Прохождения внешнего курса на тему Основы кибербезопасности. Часть 2

Основы информационной безопасности

Тойчубекова Асель Нурлановна

Содержание

# 1 3 Защита ПК/телефона

## 1.1 3.1 Шифрование диска

Вопрос/Ответ 1 (рис. 1)

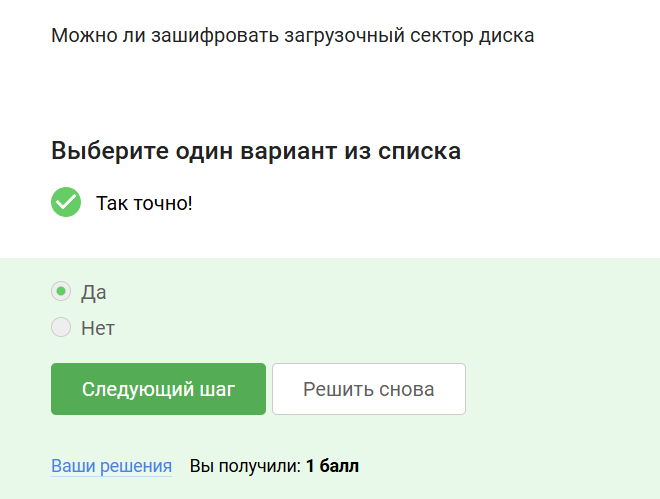


Рис. 1: Вопрос/Ответ 1

Пояснение ответа: Шифровать можно(и нужно) отдельные сектора диска(включая загрузочный сектор), флэшки с конфиденциальными данными.

Вопрос/Ответ 2 (рис. 2)

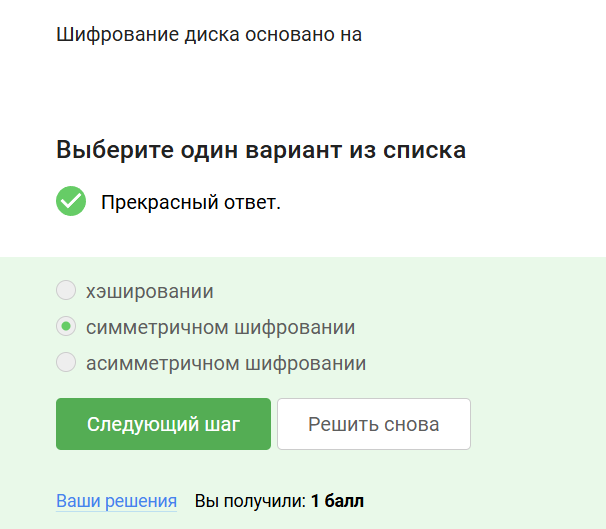


Рис. 2: Вопрос/Ответ 2

Пояснение ответа: Метод шифрования:

* Для процедуры Encrypt/Decrypt используется симметрические шифрования (AES)
* Данные шифруются секторами
* Шифрование ускоряется TMP криптопроцессом
* Шифровать можно и загрузочный сектор. При этом пользователь должен запомнить пароль для дешифрирование ключа.

Вопрос/Ответ 3 (рис. 3)

