiki/Project_Athena" \o "en:Project Athena) в [MIT](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D1%81%D0%B0%D1%87%D1%83%D1%81%D0%B5%D1%82%D1%81%D0%BA%D0%B8%D0%B9_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82).

Потому как использование Kerberos распространялось в различные среды, оказались необходимыми изменения для поддержки новых моделей использования. Для удовлетворения этих потребностей в 1989 году началась разработка Kerberos версии 5 ([Kerberos V5](https://ru.wikipedia.org/wiki/Kerberos" \l "Kerberos_5" \o "Kerberos)). И хотя версия 4 до сих пор работает на многих сайтах, пятая версия считается стандартом Kerberos.[[4]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-:1-4)

#### Описание работы Kerberos**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=9)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=9)**]**

##### Ситуация перед началом работы протокола**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=10)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=10)**]**

* 3 действующих лица: Алиса — клиент, Боб — сервер, которому Алиса хочет доказать свою подлинность, Трент — доверенный центр.
* У Алисы и Боба есть секретные ключи EA и EB соответственно для общения с Трентом.
* Алиса выбирает [число NA](https://ru.wikipedia.org/wiki/Nonce), а так же устанавливает [метку времени](https://ru.wikipedia.org/wiki/Timestamp) TA по своим часам.
* t — период валидности (lifetime), выбираемый Трентом.

[](https://commons.wikimedia.org/wiki/File:Kerberos_forwiki.jpg?uselang=ru)

Графическое описание работы Kerberos

##### Период работы протокола**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=11)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=11)**]**

* Алиса, запуская протокол, в открытом виде передает Тренту 3 вещи: свой и Боба идентификаторы, а так же выбранное число NA.

M0 = A, B, NA.

* Трент, получив сообщение от Алисы, генерирует ключ K для дальнейшего общения Алисы и Боба и передает обратно Алисе сообщение из двух частей. Первая часть зашифрована секретным ключом Алисы и содержит K, NA, период валидности t и идентификатор Боба. Вторая же часть неизвестна Алисе — она зашифрована секретным ключом Боба, и в ней содержится K, t и идентификатор Алисы.

M1 = EA(K, NA, t, B) , EB (K, A, t).

* Алиса расшифровывает первую часть принятого от Трента сообщения, получает ключ K и создает новый пакет для отправки Бобу, в который входят идентификатор Алисы, t и метка времени TA. После этого Алиса отправляет Бобу сообщение из двух частей: первая часть — это та, что пришла от Трента, а вторая — созданная Алисой.

M2 = EB (K, A, t), EK(A, TA, t).

* Боб принимает сообщение. Расшифровав первую часть, он достает новый ключ K, а затем, используя его, расшифровывает вторую часть. Чтобы подтвердить Алисе, что он знает новый ключ K, Боб отправляет ей сообщение с меткой времени, зашифрованное новым ключом K.

M3 = EK (TA).

* Алиса удостоверяется, что Боб — это Боб. Здесь применимы следующие рассуждения: Боб мог расшифровать сообщение от Алисы с меткой времени, только если он знал ключ K. А ключ K он мог узнать, только если знает EB. А так как это секретный ключ Боба и Трента, то приславший сообщение Алисе — Боб.
* Алиса и Боб готовы к обмену сообщениями, используя ключ K.[[5]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-:0-5)

#### Дополнения**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=12)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=12)**]**

##### The Kerberos Ticket**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=13)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=13)**]**

