Внешний курс раздел 2

Защита ПК/телефона

Александр Андреевич Шуплецов

Содержание

# 1 Цель работы

Изучить основы защиты данных ПК/телефона.

# 2 Выполнение работы

1. Загрузочный сектор диска, как и другие сектора диска, можно зашифровать.

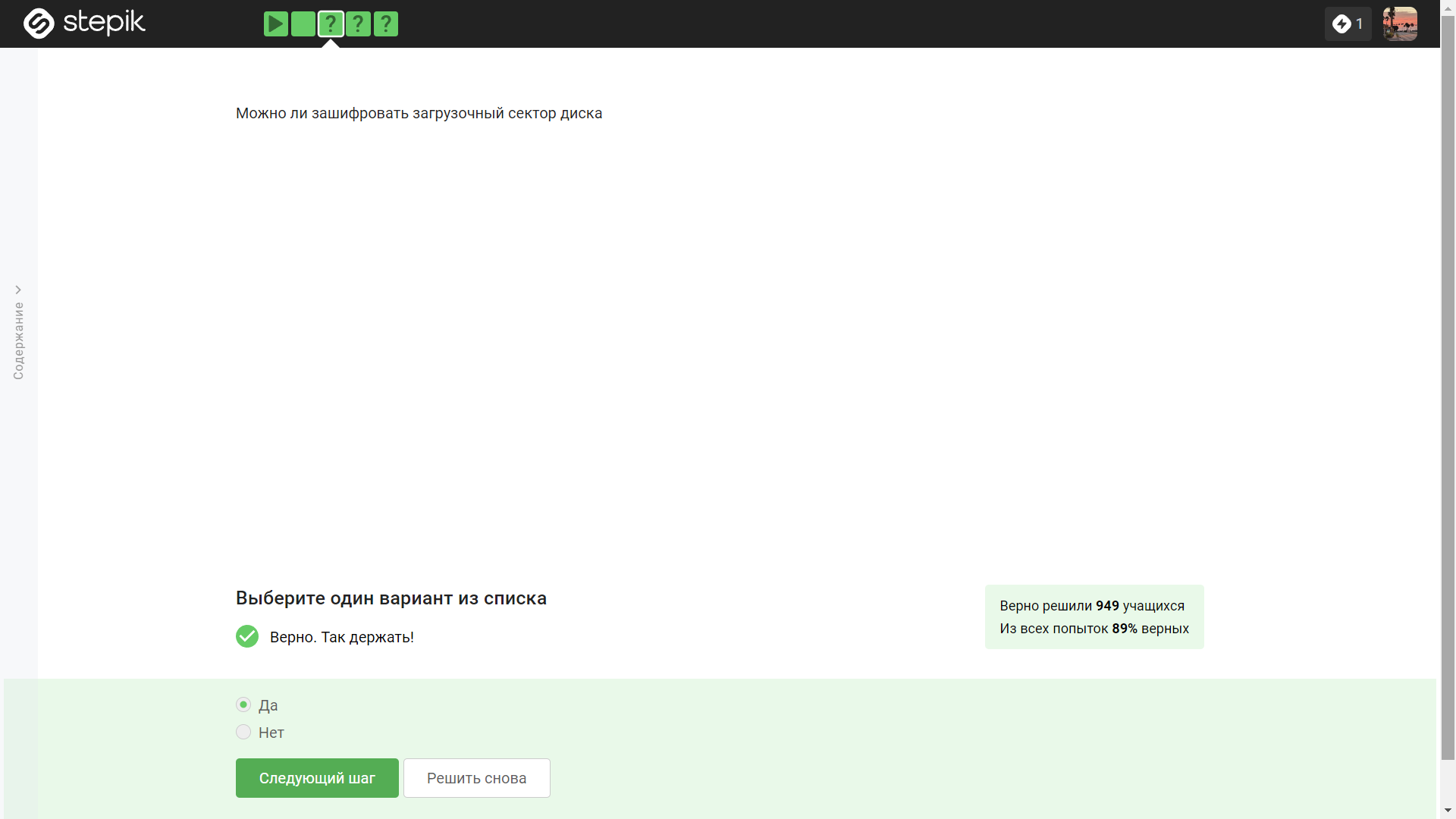


Figure 1: первое задание

1. Шифрование диска основано на симметричном шифровании, как правило на алгоритме AES.

