Отчет по части “Безопасность в сети” курса “Основы кибербезопасности”

Стариков Данила Андреевич

Содержание

# Цель работы

Цель курса:

* Понять, как происходит передача данных через Интернет, какие уязвимости могут возникнуть
* Разобраться, почему необходимо составлять сложные пароли
* Научиться различать шифрованиие и цифровую подпись
* Изучать работу электронных платежей

# 1 Первый модуль. Безопасность в сети.

## 1.1 Как работает интернет: базовые сетевые протоколы

* Вопрос 1. Выберите протокол прикладного уровня (рис. 1):

Ответ: *HTTPS*.

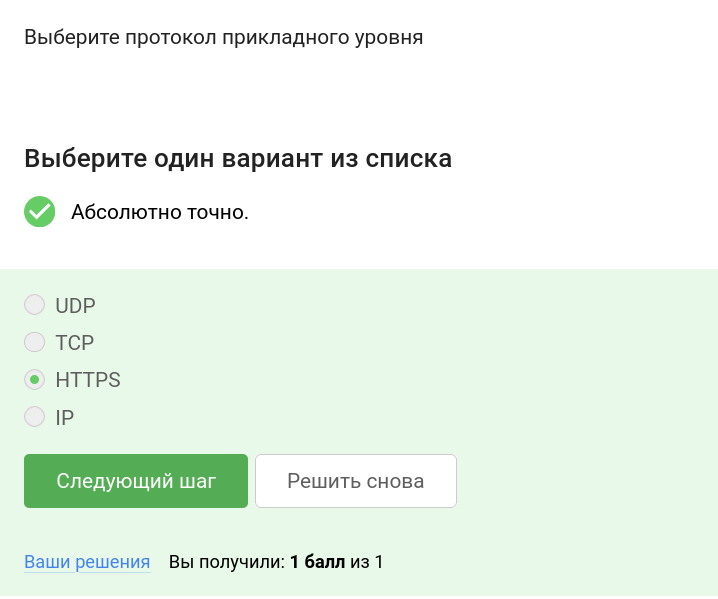


Рис. 1: Скриншот выполнения задания

* Вопрос 2. На каком уровне работает протокол TCP? (рис. 2)

Ответ: *Транспортном*.

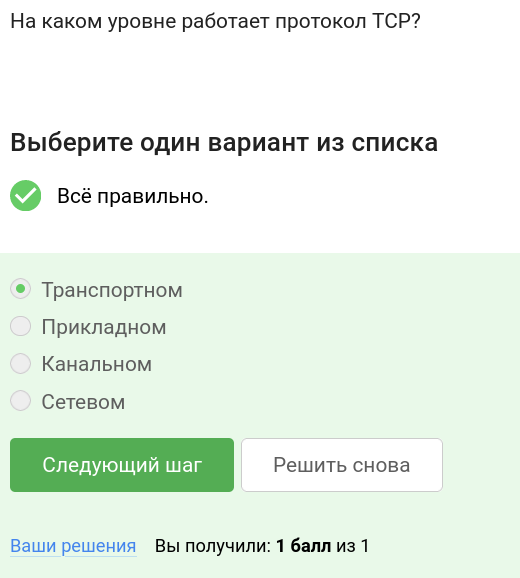


Рис. 2: Скриншот выполнения задания

* Вопрос 3. Выберите все корректные адреса IPv4. (рис. 3)

Ответ: *90.11.90.22 и 25.198.0.15*.

