Внешний курс. Блок 3: Криптография на практике

Основы информационной безопасности

Петрова Алевтина Александровна

Содержание

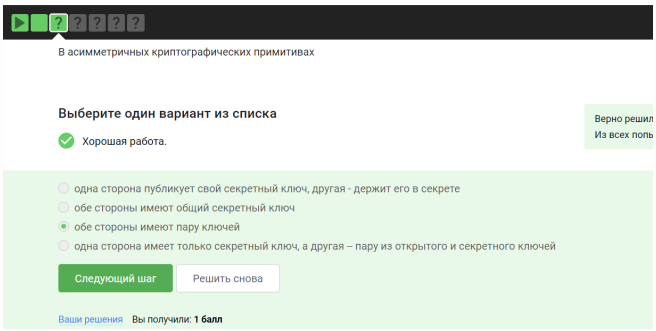
1 Цель работы

Пройти третий блок курса “Основы кибербезопасности”

2 Выполнение блока 3: Криптография на практике

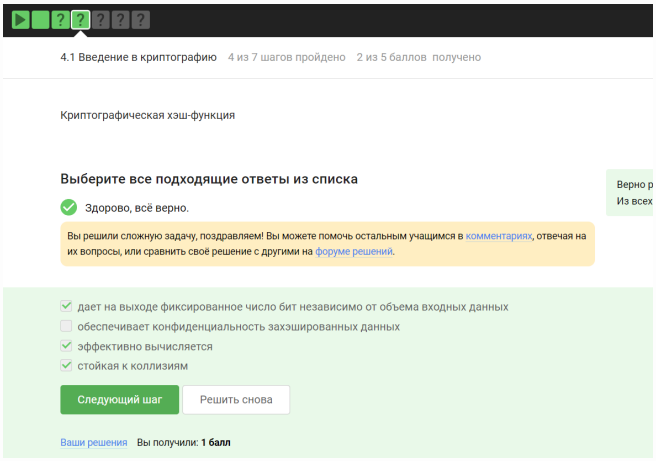
2.1 Введение в криптографию

Для ответа на вопрос используется определение ассиметричного шифрования с двумя ключами (рис. 1).



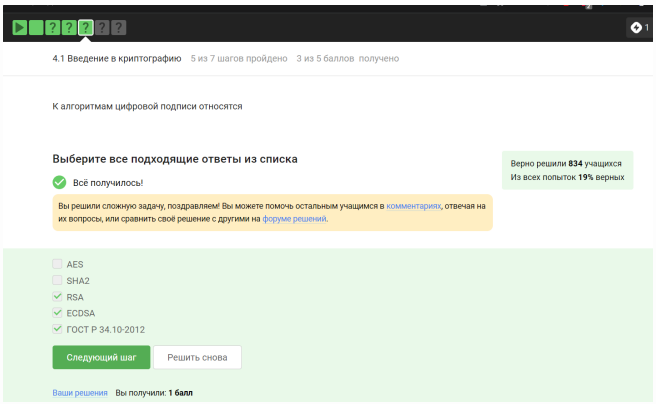
Вопрос 4.1.1

Отмечены основные условия для криптографической хэш-функции (рис. 2).



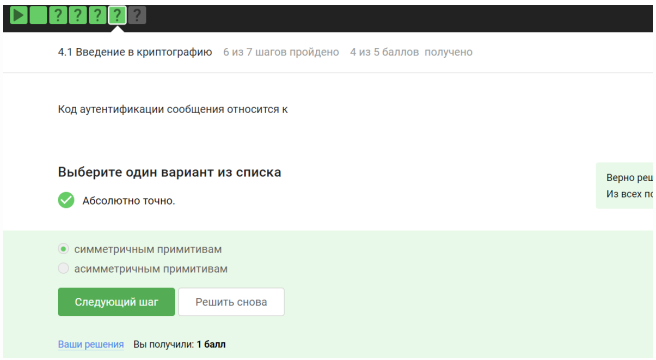
Вопрос 4.1.2

Отмечены алгоритмы цифровой подписи (рис. 3).