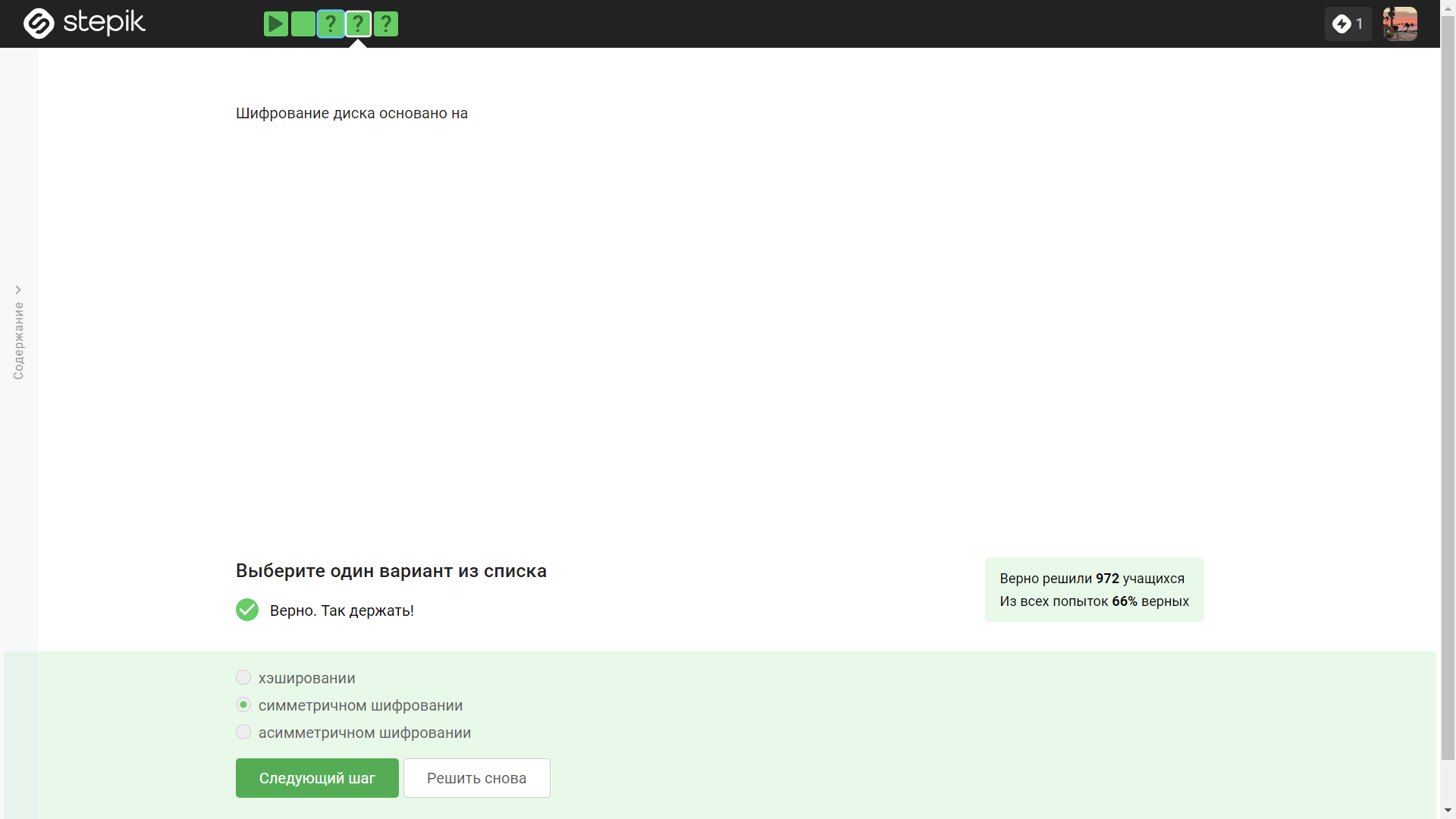


Figure 2: второе задание

1. VeraCrypt и BitLocker - примеры программ, с помощью которых можно зашифровать жесткий диск.

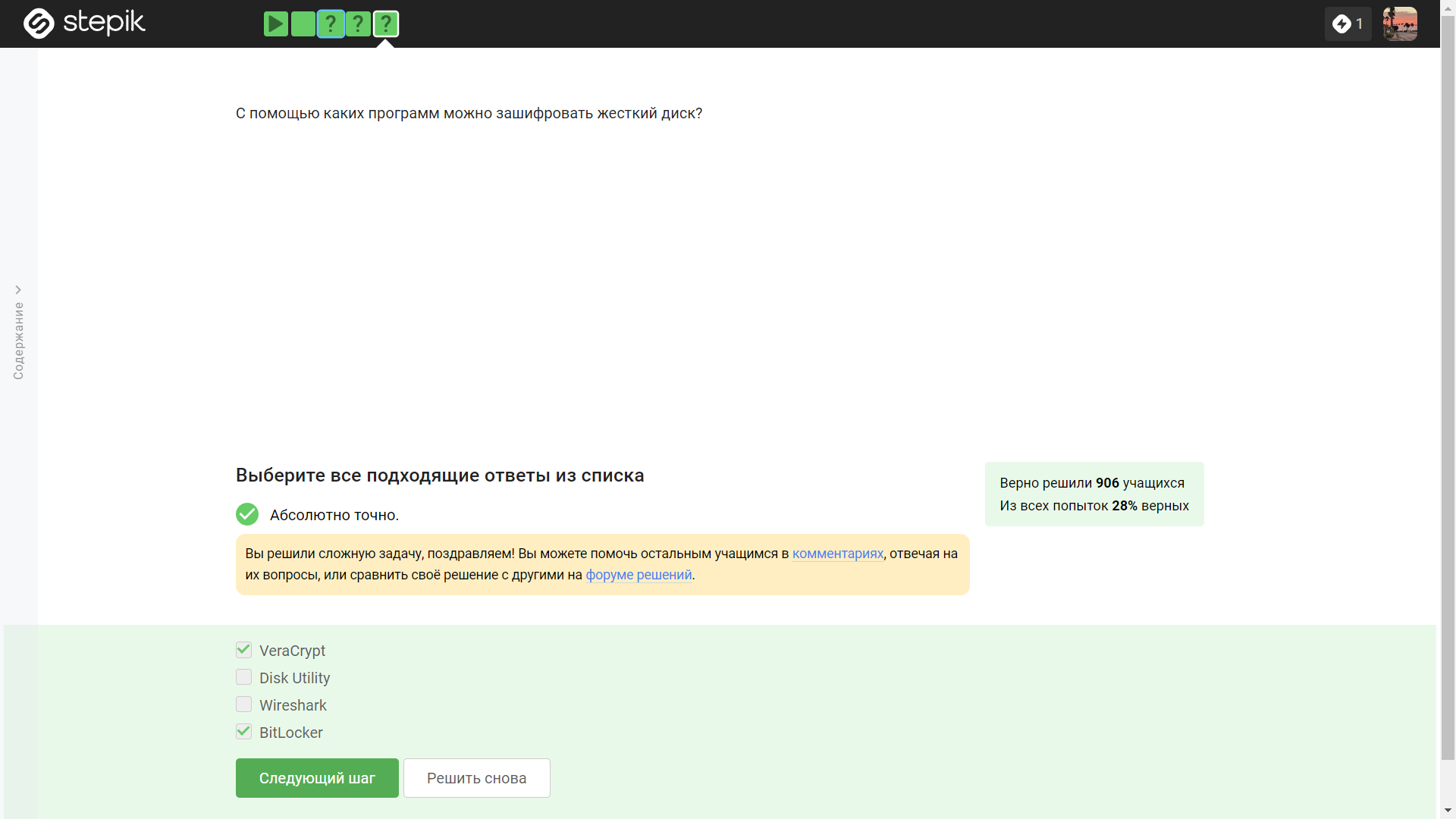


Figure 3: третье задание

1. К стойким паролям обычно относят пароли, содержащие большие и маленькие буквы алфавита, цифры, специальные символы, не имеющие реальной смысловой нагрузки, выберем такой пароль из списка.

