Внешний курс. Этап 3

Основы информационной безопасности

Симонова Полина Игоревна

2026-02-15

Содержание I

Раздел 1

1. Информация

1.1 Докладчик

Симонова Полина Игоревна; студент группы НКАбд-02-24

Раздел 2

2. Элементы презентации

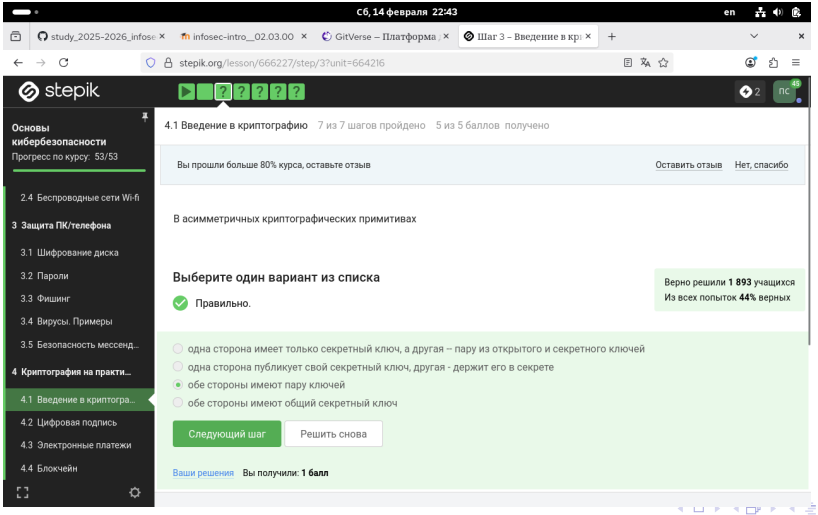
2.1 Цели и задачи

Пройти внешний курс «Основы кибербезопасности» на платформе Stepik. Получить начальные знания в сфере кибербезопасности. Пройти все обучающие материалы, на их основе выполнить задания и тесты.

Раздел 3

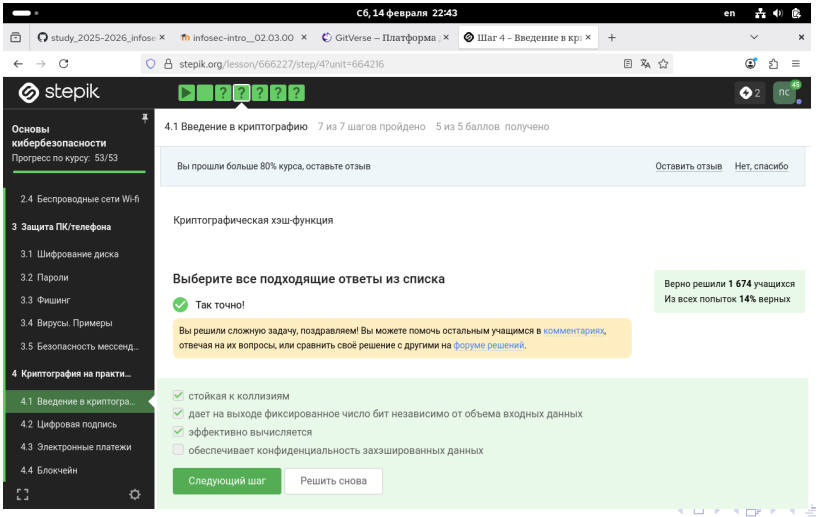
3. Выполнение внешнего курса

Из определения асимметричного шифрования с двумя ключами. (рис. 1)

