

Внешний курс. Этап 3

Основы информационной безопасности

Симонова Полина Игоревна

2026-02-15

Содержание I

1. Информация
2. Элементы презентации
3. Выполнение внешнего курса
4. Выводы

Раздел 1

1. Информация

1.1 Докладчик

Симонова Полина Игоревна; студент группы НКАбд-02-24

Раздел 2

2. Элементы презентации

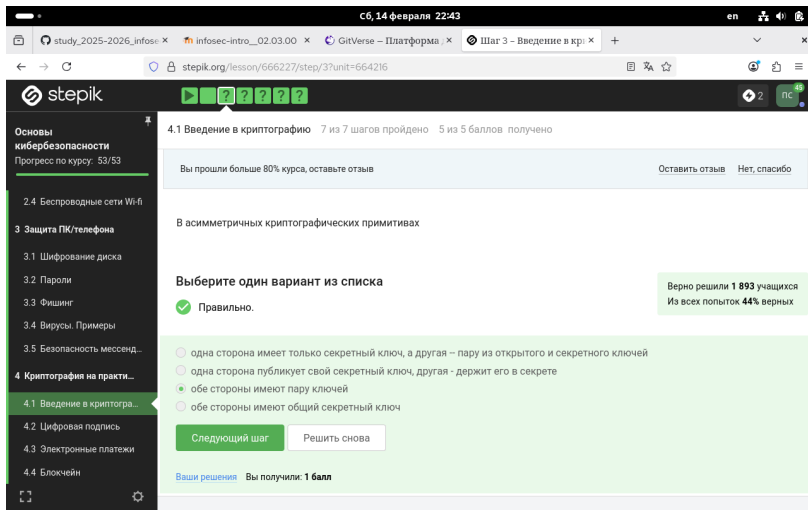
2.1 Цели и задачи

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)



Подходят все ответы кроме обеспечения конфиденциальности. (рис.2)

Сб, 14 февраля 22:43

study_2025-2026_infosec x infosec-intro__02.03.00 x GitVerse – Платформа x Шаг 4 – Введение в кр x

stepik.org/lesson/666227/step/4?unit=664216

stepik

Основы кибербезопасности
Прогресс по курсу: 53/53

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вирусы. Примеры

3.5 Безопасность мессенд...

4 Криптография на практи...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Верно решили 1 674 учащихся
Из всех попыток 14% верных

✓ Так точно!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

✓ стойкая к коллизиям

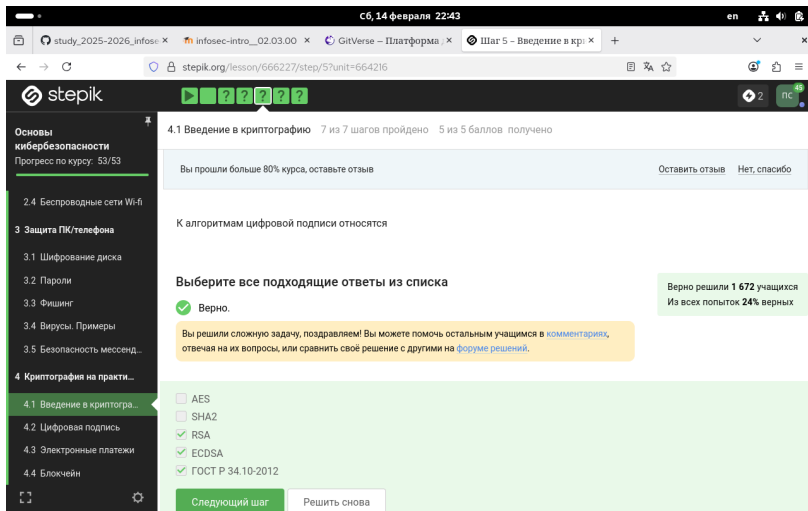
✓ дает на выходе фиксированное число бит независимо от объема входных данных

✓ эффективно вычисляется

☐ обеспечивает конфиденциальность зашифрованных данных

Следующий шаг Решить снова

Я отметила все подходящие варианты.(рис.3)



