

Внешний курс. Этап 3

Основы информационной безопасности

Симонова Полина Игоревна

2026-02-15

Содержание I

1 1. Информация

2 2. Элементы презентации

3 3. Выполнение внешнего курса

4 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

3.1 1

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

The screenshot shows a web browser window with the URL stepik.org/lesson/666227/step/3?unit=664216. The page title is "Шаг 3 – Введение в криптографию". The main content area displays a question: "В асимметричных криптографических примитивах". Below it, a green box contains the instruction "Выберите один вариант из списка". A green checkmark next to the first option indicates it is correct: "Правильно.". The correct answer is: "одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей". Other options listed are: "одна сторона публикует свой секретный ключ, другая - держит его в секрете", "обе стороны имеют пару ключей", and "обе стороны имеют общий секретный ключ". At the bottom of the green box, there are two buttons: "Следующий шаг" and "Решить снова". A green bar at the very bottom of the page says "Ваши решения Вы получили: 1 балл". The browser's address bar shows other tabs like "study_2025-2026_infosec", "infosec-intro_02.03.00", "GitVerse – Платформа", and "Шаг 3 – Введение в криптографию". The left sidebar lists course modules: "Основы кибербезопасности" (Progress: 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" (current step), "4.2 Цифровая подпись", "4.3 Электронные платежи", and "4.4 Блокчейн".

3.2 2

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

The screenshot shows a browser window with the URL stepik.org/lesson/666227/step/4?unit=664216. The title of the lesson is "4.1 Введение в криптографию". The task description is "Криптографическая хэш-функция". The question asks to select all correct answers from a list. One option is checked with a green checkmark: "стойкая к коллизиям" (resistant to collisions). Other options are also listed but are not checked.

Сб, 14 февраля 22:43

en

study_2025-2026_infosec x infosec-intro_02.03.00 x GitVerse – Платформа x Шаг 4 – Введение в крипто x

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

2 nc 48

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 практике...

4.1 Введение в криптографию...

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

Так точно!

Верно решили 1 674 учащихся
Из всех попыток 14% верных

стойкая к коллизиям

дает на выходе фиксированное число бит независимо от объема входных данных

эффективно вычисляется

обеспечивает конфиденциальность захваченных данных

Следующий шаг Решить снова

стойкая к коллизиям

дает на выходе фиксированное число бит независимо от объема входных данных

эффективно вычисляется

обеспечивает конфиденциальность захваченных данных

Следующий шаг Решить снова

3.3 3

Я отметила все подходящие варианты.(рис.3)

The screenshot shows a browser window with several tabs open at the top. The main content is a Stepik course page for '4.1 Введение в криптографию'. On the left, a sidebar lists course sections: 'Основы кибербезопасности' (Progress: 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...' (highlighted in green), '4.2 Цифровая подпись', '4.3 Электронные платежи', and '4.4 Блокчейн'. The main area displays a task titled 'Выберите все подходящие ответы из списка' (Select all correct answers from the list). It asks: 'К алгоритмам цифровой подписи относятся'. Below is a list of options: AES (unchecked), SHA2 (unchecked), RSA (checked), ECDSA (checked), and ГОСТ Р 34.10-2012 (checked). A green box indicates 'Верно.' (Correct). To the right, a green bar shows statistics: 'Верно решили 1 672 учащихся' (1 672 students solved correctly) and 'Из всех попыток 24% верных' (24% of attempts were correct). At the bottom, there are buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again).

3.4 4

Отметила верный вариант. (рис.4)

The screenshot shows a web browser window with the URL stepik.org/lesson/666227/step/6?unit=664216. The page title is "Шаг 6 – Введение в криптографию". The main content area displays a step titled "4.1 Введение в криптографию" with the message "7 из 7 шагов пройдено" and "5 из 5 баллов получено". A message encourages users to leave a review if they have completed more than 80% of the course. Below this, a question asks: "Код аутентификации сообщения относится к". A green checkmark next to the answer "Так точно!" indicates it is correct. A green box on the right states "Верно решил 1 841 учащийся Из всех попыток 70% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". The sidebar on the left lists other steps in the section, such as "Беспроводные сети Wi-fi" and "Защита ПК/телефона". The top navigation bar shows tabs for "study_2025-2026_infosec", "infosec-intro_02.03.00", "GitVerse – Платформа", and the current step.

3.5 5

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

The screenshot shows a browser window with several tabs open at the top, including 'study_2025-2026_infosec' and 'Шаг 7 - Введение в криптографию'. The main content area is from the 'stepik.org' website, displaying a course titled 'Основы кибербезопасности' with a progress bar showing 53/53 completed. A sidebar on the left lists various chapters and sub-chapters. The current chapter, '4.1 Введение в криптографию', is highlighted with a green bar. A specific task is shown: 'Обмен ключам Диффи-Хеллмана - это'. Below it, a message says 'Вы выбрали один вариант из списка' followed by a green checkmark and the text 'Правильно, молодец!'. To the right, a green box displays statistics: 'Верно решили 1 829 учащихся' and 'Из всех попыток 49% верных'. At the bottom, there are buttons for 'Следующий шаг' and 'Решить снова'. The status bar at the bottom of the browser window shows the date 'сб, 14 февраля 22:43' and the time 'en'.

3.6 6

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

The screenshot shows a web browser window with the URL stepik.org/lesson/666228/step/4?unit=664217. The page title is "4.2 Цифровая подпись". The sidebar on the left lists course modules: "Основы кибербезопасности" (Progress: 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" (highlighted in green), "4.3 Электронные платежи", and "4.4 Блокчейн". The main content area displays a question: "Протокол электронной цифровой подписи относится к". Below it is a list of two options: "протоколам с симметричным ключом" (radio button) and "протоколам с публичным (или открытым) ключом" (radio button, selected). A green message box indicates "Отличное решение!" and "Верно решили 1 776 учащихся Из всех попыток 72% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". The status bar at the bottom shows "study_2025-2026_infosec" and "infosec-intro_02.03.00".

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)

The screenshot shows a web browser window with the URL stepik.org/lesson/666228/step/5?unit=664217. The page title is "4.2 Цифровая подпись". The main content area displays a task: "Вы прошли больше 80% курса, оставьте отзыв" and "Оставить отзыв Нет, спасибо". Below this, a note says: "Алгоритм верификации электронной цифровой подписи требует на вход". A question asks: "Выберите один вариант из списка". A green checkmark indicates: "Отличное решение!". A green box at the bottom right states: "Верно решили 1 764 учащихся Из всех попыток 46% верных". The browser's address bar shows tabs for "study_2025-2026_infosec", "infosec_intro_02.03.00", "GitVerse – Платформа", and "Шаг 5 – Цифровая подпись". The top right of the browser window shows the date "Сб, 14 февраля 22:43" and the time "en".

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

The screenshot shows a web browser window on a Stepik.org course page. The title bar indicates the date as Сб, 14 февраля 22:43. The address bar shows the URL stepik.org/lesson/666228/step/6?unit=664217. The main content area displays a step titled "4.2 Цифровая подпись" with the status "8 из 8 шагов пройдено" and "5 из 5 баллов получено". A message encourages users to leave a review: "Вы прошли больше 80% курса, оставьте отзыв". Below this, a statement says "Электронная цифровая подпись не обеспечивает". A question asks "Выберите один вариант из списка" with the correct answer being "Всё правильно". A green box on the right shows statistics: "Верно решили 1 759 учащихся Из всех попыток 51% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". The sidebar on the left lists other steps in the unit, including "4.2 Цифровая подпись" (which is highlighted in green), "4.3 Электронные платежи", and "4.4 Блокчейн". The overall theme is cybersecurity.

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

The screenshot shows a computer interface with a browser window open to a Stepik course page. The browser tabs include 'study_2025-2026_infosec', 'infosec_intro_02.03.00', 'GitVerse – Платформа...', and 'Шаг 7 – Цифровая под...'. The main content area displays a Stepik lesson titled '4.2 Цифровая подпись'. The progress bar indicates '8 из 8 шагов пройдено' and '5 из 5 баллов получено'. A message at the top right says 'Вы прошли больше 80% курса, оставьте отзыв' with buttons for 'Оставить отзыв' and 'Нет, спасибо'. Below this, a question asks: 'Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?'. A green box contains the instruction 'Выберите один вариант из списка'. A correct answer is highlighted with a green checkmark and the text 'Здорово, всё верно.' To the right, a green box states 'Верно решили 1 763 учащихся Из всех попыток 71% верных'. At the bottom, there are two buttons: 'Следующий шаг' and 'Решить снова'. The sidebar on the left lists other course sections: 'Основы кибербезопасности' (Progress: 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' (highlighted in green), '4.3 Электронные платежи', and '4.4 Блокчейн'.

3.10 10

Верный ответ указан на изображении. (рис. 10)

The screenshot shows a browser window with the URL stepik.org/lesson/666228/step/8?unit=664217. The page title is "4.2 Цифровая подпись". The progress bar shows 8 из 8 шагов пройдено. A message at the top right says "Оставьте отзыв Нет, спасибо". Below it, a question asks: "В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?". A green box indicates the correct answer was selected: "Правильно". The correct answer is "в удостоверяющем (сертификационном) центре". A green box also states "Верно решили 1 760 учащихся Из всех попыток 62% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". The sidebar on the left lists other steps: 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 (the current step), 4.3 Электронные платежи, 4.4 Блокчейн.

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

The screenshot shows a browser window with the following details:

- Title Bar:** Сб, 14 февраля 22:44, study_2025-2026_infosec, infosec-intro_02.03.00, GitVerse – Платформа, Шаг 3 – Электронные...
- Tab:** stepik.org/lesson/666229/step/3?unit=664218
- Stepik Header:** stepik.org, 2 notifications, nc 48 notifications.
- Left Sidebar (Course Structure):**
 - Основы кибербезопасности (Progress: 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** (Currently selected)
 - 4.4 Блокчейн
- Content Area:**

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

Прекрасный ответ.

