Внешний курс. Блок 2: Защита ПК/телефона

Дисцеплина: Основы информационной безопасности

Неустроева Ирина Николаевна

Содержание

# 1 Цель работы

Выполненить контрольные задания второго блока “Защита ПК/телефона” внешнего курса “Основы кибербезопасности”.

# 2 Выполнение заданий блока “Основы Кибербезопасности”

## 2.1 Шифрование диска

Шифровать нужно не только жесткий диск, но и загрузочный сектор диска. Ответ-можно (рис. 1).

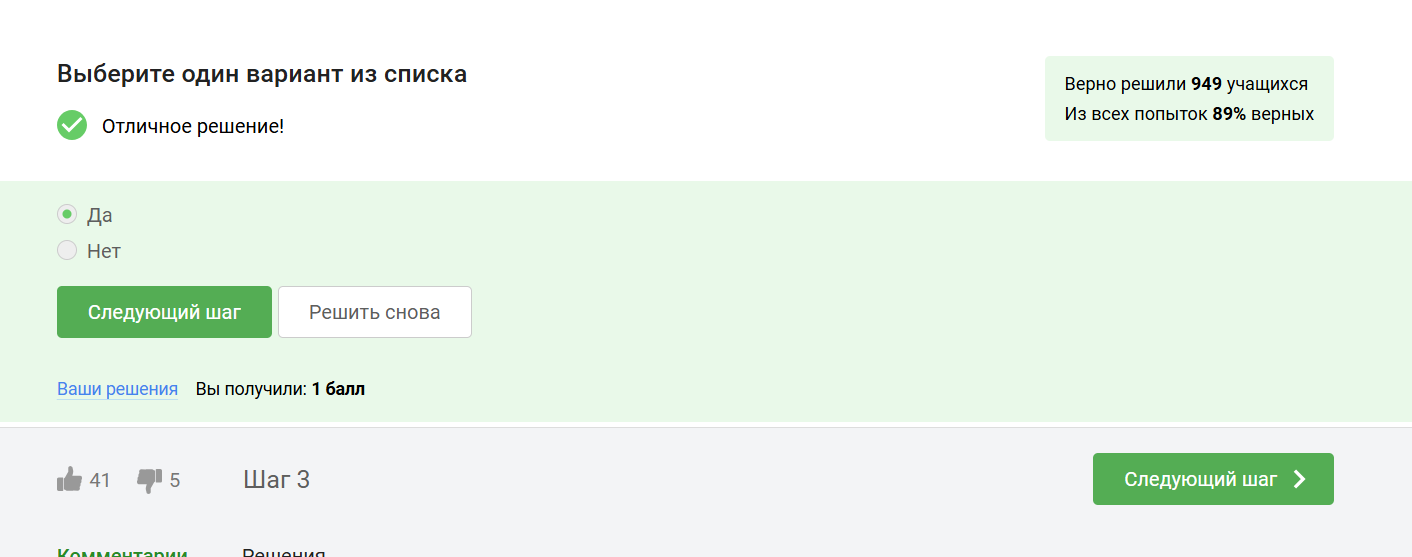


Рис. 1: Вопрос 3.1.1

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

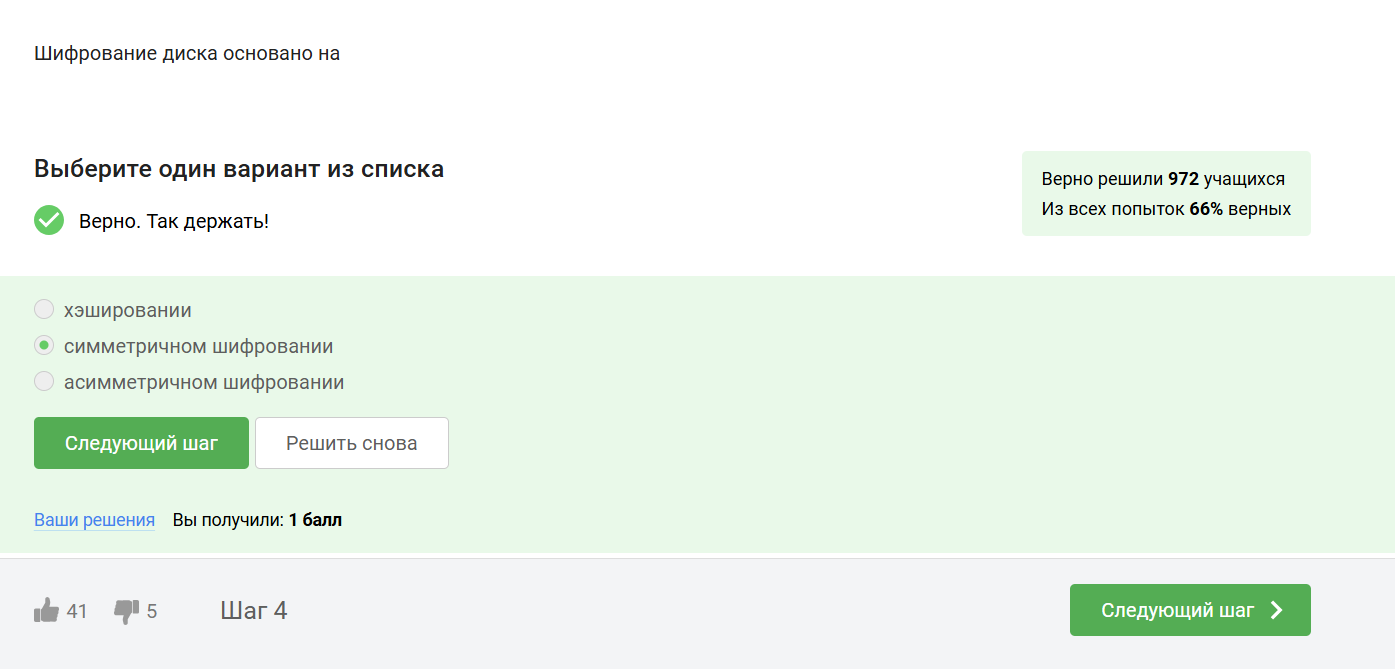


Рис. 2: Вопрос 3.1.2

Популярные ОС имеют встроенные инструменты для шифрования дисков: Windows (Bitlocker), Linux (LUKS), MacOS (FileVault). Также доступны бесплатные опенсорсные альтернативы, такие как Veracrypt и PGPDisk. (рис. 3).

