Отчёт по выполнению внешних курсов

Основы кибербезопасности

Боровиков Даниил Александрович НПИбд-01-22

Содержание

List of Figures

1 Цель работы

Пройти спец. курс “Основы кибербезопасности” и получить сертификат.

2 Выполнение лабораторной работы

2.1 Раздел 4: “Криптография на практике”

2.1.1 (4.1) “Введение в криптографию”

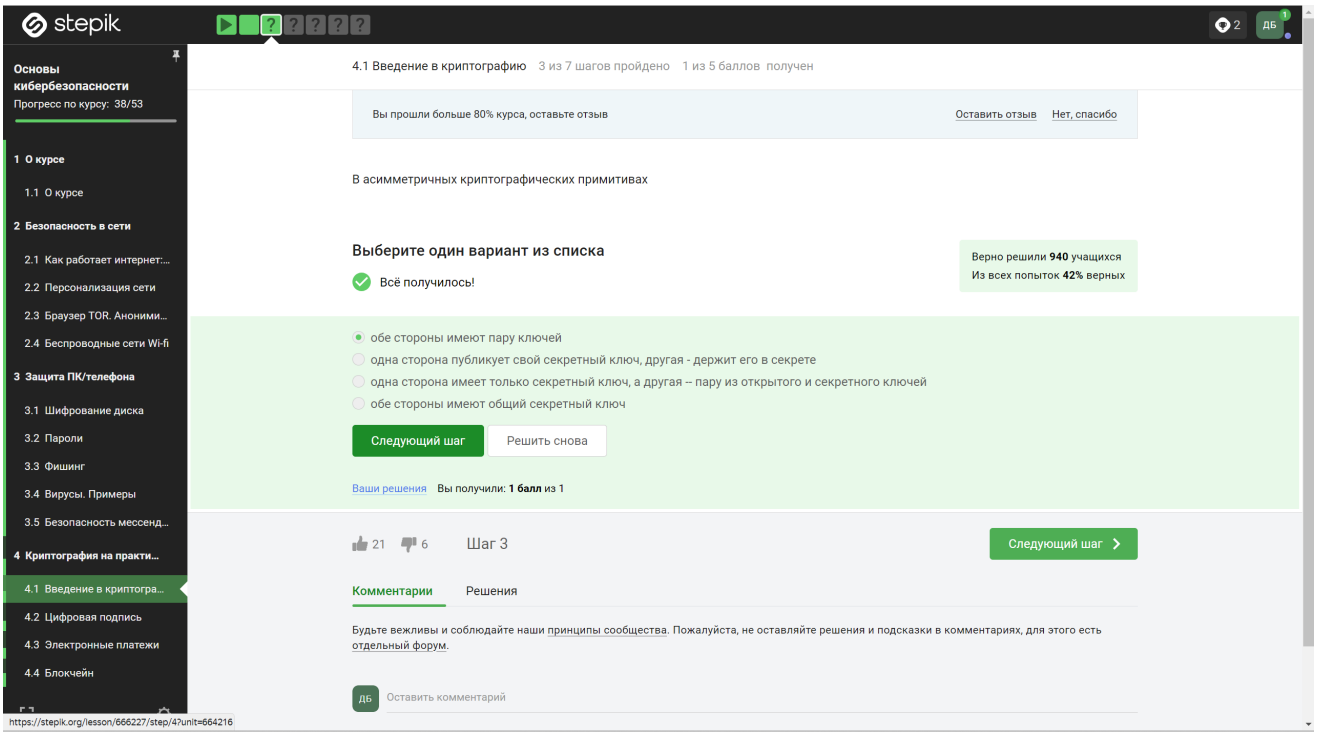

Figure 2.1: Рис. 4.1 Раздел (4.1) – Вопрос 1

Вопрос: В асимметричных криптографических примитивах

Ответ: Обе стороны имеют пару ключей

Пояснение: В асимметричной криптографии каждая сторона имеет два ключа: открытый и закрытый.

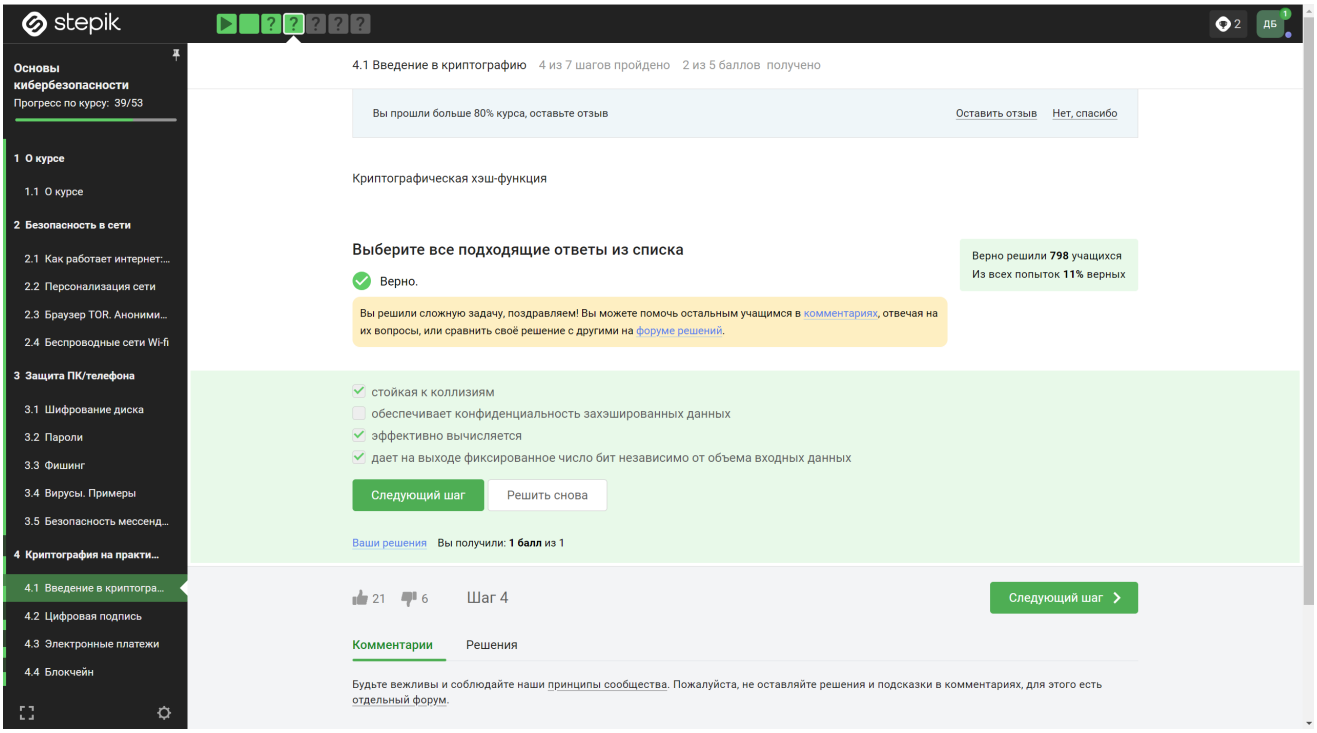

Figure 2.2: Рис. 4.2 Раздел (4.1) – Вопрос 2

Вопрос: Криптографическая хэш-функция

Ответ: Всё верно, кроме пункта “обеспечивает конфиденциальность захэшированных данных”

Пояснение: Хэш-функция обеспечивает целостность данных, но не конфиденциальность.