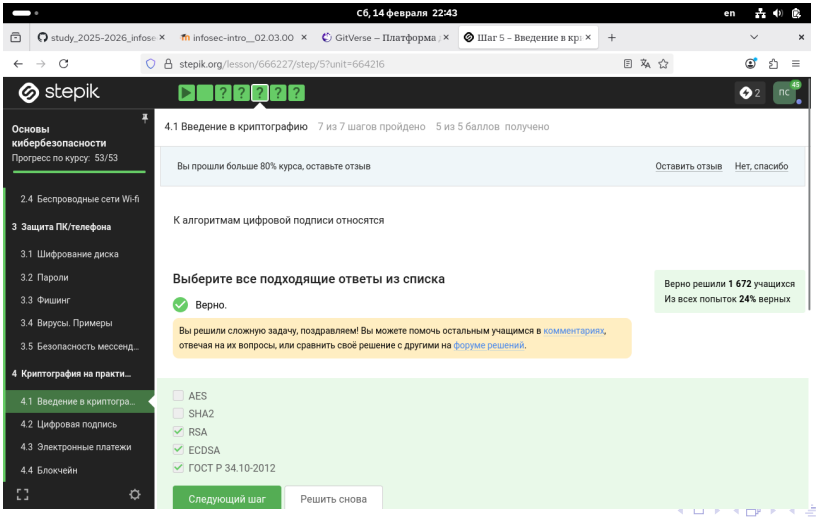


3.2 2

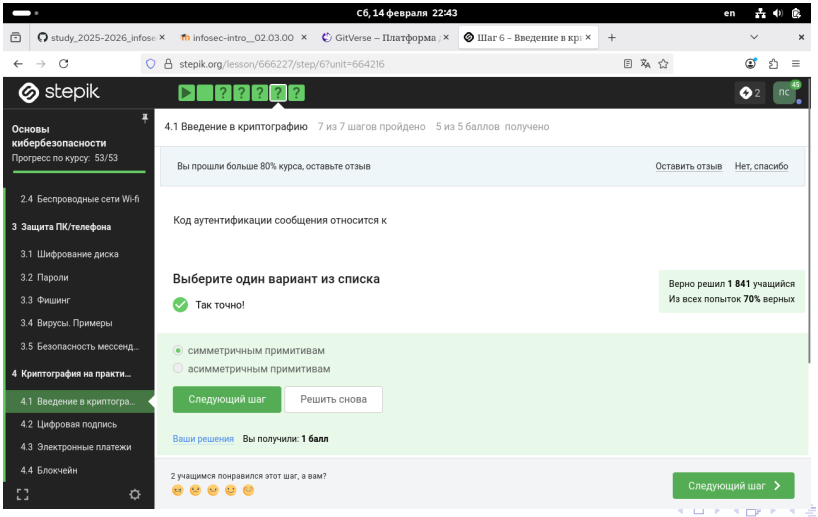
Подходят все ответы кром еобеспечния конфиденциальности. (рис.2)



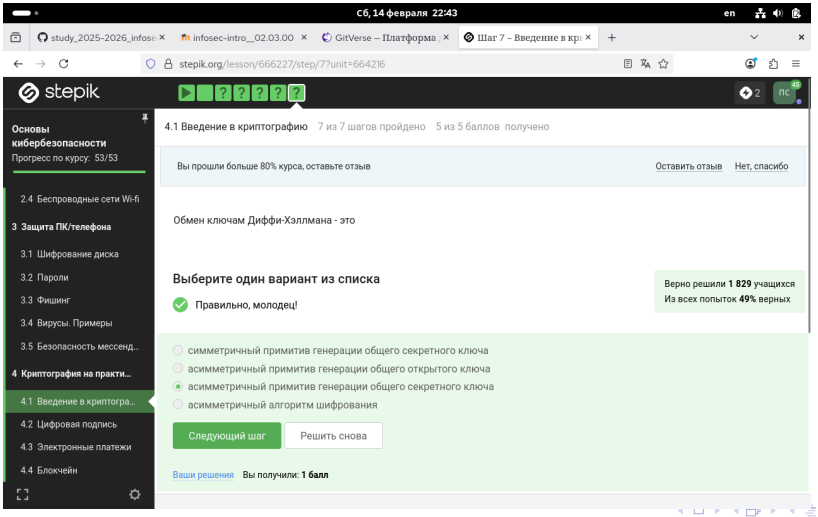
Я отметила все подходящие варианты.(рис.3)