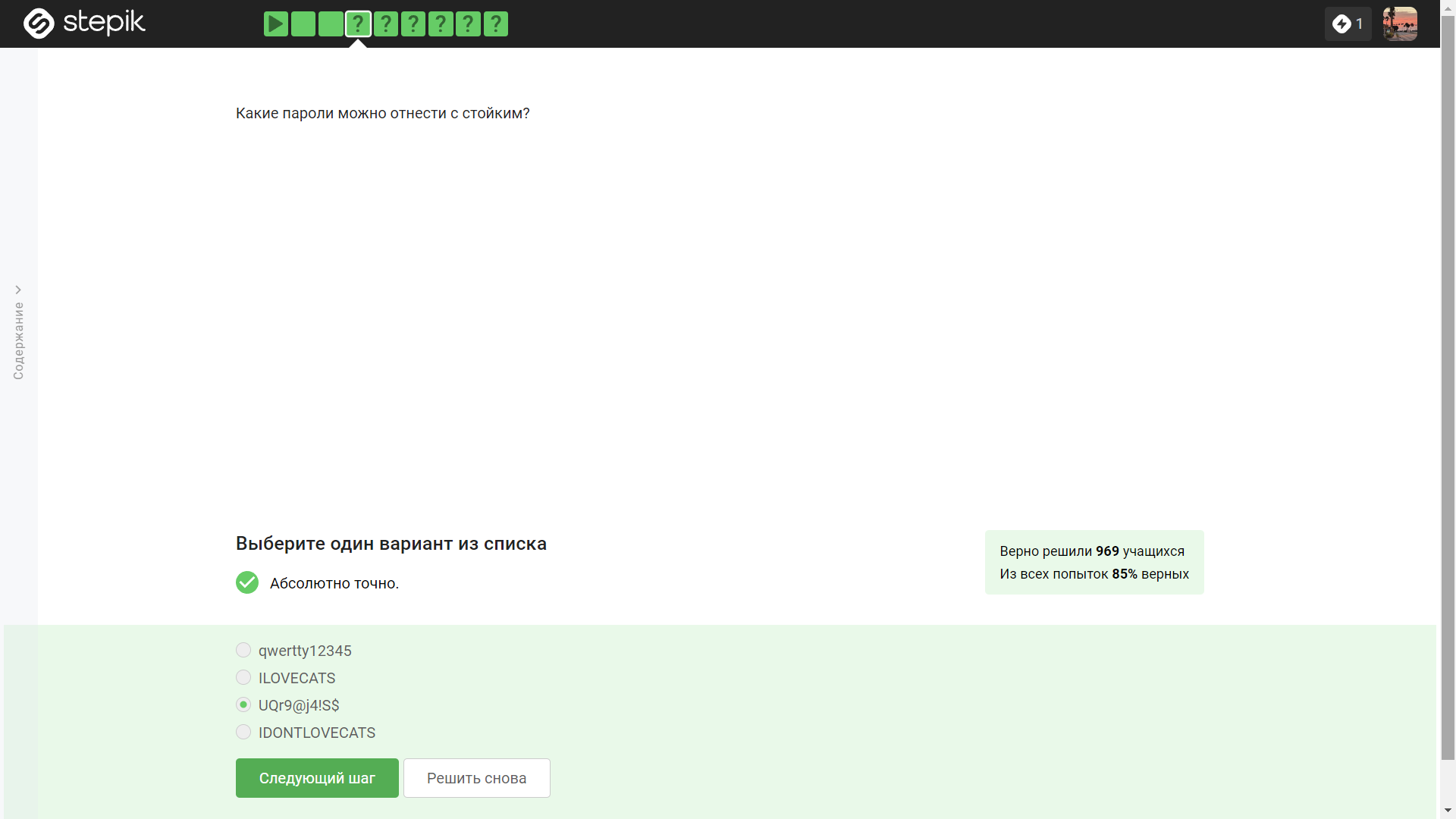


Figure 4: четвертое задание

1. Менеджеры паролей являются самым безопасным методом хранения паролей.

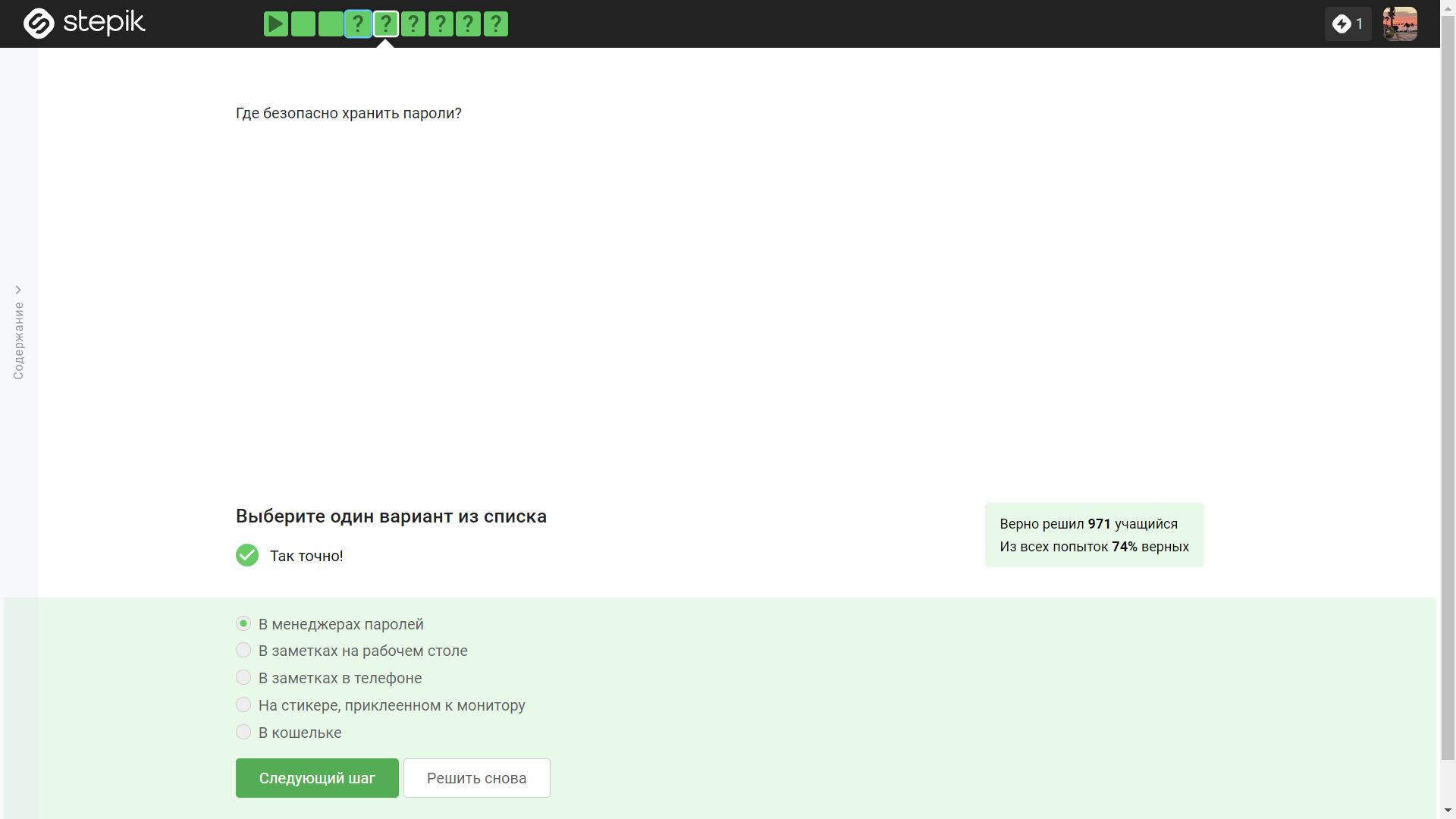


Figure 5: пятое задание

1. Капча нужна для защиты от автоматизированных атак, направленных на получение несанкционированного доступа, она не используется для замены паролей, защиты кук пользователя, безопасного хранения паролей на сервере.