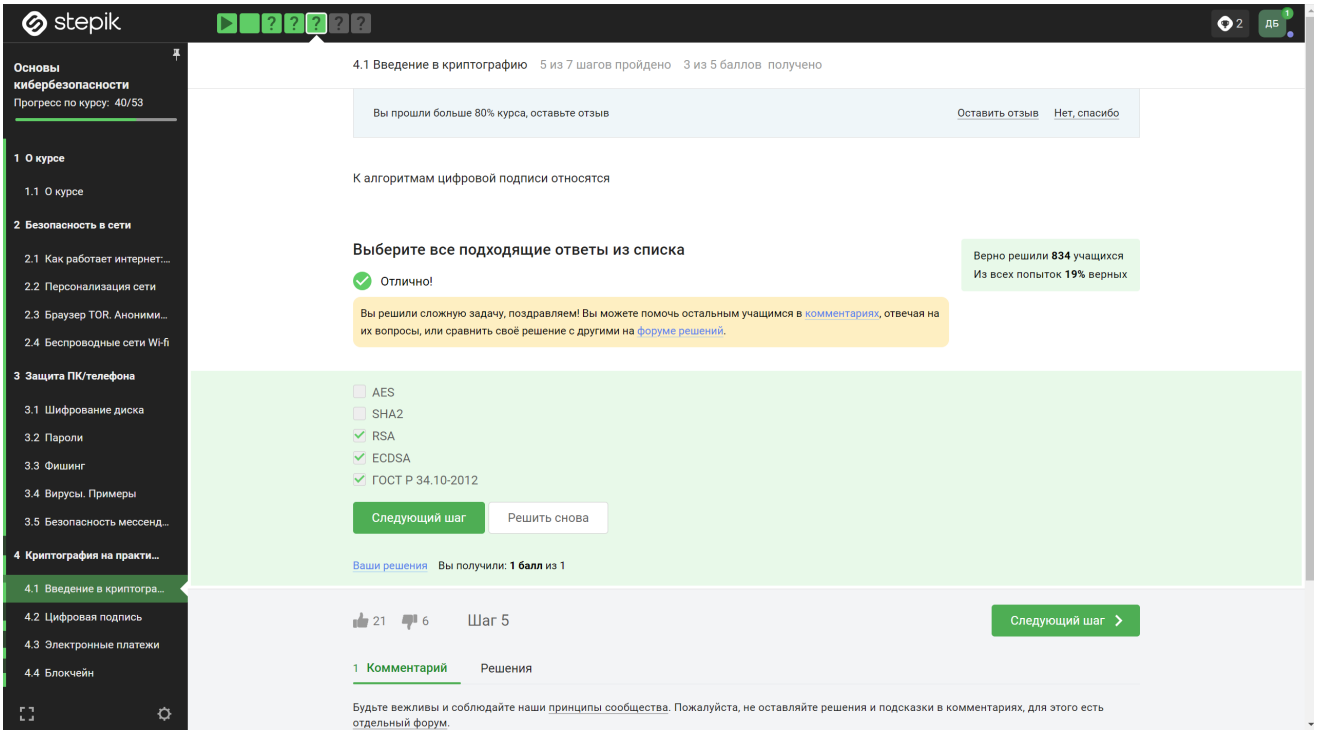

Figure 2.3: Рис. 4.3 Раздел (4.1) – Вопрос 3

Вопрос: К алгоритмам цифровой подписи относятся

Ответ: RSA, ECDSA и ГОСТ Р 34.10-2012. SHA2— это семейство криптографических хеш- функций, а AES - это алгоритм симметричного шифрования.

Пояснение: Алгоритмы цифровой подписи используются для аутентификации и целостности данных.

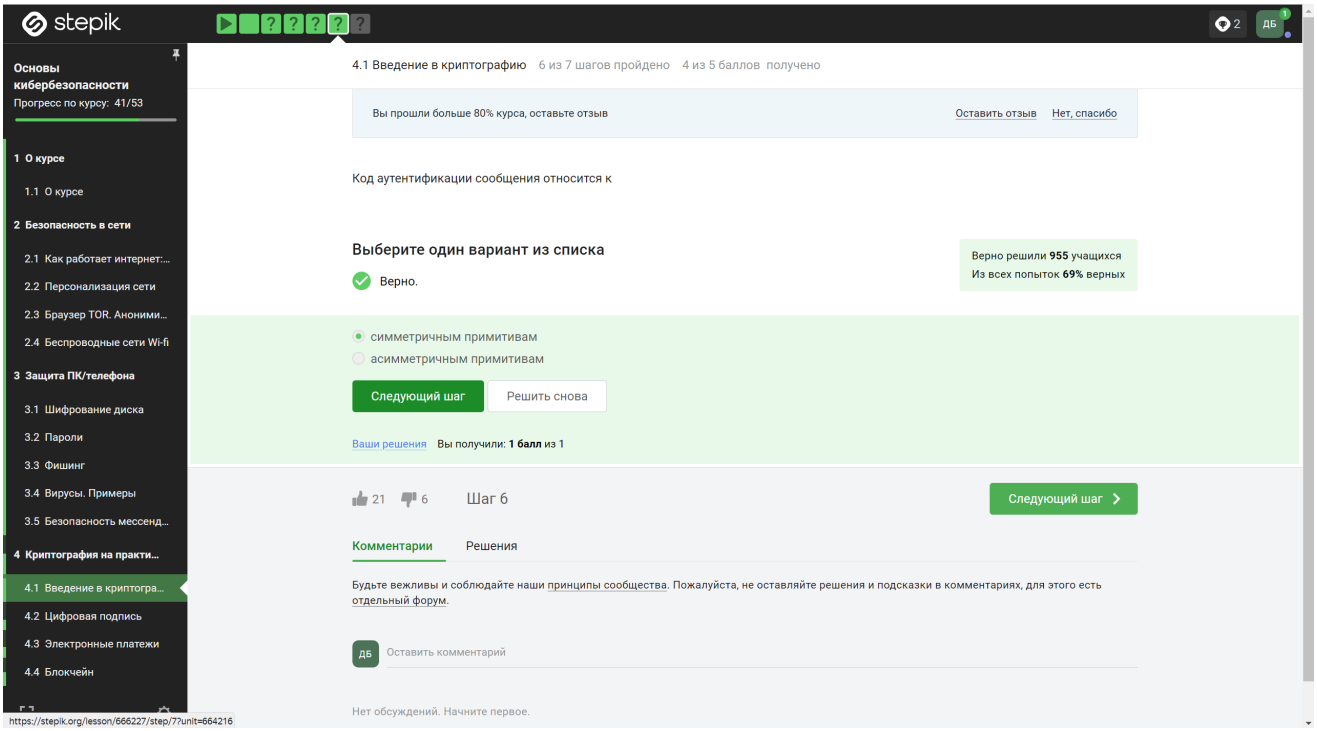

Figure 2.4: Рис. 4.4 Раздел (4.1) – Вопрос 4

Вопрос: Код аутентификации сообщения относится к

Ответ: Код аутентификации сообщения относится к симметричным примитивам

Пояснение: MAC (Message Authentication Code) — это симметричный примитив для аутентификации сообщений.

