Система PGP

Тема: Криптография

Генералов Даниил 1032212280

Две проблемы системы шифрования

Конфиденциальность:

- Симметричное шифрование (AES, DES, Salsa20, Кузнечик)
- Установление общего ключа (Diffie-Hellman)

Две проблемы системы шифрования

Конфиденциальность:

- Симметричное шифрование (AES, DES, Salsa20, Кузнечик)
- Установление общего ключа (Diffie-Hellman)

Аутентификация:

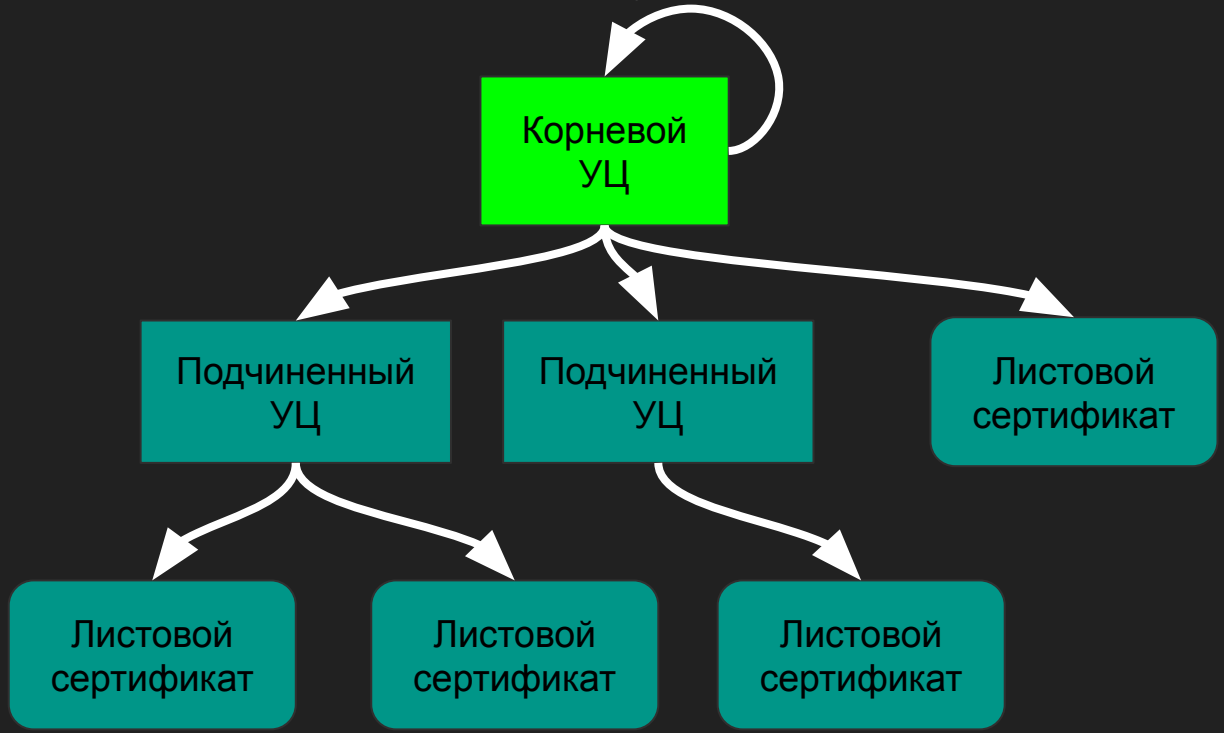
- Цифровые подписи
- Сертификаты

Сертификат проверки публичного ключа

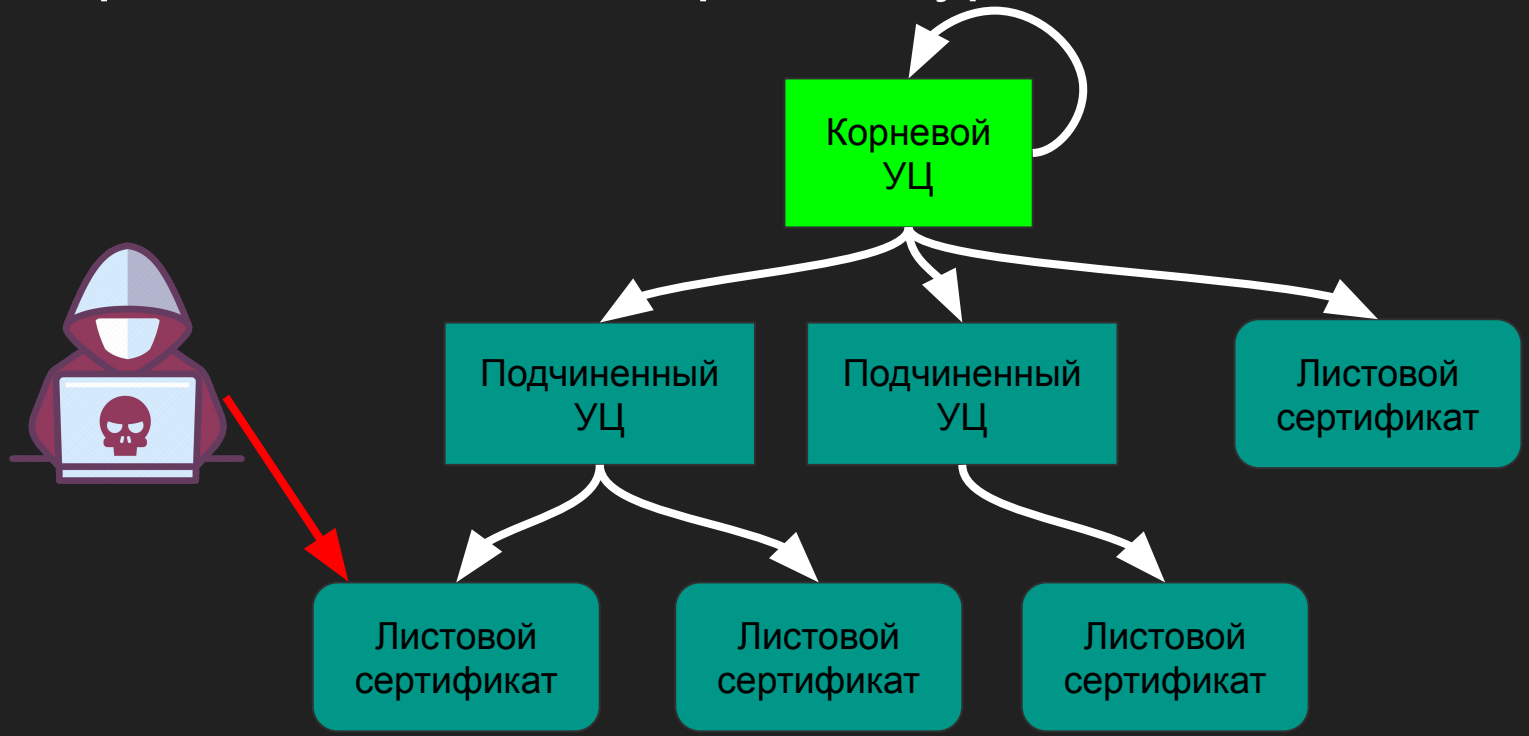
- Публичный ключ
- Идентификационные данные (имя, email, домен, …)
- Ограничения использования (назначение, срок действия, …)

+ Подпись от другого доверенного ключа, подтверждающая все вышеперечисленное.