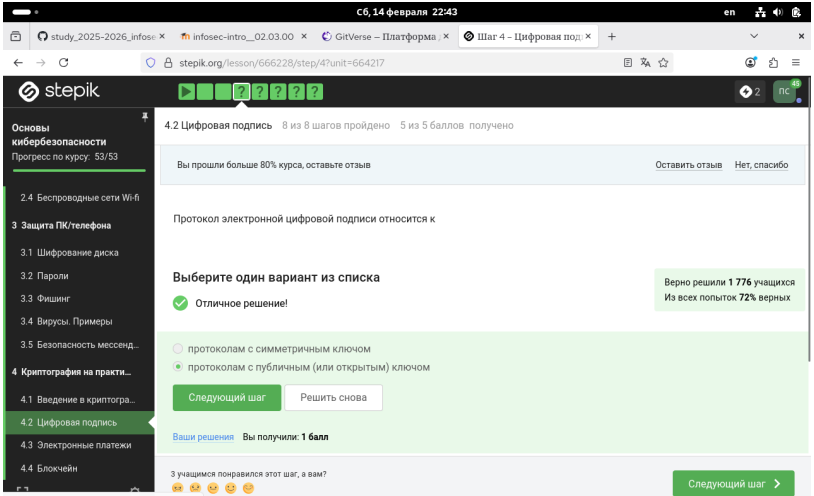
Отметила верный вариант. (рис.4)



Я выбрала вариант, который подходит по определению. (рис. 5)

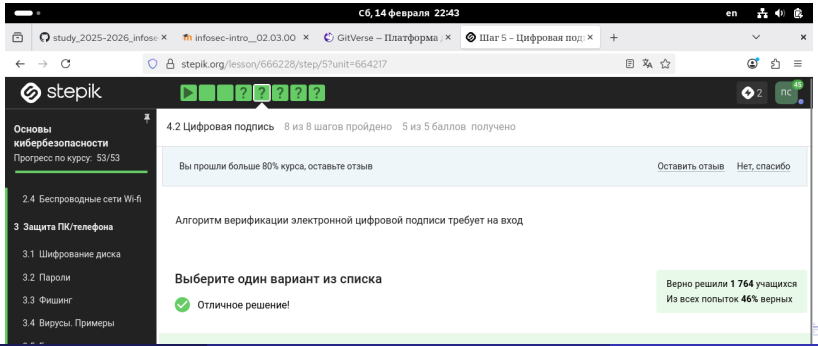


Протокол ЭЦП относится к протоколам с публичным ключом. (рис.6)



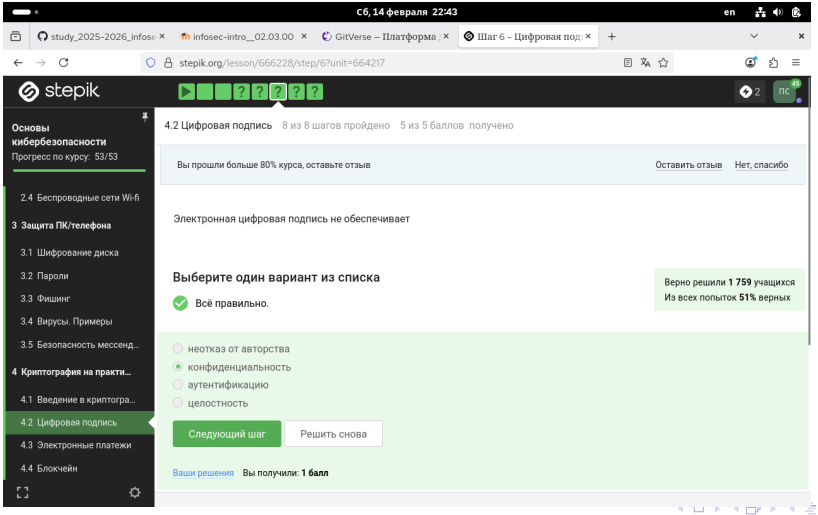
3.7 7

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, содержащейся 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)