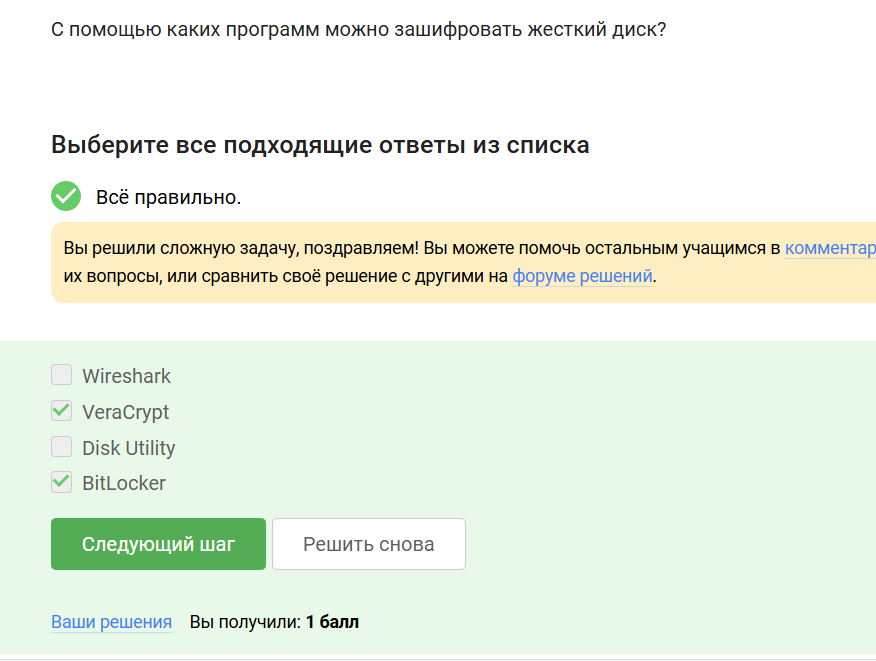


Рис. 3: Вопрос/Ответ 3

Пояснение ответа: Программы,с которыми можно зашифровать жесткий диск: VeraCrypt, BitLocker, LUKC, FileVault.

## 1.2 3.2 Пароли

Вопрос/Ответ 1 (рис. 4)

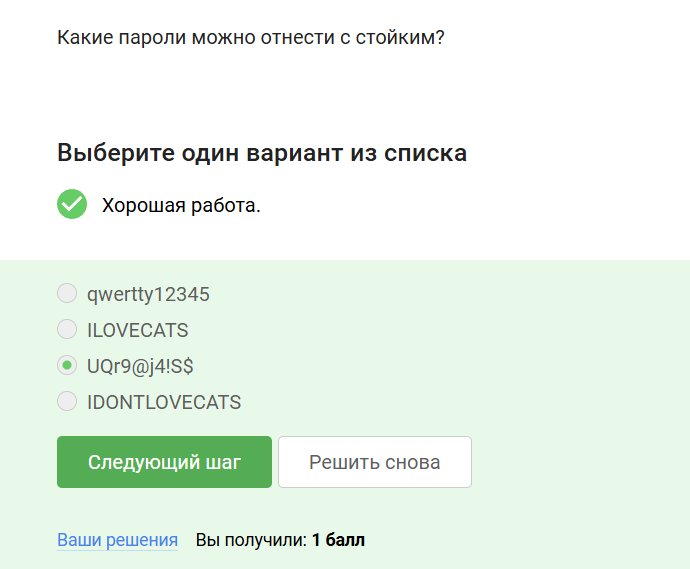


Рис. 4: Вопрос/Ответ 1

Пояснение ответа: Пароль считается стройким если в нем используются множество видов символов(буквы, цифры, знаки, буквы в большом регистре), чем больше видов, тем больше нужно переборов, чтобы его взломать.

Вопрос/Ответ 2 (рис. 5)

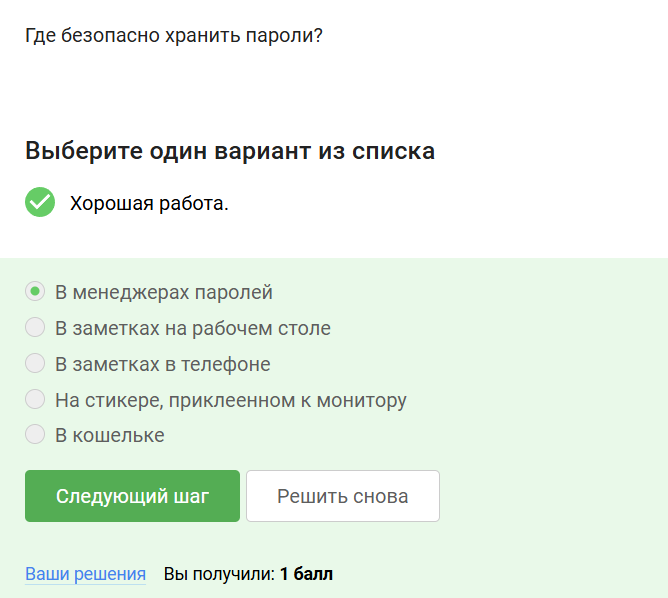


Рис. 5: Вопрос/Ответ 2

Пояснение ответа: Наиболее безопасным является хранение паролей именно в менеджерах паролей.