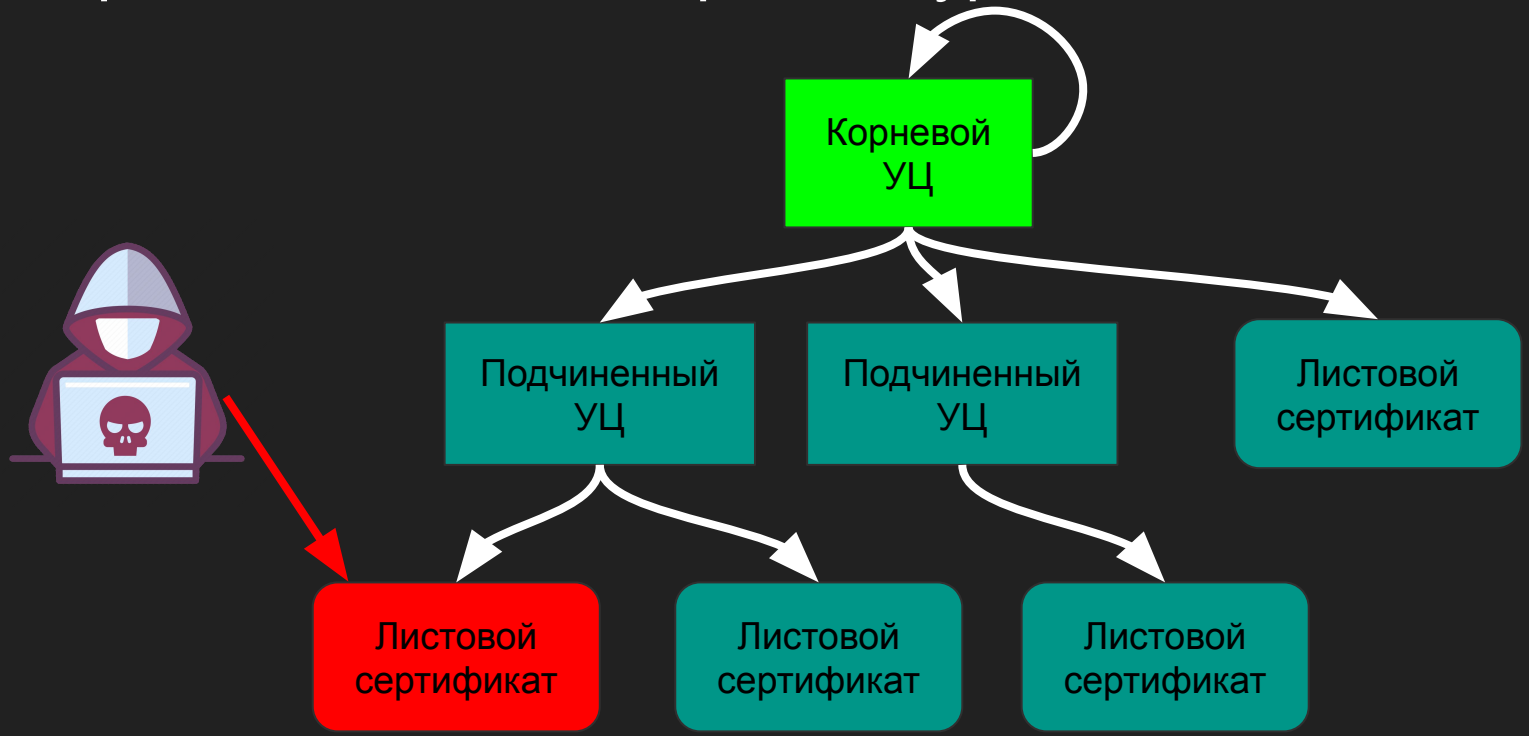
Традиционная PKI-архитектура



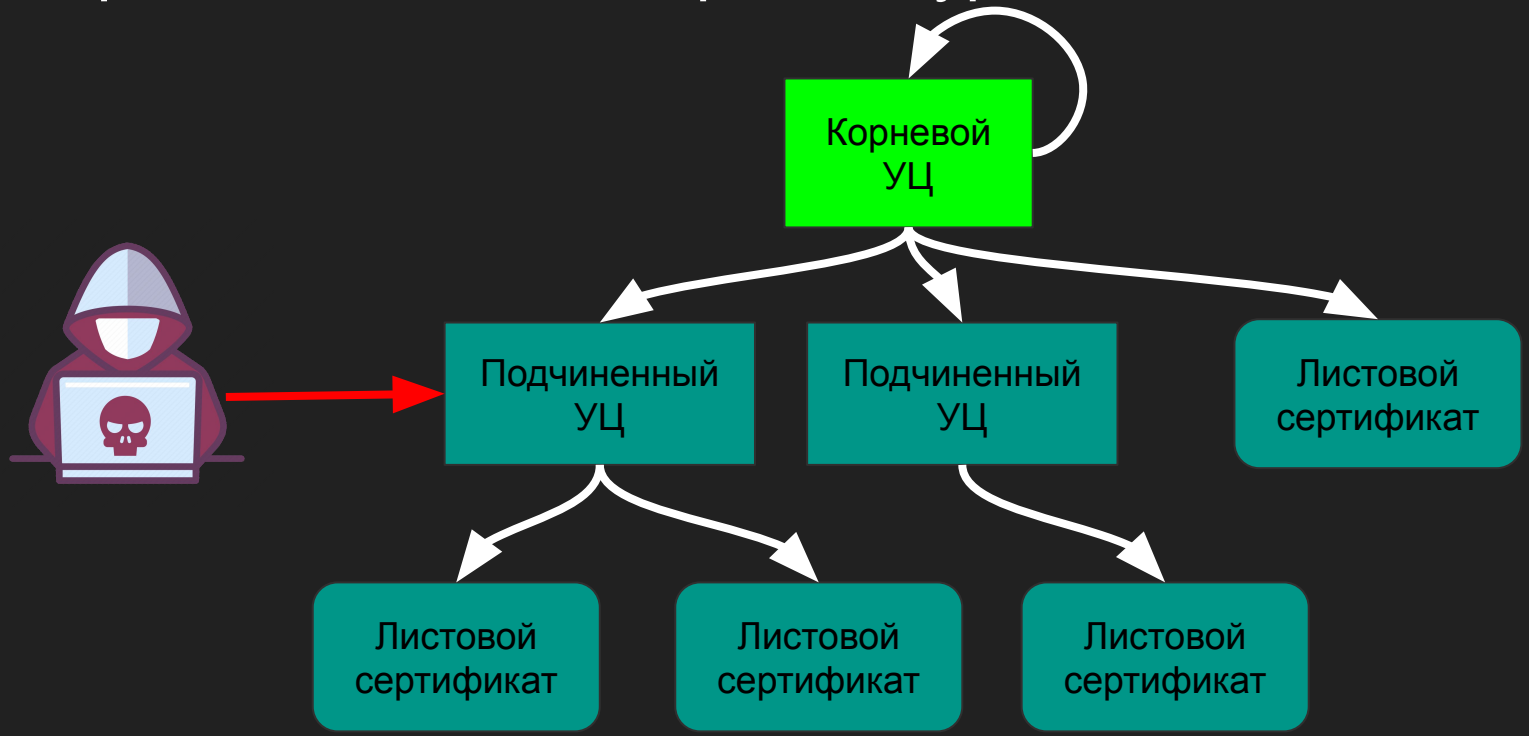
Традиционная PKI-архитектура



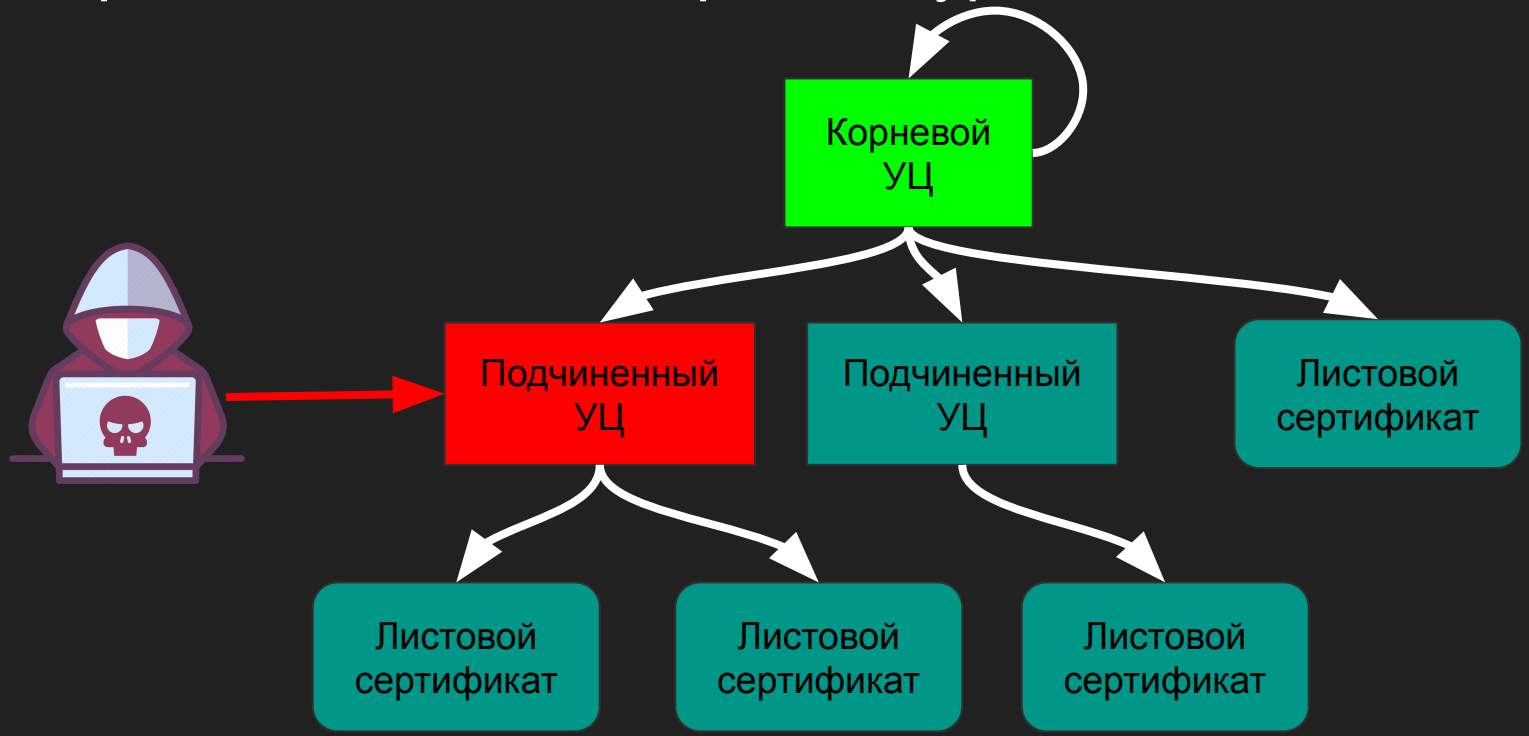
Традиционная PKI-архитектура



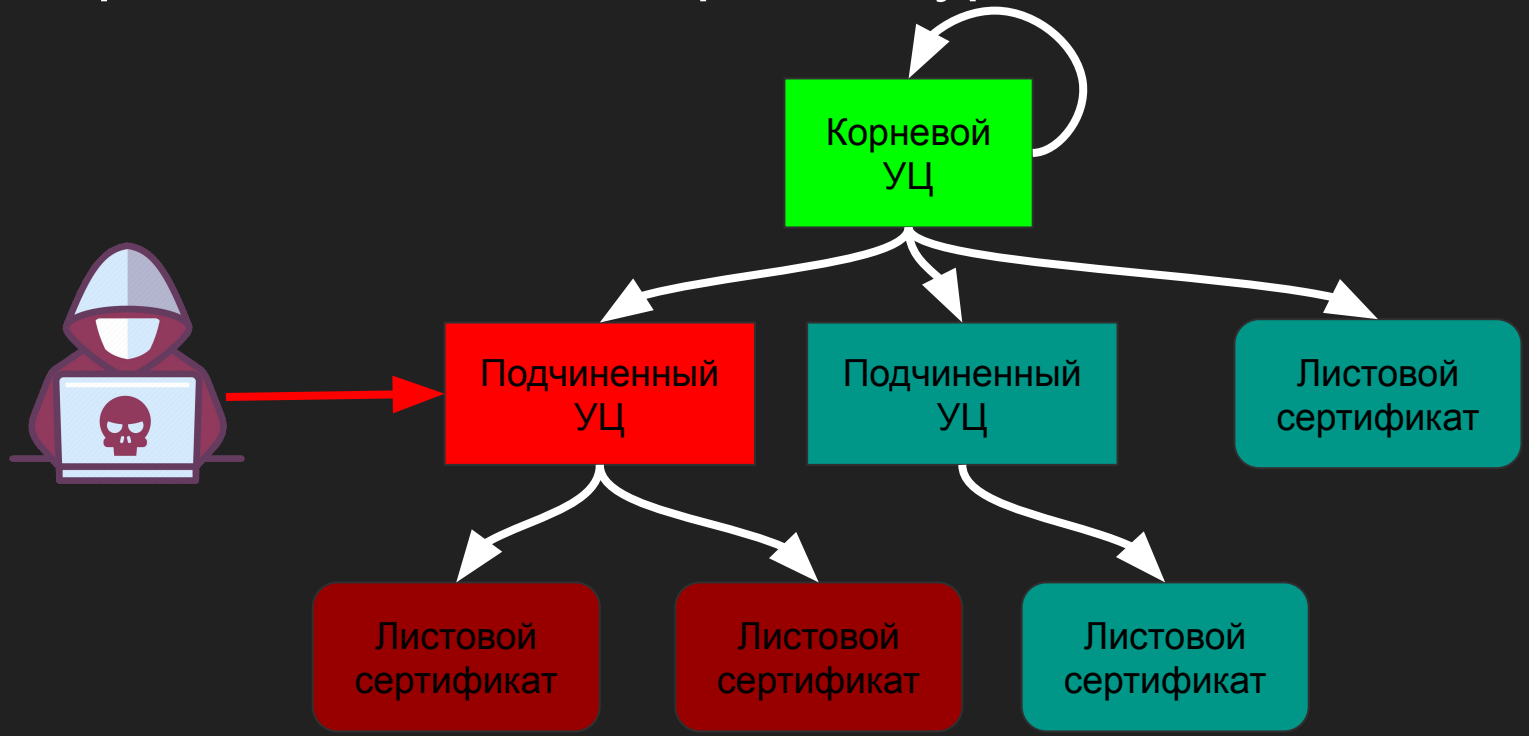
Традиционная PKI-архитектура



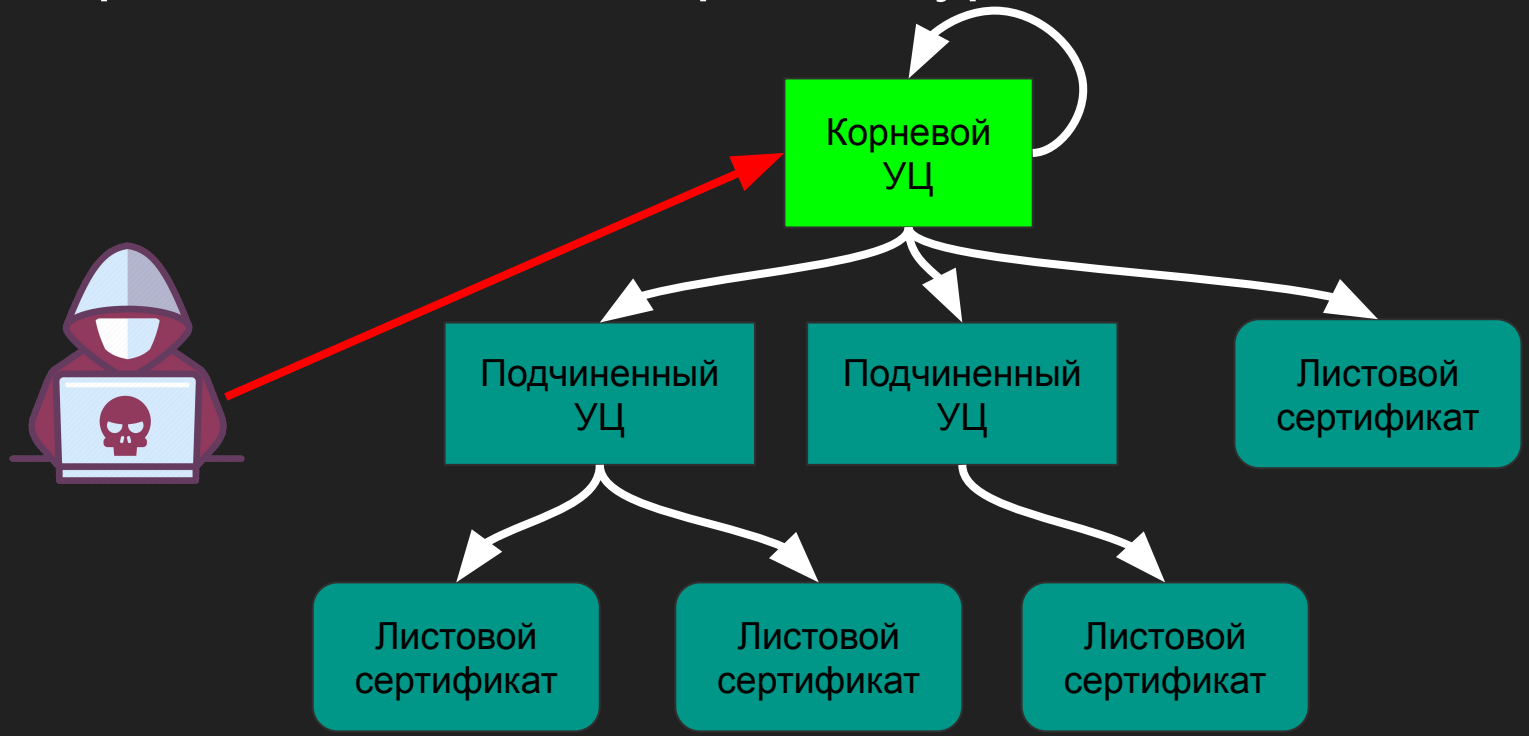