В специализированной литературе зачастую сообщение EB (K, A, t) называется ticket. Каждый раз, когда условная Алиса доказывает свою личность условному Бобу (ведь число пользователей в сети может быть гораздо больше, чем 2), она полагается на Трента ([доверенный центр](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8)), доверяя ему сгенерировать новый секретный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) и безопасно вручить его обоим пользователям. Новый секретный ключ K называется [сеансовым ключом](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B0%D0%BD%D1%81%D0%BE%D0%B2%D1%8B%D0%B9_%D0%BA%D0%BB%D1%8E%D1%87) (англ. [Session key](https://en.wikipedia.org/wiki/Session_key" \o "en:Session key)), и как раз Kerberos Ticket используется, чтобы доставить его Бобу. Kerberos Ticket является [сертификатом](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82), выданным доверенным центром и зашифрованным с помощью EB — общего ключа Боба и Трента. Среди прочей информации, билет содержит случайный сеансовый ключ, который будет использоваться для [аутентификации](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) Алисы Бобом, имя участника (в данном случае Алисе), которому сеансовый ключ был выдан, и срок действия, по истечении которого сеансовый ключ больше не действителен. Данный сертификат (Kerberos Ticket) не отправляется непосредственно Бобу, но вместо этого отправляется клиенту (Алисе), который направляет его для проверки Бобу в составе запроса. Так как сертификат шифруется на сервере ключом, известным только Тренту и Бобу, то изменить сертификат (Kerberos Ticket) для клиента (Алисы) не представляется возможным.[[4]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-:1-4)

### Протокол Отвея-Рииса[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=14) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=14)]

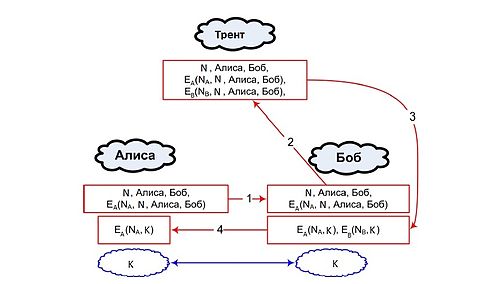
[Протокол Отвея-Рииса](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%9E%D1%82%D0%B2%D0%B5%D1%8F_%E2%80%94_%D0%A0%D0%B8%D0%B8%D1%81%D0%B0) (англ. The Otway-Rees Protocol) — протокол на симметричных ключах, позволяющий распределять ключи, не используя [метки времени](https://ru.wikipedia.org/wiki/Timestamp).

Повторимся, что перед началом работы протокола у нас есть:

* Доверенный центр Трент
* 2 пользователя: Алиса и Боб, которые получили EA и EB
* Алиса выбирает числа N и NA, Боб выбирает NB.

#### Описание работы протокола [**[6]**](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-6)**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=15)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=15)**]**

* Алиса формирует сообщение для Боба, в котором открытым текстом передает N, A, B, а также те же самые N, A, B с NA, зашифрованные общим с Трентом ключом EA.

[](https://commons.wikimedia.org/wiki/File:Otway_Rees.jpg?uselang=ru)

Графическое описание работы протокола Otway-Rees

M0 = N, A, B, EA(NA, N, A, B)

* Боб получает сообщение, вторая часть которого для него совершенно нерасшифровываема, добавляет в него еще одну строчку, которую шифрует ключом EB и отправляет Тренту.

M1 = N, A, B, EA(NA, N, A, B), EB(NB, N, A, B).

* Трент, зная оба ключа, может расшифровать сообщения Алисы и Боба. Теперь его цель — подтвердить, что он — Трент и сформировать ключ K для дальнейшего общения Алисы и Боба.

Трент генерирует ключ K и посылает Бобу сообщение.

M3 = EA (NA, K), EB (NB, K).

* Первую часть, зашифрованную ключом Алисы, Боб расшифровать совершенно не может, а вторую часть он спокойно расшифровывает и, считав, NB, удостоверяется, что сообщение пришло от Трента. Затем принимает сгенерированный ключ K. Теперь Боб готов к общению с Алисой, осталось только доставить ей ключ. Боб отправляет Алисе первую часть сообщения от Трента.

M4 = EA (NA, K).

* Алиса принимает сообщение, удостоверяется, что оно от Трента (NA), и считывает ключ K.
* Алиса и Боб готовы к общению.

#### Что в результате**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=16)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=16)**]**

Изящно получаем за 4 сообщения:

* Боб уверен, что поговорил с Трентом: Боб отправил ему число NB, шифрованное секретным ключом EB, и получил обратно другое сообщение, содержащее то же самое число и шифрованное тем же самым ключом.
* Алиса в свою очередь тоже уверена, что Боб поговорил с Трентом, потому что она послала своё число NA, шифрованное ключом EA, и получила обратно другое сообщение, но при этом тоже содержащим NA и шифрованное EA.
* У Алисы и Боба появился общий ключ K.