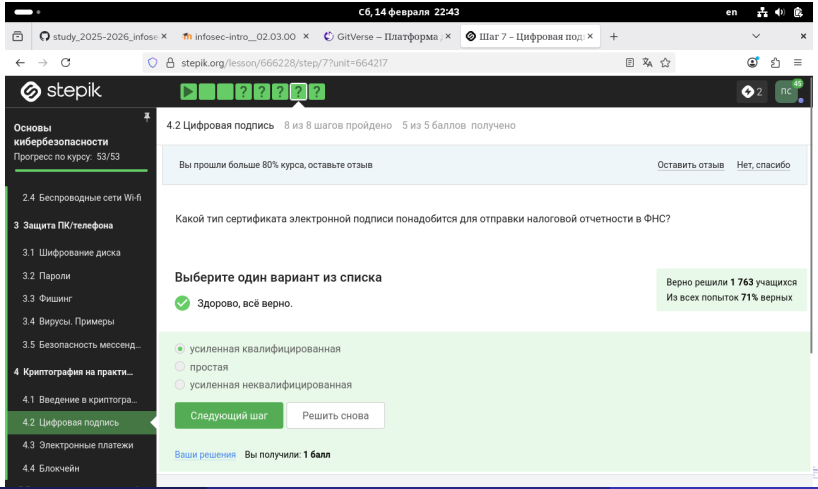


3.8 8

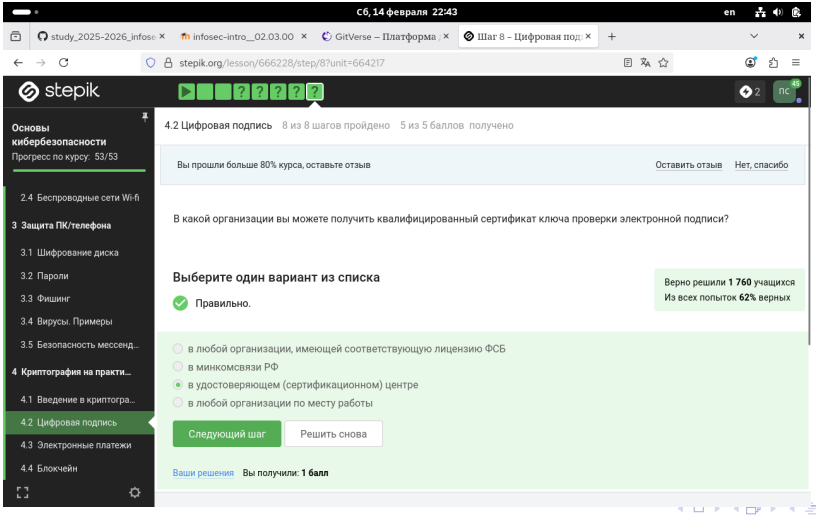
Электронная подпись обеспечивает все указанное, кроме конфиденциальности. (рис.8)



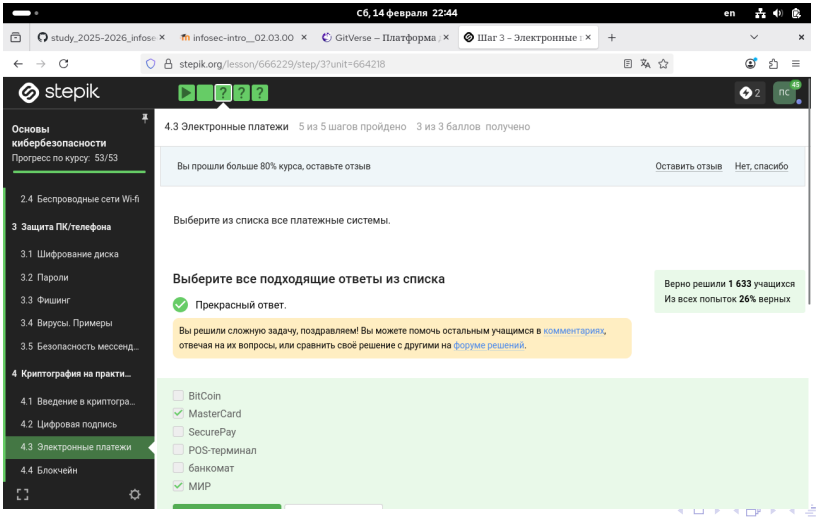
Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись. (рис.9)



