Мне нечего скрывать

Лукавите.
Говоря это, Вы говорите, что знаете будущее
и что может пойти не так.

Времена *целевой* слежки закончились.
Добро пожаловать в мир *массовой* слежки.

Массовая слежка
=
слежка за всеми

Безопасность

То, что находится между представлением того, как работают вещи и как они работают *на самом деле*.

Безопасность - не что-то, что можно купить, скачать или установить

Безопасность - это процесс

Интернет

Интернет вошел в нашу жизнь

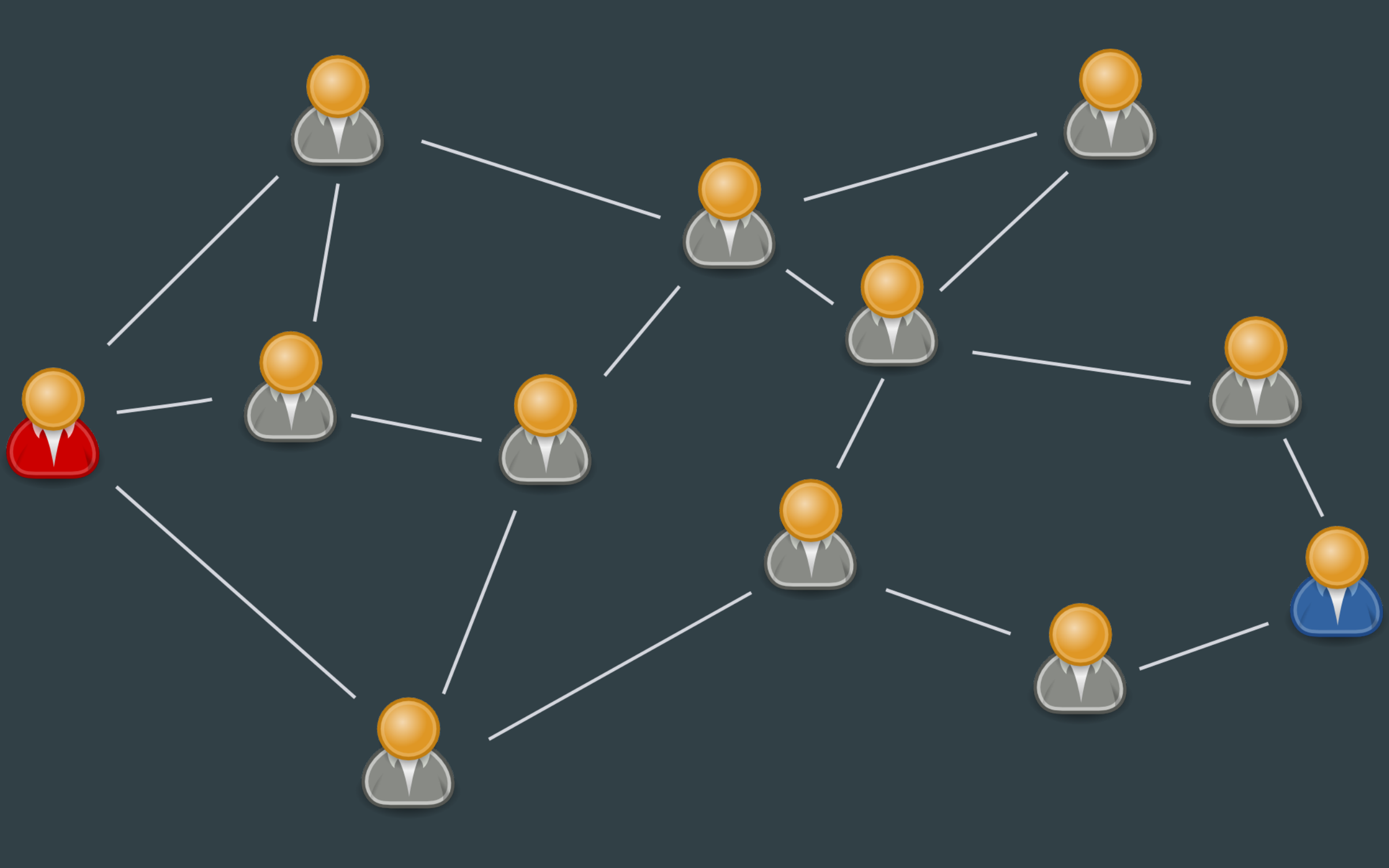
Классно, но что это за штука такая?

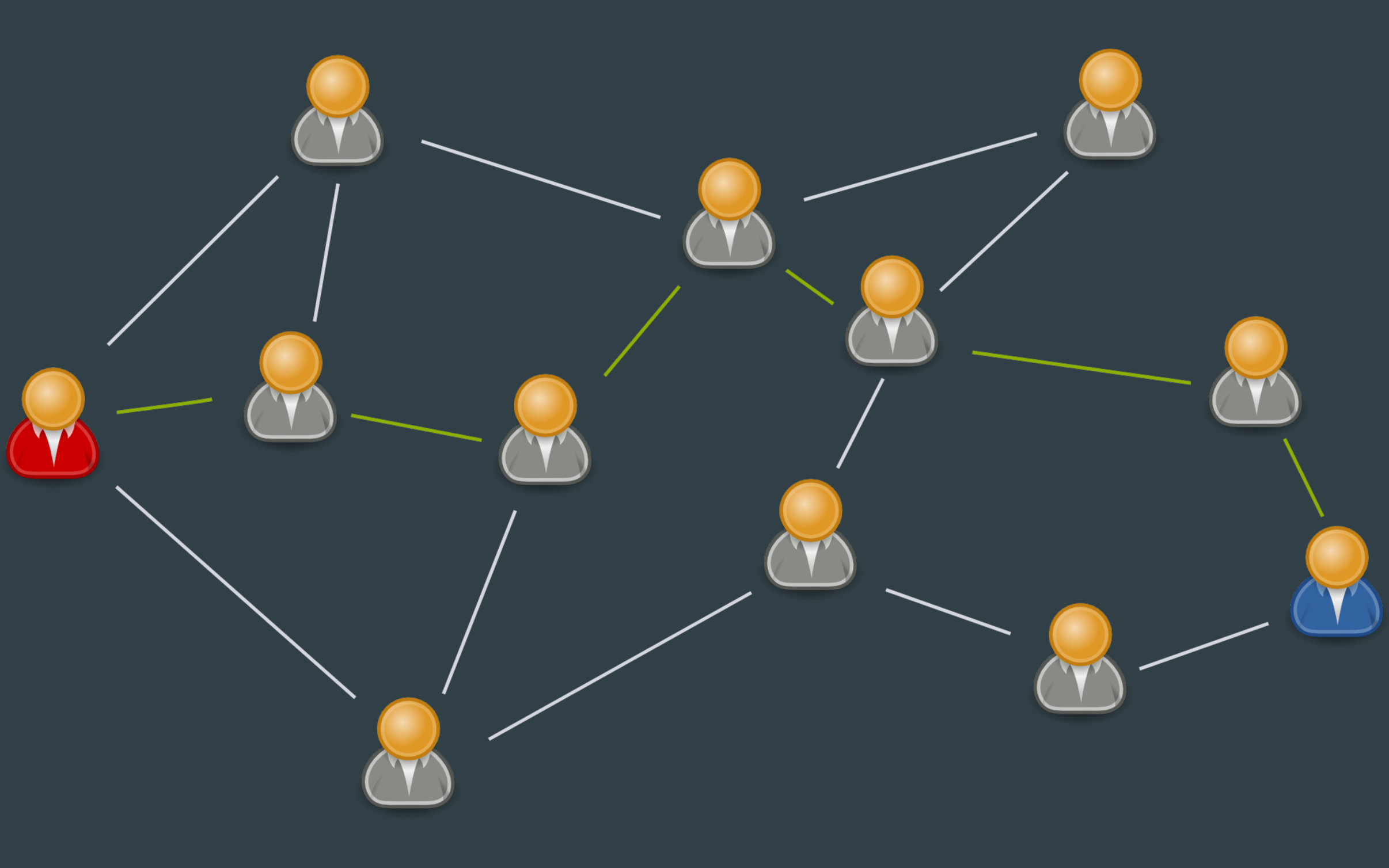
Как передается информация через Интернет?

Интернет - сеть сетей

Передача из одной сети в другую

Через множество посредников





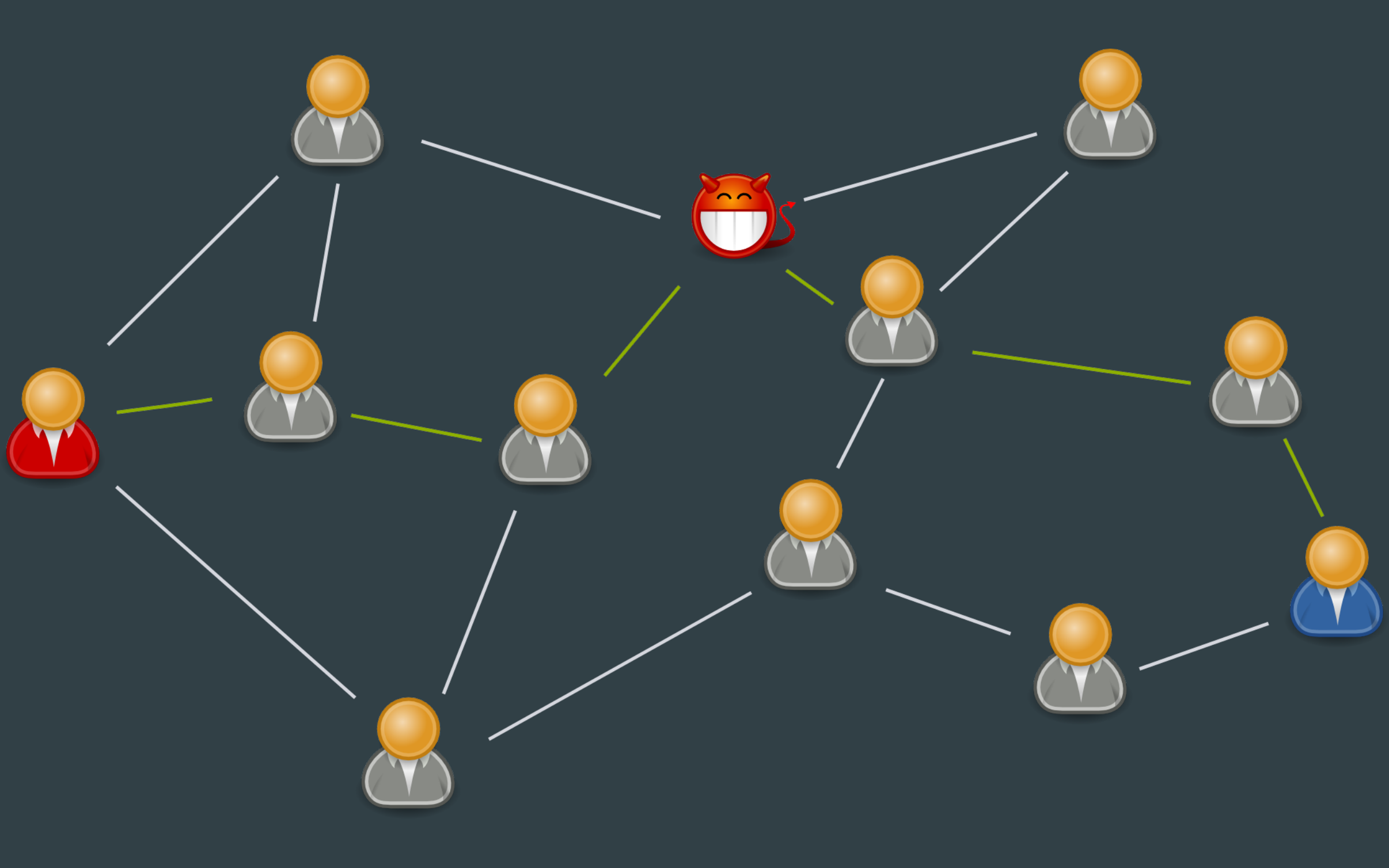
Отлично!
У нас есть Интернет!

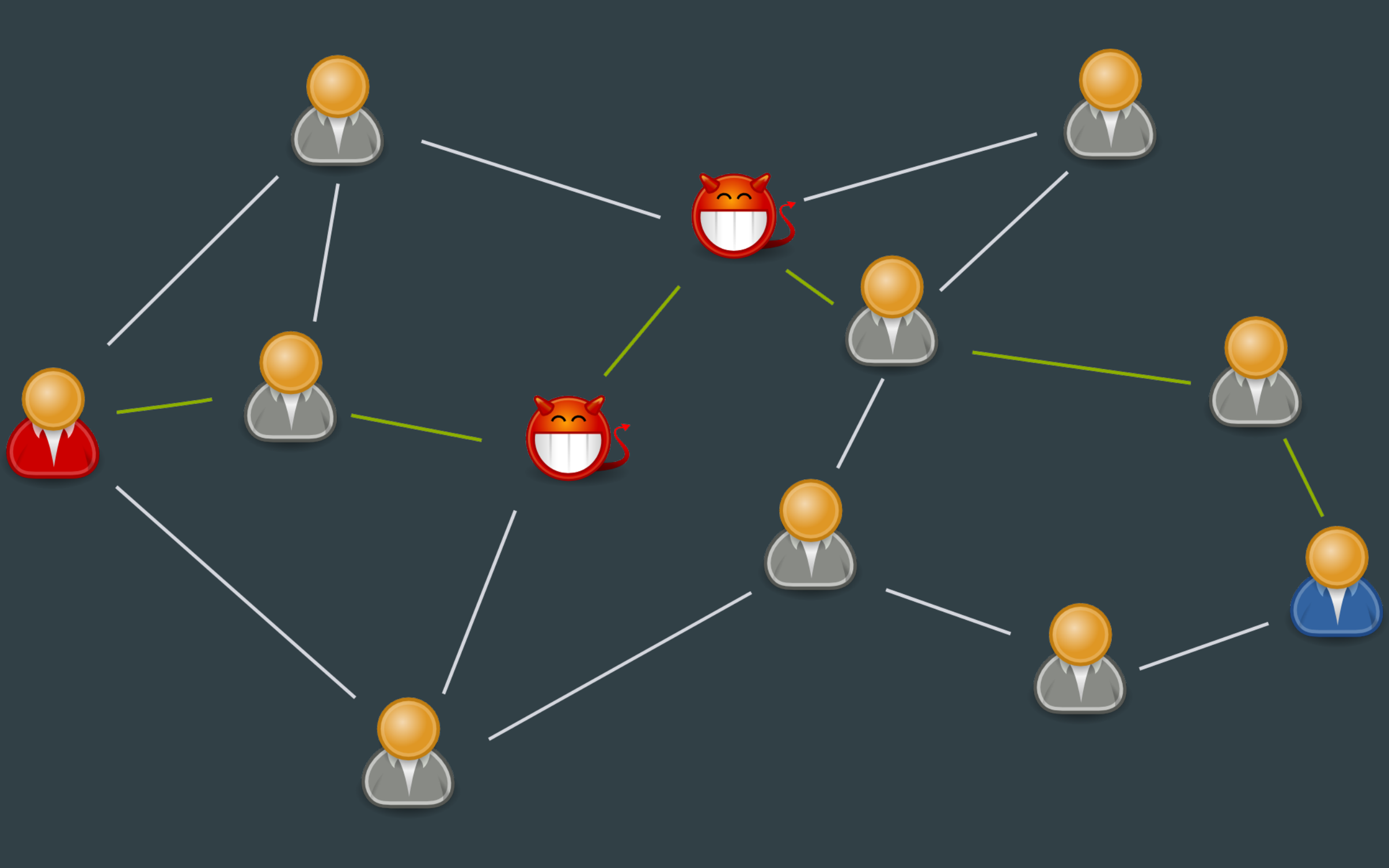
Подождите...

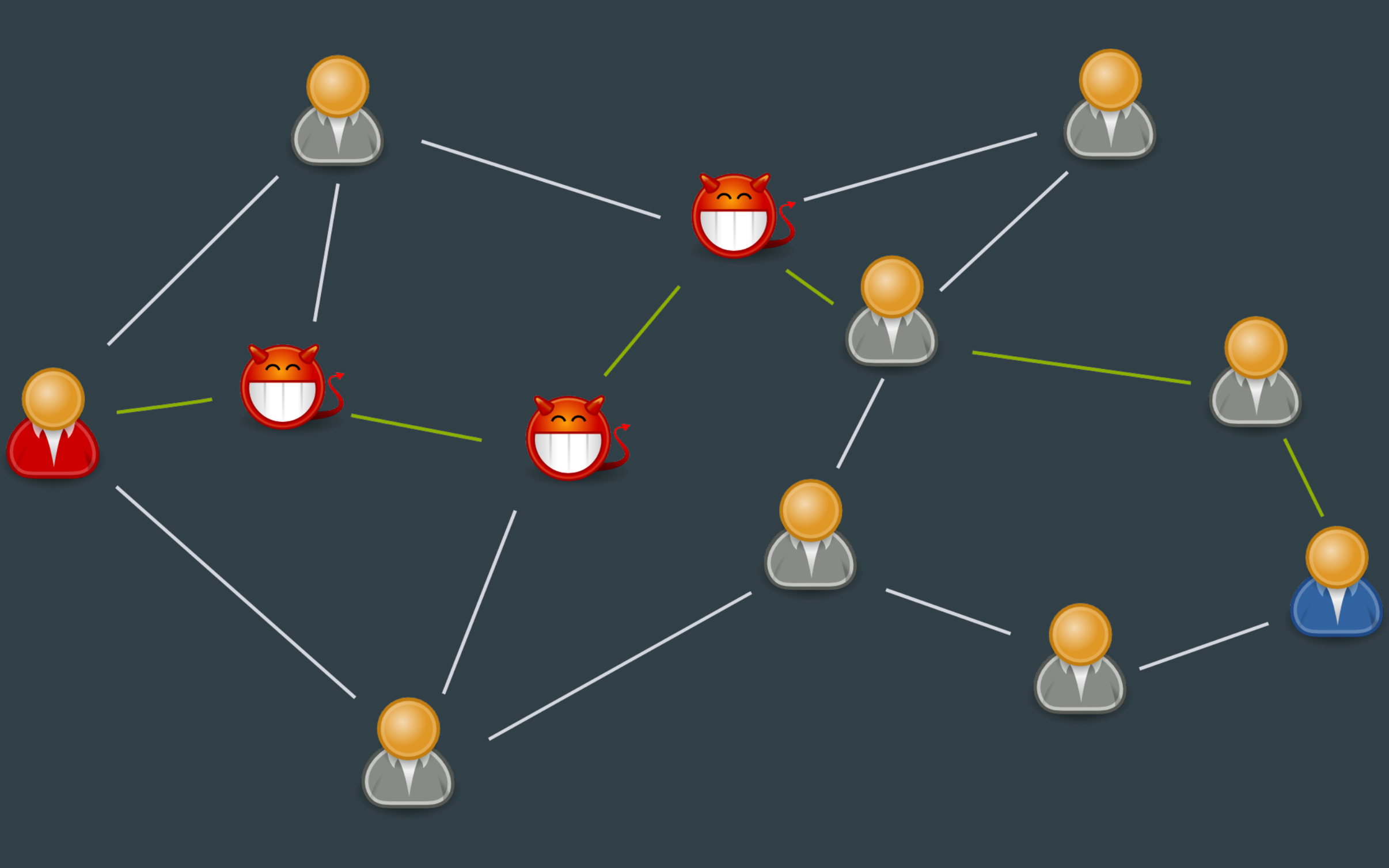
Кто все эти посредники?