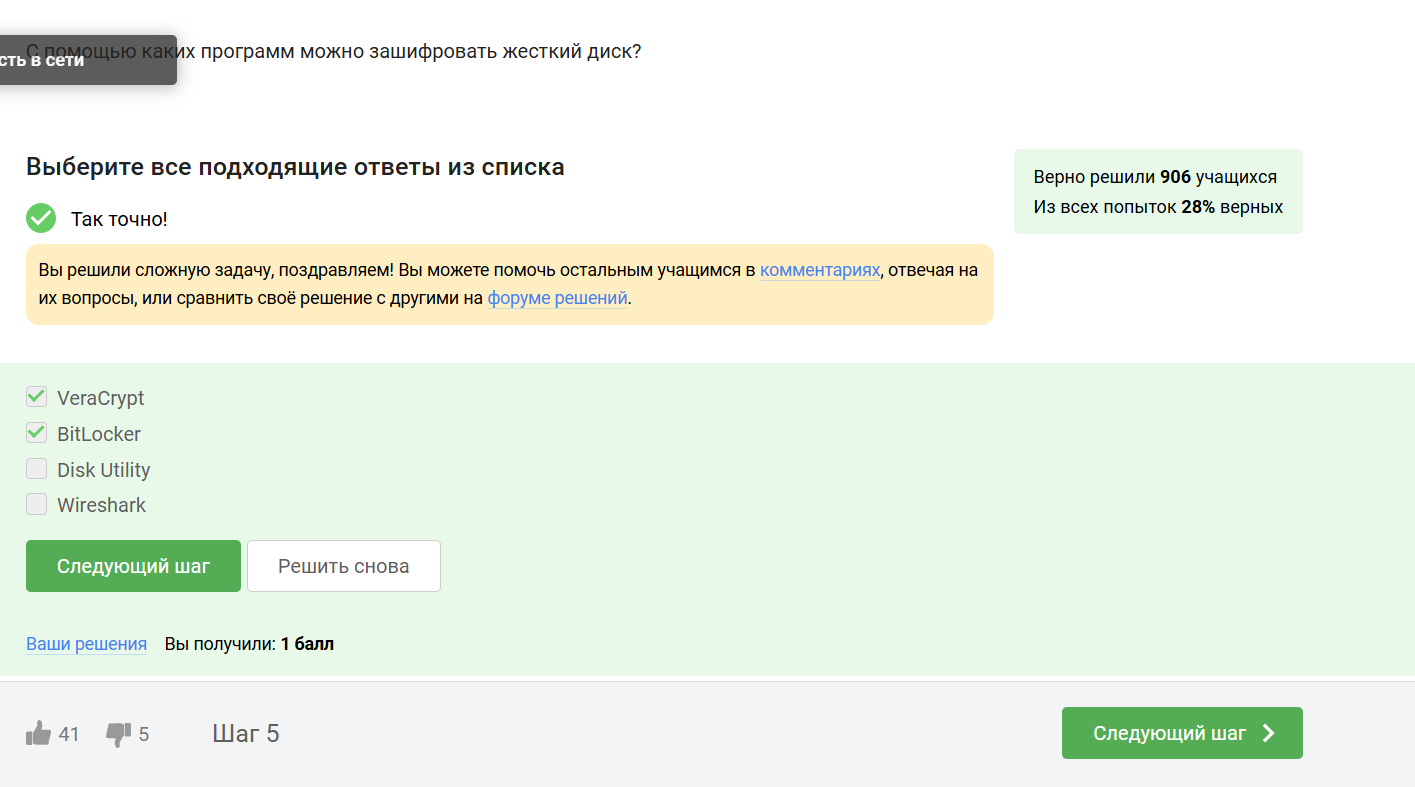


Рис. 3: Вопрос 3.1.3

## 2.2 Пароли

Стойкий пароль содержит цифры стройчные и заглавные буквы и специальные символы. Это усложняет перебор пароля (рис. 4).

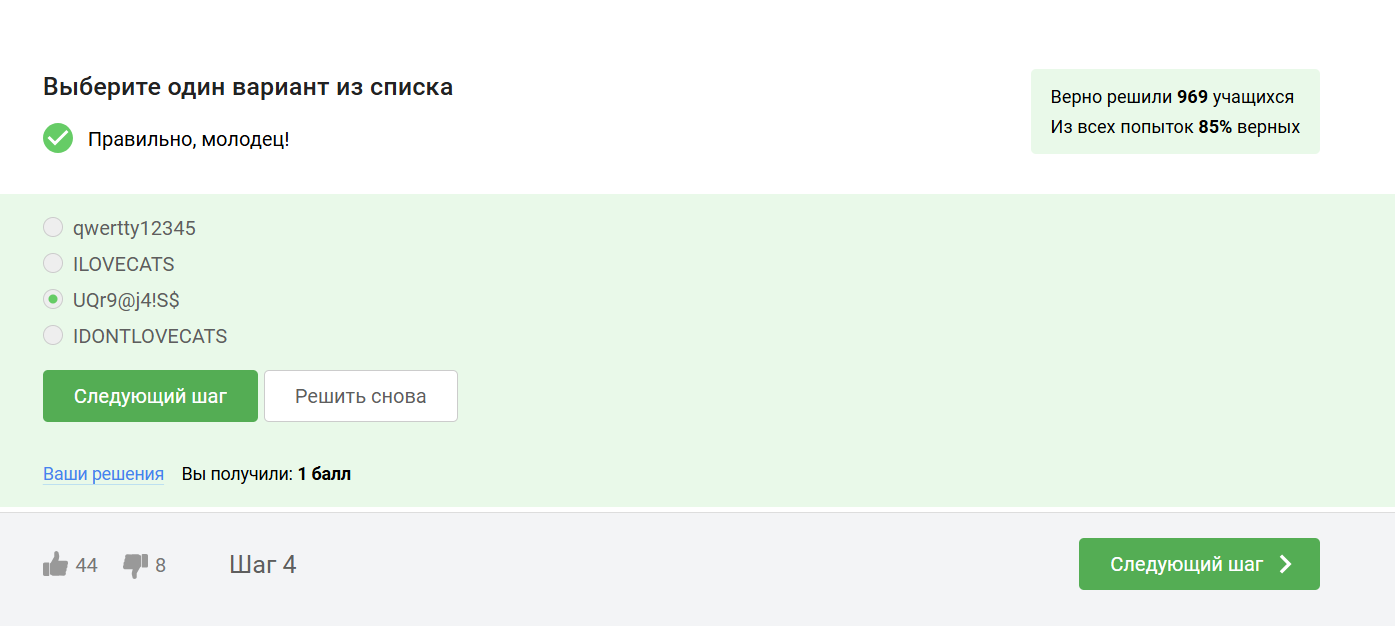


Рис. 4: Вопрос 3.2.1

Безопасно хранить пароли нужно только в месенджерах (рис. 5).

