Внешний курс. Блок 3: Криптография на практике

Дисциплина: Основы информационной безопасности

Ибатулина Дарья Эдуардовна, НКАбд-01-22

Содержание

# 1 Цель работы

Пройти третий блок курса “Основы кибербезопасности”, выполнить тестовые задания к нему.

# 2 Выполнение блока 3: Криптография на практике

## 2.1 Введение в криптографию

В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ (рис. [[1](#fig:001)]).

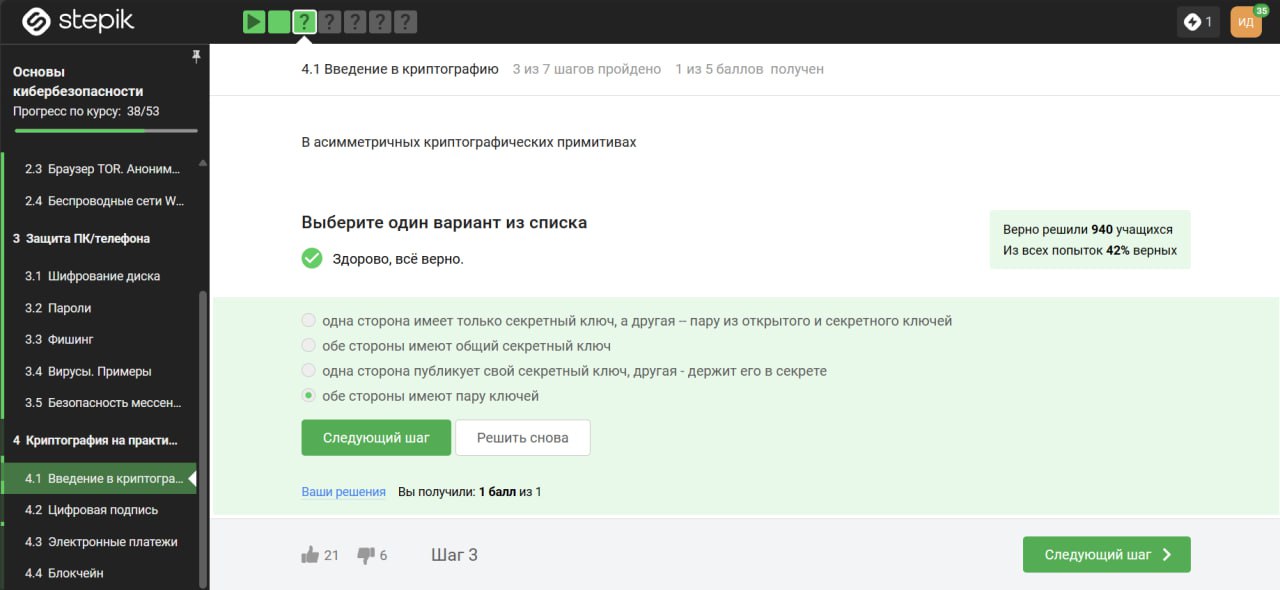


Figure 1: Вопрос 4.1.1

Важное свойство криптографической хэш-функций, то, что делает её криптографической – это стойкость к коллизиям. Криптографическая хэш-функция берет на вход произвольный объем данных, то есть какие-то биты и выдает на выходе фиксированную строку, например длины n. Важно, что, как правило, функция сжимает данные: она берет большой набор данных и выдаёт потом маленькое фиксированное значение. Кроме того, криптографическая хэш-функция эффективно вычисляется (рис. [[2](#fig:002)]).

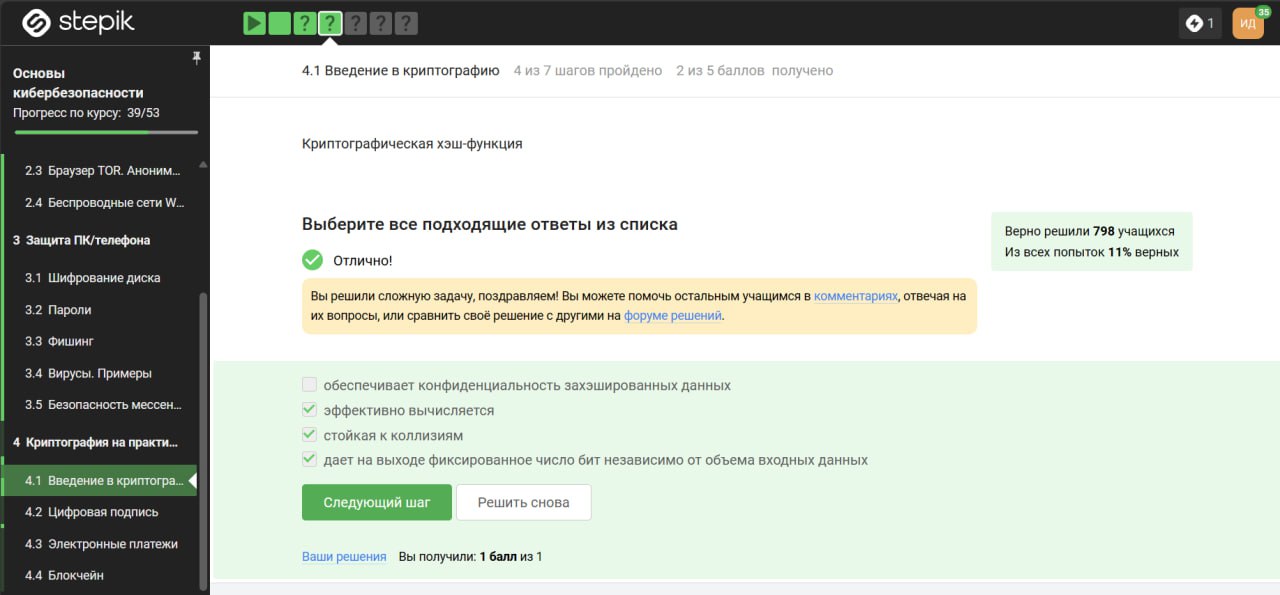


Figure 2: Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. [[3](#fig:003)]).