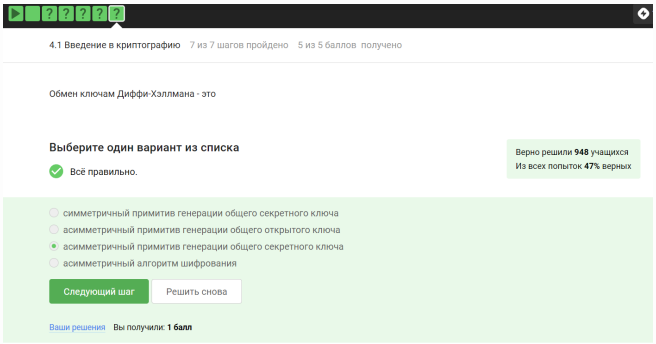
Вопрос 4.1.3

В информационной безопасности аутентификация сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения (рис. 4)



Вопрос 4.1.4

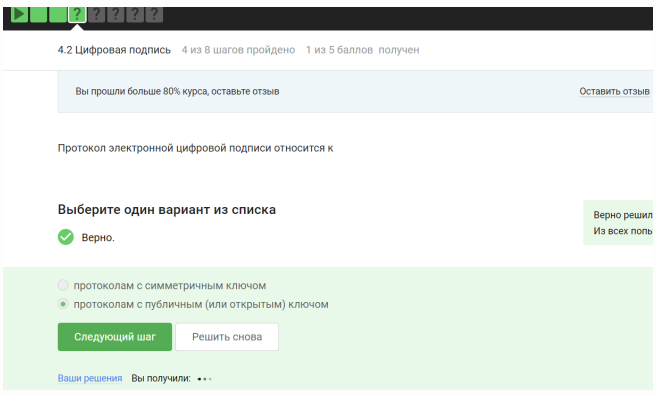
Определение обмена ключами Диффи-Хэллмана. (рис. 5).



Вопрос 4.1.5

2.2 Цифровая подпись

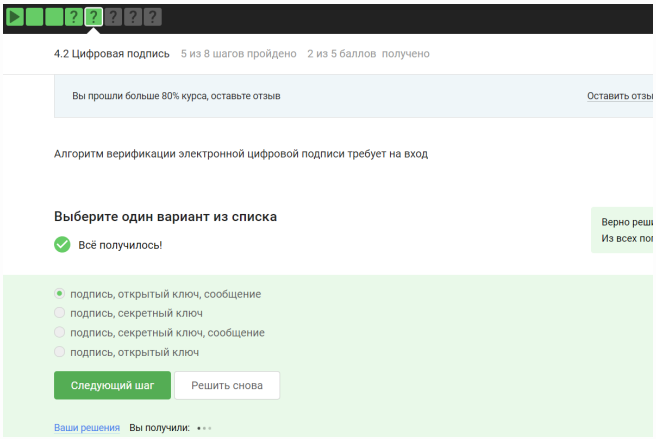
По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом (рис. 6).



Вопрос 4.2.1

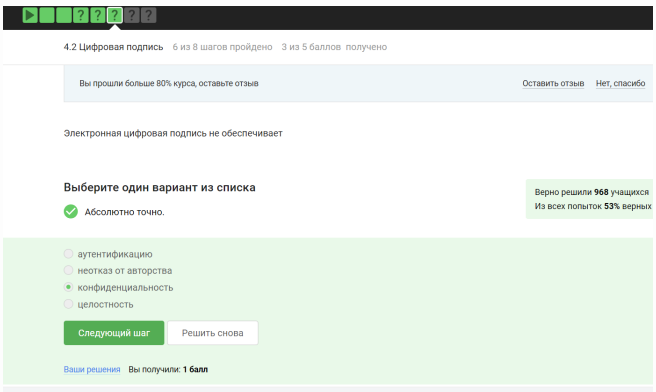
Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержа-

щейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш-функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (рис. 7).



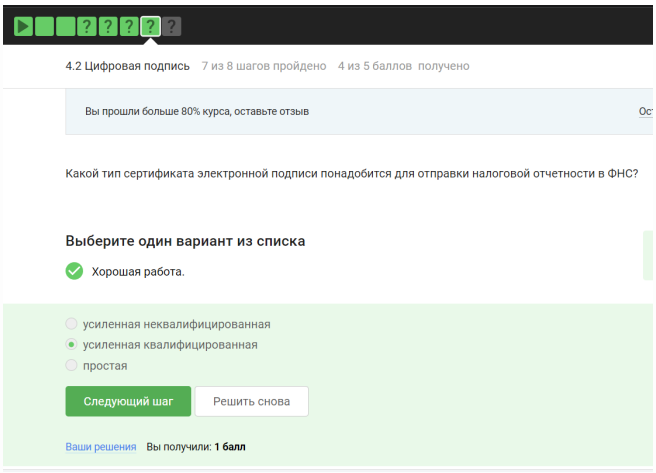
Вопрос 4.2.2

Электронная подпись обеспечивает все указанное, кроме конфиденциальности (рис. 8).