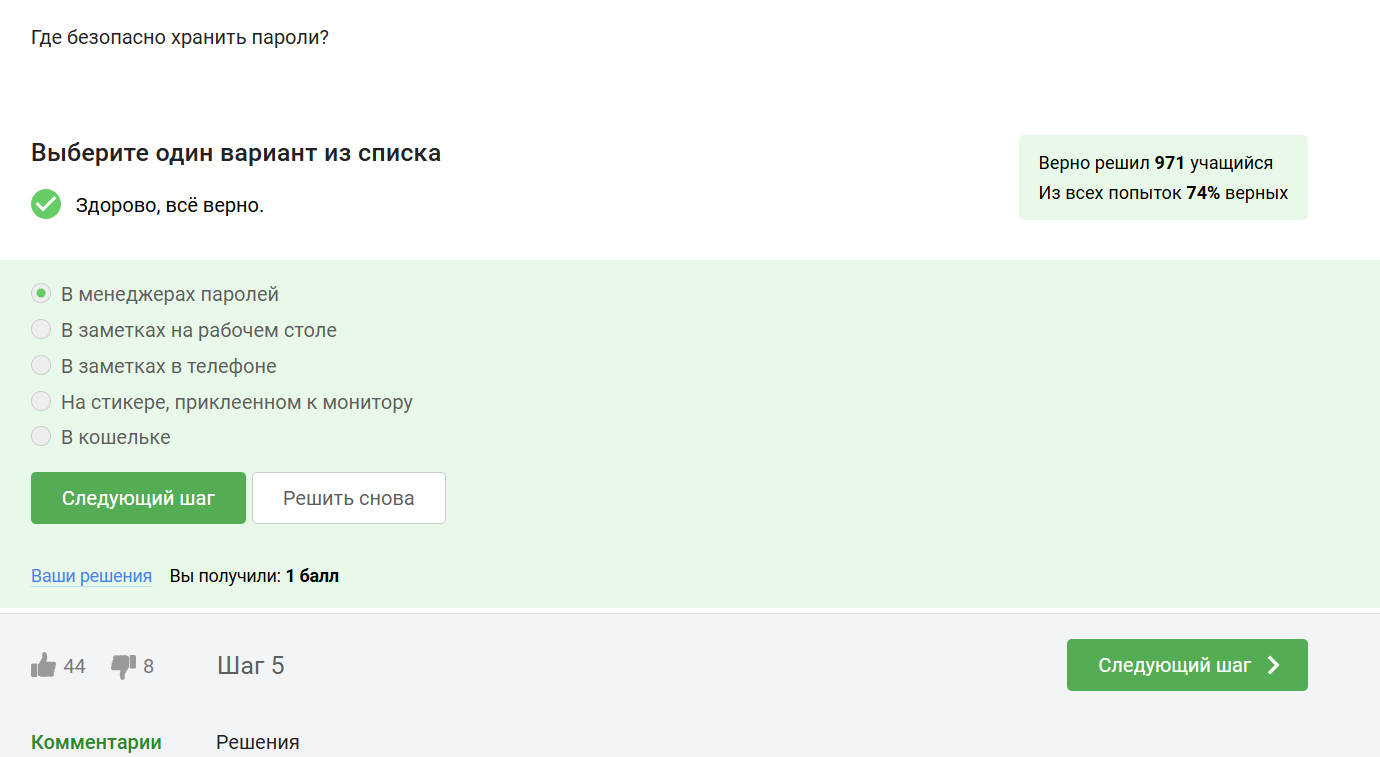


Рис. 5: Вопрос 3.2.2

Капча - тест для определения, кто общается с веб-сервисом, человек или бот(рис. 6).