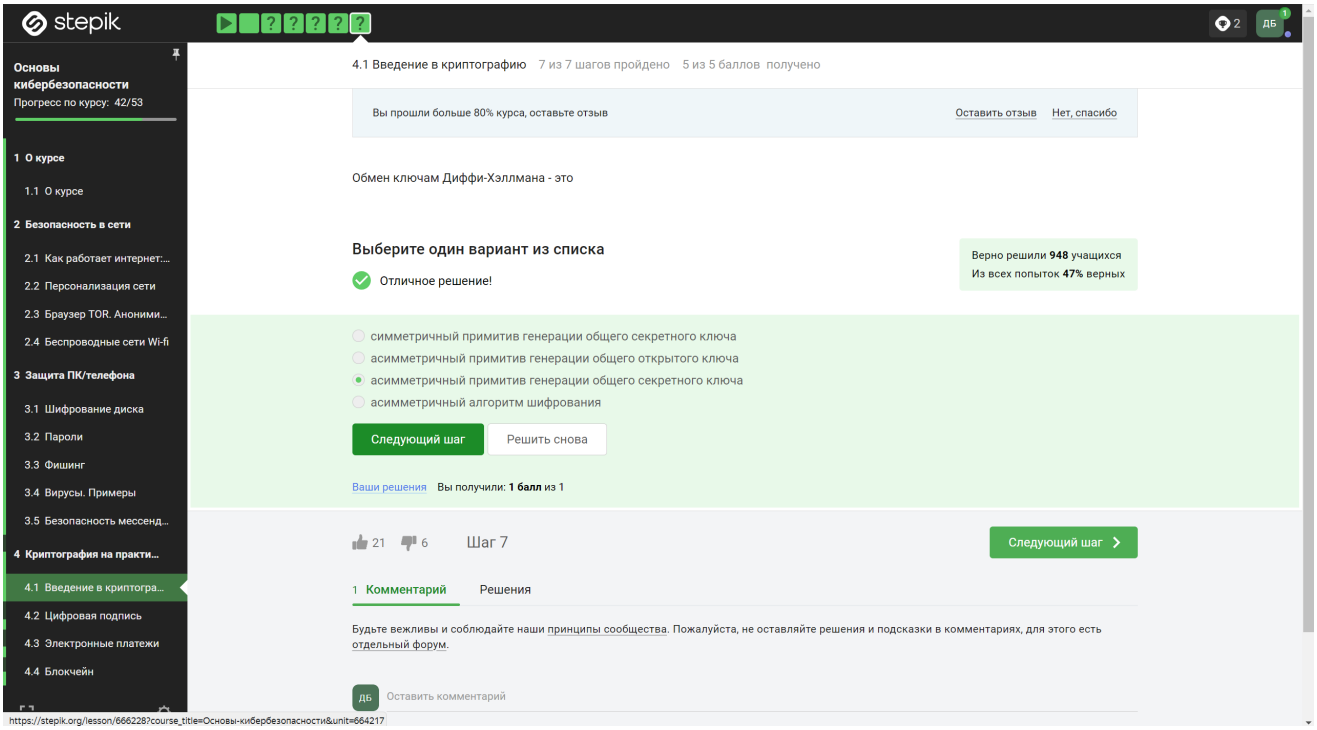

Figure 2.5: Рис. 4.5 Раздел (4.1) – Вопрос 5

Вопрос: Обмен ключам Диффи-Хэллмана - это

Ответ: Обмен ключам Диффи-Хэллмана – это асимметричный примитив генерации общего секретного ключа

Пояснение: Диффи-Хэллман используется для безопасного обмена секретными ключами через открытые каналы.

2.1.2 (4.2) “Цифровая подпись”

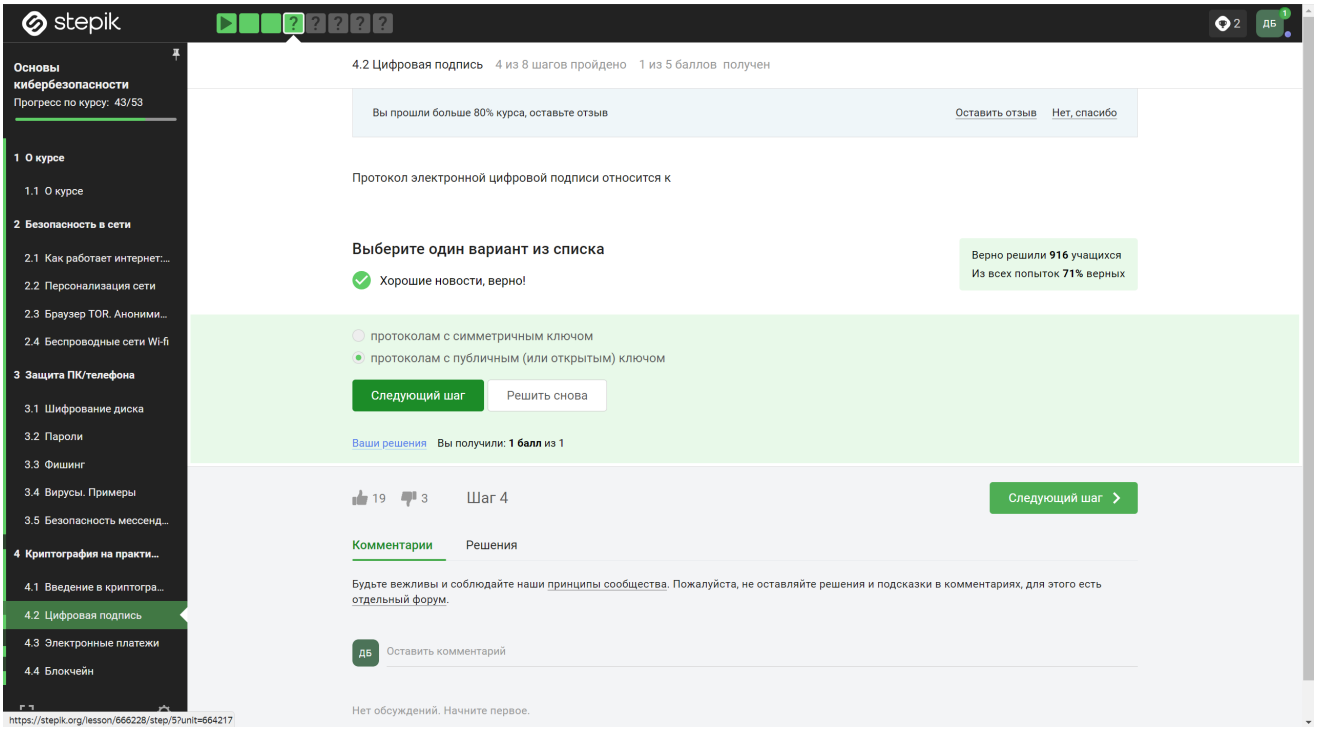

Figure 2.6: Рис. 4.6 Раздел (4.2) – Вопрос 1

Вопрос: Протокол электронной цифровой подписи относится к

Ответ: Он относится к протоколам с публичным (или открытым) ключом

Пояснение: Протоколы электронной цифровой подписи используют открытые ключи для проверки подписи.