#### Проблема**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=17)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=17)**]**

* Алиса никак не может быть уверена, что Боб — это Боб. Она лишь уверена, что общается с неким лицом, которое может ходить к Тренту. Чтобы решить эту проблему на 4 шаге Боб может отправить Алисе не только EA (NA, K), но еще и, например, EK (NA, NB), доказывая тем самым, что он знает ключ K. А Алиса в свою очередь может ответить Бобу EK (NB), тоже доказывая, что знает ключ K.[[5]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-:0-5)

## **Асимметричные протоколы[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=18)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=18)**]**

основная статья: [**Криптосистема с открытым ключом**](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC)

### Протокол Нидхема-Шрёдера[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=19) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=19)]

[Протокол Нидхема-Шрёдера на асимметричных ключах](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%9D%D0%B8%D0%B4%D1%85%D0%B5%D0%BC%D0%B0_%E2%80%94_%D0%A8%D1%80%D1%91%D0%B4%D0%B5%D1%80%D0%B0#.D0.9F.D1.80.D0.BE.D1.82.D0.BE.D0.BA.D0.BE.D0.BB_.D0.9D.D0.B8.D0.B4.D1.85.D0.B5.D0.BC.D0.B0-.D0.A8.D1.80.D1.91.D0.B4.D0.B5.D1.80.D0.B0_.D0.B4.D0.BB.D1.8F_.D0.B0.D1.83.D1.82.D0.B5.D0.BD.D1.82.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.86.D0.B8.D0.B8_.D1.81_.D0.BE.D1.82.D0.BA.D1.80.D1.8B.D1.82.D1.8B.D0.BC_.D0.BA.D0.BB.D1.8E.D1.87.D0.BE.D0.BC) (англ. The Needham-Schroeder public-key protocol) был опубликован так же, как его симметричный родственник, в 1978 году. Это широко применяемая модель при изучении формальных методов проверки криптографических протоколов. Эта популярность очевидно идет от одной из самых успешных историй в этой области — в 1994 году протокол подвергся успешной атаке повтором (replay attack) спустя 16 лет после его публикования. Атаку произвел [David G. Lowe](https://en.wikipedia.org/wiki/David_G._Lowe" \o "en:David G. Lowe) — канадский ученый в области [Computer Science](https://en.wikipedia.org/wiki/Computer_science" \o "en:Computer science).[[7]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-7)

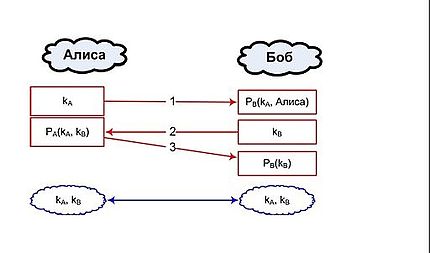
На сайте [Вурстерского политехнического института](https://ru.wikipedia.org/wiki/%D0%92%D1%83%D1%81%D1%82%D0%B5%D1%80%D1%81%D0%BA%D0%B8%D0%B9_%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B8%D0%B9_%D0%B8%D0%BD%D1%81%D1%82%D0%B8%D1%82%D1%83%D1%82" \o "Вустерский политехнический институт) (англ. [Worcester Polytechnic Institute](https://en.wikipedia.org/wiki/Worcester_Polytechnic_Institute" \o "en:Worcester Polytechnic Institute)) можно найти оригинальную статью, которую публиковал David G. Lowe [[8]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-8)

Данный протокол предоставляет взаимную передачу ключей kA и kB, а также взаимную аутентификацию.

#### Описание работы протокола**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=20)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=20)**]**

##### Ситуация перед началом работы**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=21)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=21)**]**

* У Алисы и Боба есть публичные процедуры кодирования PA и PB.
* Алиса и Боб хотят взаимно идентифицировать друг друга с помощью трёх сообщений и используя публичные ключи.

[](https://commons.wikimedia.org/wiki/File:NSPK_forwiki.jpg?uselang=ru)

Графическое описание работы протокола Нидхема-Шрёдера на открытых ключах

##### Период работы протокола**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=22)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=22)**]**

* Алиса выбирает свою часть ключа, kA, и формирует сообщение Бобу, в которое кладет свой идентификатор и kA. Все сообщение шифруется публичным ключом Боба PB и отправляется ему же.