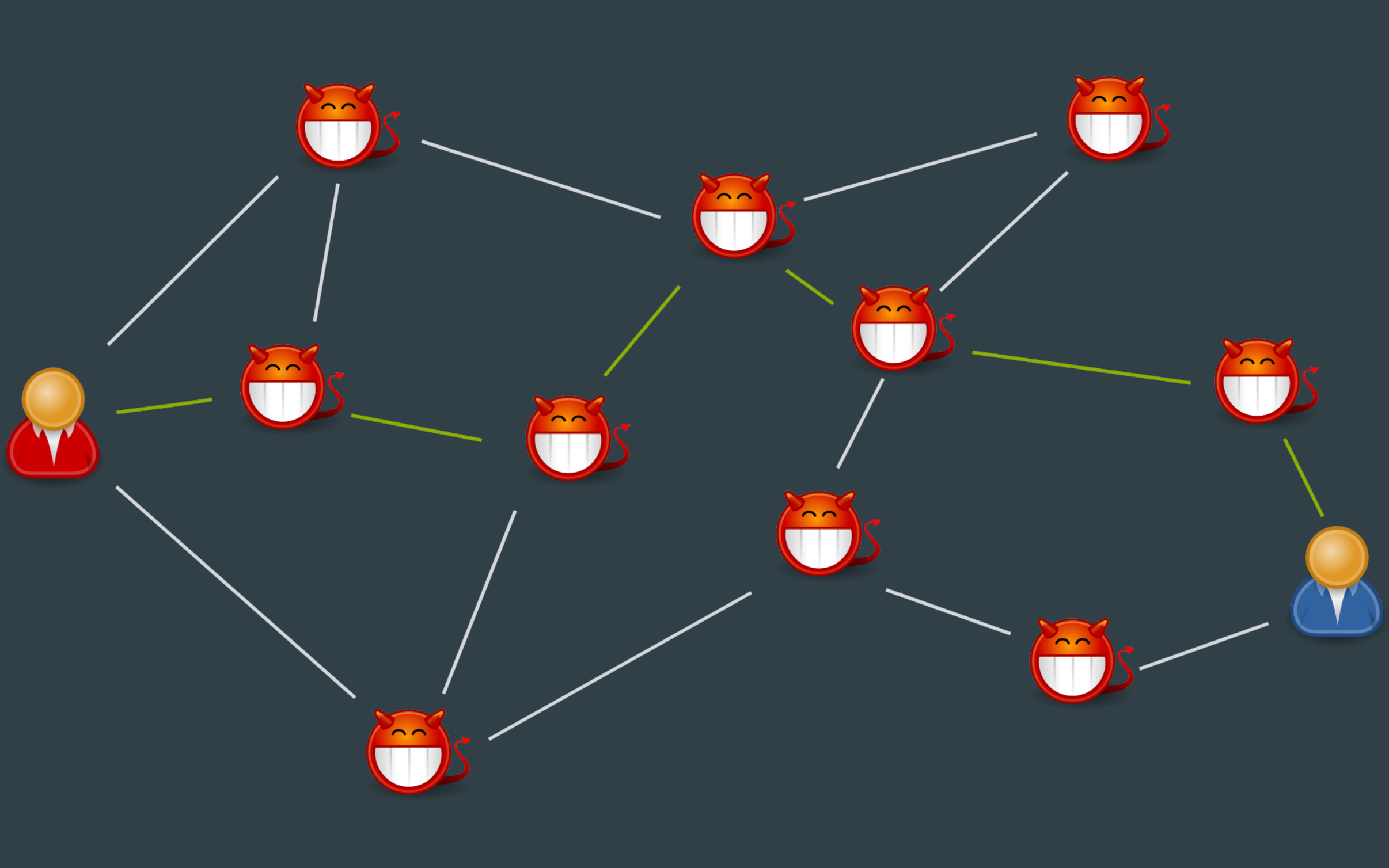
Интернет - сеть, построенная на доверии

Которого нет.









Посредниками могут быть *кто-угодно*

Как же быть?

Нам нужна Криптография

Криптография -
методы безопасных коммуникаций

Что такое шифрование?

Методы превращения полезной информации в шум

Шум, в котором никто не разбирается, кроме Вас

было: cu at cryptoparty
стало: 9d23fb0afafa37a57dafa

”Шифрование - это сложно”

Компьютеры - это тоже сложно, но вы ими пользуетесь

пользоваться

≠

разбираться

”Шифрование - для террористов и военных”

Так же как и ножи - для убийц и маньяков

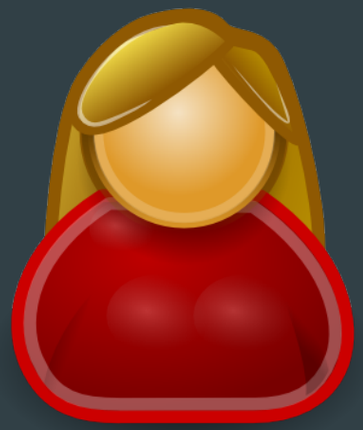
Шифрование - инструмент.
Не более, не менее.

Какое бывает шифрование?

Симметричное

Единый ключ на зашифровку и на расшифровку

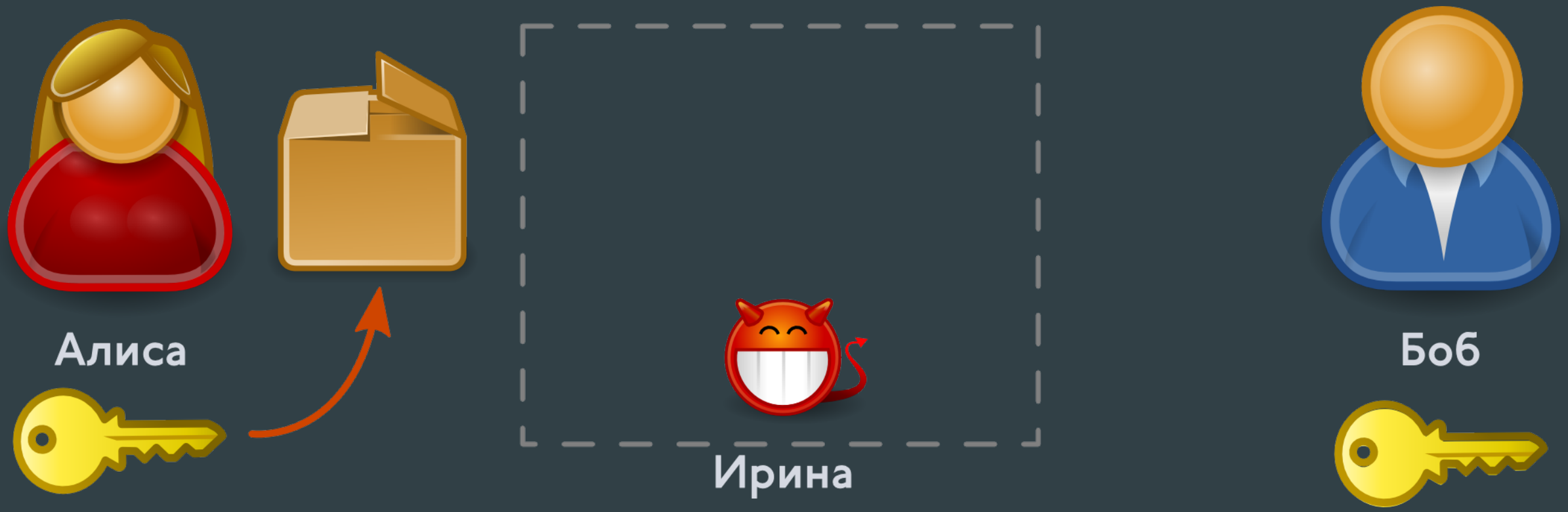
Почтовая аналогия

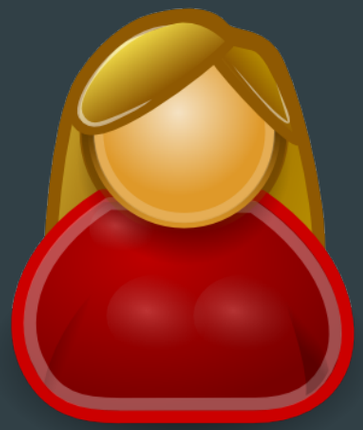


Алиса

Ирина

Боб

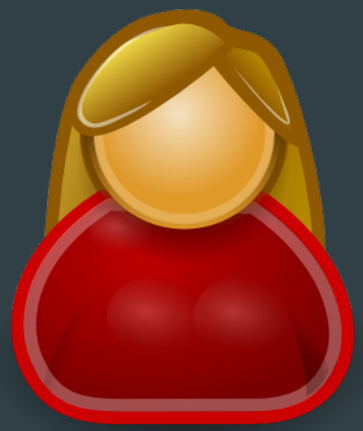

Алиса
Ирина
Боб



Алиса

Ирина

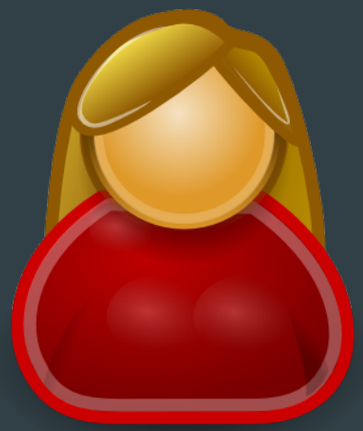
Боб



Алиса

Ирина

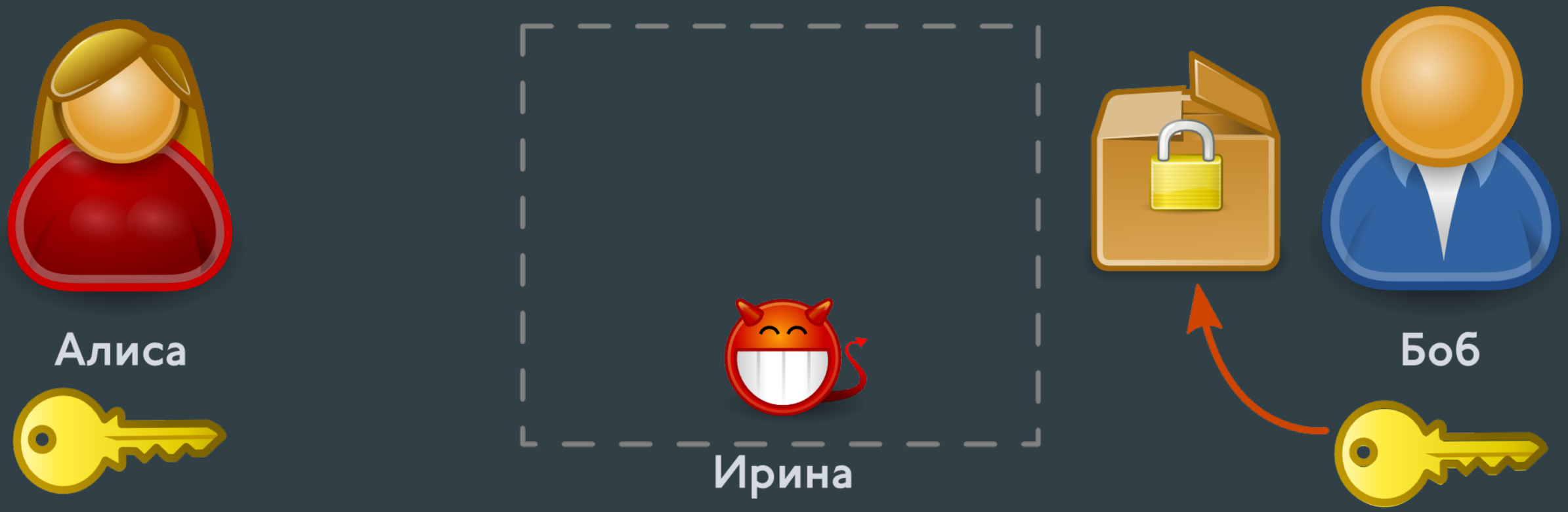
Боб

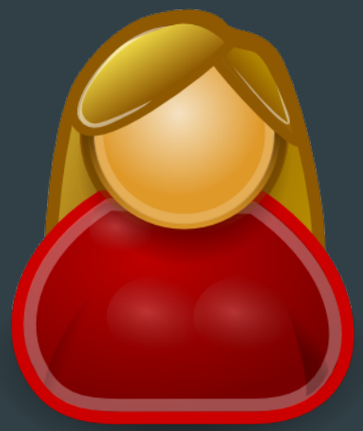


Алиса

Ирина

Боб


Алиса
Ирина
Боб



Алиса

Ирина

Боб

Например, симметричный ключ выглядит так:
e3594d0ce14fd79425921123d8ec81ea

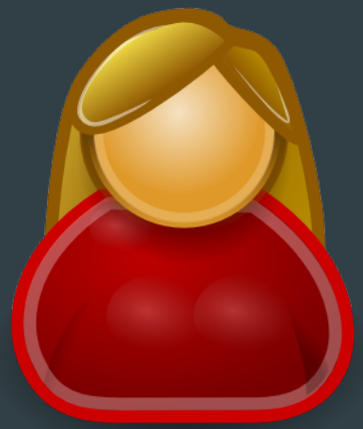
Да, но что, если Алиса не может встретится с Бобом и передать ключ?

Асимметричное

Криптосистема с публичным ключом

Публичный ключ
для зашифровки
Закрытый ключ
для расшифровки

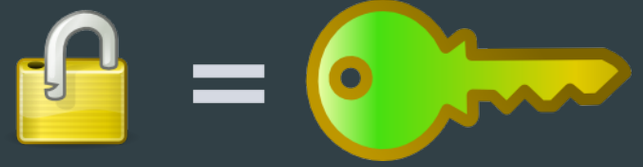
Почтовая аналогия

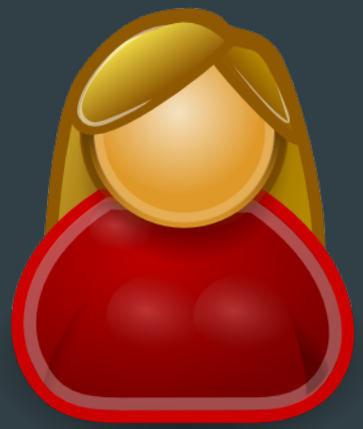


Алиса

Ирина

Боб

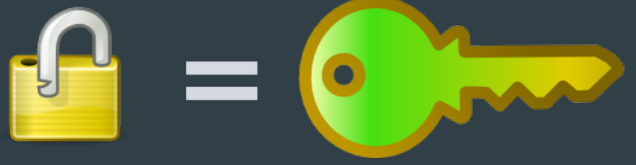


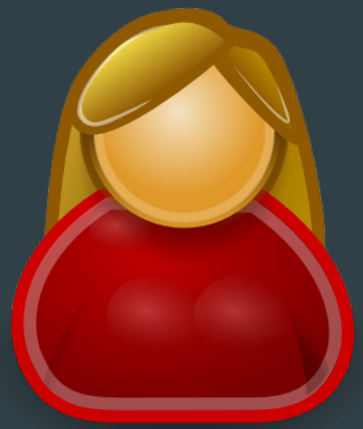


Алиса

Ирина

Боб

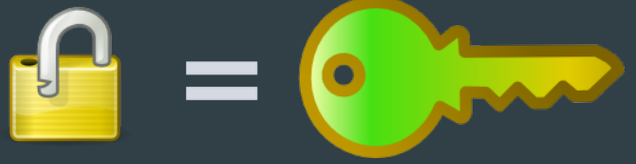


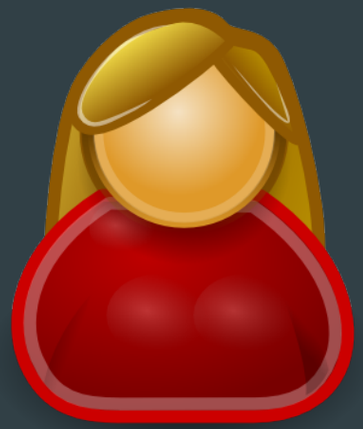


Алиса

Ирина

Боб

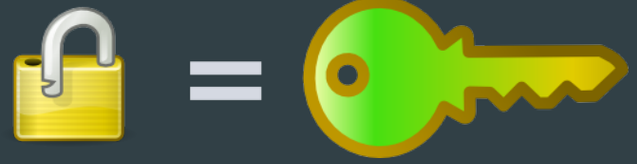


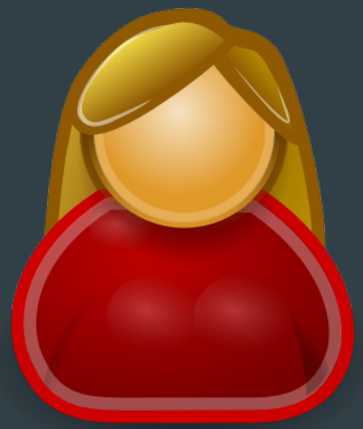


Алиса

Ирина

Боб

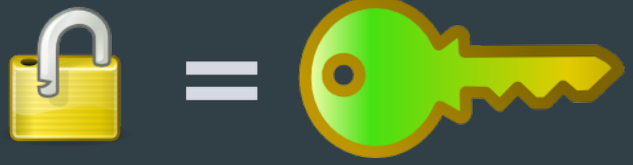


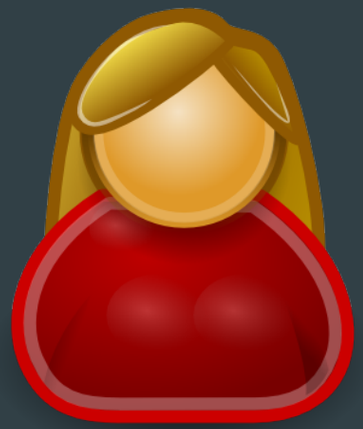


Алиса

Ирина

Боб

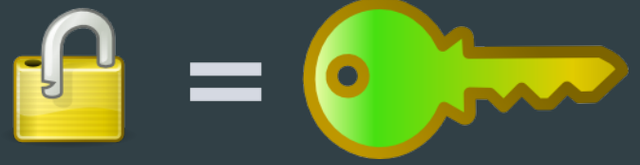


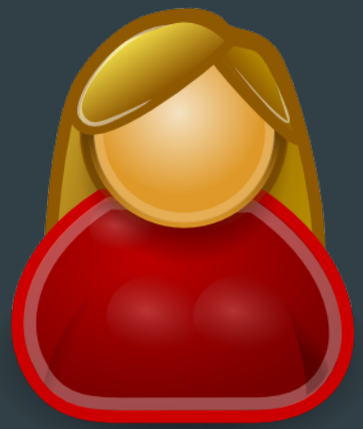


Алиса

Ирина

Боб

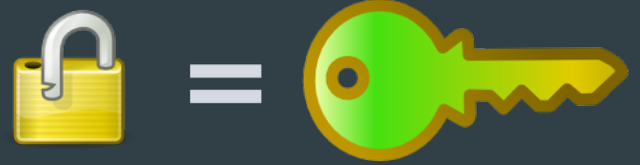


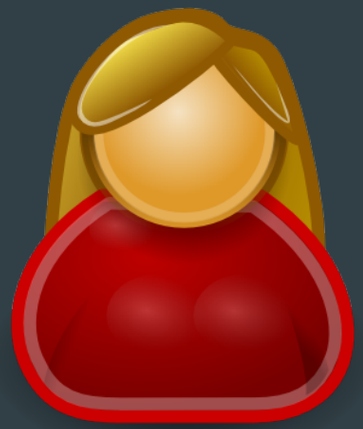


Алиса

Ирина

Боб

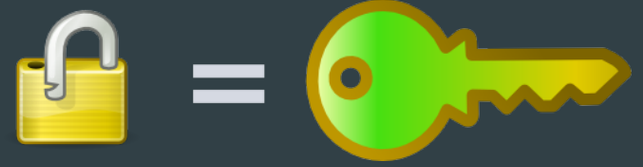




Алиса

Ирина

Боб



Например, публичный ключ выглядит так:

-----BEGIN PGP PUBLIC KEY BLOCK-----
mI0EV+8yFwEEAOygoNBKEPl/SiNxPb3Uq5W75cX9B2TmwYagLboifZdiCxozj7XX
b39QPmjeHnoxWKYGSfshGbKGW+RpqjNJkUwyjlJp5lH70Kj3JjLy36h3fJ963vcg
Ur0UKyTn+QIs5ePogSVyHhfC45RPwkZRmd4/HPhMBuNDFUIw/AN0XRYfABEBAAG0
C0NyeXB0bIBhcnR5iLgEEwECACIFAlfvMhcCGwMGCwkIBwMCBhUIAgkKCwQWAgMB
Ah4BAheAAAoJEIwmVKbI7KOs/UAD/IaZYs7gaEUtnhERkh05mRIH8xTDnPFdIdv9
bTiqrdtyIOLnSuI7P8XoUvxjkvlyI/NMgENS8WOYXK+iDXvikZ9MqnRjhM/NErNI
05apOJ0/JoTw+Ks0bUhUcfZSbjNOC0VakNKY74HEKffV3e+c/iglJzUAyEkM+sIM
A+d0XwZx
=3/wJ
-----END PGP PUBLIC KEY BLOCK-----