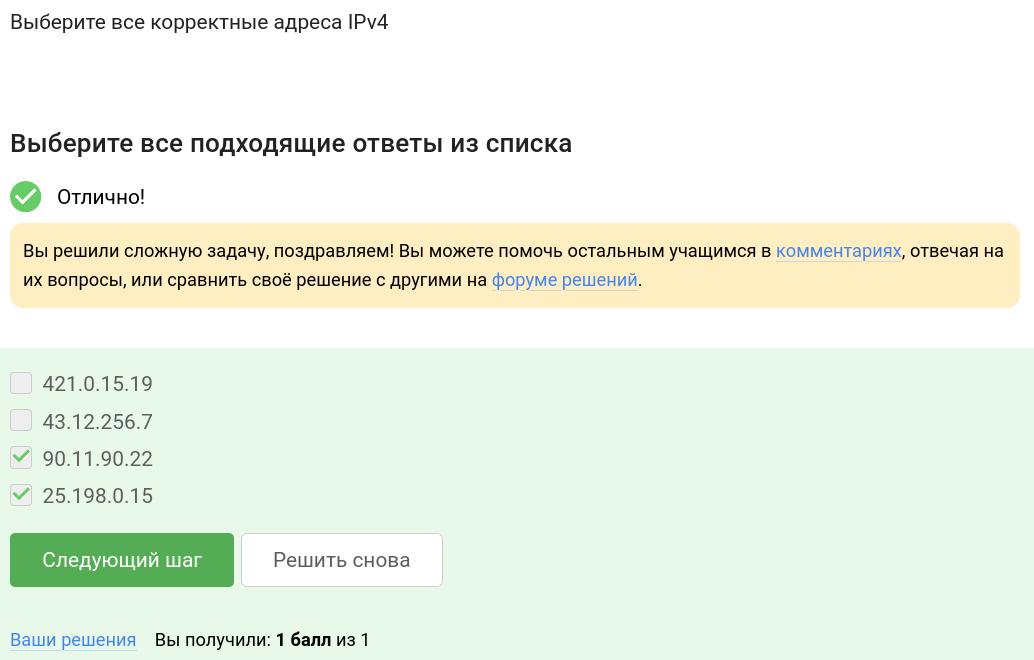


Рис. 3: Скриншот выполнения задания

* Вопрос 4. DNS сервер (рис. 4)

Ответ: *сопоставляет IP адреса доменным именам*.

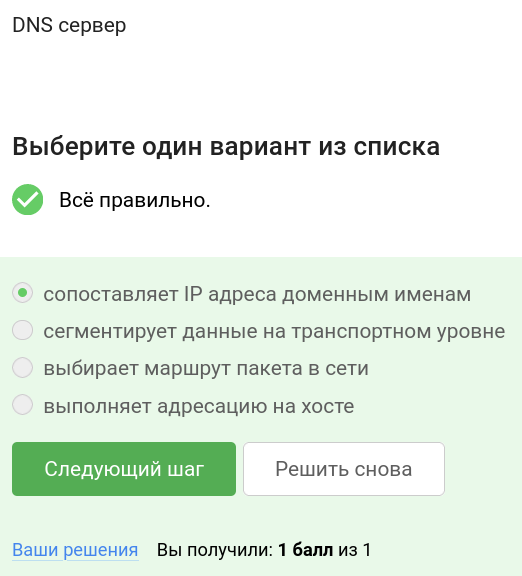


Рис. 4: Скриншот выполнения задания

* Вопрос 5. Выберите корректную последовательность протоколов в модели TCP/IP (рис. 5)

Ответ: *прикладной – транспортный – сетевой – канальный*.

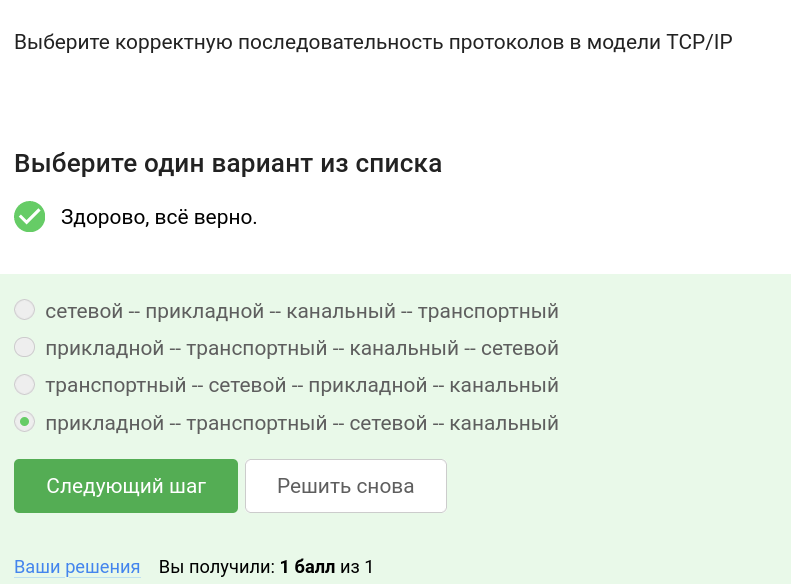


Рис. 5: Скриншот выполнения задания

* Вопрос 6. Протокол http предполагает (рис. 6)

Ответ: *передачу данных между клиентом и сервером в открытом виде*.

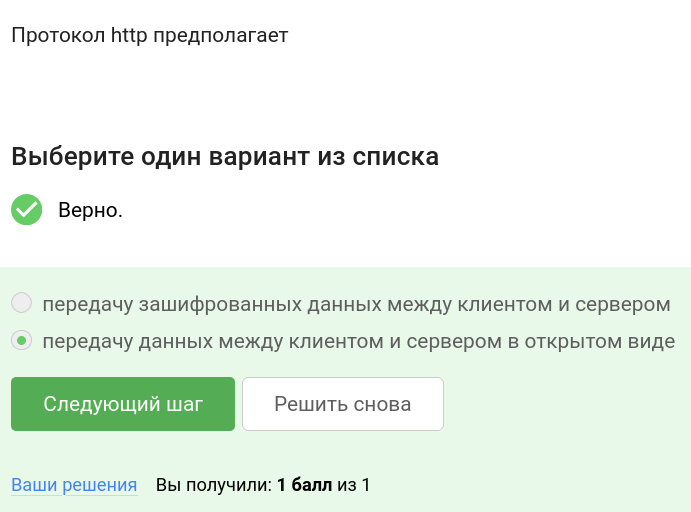


Рис. 6: Скриншот выполнения задания

* Вопрос 7. Протокол https состоит из (рис. 7)

Ответ: *двух фаз: рукопожатия и передачи данных*.