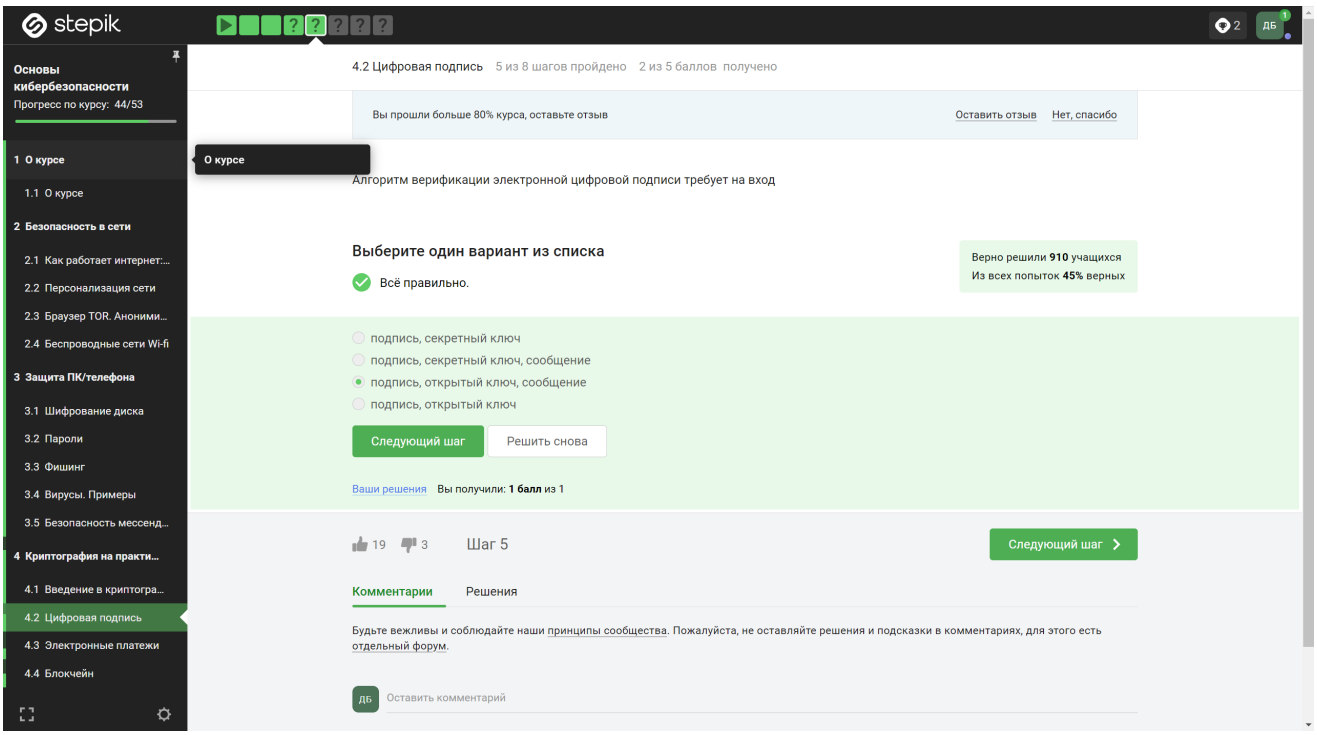

Figure 2.7: Рис. 4.7 Раздел (4.2) – Вопрос 3

Вопрос: Алгоритм верификации электронной цифровой подписи требует на вход

Ответ: Этот алгоритм вход требует подпись, открытый ключ, сообщение

Пояснение: Для верификации электронной цифровой подписи требуется подпись, соответствующий открытый ключ и сообщение.

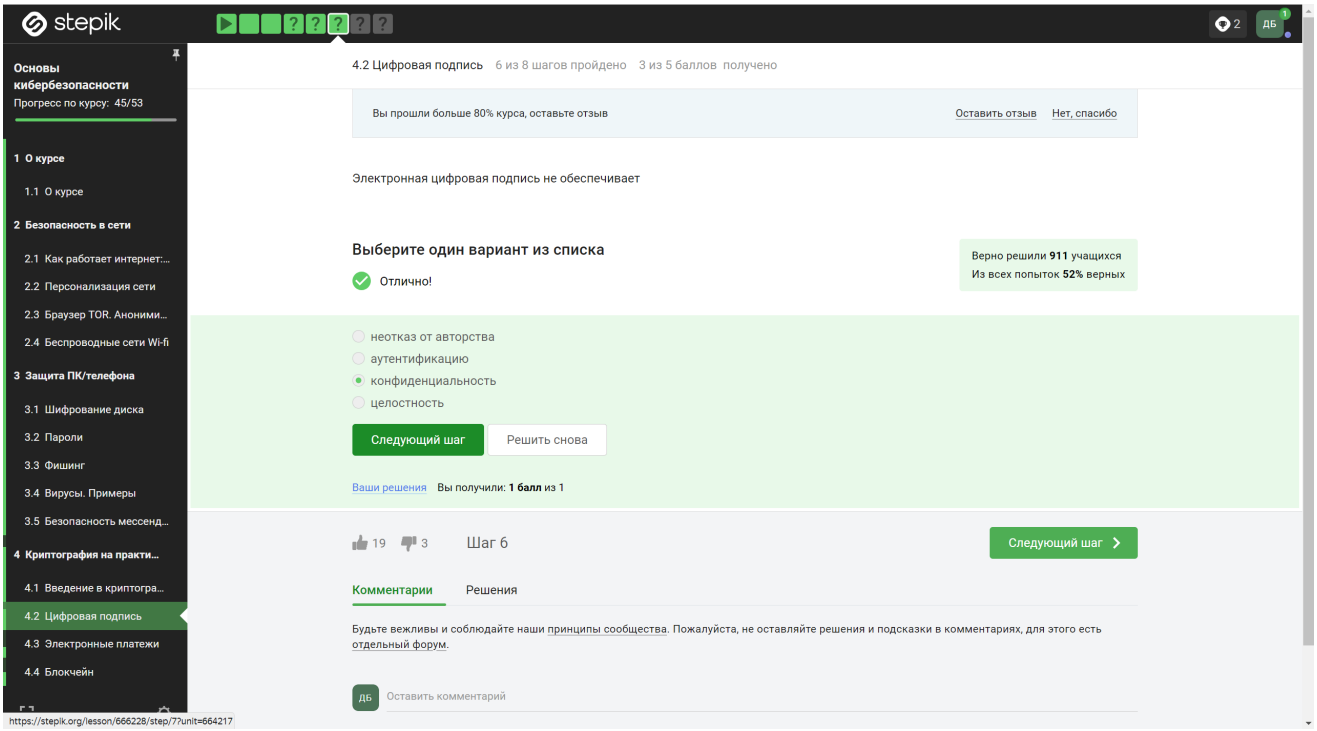

Figure 2.8: Рис. 4.8 Раздел (4.2) – Вопрос 3

Вопрос: Электронная цифровая подпись не обеспечивает

Ответ: Электронная цифровая подпись не может обеспечить конфиденциальность

Пояснение: Цифровая подпись обеспечивает аутентификацию и целостность, но не конфиденциальность.