Например, закрытый ключ выглядит так:

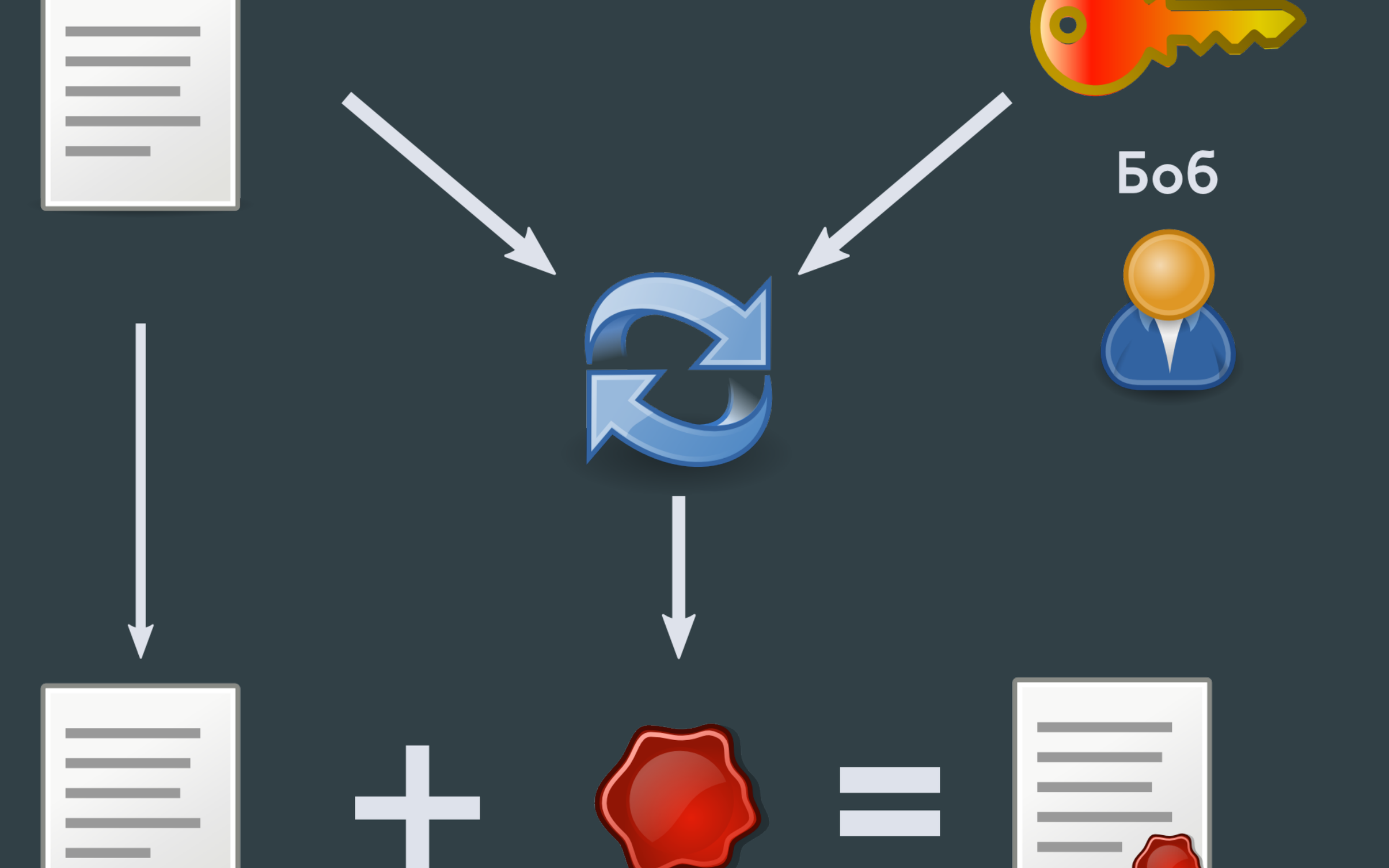
-----BEGIN PGP PRIVATE KEY BLOCK-----
lQHYBFfvMhcBBADsoKDQShD5f0ojcT29IKuVu+XF/Qdk5sGGoC26In2XYgsaM4+I
I29/UD5o3h56MVimBkn7IRmyhlvkaaozSZFMMo5SaeZR+9Co9yYy8t+od3yfet73
IFK9FCsk5/kCLOXj6IElch4XwuOUT8JGUZnePxz4TAbjQxVNcPwDdF0WHwARAQAB
AAP/XlSShzZfmfbCiWqFYH29gU2Mhece4XyUPaTxVbiWNJkjL+jKK4WcrzZACvlx
WCj/2/+50mEZq2+ghmgRL6zuPJvP38K7HY+jg5f4S87RjkIR2rP+P0X775xCNI++
v4BvJDmA98+lWEZ9DojUI8x005TMSHPfb05ah94sLWoXjyECAPIRJQRJCM7oFRrb
MkTiYBVOHjHB3O+o2KIVqirnV3n4zrfMBSBUnpRcpZ3YxHqII2Hvis9kmNDfoDBj
28LLTKkCAPo/VRNbFUs8Edtad5XaCSdoYC/r+p3UG+d5QMojpRojk5YIxRZ+ZZEC
nupThcr9CYNnREqucv6+Z7vSbAbjAYcB/RGSJOjflHQ05o+bNYaU9JeOSZ9AySoo
TeKL9b/rpS+czkzL3eyWTm97kM3bce7OeVSTP5LhOkdKHe+/jHm5RE6ni7QLQ3J5
cHRvUGFydHmluAQTAQIAIgUCV+8yFwIbAwYLCQgHAwIGFQgCCQoLBBYCAwECHgEC
F4AACgkQjCZUpvXso6z9QAP/VplizuBoRS2eERGSHTmZEgfzFMOc8V0h2/ItOKqt
23Ig4udK7Xs/xehS/GOS+XLX80yAQILxY5hcr6INe+KRn0yqdGOEz80Ss0jTlqk4
nT8mhPD4qzRtSFRx9lJuM04LRVqQ0pjvgcQp99Xd75z+KDUnNQDISQz6zUwD53Rf
BnE=
=972B
-----END PGP PRIVATE KEY BLOCK-----

Существует обратная операция - ”шифрование” закрытым ключом

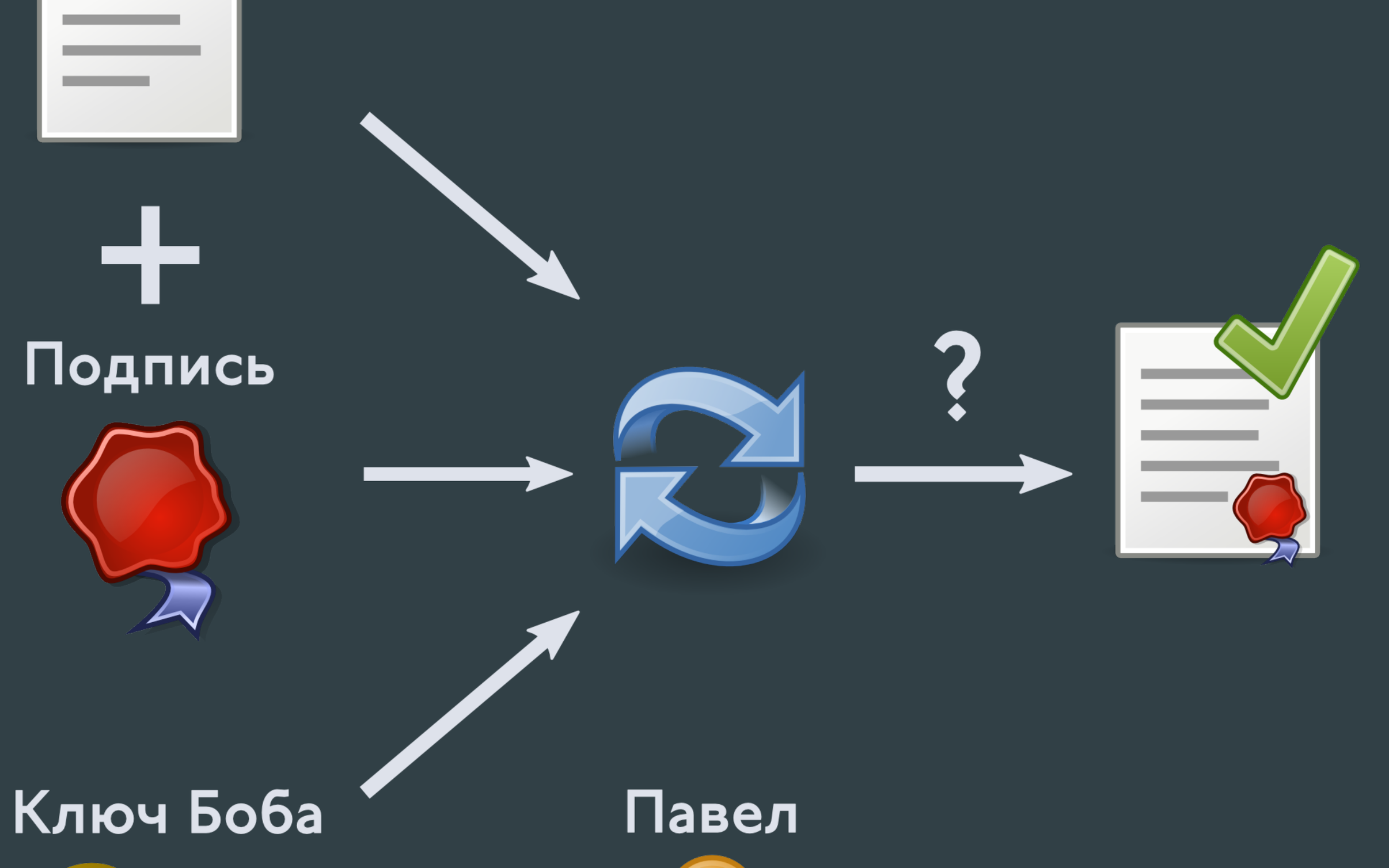
Цифровая подпись

Только Боб может создать подпись сообщения, которая связана только с этим сообщением. Её можно проверить с помощью публичного ключа Боба.

Создание подписи


Боб

Проверка подписи


Подпись
?
Ключ Боба
Павел

Например, подписанный документ выглядит так:

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

OMG, Im at CryptoParty. Such privacy! So encryption! Yay!
-----BEGIN PGP SIGNATURE-----
iJwEAQEIAAYFAlfvNH8ACgkQjCZUpvXso6zBDQP/aMKOEGTMOci5Io6Za+8s+/CO
WNHDedc/xAwXpGYGAgf4VGLqES+/CIvz/OIO0k8GsWkSeTYqlZKBvKwleio6pIAK
A2wN9zeOeQ6lCOsGoE38/CVuKsXT5J6toPH6t/0lC8NNg9fVlOQfsPwtAalju9Nx
XCgi+xFShMCm9kHJv3o
==MOAJ
-----END PGP SIGNATURE-----

А что, если замок прислал *не Боб*?

Надо убедиться, что это его ключ

Ручная проверка публичных ключей

Можно попросить кого-то подписать публичный ключ

Если вы доверяете им

Отпечаток ключа

Fingerprint

Короткий ”эквивалент” публичного ключа. Если отпечатки публичных ключей совпадают, значит совпадают и эти ключи.

Например, отпечаток ключа выглядит так:

4I5E 86BB A956 ID0C E5A5 2B95 8C26 54A6 F5EC A3AC

Сквозное шифрование

Собеседники сами генерируют свои ключи

Содержимое доступно только им

Forward Secrecy

Прямая секретность

При компрометации закрытого ключа предыдущие сообщения не поддаются расшифровке

Хорошо,
мы используем
шифрование

Содержание передаваемых нами данных неизвестно

Неужели этого недостаточно?

Метаданные

данные о данных

Размер, время передачи, место отправки, получатель, источник...

”Метаданные мало, что дают, собирайте, сколько хотите”

Метаданные несут огромную опасность

”Мы убиваем людей на основе метаданных” -

Майкл Хайден, директор АНБ (1999-2005)

Наиболее интересны

Универсальны

Не зависят от языка

Малый объем

Из них можно узнать больше, чем из самих данных

Любимые места, заболевания, пристрастия, социальные связи, настроение, планы на будущее...

Теперь с обязательным хранением

по закону - ”до трех лет”

Важность свободного ПО

Доступность всех деталей и исходного кода

Отсутствие ограничений на использование

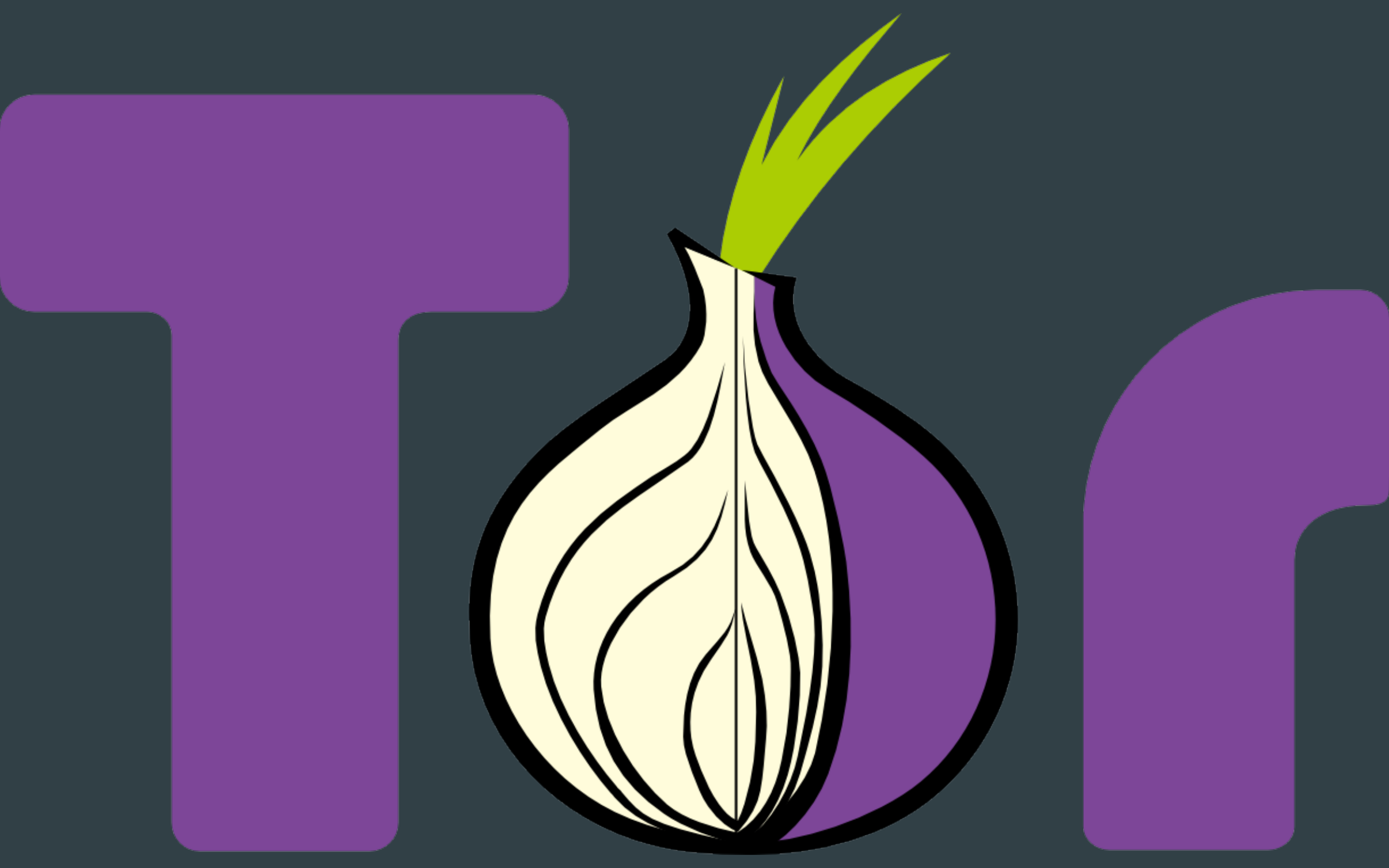
Проверяемость

очень сложно встроить лазейки

Независимость

Основные инструменты защиты приватности

Защита метаданных, сетевой активности и обход цензуры


Tor

The onion router

Луковичный маршрутизатор

Луковичная маршрутизация

Маршрут выбирает пользователь, а не операторы сети

”Не существует вездесущего наблюдателя” предположение

Никто не может контролировать *все* узлы

(S//REL) Very Secure

(S//REL) Low enough latency for most *TCP* uses

(S//REL) Still the King of high secure, low latency Internet Anonymity

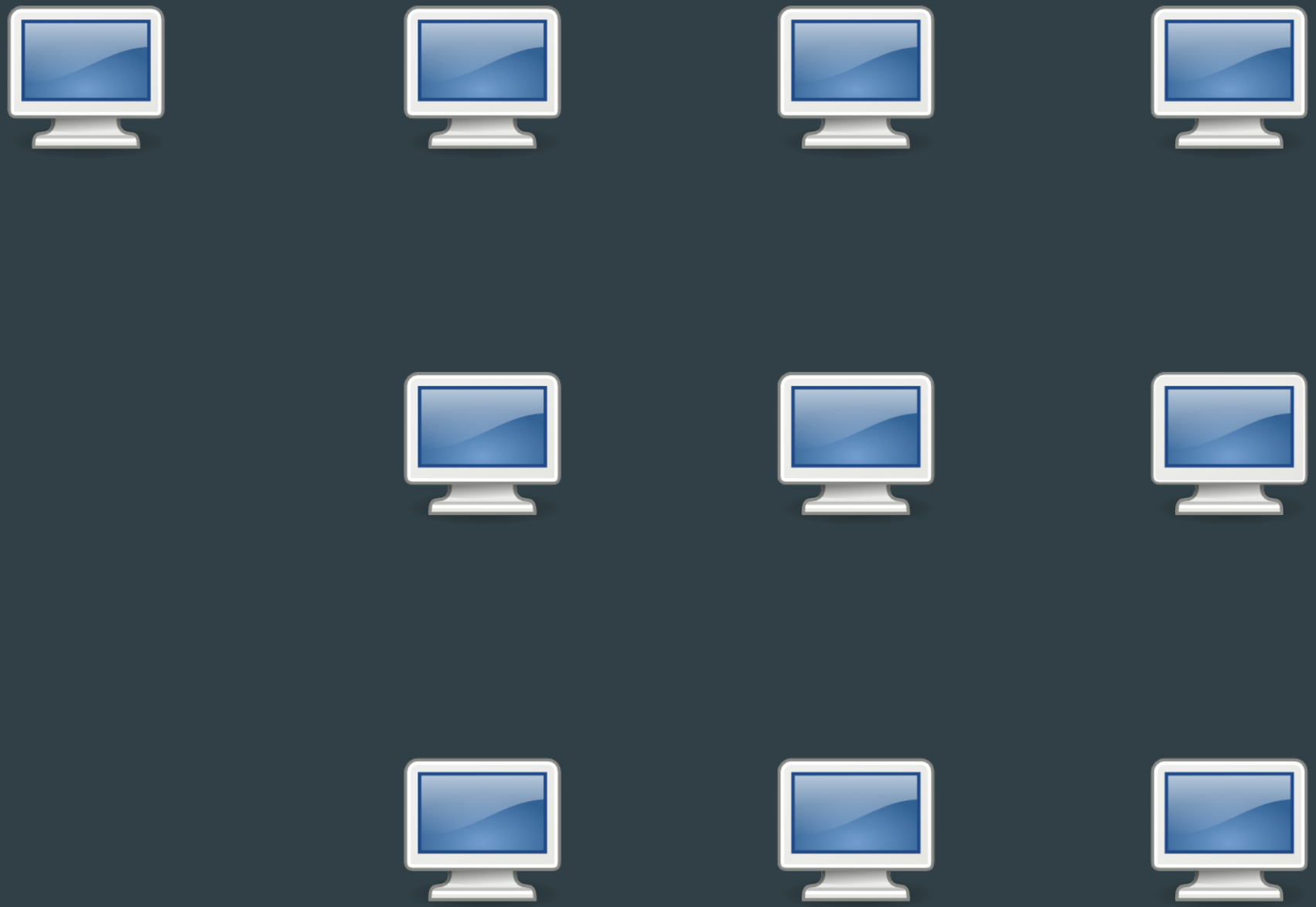
- (S//REL) There are no contenders for the throne in waiting

Как устроен Tor?