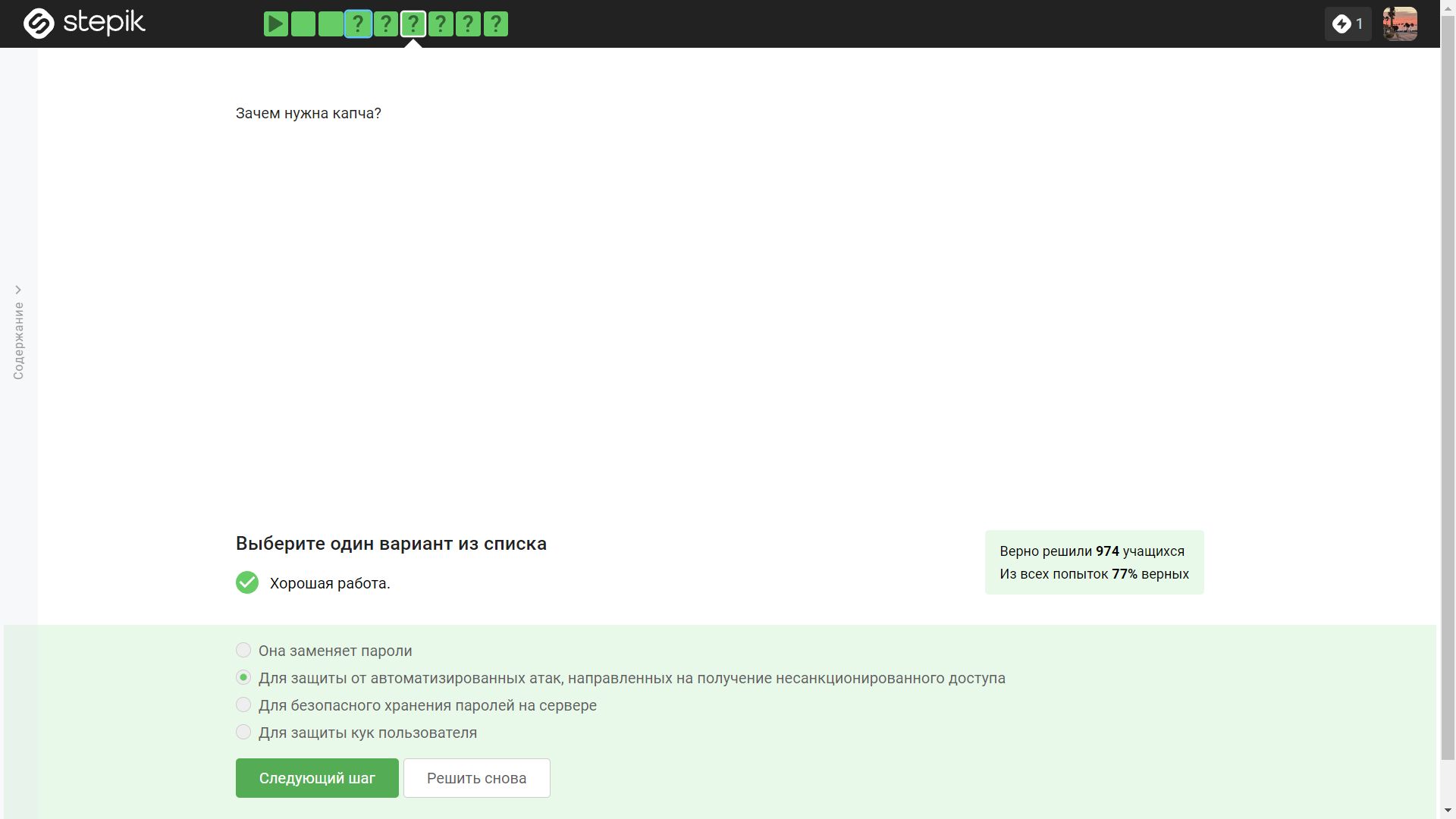


Figure 6: шестое задание

1. Хэширование паролей нужно для того, чтобы не хранить пароли на сервере в открытом виде, для конфиденциальности паролей пользователей.

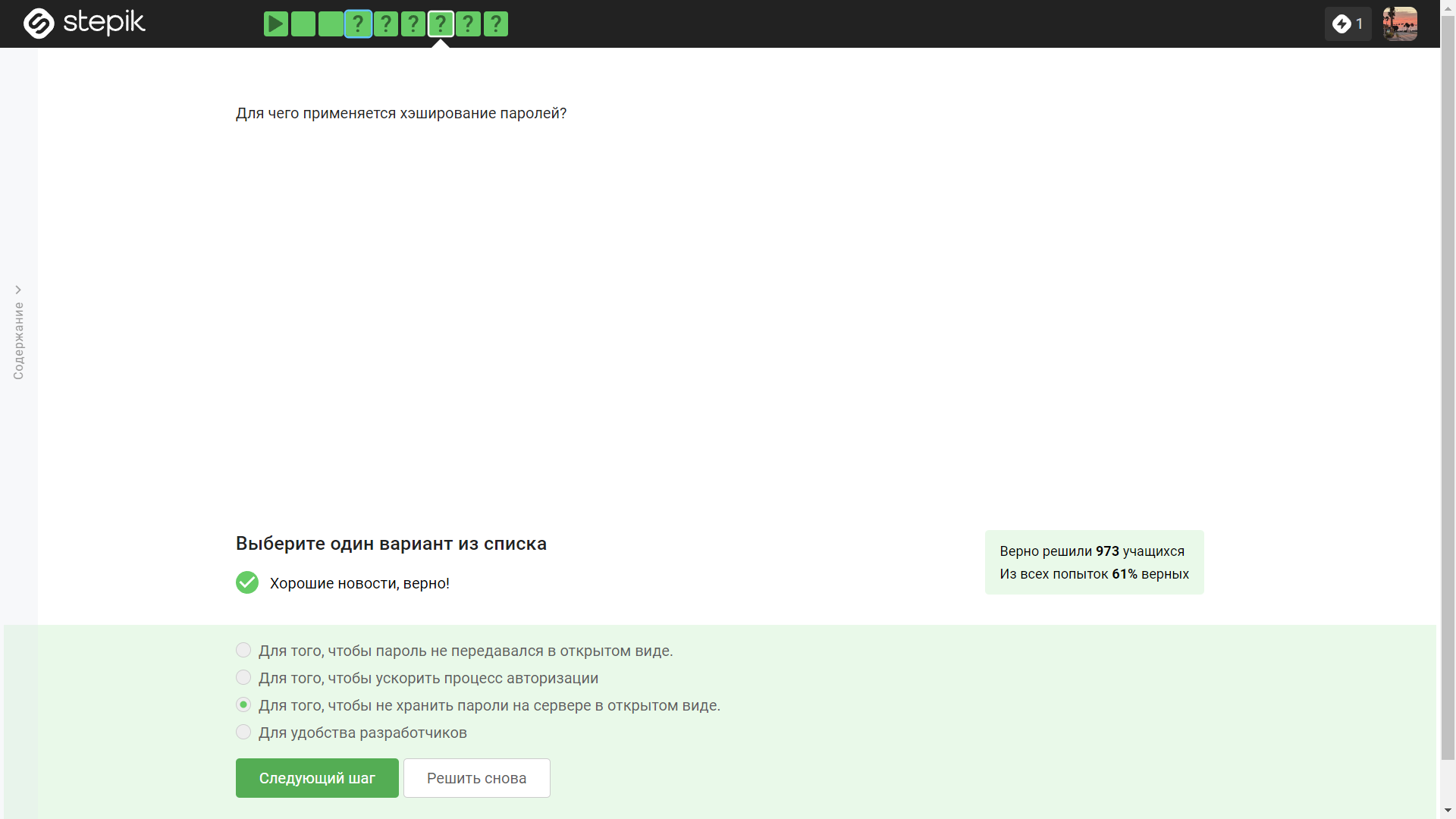


Figure 7: седьмое задание

1. Соль для улучшения стойкости паролей не поможет, если злоумышленник получил доступ к серверу, так как она хранится на сервере.

