

# Внешний курс. Этап 2

## 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

Шифрование диска переводит данные в нечитаемый код, поэтому загрузочный сектор вполне можно зашифровать. (рис. 1)

The screenshot shows a web browser window with the Stepik platform interface. The page is titled '3.1 Шифрование диска' (3.1 Disk Encryption) and indicates that 5 out of 5 steps have been completed, with 3 out of 3 points earned. The main content area asks the question: 'Можно ли зашифровать загрузочный сектор диска' (Can the boot sector of the disk be encrypted?). Below the question, it says 'Выберите один вариант из списка' (Select one option from the list). The options are 'Да' (Yes) and 'Нет' (No). The 'Да' option is selected, and a green checkmark indicates it is the correct answer. A green box on the right states: 'Верно решили 2 193 учащихся. Из всех попыток 89% верных' (2,193 students solved it correctly. 89% of all attempts were correct). At the bottom, there is a 'Следующий шаг' (Next step) button and a feedback section asking '2 учащимся понравился этот шаг, а вам?' (2 students liked this step, do you?). The left sidebar shows the course structure, with '3.1 Шифрование диска' highlighted. The top navigation bar shows the course title 'Шаг 3 – Шифрование' (Step 3 – Encryption).



## Шифрование диска основано на симметричном шифровании. (рис.2)

The screenshot shows a web browser window with the Stepik website. The browser's address bar displays the URL `stepik.org/lesson/666222/step/4?unit=664211`. The page title is "Шаг 4 - Шифрование". The left sidebar shows a course progress bar for "Основы кибербезопасности" (37/53) and a list of topics, with "3.1 Шифрование диска" selected. The main content area shows a quiz question: "3.1 Шифрование диска 5 из 5 шагов пройдено 3 из 3 баллов получено". The question text is "Шифрование диска основано на". Below it, the instruction says "Выберите один вариант из списка". The options are:   
- ☐ хешировании   
- ☒ симметричном шифровании   
- ☐ асимметричном шифровании   
The correct answer is "симметричном шифровании", indicated by a green checkmark and the text "Правильно, молодец!". A green box on the right states: "Верно решили 2 188 учащихся Из всех попыток 67% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова", and a section for "Ваши решения" showing a score of 1 ball.

С6, 14 февраля 21:58

study\_2025-2026\_info x infosec-intro\_\_02.03.00 x GitVerse – Платформ x Шаг 4 - Шифрование x study\_2023\_2024\_info x

stepik.org/lesson/666222/step/4?unit=664211

stepik

Основы кибербезопасности  
Прогресс по курсу: 37/53

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

3.1 Шифрование диска 5 из 5 шагов пройдено 3 из 3 баллов получено

Шифрование диска основано на

Выберите один вариант из списка

✓ Правильно, молодец!

☐ хешировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

Верно решили 2 188 учащихся  
Из всех попыток 67% верных

Ваши решения Вы получили: 1 балл

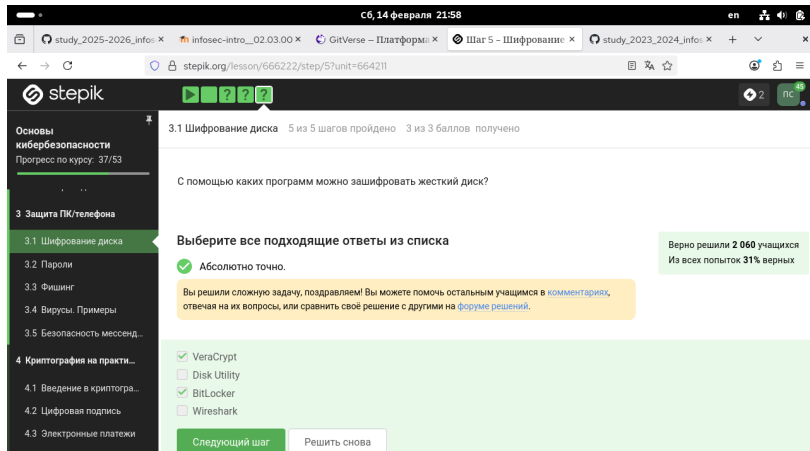
2 учащимся понравился этот шаг, а вам?