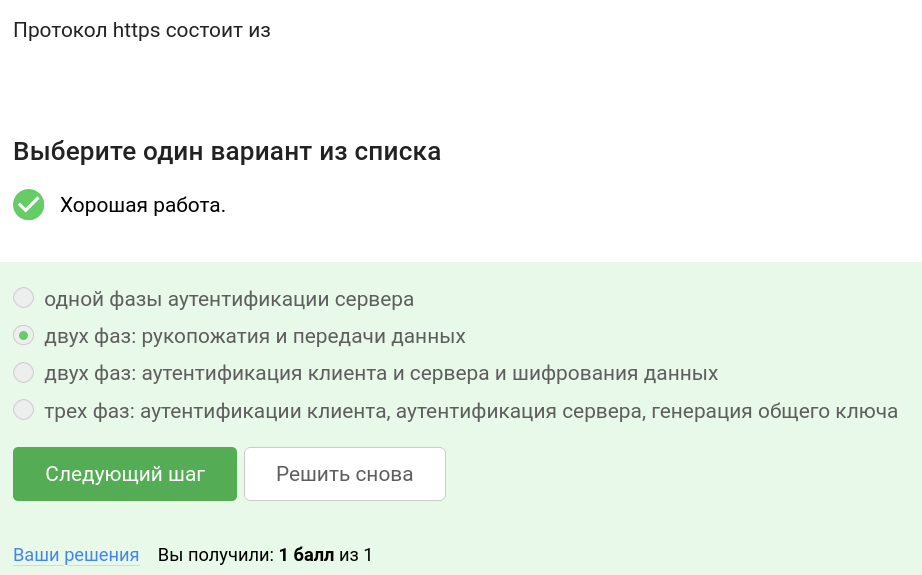


Рис. 7: Скриншот выполнения задания

* Вопрос 8. Версия протокола TLS определяется (рис. 8)

Ответ: *и клиентом, и сервером в процессе “переговоров”*.

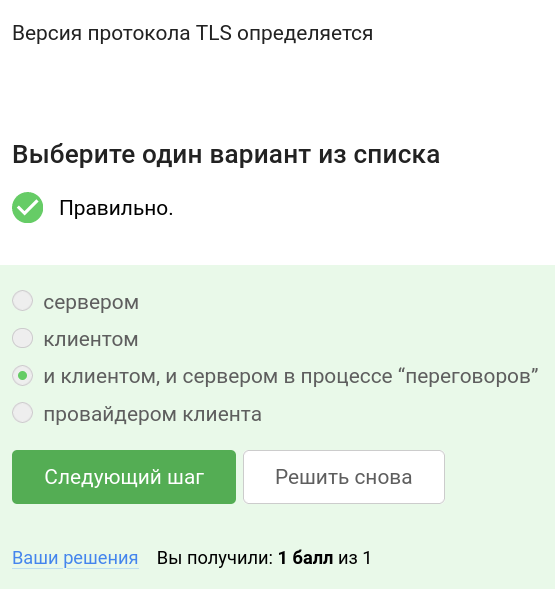


Рис. 8: Скриншот выполнения задания

* Вопрос 9. В фазе “рукопожатия” протокола TLS не предусмотрено (рис. 9)

Ответ: *шифрование данных*.

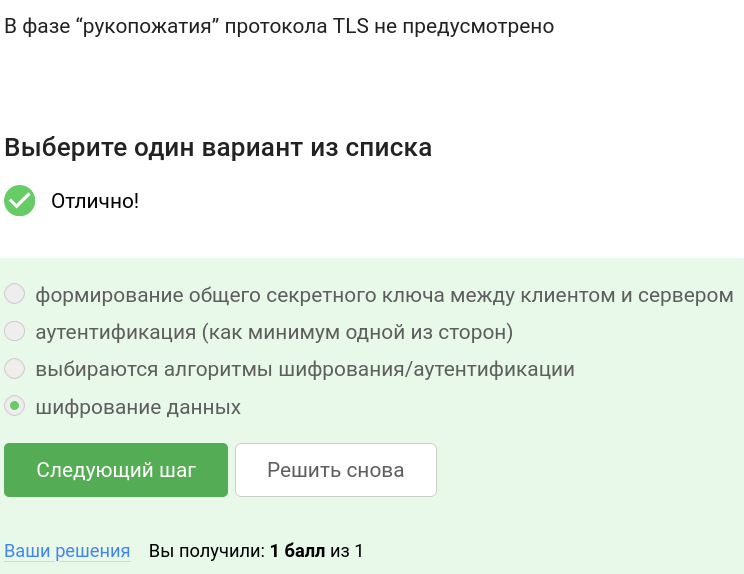


Рис. 9: Скриншот выполнения задания

## 1.2 Персонализация сети

* Вопрос 1. Куки хранят: (рис. 10)