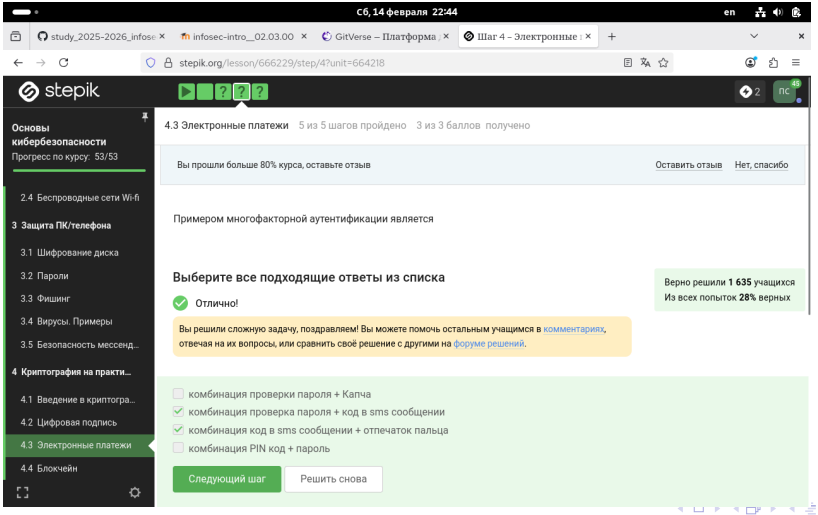
Верный ответ укзаан на изображении. (рис. 10)



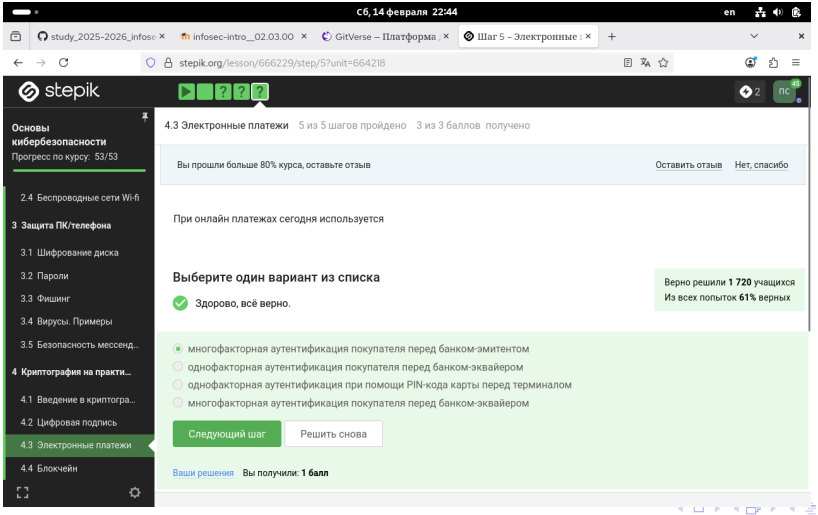
Известные платежные системы - МИР и мастеркард. (рис. 11)