😊 😊 😊 😊 😊

Следующий шаг

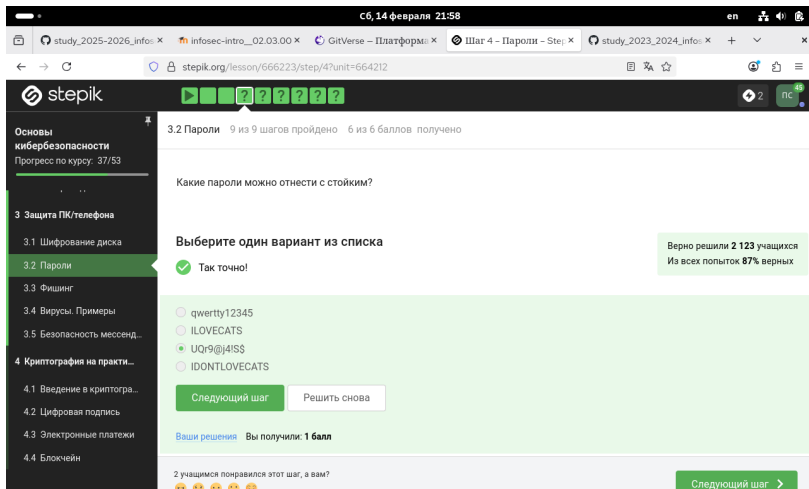
Комментарии Решения

Wireshark используется для анализа трафика, а Disk Utility - приложение для мониторинга памяти на макос. Соответственно, выделяем две оставшиеся программы.(рис.3)

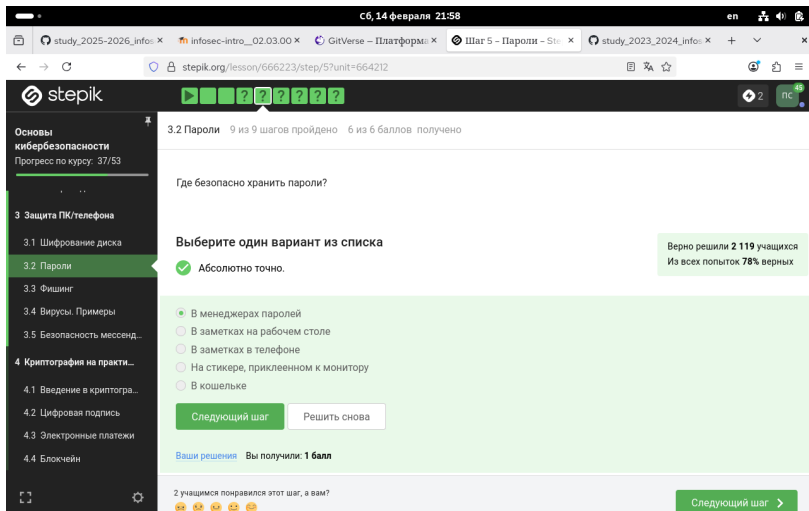


## 3.4 4

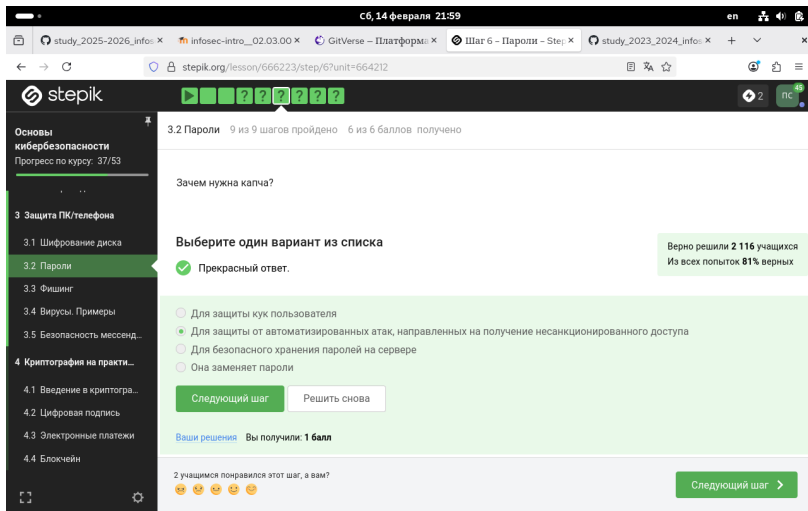
Стойкие пароли длинные, содержат заглавные и строчные символы, специальные символы и цифры. (рис.4)



Все варианты ненавдежные, кроме менеджера паролей. (рис. 5)



Капча проверяет, что действие выполняет человек. (рис.6)