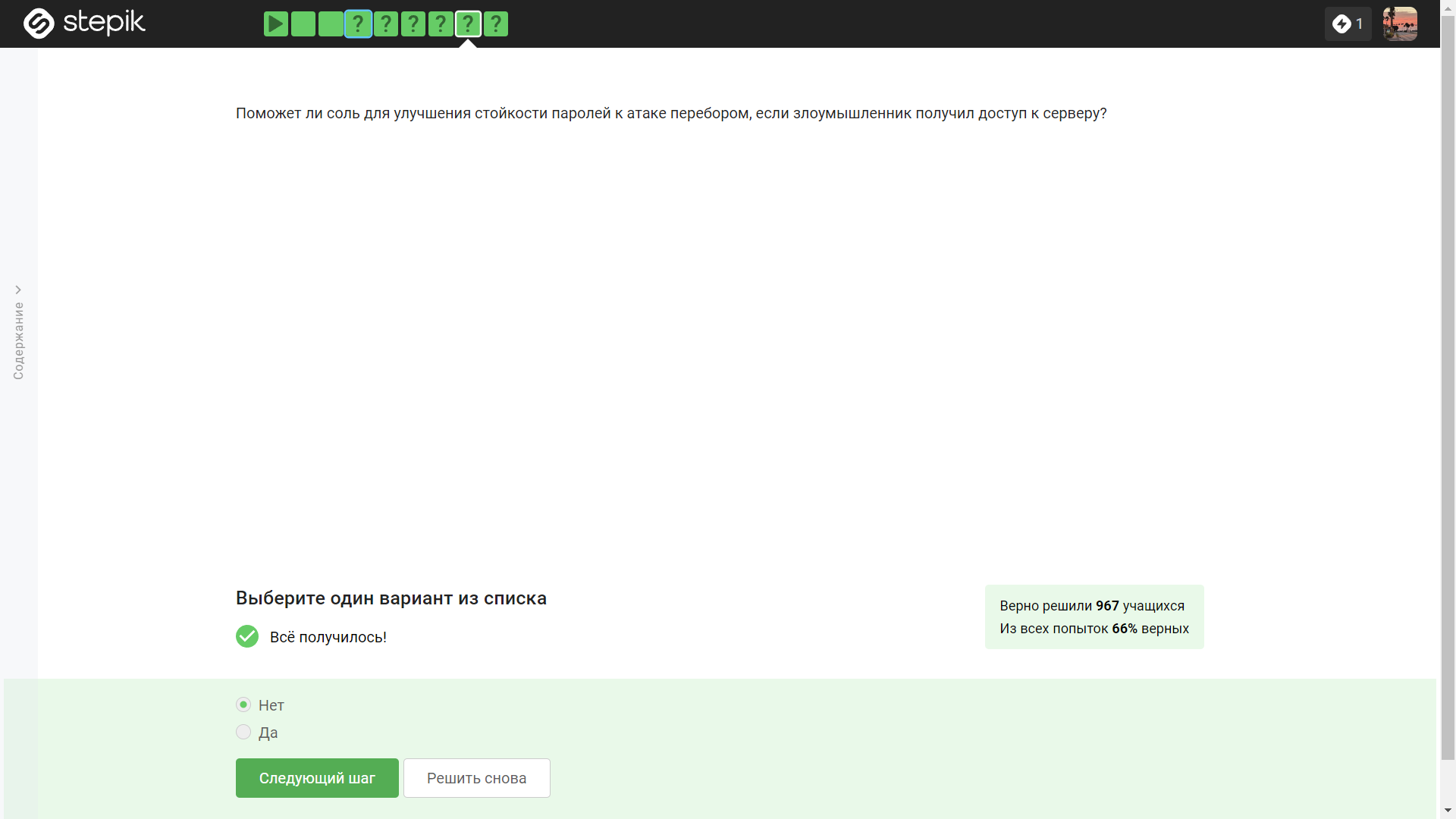


Figure 8: восьмое задание

1. Разные пароли на всех сайтах, периодическая смена паролей, сложные пароли, капча защищают от утечек данных атакой перебором.

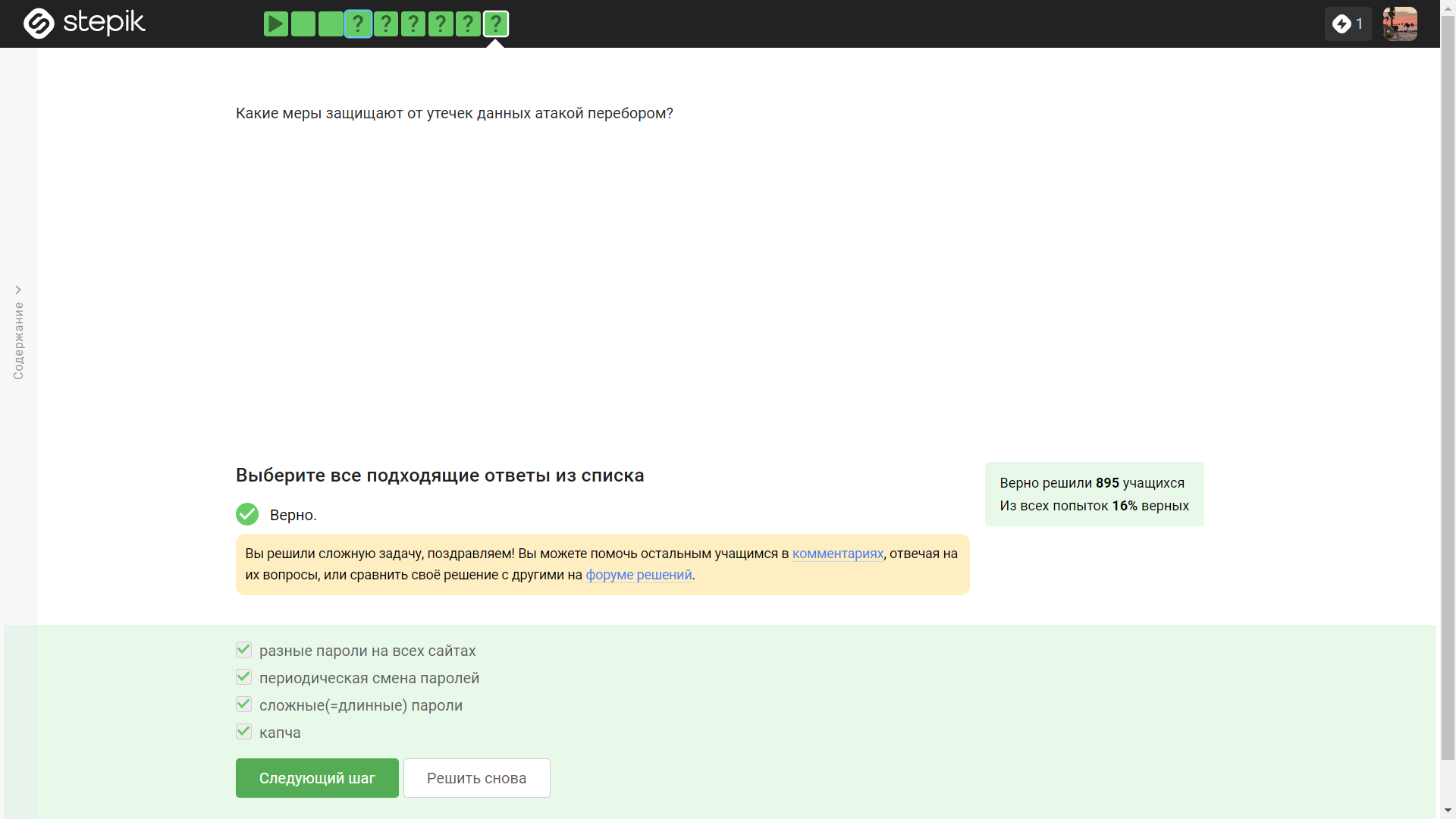


Figure 9: девятое задание

1. Среди представленных ссылок, ссылка для входа в сбербанк и для входа в яндекс являются фишинговыми, так как не имеют никакого отношения к сбербанку и яндексу соответственно.

