

# Внешний курс. Этап 2

## 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

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

The screenshot shows a web browser window with multiple tabs open. The main content is a Stepik.org lesson titled "3.1 Шифрование диска". The lesson summary indicates 5 steps completed, 3 points earned, and 3 points available. A question asks if it's possible to encrypt the boot sector of a disk. Below, a green box shows the correct answer: "Хорошие новости, верно!" (Good news, right!). It also states that 2,193 students solved the step and 89% of attempts were correct. At the bottom, there are sections for "Ваши решения" (Your solutions) showing 1 point earned, and "Комментарии" and "Решения" (Solutions) sections.

Сб, 14 февраля 21:58

en

study\_2025-2026\_info... x infosec-intro\_\_02.03.00 x GitVerse – Платформа x Шаг 3 – Шифрование x study\_2023\_2024\_info... x

stepik.org/lesson/666222/step/3?unit=66421

2 nc 49

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

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

Хорошие новости, верно!

Верно решили 2 193 учащихся  
Из всех попыток 89% верных

Да

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

2 учащимся понравился этот шаг, а вам?

Следующий шаг >

Комментарии Решения

### 3.2 2

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

The screenshot shows a browser window with multiple tabs open at the top. The main content is a Stepik.org lesson titled "3.1 Шифрование диска". The sidebar on the left lists course modules: "Основы кибербезопасности" (Progress: 37/53), "3 Защита ПК/телефона" (selected), and "4 Криптография на практике...". Under "3 Защита ПК/телефона", the sub-module "3.1 Шифрование диска" is highlighted. The main area displays the question: "Шифрование диска основано на". Below it is a button: "Выберите один вариант из списка". A green checkmark indicates the correct answer: "Правильно, молодец!". To the right, a green box shows statistics: "Верно решили 2 188 учащихся" and "Из всех попыток 67% верных". Below the list of options are two buttons: "Следующий шаг" and "Решить снова". At the bottom, there's a section for user reactions with a count of "2 учащимся понравился этот шаг, а вам?".

### 3.3 3

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

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

- Address Bar:** stepik.org/lesson/666222/step/5?unit=66421
- Page Title:** 3.1 Шифрование диска
- Progress:** 5 из 5 шагов пройдено | 3 из 3 баллов получено
- Lesson Content:** С помощью каких программ можно зашифровать жесткий диск?
- Question Type:** Выберите все подходящие ответы из списка
- Correct Answer:** Абсолютно точно.
- Feedback:** 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](#).
- Statistics:** Верно решили 2 060 учащихся | Из всех попыток 31% верных
- List of Options:** VeraCrypt, Disk Utility, BitLocker, Wireshark
- Buttons:** Следующий шаг, Решить снова

### 3.4 4

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

The screenshot shows a web browser window with multiple tabs open. The active tab is 'stepik.org/lesson/666223/step/4?unit=664212'. The main content area displays a Stepik course interface. On the left, a sidebar lists course modules: 'Основы кибербезопасности' (Progress: 37/53), '3 Защита ПК/телефона', '3.1 Шифрование диска', '3.2 Пароли' (selected), '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', and '4.4 Блокчейн'. The main content area shows a step titled '3.2 Пароли' with the message '9 из 9 шагов пройдено' and '6 из 6 баллов получено'. A question asks, 'Какие пароли можно отнести с стойким?'. Below it, a list of options is shown: 'qwerty12345' (radio button), 'ILOVECATS' (radio button), 'UQr9@j4IS\$' (radio button, selected), and 'IDONTLOVECATS' (radio button). A green feedback box says 'Верно решили 2 123 учащихся Из всех попыток 87% верных'. At the bottom, there are buttons for 'Следующий шаг' and 'Решить снова'. The status bar at the bottom indicates '2 учащимся понравился этот шаг, а вам?' with several emoji reactions, and 'Следующий шаг >'. The overall theme is cybersecurity.

