Внешний курс. Блок 2: Защита ПК/Телефона

### Основы информационной безопасности

Симонова Виктория Игоревна

Содержание

1. [Цель работы](#_bookmark0) 5
2. [Выполнение блока 2: Защита ПК/Телефона](#_bookmark1) 6
   1. [Шифрование диска](#_bookmark2) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
   2. [Пароли](#_bookmark6) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7
   3. [Фишинг](#_bookmark13) 10
   4. [Вирусы. Примеры](#_bookmark16) 11
   5. [Безопасность мессенджеров](#_bookmark19) 12
3. [Выводы](#_bookmark22) 14

Список иллюстраций

* 1. [Вопрос 3.1.1](#_bookmark3) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 6
  2. [Вопрос 3.1.2](#_bookmark4) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7
  3. [Вопрос 3.1.3](#_bookmark5) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7
  4. [Вопрос 3.2.1](#_bookmark7) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
  5. [Вопрос 3.2.2](#_bookmark8) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 8
  6. [Вопрос 3.2.3](#_bookmark9) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
  7. [Вопрос 3.2.4](#_bookmark10) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9
  8. [Вопрос 3.2.5](#_bookmark11) 10
  9. [НВопрос 3.2.6](#_bookmark12) 10
  10. [Вопрос 3.3.1](#_bookmark14) 11
  11. [Вопрос 3.3.2](#_bookmark15) 11
  12. [Вопрос 3.4.1](#_bookmark17) 12
  13. [Вопрос 3.4.2](#_bookmark18) 12
  14. [Вопрос 3.5.1](#_bookmark20) 13
  15. [Вопрос 3.5.2](#_bookmark21) 13

Список таблиц

# Цель работы

Пройти второй блок курса “Основы кибербезопасности”

# Выполнение блока 2: Защита ПК/Телефона

## Шифрование диска

Шифрование диска — технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать. Соответственно, можно (рис. [2.1).](#_bookmark3)

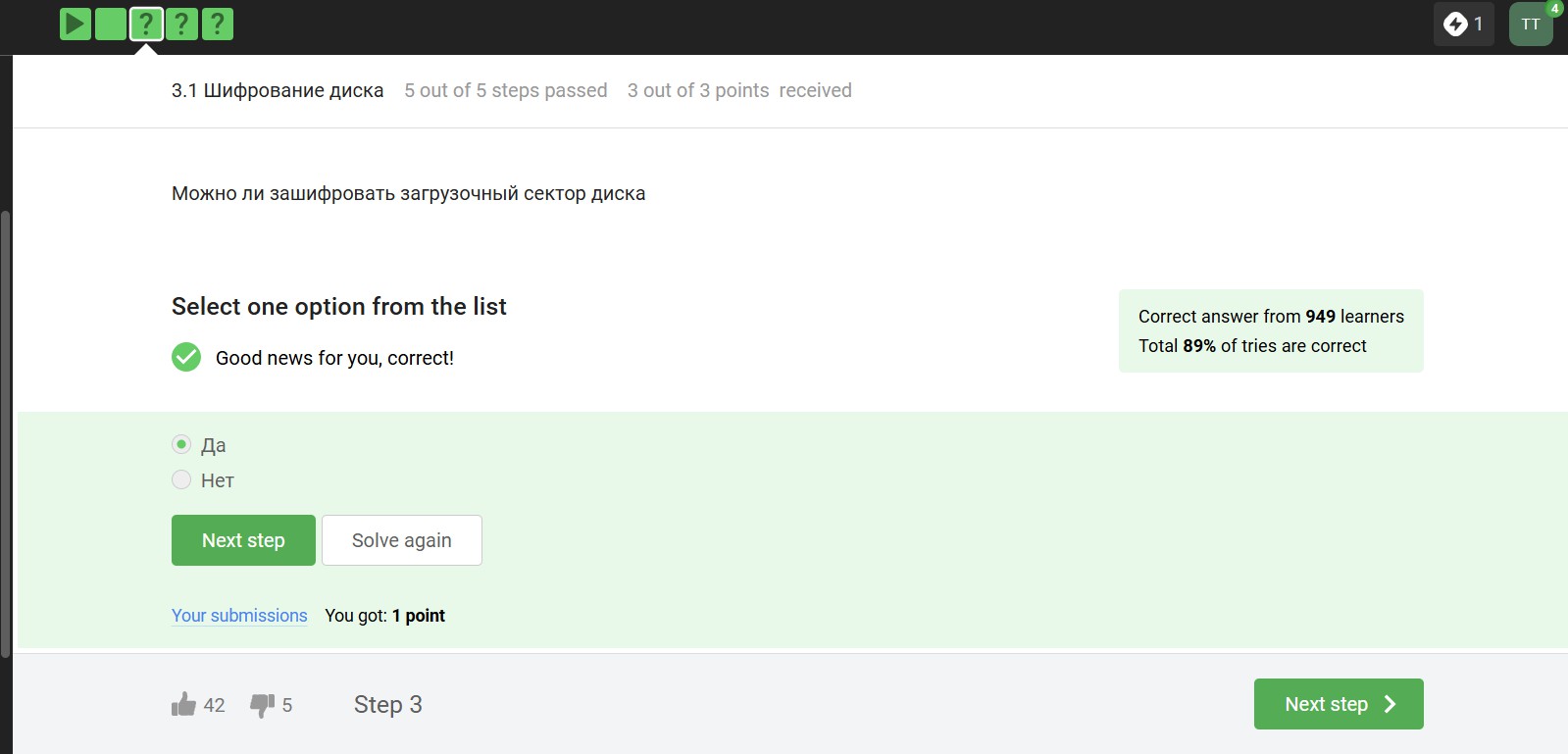


Рис. 2.1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. [2.2).](#_bookmark4)