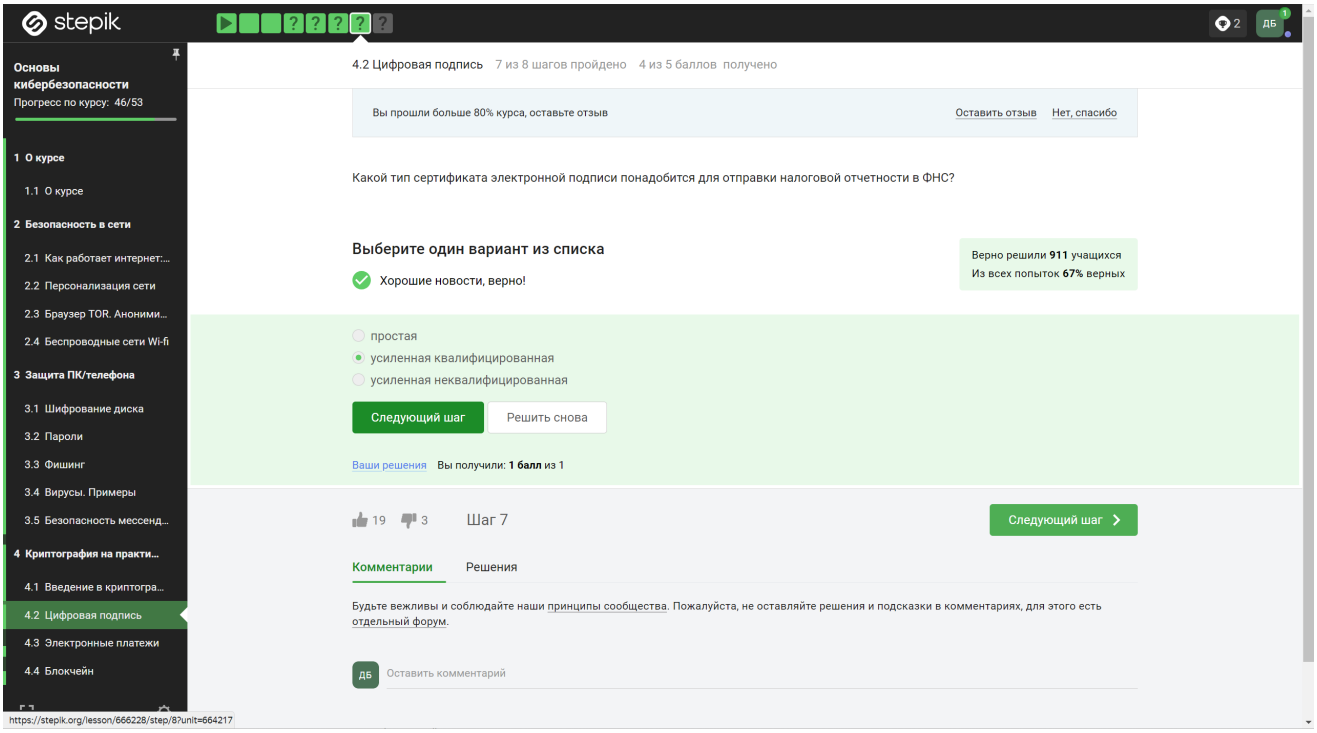

Figure 2.9: Рис. 4.9 Раздел (4.2) – Вопрос 4

Вопрос: Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Ответ: ФНС требует сертификат электронной подписи с усиленной квалификацией

Пояснение: Для отправки налоговой отчетности в ФНС требуется сертификат с усиленной квалификацией.

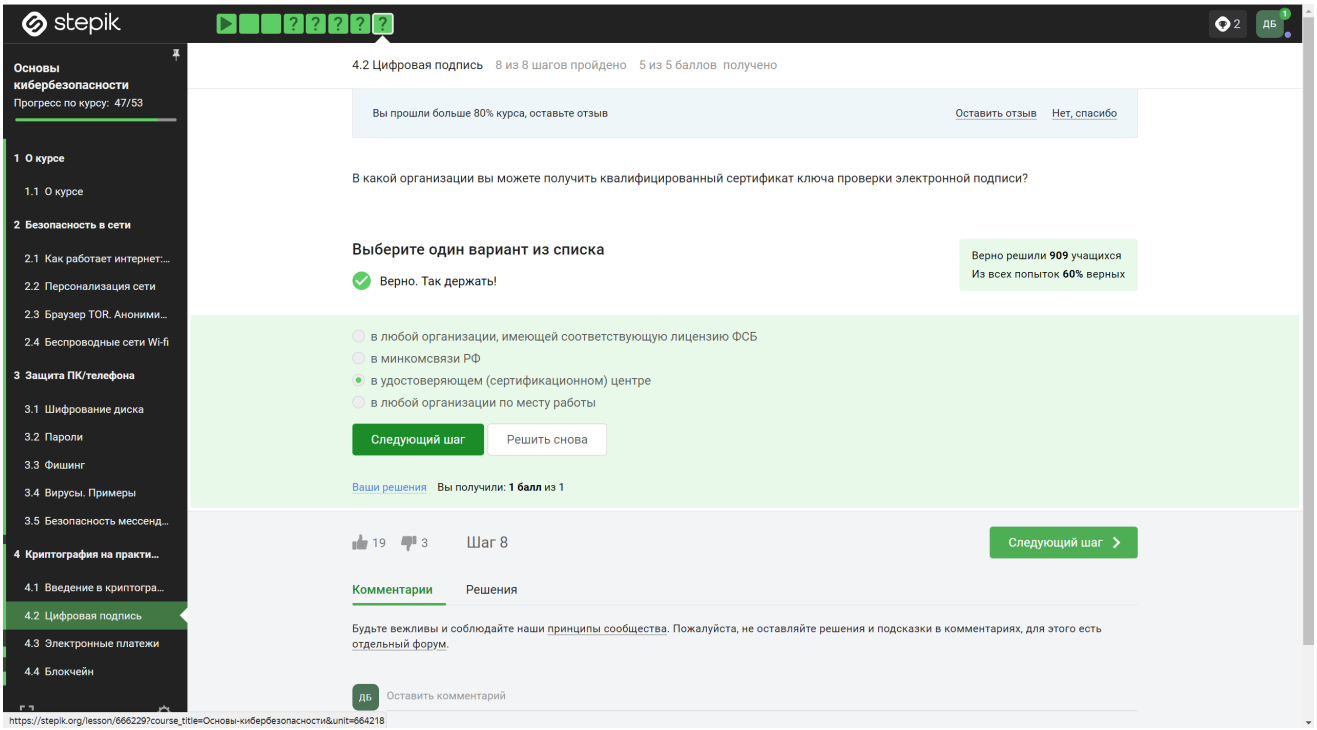

Figure 2.10: Рис. 4.10 Раздел (4.2) – Вопрос 6

Вопрос: В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Ответ: Сертификаты ключа проверки электронной подписи выдаются в сертификационном центре

Пояснение: Квалифицированные сертификаты ключа проверки электронной подписи выдаются в специальных сертификационных центрах.

2.1.3 (4.3) “Электронные платежи”

