Внешний курс. Раздел 3

Основы информационной безопасности

Малюга Валерия Васильевна

8 марта 2024

Российский университет дружбы народов

Цель работы

Цель

Пройти третий блок курса **«Основы кибербезопасности»**,
освоить основы **криптографии на практике**.

Криптография на практике

Введение: Ассиметричное шифрование

Используется определение ассиметричного шифрования с двумя ключами:

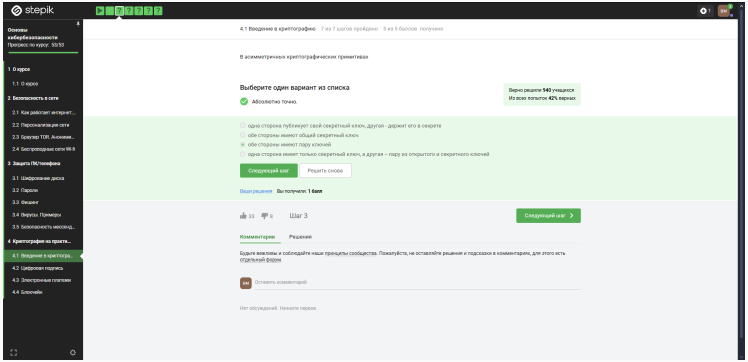


Рис. 1: Вопрос 4.1.1

Основные условия для криптографической хэш-функции:

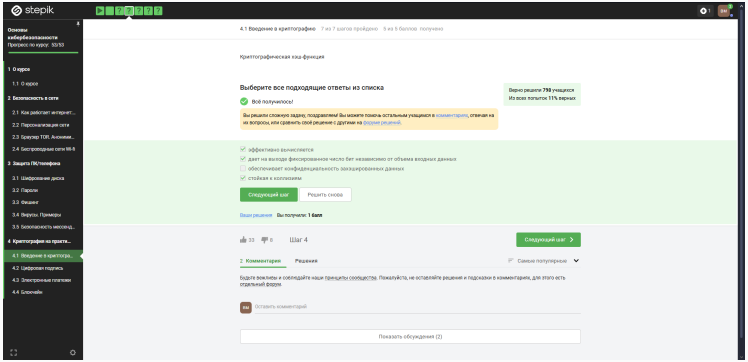


Рис. 2: Вопрос 4.1.2

Алгоритмы цифровой подписи

Отмечены алгоритмы цифровой подписи:

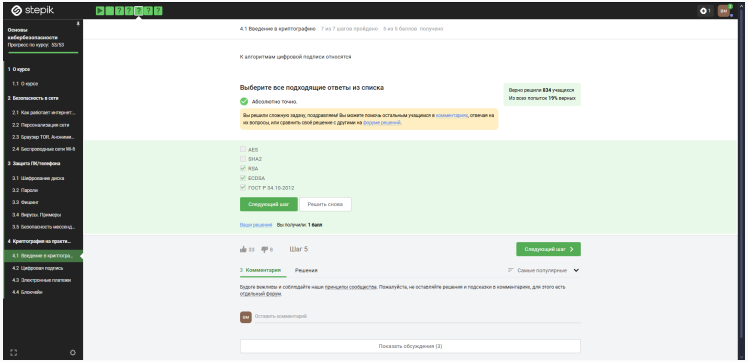


Рис. 3: Вопрос 4.1.3

Аутентификация подтверждает целостность и источник данных:

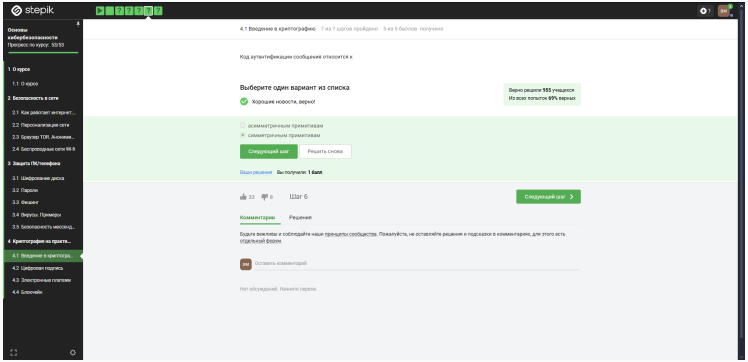


Рис. 4: Вопрос 4.1.4

Обмен ключами Диффи–Хэллмана

Определение и принцип работы обмена ключами:

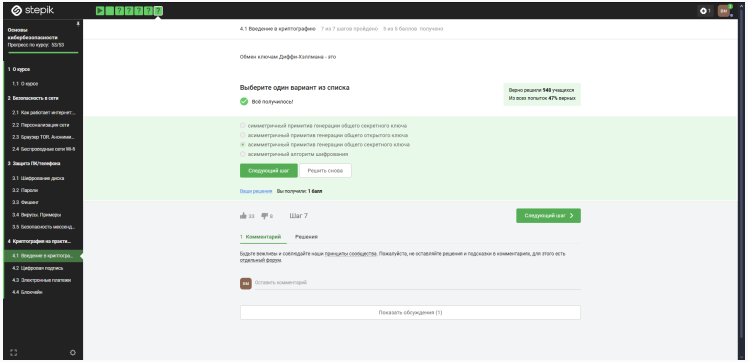


Рис. 5: Вопрос 4.1.5

Цифровая подпись

Протокол ЭЦП относится к протоколам с публичным ключом:

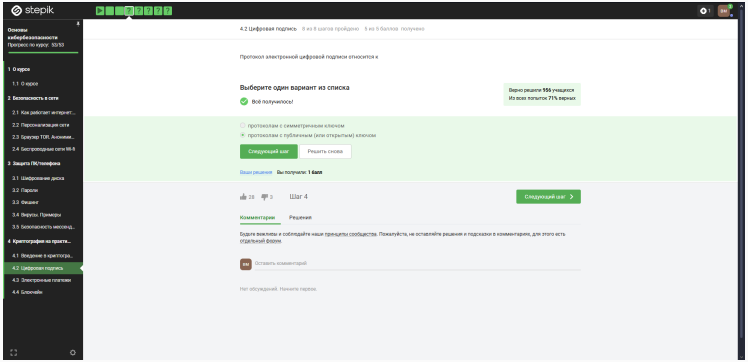
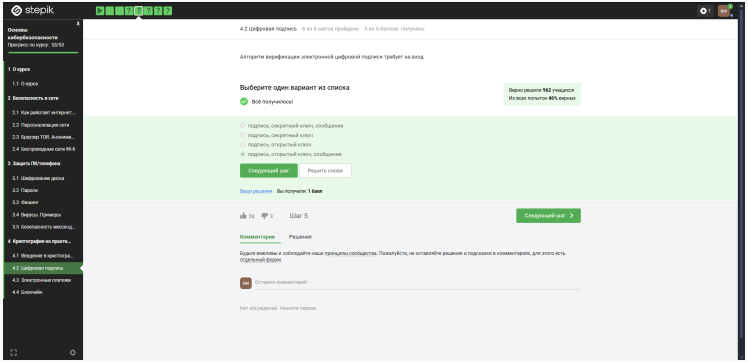


Рис. 6: Вопрос 4.2.1

Верификация ЭЦП

Алгоритм верификации:

1. Хэширование документа
2. Расшифровка подписи
3. Сравнение хэшей



Свойства ЭЦП

ЭЦП обеспечивает целостность, авторство, но не конфиденциальность:

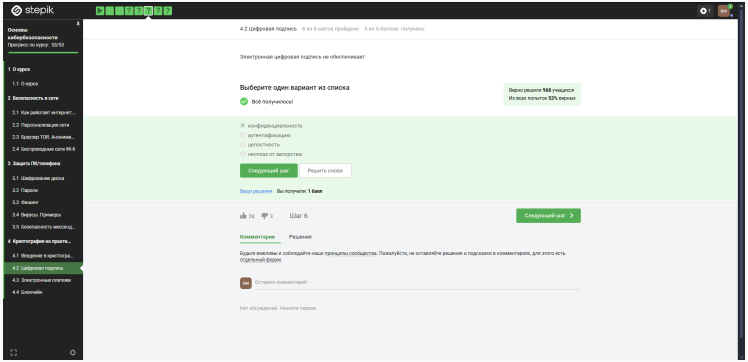


Рис. 8: Вопрос 4.2.3

Для отправки отчётности в ФНС используется усиленная квалифицированная ЭЦП:

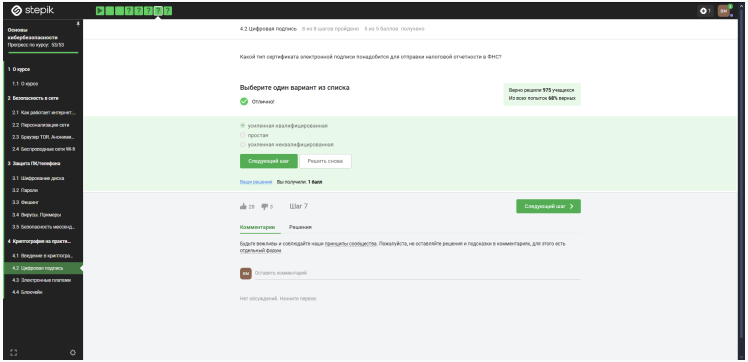


Рис. 9: Вопрос 4.2.4

Выбран верный ответ на тему ЭЦП:

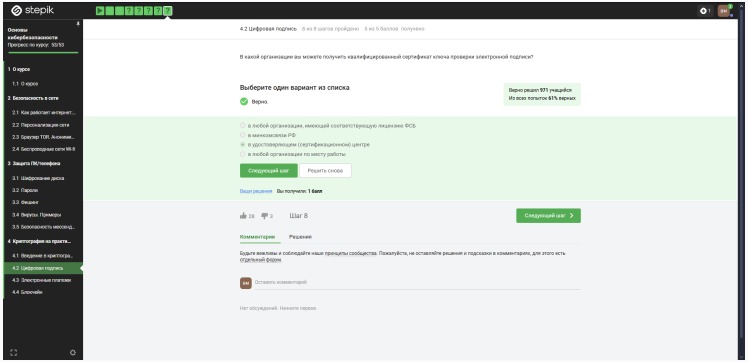


Рис. 10: Вопрос 4.2.5

Электронные платежи

Примеры платёжных систем: Visa, MasterCard, МИР:

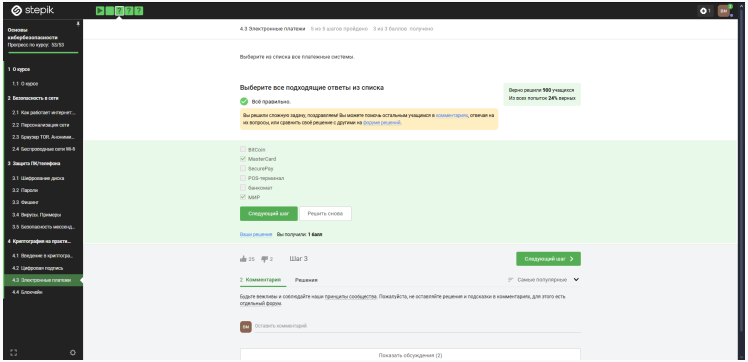


Рис. 11: Вопрос 4.3.1

Верный ответ по платёжным системам:

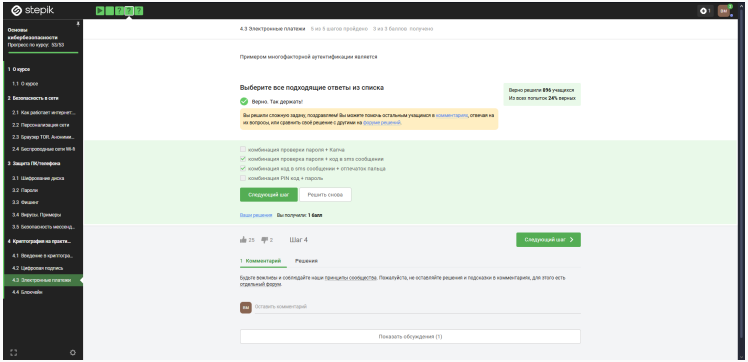


Рис. 12: Вопрос 4.3.2

Многофакторная аутентификация

Применяется при онлайн-платежах для защиты пользователя:

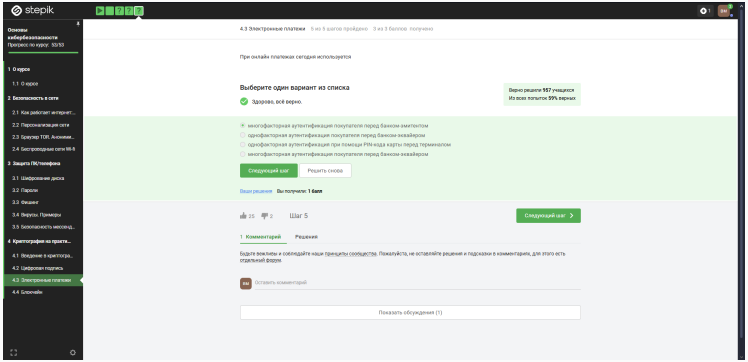


Рис. 13: Вопрос 4.3.3

Блокчейн

PoW — алгоритм консенсуса, обеспечивающий подтверждение транзакций:

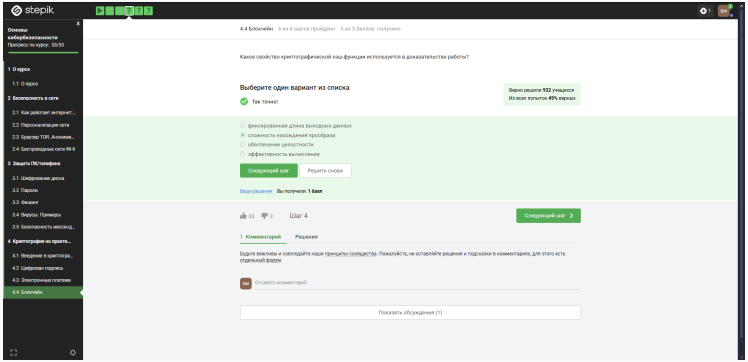


Рис. 14: Вопрос 4.4.1

Консенсус — соглашение между участниками сети о состоянии данных:

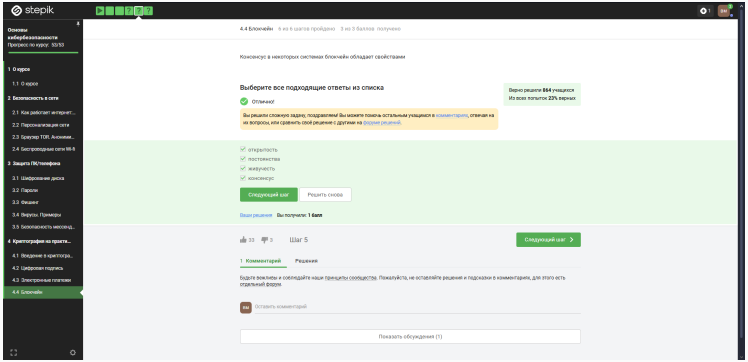


Рис. 15: Вопрос 4.4.2

Контрольный вопрос

Правильный ответ: используется цифровая подпись:

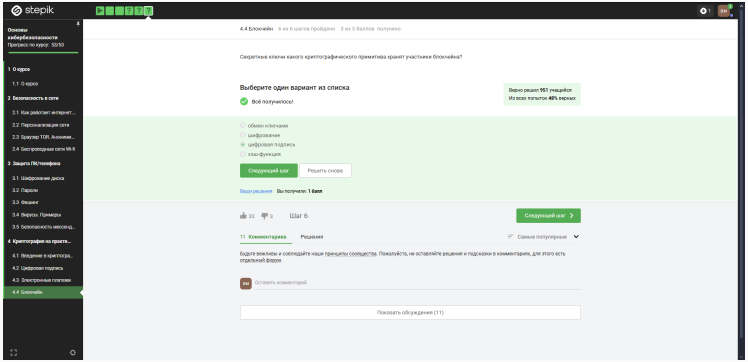


Рис. 16: Вопрос 4.4.3

Выводы

Выводы

- Изучены основы криптографии и цифровой подписи
- Поняты принципы работы с ЭЦП и блокчейном
- Освоены базовые методы защиты информации

Блок 3 пройден. Внешний курс завершён.