Отметила верный вариант. (рис.4)

The screenshot shows a web browser window with the Stepik course interface. The browser's address bar displays the URL `stepik.org/lesson/666227/step/6?unit=664216`. The course title is "Основы кибербезопасности" (Basics of Cybersecurity), and the progress is 53/53. The current step is "4.1 Введение в криптографию" (Introduction to Cryptography), which is 7 out of 7 steps completed and 5 out of 5 points received. The question asks to choose one option from the list, and the correct answer is "Так точно!" (Exactly!). The options are "симметричным примитивам" (symmetric primitives) and "асимметричным примитивам" (asymmetric primitives). The interface also shows a "Следующий шаг" (Next step) button and a "Решить снова" (Solve again) button. A feedback section at the bottom asks if the user liked the step, with a "Следующий шаг" button and a "Решить снова" button.

stepik

Основы кибербезопасности
Прогресс по курсу: 53/53

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вирусы. Примеры

3.5 Безопасность мессенд...

4 Криптография на практи...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Код аутентификации сообщения относится к

Выберите один вариант из списка

Верно решил 1 841 учащийся
Из всех попыток 70% верных

Так точно!

симметричным примитивам

асимметричным примитивам

Следующий шаг

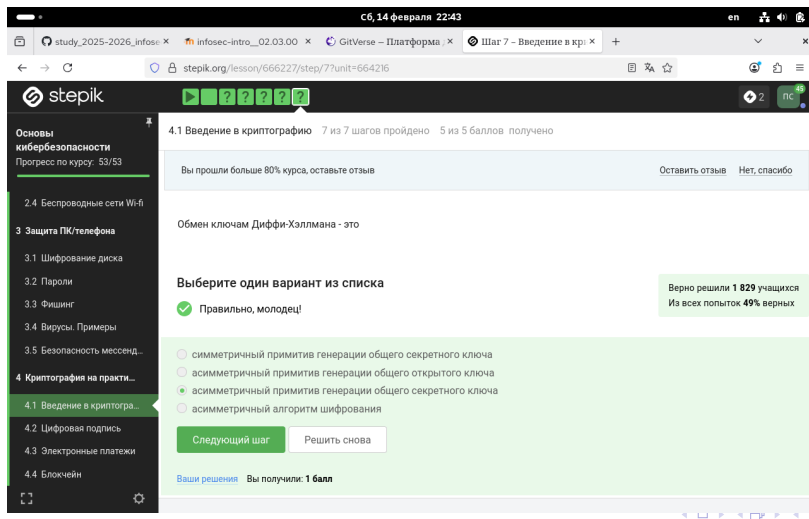
Решить снова

Ваши решения Вы получили: 1 балл

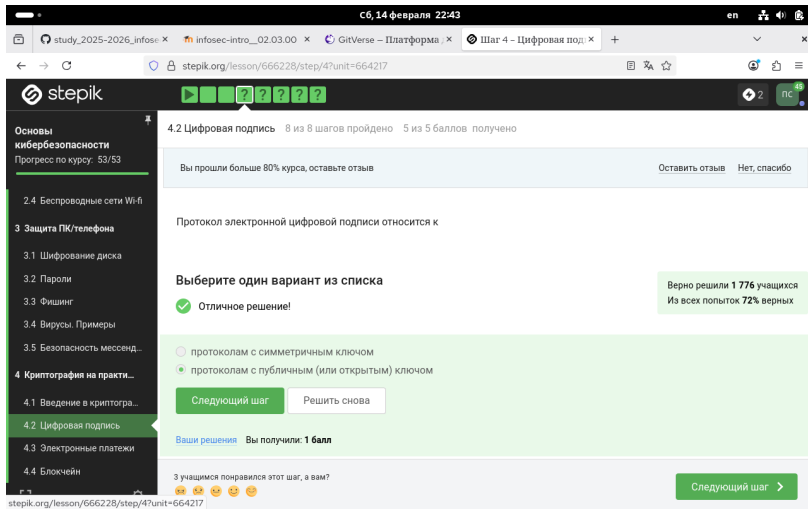
2 учащимся понравился этот шаг, а вам?