Ответ: *идентификатор пользователя и id сессии*

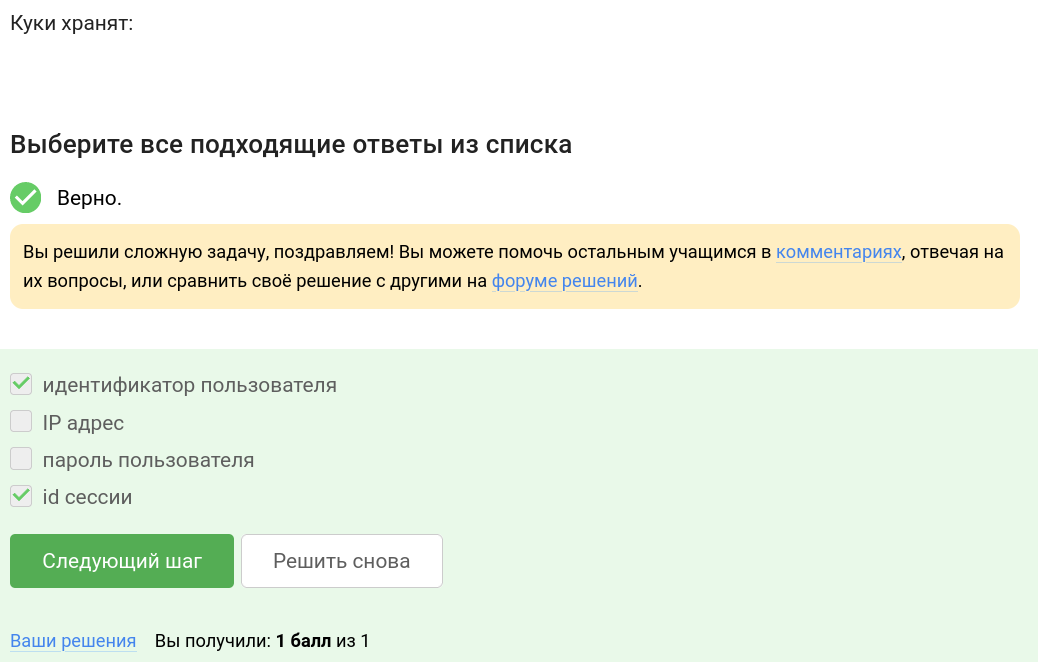


Рис. 10: Скриншот выполнения задания

* Вопрос 2. Куки не используются для (рис. 11)

Ответ: *улучшения надежности соединения*

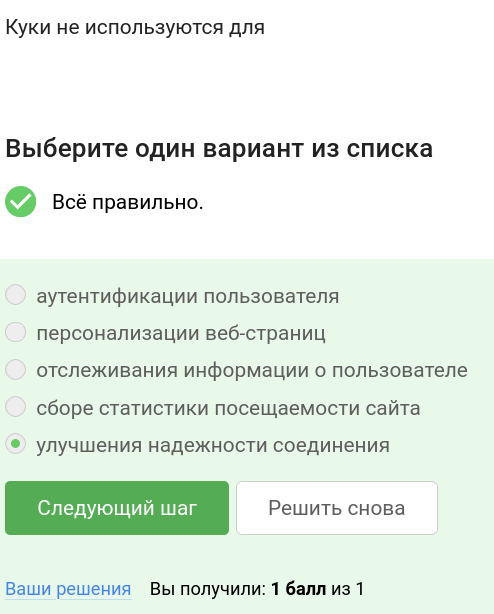


Рис. 11: Скриншот выполнения задания

* Вопрос 3. Куки генерируются (рис. 12)

Ответ: *сервером*

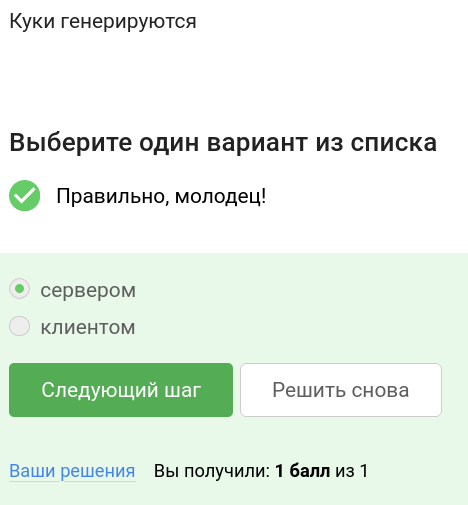


Рис. 12: Скриншот выполнения задания

* Вопрос 4. Сессионные куки хранятся в браузере? (рис. 13)