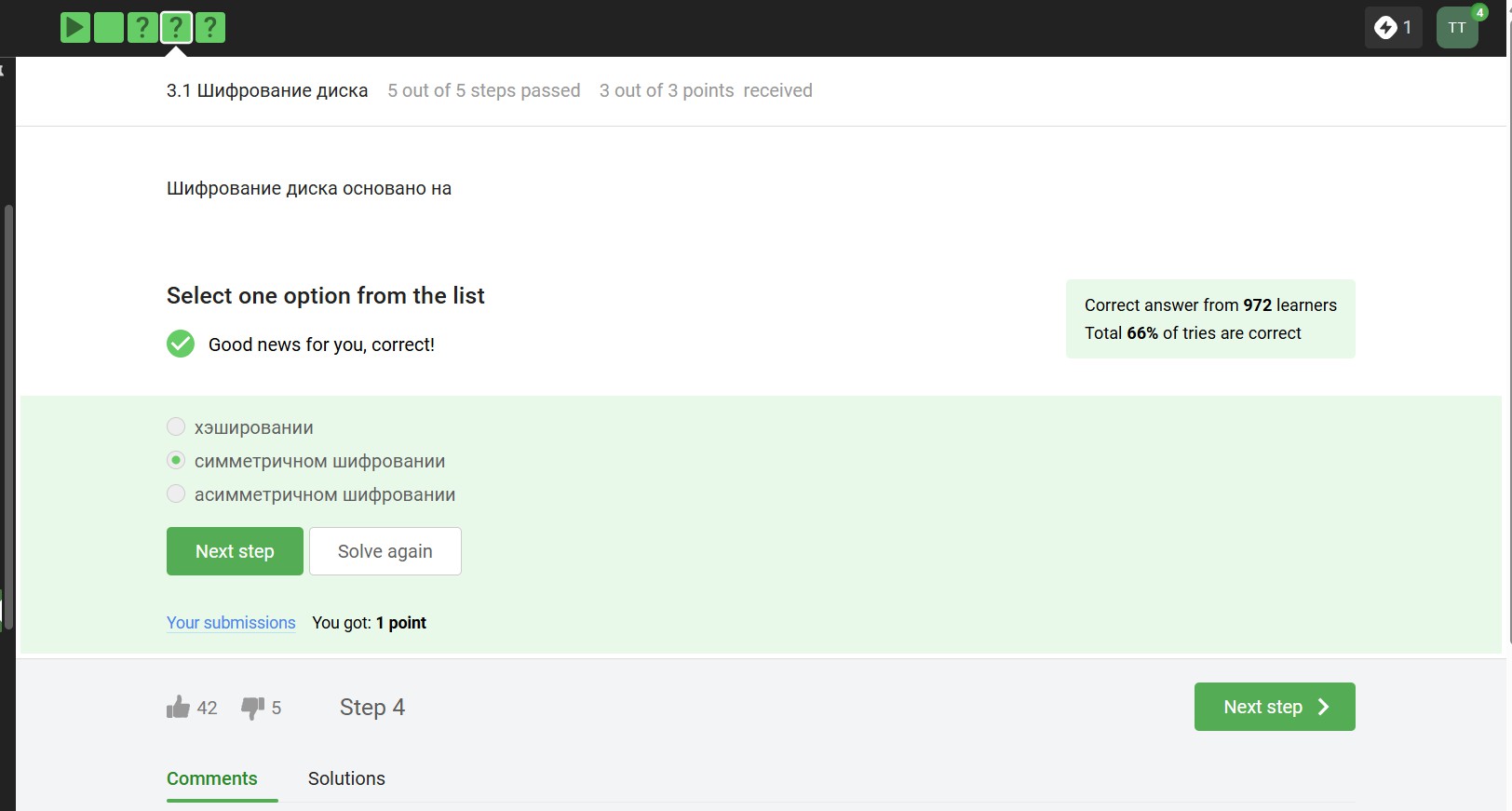


Рис. 2.2: Вопрос 3.1.2

Отмечены программы, с помощью которых можно зашифровать жетский диск (рис. [2.3).](#_bookmark5)

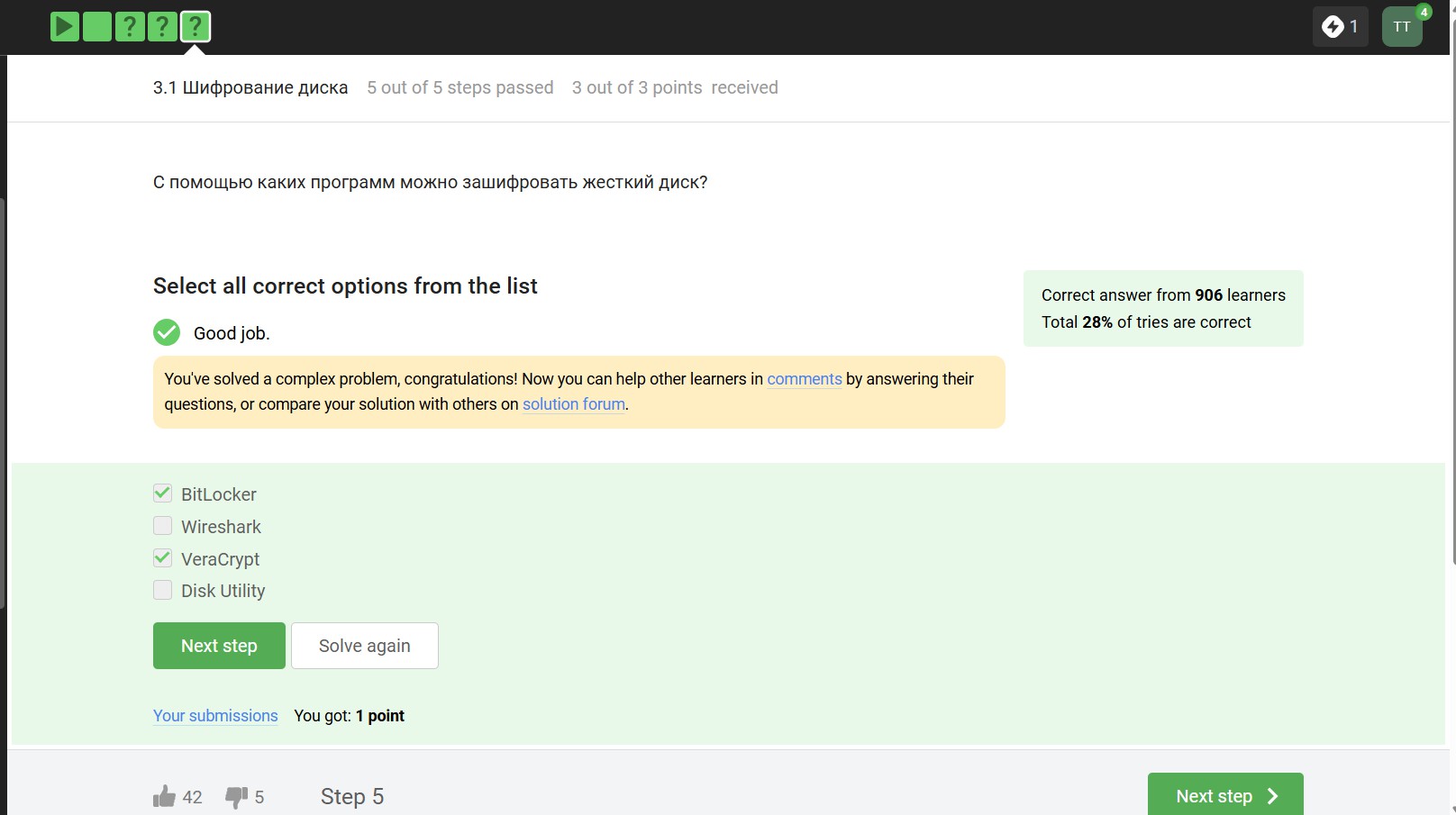


Рис. 2.3: Вопрос 3.1.3

## Пароли

Стойкий пароль - тот, который тяжлее подобрать, он должен быть со спец. символами и длинный (рис. [2.4).](#_bookmark7)