3.5 5

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

The screenshot shows a web browser window with multiple tabs open, including 'study\_2025-2026\_infoe', 'infosec-intro\_\_02.03.00', 'GitVerse – Платформа', 'Шаг 5 – Пароли – Старт', 'study\_2023\_2024\_infoe', and others. The main content is from the 'stepik.org' website, specifically a lesson titled '3.2 Пароли'. The progress bar indicates '9 из 9 шагов пройдено' and '6 из 6 баллов получено'. A question asks 'Где безопасно хранить пароли?'. Below it, a green box says 'Выберите один вариант из списка' and lists five options: 'В менеджерах паролей' (selected), 'В заметках на рабочем столе', 'В заметках в телефоне', 'На стикере, приkleенном к монитору', and 'В кошельке'. A green button at the bottom left says 'Следующий шаг' and a white button says 'Решить снова'. To the right, a green box states 'Верно решили 2 119 учащихся Из всех попыток 78% верных'. At the bottom, it says 'Ваши решения Вы получили: 1 балл' and '2 учащимся понравился этот шаг, а вам?' followed by several small emoji faces. The browser interface includes a sidebar with course navigation, a top bar with date and time ('сб, 14 февраля 21:58'), and a bottom navigation bar.

### 3.6 6

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

The screenshot shows a web browser window with multiple tabs open. The active tab is on stepik.org, displaying a lesson from the '3.2 Пароли' section of the 'Основы кибербезопасности' course. The progress bar indicates 9 из 9 шагов пройдено and 6 из 6 баллов получено. A CAPTCHA challenge is visible at the top of the page, consisting of several colored squares (blue, green, yellow, red) with question marks over them.

**Зачем нужна капча?**

**Выберите один вариант из списка**

Прекрасный ответ.

Для защиты кук пользователя  
 Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа  
 Для безопасного хранения паролей на сервере  
 Она заменяет пароли

Следующий шаг    Решить снова

Ваши решения    Вы получили: 1 балл

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

Следующий шаг >

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

The screenshot shows a web browser window with multiple tabs open. The active tab is from stepik.org, displaying a lesson titled '3.2 Пароли'. The sidebar on the left lists course modules: 'Основы кибербезопасности' (Progress: 37/53), '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). The main content area shows the lesson title '3.2 Пароли' with a progress bar indicating '9 из 9 шагов пройдено' and '6 из 6 баллов получено'. A question 'Для чего применяется хэширование паролей?' is displayed. Below it, a section titled 'Выберите один вариант из списка' shows a correct answer: 'Правильно.' with a green checkmark. The correct option is 'Для того, чтобы не хранить пароли на сервере в открытом виде.' There are also other options: 'Для того, чтобы пароль не передавался в открытом виде.', 'Для того, чтобы ускорить процесс авторизации', and 'Для удобства разработчиков'. At the bottom, there are buttons for 'Следующий шаг' and 'Решить снова'. A feedback message says 'Ваши решения Вы получили: 1 балл'. The browser interface includes a top bar with date/time ('сб, 14 февраля 21:59'), language ('en'), and other standard controls.

3.8 8

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

The screenshot shows a web browser window with the Stepik.org platform. The URL in the address bar is `stepik.org/less...`. The main content area displays a lesson titled "3.2 Пароли" (3.2 Passwords) with a progress of "9 из 9 шагов пройдено" (9 of 9 steps completed) and "6 из 6 баллов получено" (6 of 6 points earned). A central question asks: "Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?" (Will salt help improve the resistance of passwords to a brute-force attack if the attacker gained access to the server?). Below the question, a message says "Хорошая работа." (Good job.) and "Верно решили 2 095 учащихся" (2,095 students solved correctly). The user has selected the correct answer "Нет" (No). Buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again) are visible. At the bottom, there's a section for "Ваши решения" (Your solutions) with a note "Вы получили: 1 балл" (You got: 1 point) and a rating section with 2 thumbs up and 5 thumbs down. A large green button labeled "Следующий шаг >" is at the bottom right.