Вопрос/Ответ 3 (рис. 6)

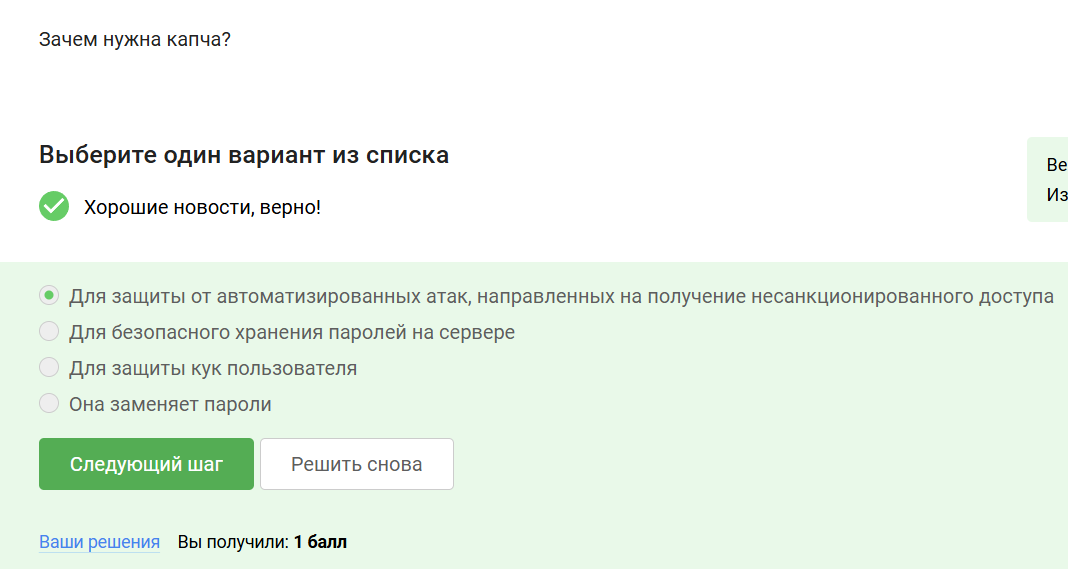


Рис. 6: Вопрос/Ответ 3

Пояснение ответа: Капча проверяет пользователя не является ли он программой перебора данных для взлома, обычно используются разные методы, такие как: нахождения правильной картинки или набора букв/цифр. Итак, капча защищает от автоматизированных атак, направленные на получение несанкционированного доступа.

Вопрос/Ответ 4 (рис. 7)

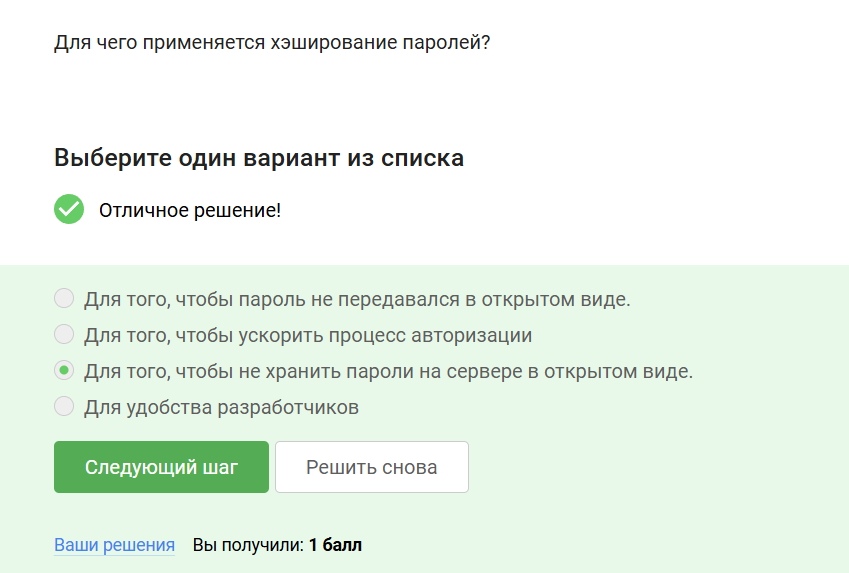


Рис. 7: Вопрос/Ответ 4

Пояснение ответа: Хеширование паролей используется для того, чтобы не хранить паролина сервере в открытом виде, это делается для безопасности.