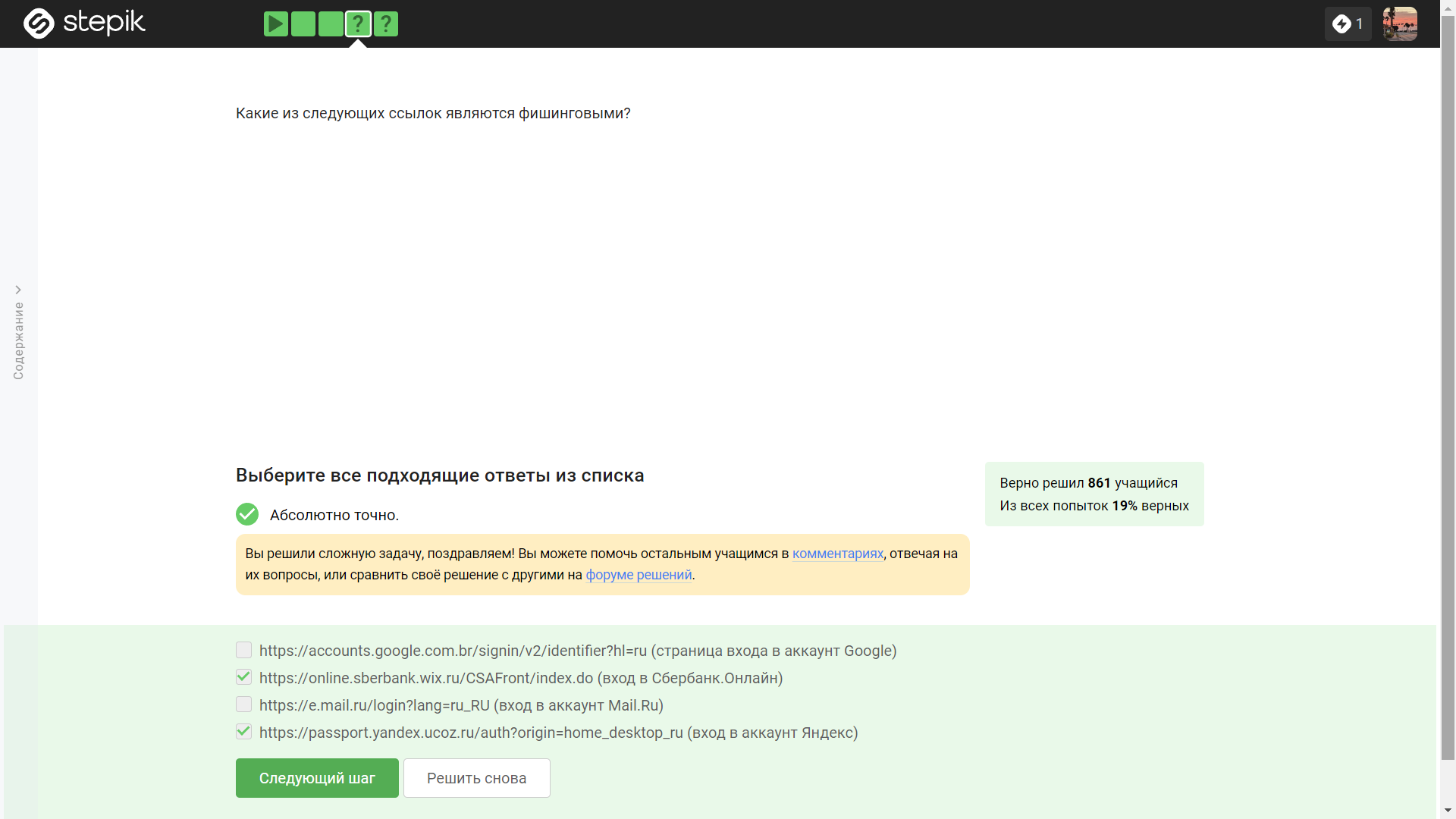


Figure 10: десятое задание

1. Фишинговый имейл может прийти от знакомого адреса, этот вид фишинга называется спуфинг.

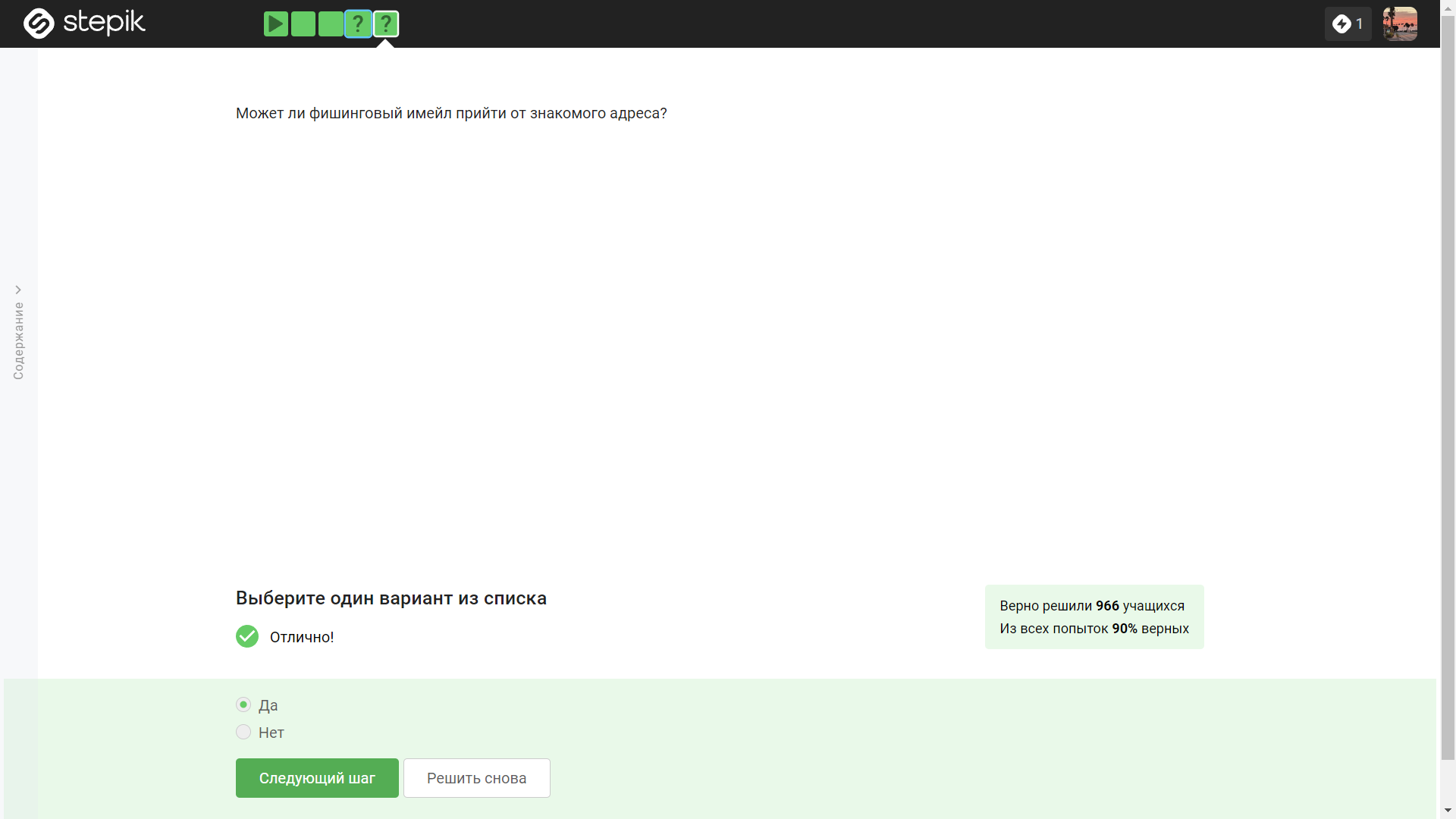


Figure 11: одиннадцатое задание

1. Спуфинг - это подмена адреса отправителя в имейлах, вид фишинга.