Ответ: *Да, на время пользования веб-сайтом*

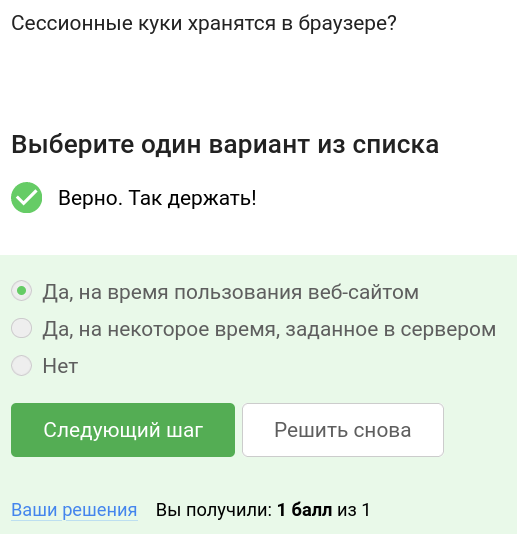


Рис. 13: Скриншот выполнения задания

## 1.3 Браузер TOR. Анонимизация

* Вопрос 1. Сколько промежуточных узлов в луковой сети TOR? (рис. 14)

Ответ: *3*

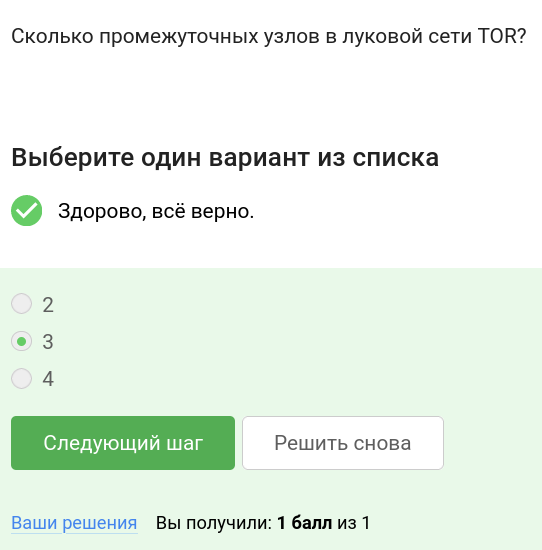


Рис. 14: Скриншот выполнения задания

* Вопрос 2. IP-адрес получателя известен (рис. 15)

Ответ: *отправителю и выходному узлу*

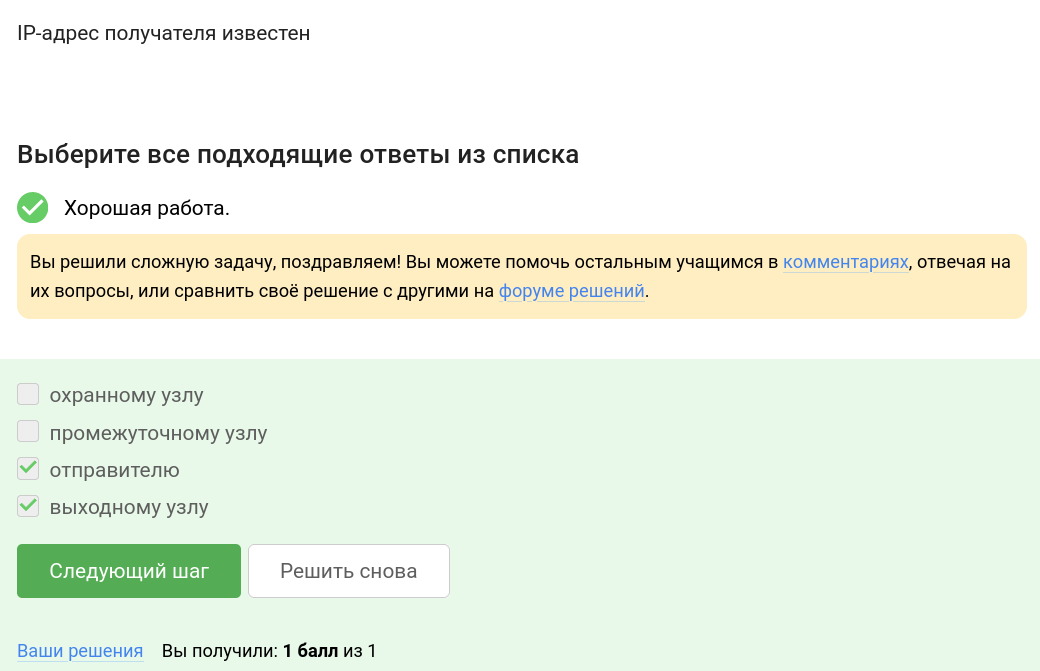


Рис. 15: Скриншот выполнения задания

* Вопрос 3. Отправитель генерирует общий секретный ключ (рис. 16)

