Отчет по третьему этапу внешнего курса

Дисциплина: основы информационнной безопасности

Казазаев Даниил Михайлович

Содержание

# 1 Цель работы

Внешний кур состоит из трех этапов.

# 2 Этап первый

Первый этап курса состоит из 4 частей:

1. Введине в криптографию
2. Цифровая подпись
3. Электронные платежи
4. Блокчейн

# 3 Выполнение первого этапа внешнего курса.

## 3.1 Введине в криптографиюВведине в криптографию

В ассиметричных криптографических примитивах обестороны имеют пару ключей. (рис. 1)

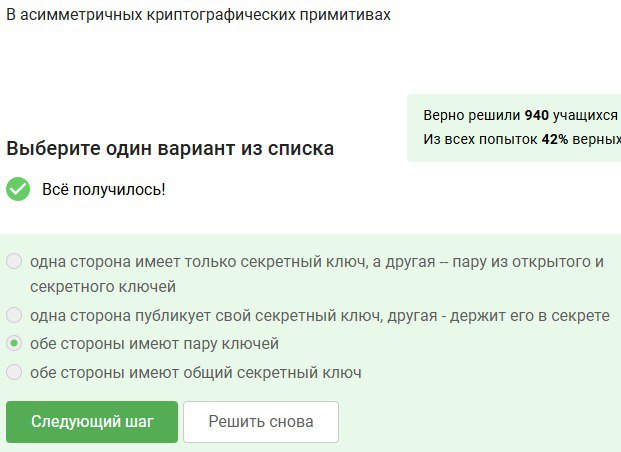


Рис. 1: Первый вопрос

Хещ-функция стойкая к колизиям, дает определенное кол-во бит вне зависимости от объема входных данных и эффективно вычисляется. (рис. 2)

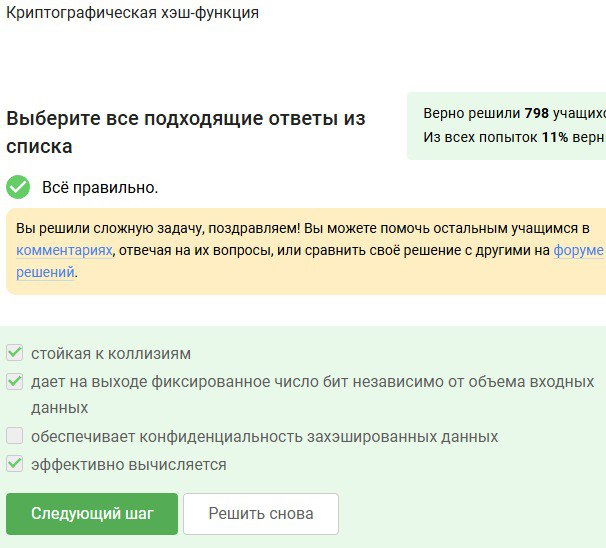


Рис. 2: Второй вопрос

RSA, ECDSA и ГОСТ стандарт(кузнечик) - алгоритмы цифровой подписи. (рис. 3)

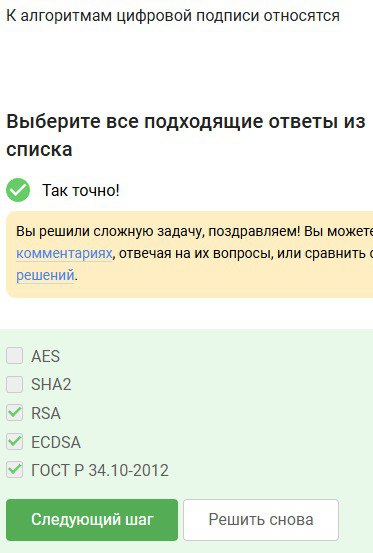


Рис. 3: Третий вопрос

Код аунтификации сообщения отеосится к симмитричным примитивам. (рис. 4)