M0 = PB (A, kA).

* Боб расшифровал сообщение и теперь знает, что с ним хочет поговорить Алиса, и для общения она хочет использовать ключ kA. Боб выбирает свою часть ключа, kB, и отправляет Алисе сообщение, состоящее из двух ключей kA и kB, зашифрованное открытым ключом Алисы. Тем самым Боб подтверждает Алисе, что получил часть её ключа KA.

M1 = PA (kA, kB).

* Теперь очередь Алисы доказать Бобу, что она — Алиса. Чтобы это сделать, она должна уметь расшифровывать сообщения, зашифрованные ключом PA. С чем она прекрасно справляется — она расшифровывает сообщение от Боба, забирает оттуда kA и отправляет Бобу сообщение, содержащее его ключ kB.

M2 = PB (kB).

* В результате на этапе сообщения M1 Алиса уверена, что Боб — это Боб, и Боб знает весь ключ. А на этапе сообщения M2 Боб уверен, что разговаривал с Алисой, и она знает весь ключ.[[5]](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-:0-5)

## **Наиболее широко известные атаки на криптографические протоколы**[**[9]**](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_note-9)**[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=23)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=23)**]**

### Подмена[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=24) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=24)]

Подмена (англ. Impersonation) — попытка подменить одного пользователя другим. Нарушитель, выступая от имени одной из сторон и полностью имитируя её действия, получает в ответ сообщения определенного формата, необходимые для подделки отдельных шагов протокола.

Методы противодействия состоят в:

* сохранении в тайне от противника информации, определяющей алгоритм идентификации;
* использование различных форматов сообщений, передаваемых на разных шагах протокола;
* вставка в них специальных идентификационных меток и номеров сообщений. В протоколах с использованием третьей стороны возможны атаки, основанные на подмене доверенного сервера.

Например, одна из сторон, имеющая доверительные отношения с сервером, выступает от его имени, подменяет его трафик обмена с другими сторонами и в результате получает возможность раскрывать значения генерируемых центром ключей.

### Атака повтором[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=25) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=25)]

[Атака повтором](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B2%D1%82%D0%BE%D1%80%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B2%D0%BE%D1%81%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F) (англ. [Replay attack](https://en.wikipedia.org/wiki/Replay_attack" \o "en:Replay attack)) — повторное использование ранее переданного в текущем или предыдущем сеансе сообщения или  его части в текущем сеансе протокола.

Например, повторная передача информации ранее проведенного протокола идентификации может привести к повторной успешной идентификации того же самого или другого пользователя.

В протоколах передачи ключей данная атака часто применяется для повторного навязывания уже использованного ранее сеансового ключа — атака на основе новизны (freshness attack).

Методы противодействия состоят в обеспечении целостности сеанса и невозможности вставки в него лишних сообщений. Для этого используется вставка в передаваемые сообщения [временных меток](https://ru.wikipedia.org/wiki/Timestamp) или [случайных чисел](https://ru.wikipedia.org/wiki/Nonce), а также идентификаторов сторон.

### Комбинированная атака[[править](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=26) | [править код](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=26)]

Комбинированная атака (англ. interleaving attack) — подмена или другой метод обмана, использующий комбинацию данных из ранее выполненных протоколов, в том числе протоколов, ранее навязанных противником.

Метод противодействия состоит в обеспечении целостности сеансов протоколов и отдельных сообщений.