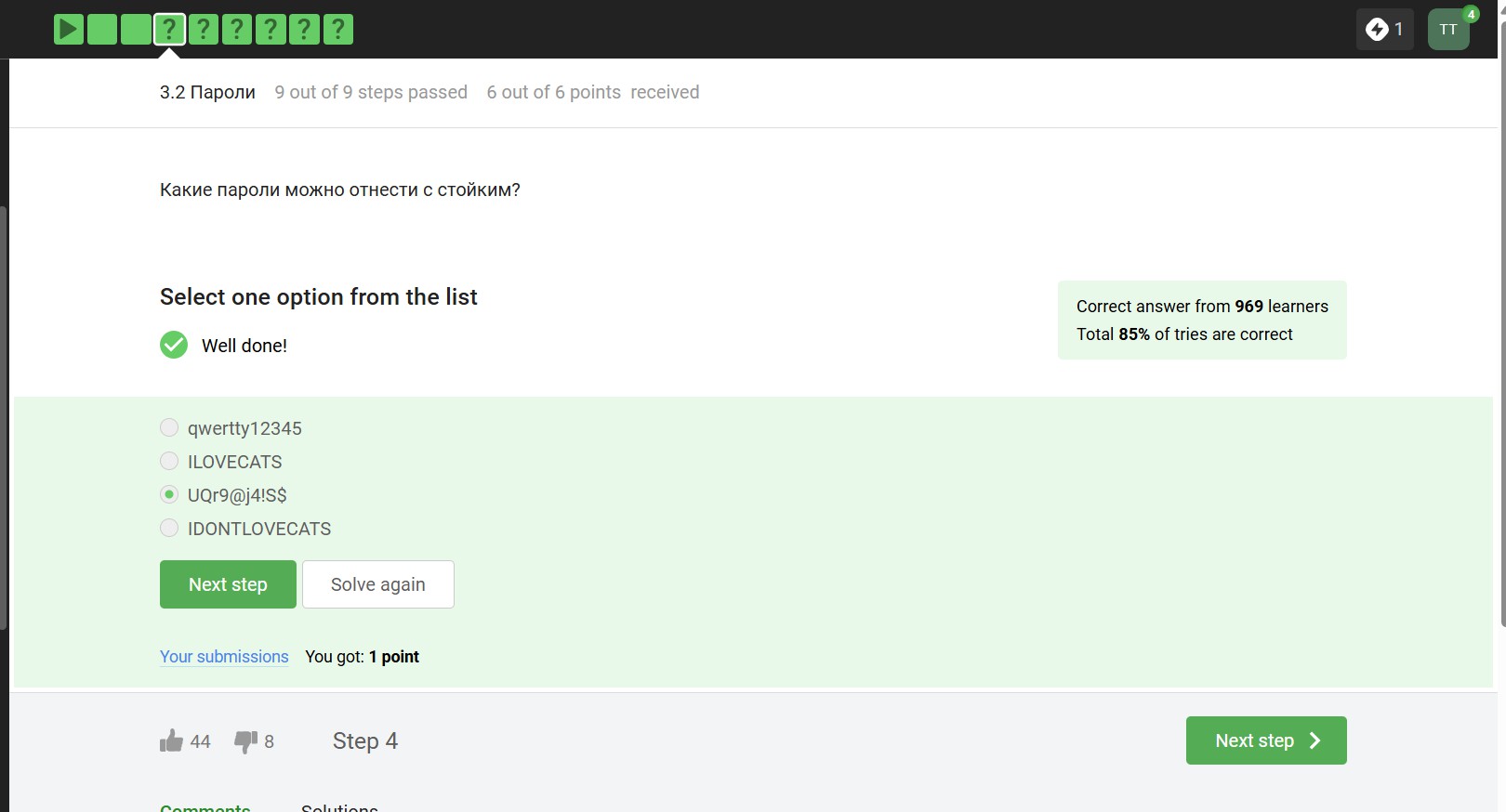


Рис. 2.4: Вопрос 3.2.1

Все варианты, кроме менеджера паролей, совершенно не надежные (рис. [2.5).](#_bookmark8)

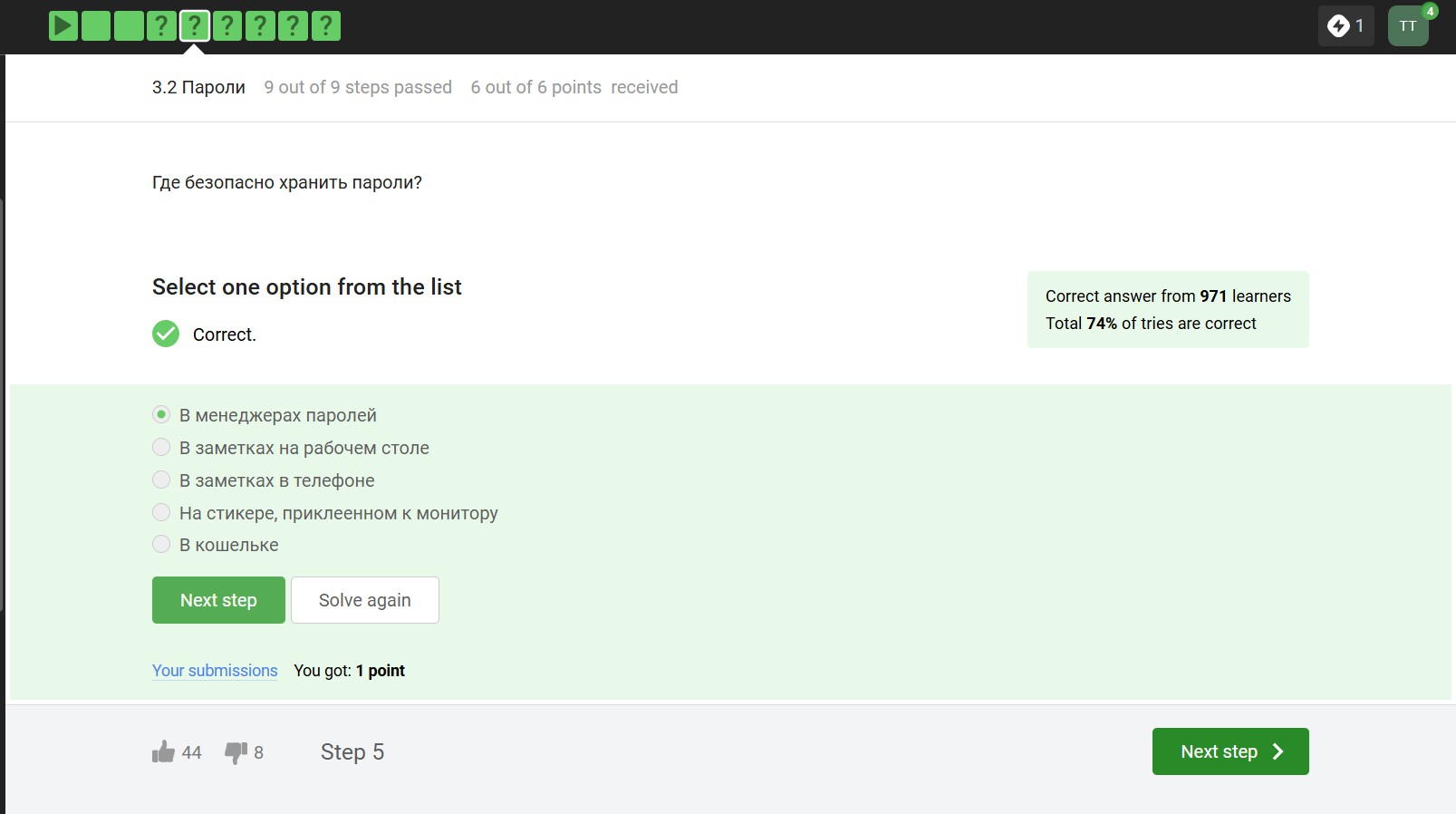


Рис. 2.5: Вопрос 3.2.2

Капча нужна для проверки на то, что за экраном “не робот”(рис. [2.6).](#_bookmark9)