Вопрос/Ответ 5 (рис. 8)

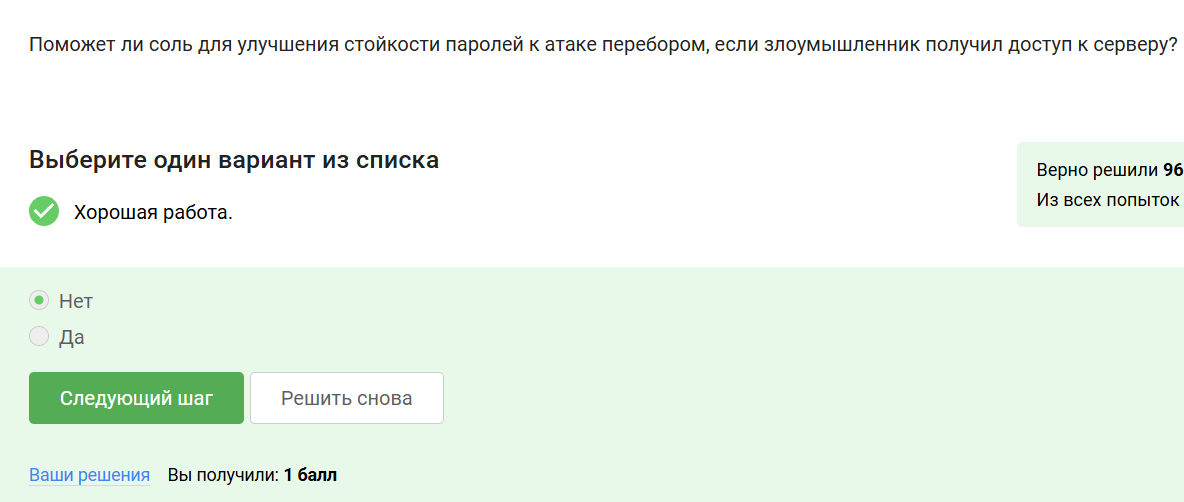


Рис. 8: Вопрос/Ответ 5

Пояснение ответа: Соль не поможет для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу, так как соль добавляется во время хеширования, но это никак не меняет пароль пользователя и он остается прежним, что позволяет злоумышленнику добраться до цели.

Вопрос/Ответ 6 (рис. 9)

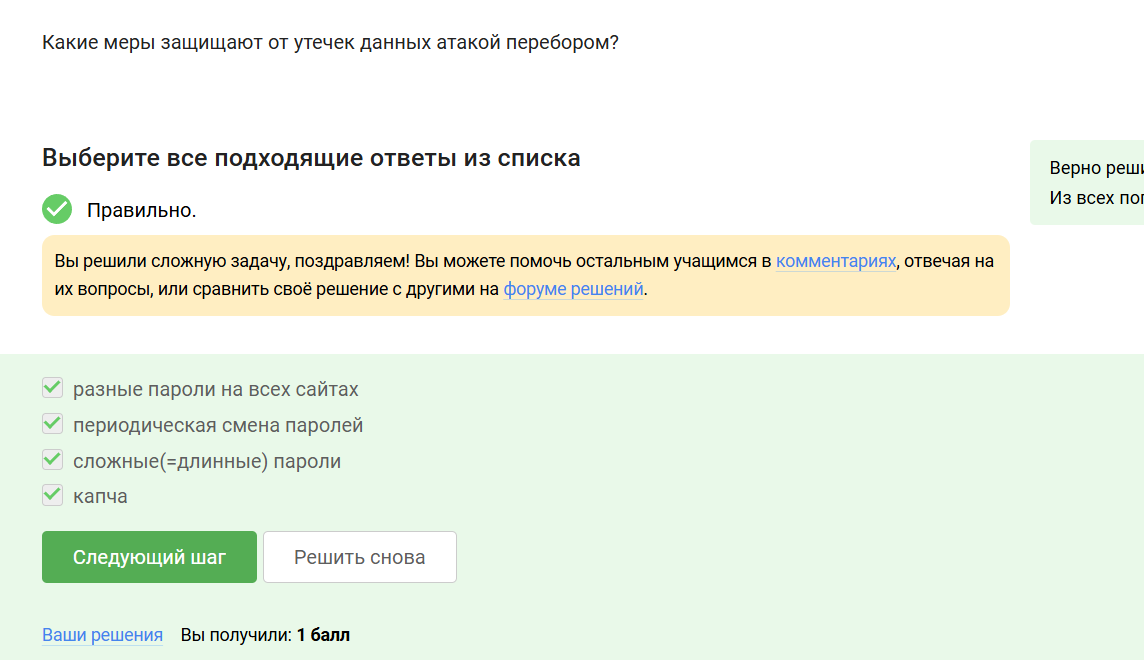


Рис. 9: Вопрос/Ответ 6

Пояснение ответа: Меры защиты от утечек данных перебором:

* Использовать длинные пароли с символами алфавита разного регистра, цифрами, спец. символами
* Использовать менеджеры паролей для хранения
* Регуляное изменение пароли к критическим сервисам
* Использование разных паролей для разных сайтов, программ.