Ответ: *с охранным, промежуточным и выходном узлом*

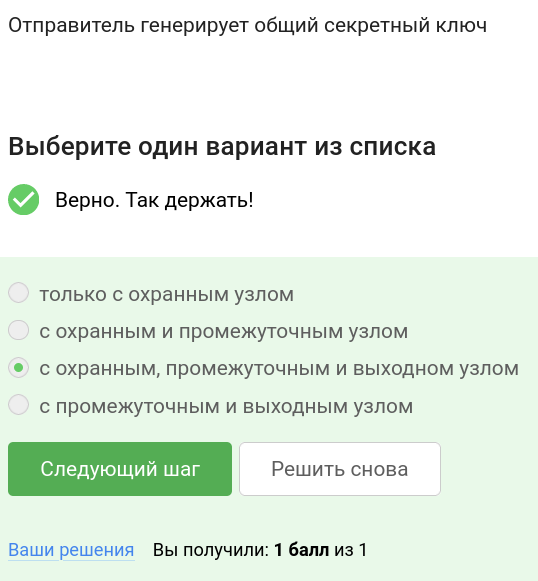


Рис. 16: Скриншот выполнения задания

* Вопрос 4. Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов? (рис. 17)

Ответ: *Нет*

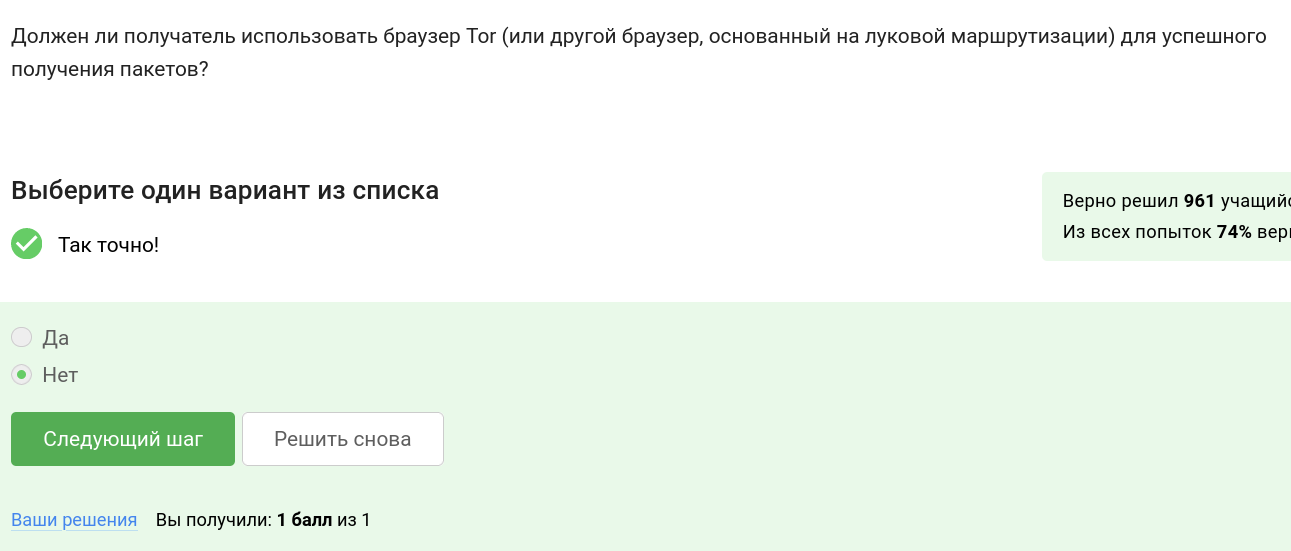


Рис. 17: Скриншот выполнения задания

## 1.4 Беспроводные сети Wi-Fi.

* Вопрос 1. Wi-Fi - это (рис. 18)

