

Внешний курс. Этап 1

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

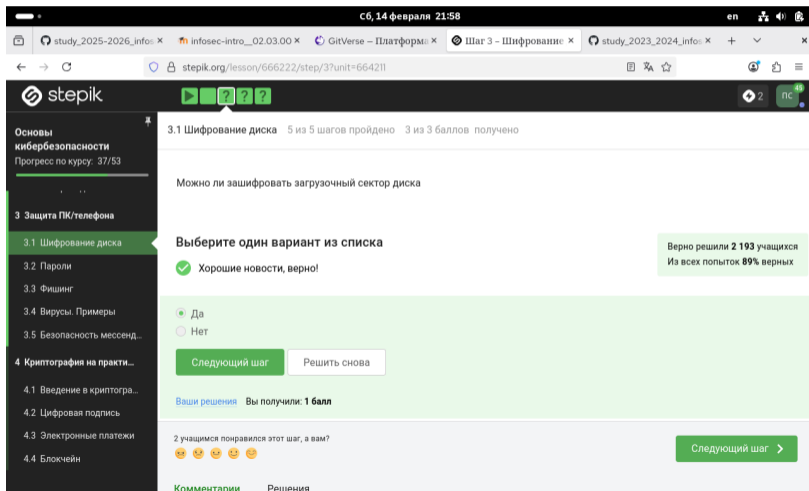
2.1 Цели и задачи

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)



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

The screenshot shows a web browser window with the Stepik interface. 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 lists the course structure, 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 is 'Выберите один вариант из списка'. The options are: 'хэшировании', 'симметричном шифровании' (selected), and 'асимметричном шифровании'. A green checkmark and the text 'Правильно, молодец!' indicate the correct answer. 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!

Верно решили 2 188 учащихся
Из всех попыток 67% верных

☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

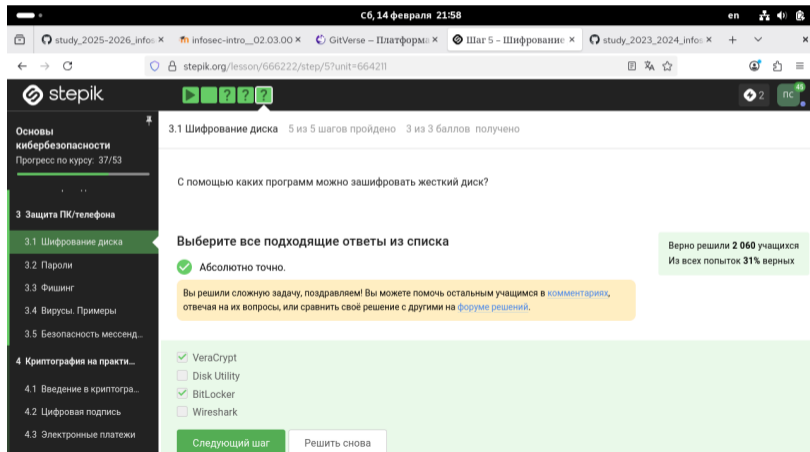
2 учащимся понравился этот шаг, а вам?