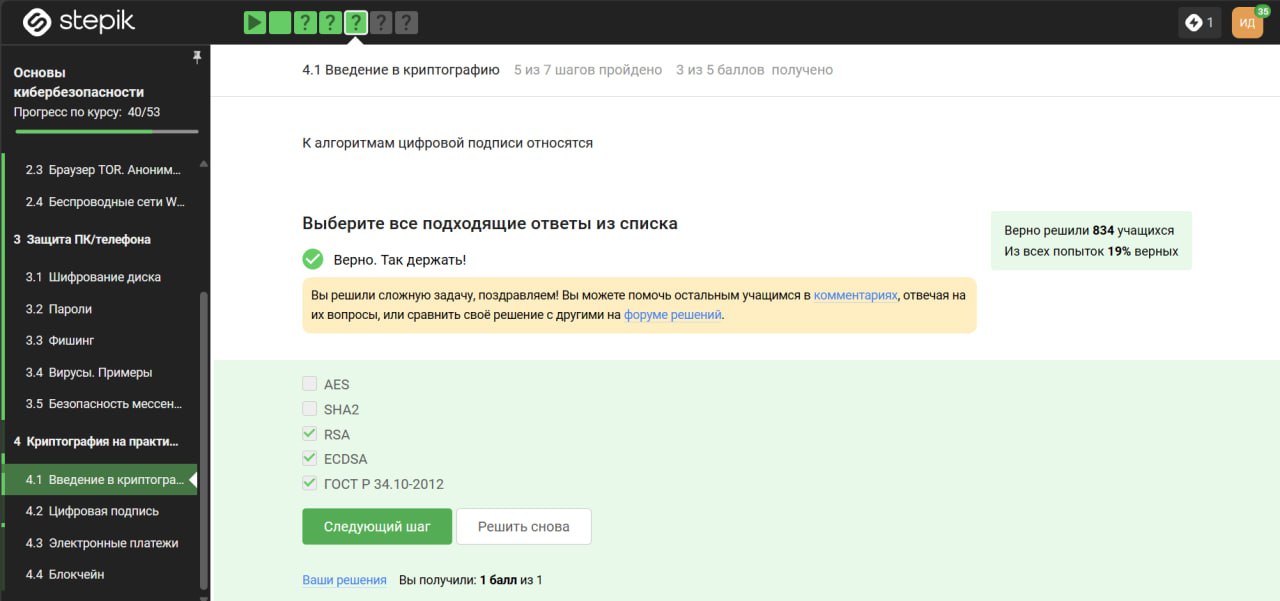


Figure 3: Вопрос 4.1.3

К шифротексту, который мы сгенерировали с помощью ключа для какого-то сообщения, мы еще добавляем код аутентификации сообщения. Это также симметричный примитив, который берет на вход какой-то ключ (это должен быть другой ключ, не тот, с которого мы шифровали) и сообщение и выдает код аутентификации сообщения (рис. [[4](#fig:004)])

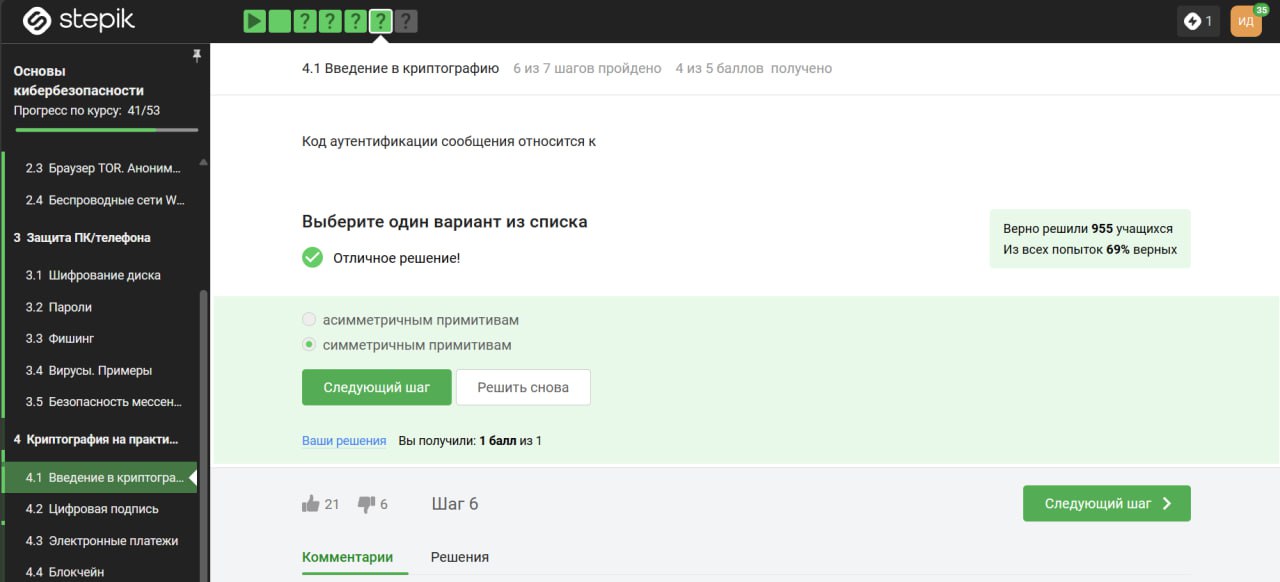


Figure 4: Вопрос 4.1.4

Использую определение обмена ключами Диффи-Хэллмана для ответа на данный вопрос (рис. [[5](#fig:005)]).