Без Tor

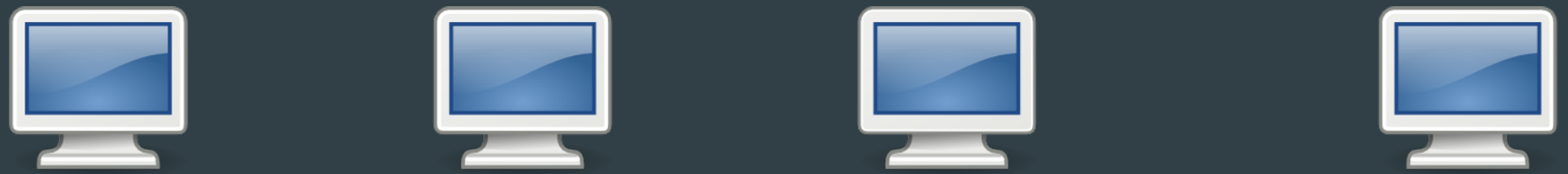
Алиса

Алиса



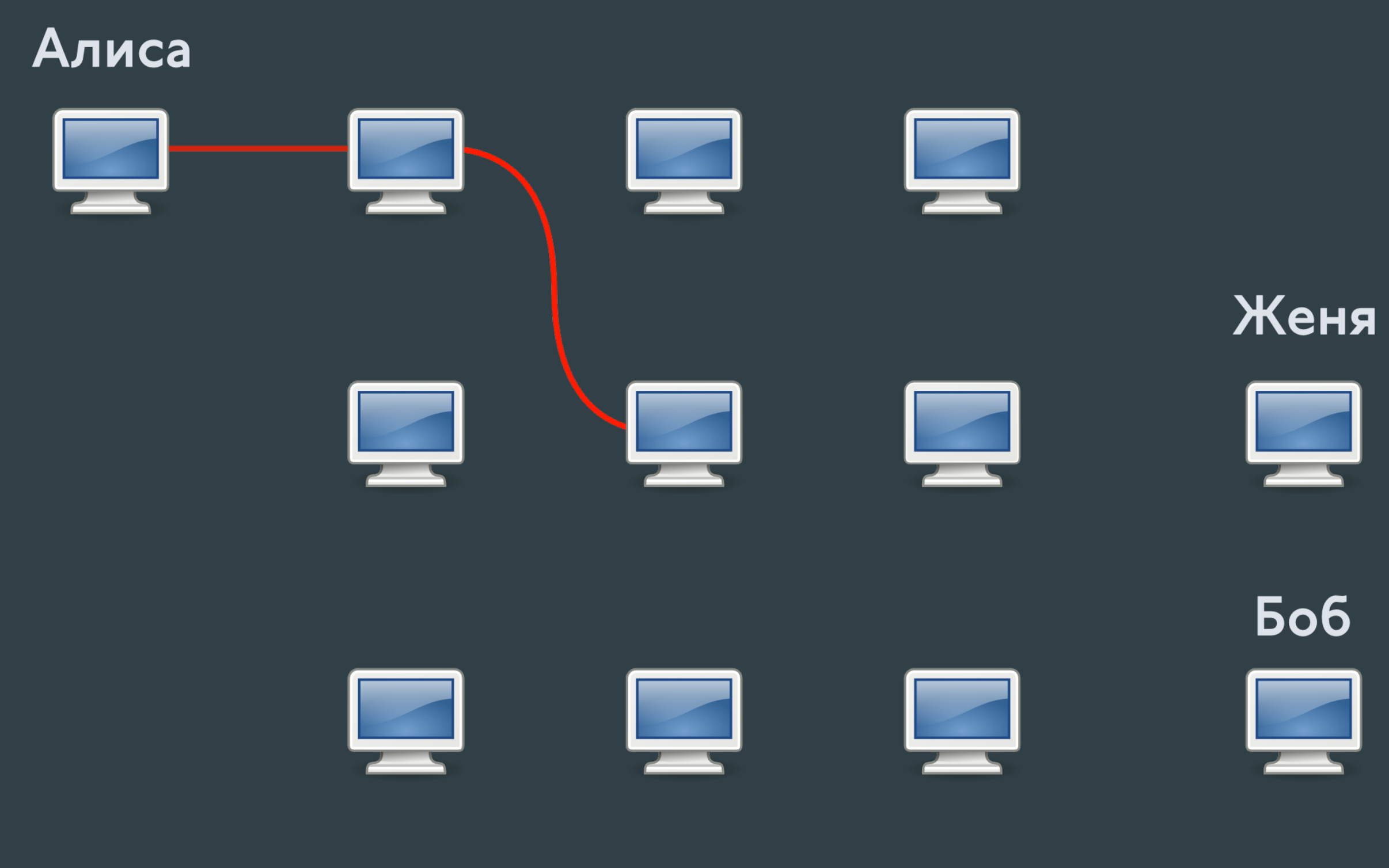
Алиса

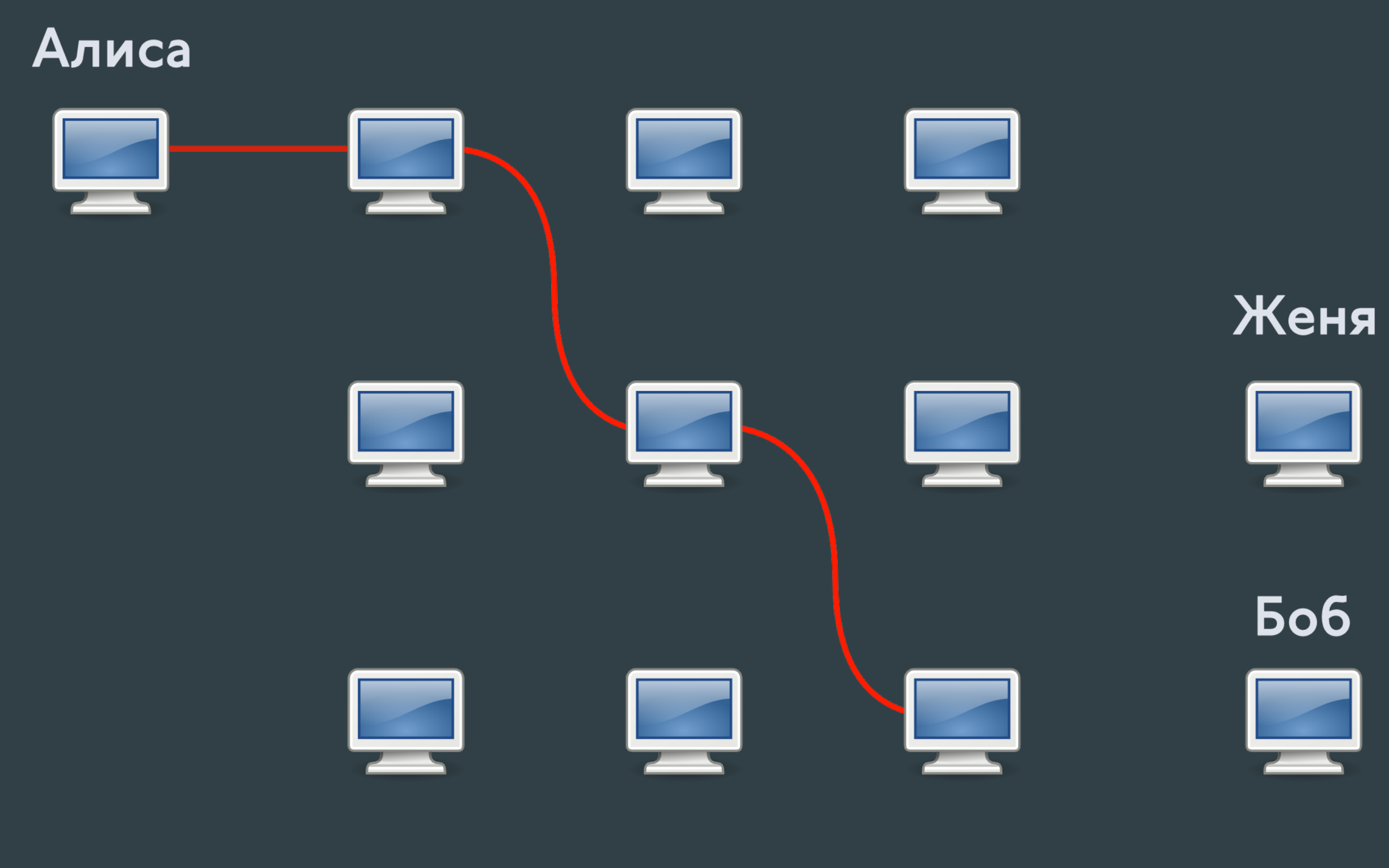
Женя

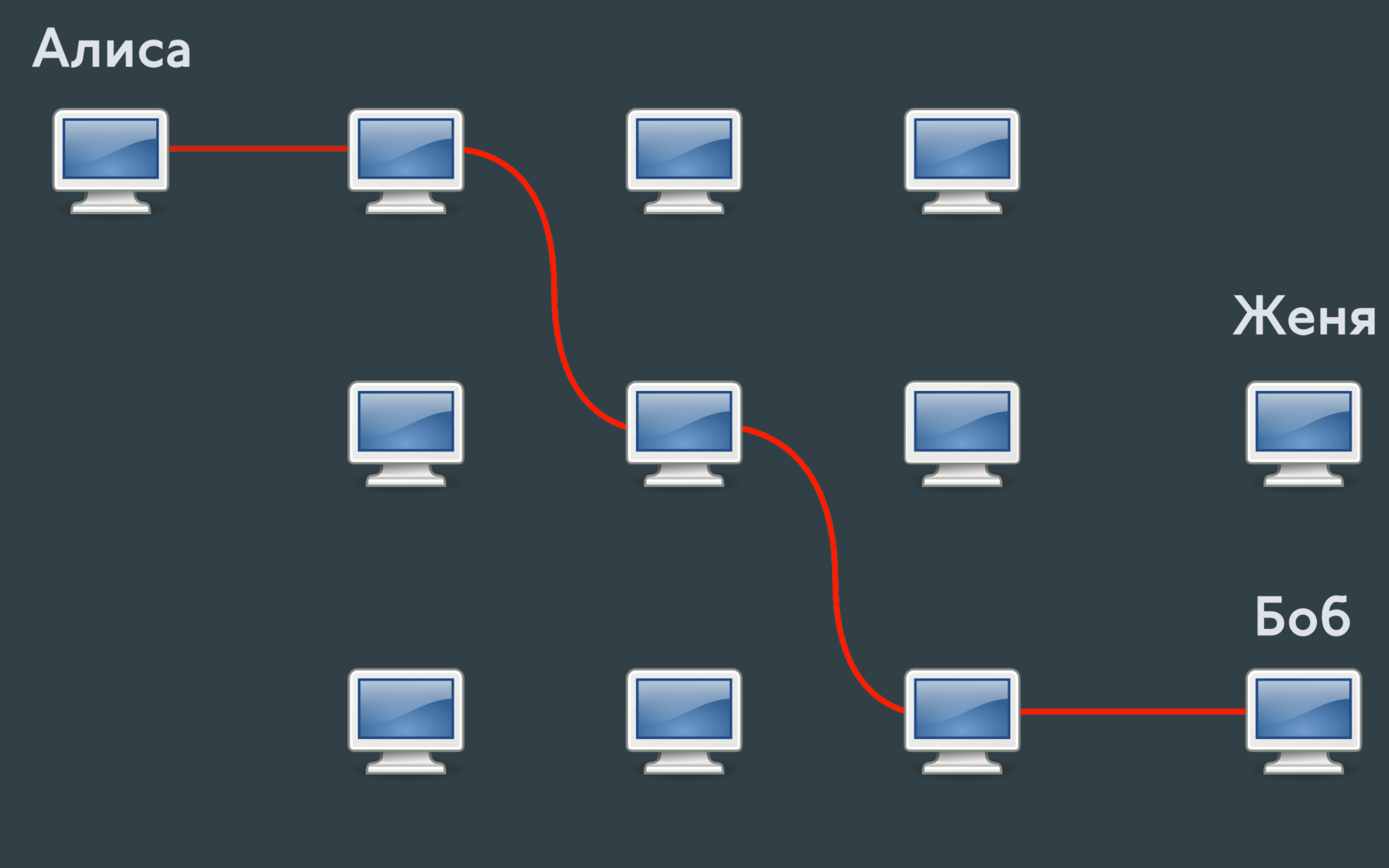


Боб


Алиса
Женя
Боб


Алиса
Женя
Боб

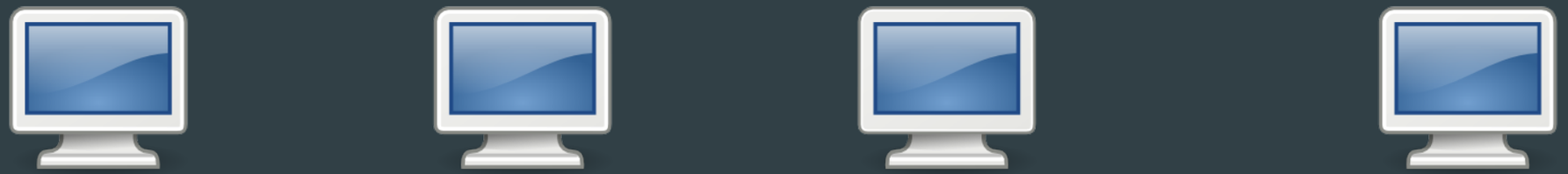

Алиса
Женя
Боб


Алиса
Женя
Боб

Выход в Интернет через Tor

Алиса

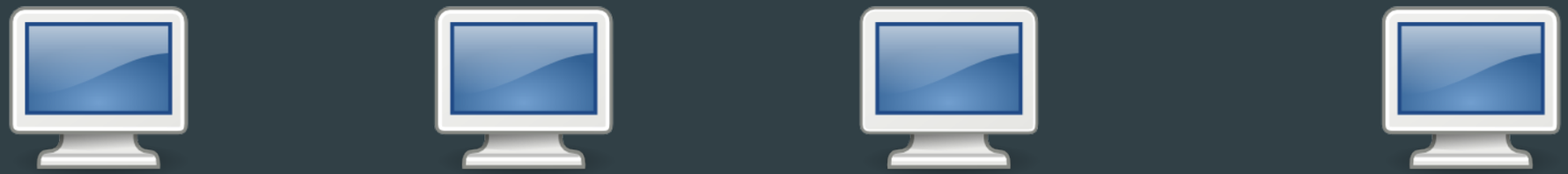
Женя



Боб

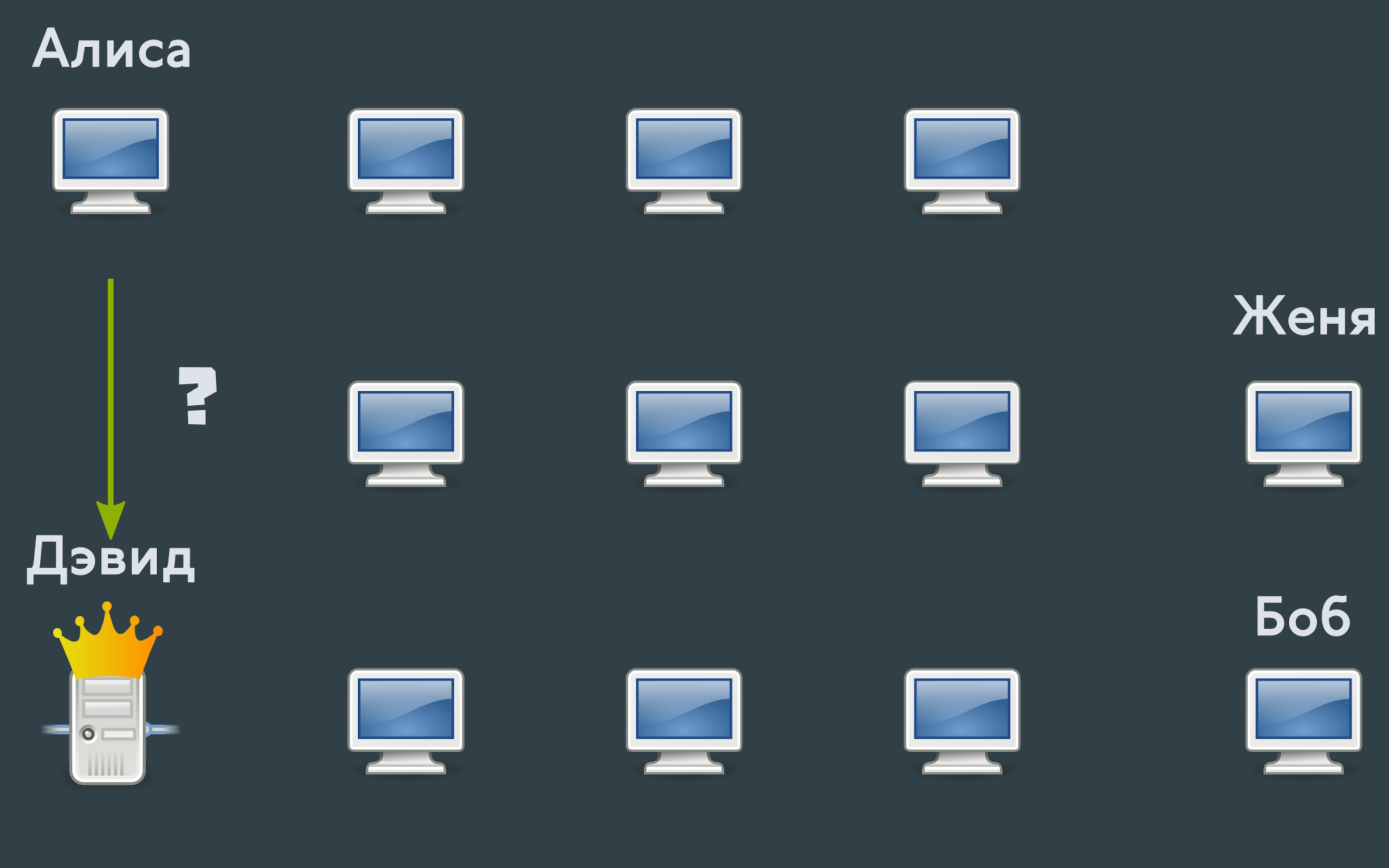
Алиса

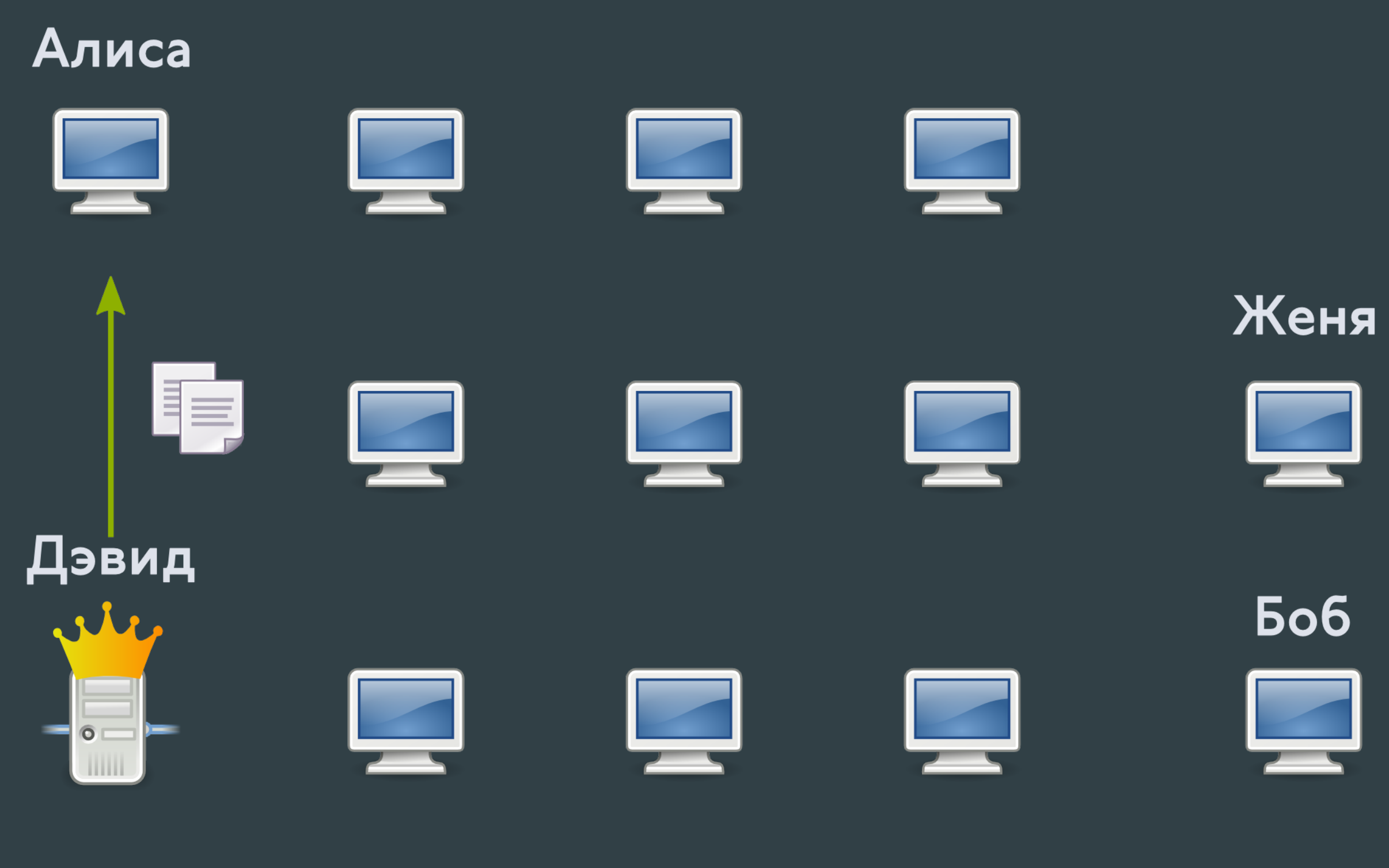
Женя



Дэвид

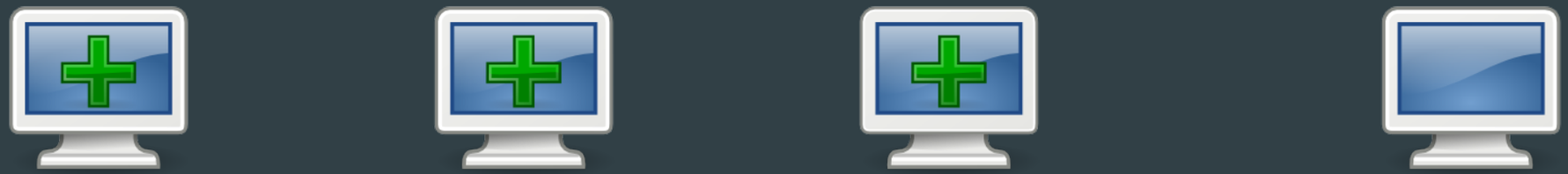
Боб


Алиса
?
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб

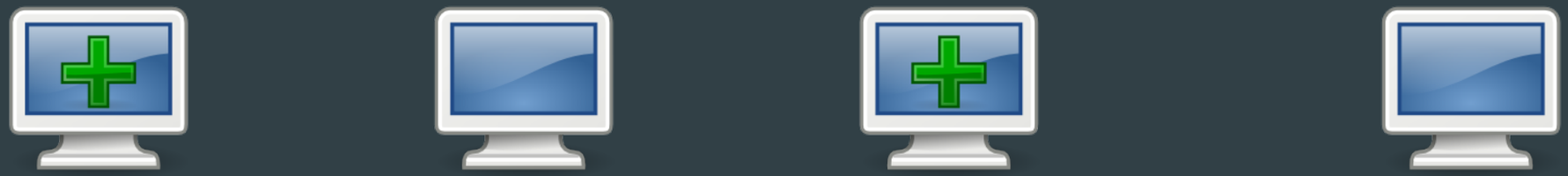
Алиса

Женя

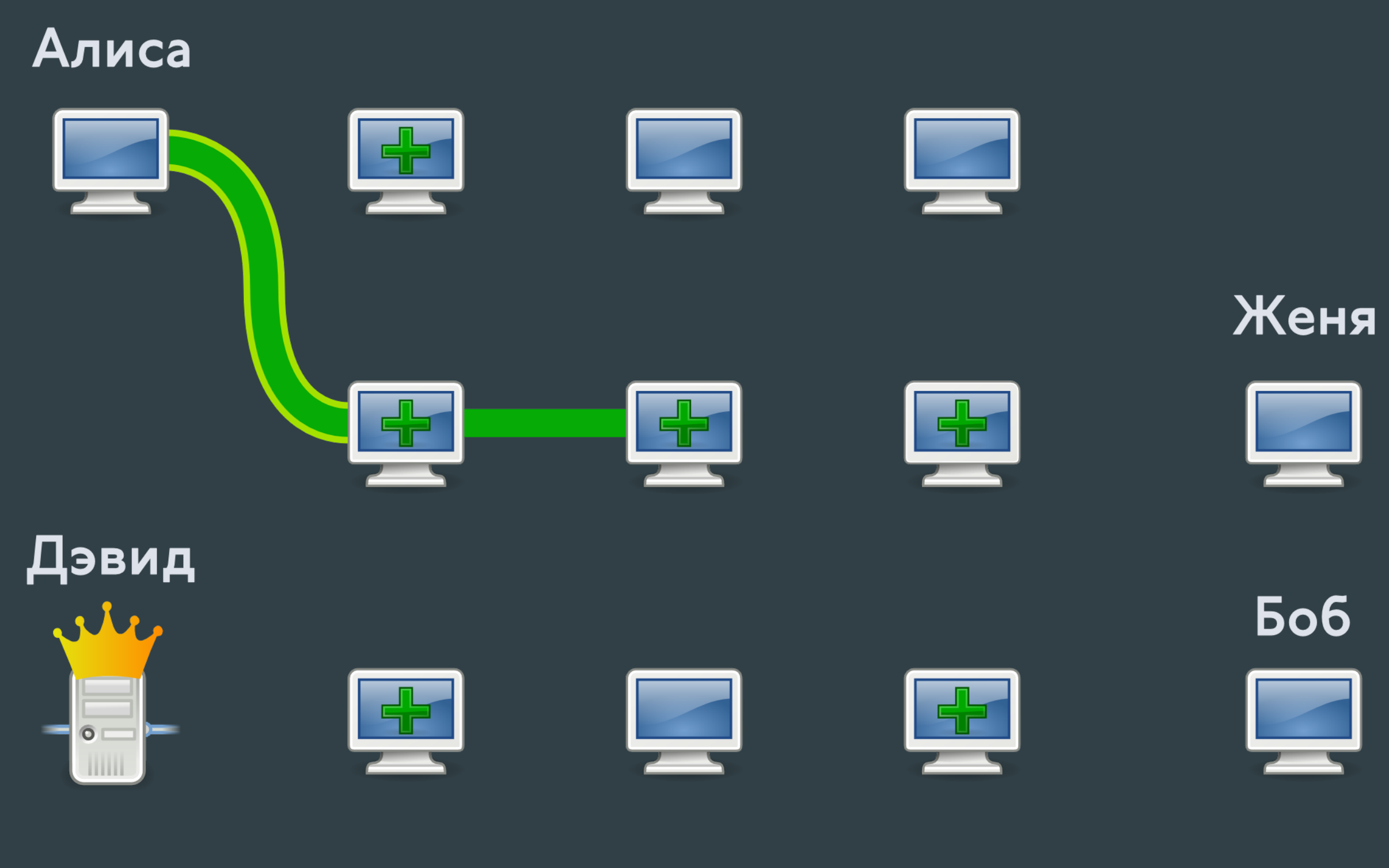


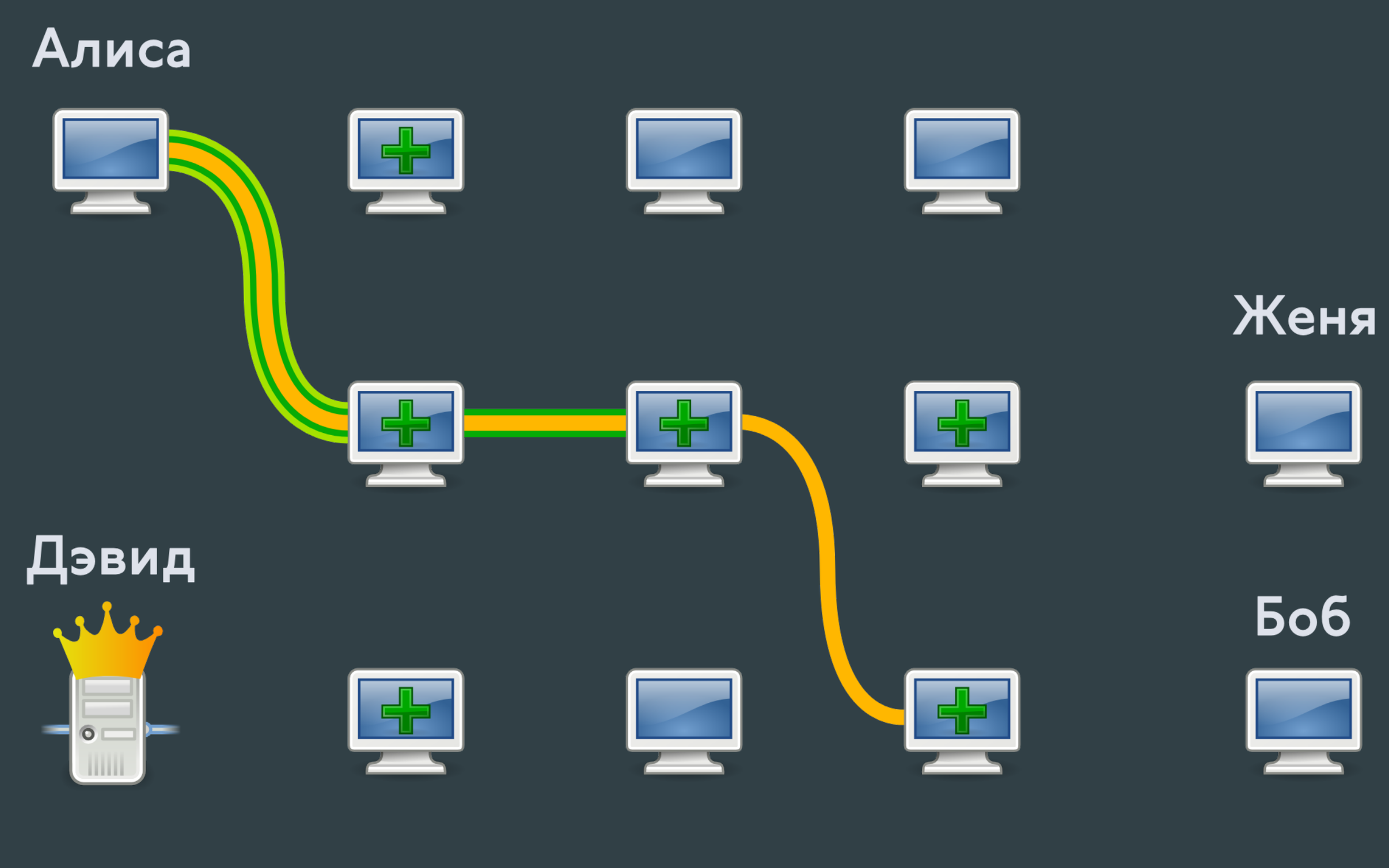
Дэвид

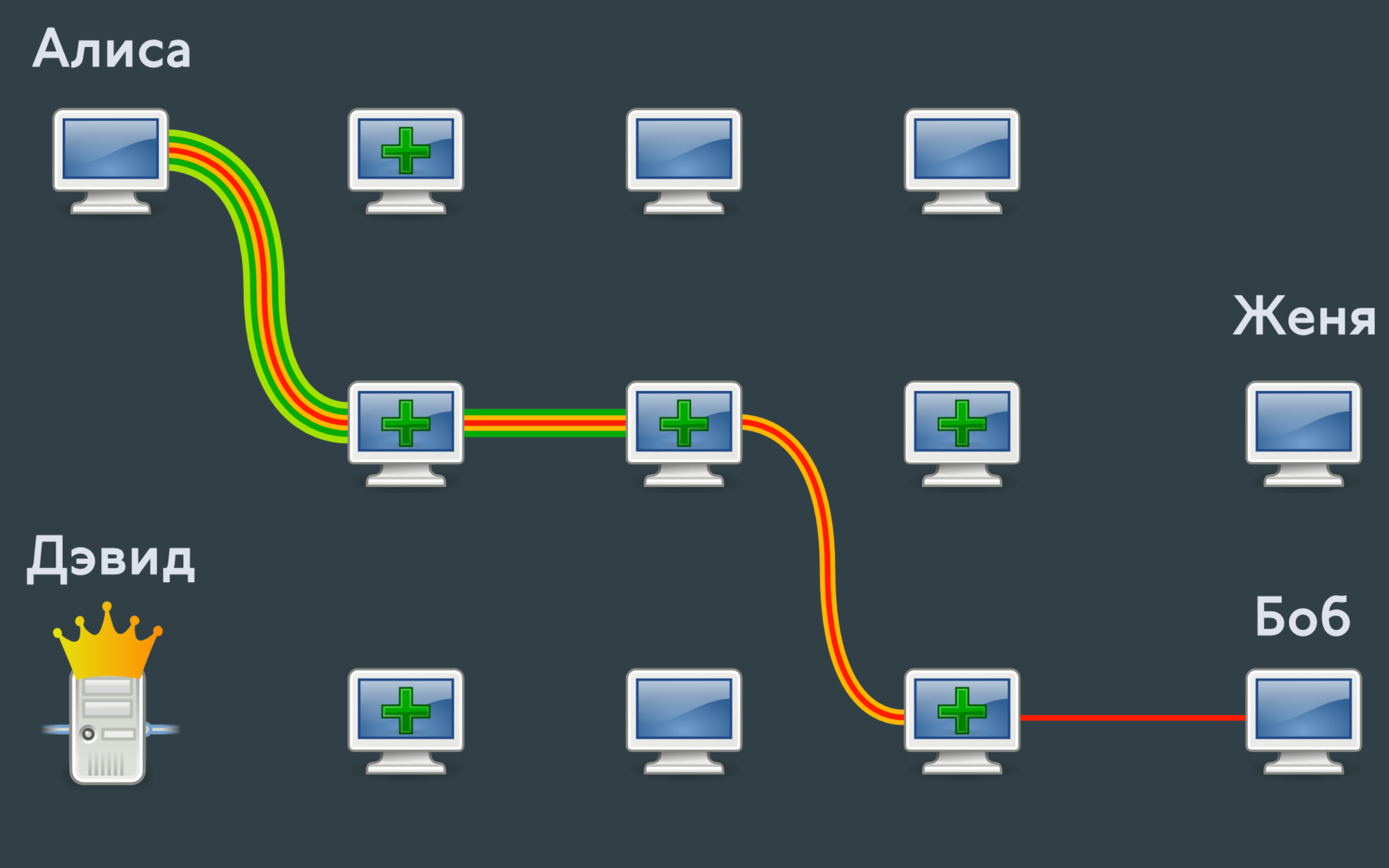
Боб




Алиса
Женя
Дэвид
Боб

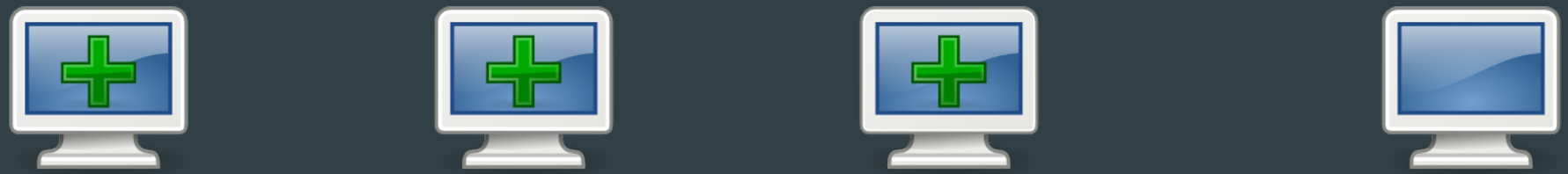

Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб

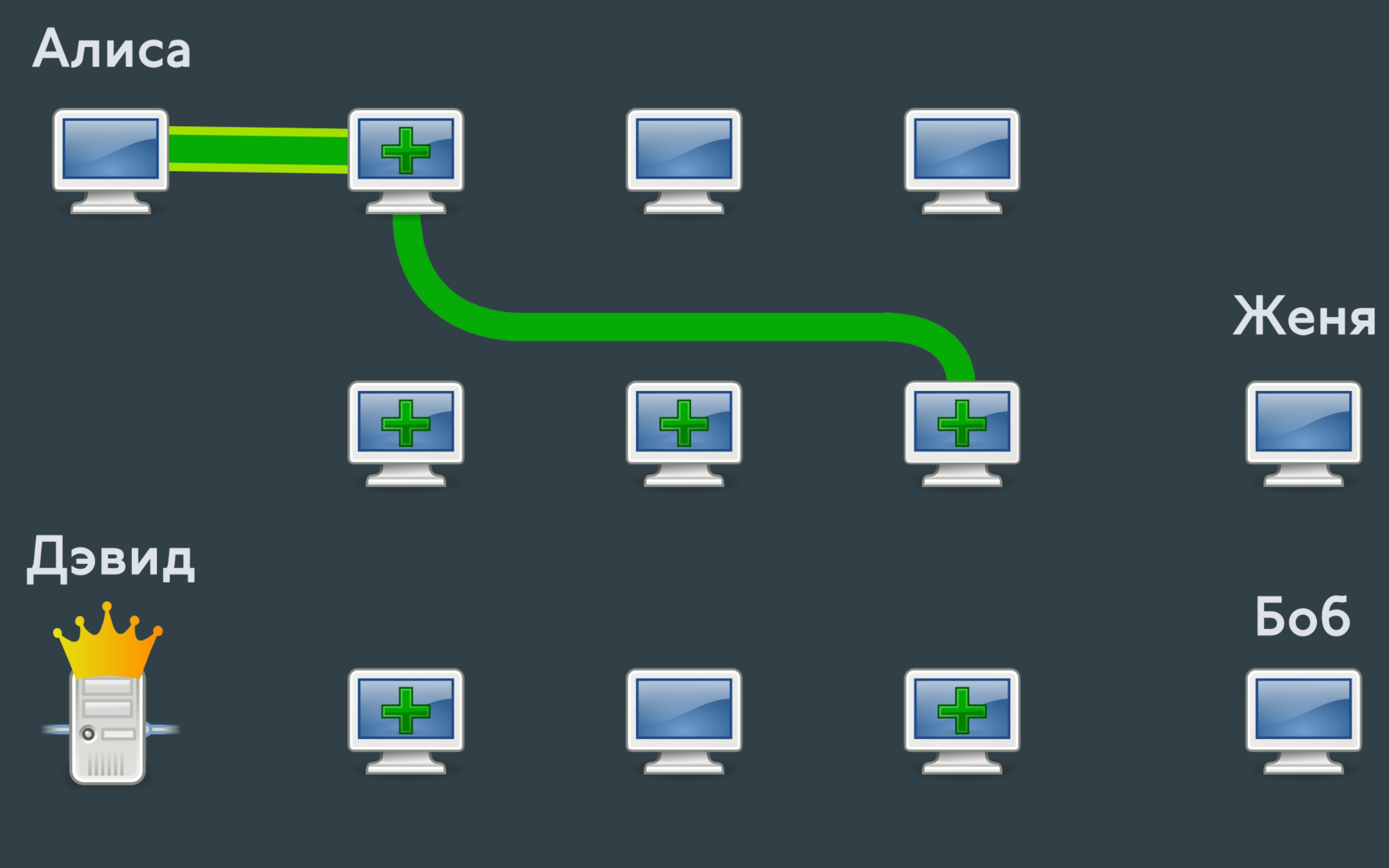
Алиса

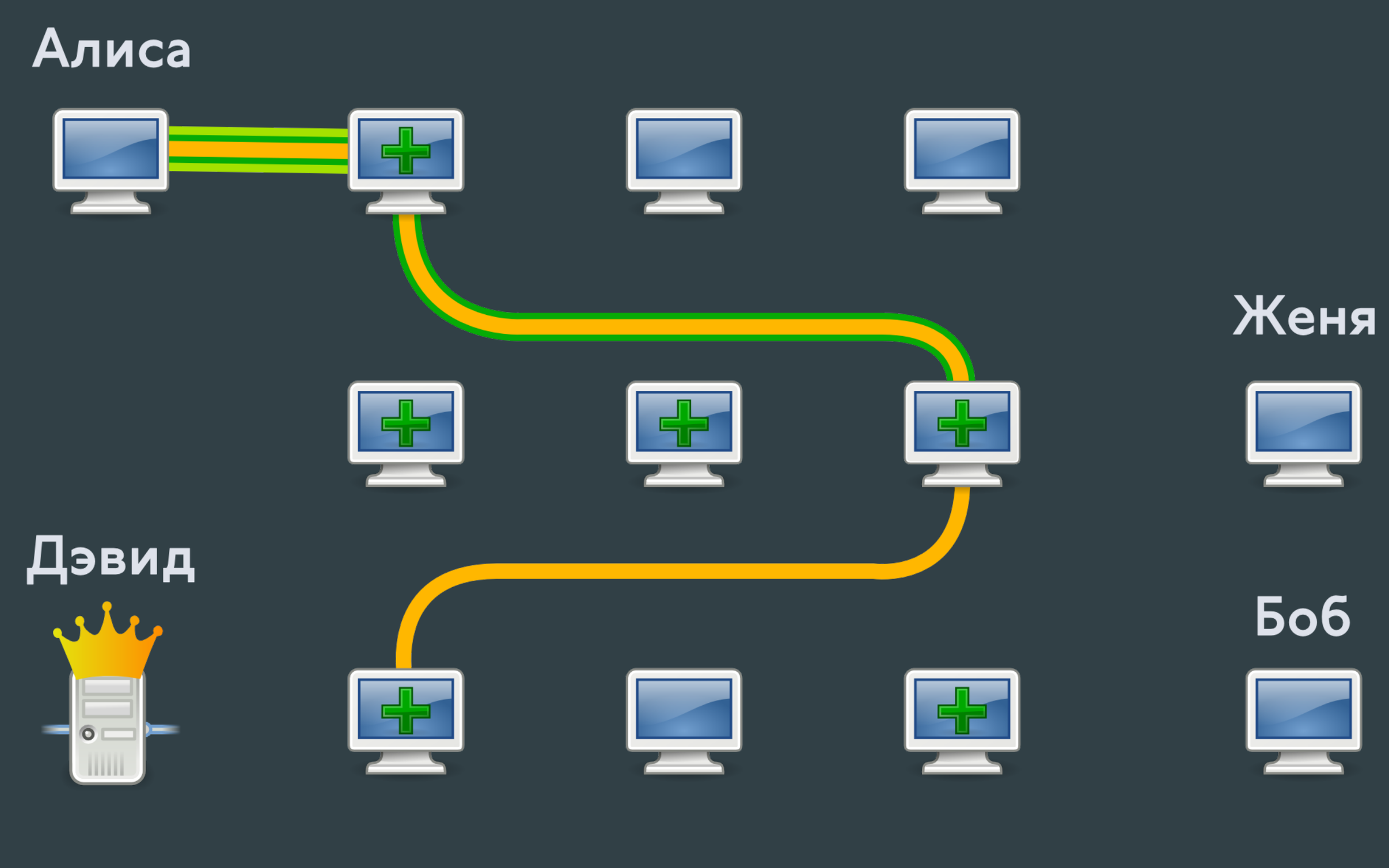
Женя

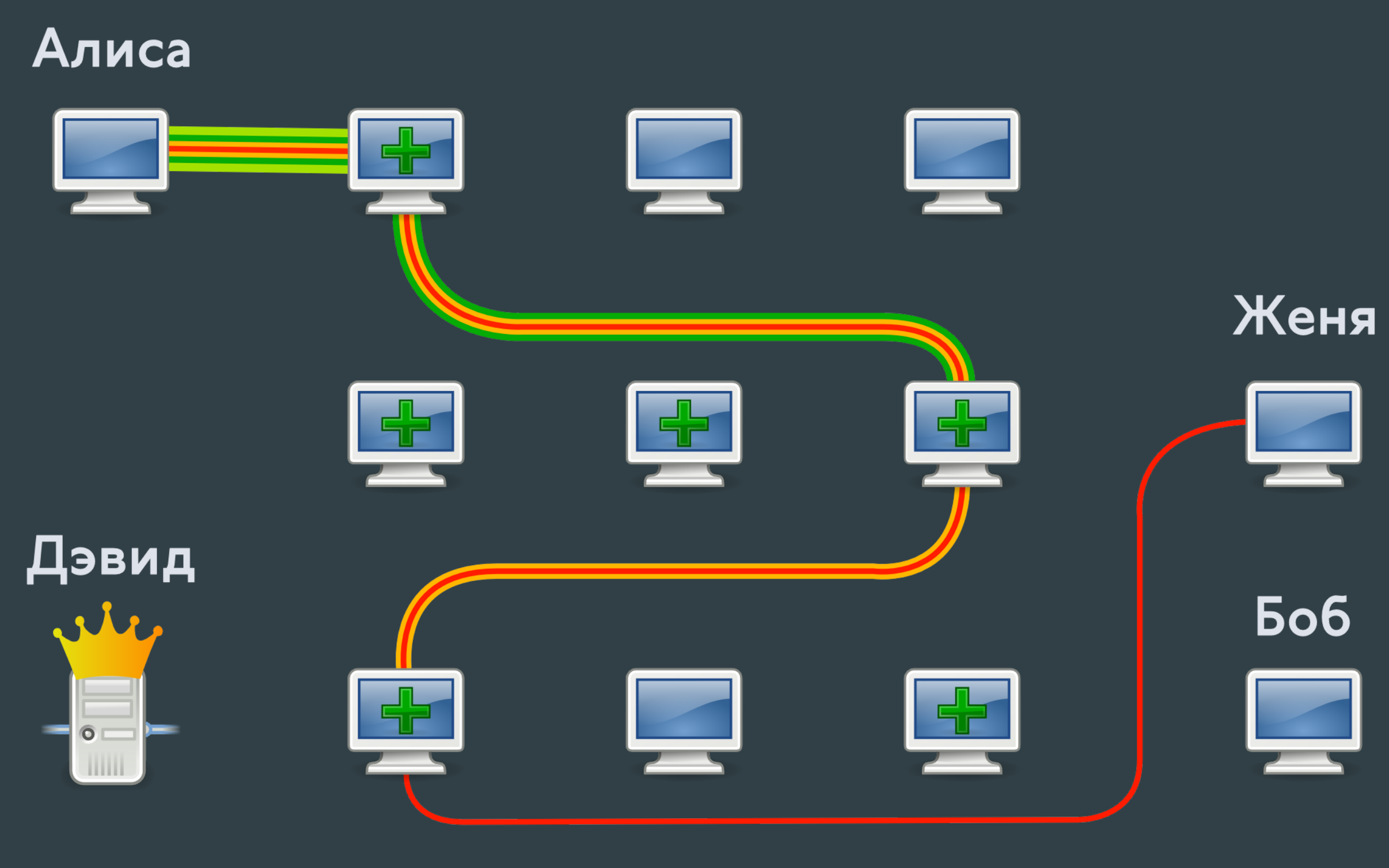


Дэвид

Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб


Алиса
Женя
Дэвид
Боб

Кто-то говорит *с кое-кем*

Выходной релей видит весь траффик!