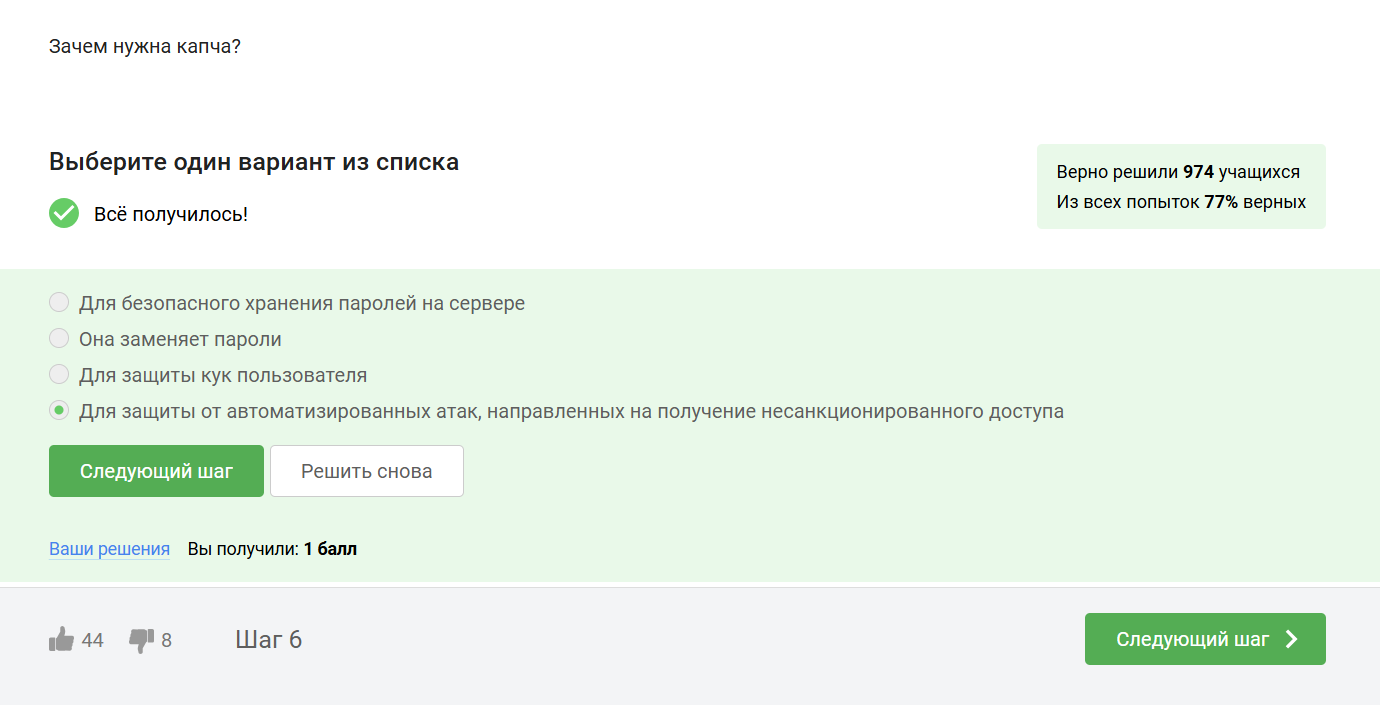


Рис. 6: Вопрос 3.2.3

В целях безопасности пароли хранят не в открвтом виде, а в виде хешей (рис. 7).

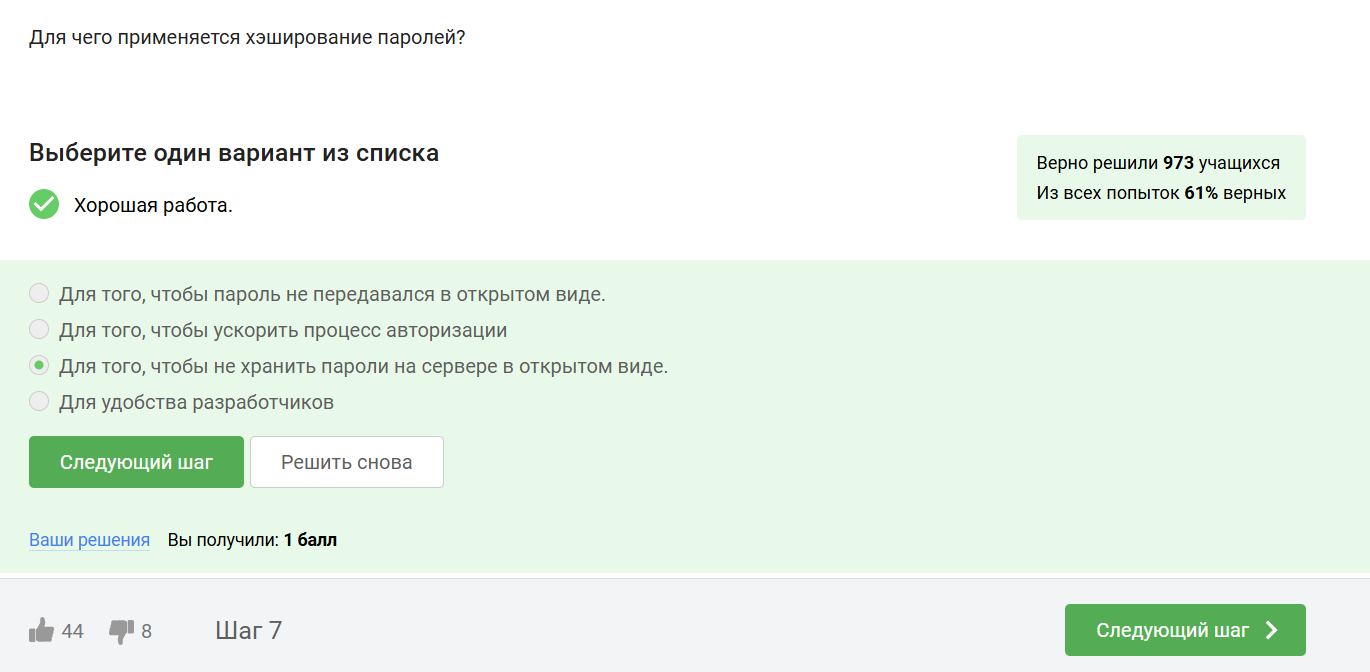


Рис. 7: Вопрос 3.2.4

Соль - это метод защиты слабых паролей. Сервер добавляет соль к паролю пользователя. Это делает взлом слабых паролей сложнее (рис. 8).