## 1.3 3.3 Фишинг

Вопрос/Ответ 1 (рис. 10)

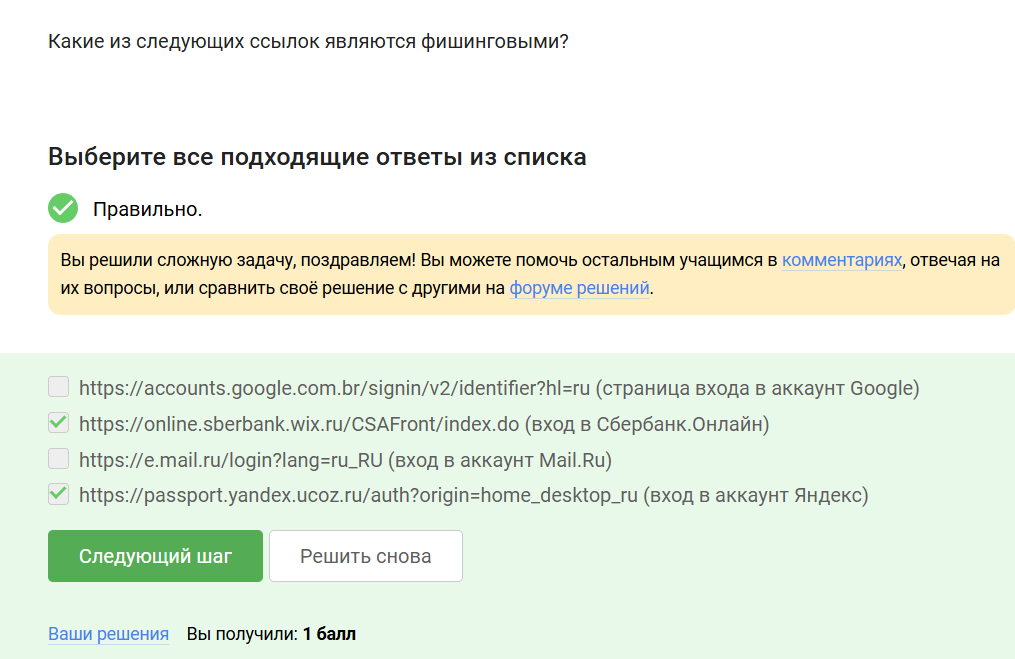


Рис. 10: Вопрос/Ответ 1

Пояснение ответа: В ссылке https://online.sberbank.wix.ru/CSAFront/index.do:

* Домен wix.ru - это беспратный хостинг, никак не связанный со Сбербанком.
* online.sberbank- это всего лишь поддомен хостинга wix.ru, а не настоящий сайт Сбербанка, настоящий- sberbank.ru или online.sberbank.ru

В ссылке https://passport.yandex.ucoz.ru/auth?origin=home\_ desktop\_ru:

* ucoz.ru- это также бесплатный конструктор сайтов
* passport.yandex- поддомен ucoz.ru

Вопрос/Ответ 2 (рис. 11)