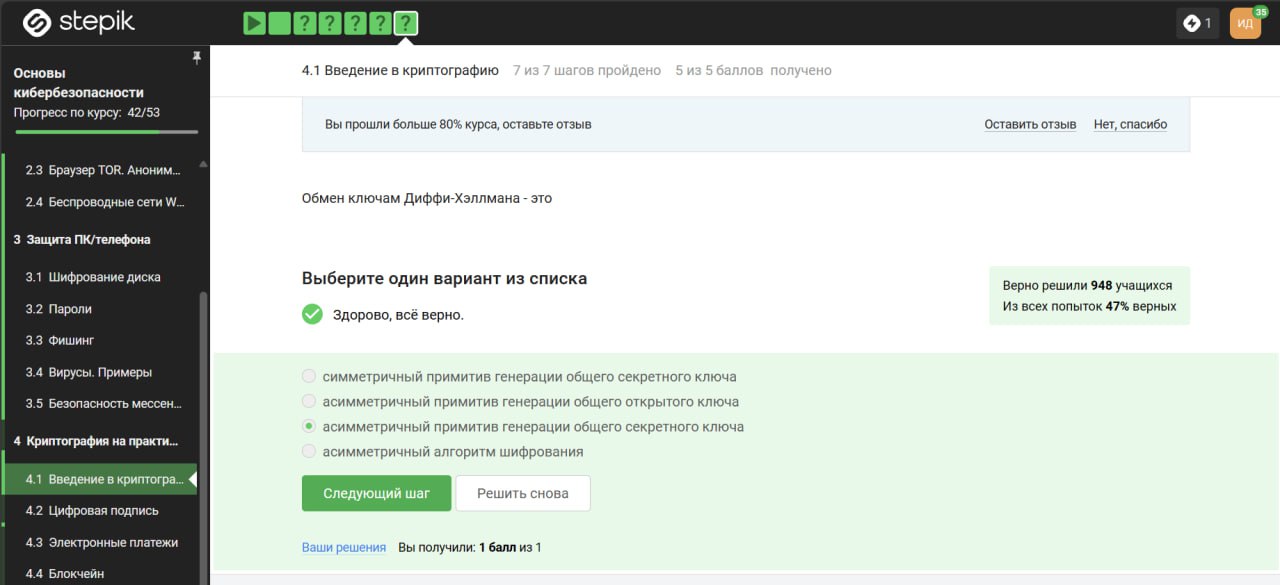


Figure 5: Вопрос 4.1.5

## 2.2 Цифровая подпись

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. [[6](#fig:006)]).

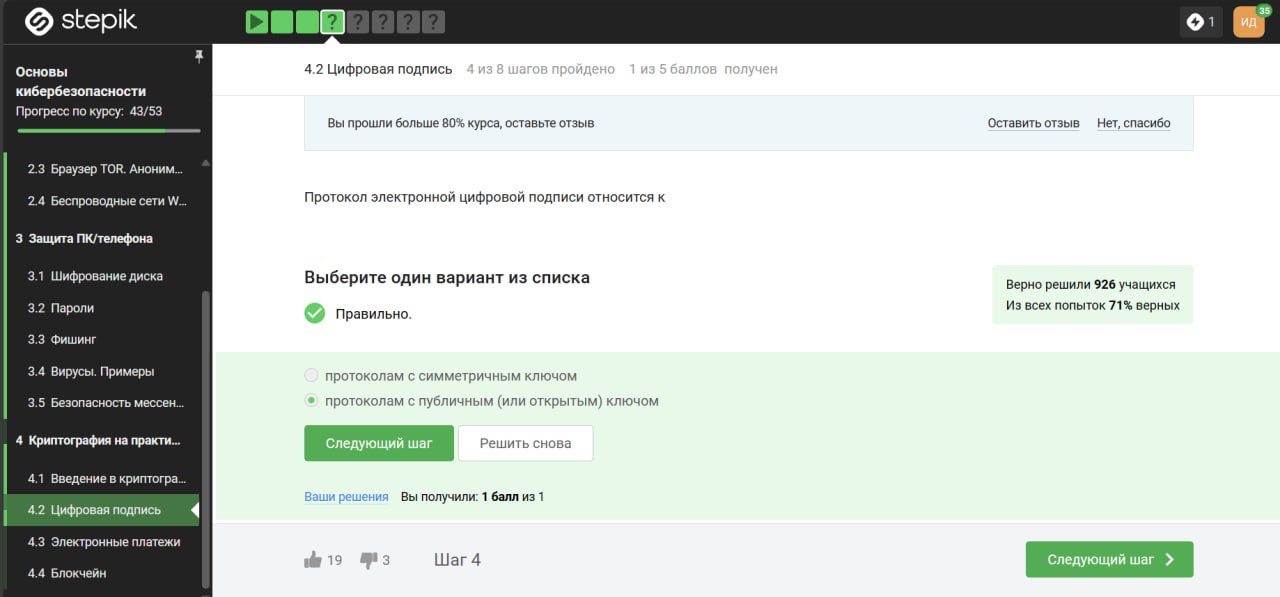


Figure 6: Вопрос 4.2.1

Rаждая машина запускает процедуру Verify, которая берет на вход само обновление, подпись и открытый ключ разработчика (рис. [[7](#fig:007)]).