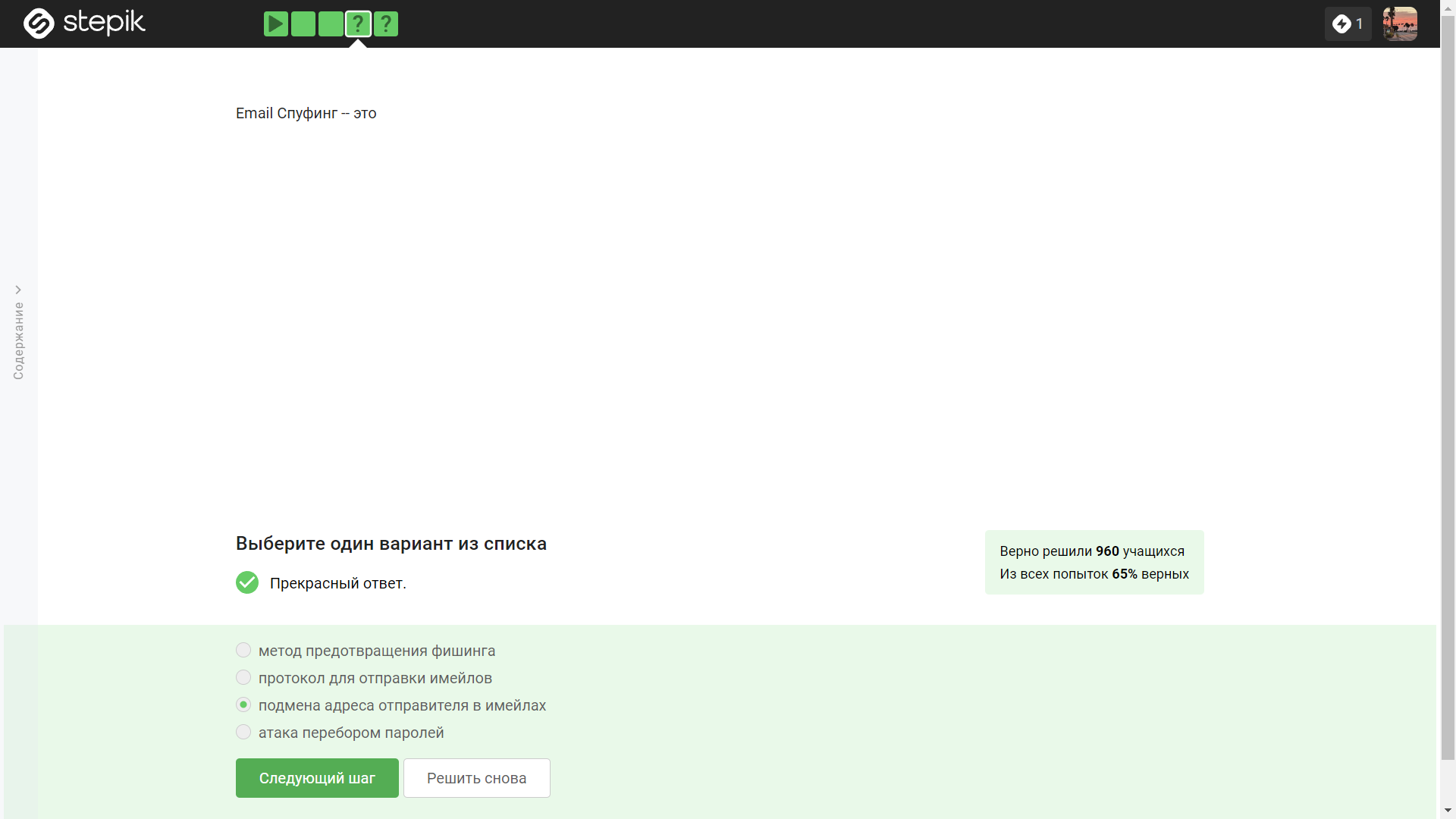


Figure 12: двенадцатое задание

1. Вирус-троян маскируется под легитимную программу, при этом содержа в себе вредоносное ПО.

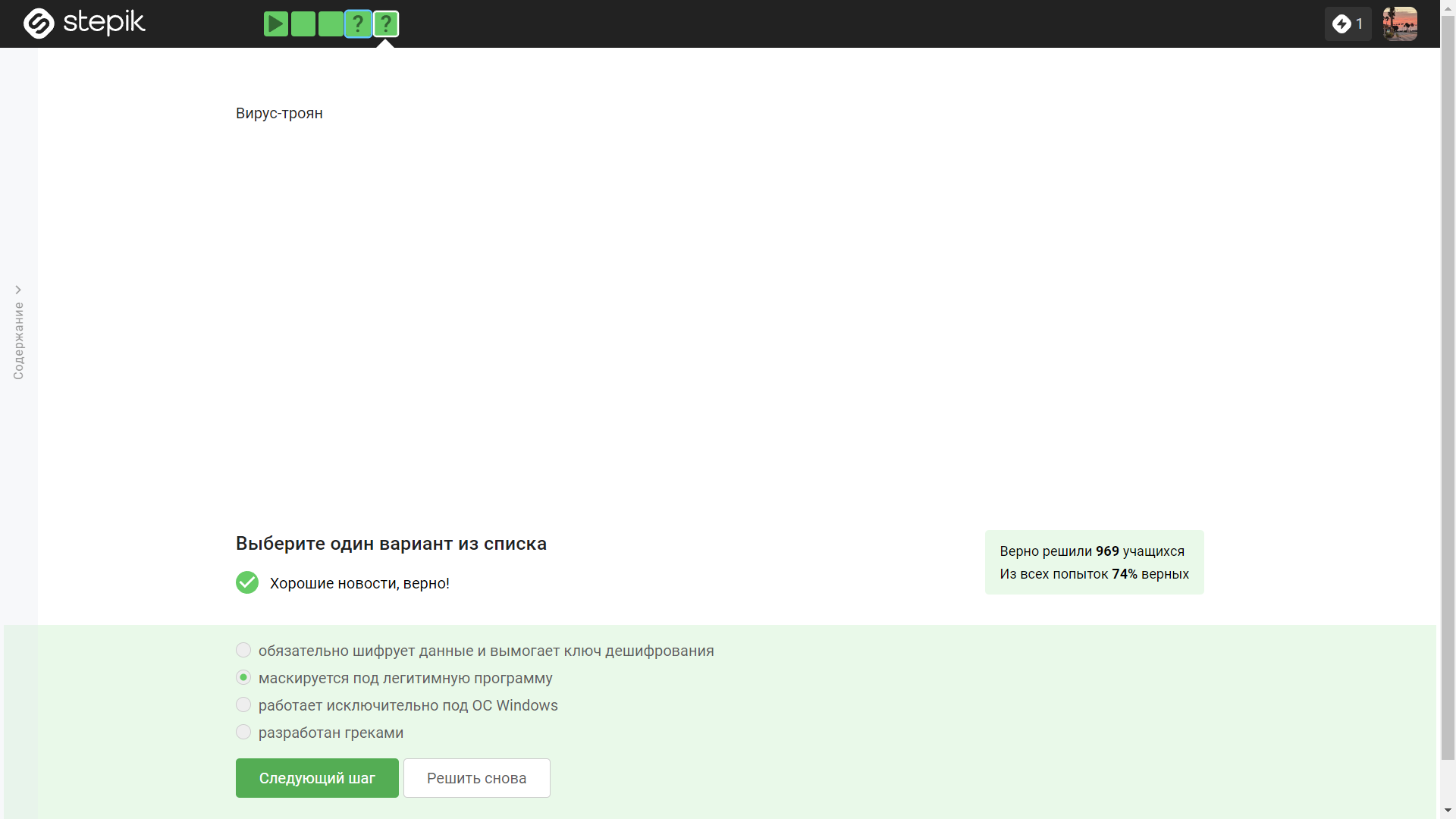


Figure 13: тринадцатое задание

1. В протоколе мессенджеров Signal ключ шифрования формируется при генерации первого сообщения стороной-отправителем.