## Хэширование паролей позволяет хранить их не в открытом виде (рис. 7)

The screenshot shows a web browser window with the Stepik course interface. The browser's address bar displays the URL `stepik.org/lesson/666223/step/7?unit=664212`. The page title is "Шаг 7 - Пароли - Stepik". The course progress bar indicates "Основы кибербезопасности" with a progress of 37/53. The current step is "3.2 Пароли", which is highlighted in the left sidebar. The question text is "Для чего применяется хэширование паролей?". The options are: "Для того, чтобы пароль не передавался в открытом виде.", "Для того, чтобы ускорить процесс авторизации", "Для того, чтобы не хранить пароли на сервере в открытом виде.", and "Для удобства разработчиков". The correct answer is "Для того, чтобы не хранить пароли на сервере в открытом виде.", which is marked with a green circle. The "Следующий шаг" button is highlighted. A green box on the right indicates "Верно решили 2 108 учащихся. Из всех попыток 64% верных". At the bottom, there is a feedback section with 2 thumbs up and a "Следующий шаг" button.

stepik

Основы кибербезопасности  
Прогресс по курсу: 37/53

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Правильно.

Верно решили 2 108 учащихся  
Из всех попыток 64% верных

☐ Для того, чтобы пароль не передавался в открытом виде.

☐ Для того, чтобы ускорить процесс авторизации

☒ Для того, чтобы не хранить пароли на сервере в открытом виде.

☐ Для удобства разработчиков

Следующий шаг

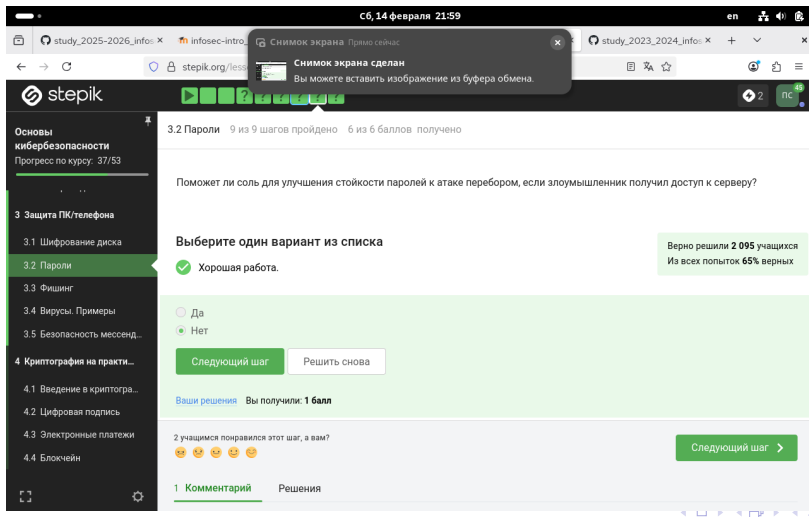
Решить снова

Ваши решения Вы получили: 1 балл

2 учащимся понравился этот шаг, а вам?

Следующий шаг

В случае доступа к серверу, соленные пароли уже не помогут. (рис.8)



Все указанные меры надежно защищают от утечек данных. (рис.9)

The screenshot shows a web browser window with the Stepik course interface. The browser's address bar displays the URL `stepik.org/lesson/666223/step/9?unit=664212`. The page title is "3.2 Пароли" (3.2 Passwords). The progress bar indicates "9 из 9 шагов пройдено" (9 of 9 steps completed) and "6 из 6 баллов получено" (6 of 6 points received). The question is "Какие меры защищают от утечек данных атакой перебором?" (Which measures protect against data leaks by brute force attack?). The instruction is "Выберите все подходящие ответы из списка" (Select all suitable answers from the list). The correct answer is "Здорово, всё верно." (Great, everything is correct.). A green box on the right states "Верно решил 1 981 учащийся" (1 981 students solved correctly) and "Из всех попыток 20% верных" (20% correct of all attempts). The list of options includes: "разные пароли на всех сайтах" (different passwords on all sites), "периодическая смена паролей" (periodic password change), "сложные(=длинные) пароли" (complex(=long) passwords), and "капча" (captcha). The "Следующий шаг" (Next step) button is highlighted. The bottom of the page shows "Ваши решения" (Your solutions) and "Вы получили: 1 балл" (You received: 1 point).

stepik

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Здорово, всё верно.

Верно решил 1 981 учащийся  
Из всех попыток 20% верных

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](#).