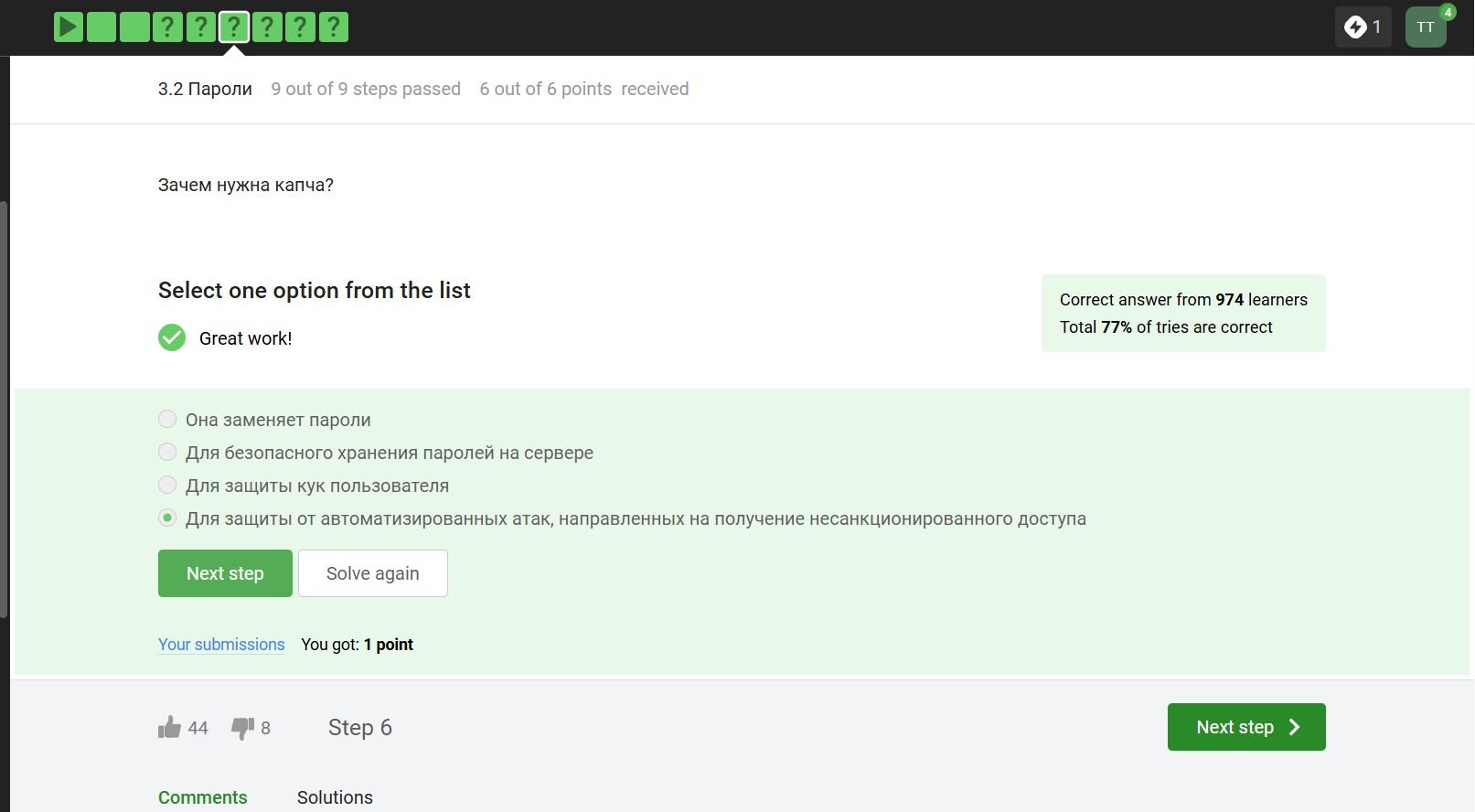


Рис. 2.6: Вопрос 3.2.3

Опасно хранить пароли в открытом виде, поэтому хранят их хэши (рис. [2.7).](#_bookmark10)

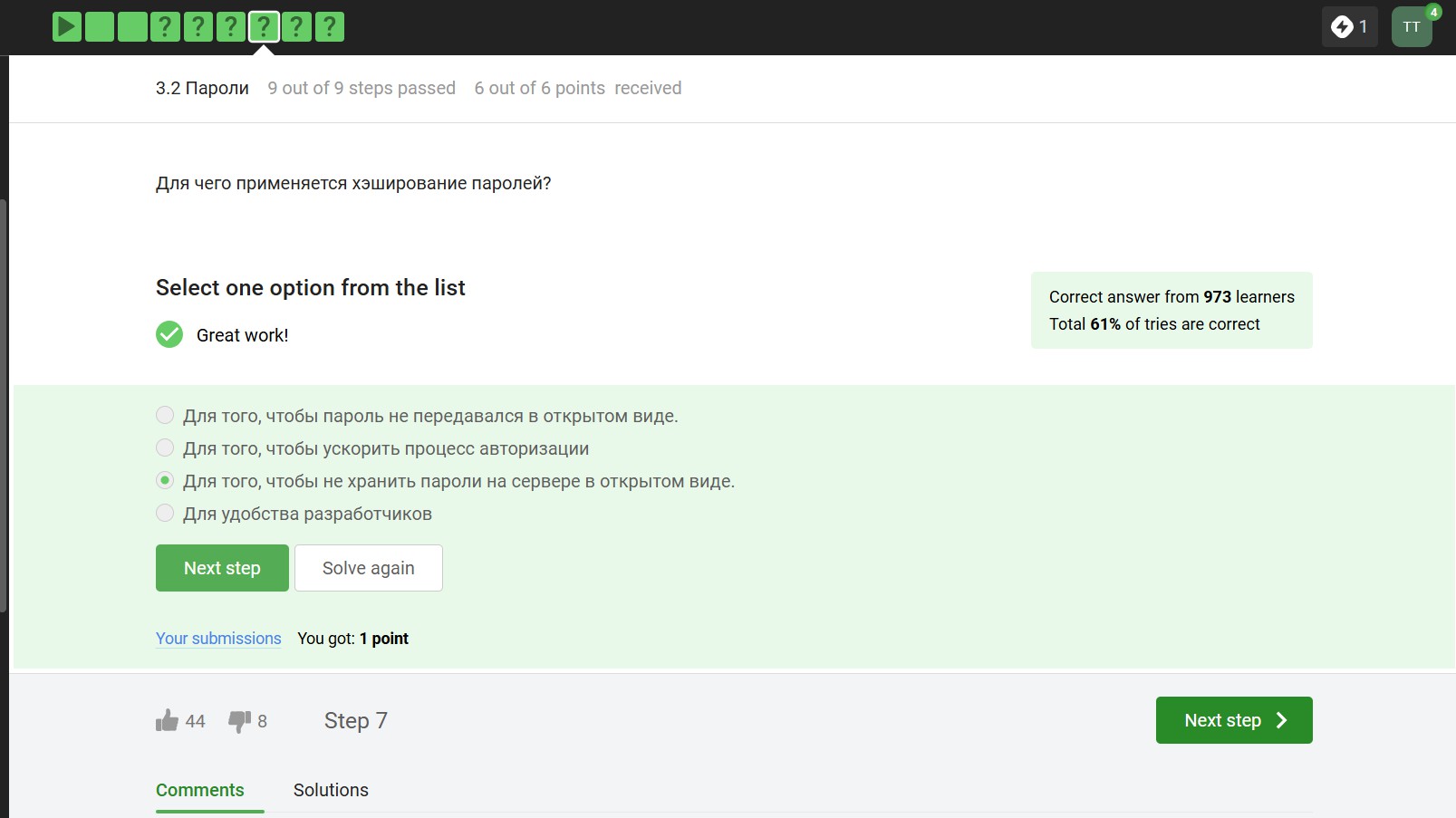


Рис. 2.7: Вопрос 3.2.4

Соль не поможет (рис. [2.8).](#_bookmark11)