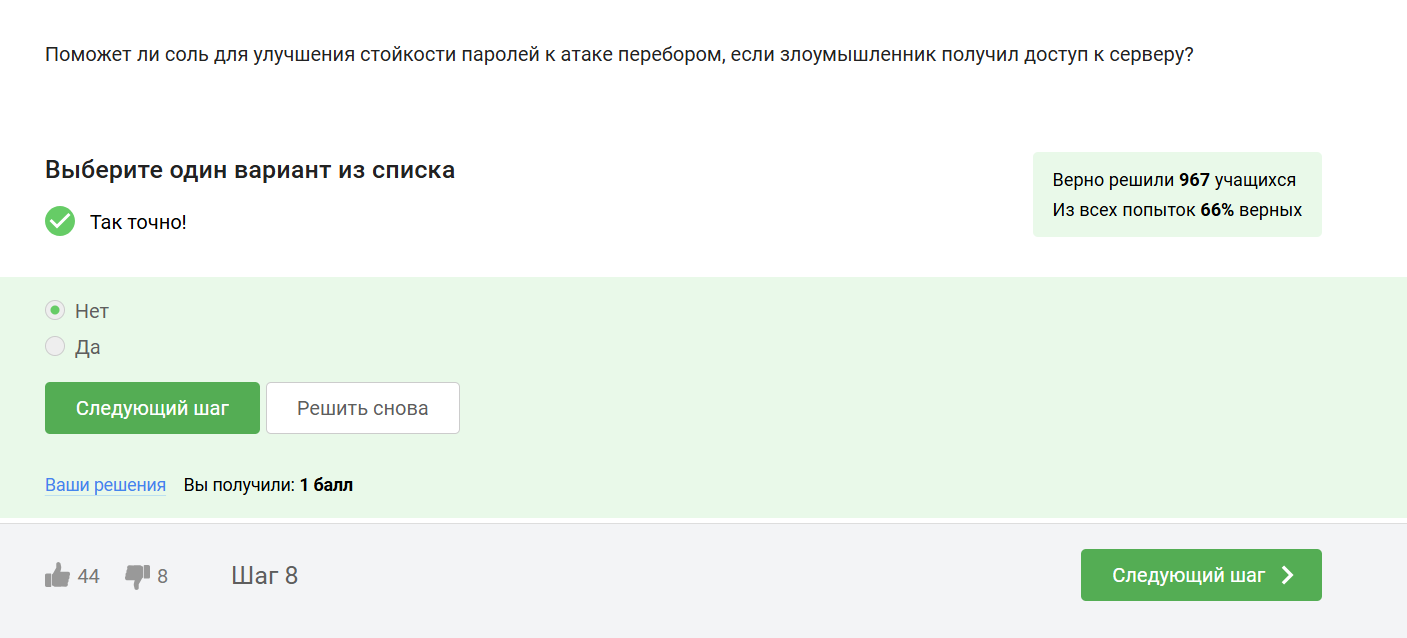


Рис. 8: Вопрос 3.2.5

Для безопасности нужно использовать длинные, сложные пароли, регулярно обновлять и хранить пароли в месенджерах паролей. (рис. 9).

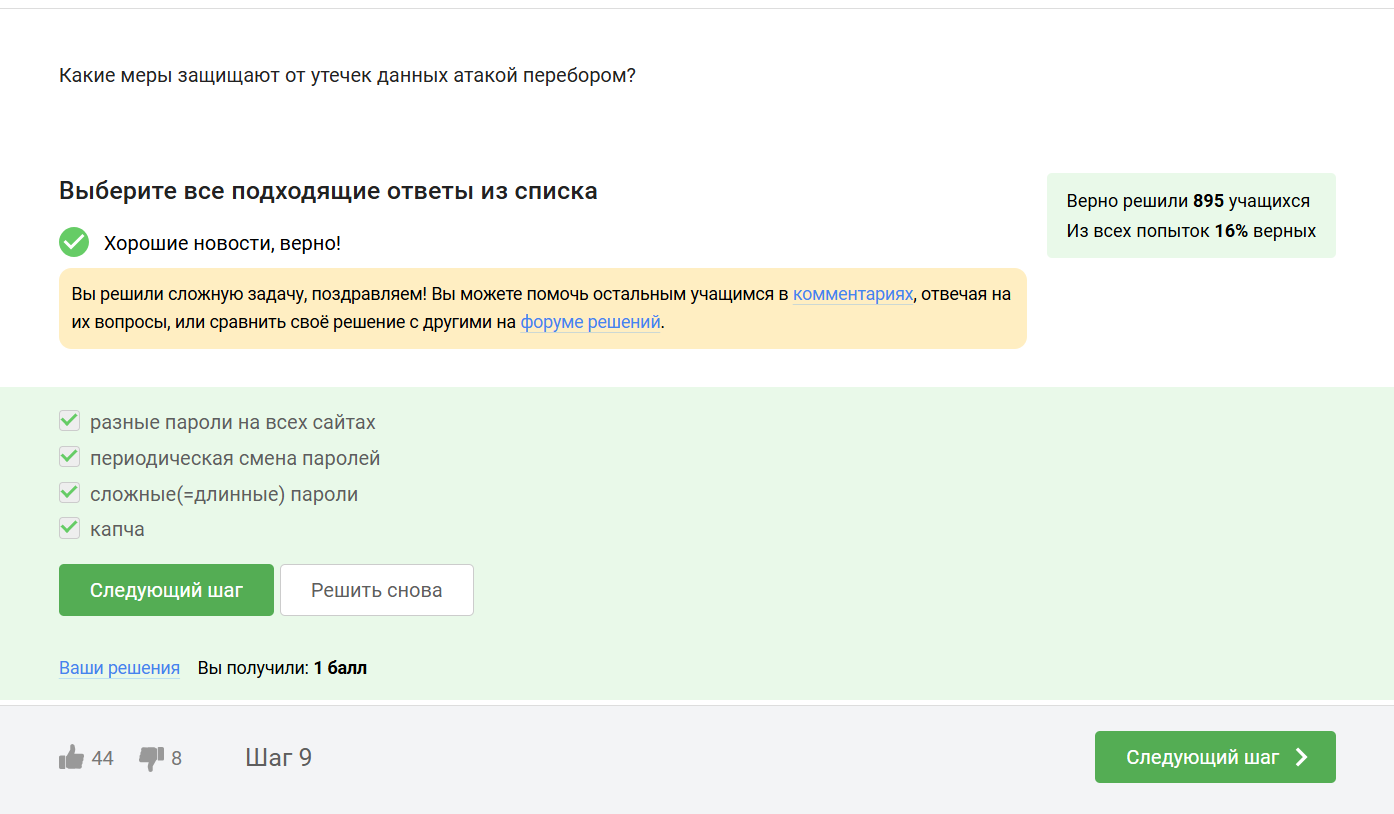


Рис. 9: Вопрос 3.2.6

## 2.3 Фишинг

Пример фишинга - эта маскировка под известные веб-сайты только с другим доменным именем (рис. 10).