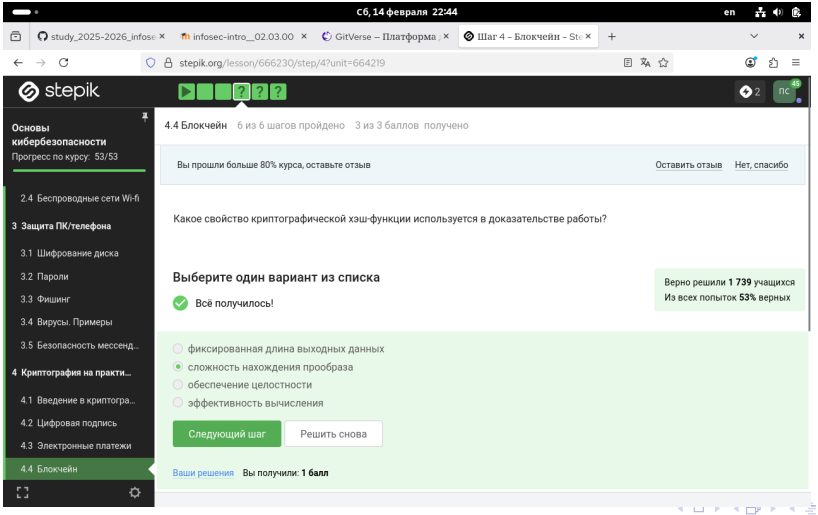
Верный ответ указан на изображении. (рис 12)



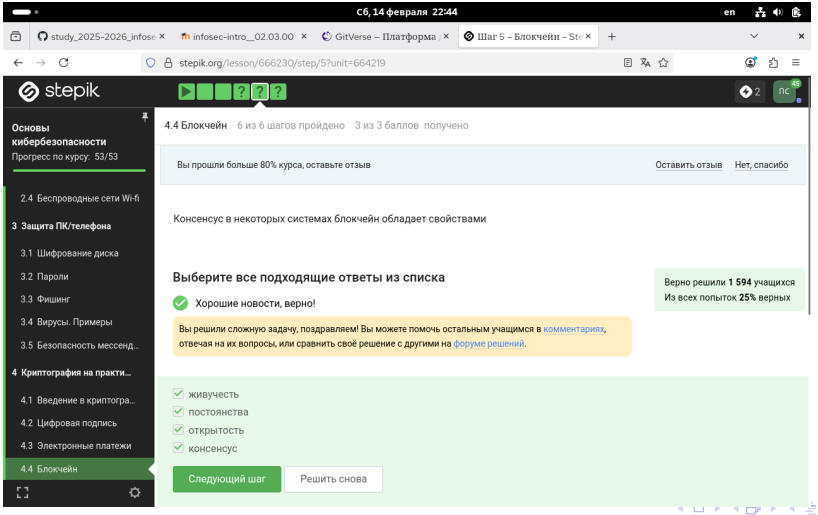
При онлайн платежах используется многофакторная аутентификация. (рис. 13)



Верный ответ указан на изображении. (рис. 14)

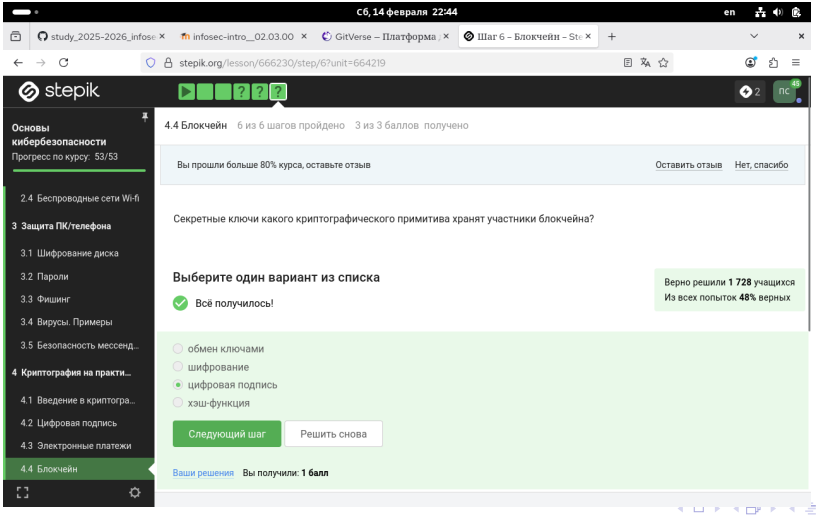


Верный ответ указан на изображении. (рис. 15)



3.16 16

Верный ответ указан на изображении



Раздел 4

4. Выводы

4. Выводы

Я прошла третий этап внешнего курса, узнала о блокчейне, цифровой подписи и о электронных платежах.