## **Примечания[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=27)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=27)**]**

1. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-1) *Pablo Giambiagi.* Secrecy for Mobile Implementations of Security Protocols. — 2001. — С. 36. — [ISSN](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BD%D1%8B%D0%B9_%D1%81%D0%B5%D1%80%D0%B8%D0%B9%D0%BD%D1%8B%D0%B9_%D0%BD%D0%BE%D0%BC%D0%B5%D1%80) [1403-5286](https://www.worldcat.org/search?fq=x0:jrnl&q=n2:1403-5286).
2. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-2) *John Kelsey, Bruce Schneier, David Wagner.* Protocol Interactions and the Chosen Protocol Attack. — 1997. — С. 8. — [ISSN](https://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9_%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BD%D1%8B%D0%B9_%D1%81%D0%B5%D1%80%D0%B8%D0%B9%D0%BD%D1%8B%D0%B9_%D0%BD%D0%BE%D0%BC%D0%B5%D1%80) [0302-9743](https://www.worldcat.org/search?fq=x0:jrnl&q=n2:0302-9743).
3. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-3) *Alexei Lisitsa.* [Needham-Schroeder authentication protocol and its formal analysis](http://cgi.csc.liv.ac.uk/~alexei/COMP522_10/COMP522-Needham-Schroeder-05.pdf).
4. ↑ [Перейти обратно:***1***](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-:1_4-0) [***2***](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-:1_4-1) *B. Clifford Neuman and Theodore Ts'o.* [<http://www.isi.edu/div7/publication_files/kerberos_an_auth.htm> Kerberos: An Authentication Service for Computer Networks] (недоступная ссылка). IEEE Communications Magazine (1994). Дата обращения: 15 декабря 2014. [Архивировано](https://web.archive.org/web/20130526063637/http:/www.isi.edu/div7/publication_files/kerberos_an_auth.htm) 26 мая 2013 года.
5. ↑ [Перейти обратно:***1***](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-:0_5-0) [***2***](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-:0_5-1) [***3***](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-:0_5-2) *Сергей Николенко.* [Ключи и протоколы для них](http://logic.pdmi.ras.ru/~sergey/teaching/cscryp09/06-keyagreement.pdf) (Осень 2009).
6. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-6) *Dr. Geoff Hamilton.* [Key Exchange and Authentication Protocols](http://computing.dcu.ie/~hamilton/teaching/CA547/notes/Protocols.pdf) (недоступная ссылка). Дата обращения: 14 декабря 2014. [Архивировано](https://web.archive.org/web/20141214232135/http:/computing.dcu.ie/~hamilton/teaching/CA547/notes/Protocols.pdf) 14 декабря 2014 года.
7. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-7) *Olivier Michel.* [An Analysis of the Needham-Schroeder Public-Key Protocol with MGS](http://psystems.disco.unimib.it/procwmc5/REGMichel.pdf).
8. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-8) *Gavin Lowe.* [An attack on the Needham-Schroeder public-key authentication protocol](http://web.cs.wpi.edu/~cs564/f12/papers/lowe95.pdf) (1995).
9. [↑](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9#cite_ref-9) *А.В. Черемушкин.* [Криптографические протоколы: основные свойства и уязвимости](http://sun.tsu.ru/mminfo/000349342/P_02/image/P_02_115.pdf) (Ноябрь 2009).

## **Литература[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=28)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=28)**]**

*Alfred J.Menezes, Paul C. van Oorschot, Scott A. Vanstone.* Handbook of Applied Cryptography. — 1996. — С. 489-534. — 816 с. — [ISBN 0-8493-8523-7](https://ru.wikipedia.org/wiki/%D0%A1%D0%BB%D1%83%D0%B6%D0%B5%D0%B1%D0%BD%D0%B0%D1%8F:%D0%98%D1%81%D1%82%D0%BE%D1%87%D0%BD%D0%B8%D0%BA%D0%B8_%D0%BA%D0%BD%D0%B8%D0%B3/0849385237).

## **Ссылки[**[**править**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&veaction=edit&section=29)**|**[**править код**](https://ru.wikipedia.org/w/index.php?title=%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D1%80%D0%B0%D1%81%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9&action=edit&section=29)**]**

* *Сергей Николенко.* [Криптографические протоколы](https://www.lektorium.tv/course/22759). Лекториум. ([Материалы курса](https://web.archive.org/web/20141216025511/http:/logic.pdmi.ras.ru/csclub/courses/cryptoprotocols))
* *Dr. Bill Young.* [Introduction to Computer Security](https://www.cs.utexas.edu/~byoung/cs361/syllabus361.html) (англ.). Texas University (2014). — Курс лекций по компьютерной безопасности, в том числе и по криптографическим протоколам.