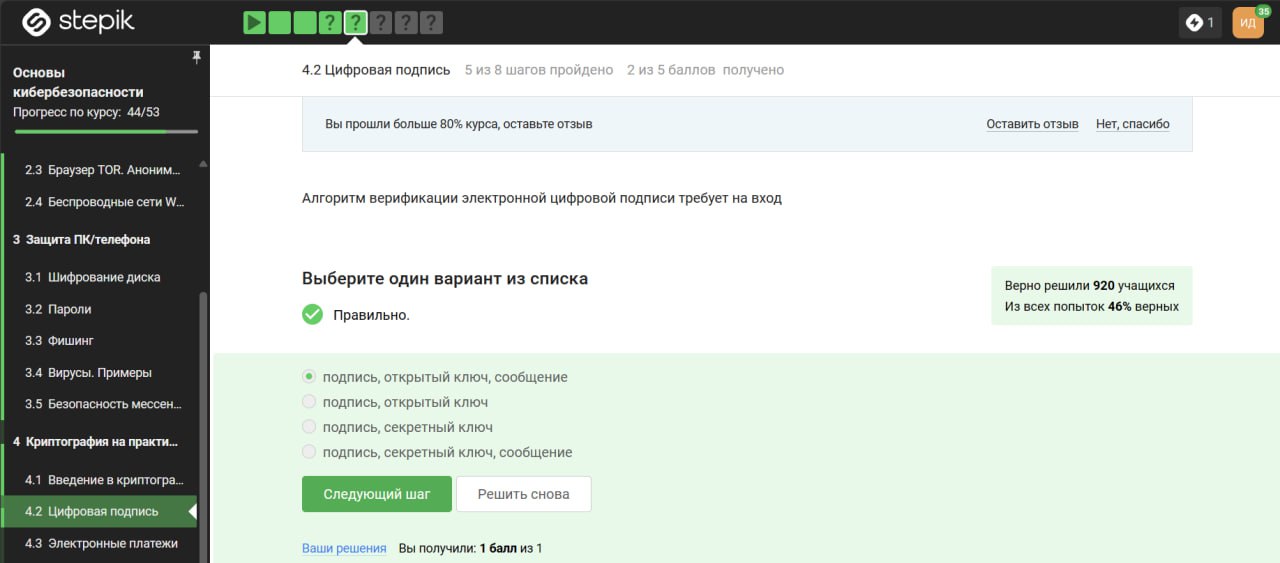


Figure 7: Вопрос 4.2.2

цифровая подпись предназначена, во-первых, для обеспечения целостности сообщения, иными словами, если сообщение в процессе передачи было изменено, то подпись этого измененного сообщения будет проверена некорректно, то есть при проверке корректности подписи мы узнаем о том, что сообщение было изменено. Во-вторых, цифровая подпись обеспечивает аутентификацию сообщения, то есть мы можем установить принадлежность подписи владельцу, иными словами, никто другой не смог бы поставить такую подпись под этим сообщением. Ну и последнее, третье – это неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта, что он ее подписал. Конечно, в случае кражи секретного ключа, с помощью которого подписывается сообщение, формируется подпись, о корректной безопасности цифровой подписи никакой речи быть не может, поскольку секретный ключ украден. Поэтому, электронная подпись не обеспечивает конфиденциальности (рис. [[8](#fig:008)]).

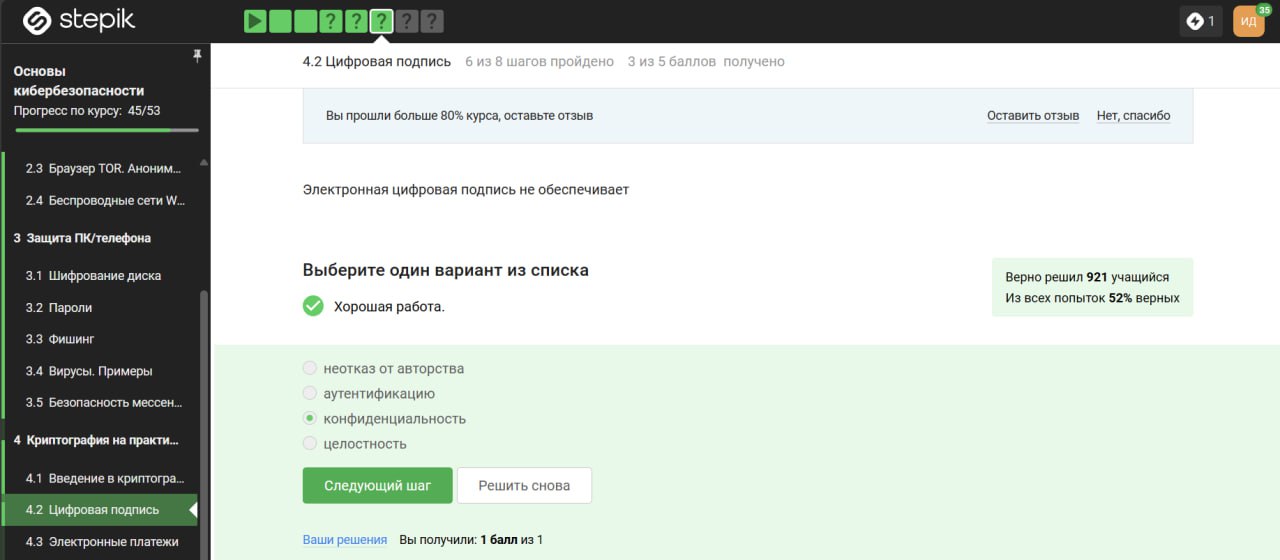


Figure 8: Вопрос 4.2.3

Что касается усиленной квалифицированной подписи, эта подпись уже имеет юридическую силу, она, как правило, равнозначна рукописной. Для того, чтобы получить такую подпись, вам нужно пойти со своим паспортом и с другими данными в сертификационный центр, который должен быть аккредитован конкретным министерством. Такие подписи используются на Госуслугах, в государственном документообороте. Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. [[9](#fig:009)]).