Традиционная PKI-архитектура



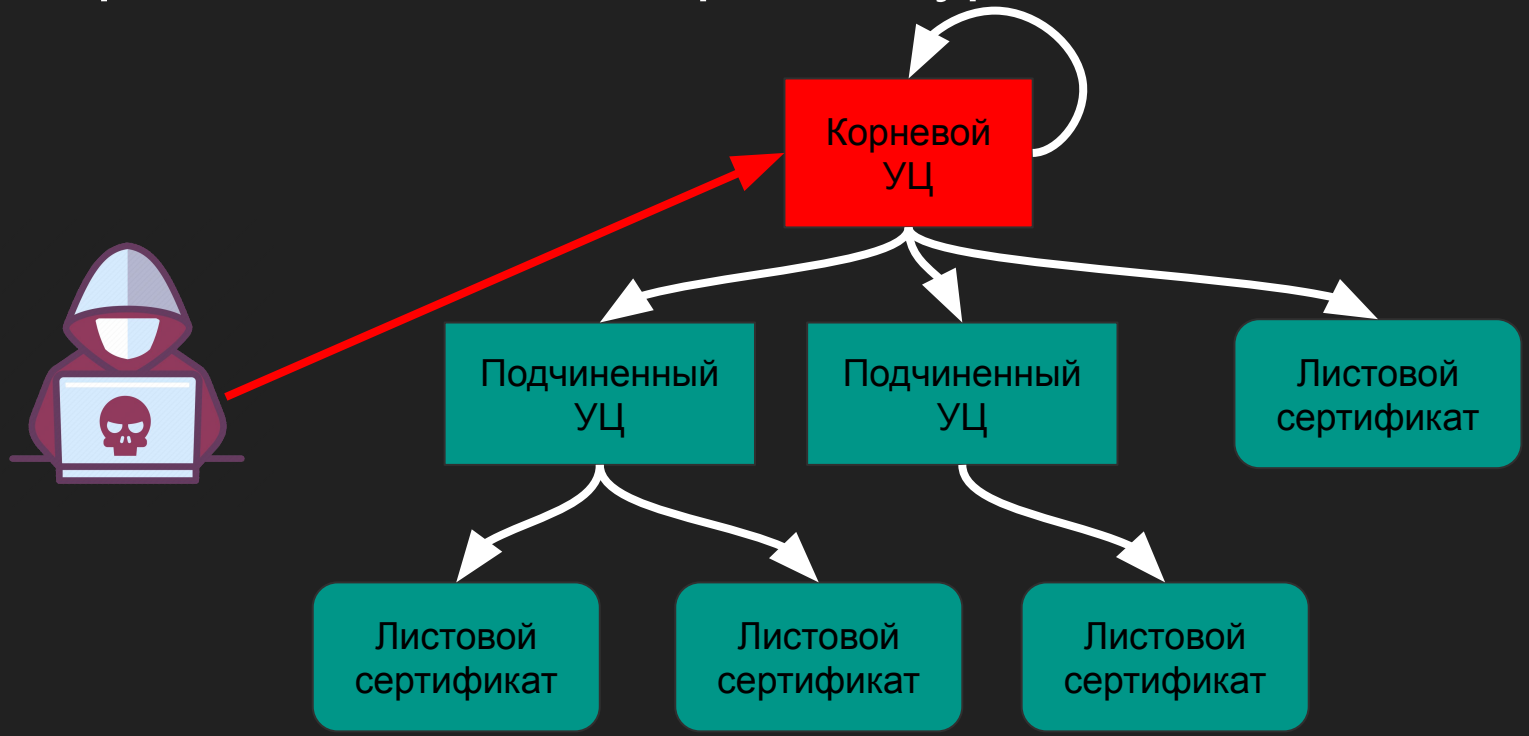
Традиционная PKI-архитектура



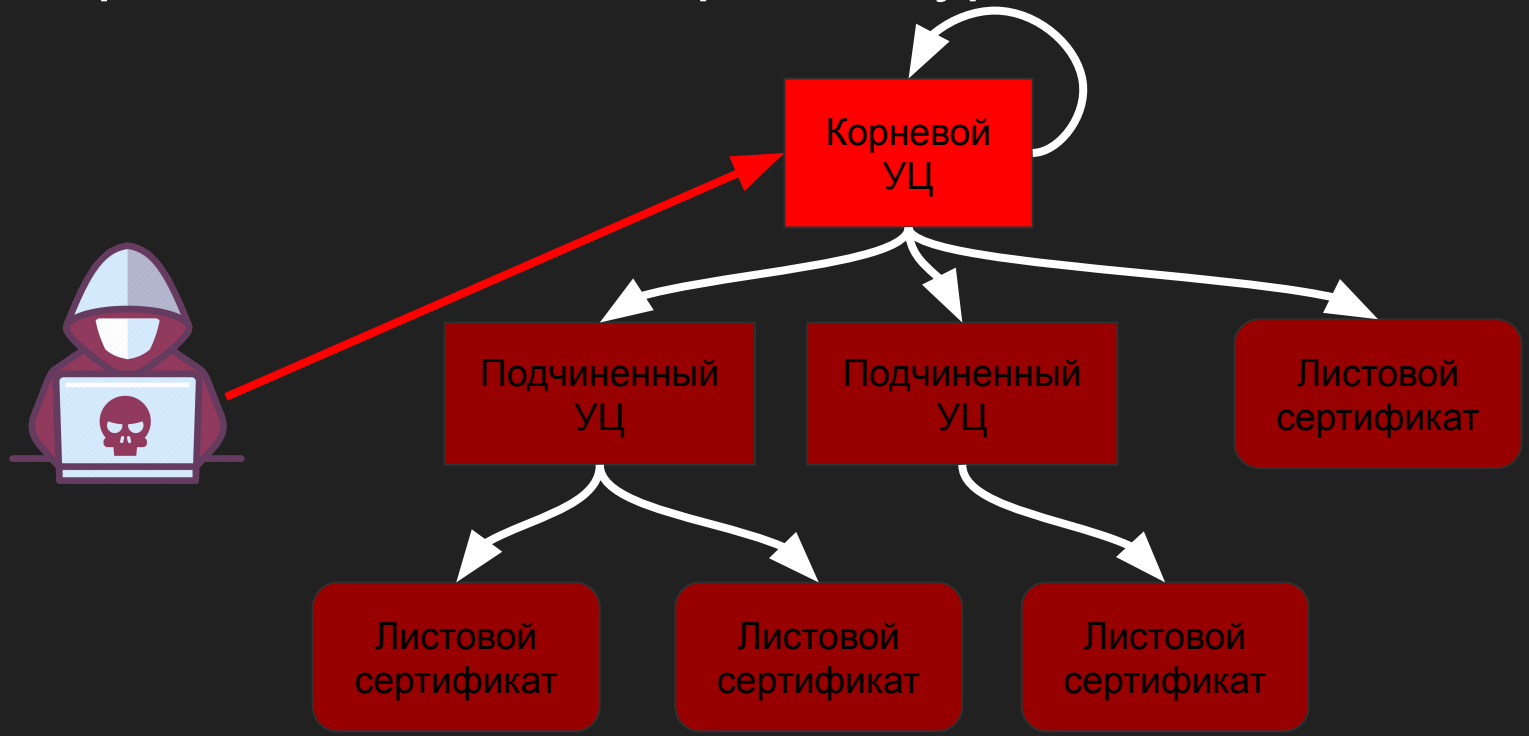
Традиционная PKI-архитектура



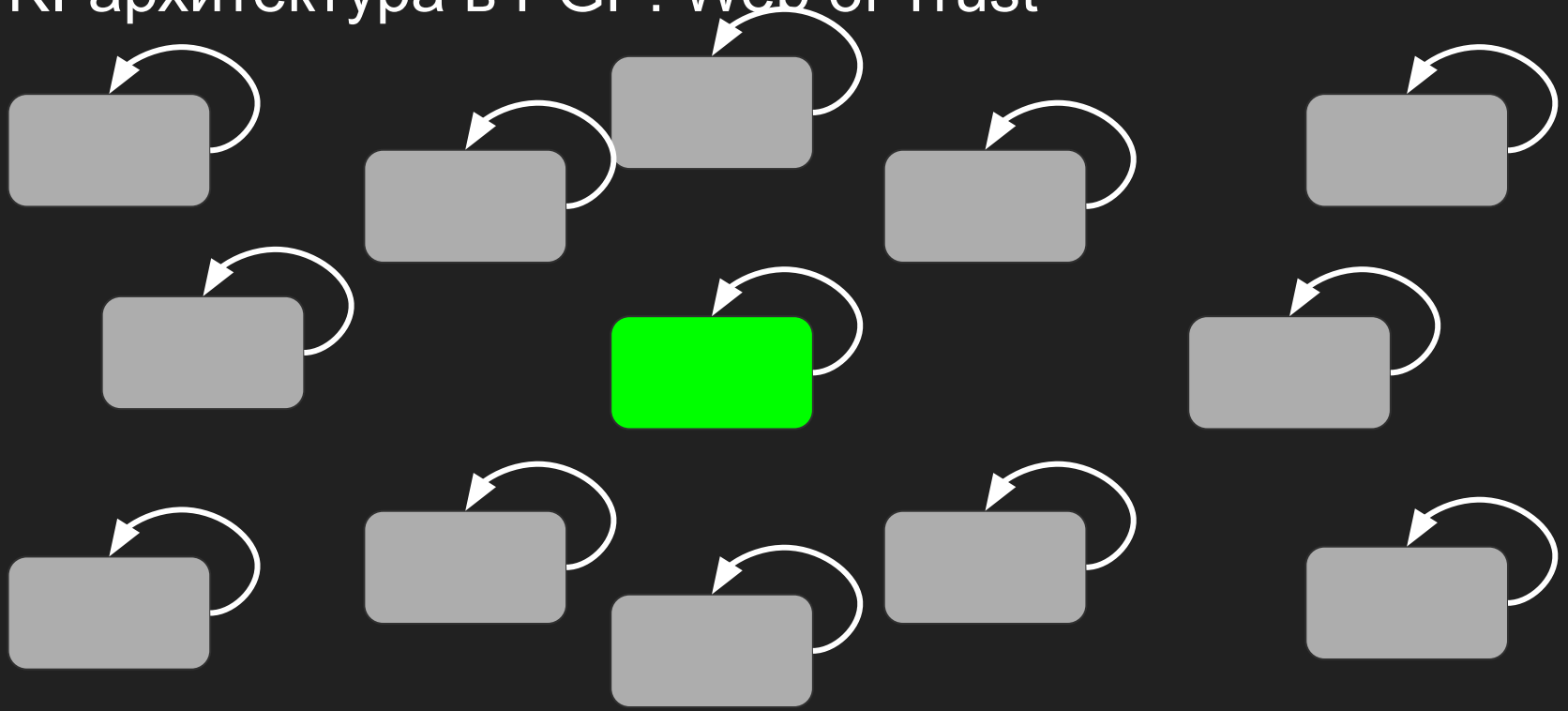
Традиционная PKI-архитектура



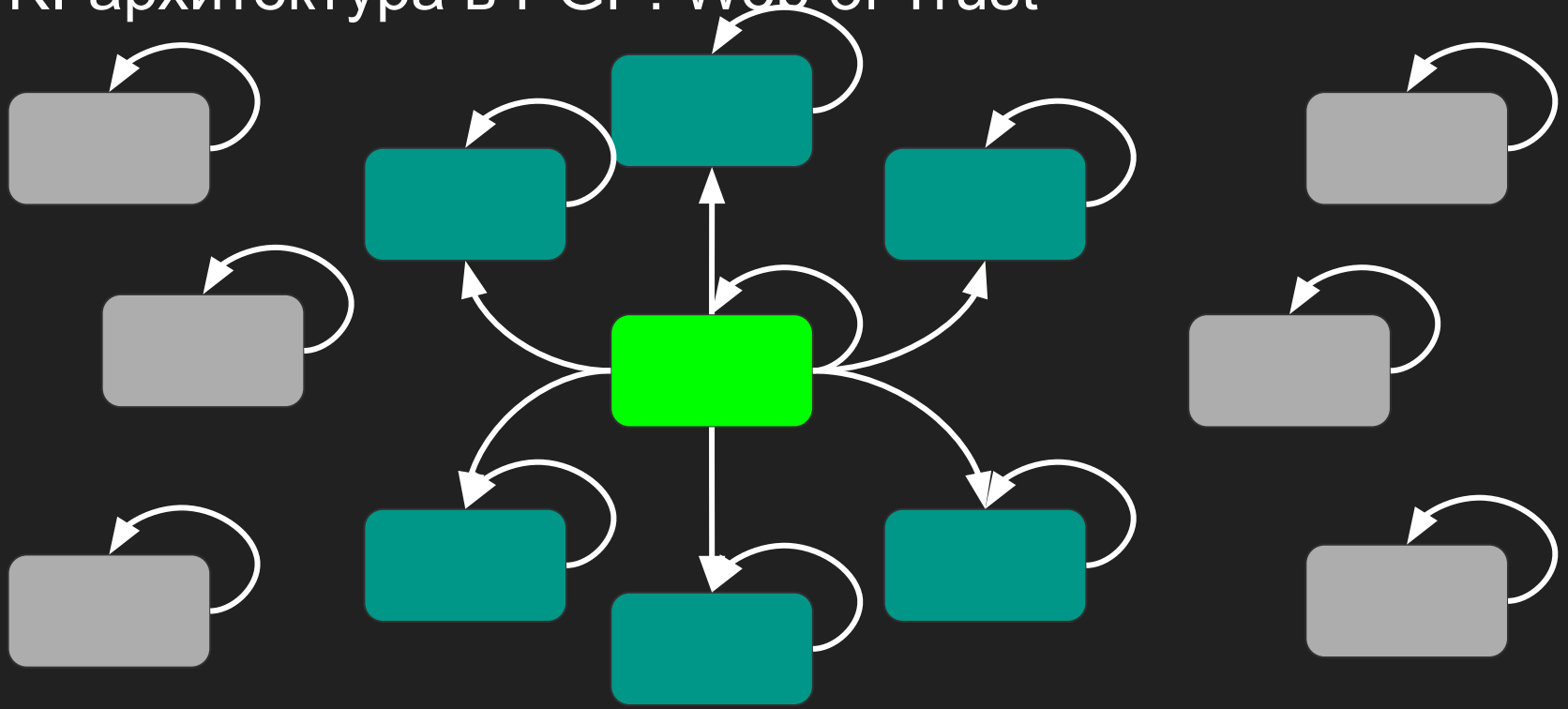
Традиционная PKI-архитектура



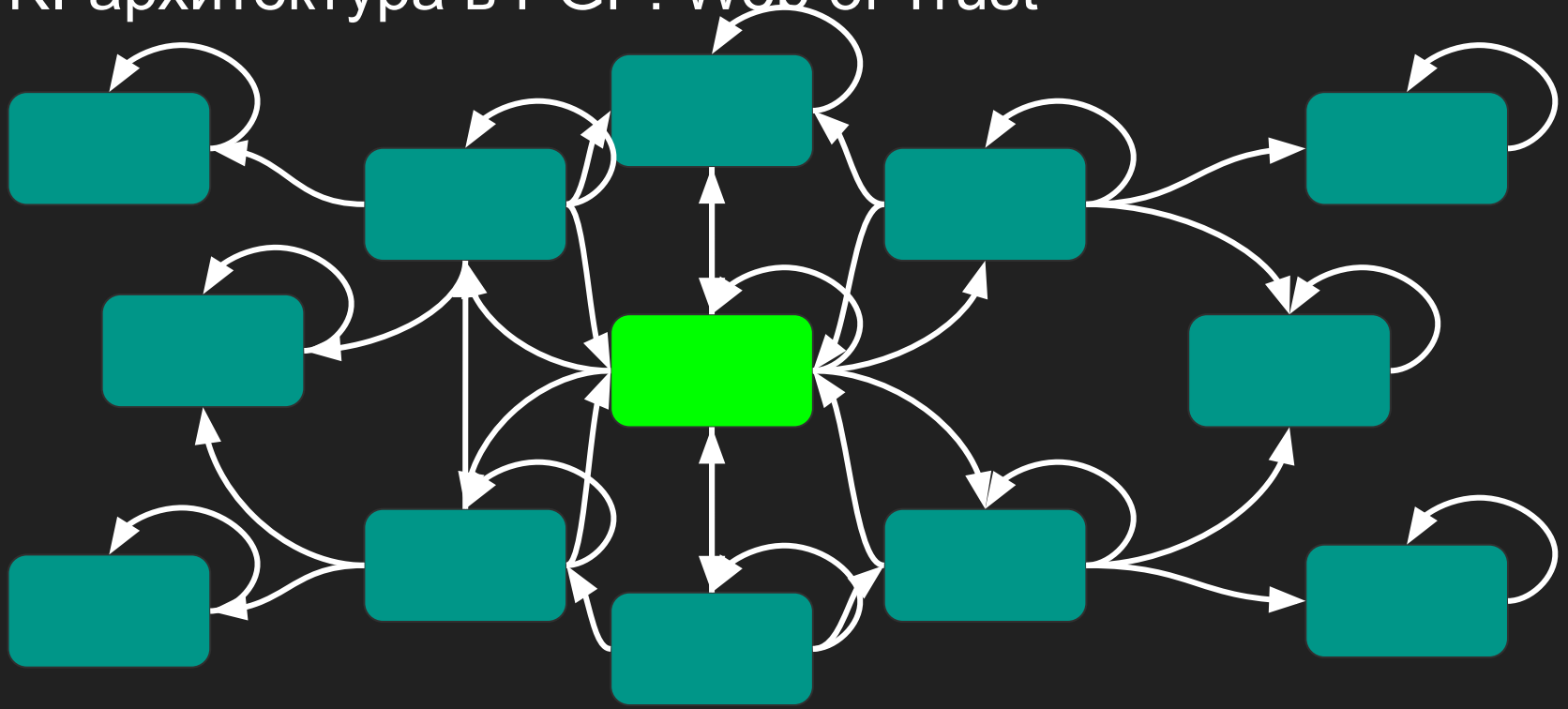