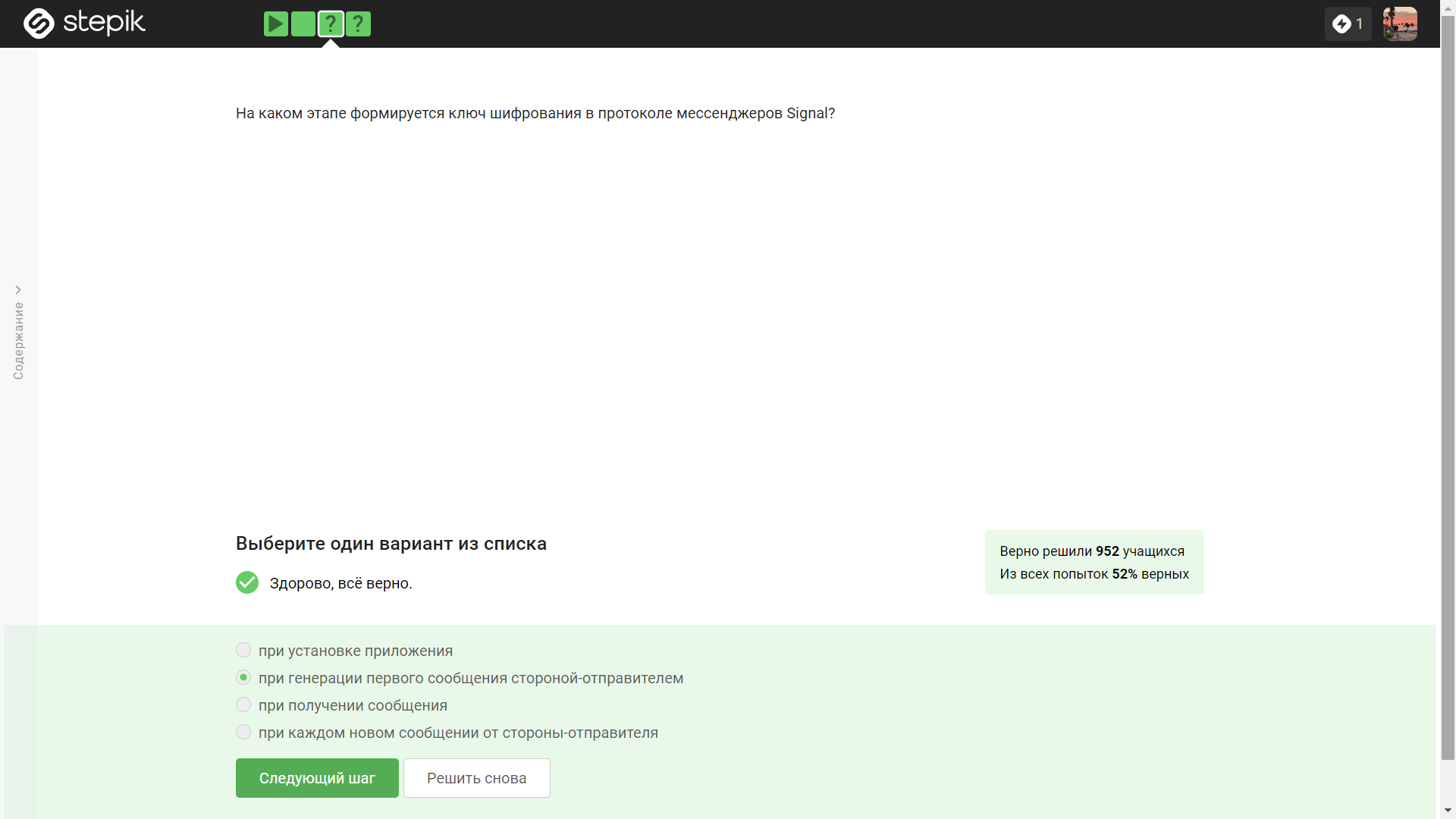


Figure 14: четырнадцатое задание

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

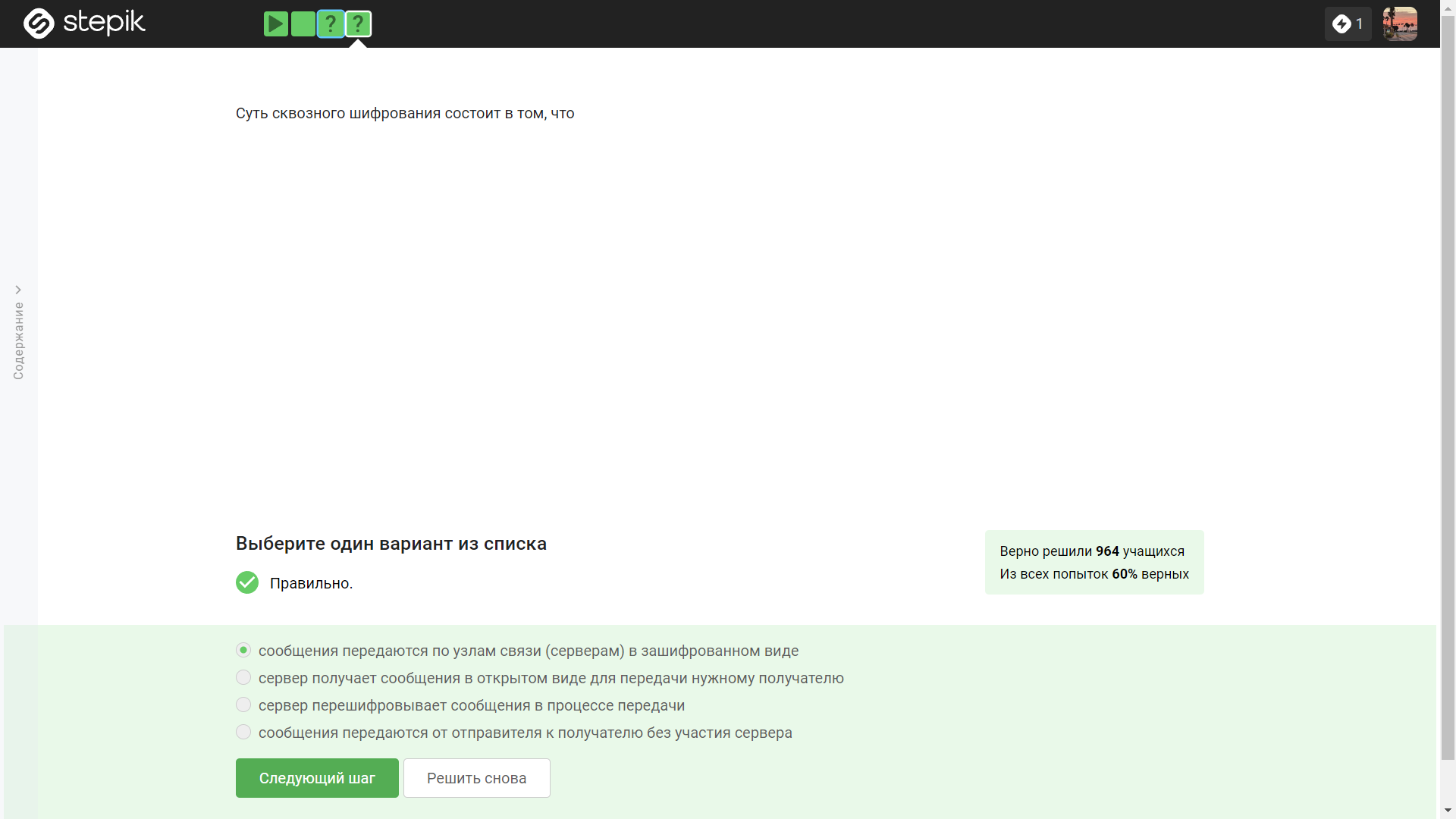


Figure 15: пятнадцатое задание

# 3 Выводы

Я изучил основы защиты данных ПК/телефона.

# 4 Список литературы

Конспекты к лекциям курса “Основы кибербезопасности”.