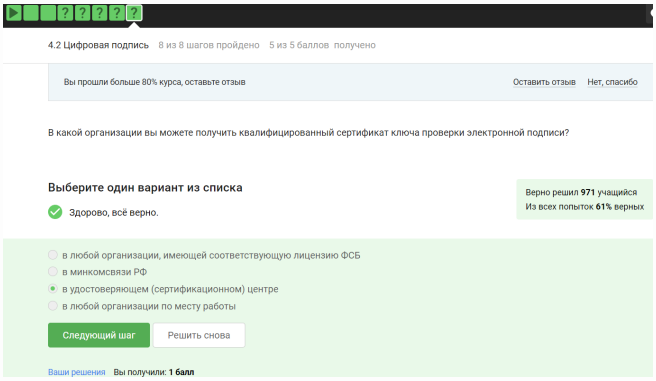
Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. 9).



Вопрос 4.2.4

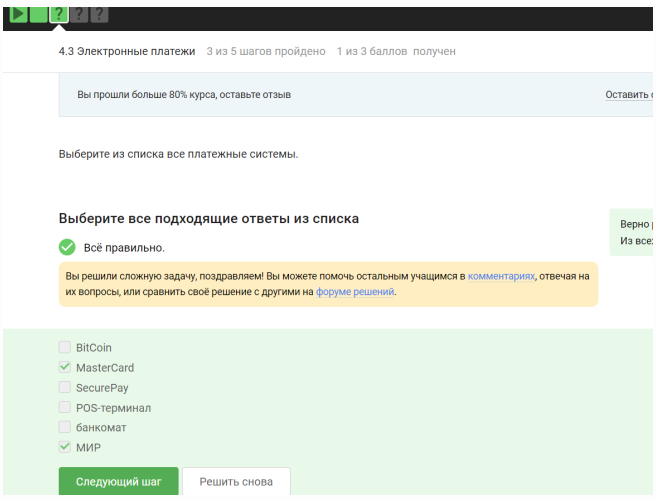
Верный ответ указан на изображении (рис. 10).



Вопрос 4.2.5

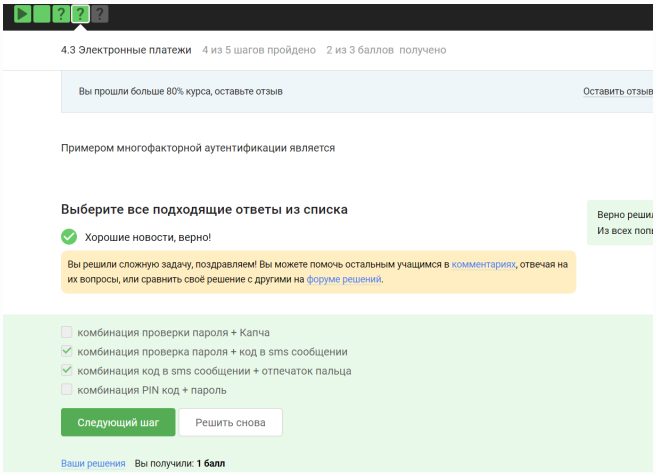
2.3 Электронные платежи

Известные платежные системы - Visa, MasterCard, МИР (рис. 11).



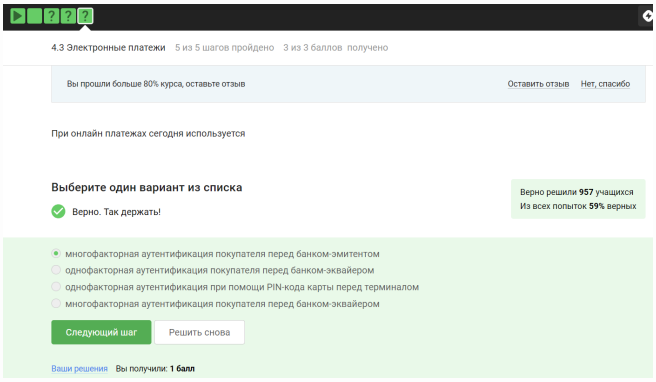
Вопрос 4.3.1

Верный ответ на изображении (рис. 12).