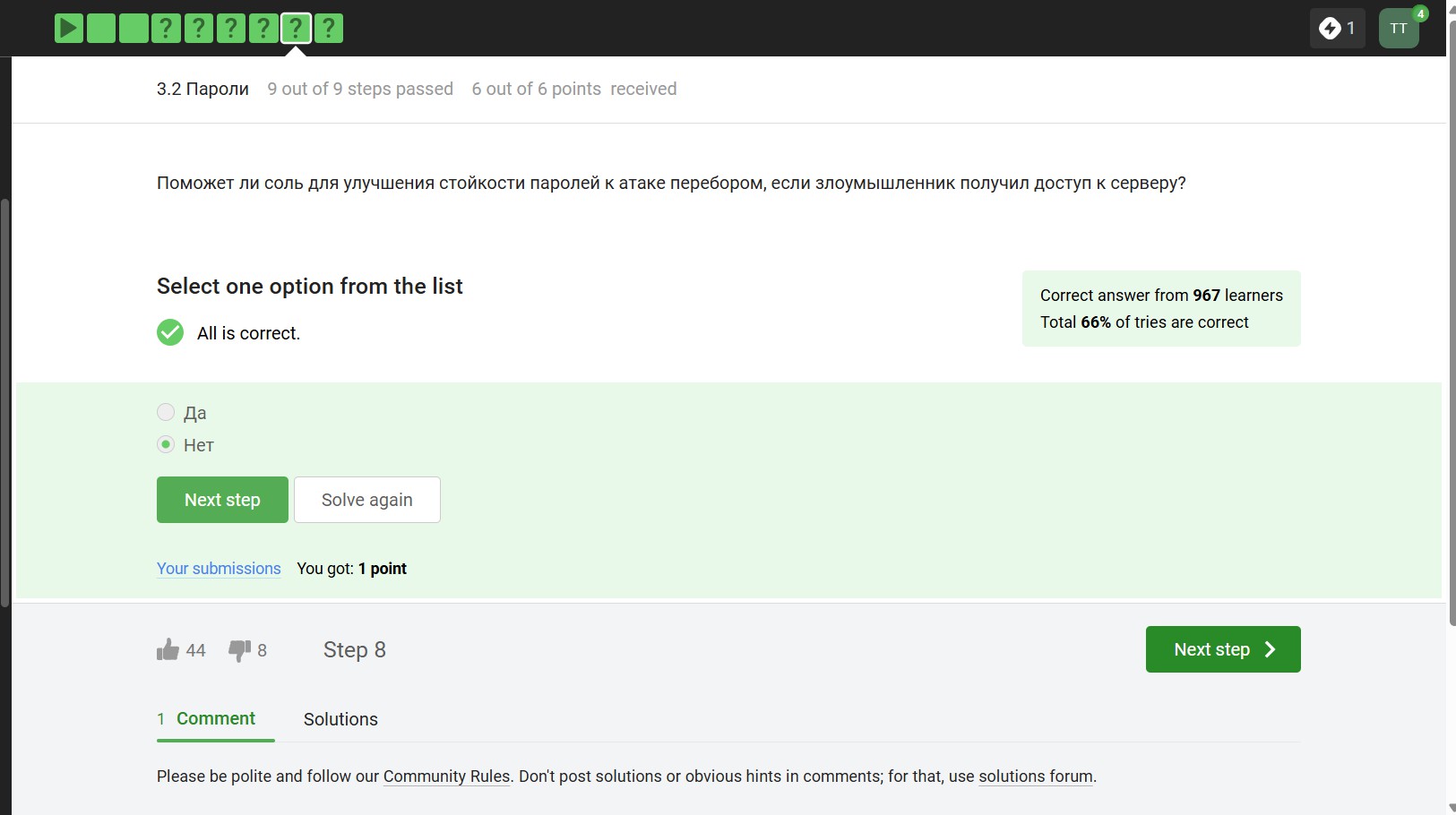


Рис. 2.8: Вопрос 3.2.5

Все приведенные меры защищают от утечек данных (рис. [2.9).](#_bookmark12)

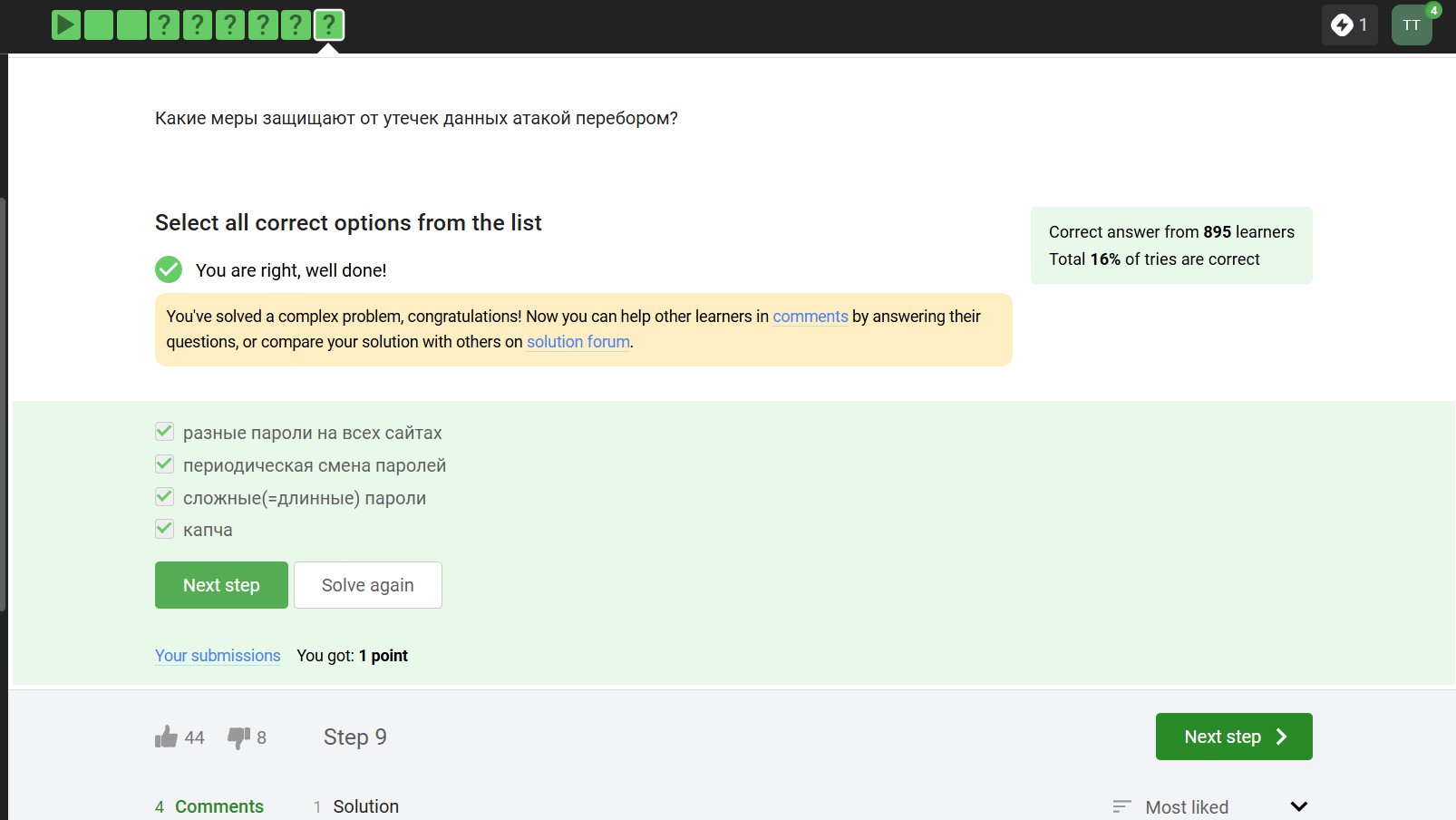


Рис. 2.9: НВопрос 3.2.6

## Фишинг

Фишинговые ссылки очень похожи на ссылки известных сервисов, но с неко- торыми отличиями (рис. [2.10).](#_bookmark14)