😊 😊 😊 😊 😊

Следующий шаг

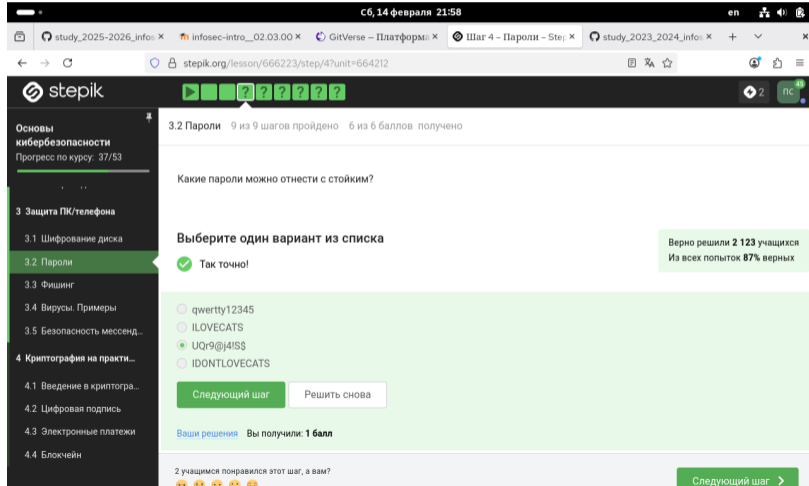
Комментарии Решения

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

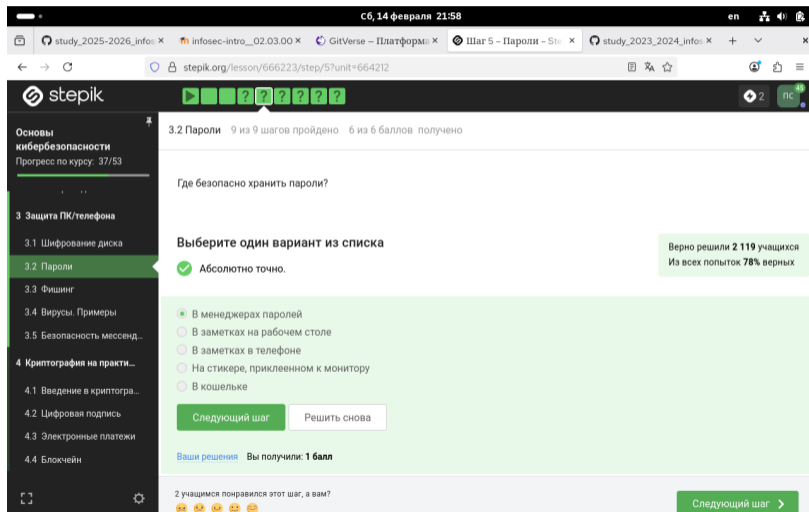


3.4 4

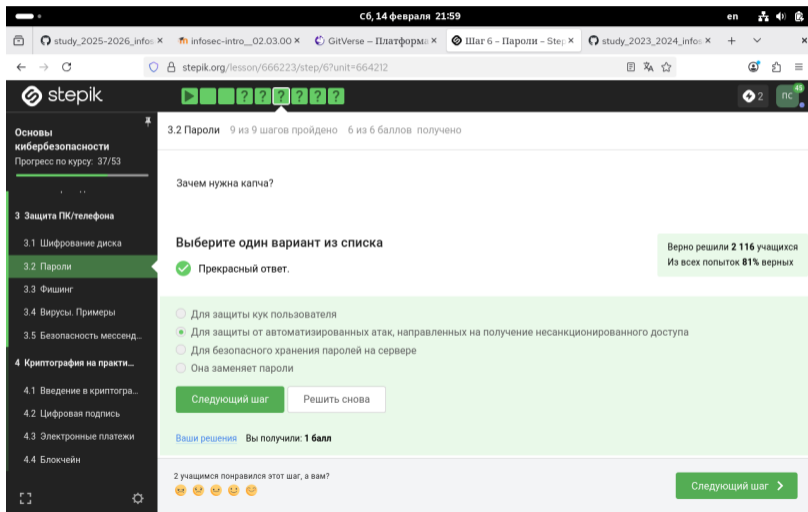
Стойкие пароли длинные, содержат заглавные и строчные символы, специальные символы и цифры. (рис.4)



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 shows "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. A green box on the right indicates "Верно решили 2 108 учащихся" and "Из всех попыток 64% верных". The "Следующий шаг" button is highlighted in green. At the bottom, there is a feedback section with a rating of 2 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

Верно решили 2 108 учащихся
Из всех попыток 64% верных

Правильно.

☐ 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

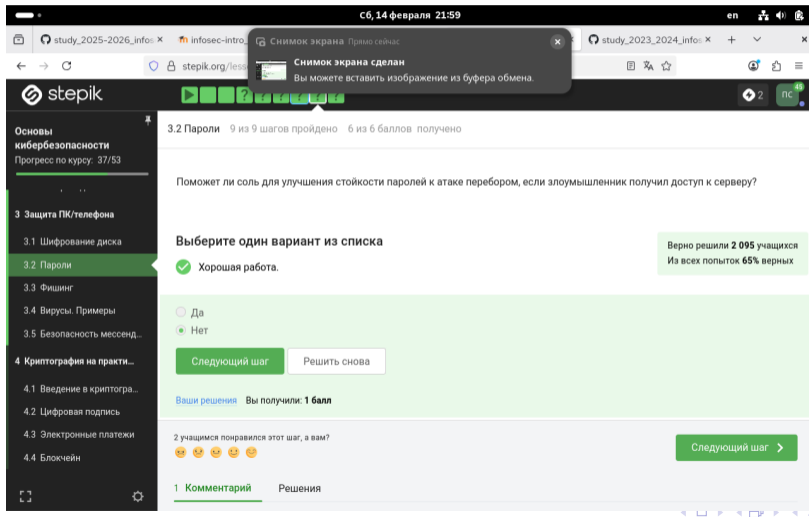
Решить снова

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 course title is "Основы кибербезопасности" (Basics of Cybersecurity), and the progress is 37/53. The current step is 3.2, titled "Пароли" (Passwords). The question asks: "Какие меры защищают от утечек данных атакой перебором?" (Which measures protect against data leaks by brute force attack?). The user has selected "Здорово, всё верно." (Great, everything is correct). The interface shows that 1,981 users have correctly answered this question, and 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" (regular password changes), "сложные(=длинные) пароли" (complex/long passwords), and "капча" (captcha). The interface also shows a "Следующий шаг" (Next step) button and a "Решить снова" (Solve again) button. The bottom of the screen shows the course navigation menu with sections 3 and 4, and the current step 3.2 highlighted.

stepik

С6, 14 февраля 21:59

study_2025-2026_infos × infosec-intro__02.03.00 × GitVerse – Платформ... × Шаг 9 - Пароли – Step... × study_2023_2024_infos ×

stepik.org/lesson/666223/step/9?unit=664212

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

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

✓ Здорово, всё 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](#).