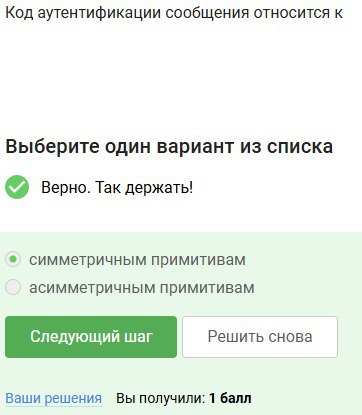


Рис. 4: Четвертый вопрос

Обмен ключами Диффи-Хэллмана - ассиметрический примитив генерации обзего секретного ключа. (рис. 5)

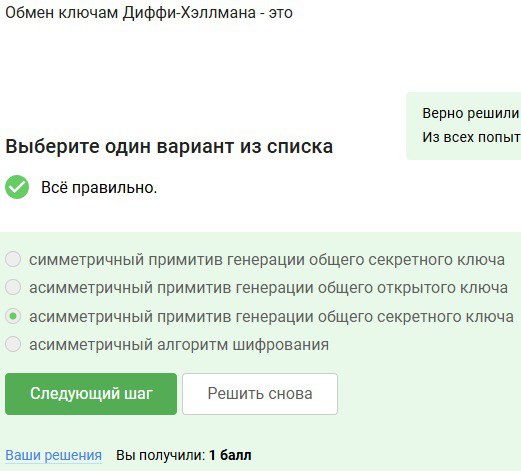


Рис. 5: Пятый вопрос

# 4 Цифровая подпись

Протоколы цифровой подписи с публичным ключом.(рис. 6)

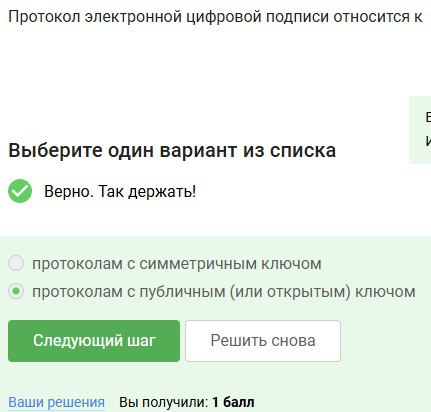


Рис. 6: Первый вопрос

Алгоритм верификации требует на вход: подпись, открытый ключ, сообщение.(рис. 7)

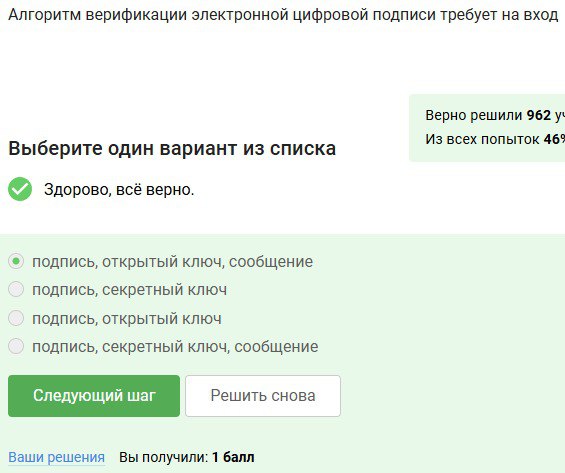


Рис. 7: Второй вопрос

Электронная подпись не обеспечивает конфиденциальность.(рис. 8)

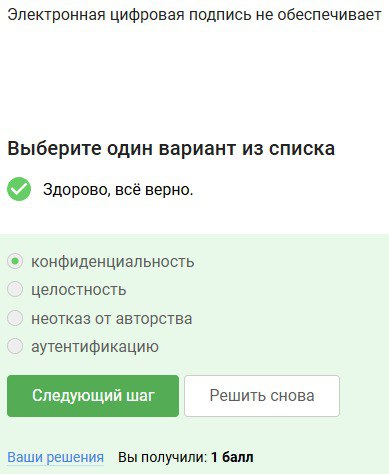


Рис. 8: Третий вопрос

Для отправки налоговой отчетности необходим сертификат с усилненной квалификацией.(рис. 9)