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

The screenshot shows a browser window with multiple tabs open, including one for the Stepik.org platform. The main content is a lesson titled '3.2 Пароли' (Passwords) from a course on 'Основы кибербезопасности' (Basics of Cybersecurity). The progress bar indicates 37/53 steps completed. A specific challenge asks: 'Какие меры защищают от утечек данных атакой перебором?' (What measures protect against data leaks during a brute-force attack?). Below the question, a green box states: 'Выберите все подходящие ответы из списка' (Select all correct answers from the list). One option is checked with a green checkmark: 'Здорово, всё верно.' (Great, everything is correct). A message box says: '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.' (You solved a difficult task, congratulations! You can help other students in the comments, answer their questions, or compare your solution with others on the forum of solutions.). A green box at the bottom right shows statistics: 'Верно решил 1 981 учащийся' (1,981 students solved correctly) and 'Из всех попыток 20% верных' (20% of all attempts were correct). The list of correct answers includes: 'разные пароли на всех сайтах' (different passwords on all sites), 'периодическая смена паролей' (periodic password changes), 'сложные(=длинные) пароли' (complex (=long) passwords), and 'капча' (CAPTCHA). At the bottom, there are buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). The status bar at the bottom of the browser shows the date and time: 'Сб, 14 февраля 21:59'.

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

The screenshot shows a browser window with multiple tabs open. The active tab is from stepik.org, displaying a lesson titled '3.3 Фишинг' (Phishing) with 5 steps completed and 2 points earned. The question asks: 'Какие из следующих ссылок являются фишинговыми?' (Which of the following links are phishing links?). A green checkmark indicates the user has selected the correct answer: 'Всё получилось!' (All correct!). A yellow box states: '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](#)' (You solved a difficult task, congratulations! You can help other students in the [comments](#), answering their questions, or compare your solution with others in the [solution forum](#)). Below the question, a list of URLs is provided, with the last two being correct (marked with a green checkmark):

- <https://accounts.google.com.br/signin/v2/identifier?hl=ru> (страница входа в аккаунт Google)
- <https://online.sberbank.wix.ru/CSAFront/index.do> (вход в Сбербанк.Онлайн)
- [https://e.mail.ru/login?lang=ru\\_RU](https://e.mail.ru/login?lang=ru_RU) (вход в аккаунт Mail.Ru)
- [https://passport.yandex.ucoz.ucoz.ru/auth?origin=home\\_desktop\\_ru](https://passport.yandex.ucoz.ucoz.ru/auth?origin=home_desktop_ru) (вход в аккаунт Яндекс)

At the bottom of the page are buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again).

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

The screenshot shows a web browser window with multiple tabs open. The active tab is from stepik.org, displaying a lesson titled '3.3 Фишинг'. The sidebar on the left lists several sections: 'Основы кибербезопасности' (Progress: 37/53), '3 Защита ПК/телефона', '3.1 Шифрование диска', '3.2 Пароли', '3.3 Фишинг' (highlighted in green), '3.4 Вирусы. Примеры', and '3.5 Безопасность мессенджеров'. The main content area shows a question: 'Может ли фишинговый имейл прийти от знакомого адреса?'. Below it, a message says 'Выберите один вариант из списка' with a checked green circle next to the text 'Прекрасный ответ.' A green button labeled 'Следующий шаг' is visible. To the right, a green box displays statistics: 'Верно решили 2 048 учащихся' and 'Из всех попыток 91% верных'. At the bottom, there's a section for user reactions with several smiley faces and a green button labeled 'Следующий шаг >'. The browser interface includes standard navigation buttons and a search bar at the bottom.