Цель:
кто-то говорит с *кем-то*

Луковичные сервисы Tor

Tor Onion Services

Анонимность как клиента, так и сервера

Публичные ключи вместо имен

Достаточно сгенерировать ключевую пару

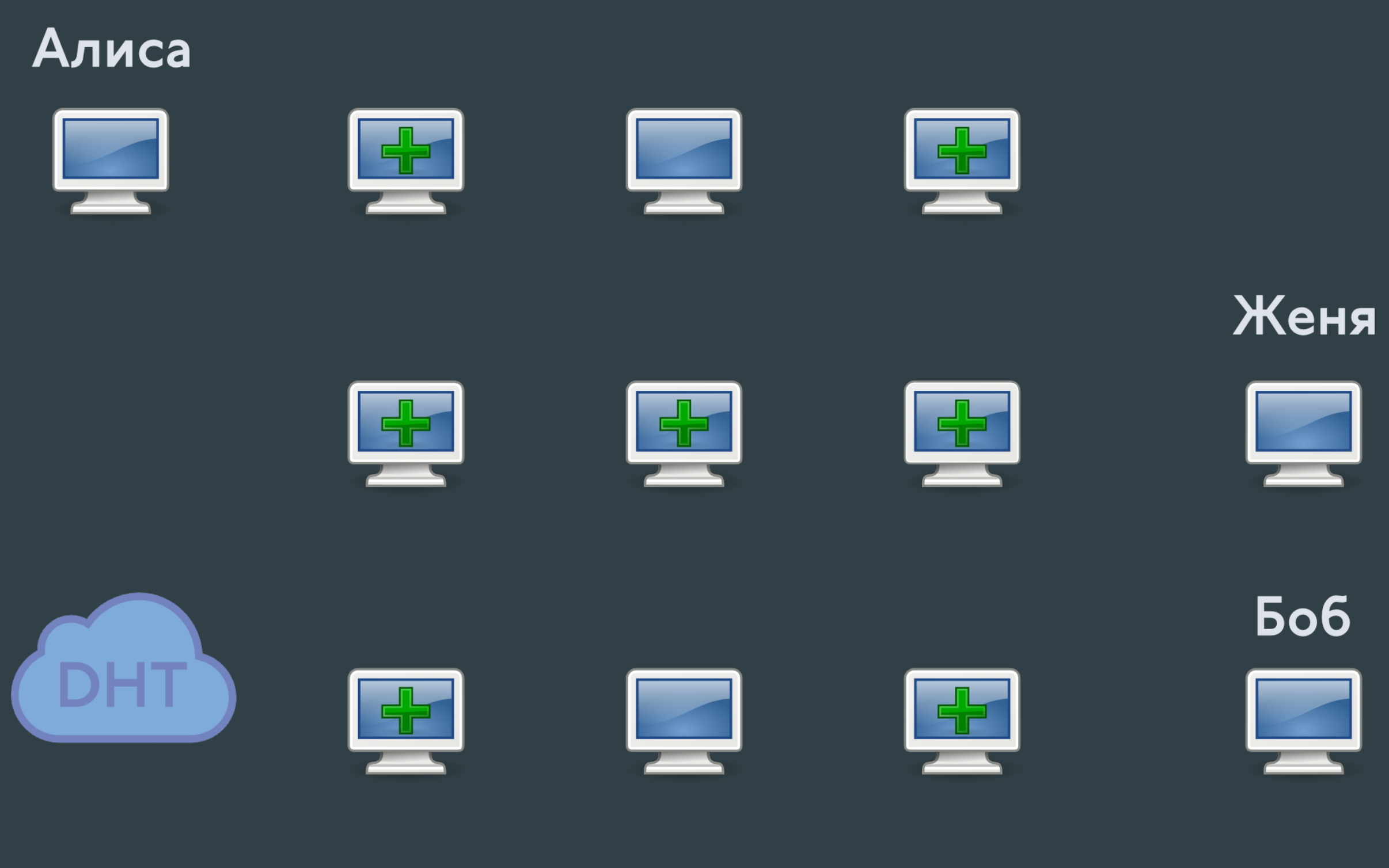
zkym3uprkoddlxpq.onion

facebookcorewwwi.onion

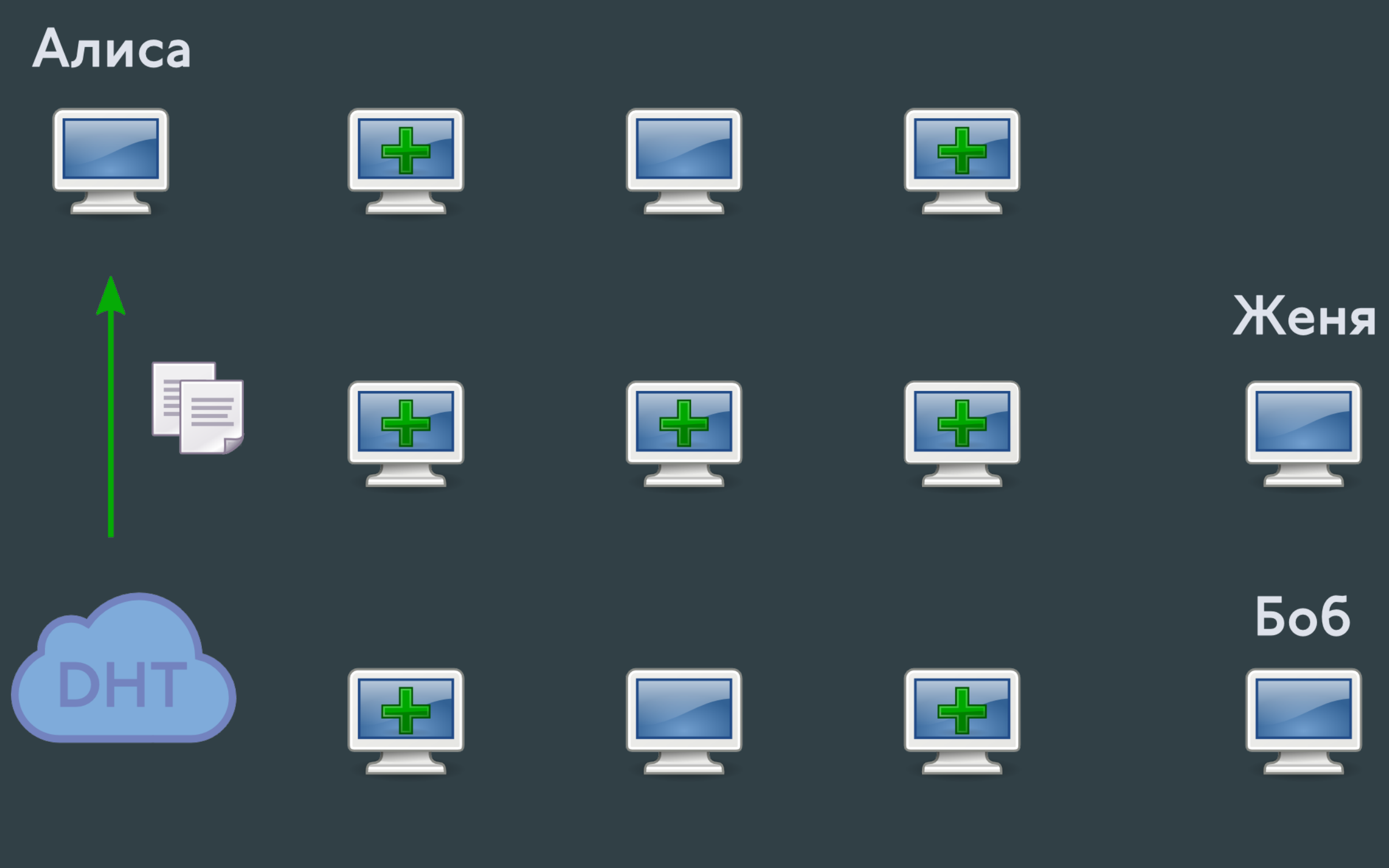
Сквозное шифрование

Forward Secrecy

Запускаются везде, где есть tor

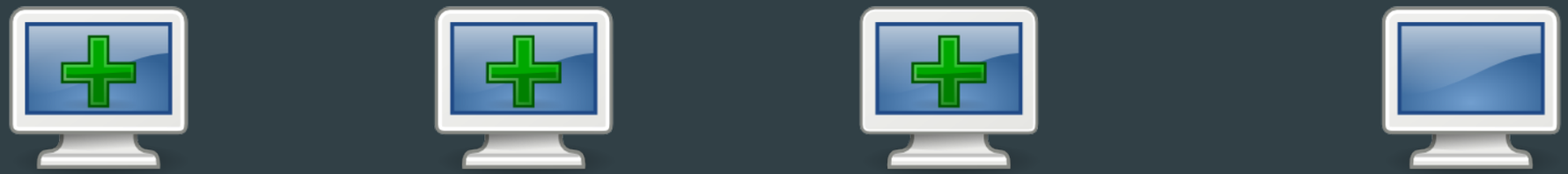

Алиса
Женя
Боб
DHT


Алиса
.onion
?
Женя
DHT
Боб

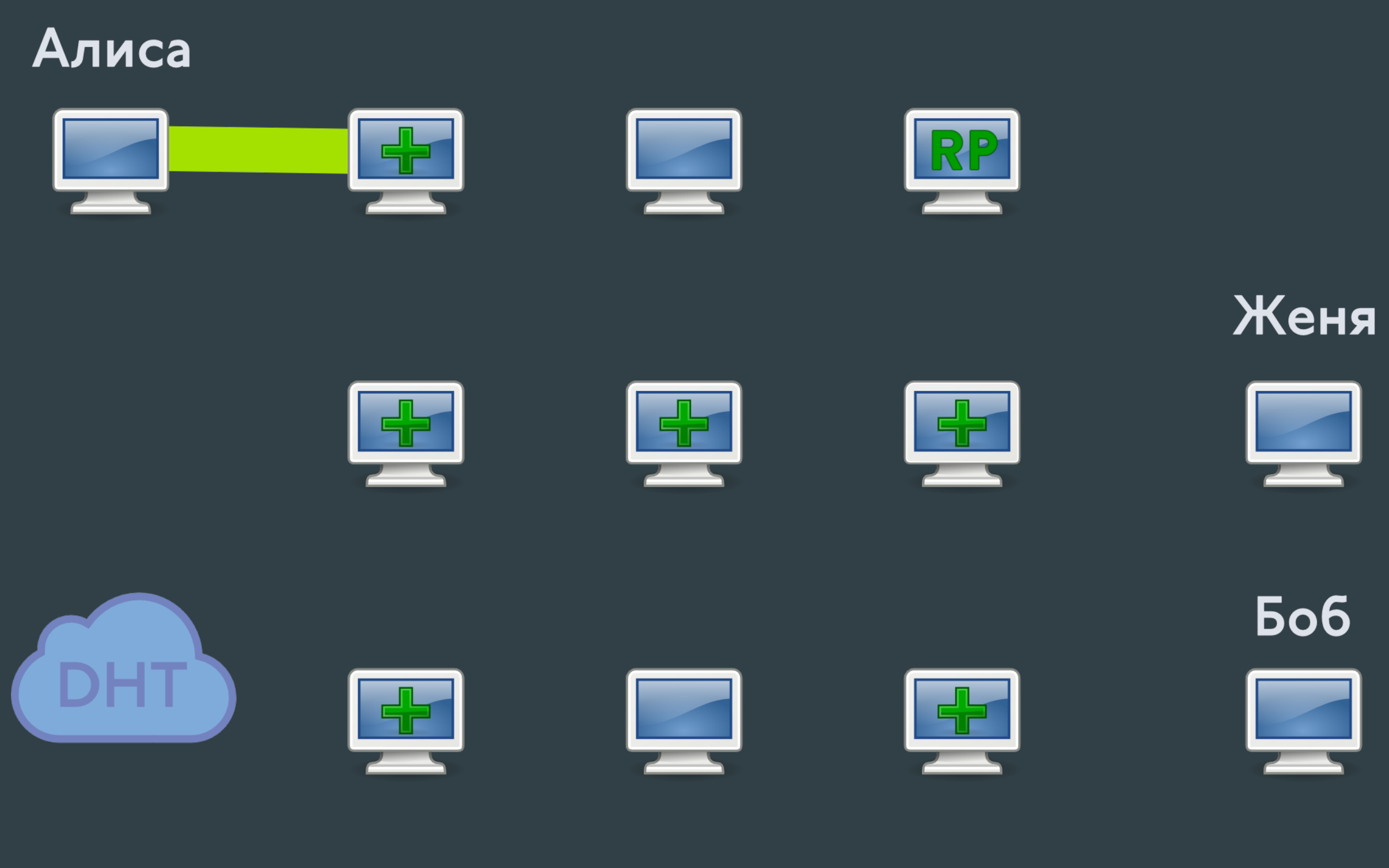

Алиса
Женя
Боб
DHT

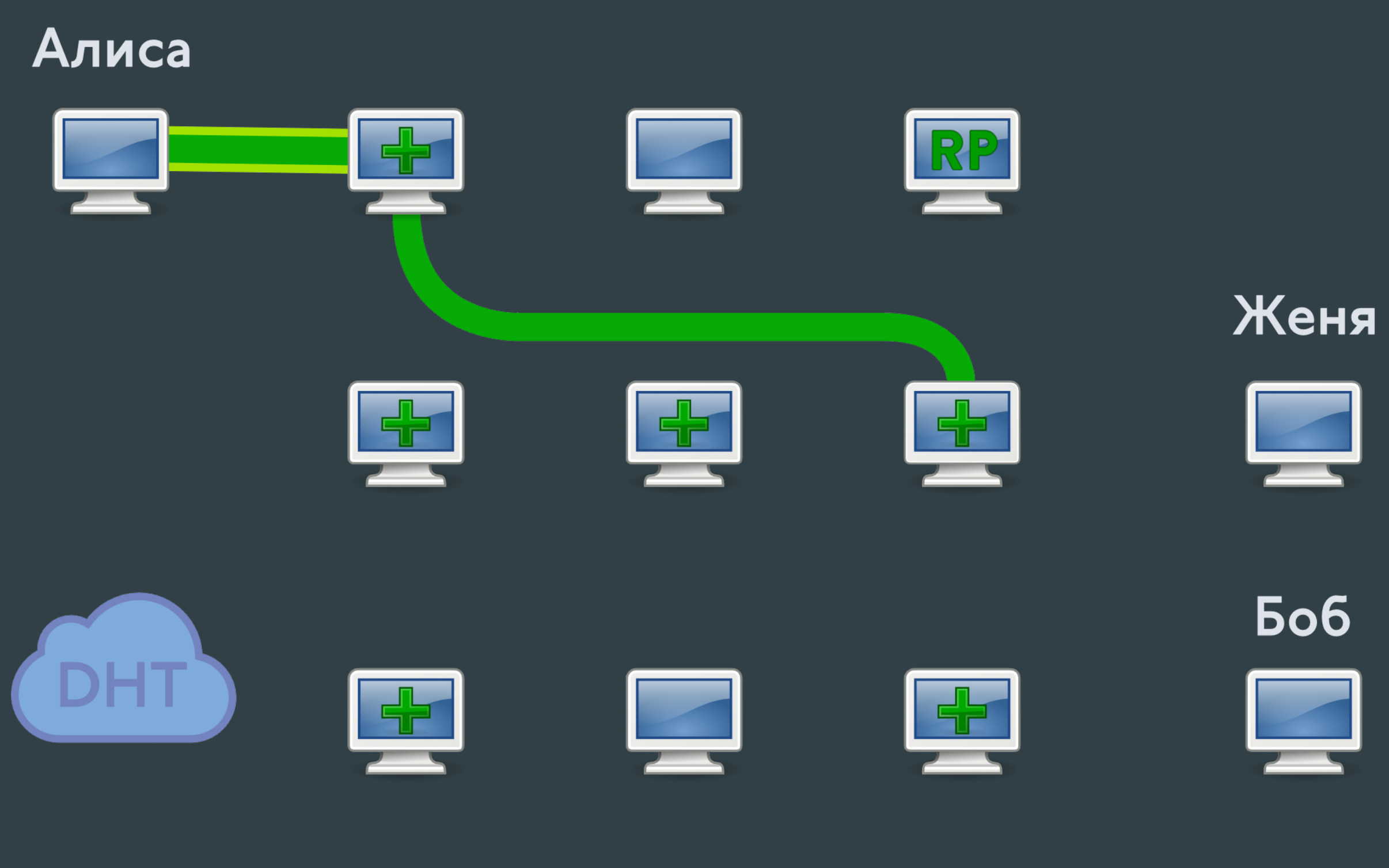
Алиса

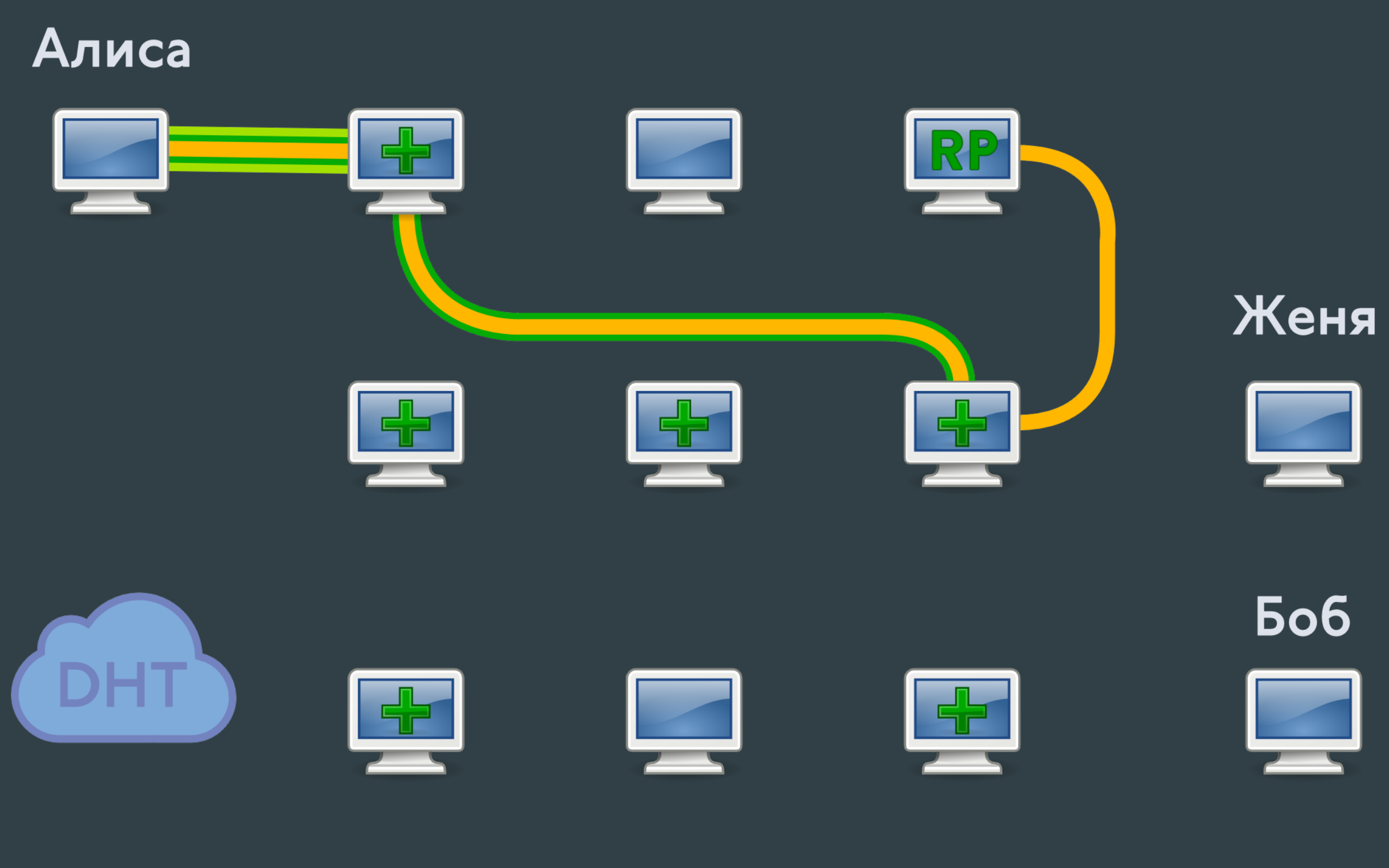
Женя



Боб

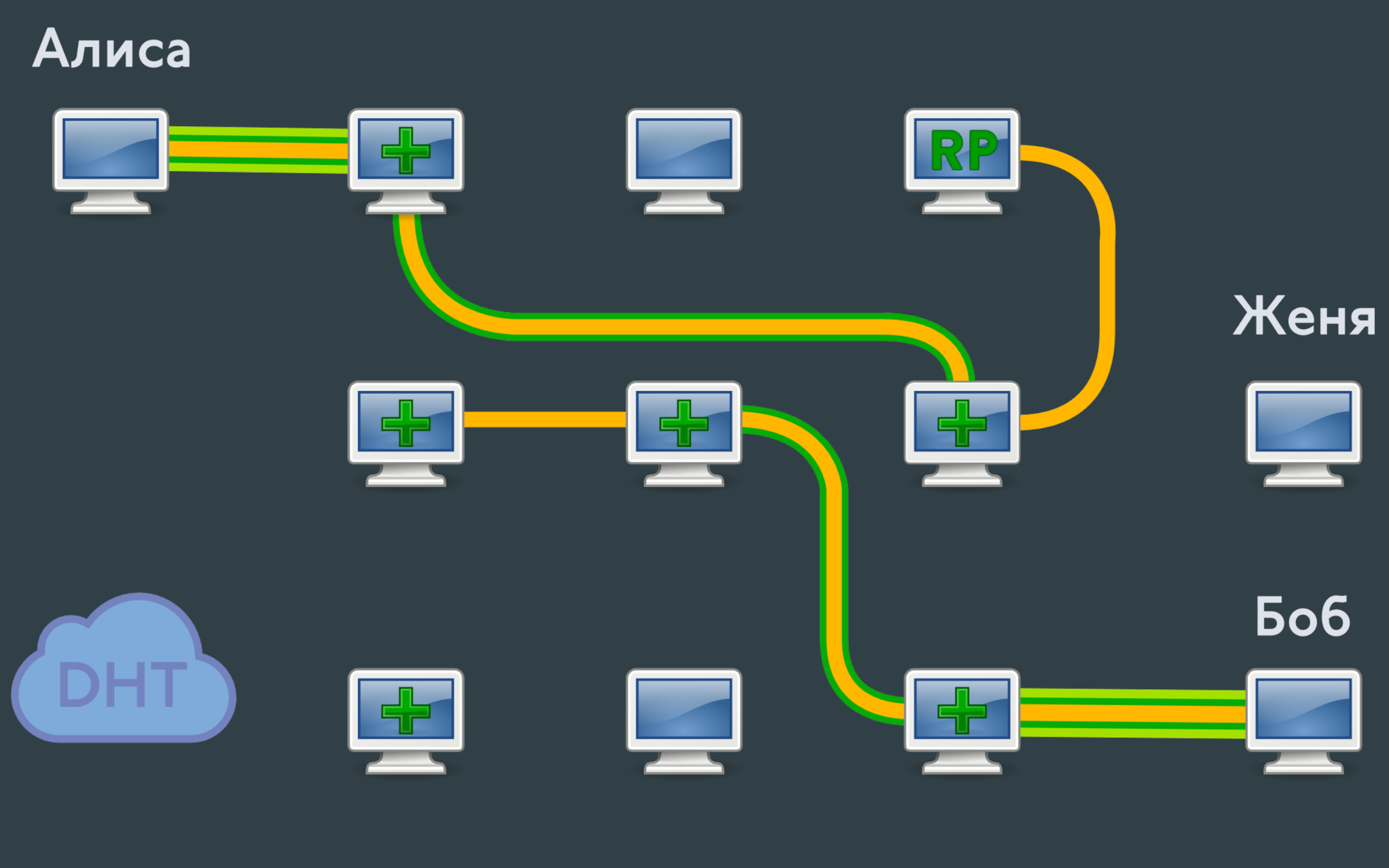

Алиса
RP
Женя
DHT
Боб