Верно решил 1 981 учащийся
Из всех попыток 20% верных

✓ 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)

С6, 14 февраля 22:00

study_2025-2026_infos x infosec-intro__02.03.00 x GitVerse – Платформ x Шаг 4 – Фишинг – Ste x study_2023_2024_infos x

stepik.org/lesson/666224/step/4?unit=664213

stepik

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

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Всё получилось!

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.

Верно решили 1 902 учащихся
Из всех попыток 21% верных

- ☐ <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.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс)

Следующий шаг Решить снова

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 - Ст...'. The Stepik logo is in the top left corner. The left sidebar shows a course progress bar for 'Основы кибербезопасности' (37/53) and a list of topics. '3.3 Фишинг' is highlighted in green. The main content area shows the lesson title '3.3 Фишинг' with a progress indicator '5 из 5 шагов пройдено' and '2 из 2 баллов получено'. The question is 'Может ли фишинговый имейл прийти от знакомого адреса?'. Below the question, it says 'Выберите один вариант из списка'. There are two radio button options: 'Да' (selected) and 'Нет'. A green box on the right says 'Верно решили 2 048 учащихся' and 'Из всех попыток 91% верных'. At the bottom, there is a 'Следующий шаг' button and a 'Решить снова' button. The bottom of the page shows a navigation bar with icons for back, forward, and other controls.

stepik

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

Может ли фишинговый имейл 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 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 is titled "Email Спуфинг – это" and contains a multiple-choice question: "Выберите один вариант из списка". The correct answer, "Верно. Так держать!", is marked with a green checkmark. The other options are: "атака перебором паролей", "подмена адреса отправителя в имейлах", "метод предотвращения фишинга", and "протокол для отправки имейлов". A green box on the right indicates that 2,042 students correctly answered the question with a 70% success rate. At the bottom, there are buttons for "Следующий шаг" and "Решить снова", and a feedback section asking if the user liked the step.

stepik

С6,14 февраля 22:00

study_2025-2026_infos × infosec-Intro__02.03.00 × GitVerse – Платформ × Шаг 4 - Вирусы. При × study_2023_2024_infos ×

stepik.org/lesson/666225/step/4?unit=664214

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!

Верно решили 2 042 учащихся
Из всех попыток 70% верных

☐ 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 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 feedback box on the right states: "Верно решил 2 041 учащийся. Из всех попыток 77% верных". 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 2 likes and a "Следующий шаг" button.

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

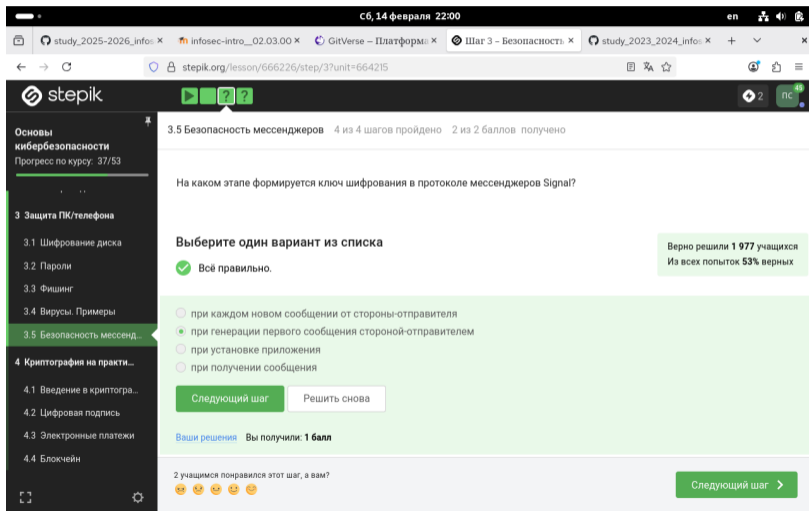
Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

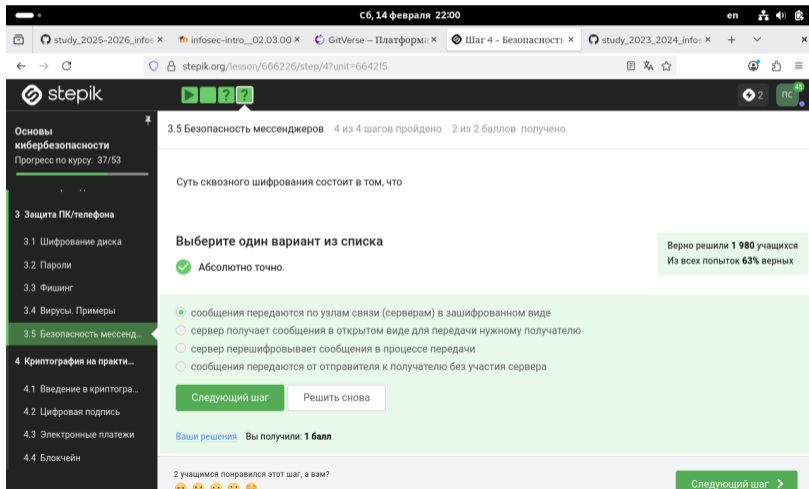
2 учащимся понравился этот шаг, а вам?

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.