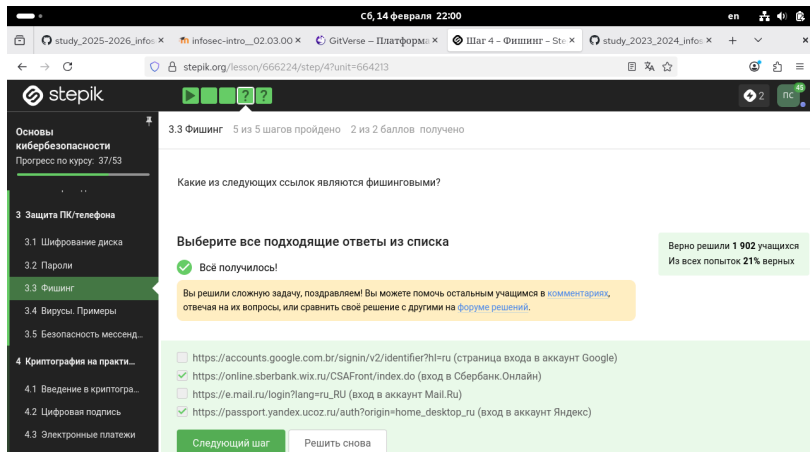
- разные пароли на всех сайтах
- периодическая смена паролей
- сложные(=длинные) пароли
- капча

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл



Фишинговые ссылки часто сделаны на сервисах создания сайтов, например вика или тильда, также фишинговые ссылки очень похожи на ссылки известных сервисов, но имеют небольшие различия, которые легко не заметить. (рис. 10)



Фишинговое письмо может прийти от кого угодно, например если их взломали. (рис. 11)

The screenshot shows a web browser window with the Stepik website. The browser's address bar shows the URL `stepik.org/lesson/666224/step/5?unit=664213`. The page title is "Шаг 5 - Фишинг". The left sidebar shows a course progress for "Основы кибербезопасности" (37/53) and a list of topics. The current topic is "3.3 Фишинг". The main content area displays a question: "Может ли фишинговый email прийти от знакомого адреса?". Below the question, it says "Выберите один вариант из списка". The options are "Да" (selected) and "Нет". A green box indicates "Верно решили 2 048 учащихся" and "Из всех попыток 91% верных". A green button "Следующий шаг" is visible. At the bottom, there is a section for "Ваши решения" showing "Вы получили: 1 балл" and a "Следующий шаг" button.

stepik

3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено

Может ли фишинговый email прийти от знакомого адреса?

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решили 2 048 учащихся  
Из всех попыток 91% верных

☒ Да  
☐ Нет

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

2 учащимся понравился этот шаг, а вам?  
😊 😊 😊 😊 😊

Следующий шаг >

Комментарии Решения

Спуфинг - от английского слова spoof, что значит подменять. (рис 12)

The screenshot shows a web browser window with the Stepik platform interface. The browser's address bar displays the URL `stepik.org/lesson/666225/step/4?unit=664214`. The page title is "3.4 Вирусы. Примеры". The main content area is titled "Email Спуфинг – это" and asks the user to "Выберите один вариант из списка" (Choose one option from the list). The correct answer, "Верно. Так держать!" (Correct. Keep it up!), is highlighted with a green checkmark. Below the question, there are four radio button options: "атака перебором паролей" (password brute-force attack), "подмена адреса отправителя в имейлах" (spoofing sender address in emails), "метод предотвращения фишинга" (phishing prevention method), and "протокол для отправки имейлов" (protocol for sending emails). The second option is selected. At the bottom of the question area, there are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). A feedback section at the bottom shows "Ваши решения" (Your solutions) with a score of "1 балл" (1 point) and a prompt to rate the step. The left sidebar shows the course progress, with "3.4 Вирусы. Примеры" highlighted. The top of the page shows the Stepik logo and navigation icons.

stepik

3.4 Вирусы. Примеры 5 из 5 шагов пройдено 2 из 2 баллов получено

Email Спуфинг – это

Выберите один вариант из списка

Верно. Так держать!

☐ атака перебором паролей

☒ подмена адреса отправителя в имейлах

☐ метод предотвращения фишинга

☐ протокол для отправки имейлов

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

2 учащимся понравился этот шаг, а вам?