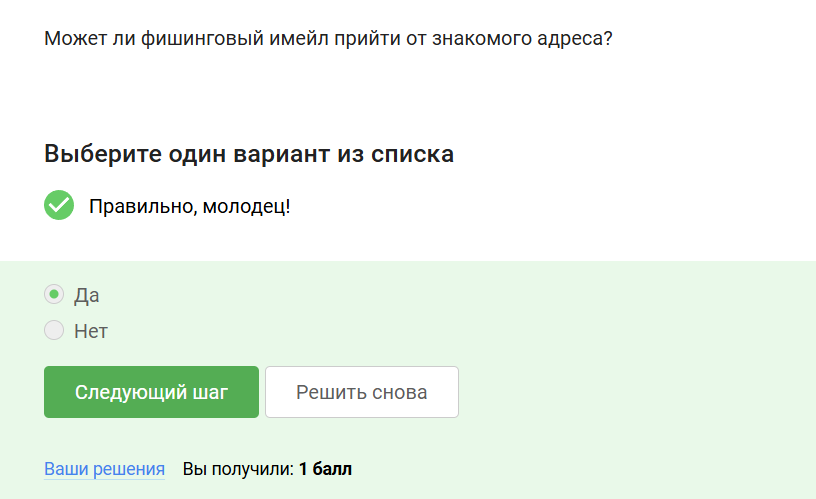


Рис. 11: Вопрос/Ответ 2

Пояснение ответа: Фишинговый имейл может прийти от знакомого адреса, это называется ip или имейл spoofing- подмена адреса отправителя.

## 1.4 3.4 Беспроводные сети WiFi

Вопрос/Ответ 1 (рис. 12)

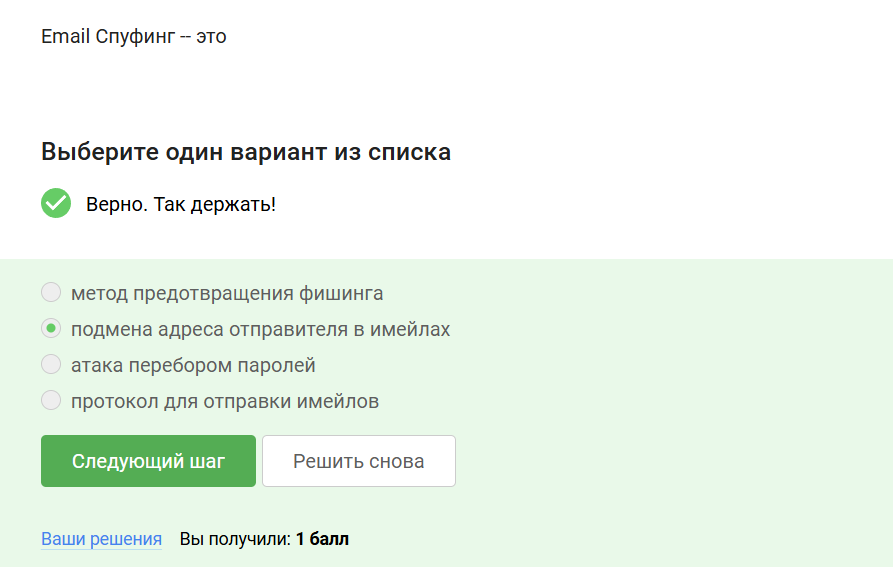


Рис. 12: Вопрос/Ответ 1

Пояснение ответа: Email Спуфинг- это подмена адреса отправителя в имейлах.

Вопрос/Ответ 2 (рис. 13)

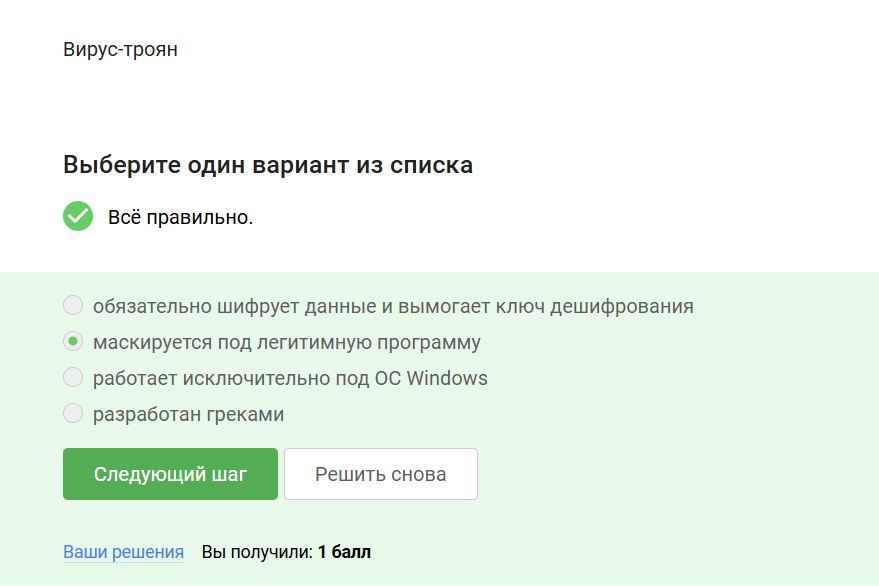


Рис. 13: Вопрос/Ответ 2

Пояснение ответа:

Троян- вирус, проникающий в систему под видом легитимного ПО.