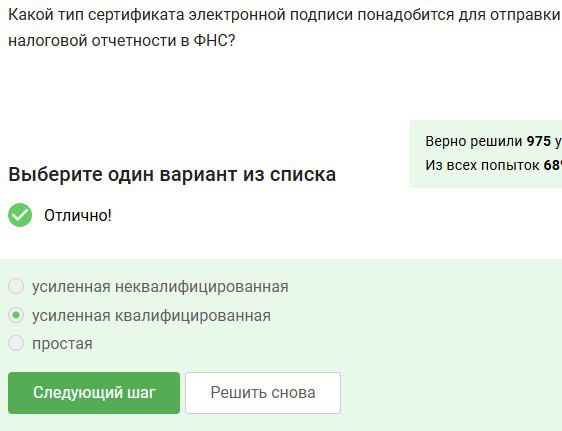


Рис. 9: Четвертый вопрос

Квалифицированный сертификат можно получить в удостоверяющем центре.(рис. 10)

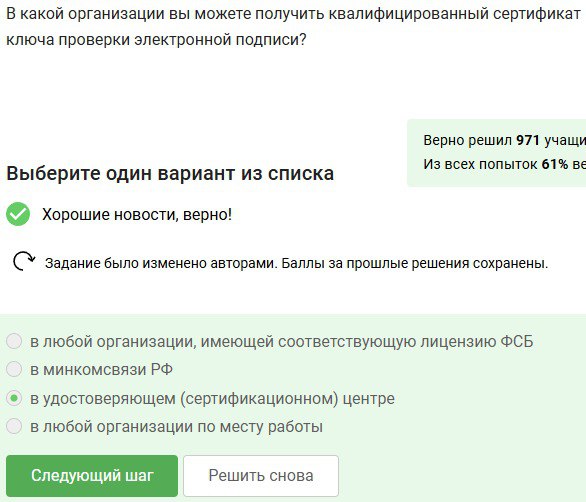


Рис. 10: Пятый вопрос

# 5 Электронные платежи

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

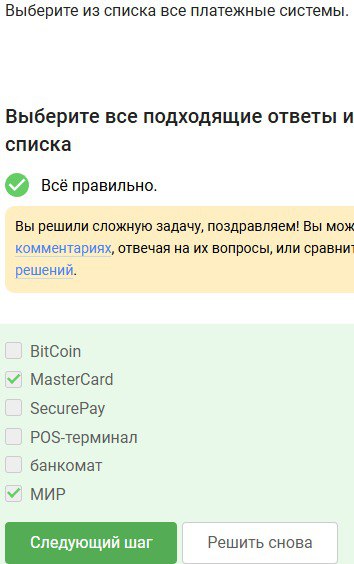


Рис. 11: Первый вопрос

Отмеченные варианты ответов являются примером многофакторной аутентификации. (рис. 12)

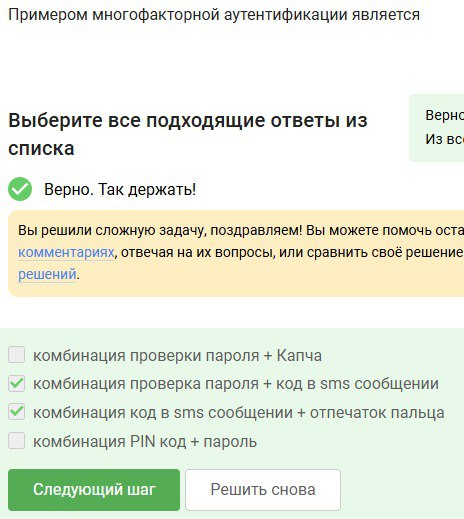


Рис. 12: Второй вопрос

Сегодня при онлайн платежах используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 13)