Следующий шаг

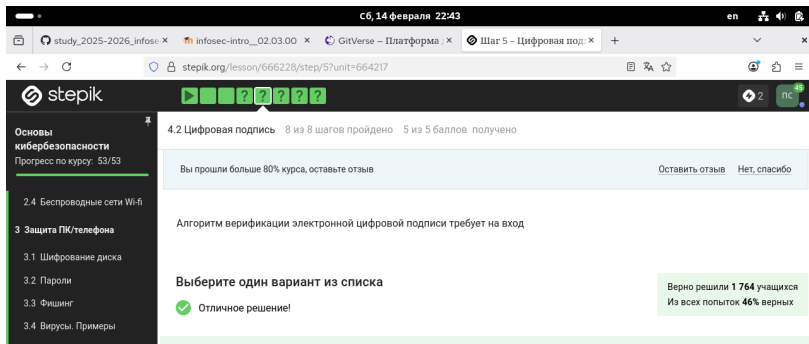
Я выбрала вариант, который подходит по определению. (рис. 5)



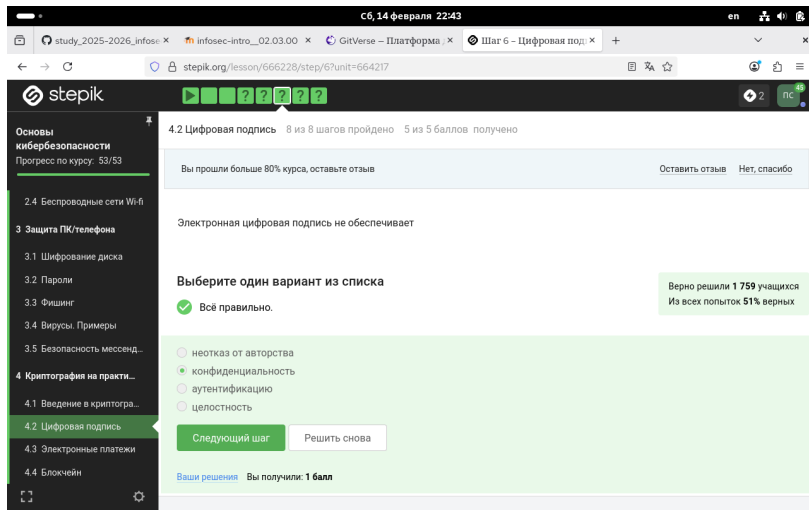
Протокол ЭЦП относится к протоколам с публичным ключом. (рис.6)



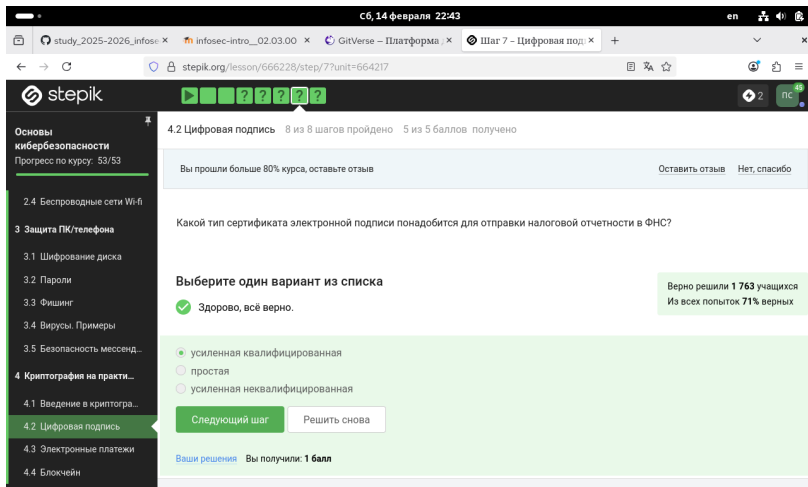
Алгоритм верификации электронной подписи состоит в следующем. На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш- функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства (рис. 7)