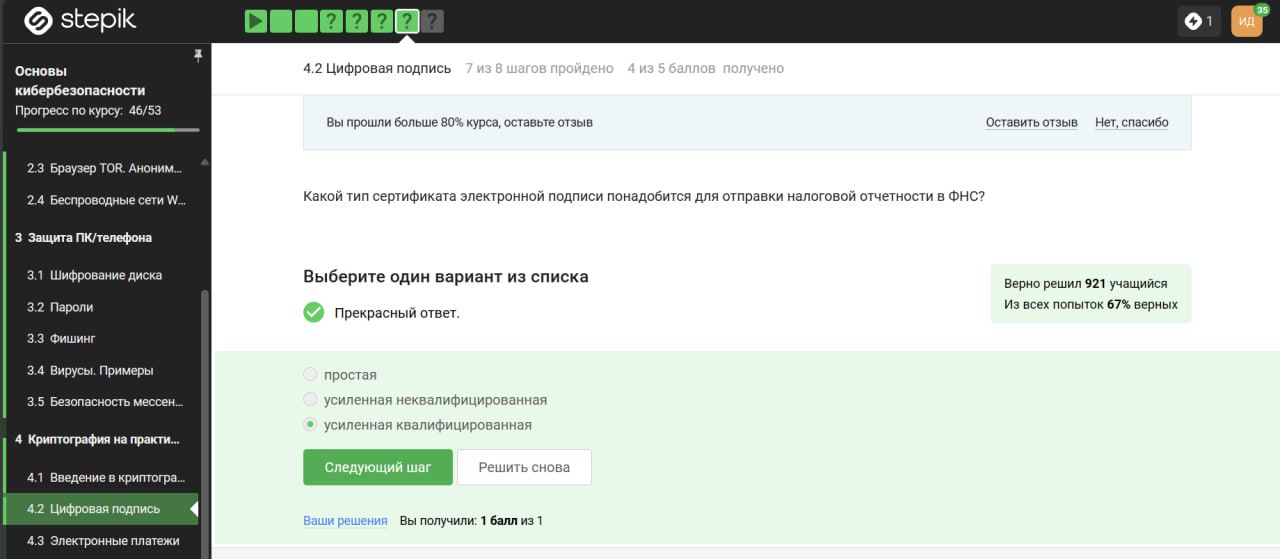


Figure 9: Вопрос 4.2.4

Сертификат подписывается с помощью электронной подписи уже доверенной стороной, удостоверяющим центром, тем центром, который имеет лицензию министерства (рис. [[10](#fig:010)]).

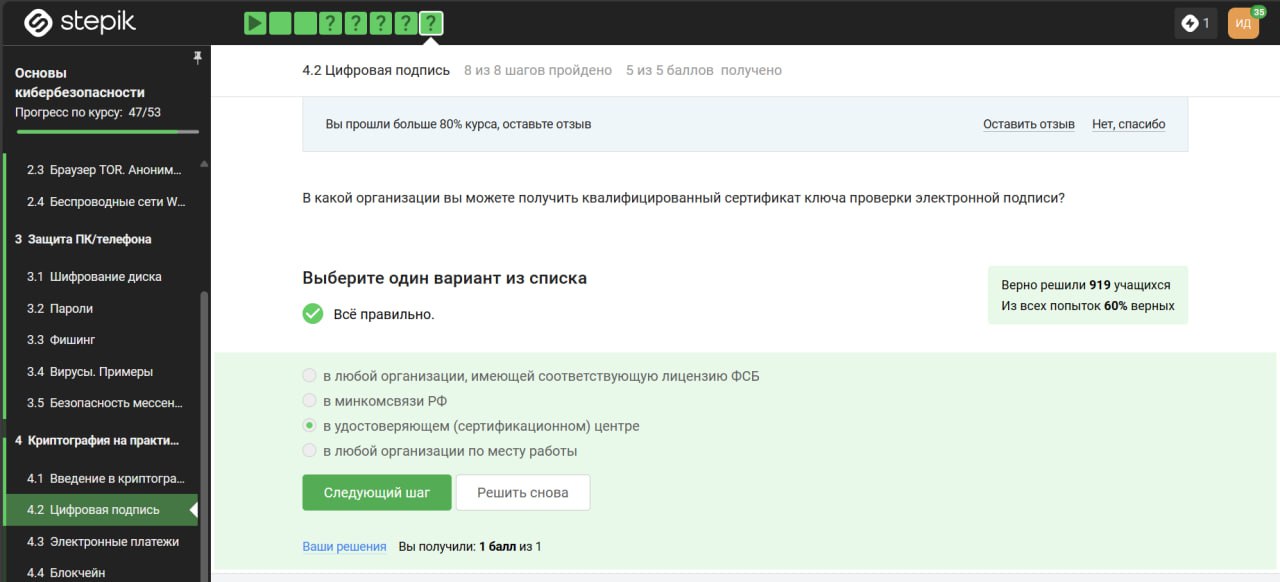


Figure 10: Вопрос 4.2.5

## 2.3 Электронные платежи

На данный момент существуют такие платежные системы, как: Visa, MasterCard, МИР (рис. [[11](#fig:011)]).

