

Внешний курс. Этап 1

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 course page titled "3.1 Шифрование диска".

Course Navigation: On the left, there's a sidebar with a tree view of the course structure. The "3.1 Шифрование диска" section is currently selected.

Question Content: The main area displays the question: "Можно ли зашифровать загрузочный сектор диска". Below it, a green box contains the instruction: "Выберите один вариант из списка".

Feedback: A green checkmark icon next to the text "Хорошие новости, верно!" indicates the correct answer was selected. To the right, a green box shows statistics: "Верно решили 2 193 учащихся" and "Из всех попыток 89% верных".

Answer Options: Two radio buttons are shown: "Да" (selected) and "Нет".

Buttons: At the bottom of the main area are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again).

Feedback Summary: Below the main area, a summary states: "Ваши решения Вы получили: 1 балл".

Bottom Navigation: At the very bottom, there are navigation icons for the browser and the Stepik platform.

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 states: "Верно решили 2 188 учащихся 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: "2 учащимся понравился этот шаг, а вам?" followed by several smiley face icons. There are also buttons for "Комментарии" and "Решения". The browser interface includes standard navigation buttons at the bottom.

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 the Stepik platform open. The URL in the address bar is stepik.org/lesson/666223/step/4?unit=664212. The page title is "3.2 Пароли". The sidebar on the left lists course modules: "Основы кибербезопасности" (Progress: 37/53), "3 Защита ПК/телефона", "3.1 Шифрование диска" (selected), "3.2 Пароли" (highlighted in green), "3.3 Фишинг", "3.4 Вирусы. Примеры", and "3.5 Безопасность мессенджеров". The main content area displays a question: "Какие пароли можно отнести к стойким?". Below it, a box says "Выберите один вариант из списка" with the message "Так точно!" and a checkmark. A green box on the right shows statistics: "Верно решили 2 123 учащихся" and "Из всех попыток 87% верных". A list of password options is shown with "UQr9@j4IS\$" selected. Buttons at the bottom include "Следующий шаг" and "Решить снова". At the very bottom, a message says "Вы получили: 1 балл". The top of the browser window shows the date and time as "сб, 14 февраля 21:58" and the system status as "en ⚡ 49".

3.5

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

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 a question: 'Где безопасно хранить пароли?'. Below it, a green box says 'Выберите один вариант из списка' with the correct answer 'Абсолютно точно.' highlighted. A list of options follows: 'В менеджерах паролей' (selected), 'В заметках на рабочем столе', 'В заметках в телефоне', 'На стикере, приkleенном к монитору', and 'В кошельке'. At the bottom, there are buttons for 'Следующий шаг' and 'Решить снова'. A message at the bottom says 'Ваши решения Вы получили: 1 балл'.

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 the Stepik platform, specifically 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 question titled 'Зачем нужна капча?' is displayed, with the instruction 'Выберите один вариант из списка'. A green checkmark next to the option 'Прекрасный ответ.' indicates it is the correct answer. Below the list of options, a green box displays statistics: 'Верно решили 2 116 учащихся' and 'Из всех попыток 81% верных'. At the bottom of the page, there are two buttons: 'Следующий шаг' and 'Решить снова'. The footer of the page shows a message: '2 учащимся понравился этот шаг, а вам?' followed by several smiley face icons, and a large green 'Следующий шаг >' button.

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

The screenshot shows a web browser window with multiple tabs open, including one for the Stepik.org platform. The main content is a course step titled "3.2 Пароли" (3.2 Passwords) with 9 of 9 steps completed and 6 of 6 points earned. The question asks: "Для чего применяется хэширование паролей?" (For what purpose is password hashing used?). Below the question, a green box indicates "Правильно." (Correct). A list of four options is shown, with the third option selected: "Для того, чтобы не хранить пароли на сервере в открытом виде." (To store passwords on the server in an unencrypted form). At the bottom, there are buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again), and a message: "Ваши решения Вы получили: 1 балл" (Your solutions You got: 1 point).

3.8 8

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

The screenshot shows a web browser window on a Stepik.org course page. The title of the page is "3.2 Пароли" (Passwords), indicating 9 of 9 steps completed, with 6 out of 6 points earned. A central message box says "Снимок экрана сделан" (Screenshot taken) and "Вы можете вставить изображение из буфера обмена." (You can insert an image from the clipboard). The sidebar on the left lists course modules: "Основы кибербезопасности" (Cybersecurity Basics), "3 Защита ПК/телефона" (PC/Phone Protection), "3.1 Шифрование диска", "3.2 Пароли" (selected), "3.3 Фишинг", "3.4 Вирусы. Примеры", and "3.5 Безопасность мессенджеров". Below these are sections "4 Криптография на практике..." and "4.1 Введение в криптографию", "4.2 Цифровая подпись", "4.3 Электронные платежи", and "4.4 Блокчейн". The main content area displays a question: "Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?". Below it, a message says "Выберите один вариант из списка" (Select one option from the list) and "Хорошая работа." (Good job). Two radio button options are shown: "Да" (Yes) and "Нет" (No), with "Нет" selected. Buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again) are present. A green box at the bottom right states "Верно решили 2 095 учащихся" (2,095 students solved correctly) and "Из всех попыток 65% верных" (65% of all attempts were correct). At the very bottom, there are 2 likes, 1 comment, and a "Следующий шаг" button.

3.9 9

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: 'Вы выбрали все подходящие ответы из списка' (You selected all correct answers from the list). It also says: 'Здорово, всё верно.' (Great, everything is correct). A message box notes: '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: 'Верно решил 1 981 учащийся' (Correctly solved by 1 981 student) and 'Из всех попыток 20% верных' (Of all attempts, 20% 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 course titled '3.3 Фишинг' (3.3 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?). A green checkmark indicates the answer is correct: '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 (вход в аккаунт Mail.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 like back, forward, and search.

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 PC/mobile phone), '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's a feedback section with a message '2 учащимся понравился этот шаг, а вам?' (2 students liked this step, do you like it?) and several smiley face icons. A green 'Следующий шаг >' button is at the bottom right.

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 indicates that 2,041 students 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". The sidebar on the left lists course modules 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?". Below the question, a list of four options is shown, with the second option selected: "при генерации первого сообщения стороной-отправителем". A green button labeled "Всё правильно." indicates the answer is correct. A green box on the right states "Верно решили 1 977 учащихся Из всех попыток 53% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова". Below the question, a message says "Ваши решения Вы получили: 1 балл". At the very bottom, there are rating icons and a "Следующий шаг >" button.

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'. The question asks: 'Суть сквозного шифрования состоит в том, что'. Below it, a list of options is shown, with the first one selected: 'сообщения передаются по узлам связи (серверам) в зашифрованном виде'. A green button at the bottom left says 'Следующий шаг'.

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.

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

Верно решили 1 980 учащихся
Из всех попыток 63% верных

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.