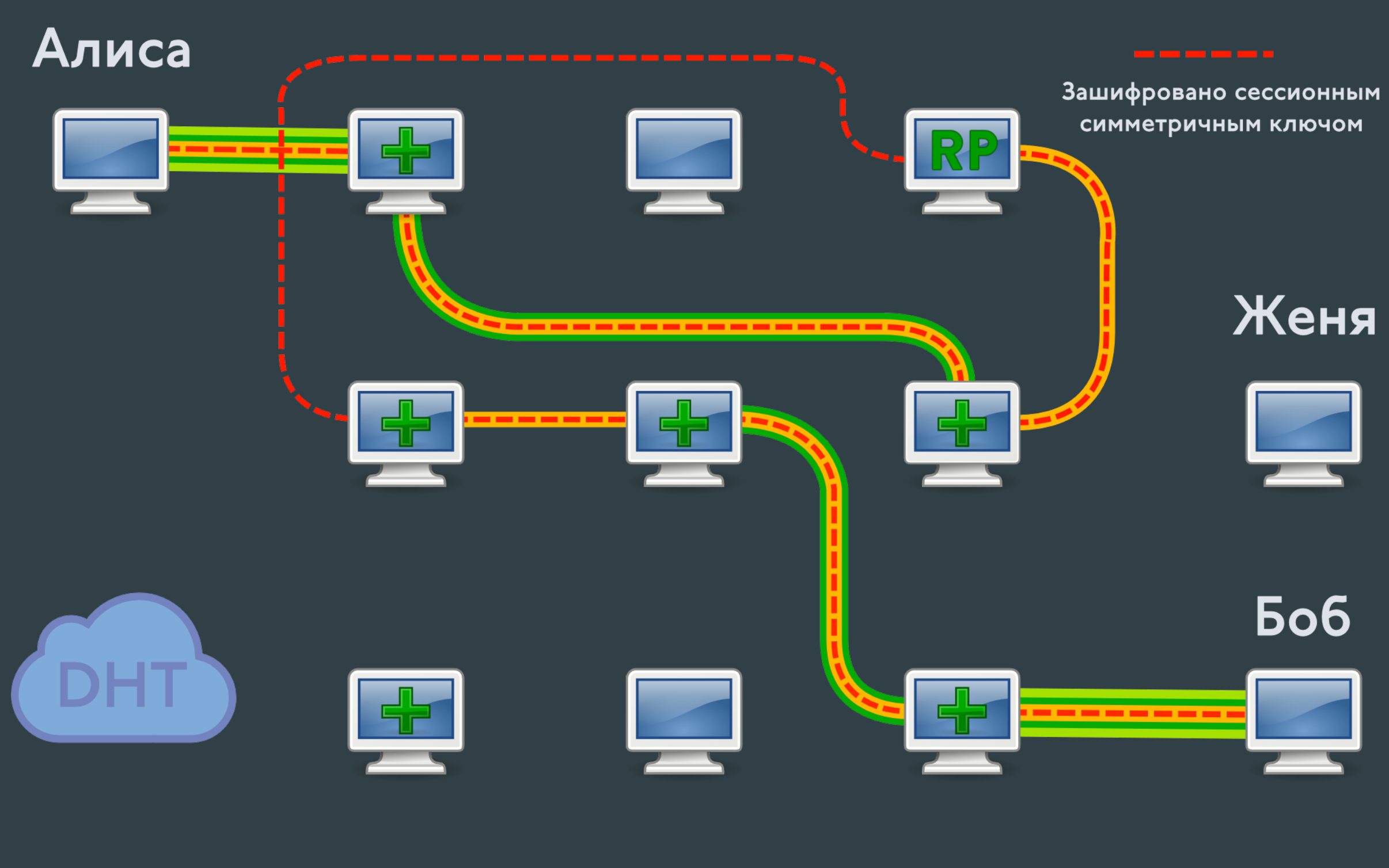

Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб


Алиса
RP
Женя
DHT
Боб

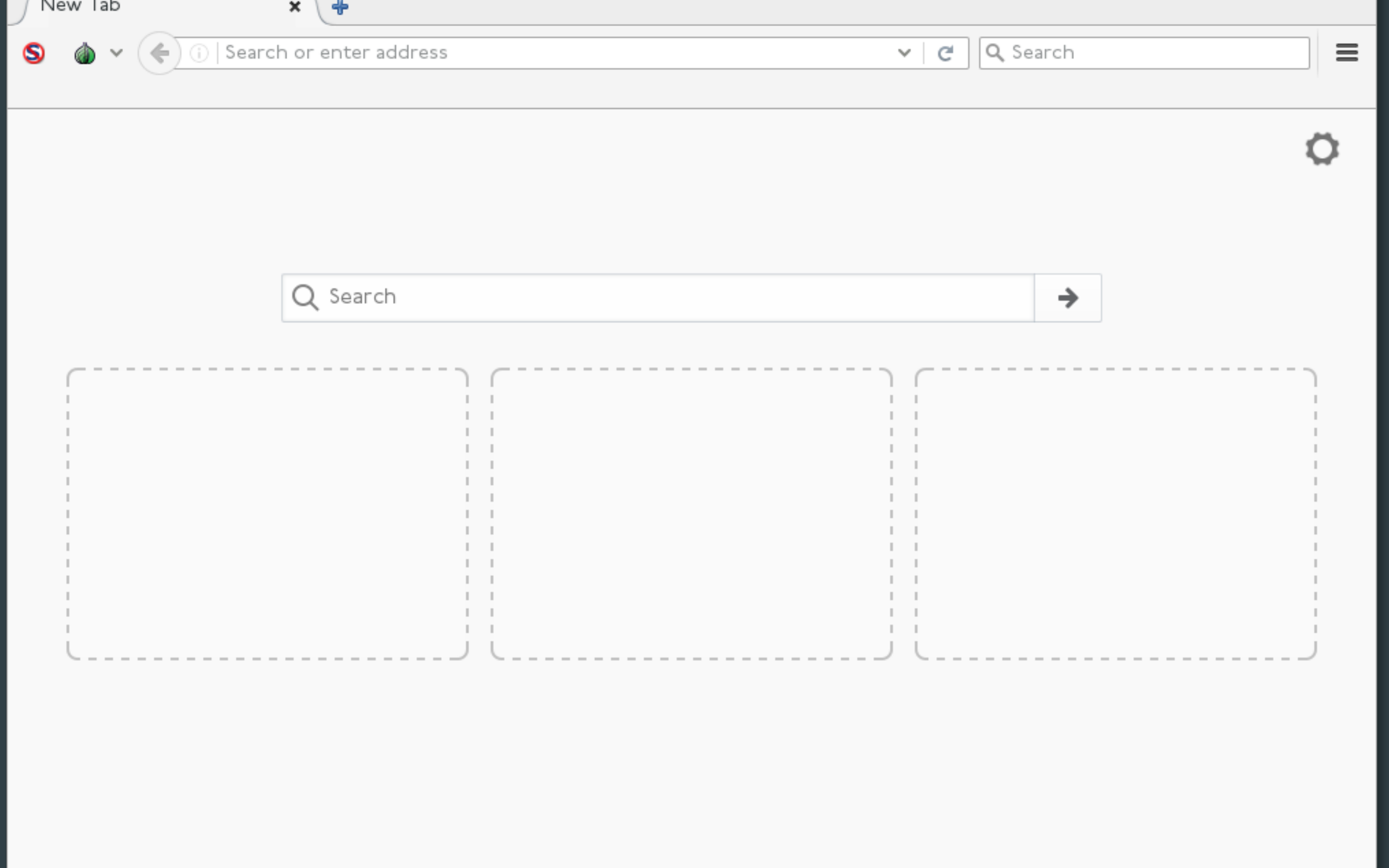

Алиса
Зашифровано сессионным симметричным ключом
RP
Женя
Боб
DHT

Tor Browser

Mozilla Firefox* + tor

* с огромным количеством исправлений для повышения приватности

Tor Browser выглядит так:


New Tab
Search or enter address
Search
Search

Мосты

Релеи Tor, которых нет в публичном состоянии сети

Используются как входные релеи в цепочках

В чистом виде потеряли смысл.
Для подключения к мостам используются...

Подключаемые Транспорты

Pluggable Transports

Алгоритмы маскировки подключений Tor

для обхода цензуры

Защита чатов

OTR

Off-The-Record Messaging

Почему OTR?