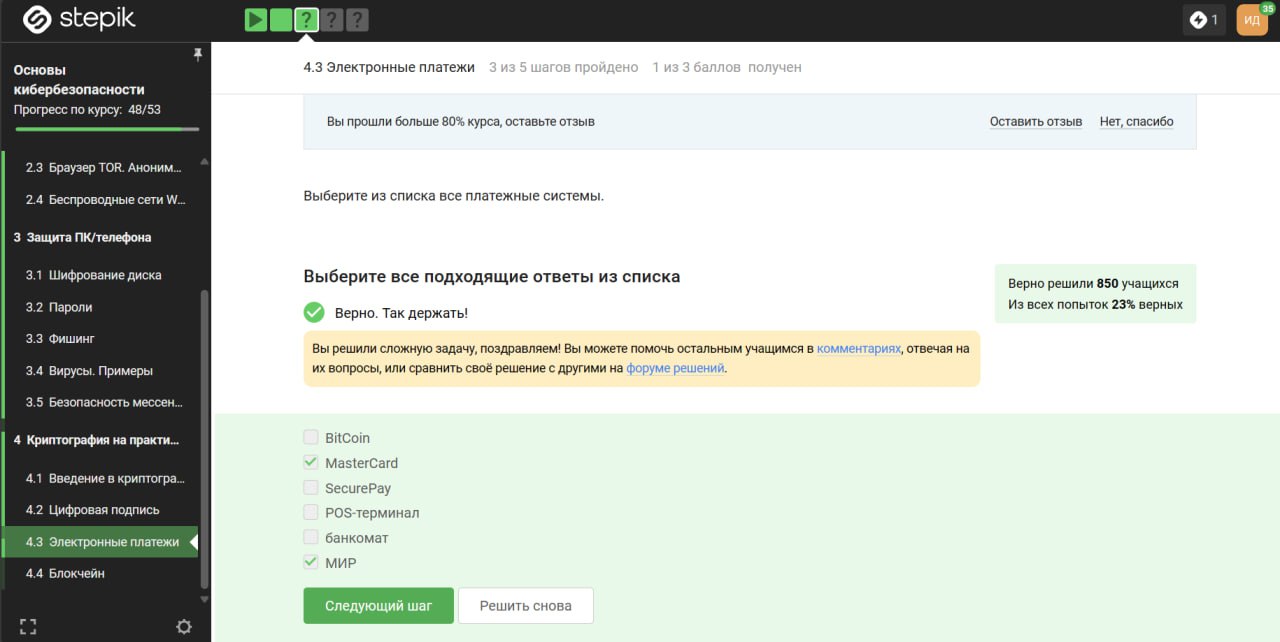


Figure 11: Вопрос 4.3.1

Основные категории вещей, которые мы можем доказать: 1) то, что я знаю – это либо пароль, либо PIN-код, либо в случае онлайн-платежей это секретный код, 2) конкретно в онлайн-платежах мы еще используем второй фактор – это то, чем я владею, например, телефон, именно поэтому нам часто приходит код, который вы должны подтвердить или вбить в ваш браузер, 3) другой фактор аутентификации – это свойства, например, биометрия, опечаток пальца, сетчатки глаза, 4) четвертый фактор аутентификации – локация (рис. [[12](#fig:012)]).

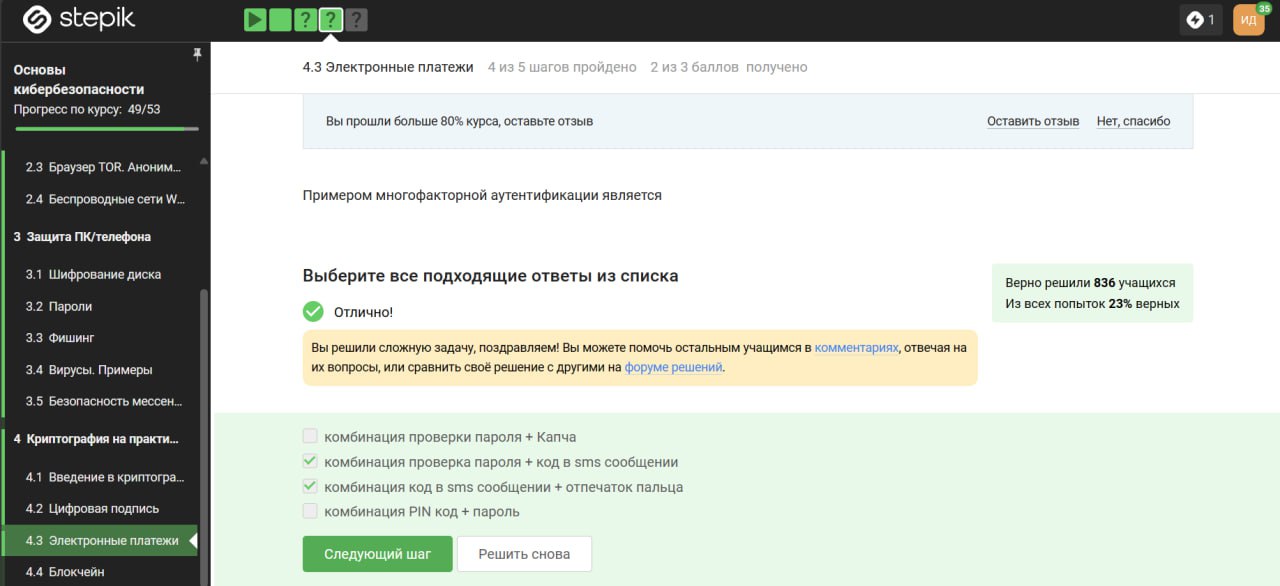


Figure 12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация банком-эмитентом (выпустившим карту), чтобы удостовериться, что транзакцию совершает именно владелец карты или счета, а не злоумышленник (рис. [[13](#fig:013)]).