Вопрос 4.3.2

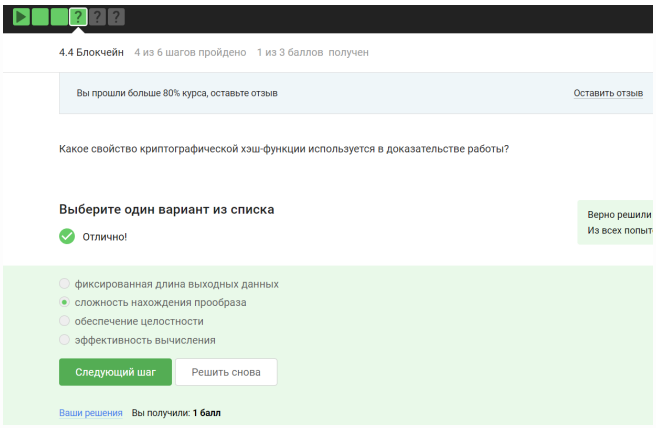
При онлайн платежах используется многофакторная аутентификация (рис. 13).



Вопрос 4.3.3

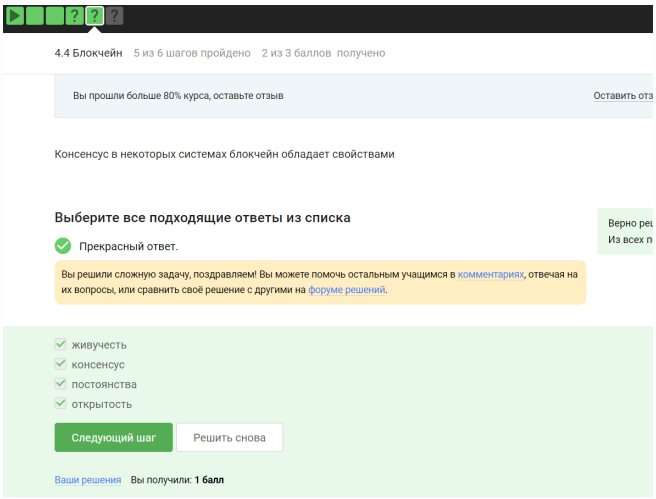
2.4 Блокчейн

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. (рис. 14).



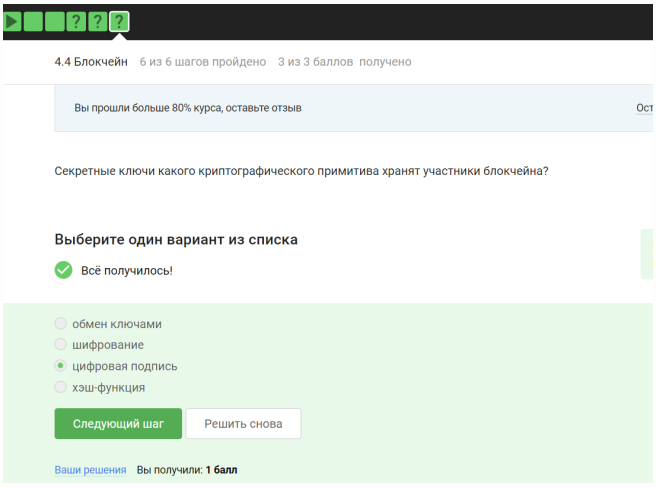
Вопрос 4.4.1

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети. Благодаря этому алгоритмы консенсуса устанавливают надежность и доверие к самоу сети. (рис. 15).



Вопрос 4.4.2

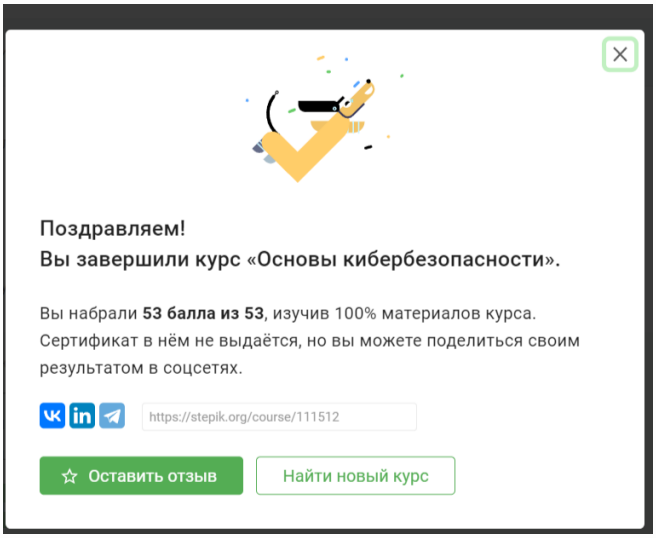
Ответ - цифровая подпись (рис. 16).



Вопрос 4.4.3

3 Выводы

Третий блок пройден успешно



Итоги