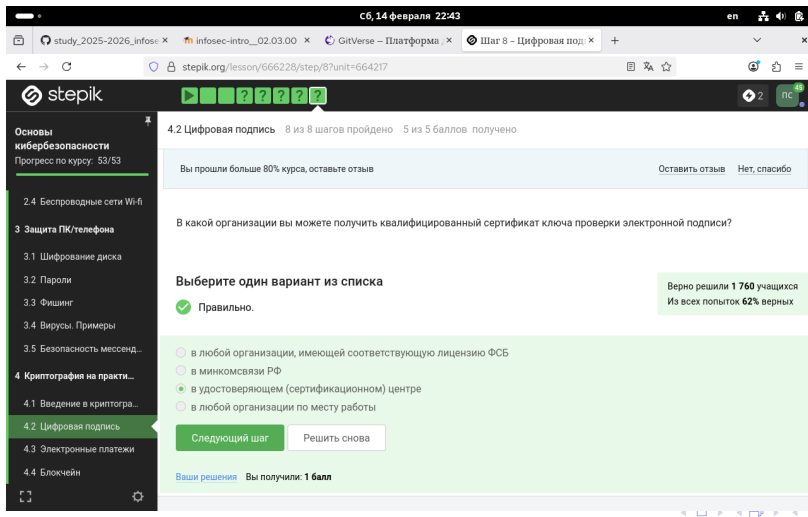
Электронная подпись обеспечивает все указанное, кроме конфиденциальности. (рис.8)



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



Верный ответ указан на изображении. (рис. 10)



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

The screenshot shows a web browser window with the Stepik interface. The course title is 'Основы кибербезопасности' (Basics of Cybersecurity) with a progress of 53/53. The current lesson is '4.3 Электронные платежи' (4.3 Electronic Payments). The quiz question asks to select all payment systems from a list. The correct answers are 'MasterCard' and 'МИР' (Mir), which are marked with green checkmarks. Other options like BitCoin, SecurePay, POS-терминал, and банкомат are unchecked. A feedback message states that 1,633 users got it right, with 26% of attempts being correct. A yellow box encourages users to leave comments or compare answers on the forum.

stepik

Сб, 14 февраля 22:44

study_2025-2026_infosec x infosec-intro_02.03.00 x GitVerse – Платформа x Шар 3 – Электронные : x

stepik.org/lesson/666229/step/3?unit=664218

Основы кибербезопасности
Прогресс по курсу: 53/53

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вирусы. Примеры

3.5 Безопасность мессенд...

4 Криптография на практи...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Верно решили 1 633 учащихся
Из всех попыток 26% верных

✓ Прекрасный ответ.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений.

☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР

Верный ответ указан на изображении. (рис 12)

Сб, 14 февраля 22:44 en

study_2025-2026_infosec x infosec-intro_02.03.00 x GitVerse – Платформа x Шаг 4 – Электронные платежи x

stepik.org/lesson/666229/step/4?unit=664218

stepik

Основы кибербезопасности
Прогресс по курсу: 53/53

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вирусы. Примеры

3.5 Безопасность мессенджеров

4 Криптография на практике

4.1 Введение в криптографию

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

Верно решили 1 635 учащихся
Из всех попыток 28% верных

Отлично!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений.