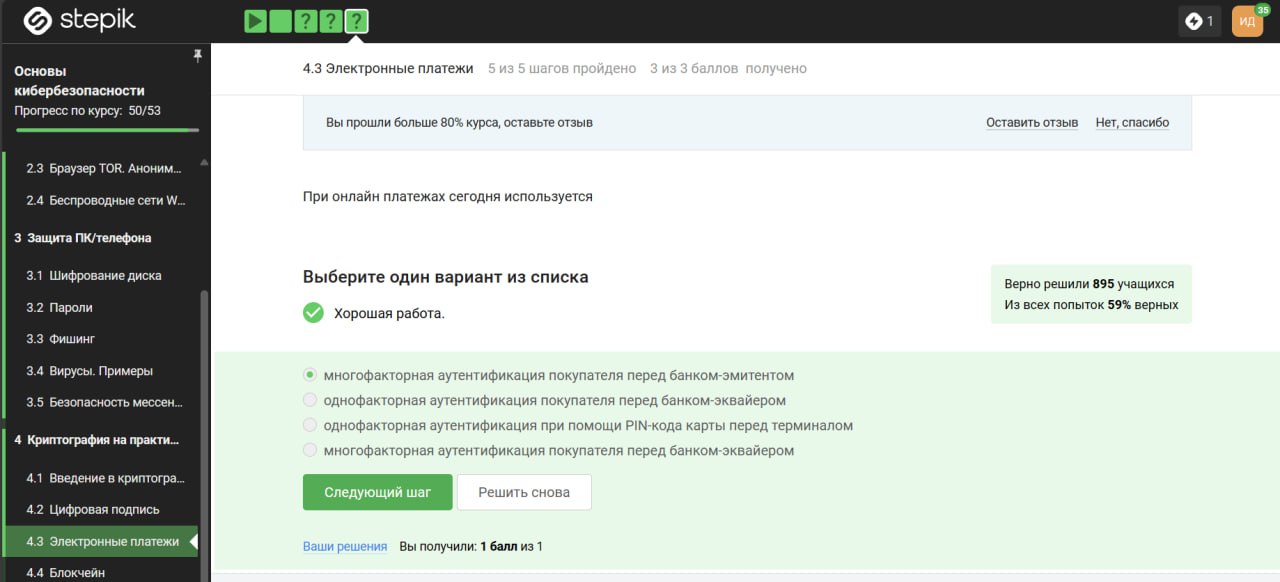


Figure 13: Вопрос 4.3.3

## 2.4 Блокчейн

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне; он используется для подтверждения транзакций и создания новых блоков. С помощью PoW майнеры конкурируют друг с другом за завершение транзакций в сети и за вознаграждение. Пользователи сети отправляют друг другу цифровые токены, после чего все транзакции собираются в блоки и записываются в распределенный реестр, то есть в блокчейн. Следовательно, в доказательстве работы криптографической хэш-функции используется такое ее свойство, как сложность нахождения прообраза (рис. [[14](#fig:014)]).

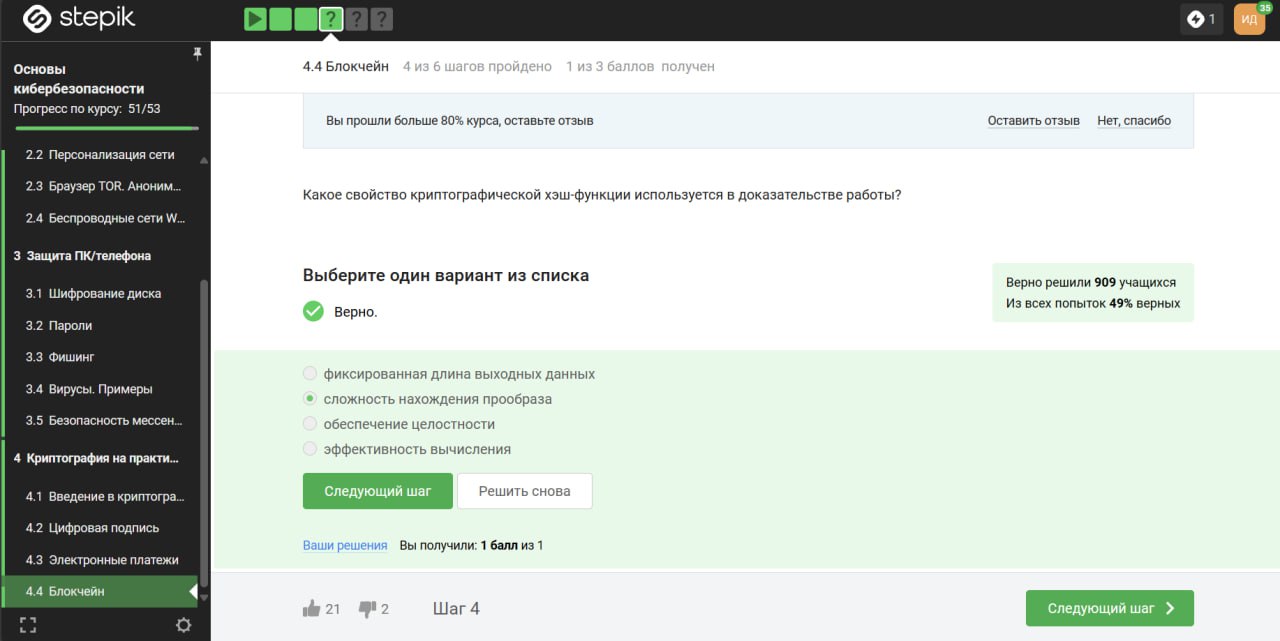


Figure 14: Вопрос 4.4.1

В основе любого блокчейна, в частности биткоина, лежит консенсус – соглашение, в терминах криптовалют консенсус - это некая публичная структура данных или ledger (переводится с английского как «бухгалтерская книга»), где просто содержится история всех переводов, хранится список того, кто что кому заплатил, в какое время. Почему консенсус? Потому что эта публичная структура, и бухгалтерский учет должен обеспечивать четыре основных свойства. Первое - это постоянство, то есть когда-либо добавленНые данные не должны быть удалены из этой структуры. Второе - это сам консенсус, то есть все участники видят одни и те же данные и соглашаются с одним и теми же данными, исключением могут быть последние пары блоков, то есть последние изменения в этом блокчейне, в этой публичной структуре данных. Третье - это живучесть, это означает, что мы можем добавлять новые транзакции, когда хотим, мы можем осуществлять платежи, когда хотим. И последнее четвертое свойство - это открытость, то есть любой человек может быть участником блокчейна. Это справедливо не для всех блокчейнов, для биткоина это справедливо. Значит, выбираем все 4 свойства (рис. [[15](#fig:015)]).