## 1.5 3.5 Безопасность мессенджеров

Вопрос/Ответ 1 (рис. 14)

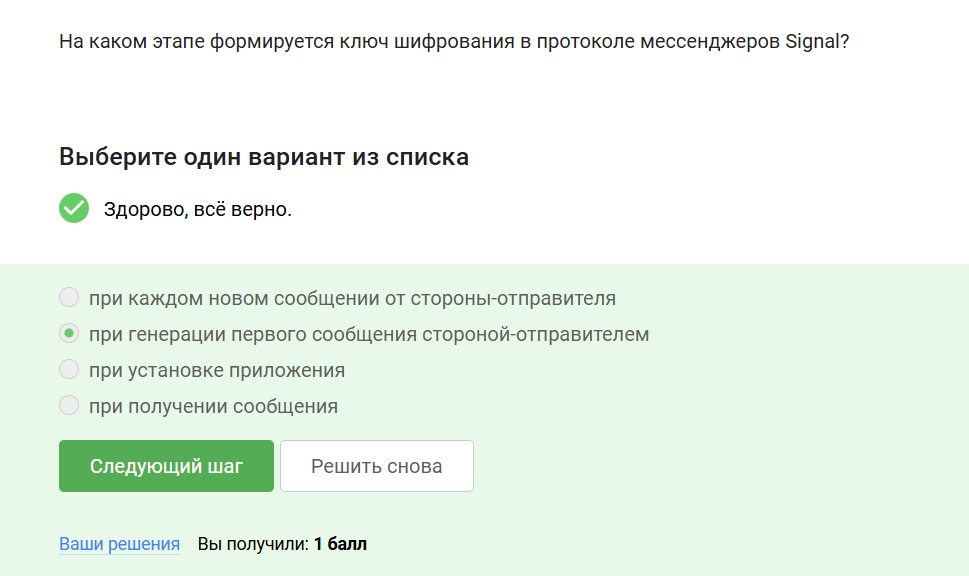


Рис. 14: Вопрос/Ответ 1

Пояснение ответа: Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителя.

Вопрос/Ответ 2 (рис. 15)

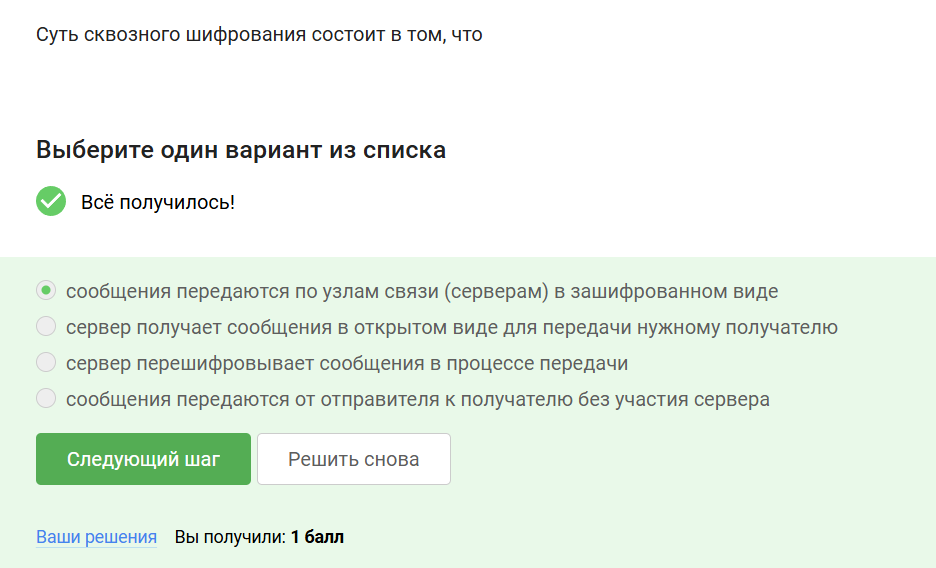


Рис. 15: Вопрос/Ответ 2

Пояснение ответа: Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде.