

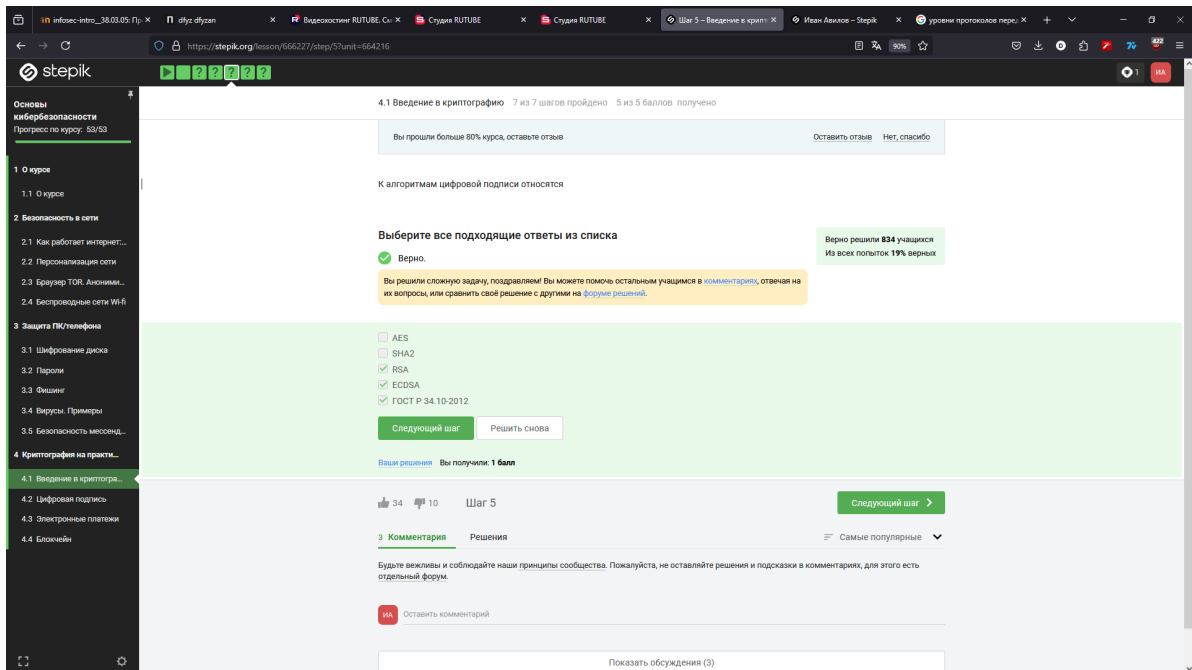
Задание

The screenshot shows a Stepik course page for "Основы кибербезопасности". The current lesson is "4.1 Введение в криптографию". The question asks: "В асимметричных криптографических примитивах Выберите один вариант из списка". The options are: "обе стороны имеют общий секретный ключ", "одна сторона имеет только секретный ключ, а другая - пару из открытого и секретного ключей", "одна сторона публикует свой секретный ключ, другая - держит его в секрете", and "обе стороны имеют пару ключей". The correct answer is "Правильно, молодец!". The page also shows a sidebar with the course structure and a bottom section for comments and a "Следующий шаг" button.

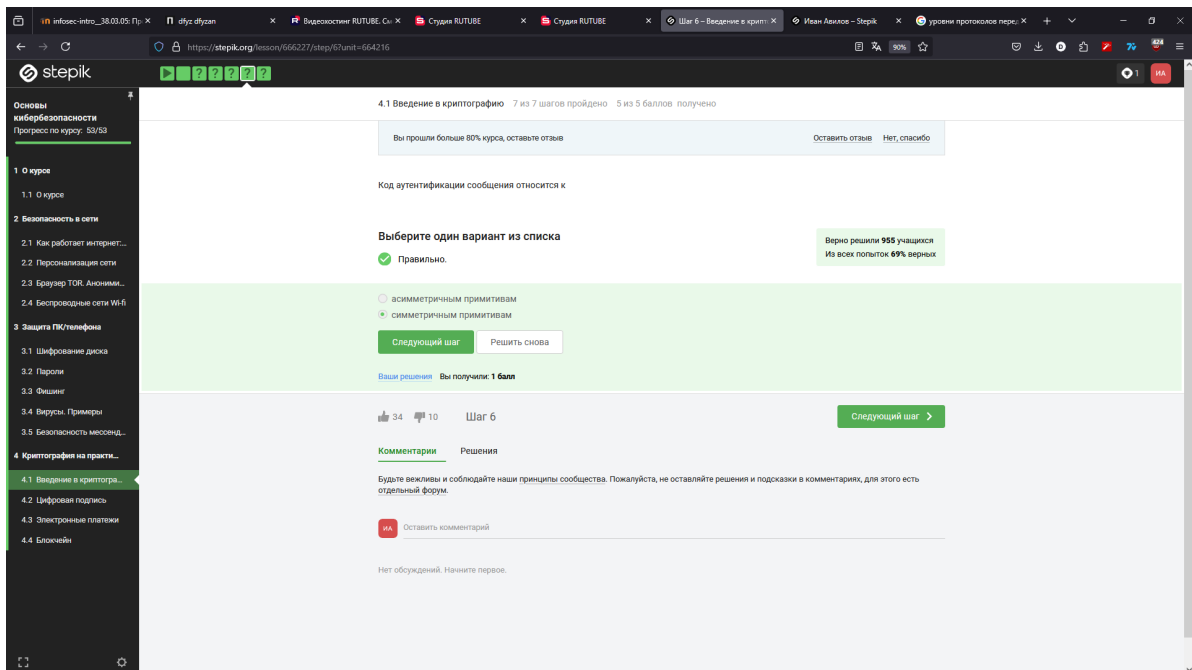
Правильный ответ - последний

The screenshot shows a Stepik course page for "Основы кибербезопасности". The current lesson is "4.1 Введение в криптографию". The question asks: "Криптографическая хэш-функция Выберите все подходящие ответы из списка". The options are: "обеспечивает конфиденциальность зашифрованных данных", "эффективно вычисляется", "дает на выходе фиксированное число бит независимо от объема входных данных", and "стойкая к коллизиям". The correct answer is "Правильно.". The page also shows a sidebar with the course structure and a bottom section for comments and a "Следующий шаг" button.

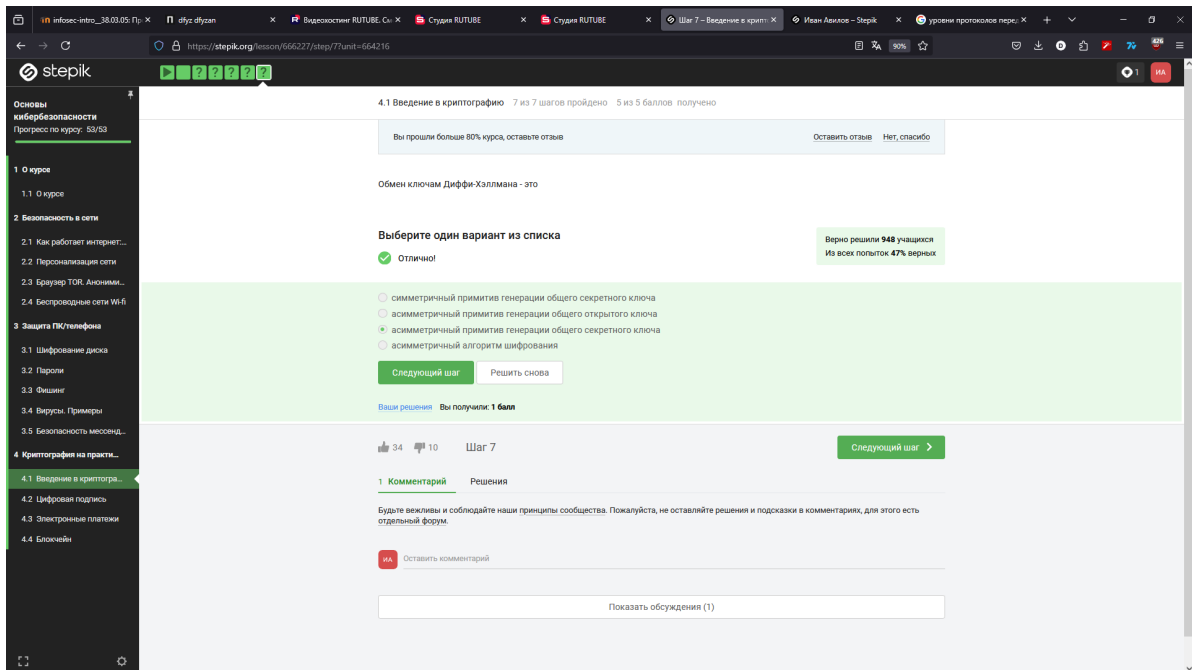
Хэш-функция должна быть быстрой, иметь одинаковую длину выхода и быть максимально стойкой к коллизиям



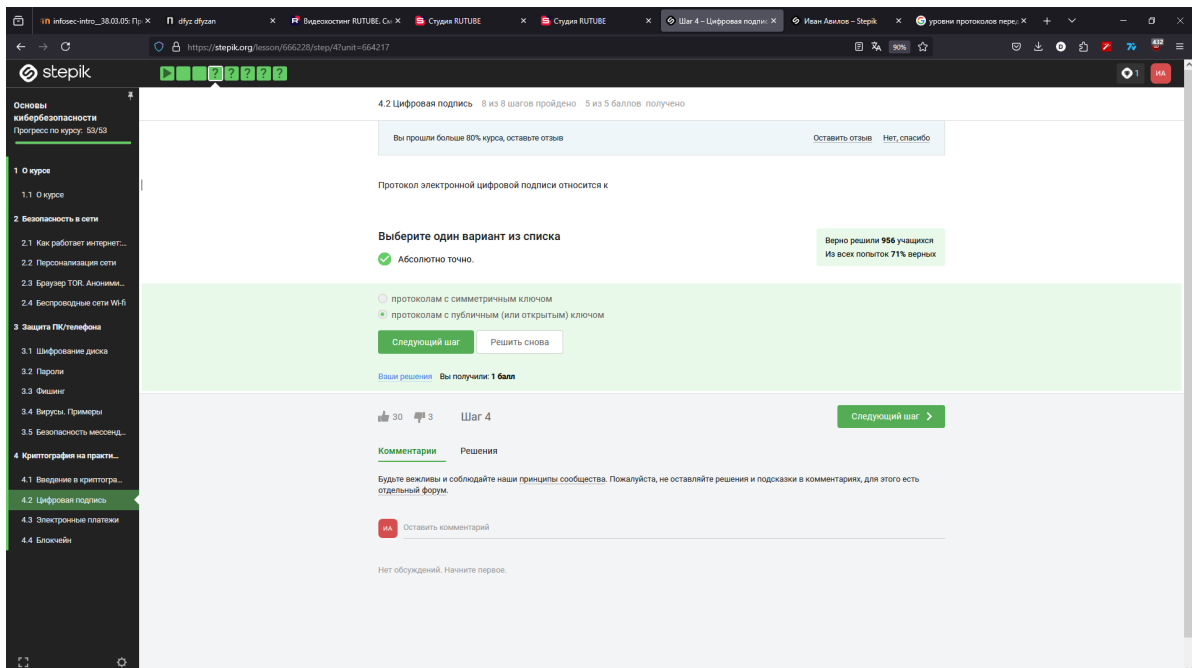
AES и SHA2 - хэш-функции, а не алгоритмы цифровой подписи



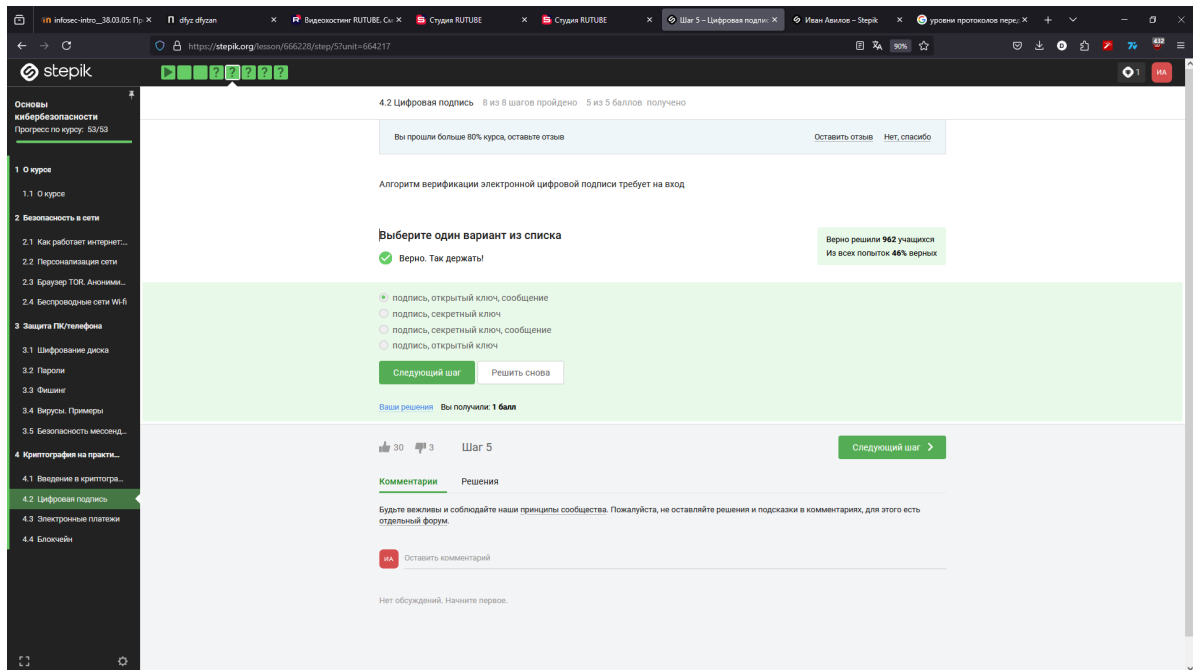
Код аутентификации сообщения является симметричным примитивом



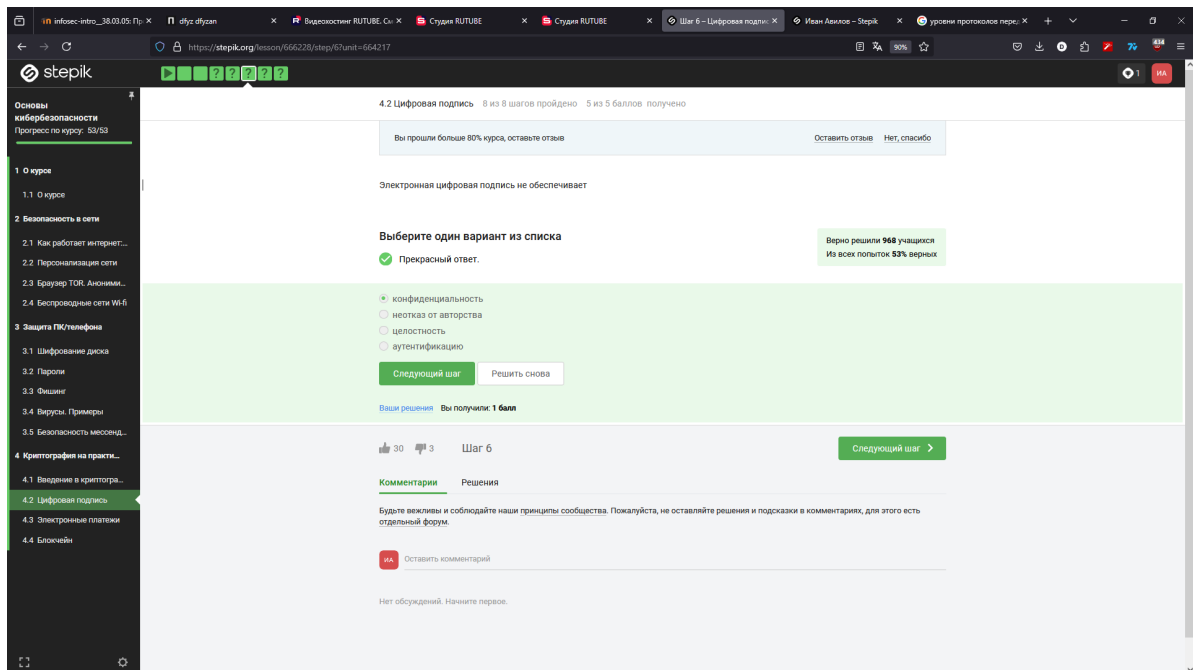
Правильный ответ - асимметричный примитив генерации общего секретного ключа



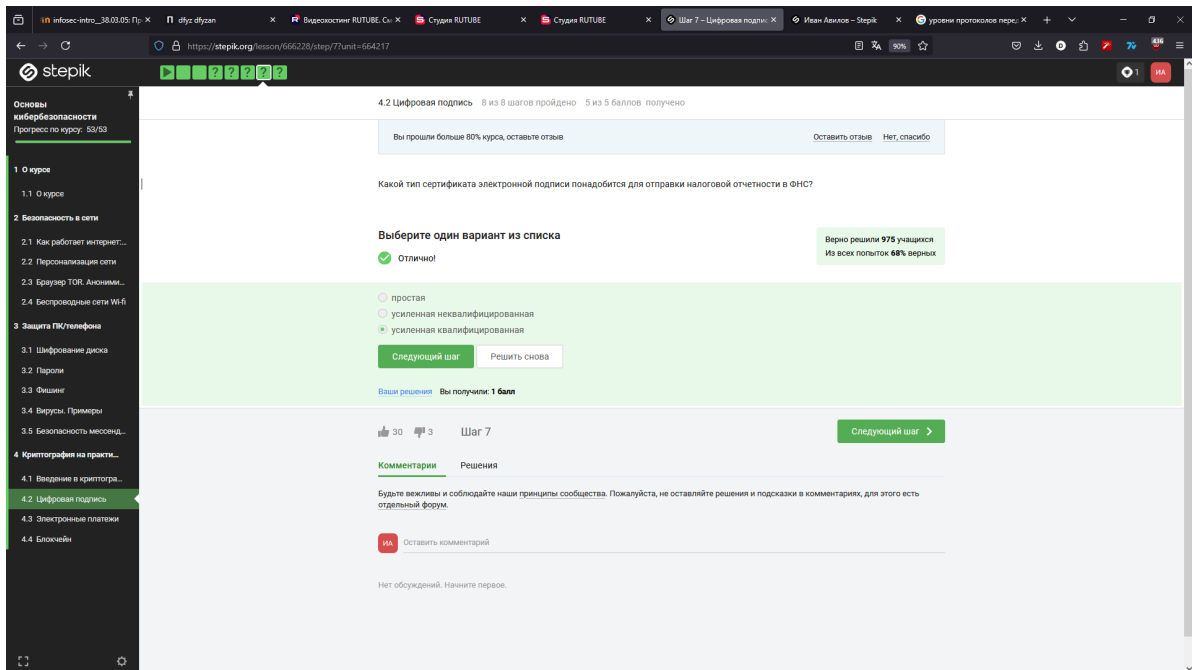
Для проверки подписи используется открытый ключ