Ответ: *технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11*

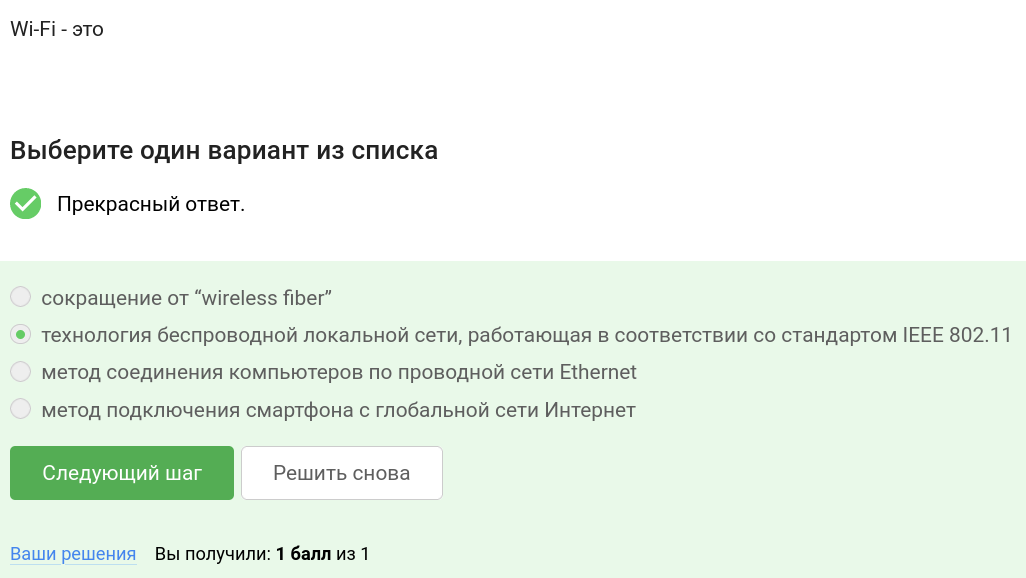


Рис. 18: Скриншот выполнения задания

* Вопрос 2. На каком уровне работает протокол WiFi? (рис. 19)

Ответ: *Канальном*

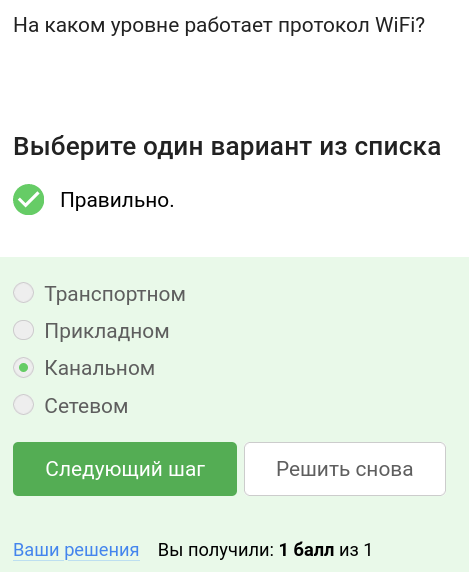


Рис. 19: Скриншот выполнения задания

* Вопрос 3. Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi (рис. 20)

Ответ: *WEP*

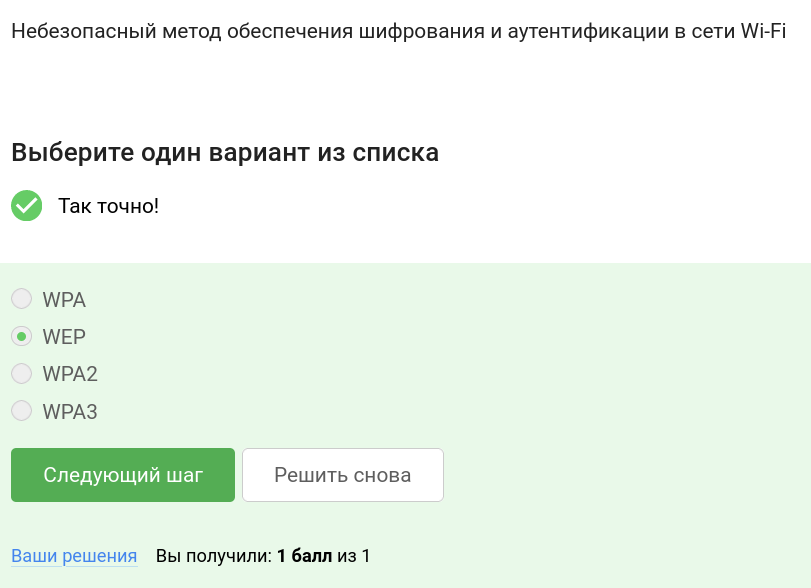


Рис. 20: Скриншот выполнения задания

* Вопрос 4. Данные между хостом сети (компьютером или смартфоном) и роутером (рис. 21)