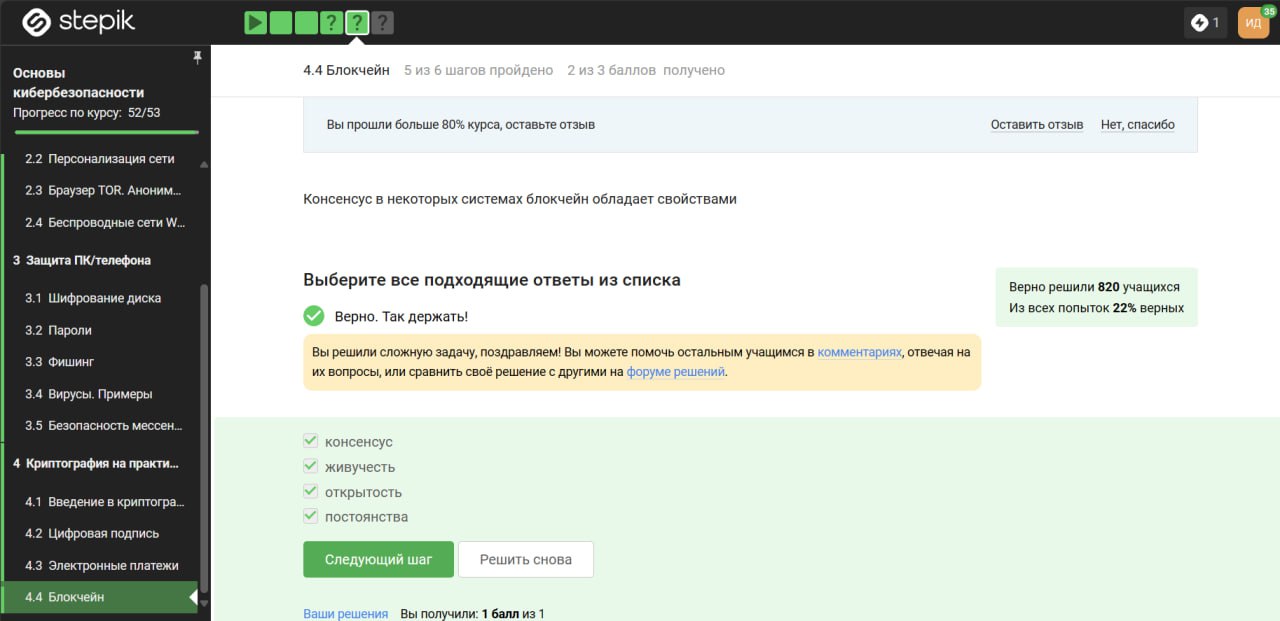


Figure 15: Вопрос 4.4.2

Допустим, у нас вами есть в блокчейне 3 участника, которые обмениваются друг с другом транзакциями. Важно то, что у каждого участника есть свой секретный ключ, и своим секретным ключом мы всегда будем подтверждать какую-то транзакцию. Важно то, что этот ключ у нас секретный, мы его используем для подписи. Подпись – это и есть подтверждение моей транзакции. Мы с вами разбирали в одной из лекций, как работает электронная цифровая подпись, у этого примитива есть секретный и открытый ключи, и наш секретный ключ - это то, что позволяет нам совершать транзакции от нашего лица. Тогда ответ - цифровая подпись (рис. [[16](#fig:016)]).

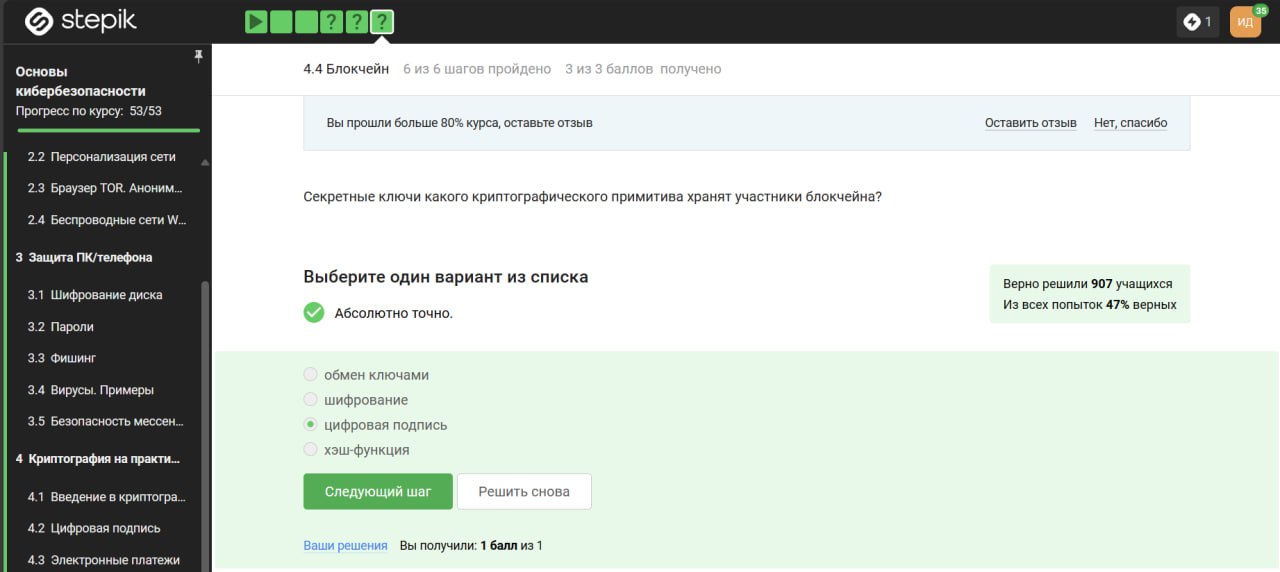


Figure 16: Вопрос 4.4.3

# 3 Выводы

Я прошла третий блок курса, узнала много нового о криптографии, цифровых подписях и технологии блокчейн, а также освежила в памяти знания о том, как работают переводы криптовалюты с точки зрения безопасности транзакций.