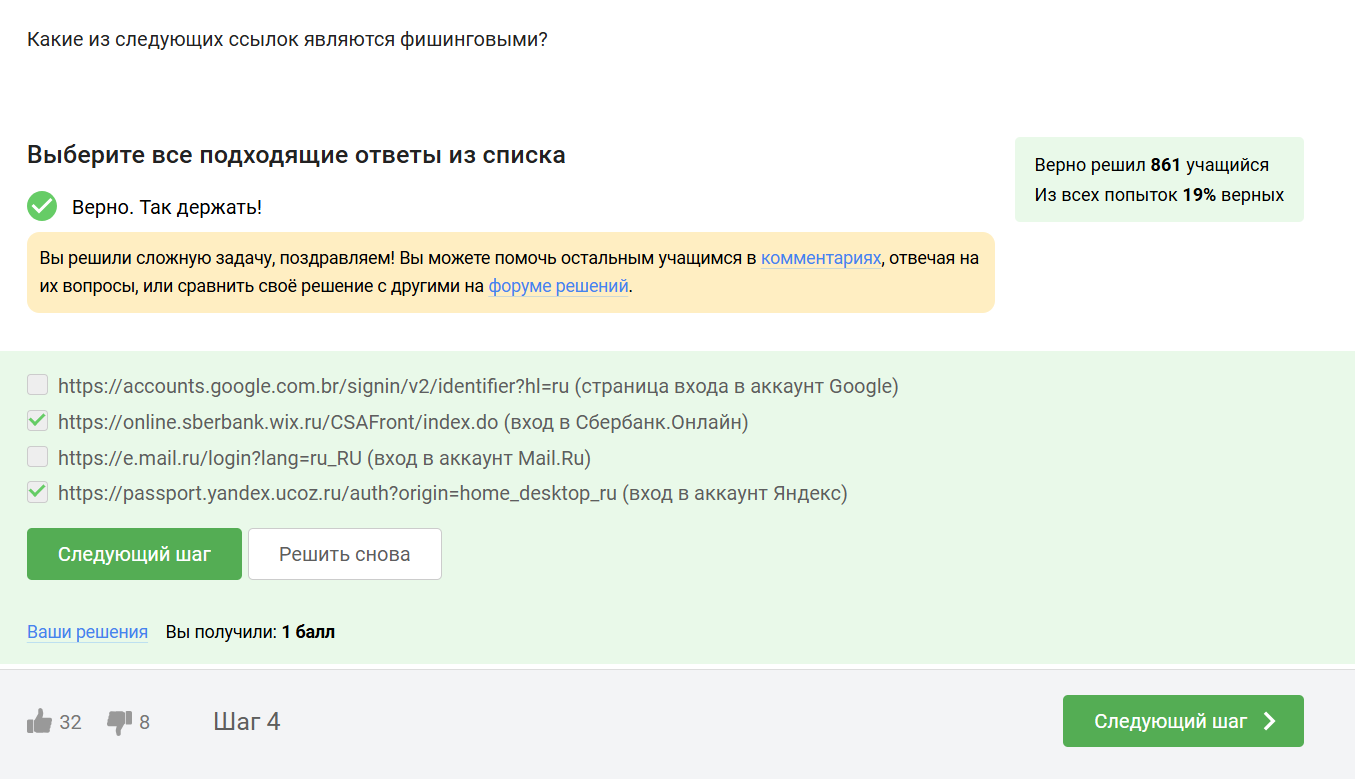


Рис. 10: Вопрос 3.3.1

Может фишинговое письмо прийти и от знакомого(рис. 11).

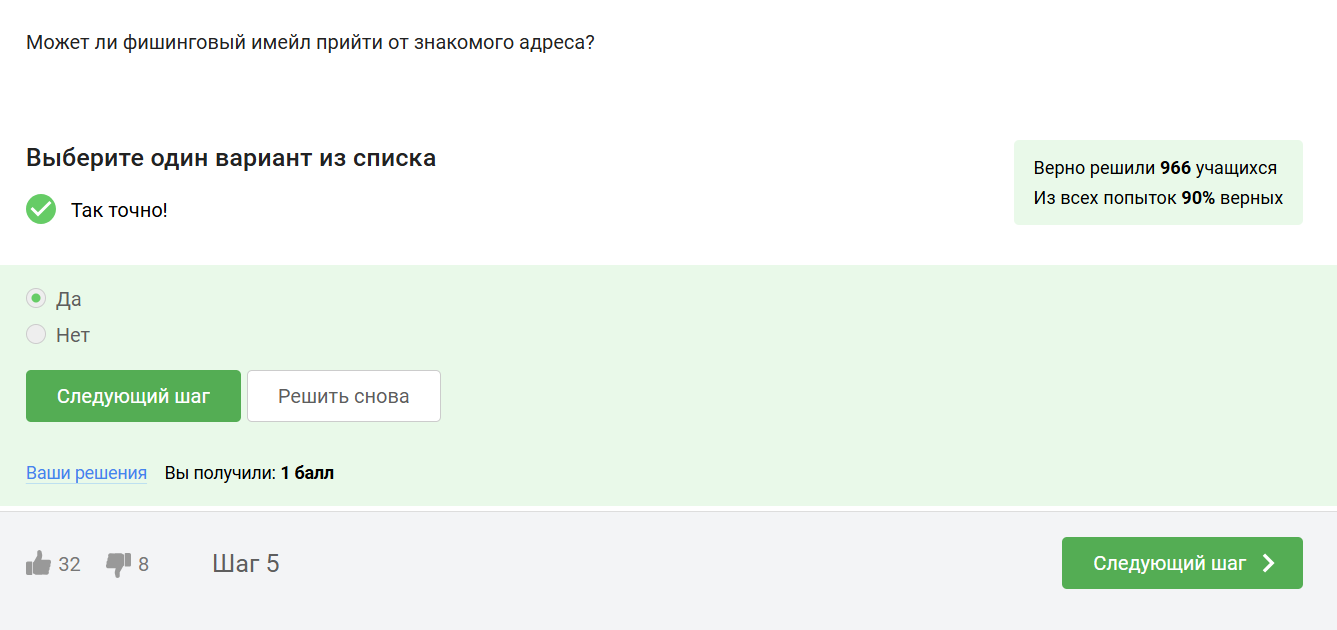


Рис. 11: Вопрос 3.3.2

## 2.4 Вирусы.

Спуфинг - это подмена адреса отправителя в имейлах (рис. 12).