3.12 12

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

The screenshot shows a web browser window with multiple tabs open. The active tab is from stepik.org, displaying a lesson titled '3.4 Вирусы. Примеры' (3.4 Viruses. Examples). The sidebar on the left lists course modules: 'Основы кибербезопасности' (Basics of Cybersecurity), '3 Защита ПК/телефона' (3 Protection of PCs/Phones), '3.1 Шифрование диска', '3.2 Пароли', '3.3 Фишинг', '3.4 Вирусы. Примеры' (selected), '3.5 Безопасность мессенджеров', '4 Криптография на практике...', '4.1 Введение в криптографию', '4.2 Цифровая подпись', '4.3 Электронные платежи', and '4.4 Блокчейн'. The main content area shows the text 'Email Спуфинг – это' followed by a question 'Выберите один вариант из списка' (Select one option from the list). A green checkmark next to the first option indicates it is correct: 'Верно. Так держать!' (Correct. Keep it up!). Below the list are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green box on the right states 'Верно решили 2 042 учащихся' (2,042 students solved correctly) and 'Из всех попыток 70% верных' (70% of all attempts were correct). At the bottom, there are 5 smiley face rating icons and a 'Следующий шаг >' button.

3.13 13

Троян маскируется под обычную программу. (рис. 13)

The screenshot shows a web browser window with multiple tabs open. The active tab is from stepik.org, displaying a lesson titled '3.4 Вирусы. Примеры'. The sidebar on the left lists various sections of the course, including 'Основы кибербезопасности', 'Защита ПК/телефона', 'Вирус-троян', and 'Безопасность мессенджеров'. The main content area shows a question: 'Выберите один вариант из списка' (Select one option from the list). The correct answer, 'маскируется под легитимную программу' (Masquerades as legitimate software), is selected with a green checkmark. A green box on the right indicates that 2,041 users answered correctly, which is 77% of all attempts. Below the question, there are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). At the bottom of the page, it says 'Вы получили: 1 балл' (You received: 1 point) and shows a rating section with several smiley faces.

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

The screenshot shows a web browser window with multiple tabs open at the top. The main content is a Stepik lesson page titled '3.5 Безопасность мессенджеров' (3.5 Security of messengers). The progress bar indicates '37/53' completed. A sidebar on the left lists course sections and lessons, with '3.5 Безопасность мессенджеров' currently selected. The main area displays a question: 'На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?' (At what stage is the encryption key formed in the Signal messenger protocol?). Below the question, a green button says 'Выберите один вариант из списка' (Select one option from the list). A message box shows 'Всё правильно.' (All correct) with a checkmark. To the right, a green box states 'Верно решили 1 977 учащихся' (1 977 students solved correctly) and 'Из всех попыток 53% верных' (53% of attempts were correct). Below the list of options, there are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). At the bottom, it says 'Вы получили: 1 балл' (You got: 1 point) and '2 учащимся понравился этот шаг, а вам?' (2 students liked this step, do you like it?). There are several smiley face icons below this. At the very bottom, there are navigation icons for the browser.

3.15 15

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

The screenshot shows a web browser window with multiple tabs open. The active tab is from stepik.org, displaying a lesson titled '3.5 Безопасность мессенджеров' (3.5 Security of messengers). The question asks: 'Суть сквозного шифрования состоит в том, что'. Below it, a list of options is shown, with the first one checked: 'сообщения передаются по узлам связи (серверам) в зашифрованном виде'. A green button at the bottom left says 'Следующий шаг' (Next step), and another at the bottom right says 'Решить снова' (Solve again).

Сб, 14 февраля 22:00

en

study\_2025-2026\_info... x infosec-intro\_\_02.03.00 x GitVerse – Платформа x Шаг 4 – Безопасность x study\_2023\_2024\_info... x +

stepik.org/lesson/666226/step/4?unit=664215

steplk.org

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 мессенджеров

4 Криптография на практике

4.1 Введение в криптографию

4.2 Цифровая подпись

4.3 Электронные платежи

4.4 Блокчейн

3.5 Безопасность мессенджеров 4 из 4 шагов пройдено 2 из 2 баллов получено

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

Абсолютно точно.

Верно решили 1 980 учащихся  
Из всех попыток 63% верных

сообщения передаются по узлам связи (серверам) в зашифрованном виде

сервер получает сообщения в открытом виде для передачи нужному получателю

сервер перешифровывает сообщения в процессе передачи

сообщения передаются от отправителя к получателю без участия сервера

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

2 учащимся понравился этот шаг, а вам?

Следующий шаг >

## Раздел 4

### 4. Выводы

## 4. Выводы

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