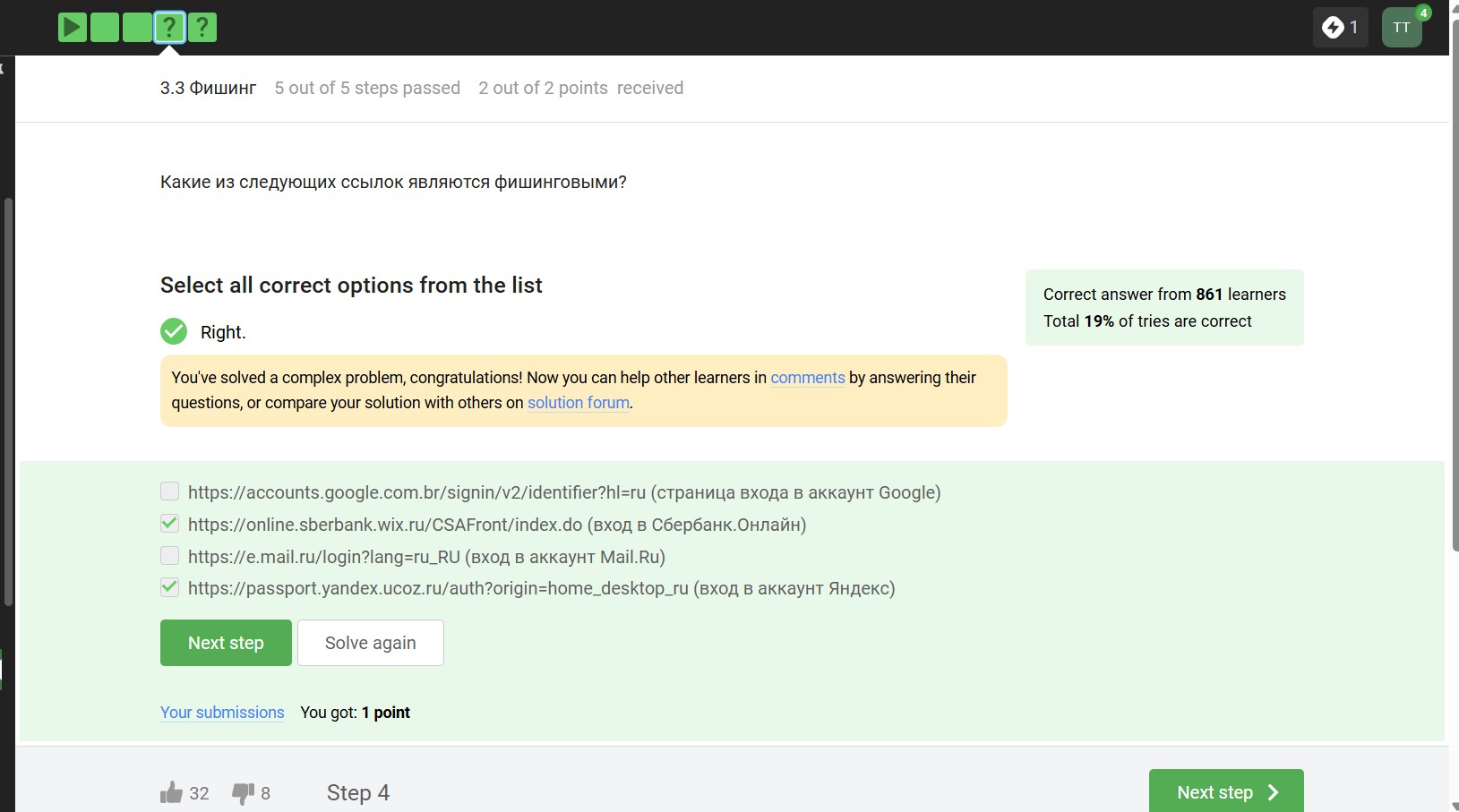


Рис. 2.10: Вопрос 3.3.1

Да, может, например, если пользователя со знакомым адресом взломали (рис.

[2.11).](#_bookmark15)

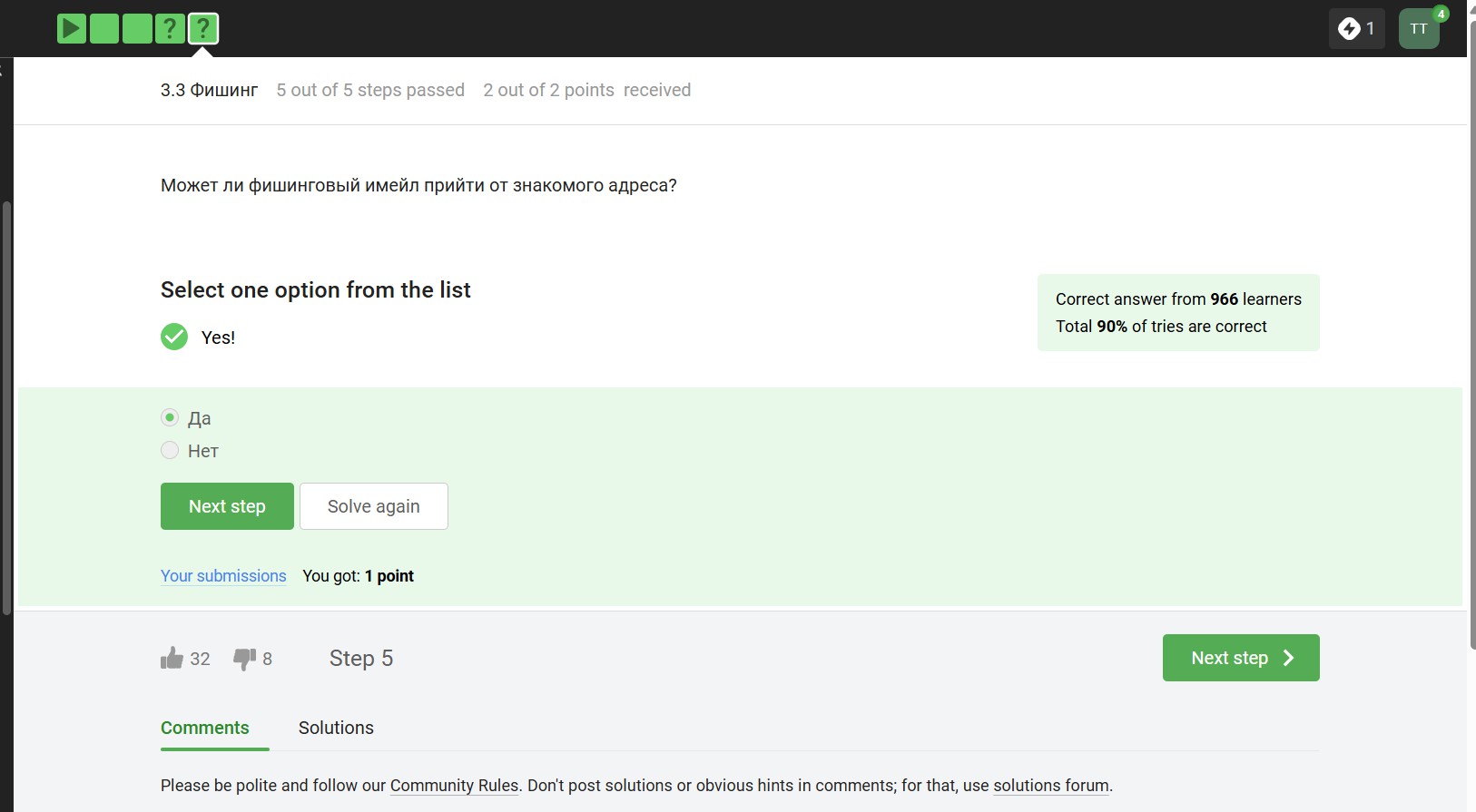


Рис. 2.11: Вопрос 3.3.2

## Вирусы. Примеры

Ответ дан в соответствии с определением (рис. [2.12).](#_bookmark17)