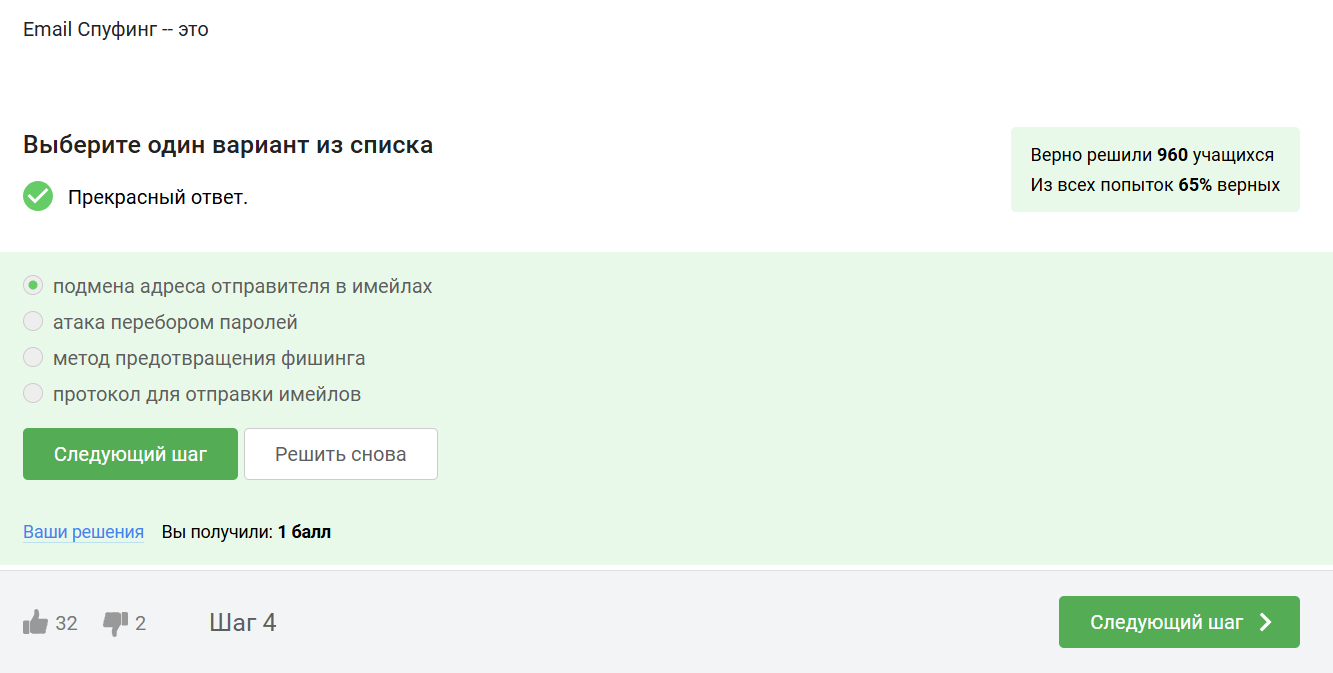


Рис. 12: Вопрос 3.4.1

Троян маскируется под обыкновенную безобидную программу, при запуске которой вирус легко проникает в ваш компьютер и поражает его(рис. 13).

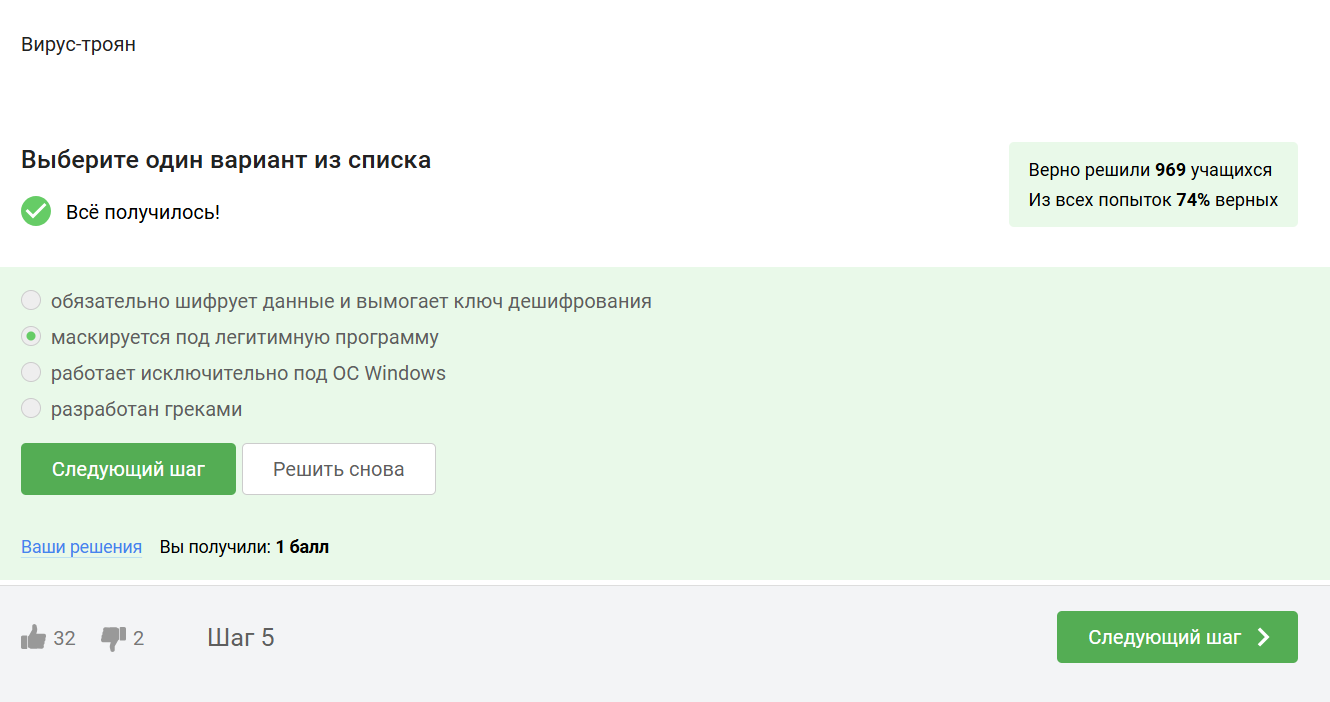


Рис. 13: Вопрос 3.4.2

## 2.5 Безопасность мессенджеров

При генерации первого сообщения отправителем формируется ключ шифрования (рис. 14).