PKI-архитектура в PGP: Web of Trust



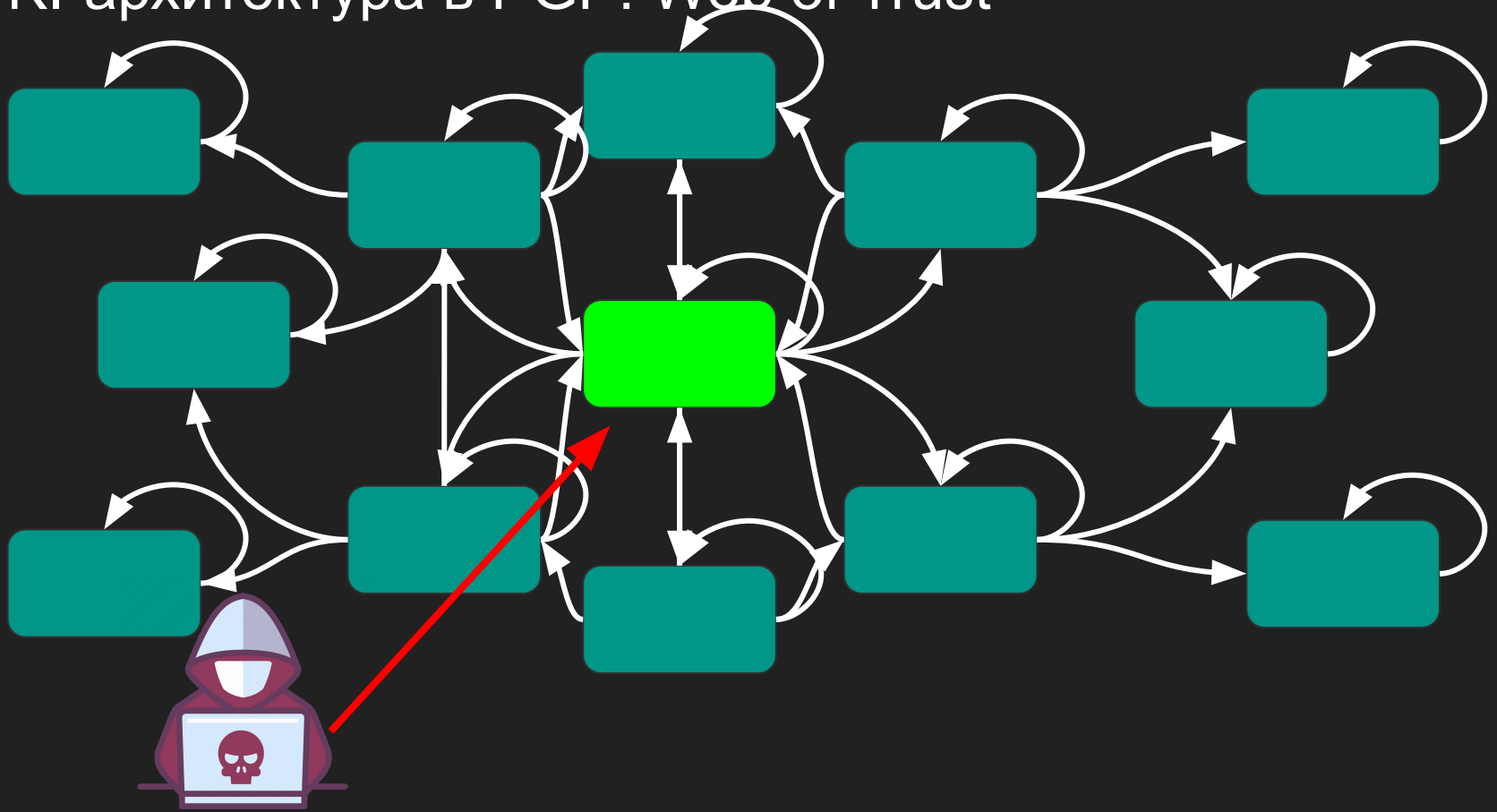
PKI-архитектура в PGP: Web of Trust



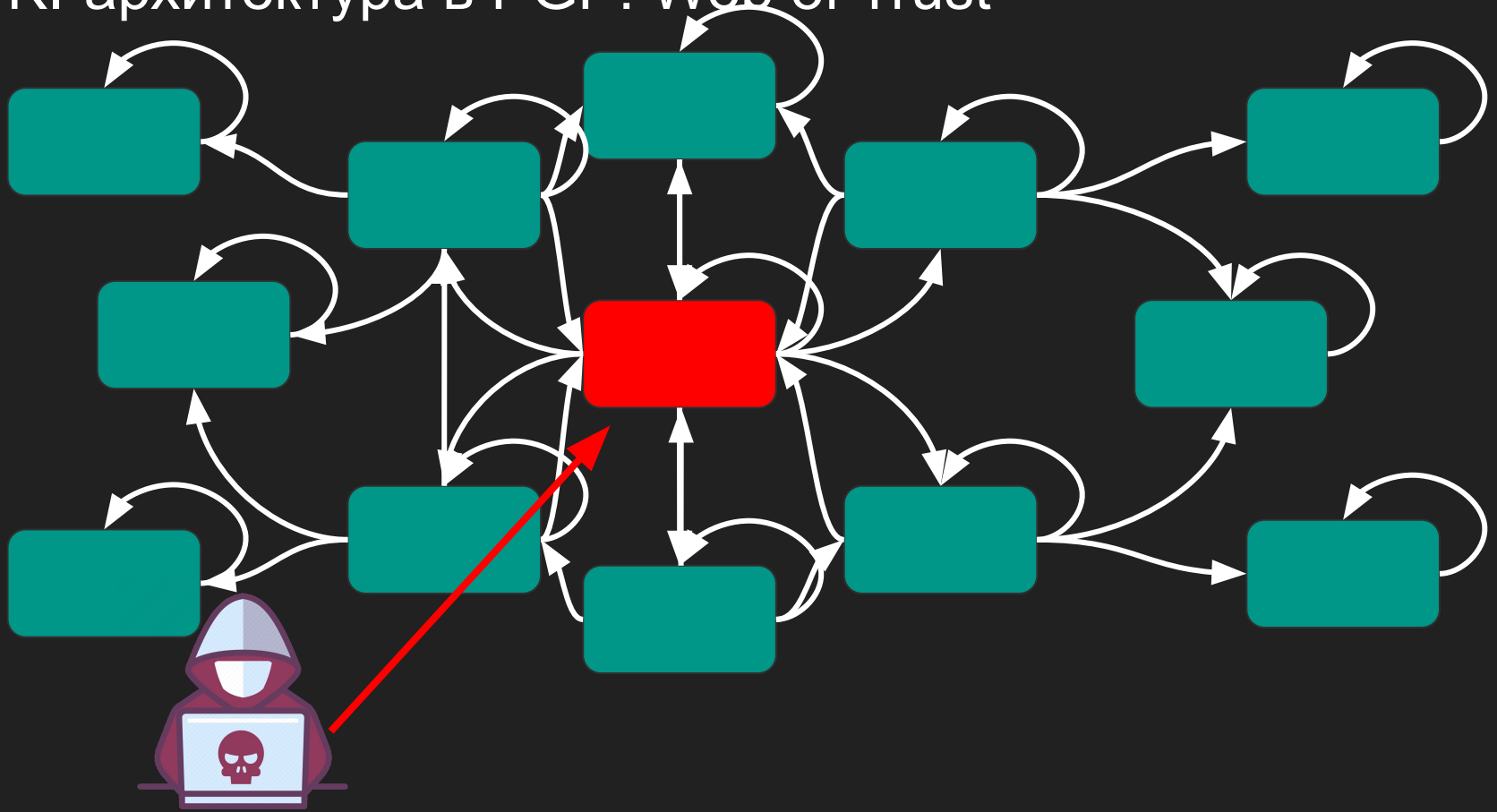
PKI-архитектура в PGP: Web of Trust



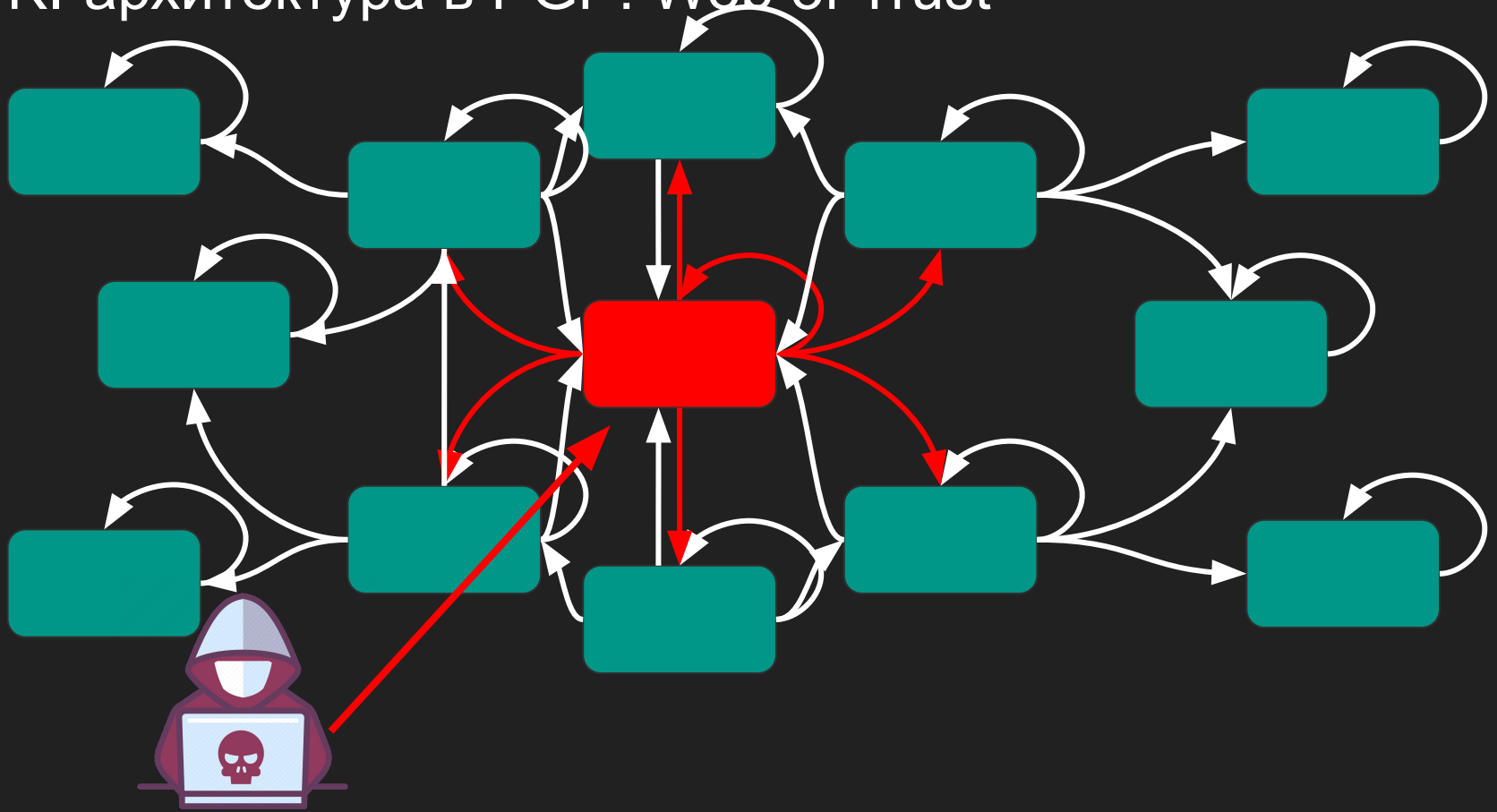
PKI-архитектура в PGP: Web of Trust



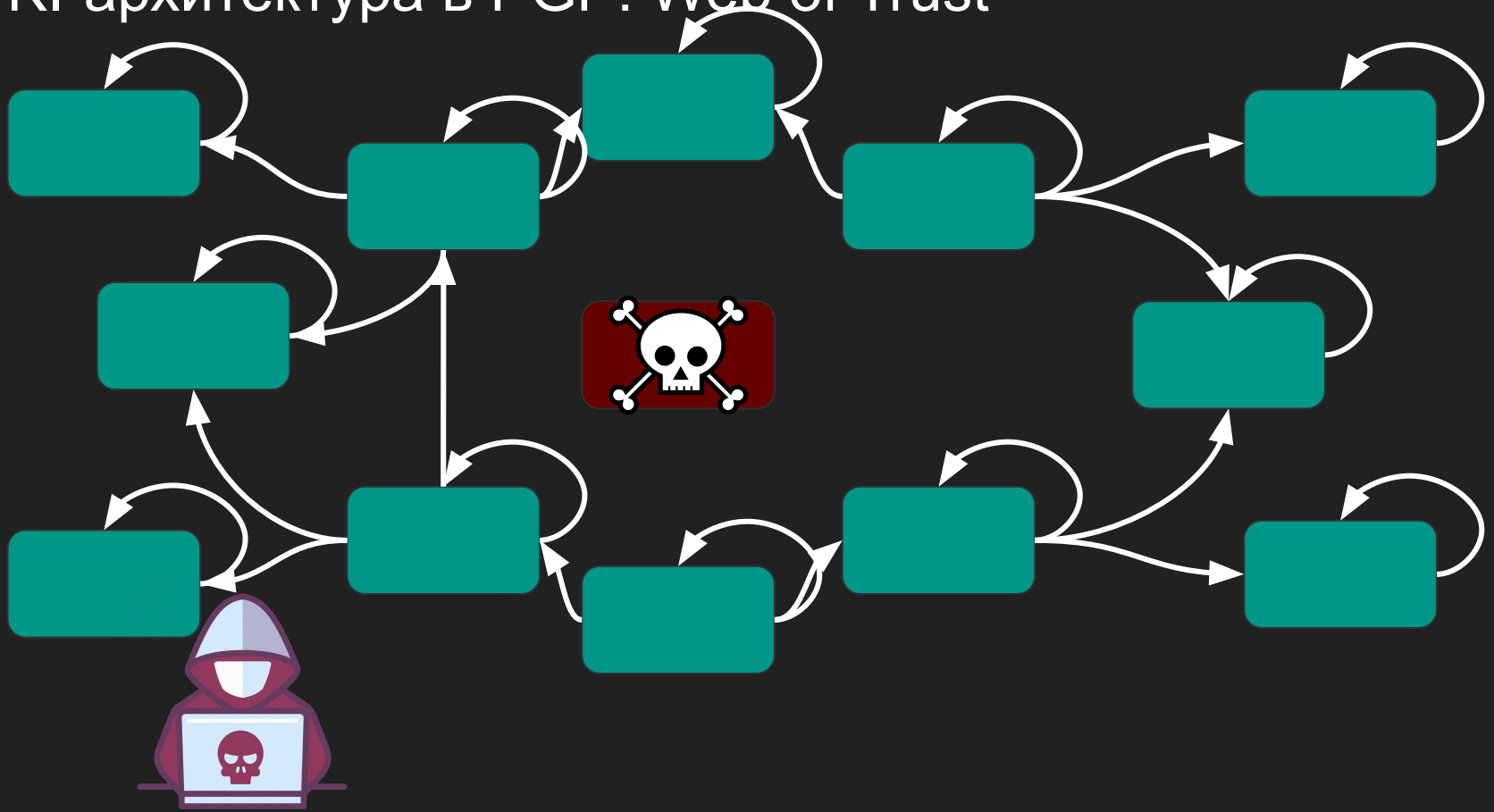
PKI-архитектура в PGP: Web of Trust



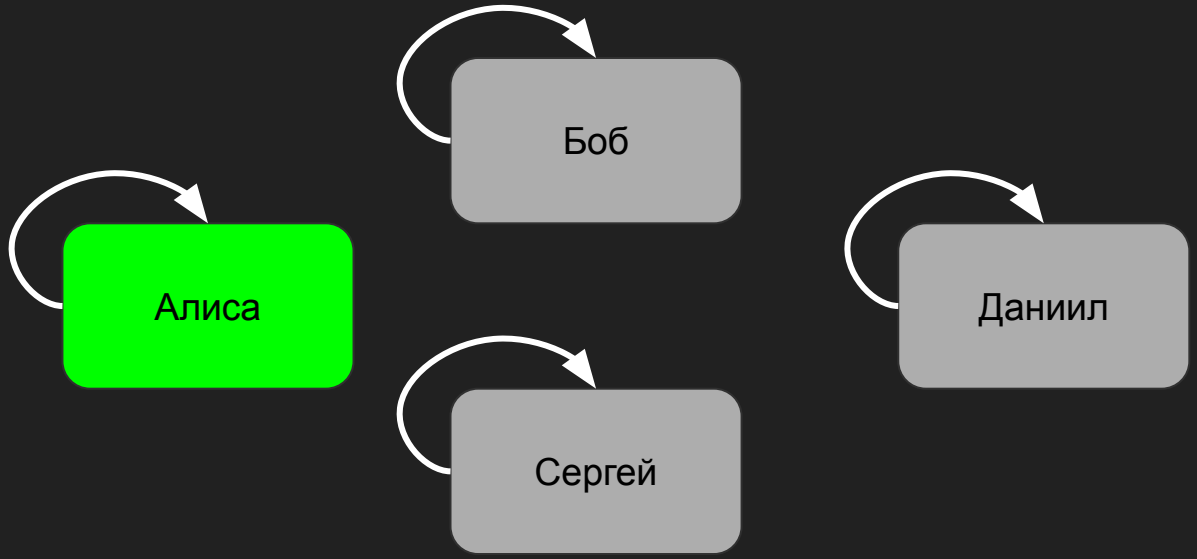
PKI-архитектура в PGP: Web of Trust



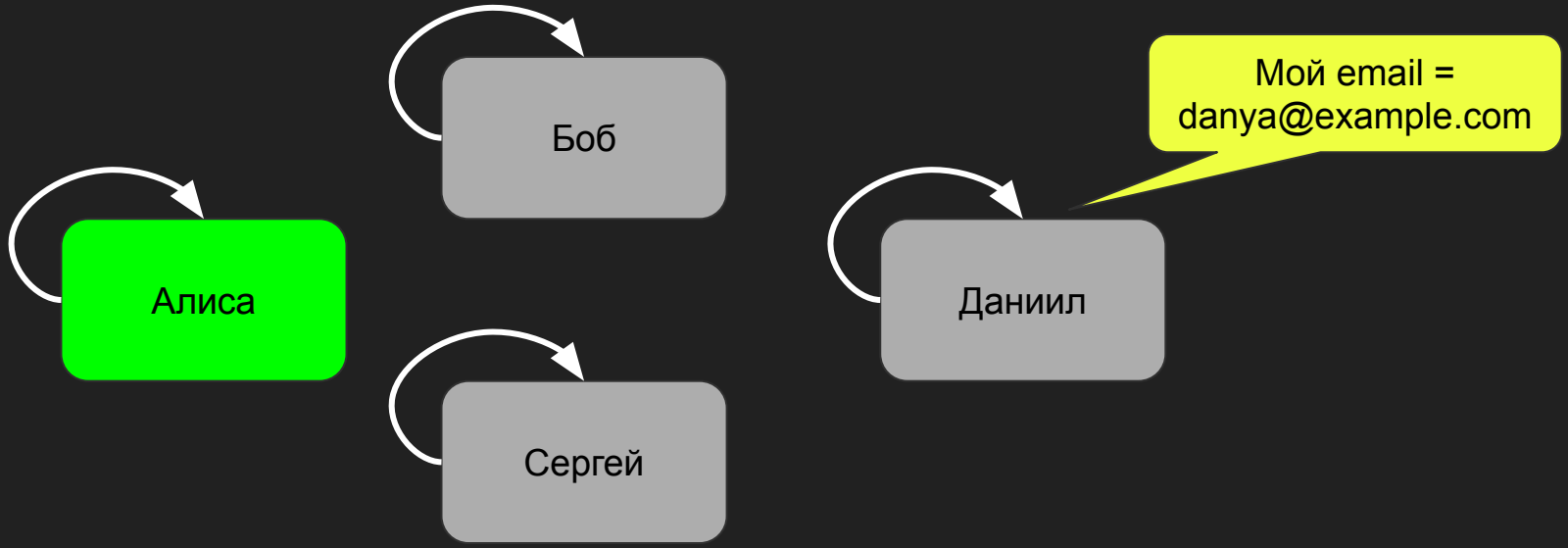
PKI-архитектура в PGP: Web of Trust



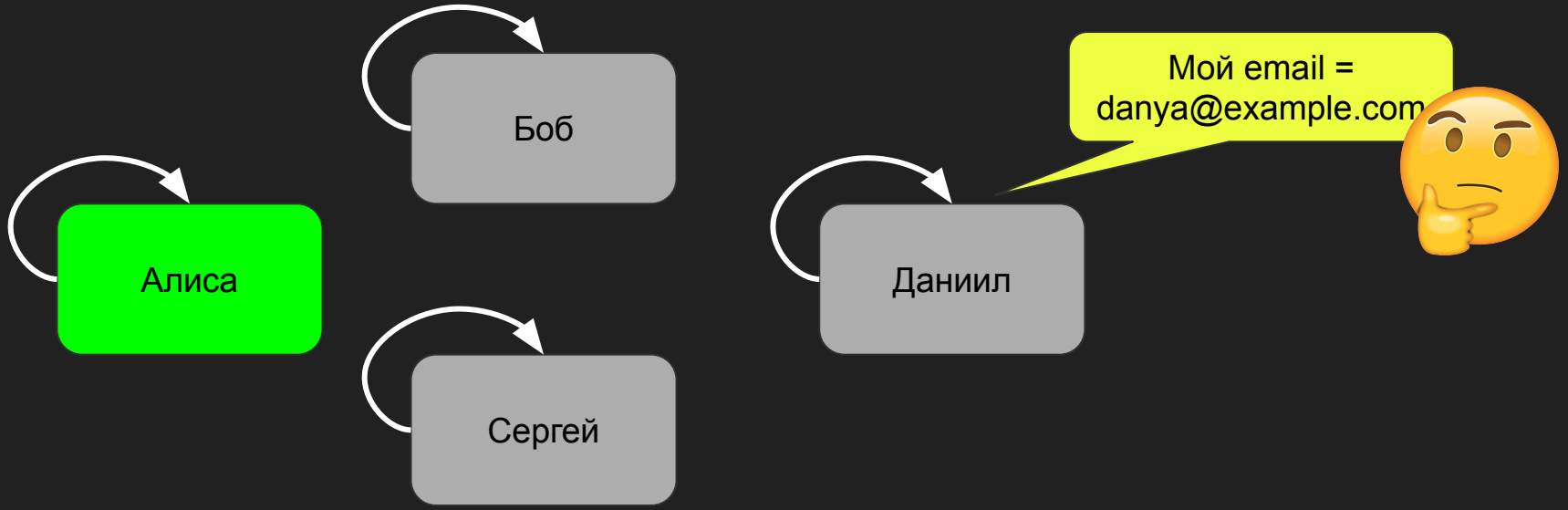
Транзитивность доверия



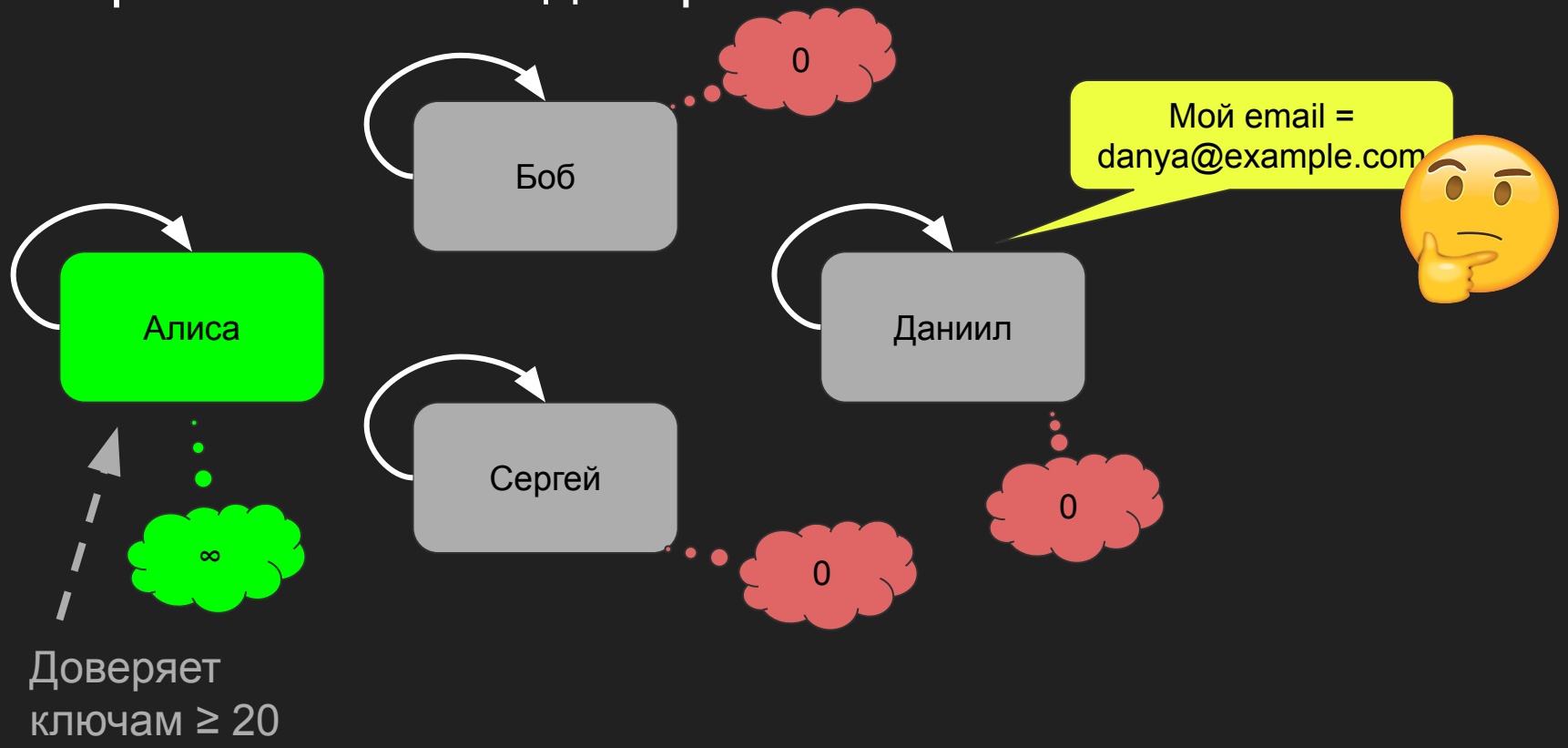
Транзитивность доверия



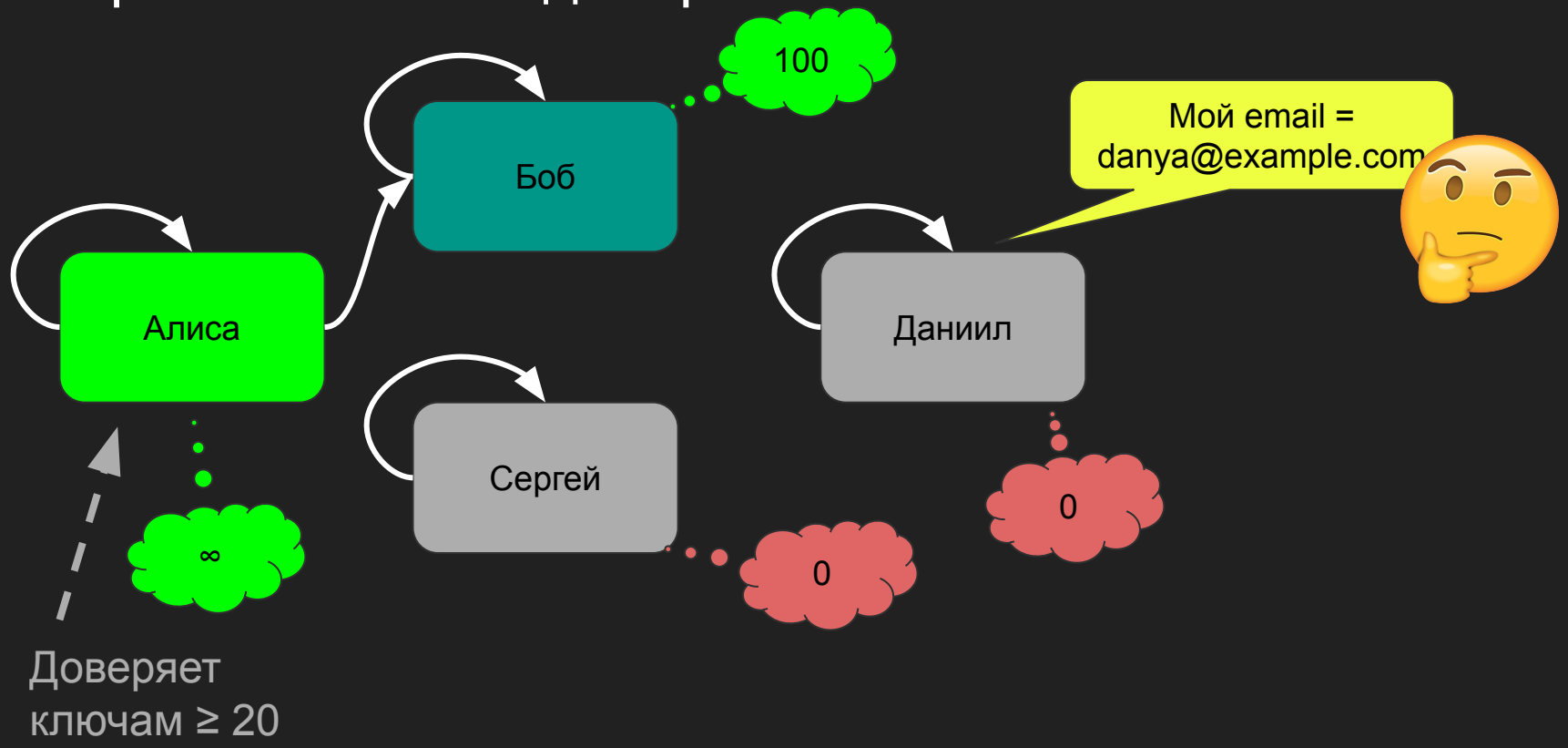
Транзитивность доверия



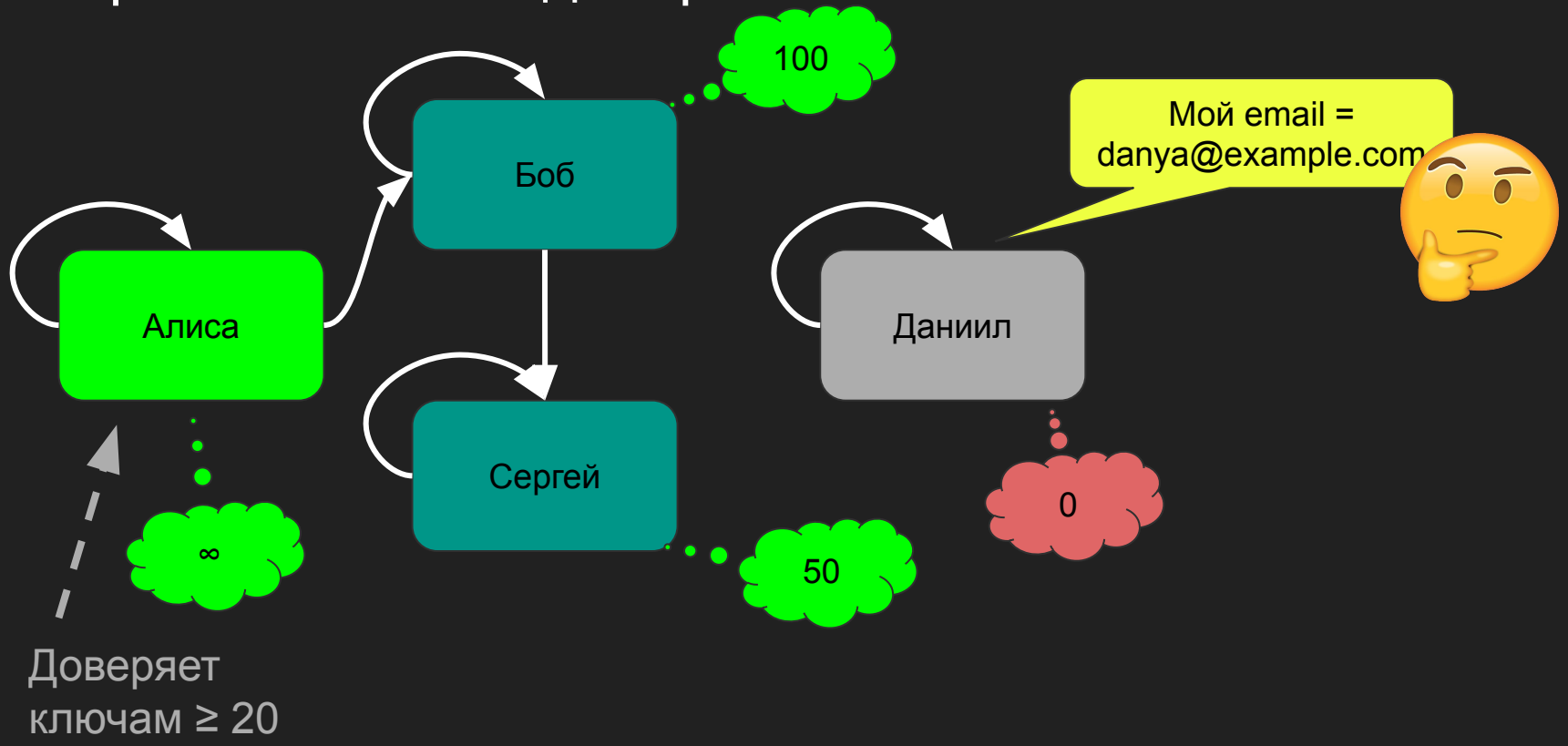
Транзитивность доверия



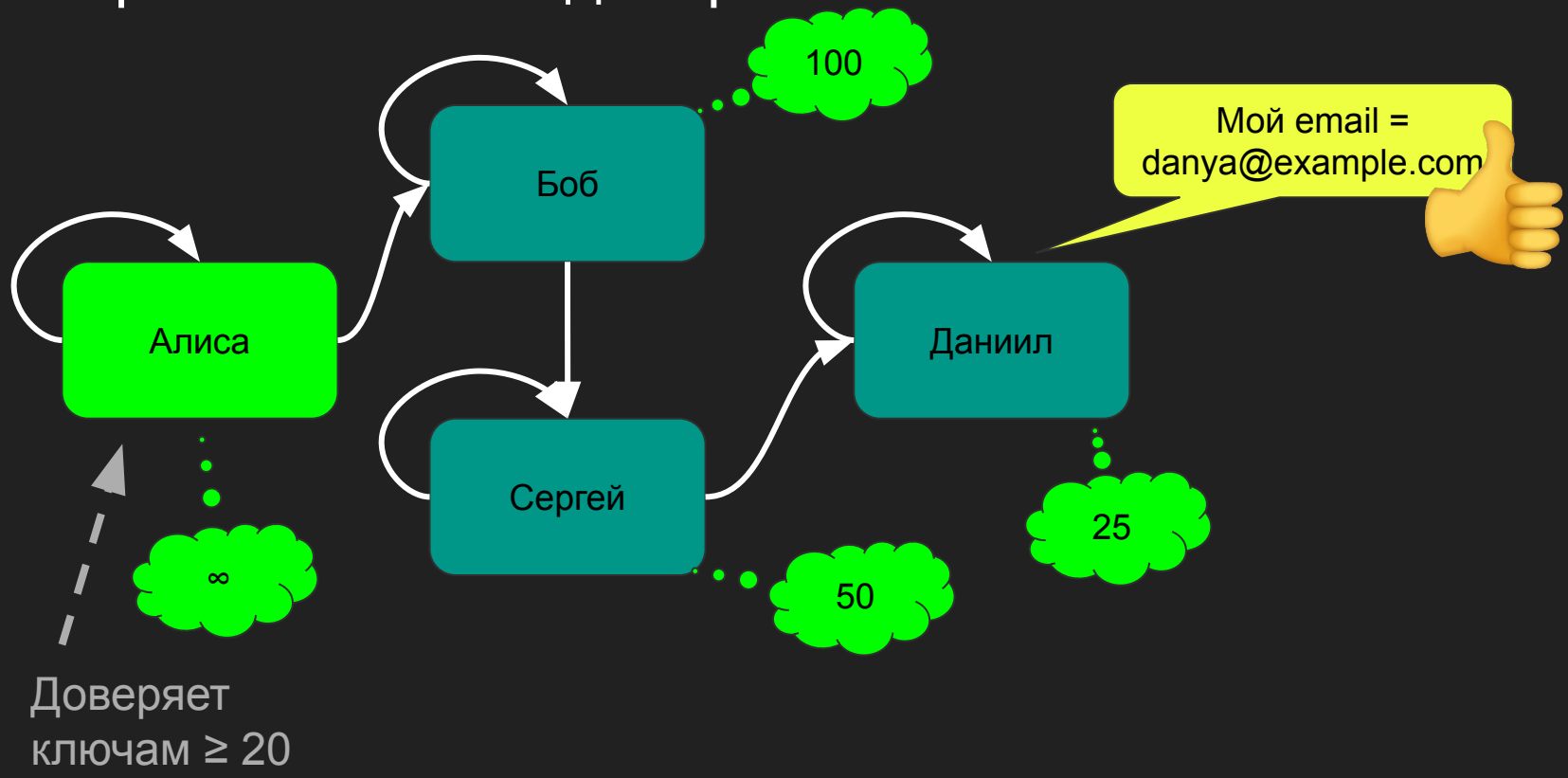
Транзитивность доверия



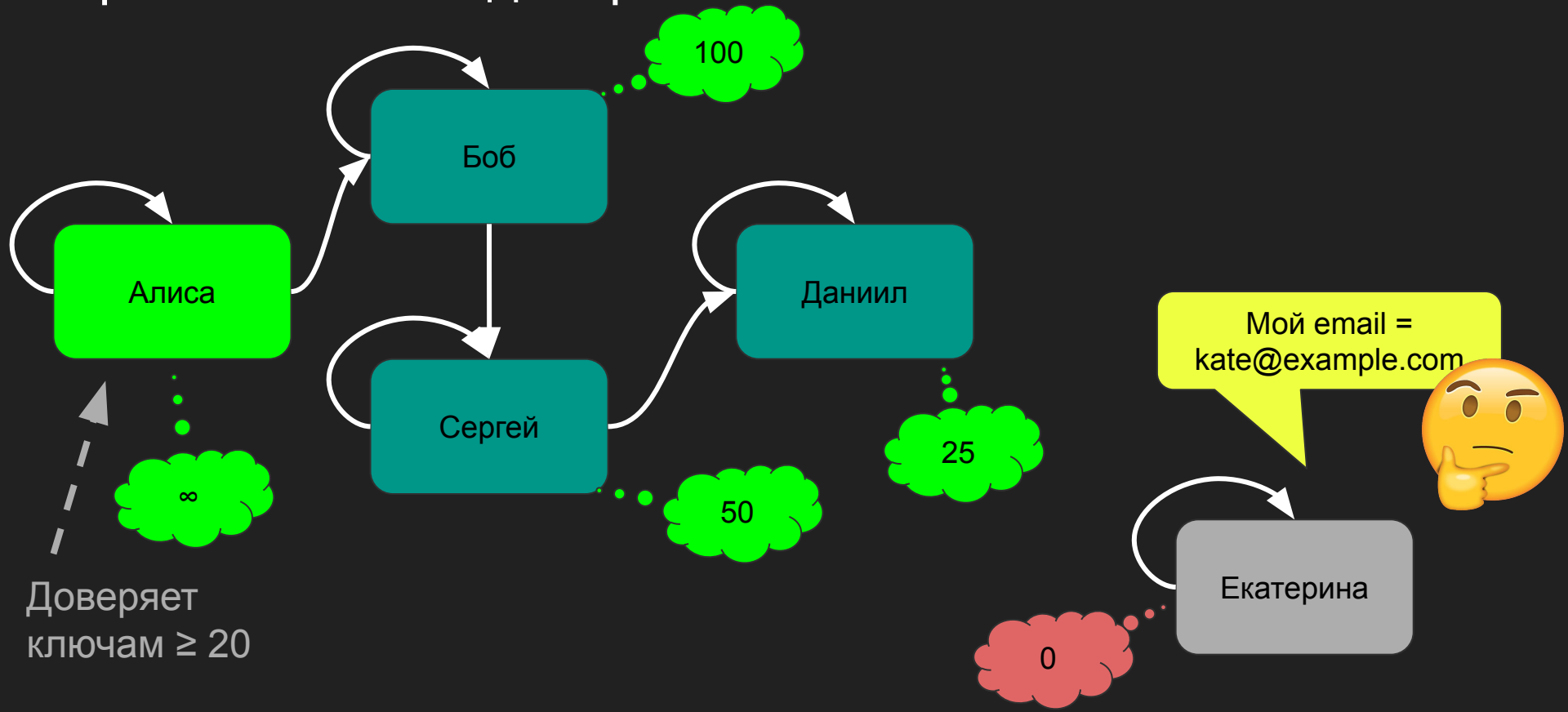
Транзитивность доверия



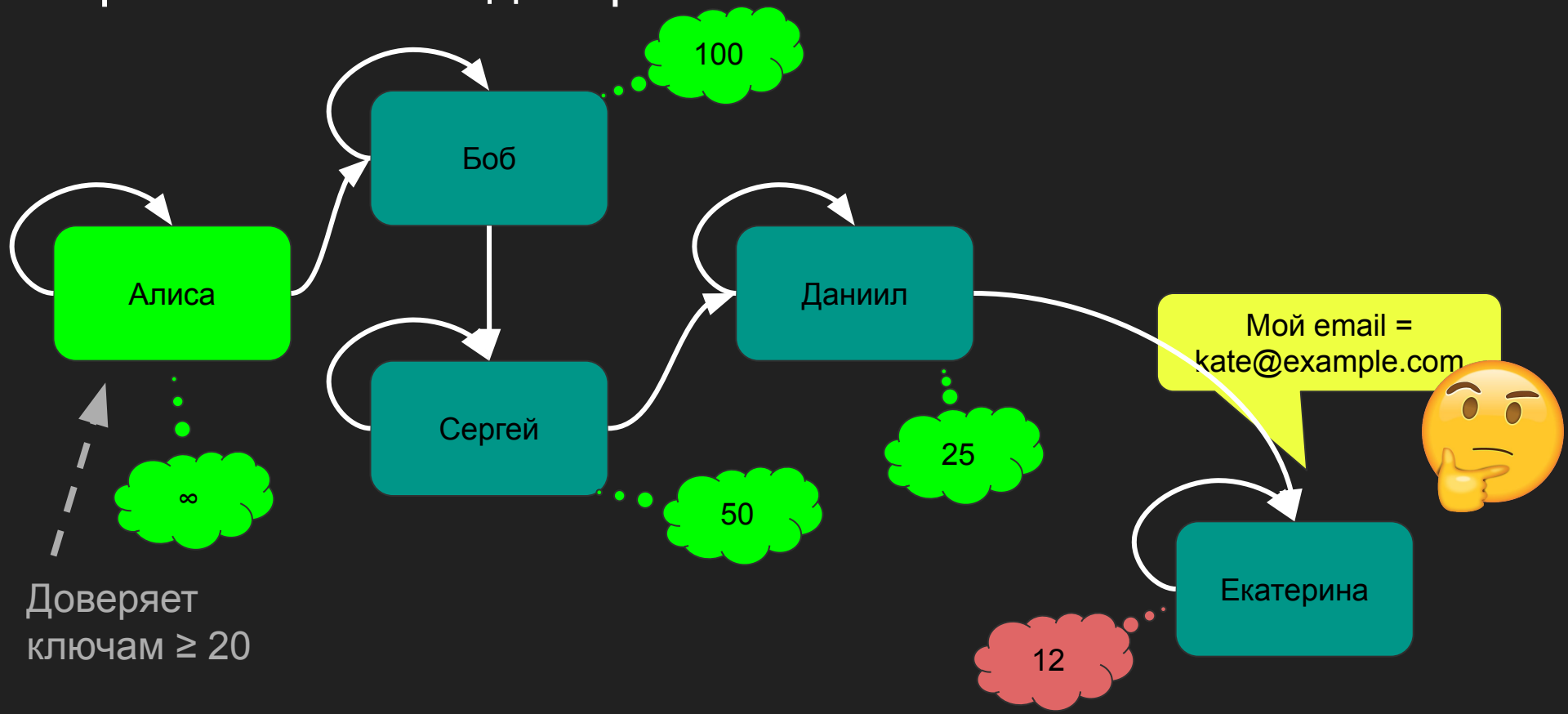
Транзитивность доверия



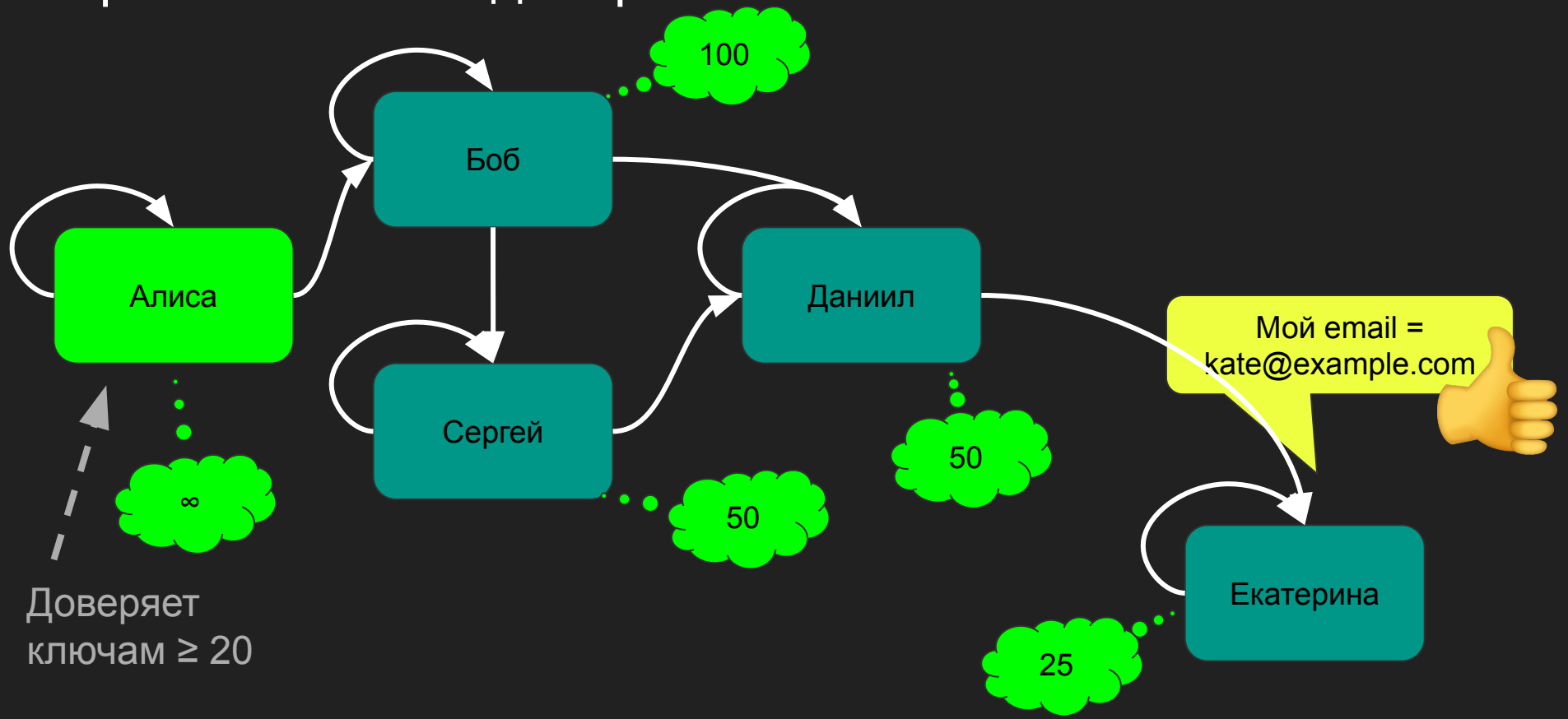
Транзитивность доверия



Транзитивность доверия

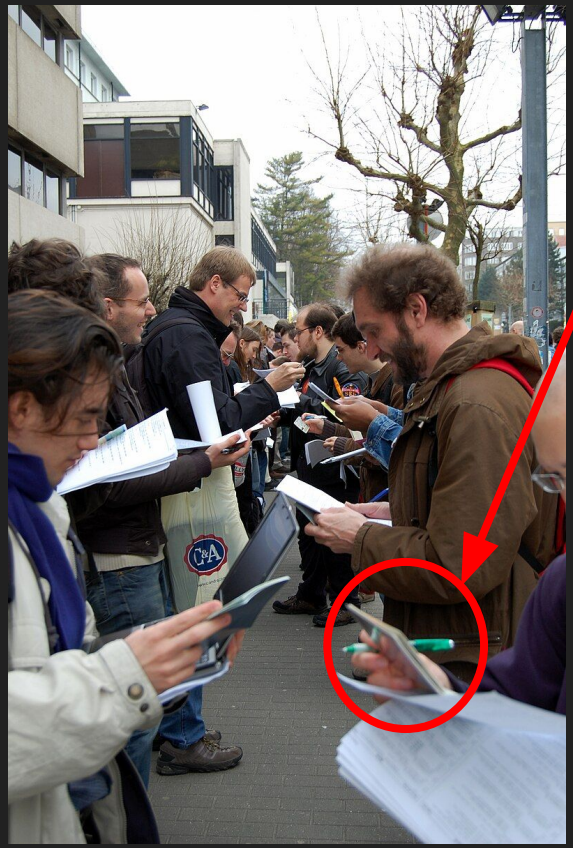


Транзитивность доверия



Key-Signing Party

Key-Signing Party



1. Проверить паспорт

Key-Signing Party

1. Проверить паспорт
2. Проверить информацию в ключе

Key-Signing Party

1. Проверить паспорт
2. Проверить информацию в ключе
3. Создать и опубликовать подпись

Key-Signing Party

1. Проверить паспорт
2. Проверить информацию в ключе
3. Создать и опубликовать подпись
4. (Или записать инфу, чтобы сделать дома)

Употребления PGP

- Зашифрованная электронная почта (изначальное применение)

Употребления PGP

- Зашифрованная электронная почта (изначальное применение)
- Подтверждение подлинности Git-коммитов

Употребления PGP

- Зашифрованная электронная почта (изначальное применение)
- Подтверждение подлинности Git-коммитов
- Подпись пакетов репозиториев ПО

Употребления PGP

- Зашифрованная электронная почта (изначальное применение)
- Подтверждение подлинности Git-коммитов
- Подпись пакетов репозиториев ПО
- Подпись запускаемых файлов с помощью digsig (только в Astra Linux)

Недостатки

- RSA + сертификаты → большие ключи

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFeHhzMBEADn0rLyZYTiwEoGnHLgNSV2HJ/JD9+Qz6wG+V3vHa/ahHyQ1YsL
LYyA0x3SG99Ur7UeEBhbGt8cb8x4llhQNpFL60AJAKAkJb34uIkaC1oNWrr3FAKe
DIp1cu3BvgM2Arj2L9T4UvrjjgspKjLBgGlVkhzkR07HKM9IUePeV3mxYQgsYTfb
XjdoDnm+ZHc0sY3YNZsN6XWFRZp07urxOOxkdkOtXahAyMfNMLEbJ2t9TXA7Y6RX
vvH6tY73S5zeFRum7SW0zNPMhe7Ow9ArAB33eELHsYQkMfnrGEnvXlGc+09wVKzy
JQf/mZxPwCkye5mUpkMokFAuCuFHrPHhlct39XxaMwfeFsz+WoC3Z3A8inFi5wWL
X8MgvOuJY33uS0h2Pav9T8MHPzgydtgBt3g6tFZSE629PPmWM8oCTN2QbvXxkyn4
2ABu/ne+FGbmAsEzc2oZF150tH+LPf1xAzwz9+f/0yD9wVBO9VqseinfYRMoxDD8
Gz3Dfz2PGeZUYexQ/1afMkPjhUR9MgY2CvPLYJWkvLN2z3fWT10dTU1PAMVzjC3c
dorHLAltCB2g66MMFBweZgYEf51EO3OnPctO5uVq4Q5vIaVkKcJQ7GKoMWh0bLVd
/brerNy36l4SxkJCa1MOFIoQXIKyFM/NmP0yl1mT4Ndv7zkFJoK/kwHRfwARAQAB
tCJEYW55YSBHZW5lcmFsb3YgPGRhbnlhQGRhbnlhMDIucnU+iQJRBBMBCAA7AhsD
BQsJCAcCBhUICQoLAgQWAgMBAh4BAheAFiEEHUJ1beqp5zcYwHPS81zVoEcgfjQF
Alv14vcCGQEACgkQ81zVoEcgfjQpIA/+LrmNOXDKqwfW8UZ8g68mfHE8BHTrDOex
J2jd/upAlEok6OqCVaCAdFJTI/h++u7fY5IxoOTSWW8KPmO2unQcJJhnOJz/46Es
WHz6/y6GGiyiHOz3trbEi4vtwFkFQAKvu+TrSv+tjbkNlIzICG8iDRol1W7Bsc+9
/KqLst29Ox+Re5aRRCECkn8cYvAv6SxdqtnNVlc9m34zekTo//AnUmMICK1QZaZG
6uQ7aCo47WBilJX27S7afpujTIag44iRX8+0NbByEMwmBNsOvhlQciKTeqrRiPnS
ahwBfAxMFTF16wTFgO4ZQTdNJmHA9YzGqWWTbWKU9mLJFx8IPvcJgV/CN+z3RUEZ
e2dxdNuqksAfBuNONdexa+1PiJNP8RX+XAKiWT/dXLDbkMKVIy6Zh31bQ6LtpDyv
LuTMF2l9e2tpLW5MK3vvJ4E0aKQad/DD6sCdrYeGxJ6+cXjoP5xEA7w1SZFLZRHA
uJV7Y++CVKqBhJC/RlbZwbOuD7h5QcbYx3uNrqkSBz9nga5f0JHk0L8gGgINK8Py
zqHVBWtAfaJQ6vvlClmik+5ZR0p2spmH6F/gm7FxApIMmkXrgQx4e8YgRoEVXzZk
tagbQ2pCOOd3n7/TuFLWQO2Qc5R8DYO7ehxrPgDZ980jZGt9MgLmiNOIYwXmB6Z7
yttoCci1v+W0LURhbnlhIEdlbmVyYWxvdiAoR21haWwpIDxkYW51Z2VuZXJAZ21h
aWwuY29tPokCTgQTAQoAOBYhBB1CdW3qqec3GMBz0vNc1aBHIH40BQJb9eLxAhsD
BQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEPNc1aBHIH40LPMQAKxEjfs3JOnC
Nn08VbU0WPAZDvM9Rk68IcQvjrLftN/vkINENI0ZNl5X2DYQoYkEDj02mdM1+5Fb
yWV6Pj4bXVUp1SumYpkH1bPpT5G1qhc2J6W8i7pf81nm9Uivu9zzYdff6MKqTdlV
uR/W67bTgz1V870YGXFEN2bhCmTmyQH9skeBOb5ol/ylN393cmG4nnzLnoj7d7sw
10tpvQjGsdwuzjkpC4A+SCmtd2KRGnG1ebAxlfSHt/XyUBwQah94zn/cvLWRaz41
FZdqAVZ6qDCZdlHfnWACfvEhCUox//kQSnqeVVMPuQrFUsCiOBMVlM4jbVXluTUM
68LaIcydYdhckvK42LbpB/qtP0gcMOatoPYF2/J43zRiJoCtBhzrsHRL5tGxW6e7
BuCO7ZJYejom+8LNfTf0dmXgYMy878E/4Xct5vMb+1tRm3e0Cgzx/63Ae4FPBofo
FjkU1c6Px72PGJJUs1B5XX/oU0rK64LfhpQ3CHK1SGcDFzEXzbraKiSpD3eTPcYj
DyYfG4g1GuFWnPW8he4K4qVZslINnOEX6+xedVf+v33S+GSaHFjLaZdlt2v+WzXv
28pqU7iBIS5Beq61PxY3CMD7SiQh93hcurjTt+a2/O8IhU3kPKN9zhRQK0BH1yHI
hs2Rq8Z4+iqY9yF8uJqEVn7D2XFsrvkFtClEYW55YSBHZW5lcmFsb3YgKGlDbG91
ZCkgPGRhbnlhMDJAbWUuY29tPokCTgQTAQoAOBYhBB1CdW3qqec3GMBz0vNc1aBH
IH40BQJb9eMhAhsDBQsJCAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEPNc1aBHIH40
T4EQAJwg9veGzGBNn5b1gxdJPiOLRzKNJHxhV++gW61hQiuw6Q3GzHQ8MSqO5EnC
E/SaHj6+XT6aitgez+uPZUgLYpAIgxB1vD3QIcW9SUKKe6Hmw9Fz8gOeEznWtdBr
mQ5/K5ufc8fNpYchOFAPrrkryI5Ek0YK4/RZtd9pflyvpY3Xgl1PZ4j0wilDeWrk
GimGGBCQRCqtT3otr8vxo2VSF5P1JuCLPX640HiH2XLSYWcaSUP/M7/sa0HOXezg
Fh8kiaB2ABWrOanN+n+EZ0dQ6MwlrMZX3StkrpgeteTbDaoGWhqrSshkQUwNFUPz
BCNkN7UAdIN+xCPdUBB9g+veRxjoJj7xUWFnua+ICGq2WxYGgXqzsOVPXweOf8RH
1P6DWGK2h8GDJDTvUR54fnhWg8coIR32ghifxASx/tTmTIAhZy7cXCDKU0unhDz7
gs95h9HwbgJZl57n1fXb7GlYF7R4kusr6nWV9AfKEYZEZK+75LIys5GDdNi5eovi
xZDAne6tfUh3yyJ9pHQXivRCiQ/LC3dTO9PuRAcTvS8C5Y2/JKVu67j7jy4u1hRw
gjk7wiY4PkxkK+7UZIezqzE2d4cLOz+Nqiy+FeR5iFzE5A1YOAA9uo2R/NSJ87cC
5k3J7agNfY5IBfd5+FIpiKBfrHoy5LuoXfpA01zVeMK4y47juQINBFeHhzMBEACz
I9L1D3doNt2TmhBLhL2kGMPmpCu8909xBF2ZQ+Ay7iu9ZIo8lsA3QM0xV0V5+Ios
lh7xS1WXJFgerwNZd6O9xLjFz7ZgMgEyob2LDjNfxBsuJgKm87yiqBrTzv+2hdPS
Y2kKDBTo4TasEBuW/vU/Nr6Sa9XDaLhVAQaSKRze5gRwee3JUX95Iejn2wjJMdWw
DkRZ/TrFgm+eYCBsZmaFgJKKNk6HWmRKnoFmAc/q75NIP25mcJWW3BbXr+hs6fdm
oaShARFtEWHptBuMtJflw7lTuQrhqG8nlMjA8M+JYIJ3+v6D0Q4RLaRpeXH47EU+
H+7M2YeRXLBi0D3l/mLE2/pSH+PLTSNtiw8ipKAYQcSgaiEaMyEs1xjM/dpNjJH8
q/h+7XBllpjDLjs9OXMR8uOKn6w9j5yhdlDT8sx+i/TWbBn8EZ7M5vupgWlZliHI
GDpgv+fLbFUEJlCAEMSGD2/zHqWRamNLV+eERr/oEU+UHeoPcGzalnwQNkkFg3fj
8FFN28LdlBte3EJSToBfO+nAsGesZRmgVeHBZamaQgX5nxb2b1zdLAhmKnVLPr42
uZMoz7h7It9hVv1z2tEUbTPke68/+c4ktsUs2ps7Tqey9rbYZhnc7pCLXRs/6skl
fQk3qG6kPQO6ayyQ3C3O+RVA5BNuOkdeerNZQliWXQARAQABiQIfBBgBAgAJBQJX
h4czAhsMAAoJEPNc1aBHIH40WA8QAJrJ2vWNbOw0htxd/AIn+3YvIxM+3dBd+SmH
fFsM/OSeTa04b/t6NokZ+ZSHIaxIHNDflS6UsCy8zopbedpsCVcQRs+/TQXkzskF
I+mrfefcgBk8uoXVyRspigCM1AzxEH/OFObWl+kI85Gka+M4pN/FYc11+F+ldNLw
SkHti7TINrCBmkvjga7DW/Zn8z5QejK3dOOHkEU4/eVAEHqhlBnMMBf6Db7bBjfM
Ob4VYTRPiKxdqyCzOZfYOkEvPToh9omTiaSnTbgqjO1mX1T3upz9xGVFzN78BIPe
b8UkaKreoJLH2M1OVYZDj3lLtEWhGkJrvPFmSjMZifPR1ki/M5Dd++Wy95atrc5U
yZSYpLAWZXpJ5+tDF1R8Xd6dS3afW2szY5AaHxYYRj1LdOrm7Fj+7sm0ztGkn+SS
BCM89zoP2KSd6EZdN2P/4SnvLgMp7XvHkZCc/xSy2970Nt21lcNRBUg6gEagcn/J
nAIfb0uNx9wJqfYSdqd/GXjTX4tpur8Wg0JCRABSN6AF54e3jE19+Kw2Ne+Di2FK
6Ris9BUPACWXPdrZvU7trhFJ3SVN7MzwHX1j7GazkKC2EwpKw3+WOtaRGjqiAKsc
Yyo5ZP89t9DnAt1gbnu4/Ejn215fBDLhW1/9FUbDHlhP/NhOoQgwGZEuSSykkEm4
Cy9HFCjP
=KeUj
-----END PGP PUBLIC KEY BLOCK-----

Недостатки

- RSA + сертификаты → большие ключи
- Нет совершенной прямой секретности: если ключи утекут, то старые сообщения можно расшифровать

Недостатки

- RSA + сертификаты → большие ключи
- Нет совершенной прямой секретности: если ключи утекут, то старые сообщения можно расшифровать
- Протокол сложный для реализации и использования

Спасибо за внимание

0xF35CD5A0 47207E34