Следующий шаг

## Троян маскируется под обычную программу. (рис. 13)

The screenshot shows a web browser window with the Stepik platform interface. The browser's address bar displays the URL `stepik.org/lesson/666225/step/5?unit=664214`. The page title is "3.4 Вирусы. Примеры". The left sidebar contains a navigation menu with the following items: "Основы кибербезопасности", "3 Защита ПК/телефона", "3.1 Шифрование диска", "3.2 Пароли", "3.3 Фишинг", "3.4 Вирусы. Примеры" (highlighted), "3.5 Безопасность мессенд...", "4 Криптография на практи...", "4.1 Введение в криптогра...", "4.2 Цифровая подпись", "4.3 Электронные платежи", and "4.4 Блокчейн". The main content area displays the question "Вирус-троян" and asks the user to "Выберите один вариант из списка". The options are: "обязательно шифрует данные и требует ключ дешифрования", "маскируется под легитимную программу" (selected with a green radio button), "работает исключительно под ОС Windows", and "разработан греками". A green box on the right indicates that 2,041 users answered correctly, with a 77% success rate. Below the options are buttons for "Следующий шаг" and "Решить снова". At the bottom, it shows "Ваши решения: Вы получили: 1 балл" and a feedback section with five smiley face icons and the text "2 учащимся понравился этот шаг, а вам?".

stepik

3.4 Вирусы. Примеры 5 из 5 шагов пройдено 2 из 2 баллов получено

Вирус-троян

Выберите один вариант из списка

Верно решил 2 041 учащийся  
Из всех попыток 77% верных

☒ Так точно!

☐ обязательно шифрует данные и требует ключ дешифрования

☒ маскируется под легитимную программу

☐ работает исключительно под ОС Windows

☐ разработан греками

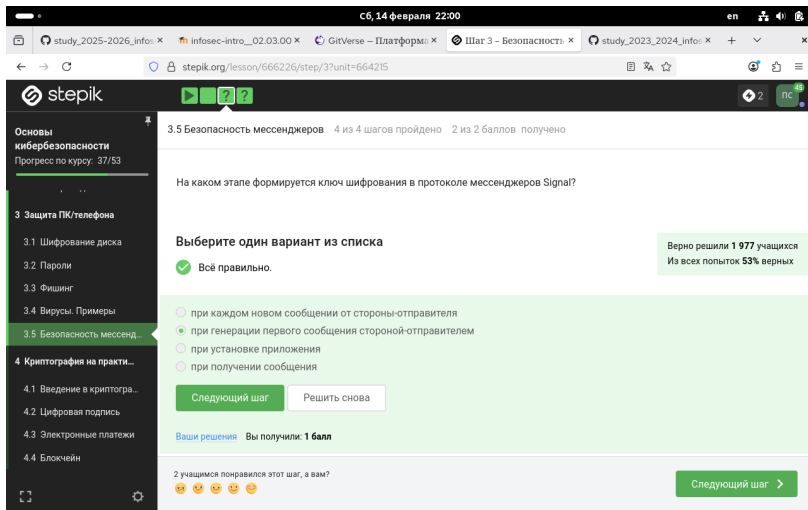
Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

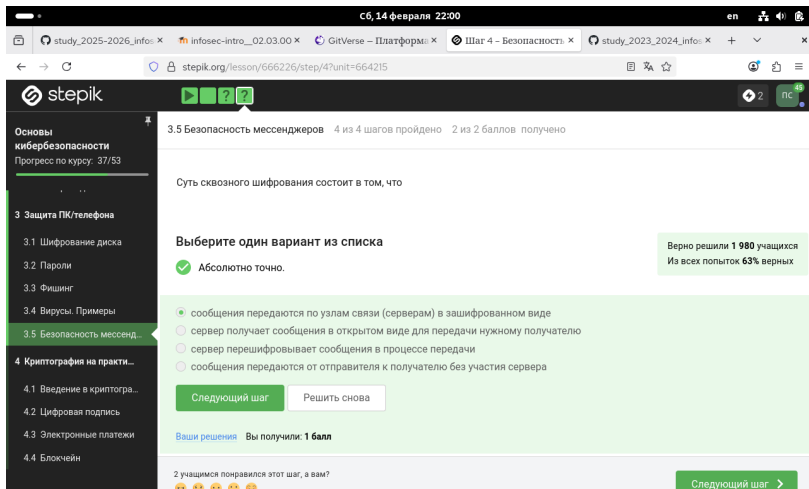
2 учащимся понравился этот шаг, а вам?

Следующий шаг

Ключ шифрования в сигнале формируется при первом сообщении от отправителя. (рис. 14)



Суть сквозного шифрования в том, что сообщения передаются по узлам связи (серверам) в зашифрованном виде. (рис. 15)



## Раздел 4

### 4. Выводы

## 4. Выводы

Я выполнила 2 этап внешнего курса и приобрела знания о том, как приавильно защищать ПК/телефон, узнала о вирусах и фишинге, а так же научилась составлять надежные пароли.