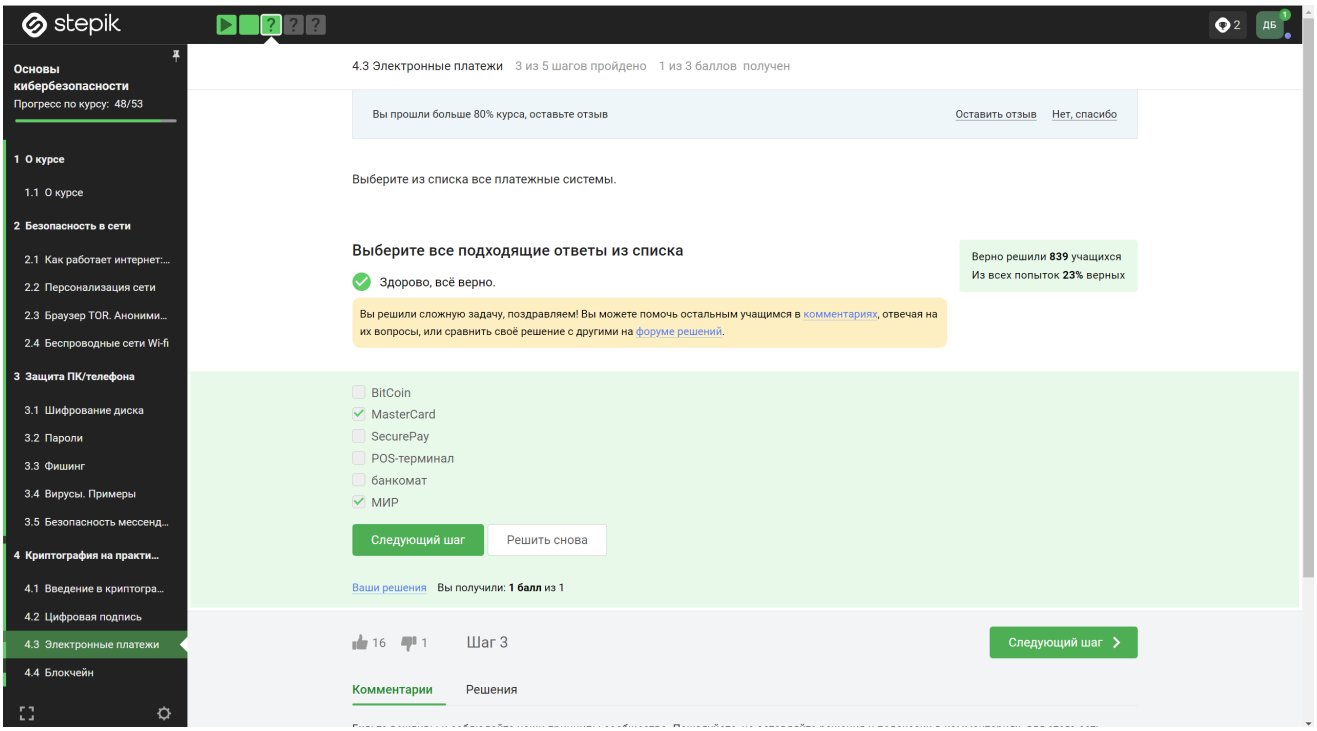

Figure 2.11: Рис. 4.11 Раздел (4.3) – Вопрос 1

Вопрос: Выберите из списка все платежные системы.

Ответ: МИР и MasterCard являются платежными системами

Пояснение: МИР и MasterCard представляют собой платежные системы, через которые можно осуществлять денежные переводы и платежи.

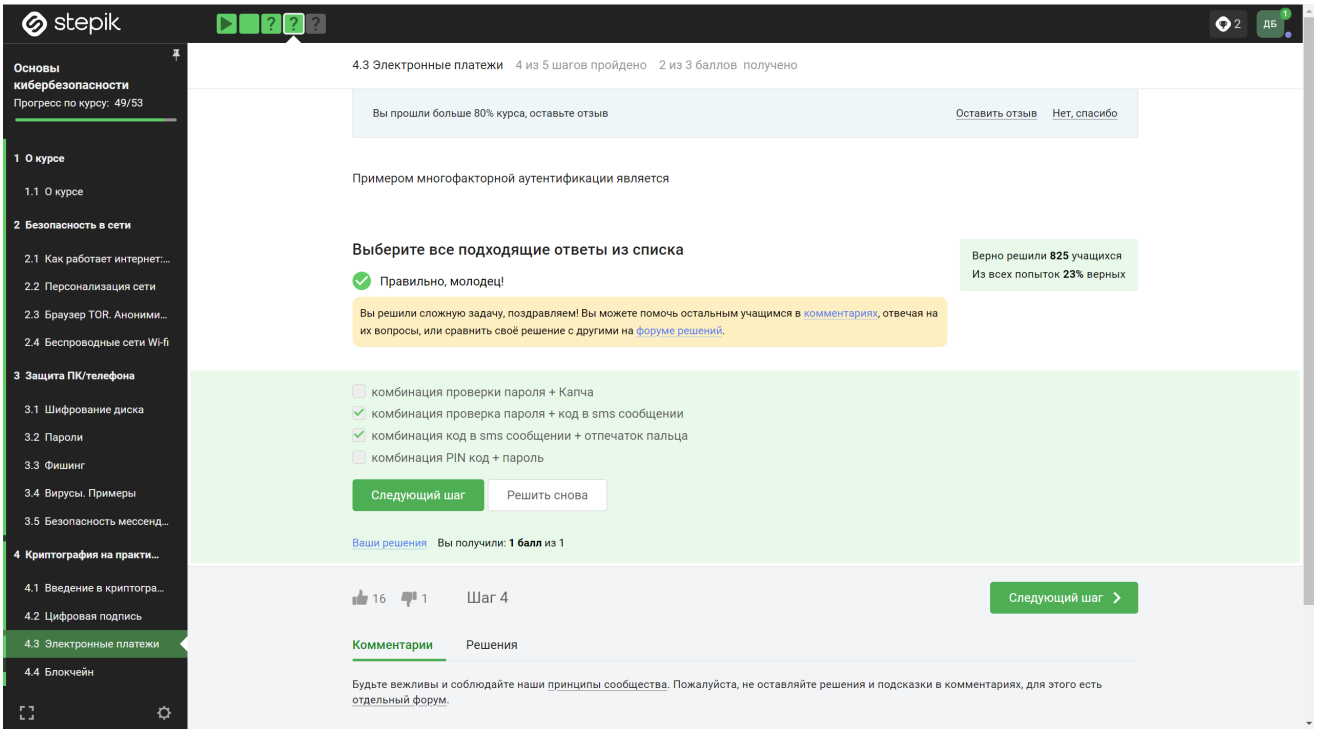

Figure 2.12: Рис. 4.12 Раздел (4.3) – Вопрос 2

Вопрос: Примером многофакторной аутентификации является

Ответ: К многофакторной аутентификации относятся: проверка пароля, код в sms сообщении и отпечаток пальца

Пояснение: Многофакторная аутентификация включает в себя несколько методов проверки личности, таких как пароль, SMS-коды и биометрические данные.

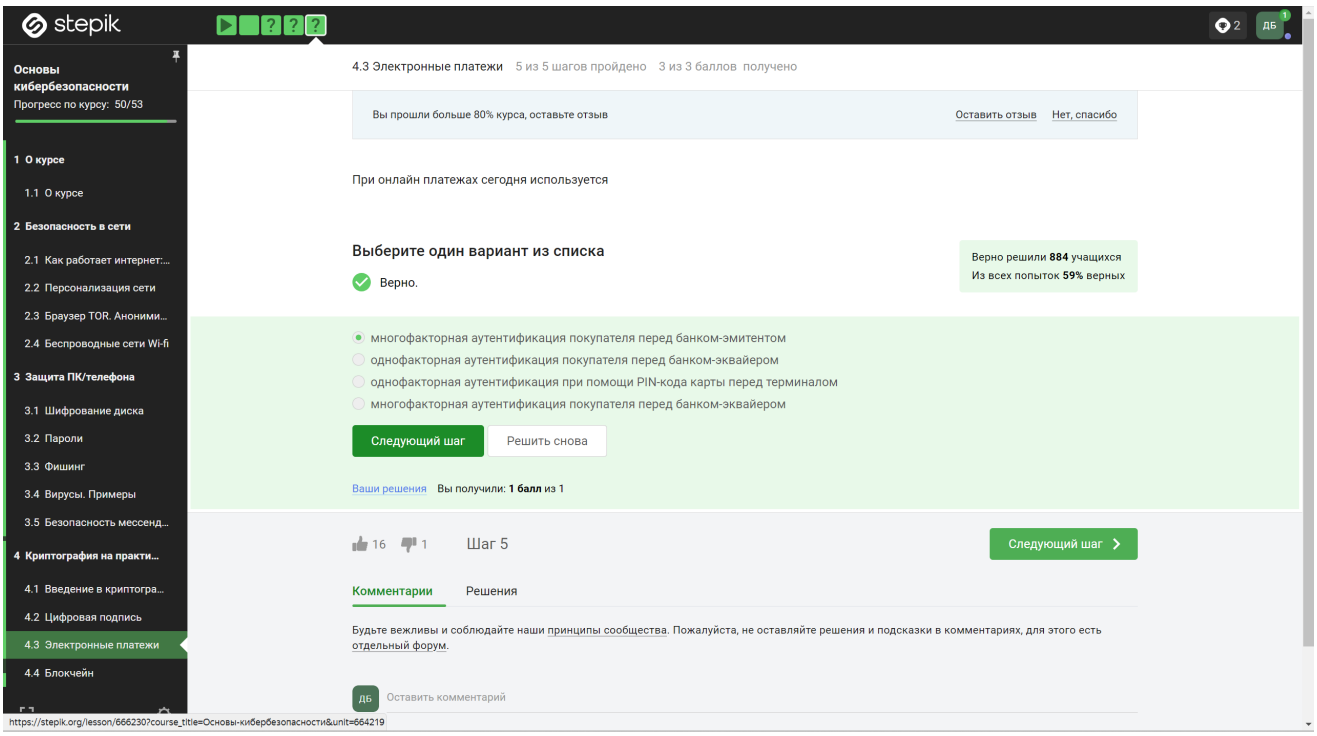

Figure 2.13: Рис. 4.13 Раздел (4.3) – Вопрос 3

Вопрос: При онлайн платежах сегодня используется

Ответ: Онлайн платежи используют многофакторную аутентификацию покупателя перед банком-эмитентом

Пояснение: Для повышения безопасности онлайн платежей часто требуется многофакторная аутентификация клиента перед банком-эмитентом.