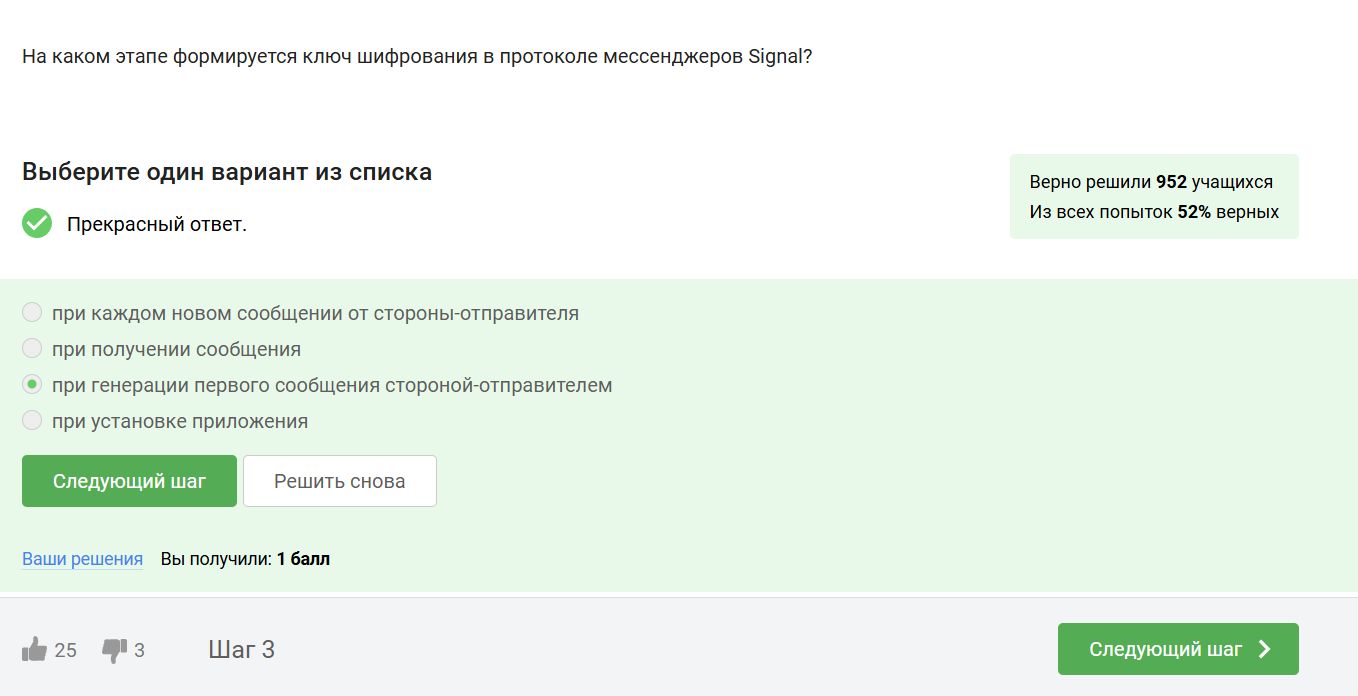


Рис. 14: Вопрос 3.5.1

Сквозное шифрование позволяет передавать сообщения между пользователями (Алиса и Боб) так, что сервер знает только адресата, но не может прочитать содержимое. Алиса шифрует сообщение, сервер передает шифрованный текст Бобу, а Боб его расшифровывает. Сервер не имеет доступа к ключам или открытому тексту сообщения. (рис. 15).

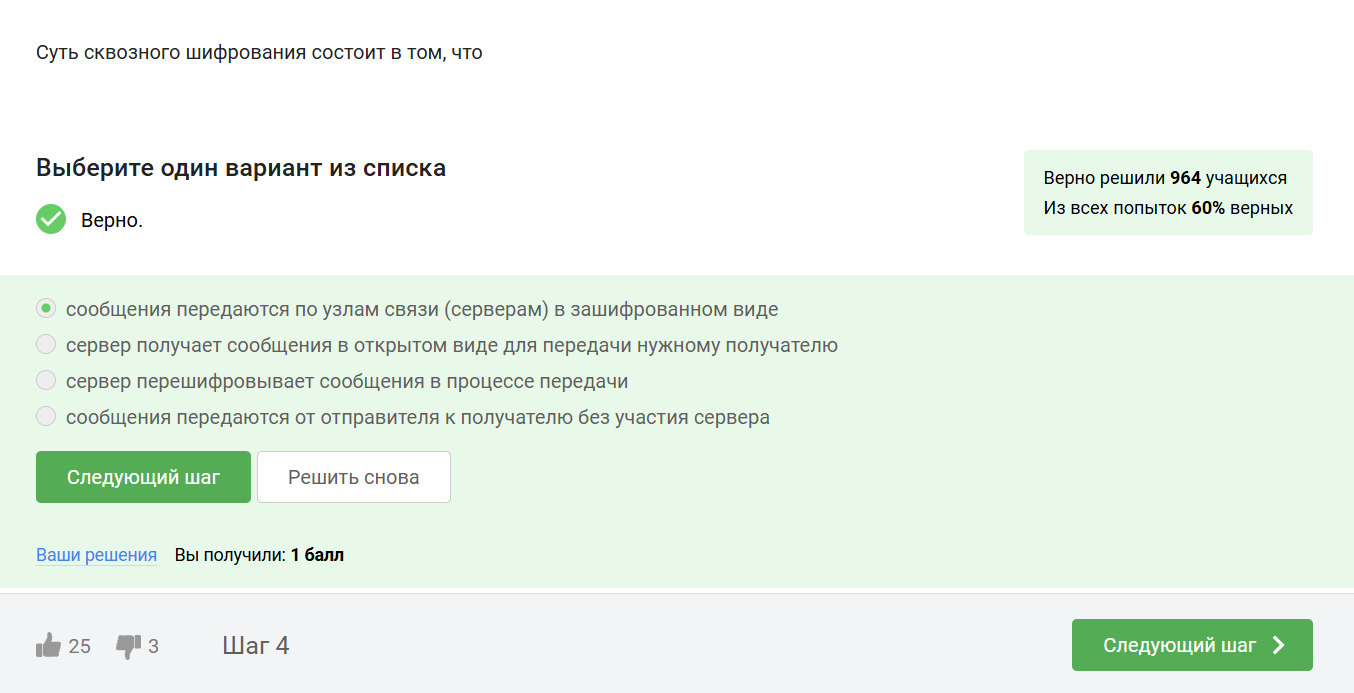


Рис. 15: Вопрос 3.5.1

# 3 Выводы

В результате я сделала второй блок курса “Основы кибербезопасности”. Узнала правила составления и хранения паролей, поняла много нового о вирусах и мерах безопасности против них.