Открытый

Простой

Хорошо проанализирован

Отрицание авторства

Forward Secrecy

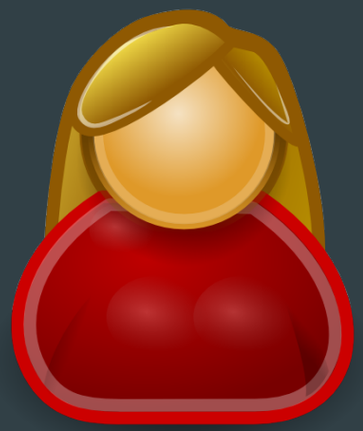
Mar 16, 2012 13:43:55 [redacted] **[OC: No decrypt available for this OTR encrypted message.]**

Mar 16, 2012 13:43:59 **[OC: No decrypt available for this OTR encrypted message.]**

Mar 16, 2012 13:44:20 **[OC: No decrypt available for this OTR encrypted message.]**

Mar 16, 2012 13:44:46 **[OC: No decrypt available for this OTR encrypted message.]**

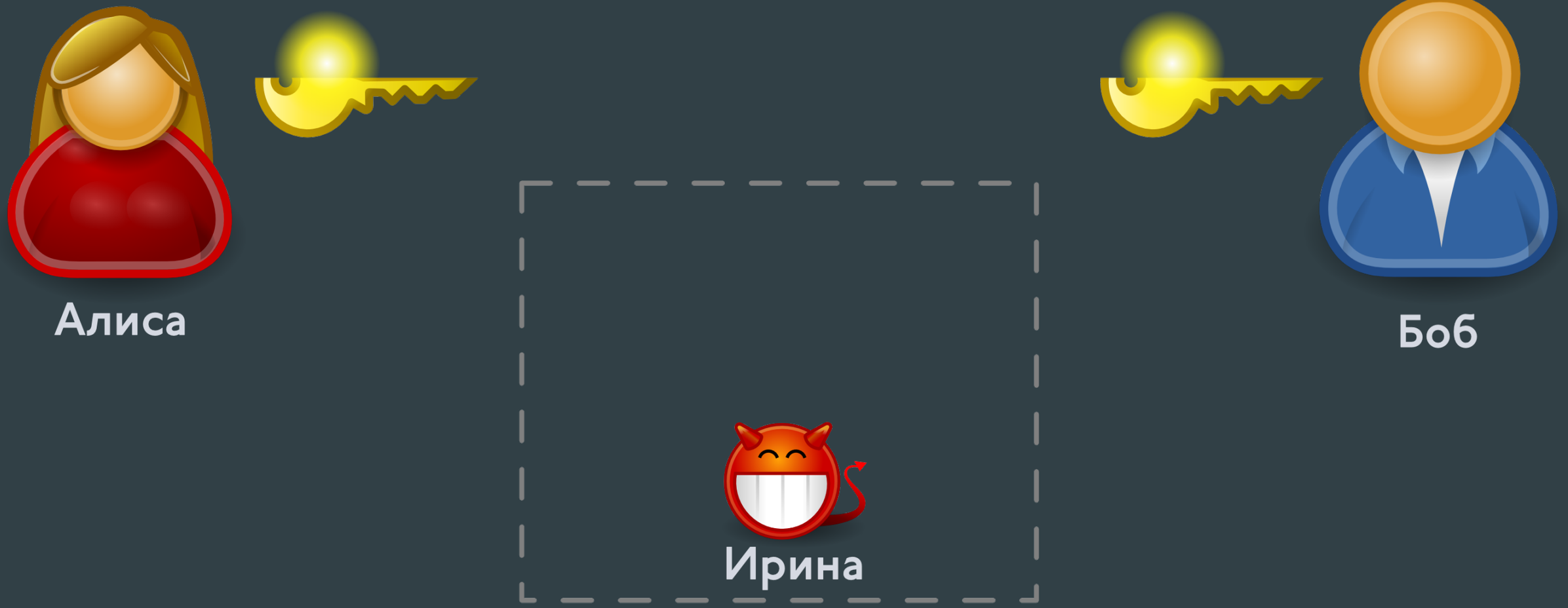
***



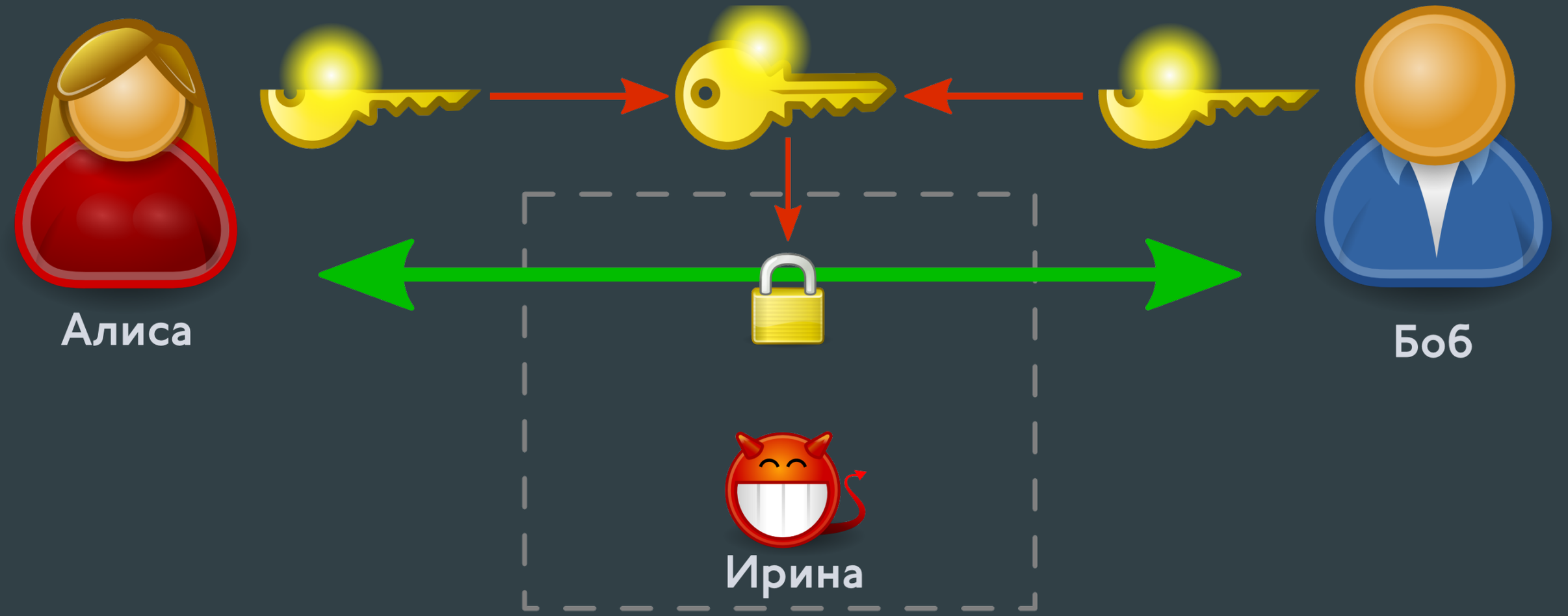
Алиса

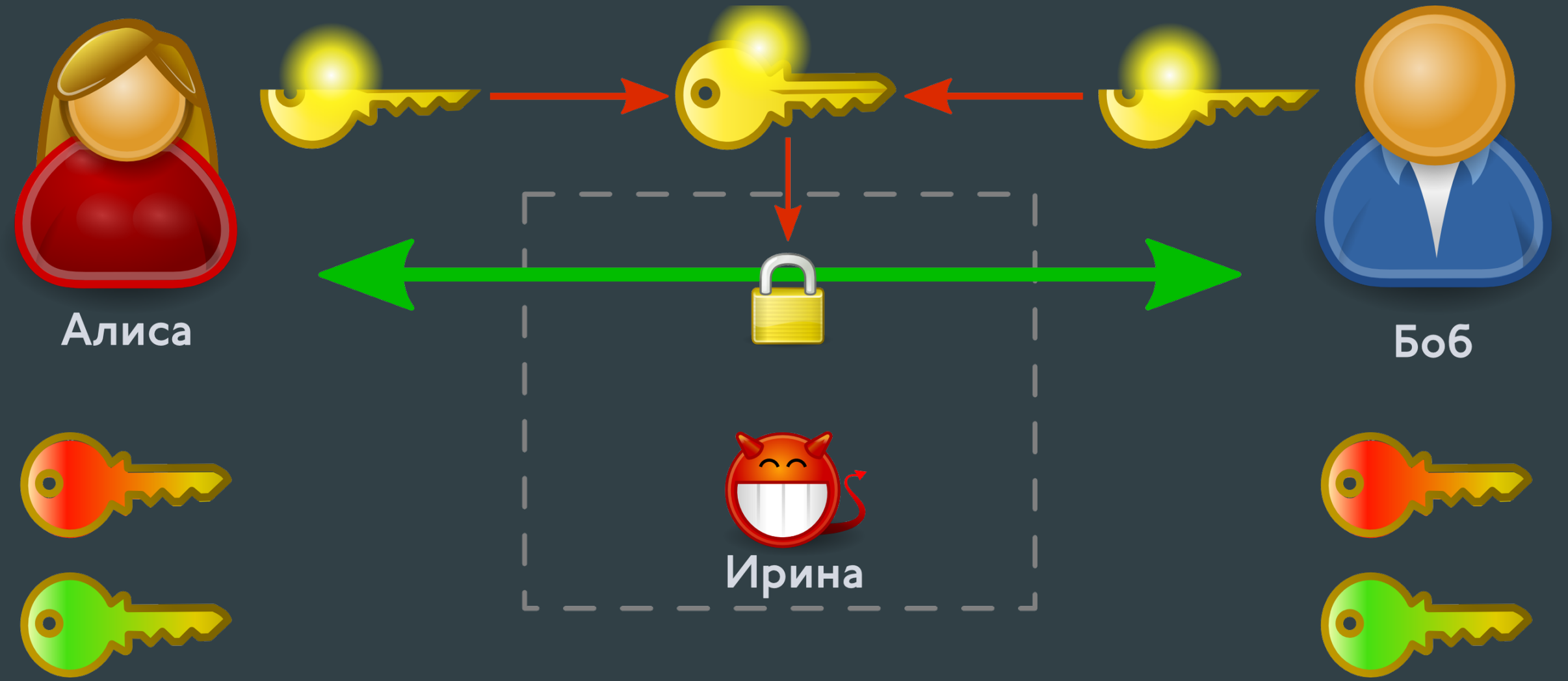
Ирина

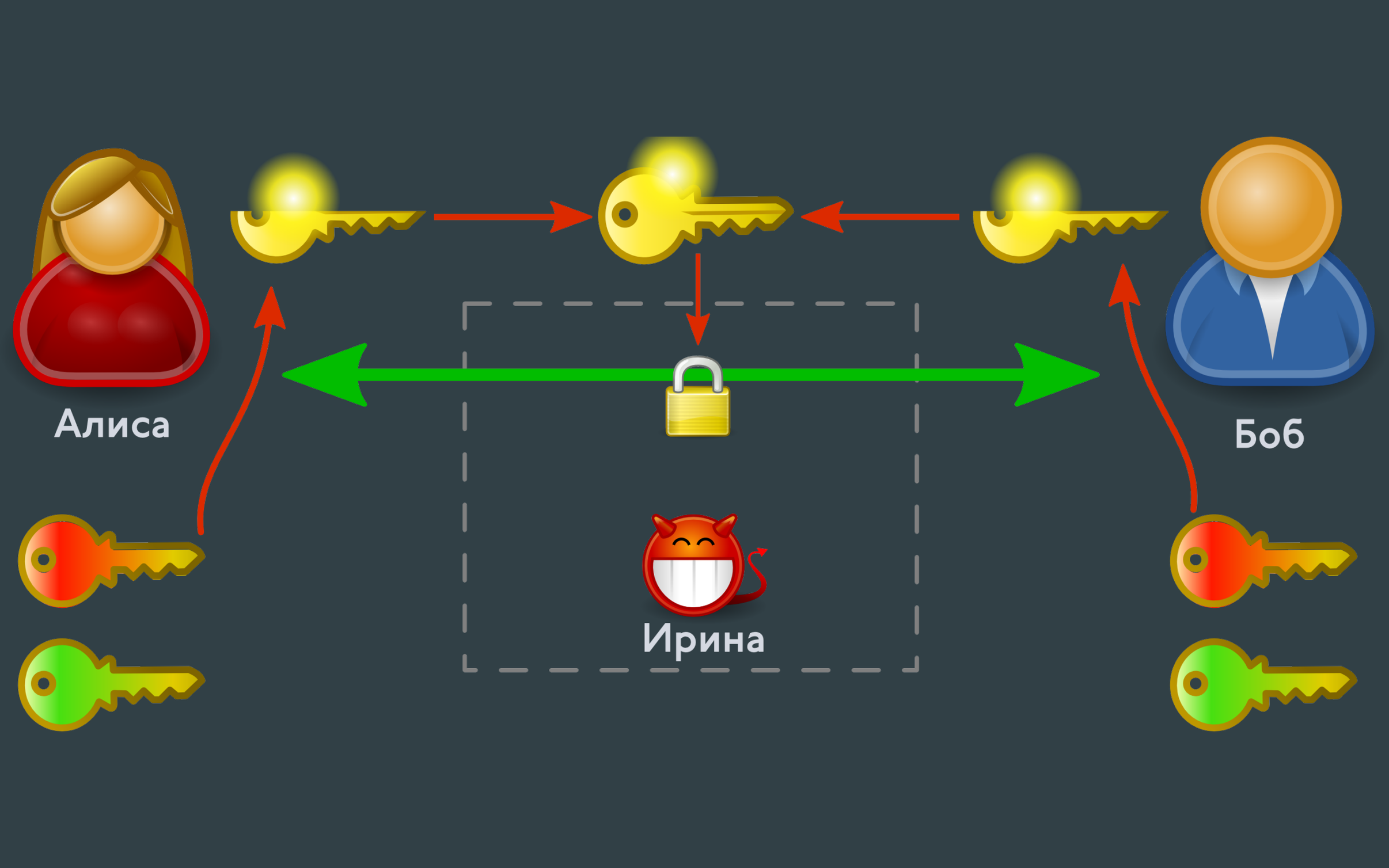
Боб


Алиса
Ирина
Боб


Алиса
Боб
Ирина


Алиса
Боб
Ирина


Алиса
Боб
Ирина


Алиса
Боб
Ирина

Сообщение OTR выглядит так:

?OTRv2?Y3J5cHRvcGFydHkK

В текущей версии протокола нет передачи файлов

Используйте OnionShare или PGP

Предпочтительный вариант использования OTR

Протокол XMPP

Похож на эл. почту

cryptoparty@jabber.ccc.de

Децентрализованный

Можно зарегистрироваться на любом сервере

Можно связываться с пользователями на любом сервере

Но не распределенный!

Защита файлов и почты

PGP

Pretty Good Privacy

Почему PGP?

30 лет шифрования "военного уровня"

Многочисленные аудиты

Стандарт интернета

[redacted]

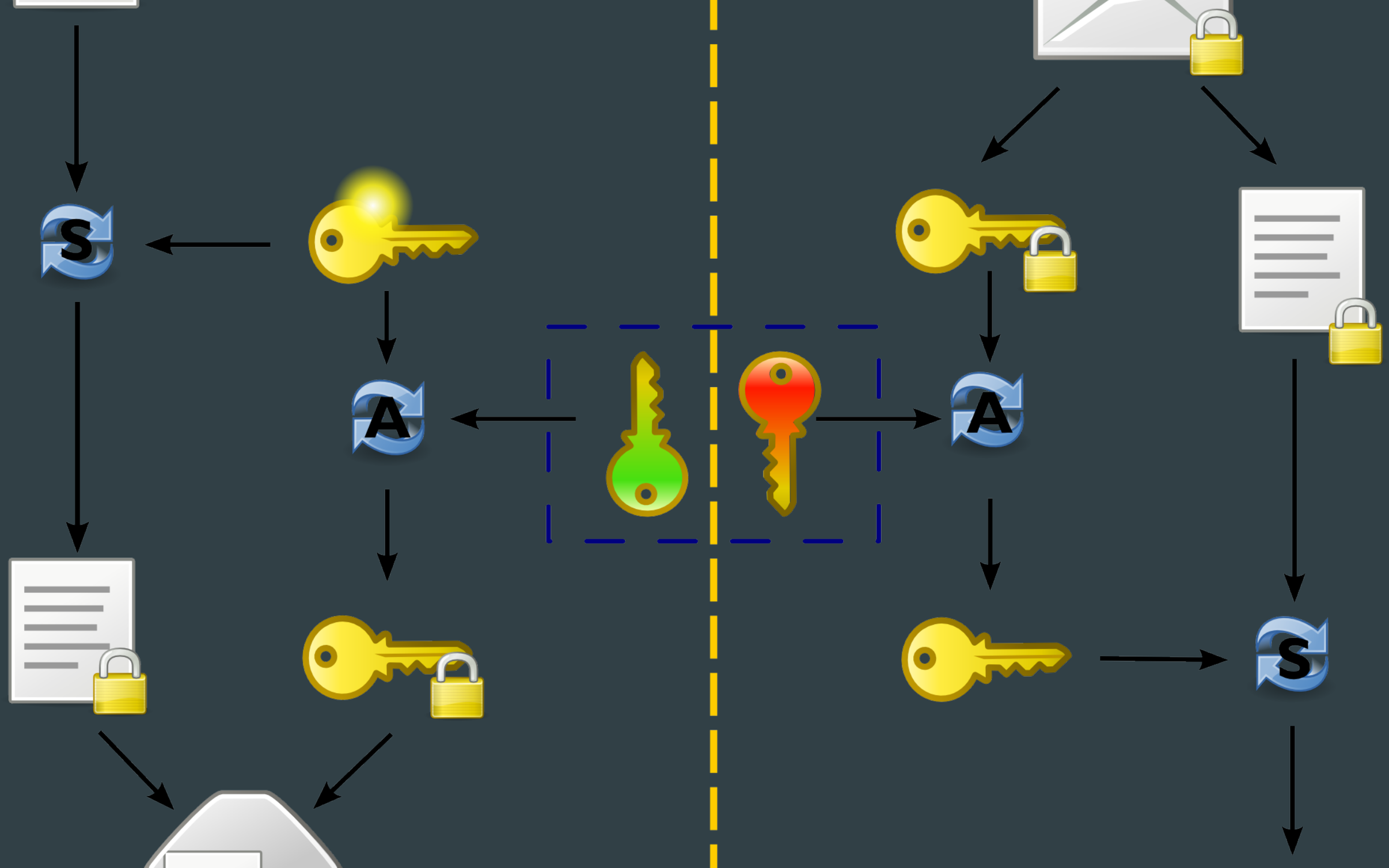
SIGAD: US-984XN
PDDG: AX
CASE_NOTATION: [redacted]
DTG: 31JA0546Z12

Received from: [redacted]
Date: Mon, 30 Jan 2012 21:46:03 -0800 (PST)
From: [redacted]@yahoo.com>
Subject: Re: Untitled
To: [redacted]@yahoo.com

[OC: No decrypt available for this PGP encrypted message.]

***

Как работает PGP?


S
A
A
S

Публичный ключ выглядит так:

-----BEGIN PGP PUBLIC KEY BLOCK-----
mI0EV+8yFwEEAOygoNBKEPl/SiNxPb3Uq5W75cX9B2TmwYagLboifZdiCxozj7XX
b39QPmjeHnoxWKYGSfshGbKGW+RpqjNJkUwyjlJp5lH70Kj3JjLy36h3fJ963vcg
Ur0UKyTn+QIs5ePogSVyHhfC45RPwkZRmd4/HPhMBuNDFUIw/AN0XRYfABEBAAG0
C0NyeXB0bIBhcnR5iLgEEwECACIFAlfvMhcCGwMGCwkIBwMCBhUIAgkKCwQWAgMB
Ah4BAheAAAoJEIwmVKbI7KOs/UAD/IaZYs7gaEUtnhERkh05mRIH8xTDnPFdIdv9
bTiqrdtyIOLnSuI7P8XoUvxjkvlyI/NMgENS8WOYXK+iDXvikZ9MqnRjhM/NErNI
05apOJ0/JoTw+Ks0bUhUcfZSbjNOC0VakNKY74HEKffV3e+c/iglJzUAyEkM+sIM
A+d0XwZx
=3/wJ
-----END PGP PUBLIC KEY BLOCK-----

Например, зашифрованное сообщение выглядит так:

-----BEGIN PGP MESSAGE-----
jA0EAwMCgIjZTeRJlkNgyVDGJu44088NxfOmvDBZovUjkgAuEsBU6CjRRpwqrVFh
T+MFmt6+FYh/yKPt8kiDtO0d0/xkvckNMU2M/iPD5uIlqM+HACmZv06HioE9mZeY
8g==
=V84U
-----END PGP MESSAGE-----

Сертификат отзыва

Сообщение о недействительности ключа, подписанное самим ключом.
При публикации сертификата ключ ”становится недействительным”

Защита работы на компьютере

Tails

Запускается с флешки

Ориентированный на приватность вариант GNU\Linux

Все соединения через Tor или I2P

OTR, GPG и все,
что нужно для работы

Ссылки

Tor
https://torproject.org/
Orbot (Android)

OTR
Pidgin/Adium/CoyIM
(Linux, Windows, macOS)
Conversations (Android)
ChatSecure (iOS, Android)

GnuPG
https://gnupg.org/
GnuPG+Thunderbird+Enigmail (Desktop)
OpenKeyChain+K9-Mail (Android)

Tails
https://tails.boum.org/