2.1.4 (4.4) “Блокчейн”

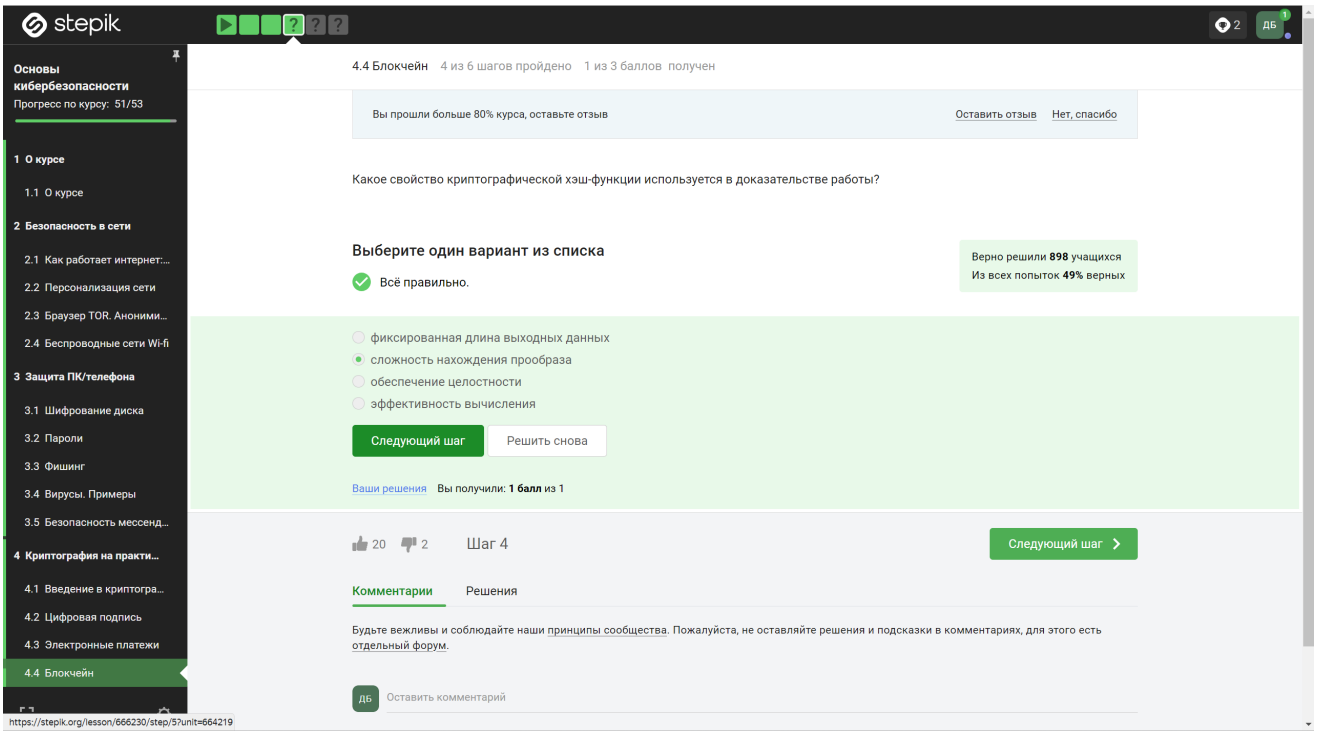

Figure 2.14: Рис. 4.14 Раздел (4.4) – Вопрос 1

Вопрос: Какое свойство криптографической хэш-функции используется в доказательстве работы?

Ответ: Используется сложность нахождения прообраза

Пояснение: В доказательстве работы используется свойство хэш-функции, обеспечивающее сложность нахождения прообраза.

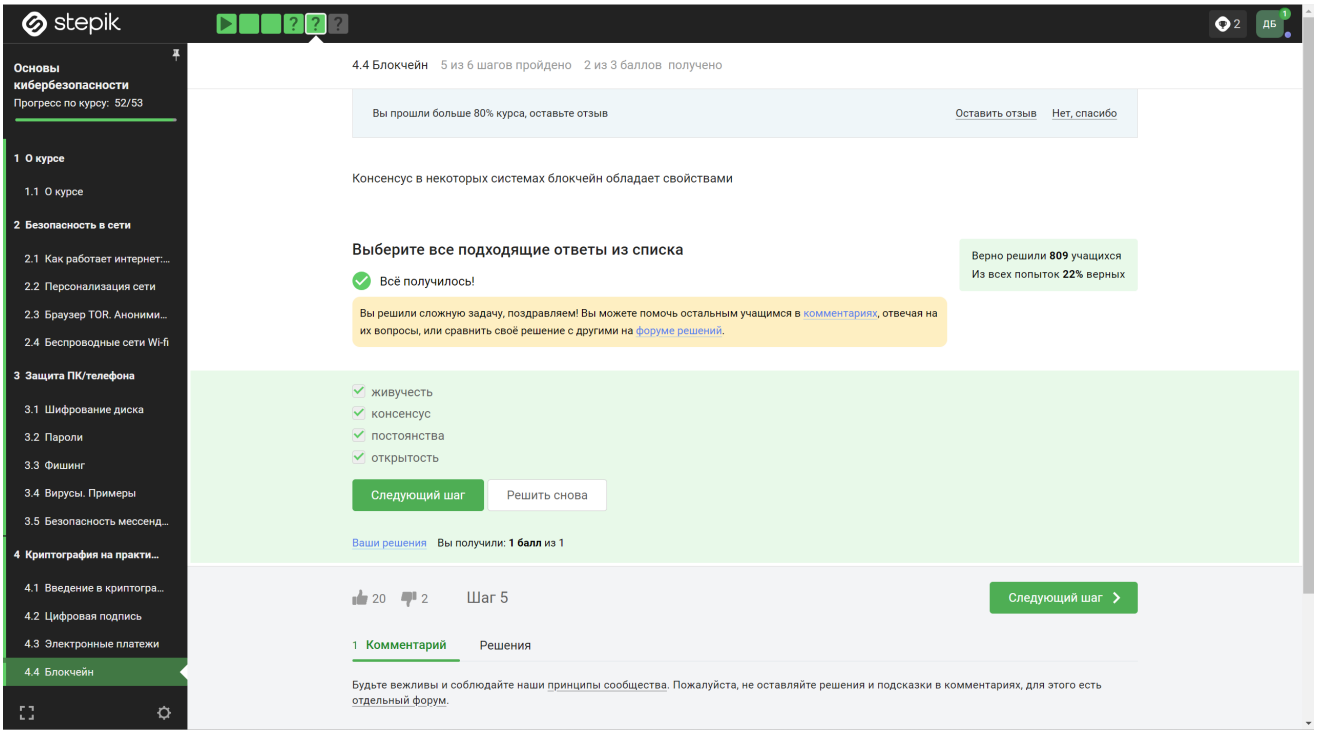

Figure 2.15: Рис. 4.15 Раздел (4.4) – Вопрос 2

Вопрос: Консенсус в некоторых системах блокчейн обладает свойствами

Ответ: Обладает всеми перечисленными свойствами

Пояснение: Консенсус в блокчейне может обладать свойствами, такими как надежность, децентрализация и устойчивость к взлому.