☐ комбинация проверки пароля + Капча

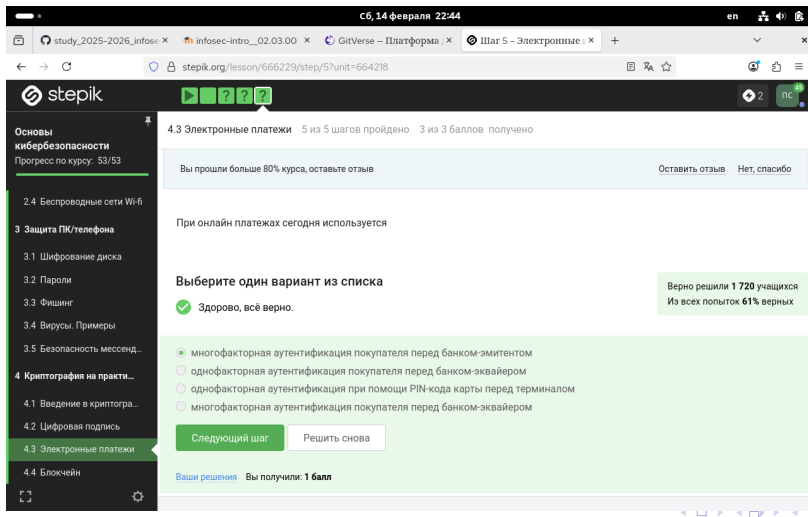
☒ комбинация проверка пароля + код в sms сообщении

☒ комбинация код в sms сообщении + отпечаток пальца

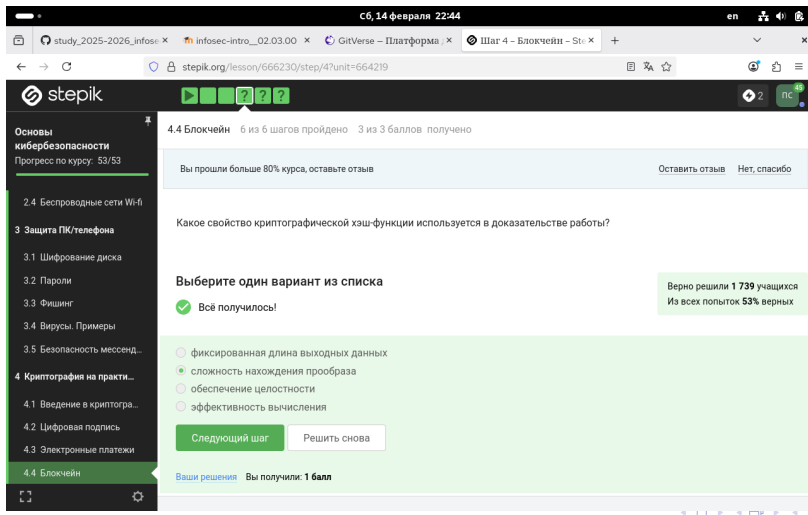
☐ комбинация PIN код + пароль

Следующий шаг Решить снова

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



Верный ответ указан на изображении. (рис. 14)



Верный ответ указан на изображении. (рис. 15)

stepik

С6, 14 февраля 22:44 en

study_2025-2026_infosec x infosec-intro_02.03.00 x GitVerse – Платформа x Шар 5 – Блокчейн – Ste x

stepik.org/lesson/666230/step/5?unit=664219

Основы кибербезопасности
Прогресс по курсу: 53/53

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вирусы. Примеры

3.5 Безопасность мессенд...

4 Криптография на практи...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Верно решили 1 594 учащихся
Из всех попыток 25% верных

✓ Хорошие новости, верно!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

✓ живучесть
✓ постоянства
✓ открытость
✓ консенсус

Следующий шаг Решить снова

Верный ответ указан на изображении

С6, 14 февраля 22:44

study_2025-2026_infosec x infosec-intro_02.03.00 x GitVerse – Платформа x Шаг 6 – Блокчейн – Ste x

stepik.org/lesson/666230/step/6?unit=664219

stepik

Основы кибербезопасности
Прогресс по курсу: 53/53

2.4 Беспроводные сети Wi-Fi

3 Защита ПК/телефона

3.1 Шифрование диска

3.2 Пароли

3.3 Фишинг

3.4 Вирусы. Примеры

3.5 Безопасность мессенд...

4 Криптография на практи...

4.1 Введение в криптогра...

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 1 728 учащихся
Из всех попыток 48% верных

☐ обмен ключами

☐ шифрование

☒ цифровая подпись

☐ хэш-функция

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Раздел 4

4. Выводы

4. Выводы

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