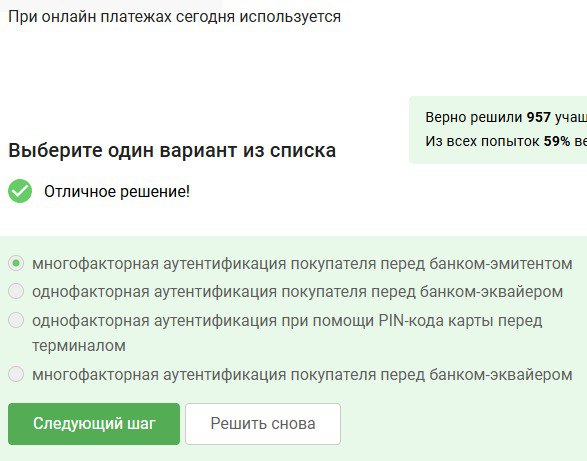


Рис. 13: Третий вопрос

# 6 Блокчейн

В доказательстве работы криптографической хеш-функции используется сложность нахождения прообраза. (рис. 14)

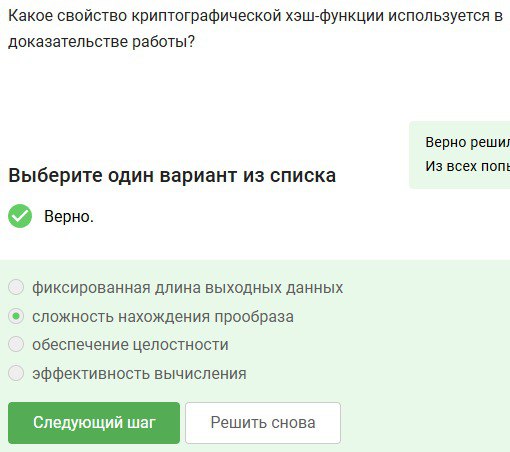


Рис. 14: Первый вопрос

Все ответы являются верными для консенсуса некоторых блокчейн систем. (рис. 15)

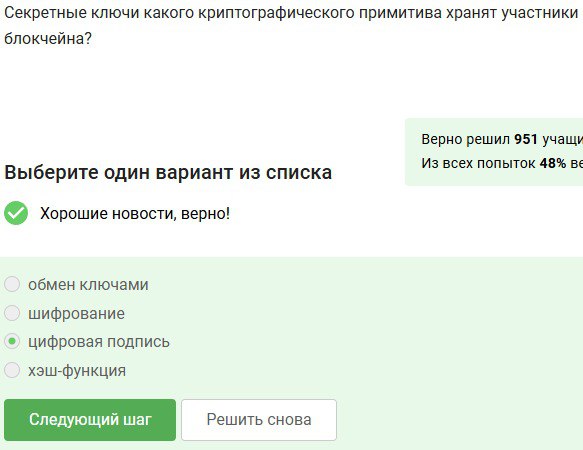


Рис. 15: Второй вопрос

Участники криптографического примитива хранят при себе только цифровую подпись. (рис. 16)

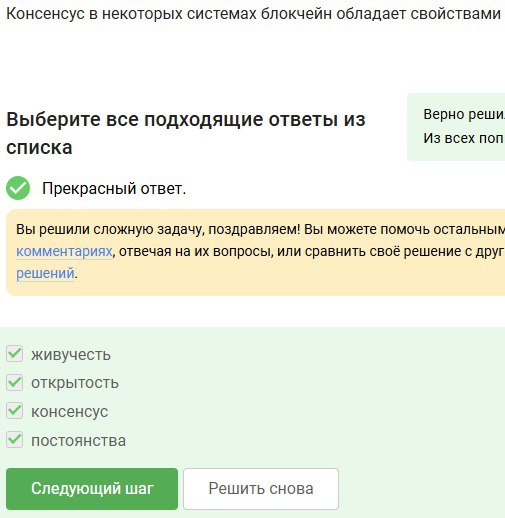


Рис. 16: Третий вопрос

# 7 Вывод

Выполнен третий этап внешнего курса