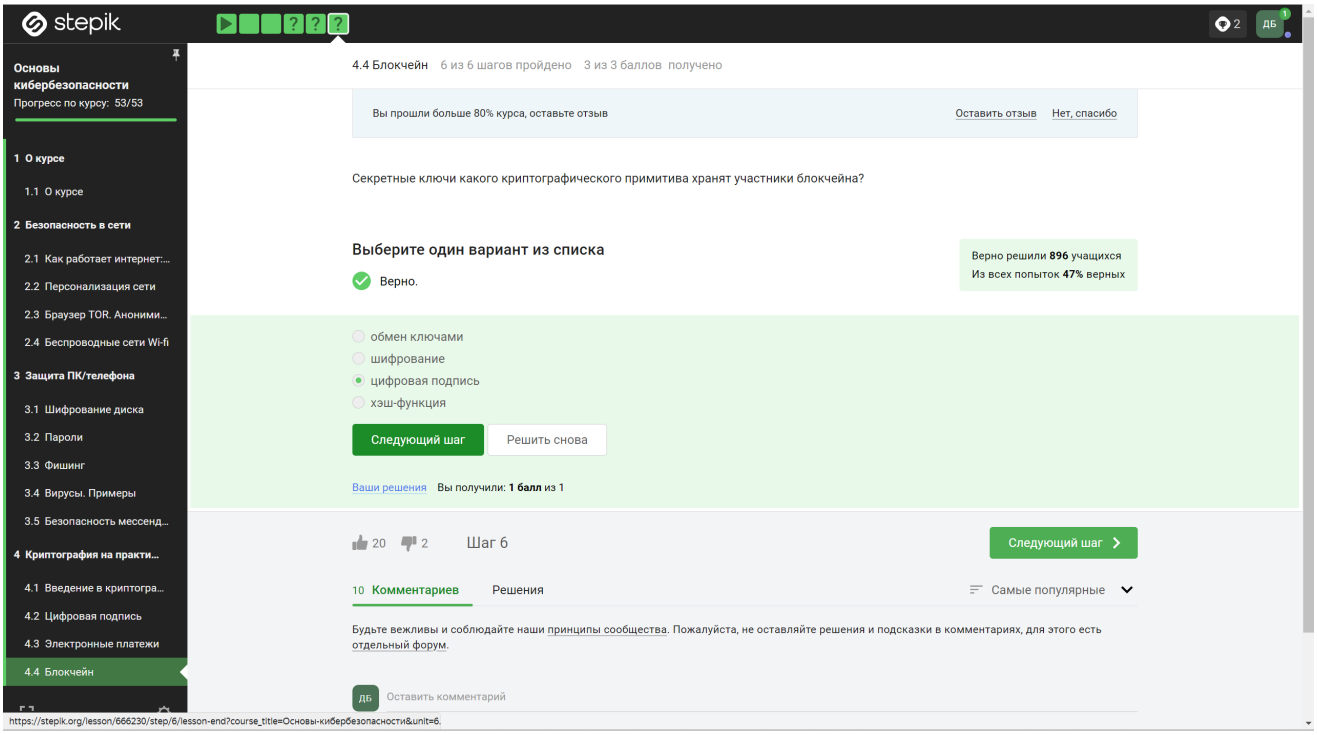

Figure 2.16: Рис. 4.16 Раздел (4.4) – Вопрос 4

Вопрос: Секретные ключи какого криптографического примитива хранят участники блокчейна?

Ответ: Участники блокчейна хранят секретные ключи, которые используются для цифровой подписи

Пояснение: Секретные ключи в блокчейне используются для создания и проверки цифровых подписей, обеспечивая аутентификацию и целостность данных.

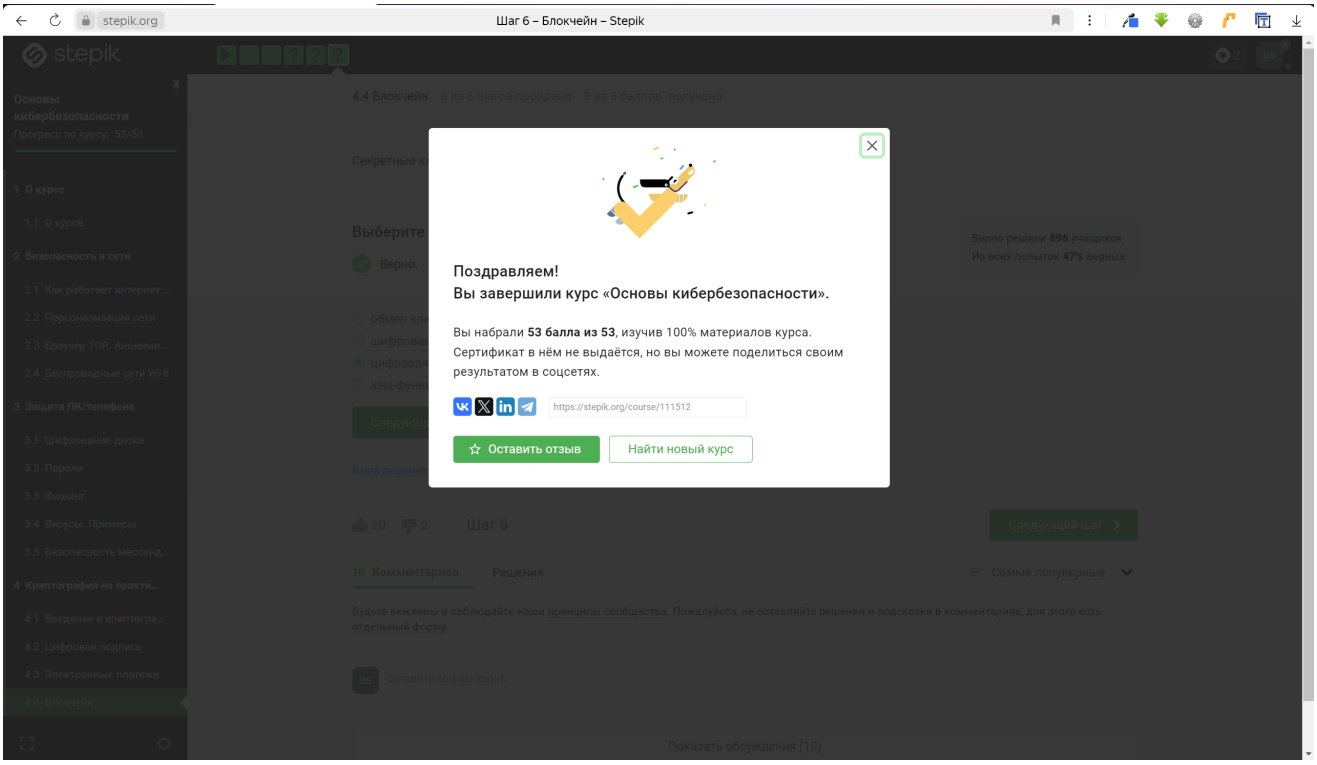

Figure 2.17: Рис. 4.17 Сертификат

3 Вывод

В ходе прохождения внешних курсов были получены навыки о “Безопасности в сети”, “Защите ПК/телефона” и “Криптографии”.