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

Верно решили 1 633 учащихся
Из всех попыток 26% верных

BitCoin
 MasterCard
 SecurePay
 POS-терминал
 банкомат
 МИР

3.12 12

Верный ответ указан на изображении. (рис 12)

The screenshot shows a web browser window with the URL stepik.org/lesson/666229/step/4?unit=664218. The page title is "4.3 Электронные платежи". The sidebar on the left lists course modules: "Основы кибербезопасности" (Progress: 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" (highlighted in green), and "4.4 Блокчейн". The main content area displays a step titled "Примером многофакторной аутентификации является". Below it is a question: "Выберите все подходящие ответы из списка". The correct answer is "комбинация проверка пароля + Капча", indicated by a checked checkbox and the message "Отлично!". A green box on the right states "Верно решили 1 635 учащихся Из всех попыток 28% верных". At the bottom are buttons for "Следующий шаг" and "Решить снова".

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

The screenshot shows a web browser window with the following details:

- Address bar:** study_2025-2026_infosec_intro_02.03.00 - GitVerse – Платформа | Шаг 5 – Электронные ...
stepik.org/lesson/666229/step/5?unit=664218
- Page title:** 4.3 Электронные платежи
- Progress:** 5 из 5 шагов пройдено | 3 из 3 баллов получено
- Left sidebar (Course Structure):**
 - 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
- Main Content Area:**

Вы прошли больше 80% курса, оставьте отзыв

Оставить отзыв | Нет, спасибо

При онлайн платежах сегодня используется

Выберите один вариант из списка

Здорово, всё верно.

Верно решили 1 720 учащихся
Из всех попыток 61% верных

многофакторная аутентификация покупателя перед банком-эмитентом

однофакторная аутентификация покупателя перед банком-эквайером

однофакторная аутентификация при помощи PIN-кода карты перед терминалом

многофакторная аутентификация покупателя перед банком-эквайером

Buttons: Следующий шаг | Решить снова

Bottom Status Bar: Ваши решения | Вы получили: 1 балл

3.14 14

Верный ответ указан на изображении. (рис. 14)

The screenshot shows a browser window with the URL stepik.org/lesson/666230/step/4?unit=664219. The title of the page is "4.4 Блокчейн". The progress bar indicates "6 из 6 шагов пройдено" and "3 из 3 баллов получено". A message says "Вы прошли больше 80% курса, оставьте отзыв". There are two buttons: "Оставить отзыв" and "Нет, спасибо". Below this, a question asks: "Какое свойство криптографической хэш-функции используется в доказательстве работы?". The correct answer is selected: "Всё получилось!". A green box on the right says "Верно решили 1 739 учащихся Из всех попыток 53% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". The status bar at the bottom of the page shows "Ваши решения Вы получили: 1 балл".

3.15 15

Верный ответ указан на изображении. (рис. 15)

The screenshot shows a browser window with several tabs open at the top. The main content is a Stepik.org course page for a lesson titled '4.4 Блокчейн'. The sidebar on the left lists various sections of the course, and the main area displays a task about blockchain properties. The task asks to select all applicable properties from a list. One option, 'консенсус' (consensus), is checked and marked as correct. A green box on the right indicates that 1,594 users solved the task, which is 25% of all attempts. Below the task, there is a message encouraging users to help others by leaving comments or sharing their solutions.

Сб, 14 февраля 22:44

en

study_2025-2026_infosec × infosec-intro_02.03.00 × GitVerse – Платформа × Шаг 5 – Блокчейн – Ste × +

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

2 nc 45

steplk

Основы кибербезопасности
Прогресс по курсу: 53/53

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

Бы прошли больше 80% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

Хорошие новости, верно!

Верно решили 1 594 учащихся
Из всех попыток 25% верных

живучесть
постоянства
открытость
консенсус

Следующий шаг Решить снова

Симонова Полина Игоревна

Внешний курс. Этап 3

2026-02-15

22 / 25

3.16 16

Верный ответ указан на изображении

The screenshot shows a browser window with the URL stepik.org/lesson/666230/step/6?unit=664219. The title of the step is "4.4 Блокчейн". The progress bar indicates "6 из 6 шагов пройдено" and "3 из 3 баллов получено". A message encourages users to leave a review: "Вы прошли больше 80% курса, оставьте отзыв". There are two buttons: "Оставить отзыв" and "Нет, спасибо". The main question asks: "Секретные ключи какого криптографического примитива хранят участники блокчейна?". Below it, a green box says "Всё получилось!". The correct answer is "цифровая подпись". Other options listed are "обмен ключами", "шифрование", and "хэш-функция". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". A summary at the bottom states: "Ваши решения Вы получили: 1 балл". A green box on the right says "Верно решили 1 728 учащихся Из всех попыток 48% верных". The browser interface includes tabs for other courses like "study_2025-2026_infosec" and "infosec_intro_02.03.00", and a sidebar with a navigation menu.

Раздел 4

4. Выводы

4. Выводы

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