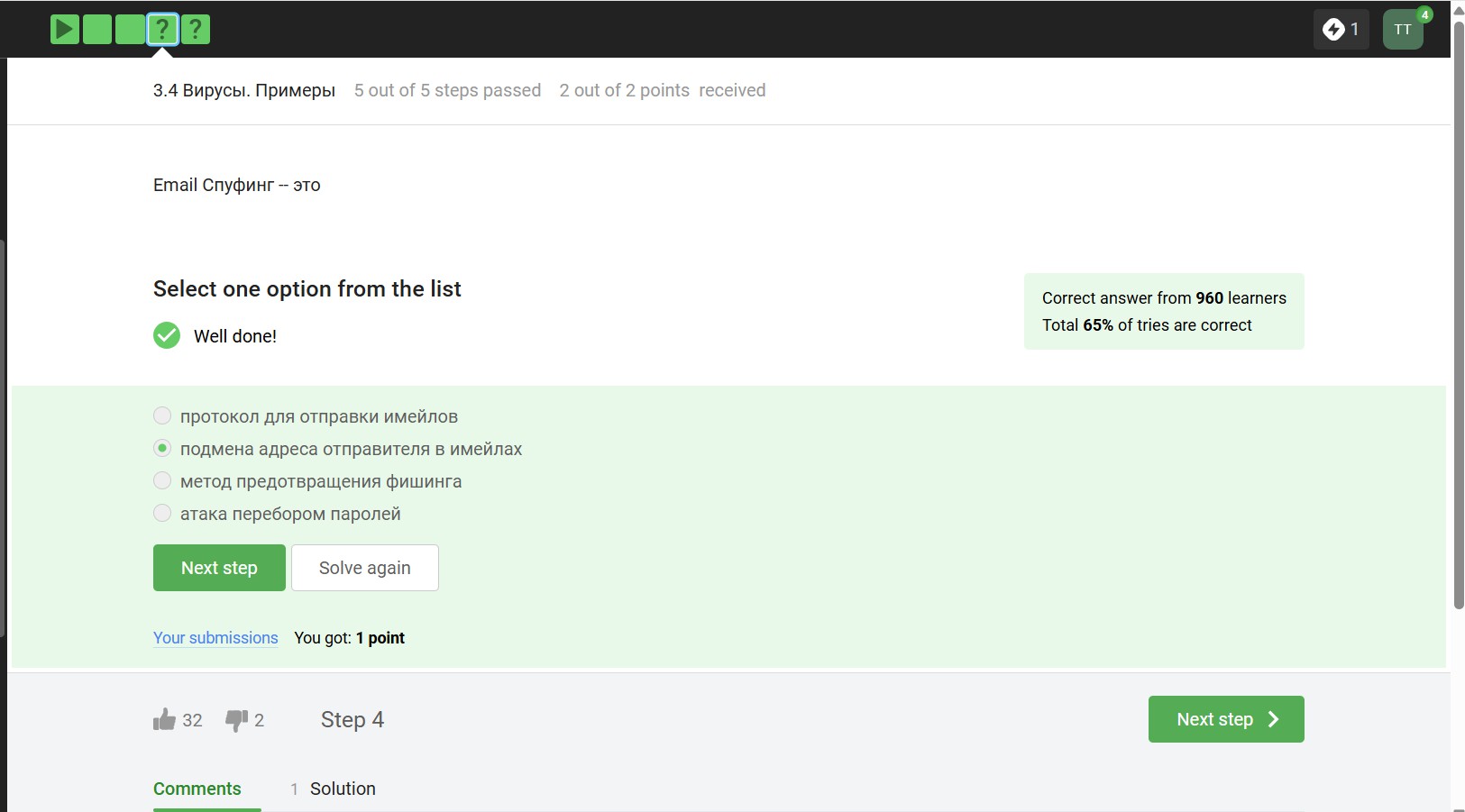


Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. [2.13).](#_bookmark18)

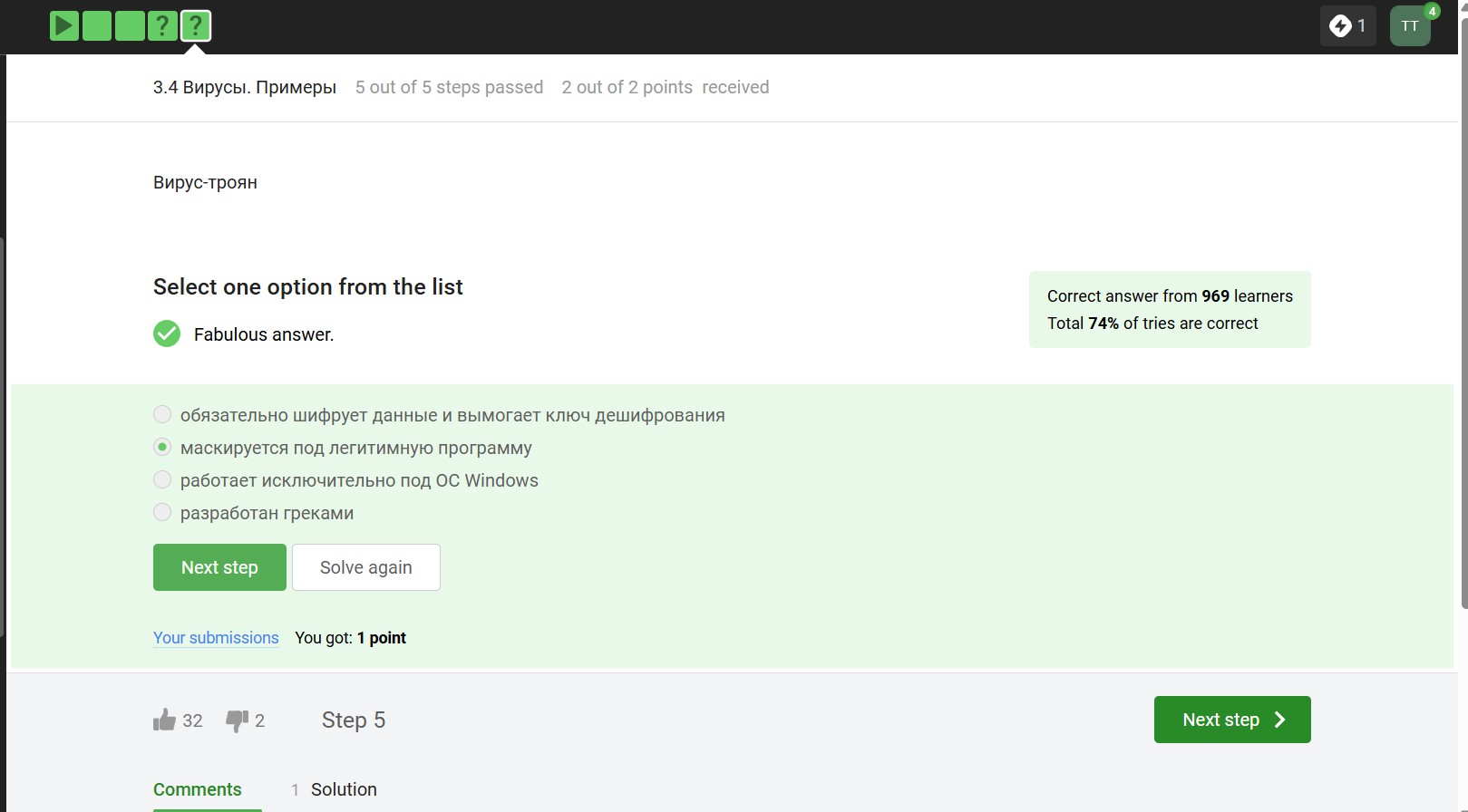


Рис. 2.13: Вопрос 3.4.2

## Безопасность мессенджеров

При установке первого сообщения отправителем формируется ключ шифрова- ния (рис. [2.14).](#_bookmark20)