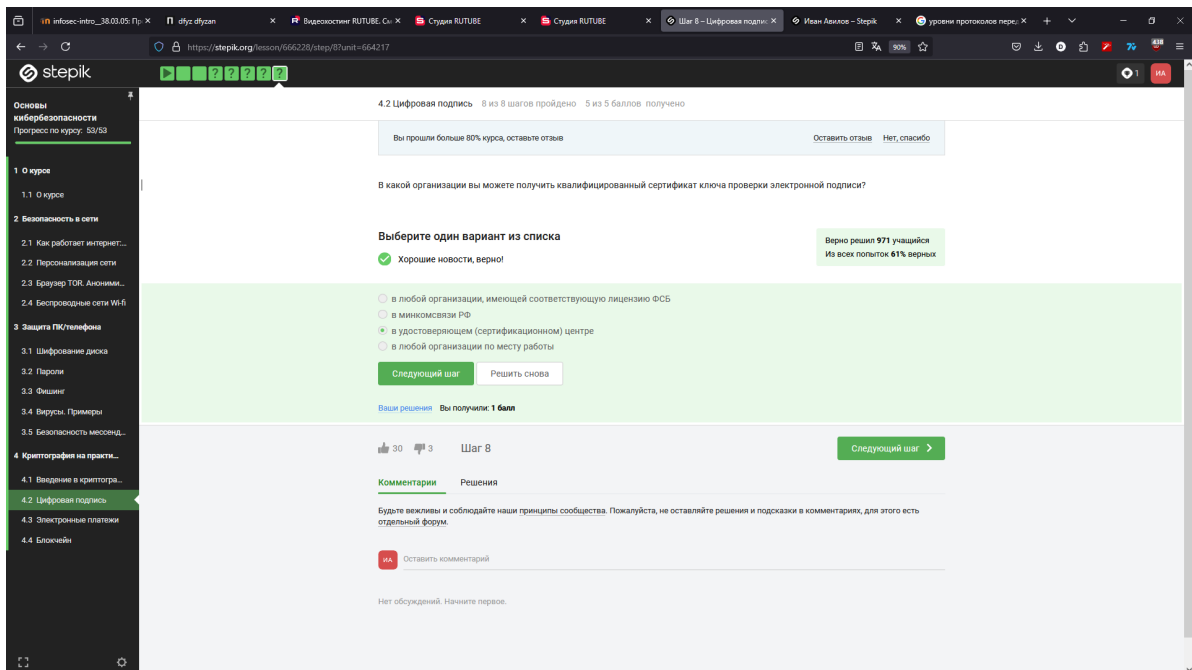
Необходимы подпись, открытый ключ и само сообщение



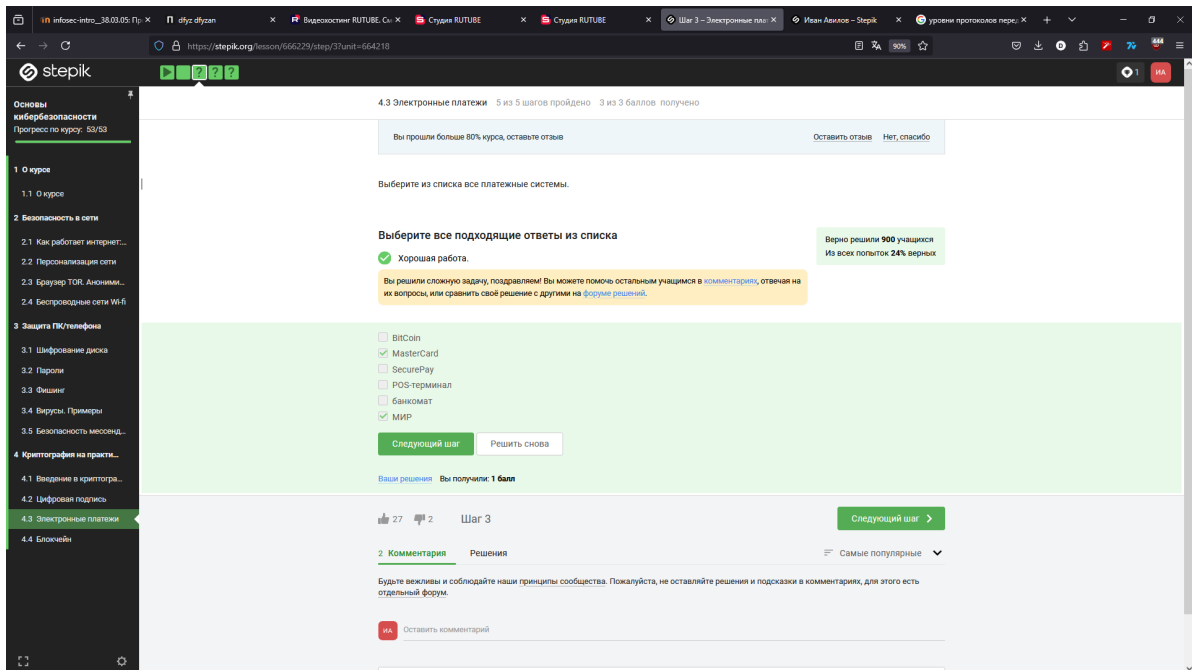
Конфиденциальность не обеспечивается цифровой подписью



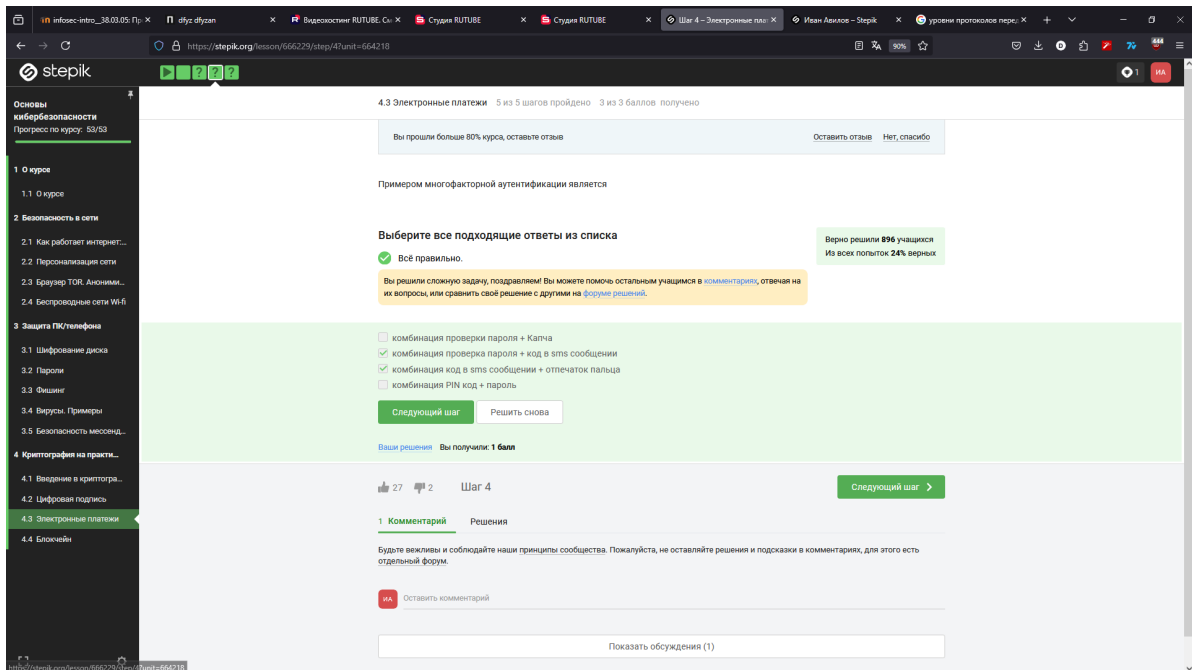
Для подачи налоговой отчётности необходима усиленная квалифицированная подпись



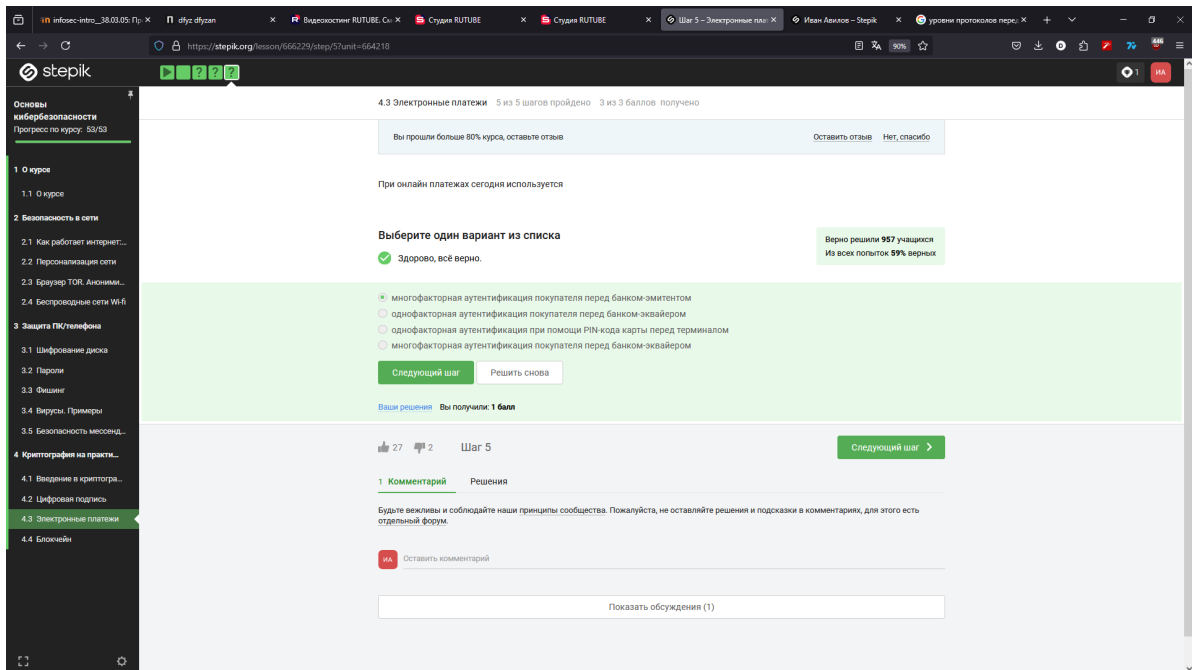
Такую подпись можно получить в специальном удостоверяющем центре



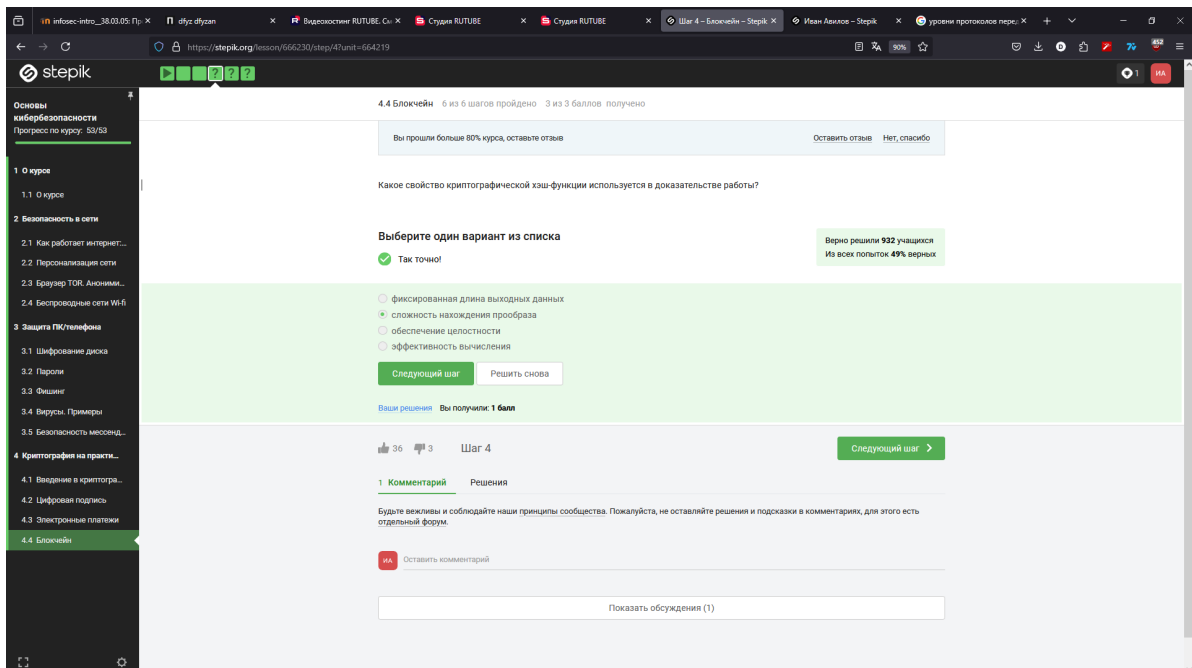
Платёжная система - система, обеспечивающая передачу данных между разными участниками платежа



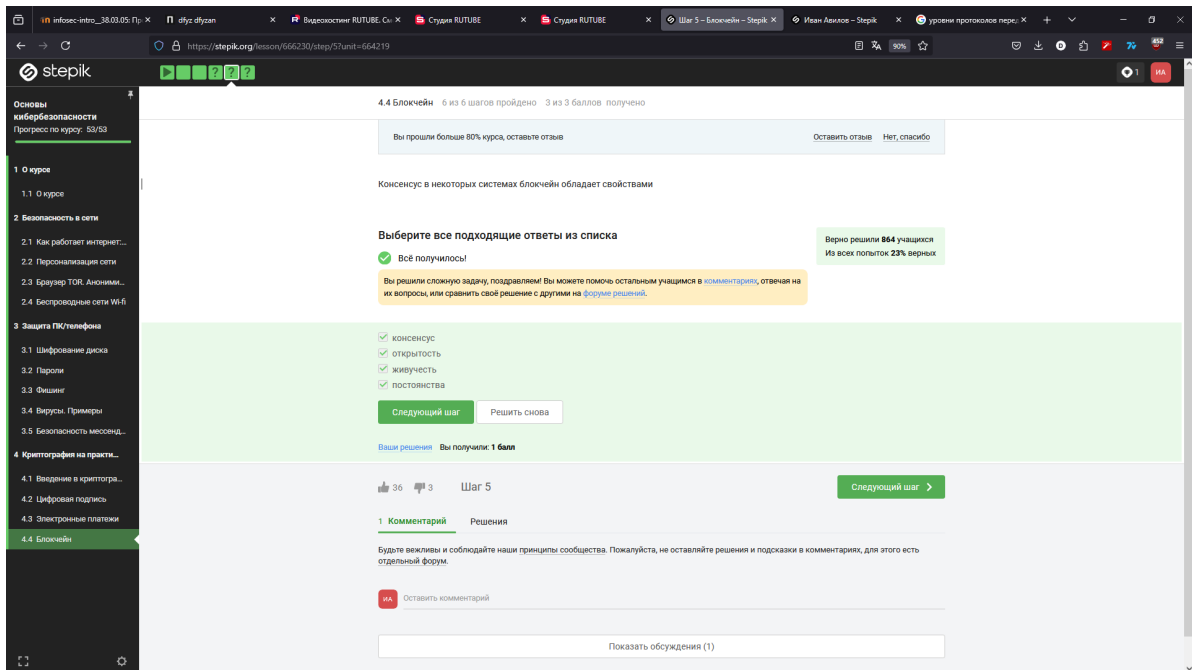
Многофакторная аутентификация - аутентификация, использующая несколько РАЗЛИЧНЫХ факторов



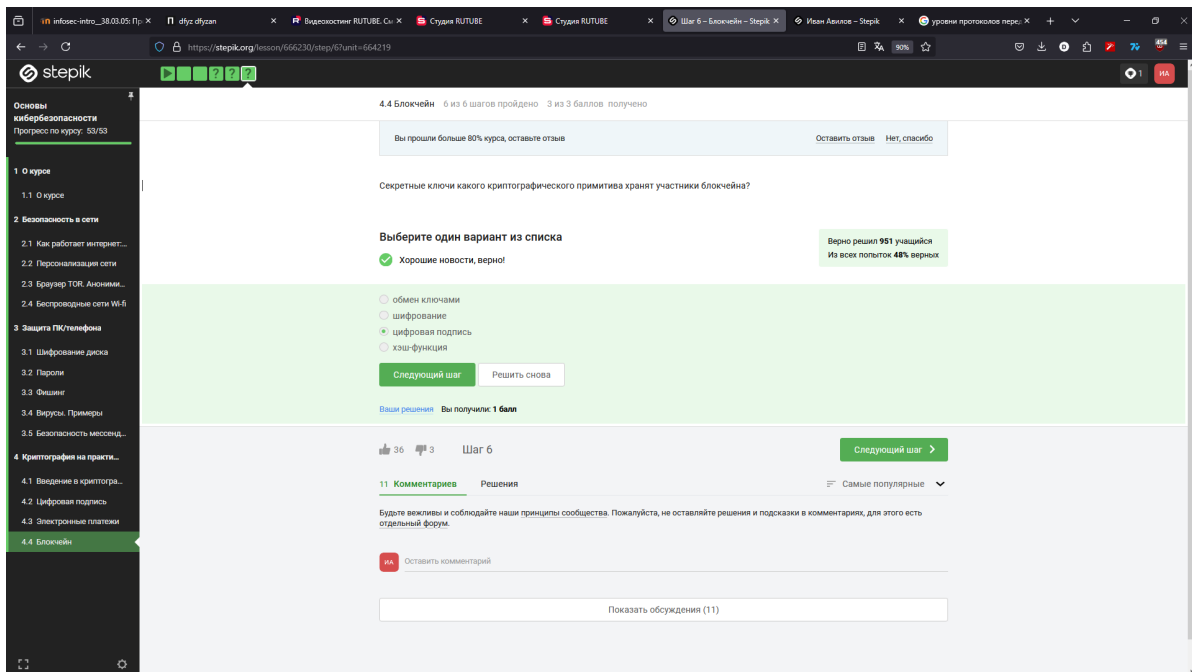
При онлайн платеже вы подтверждаете личность банку, выпустившему вашу карту (эмитенту)



Proof-of-work требует высокую сложность нахождения прообраза



Он обладает всеми свойствами



Цифровая подпись необходима для проверки