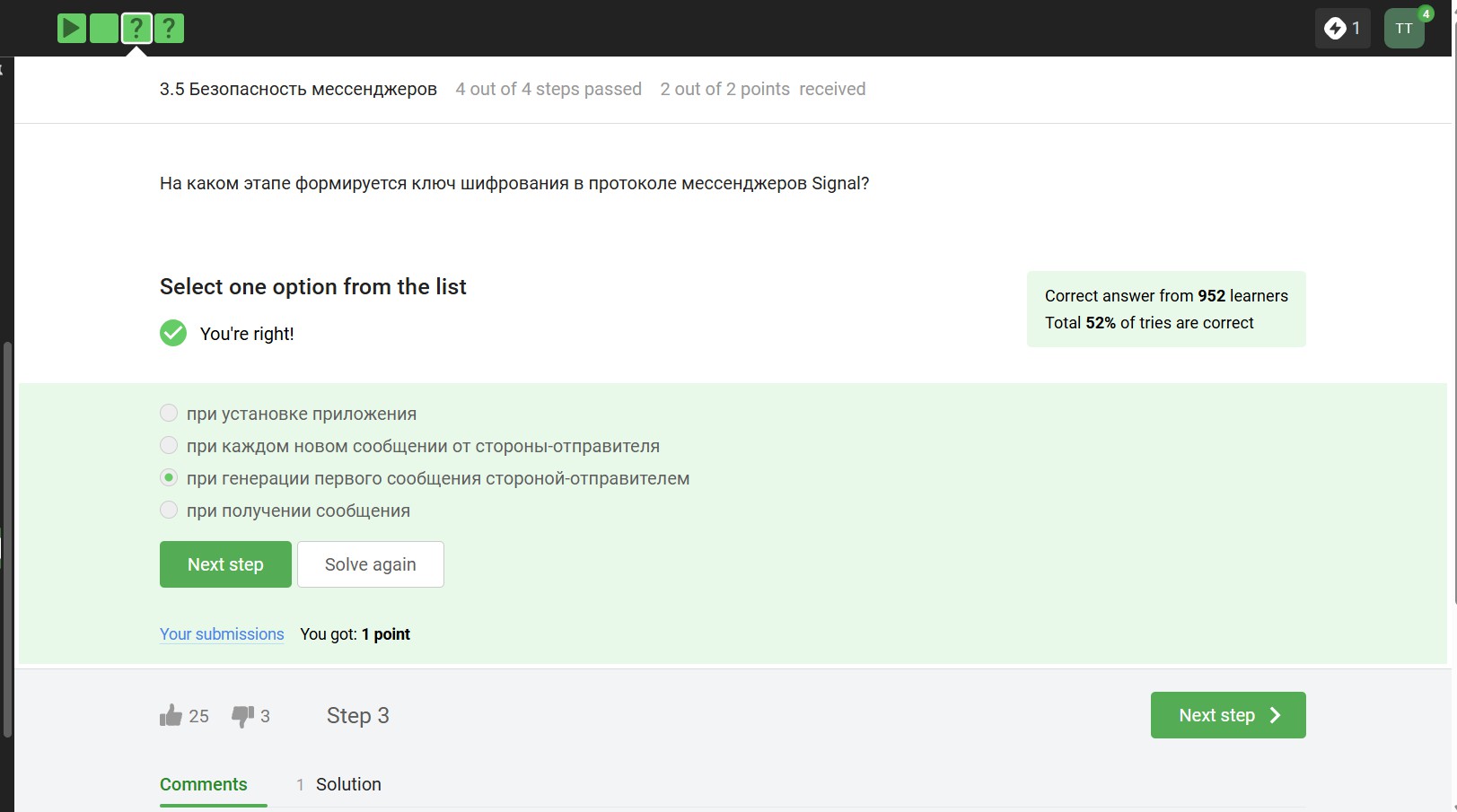


Рис. 2.14: Вопрос 3.5.1

Суть сквозного шифрования состоит в том, что сообзения передаются по узлам связи в зашифрованном виде (рис. [2.15).](#_bookmark21)

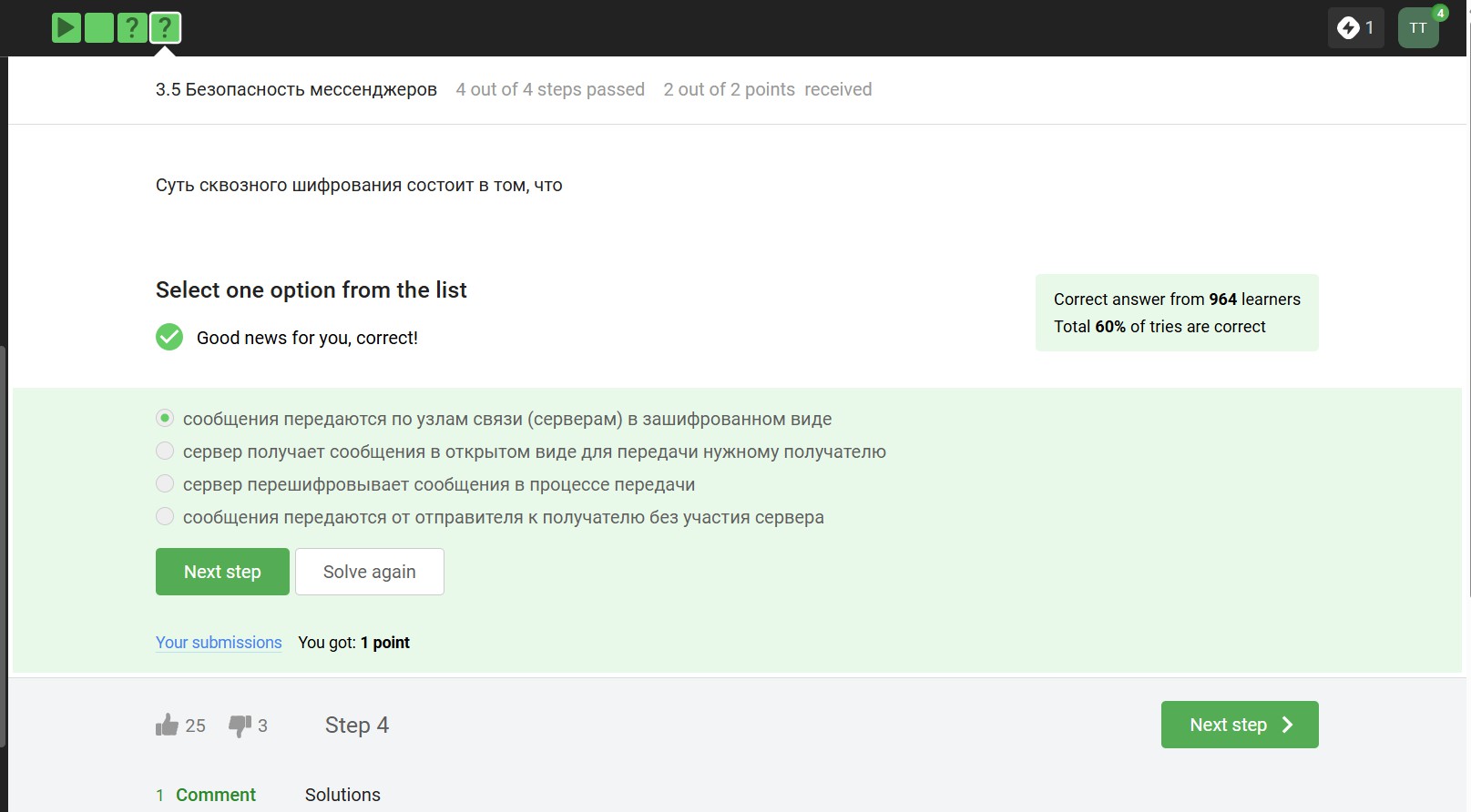


Рис. 2.15: Вопрос 3.5.2

# Выводы

Был пройден второй блок курса “Основы кибербезопасности”, изучены правила хранения паролей и основная информация о вирусах