Ответ: *передаются в зашифрованном виде после аутентификации устройств*

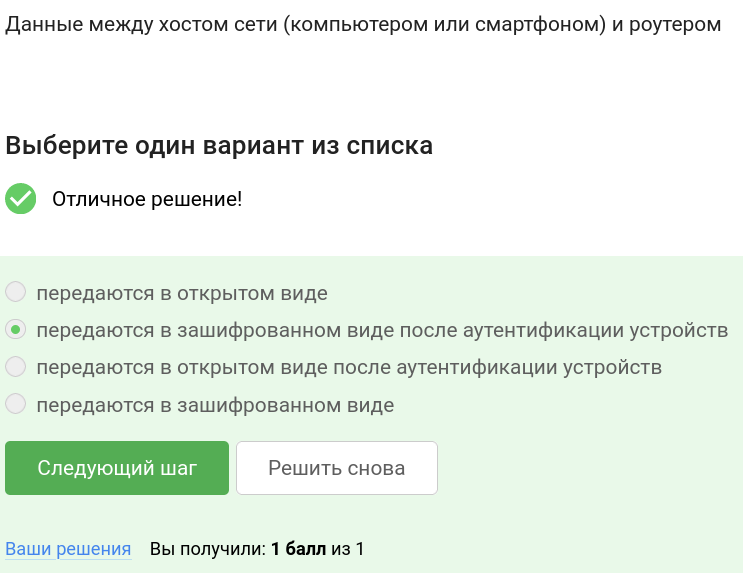


Рис. 21: Скриншот выполнения задания

* Вопрос 5. Для домашней сети для аутентификации обычно используется метод (рис. 22)

Ответ: *WPA2 Personal*

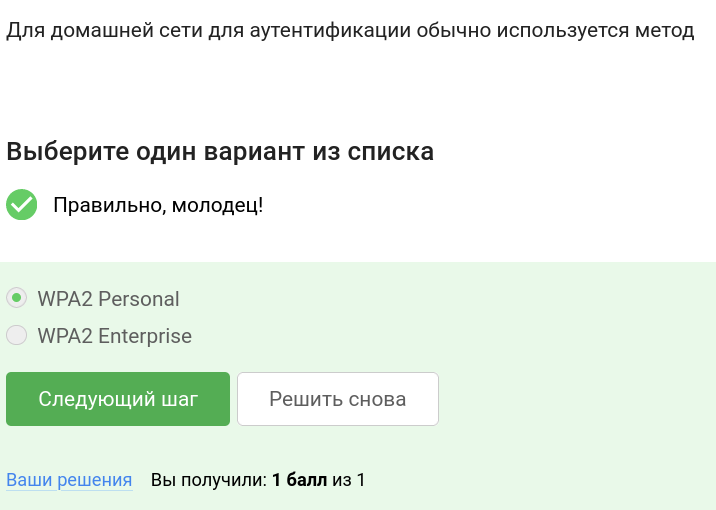


Рис. 22: Скриншот выполнения задания

# 2 Второй модуль. Защита ПК/Телефона.

## 2.1 Шифрование диска

* Вопрос 1. Можно ли зашифровать загрузочный сектор диска (рис. 23)

Ответ: *Да*.

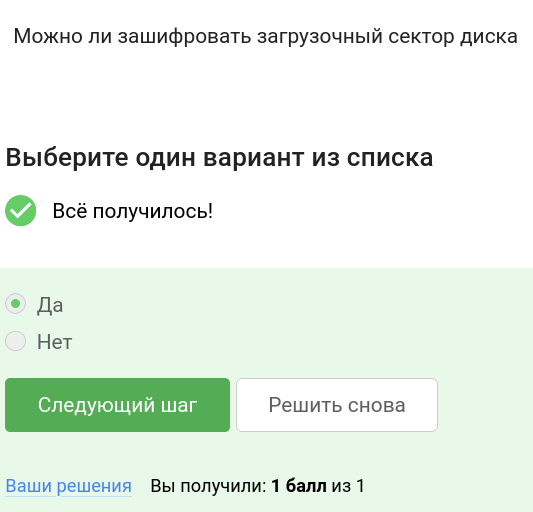


Рис. 23: Скриншот выполнения задания

* Вопрос 2. Шифрование диска основано на (рис. 24)

Ответ: *симметричном шифровании*.

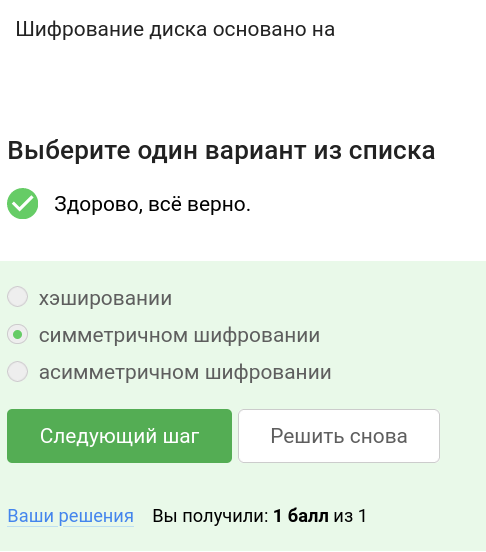


Рис. 24: Скриншот выполнения задания

* Вопрос 3. С помощью каких программ можно зашифровать жесткий диск? (рис. 25)

Ответ: *BitLocker и VeraCrypt*.

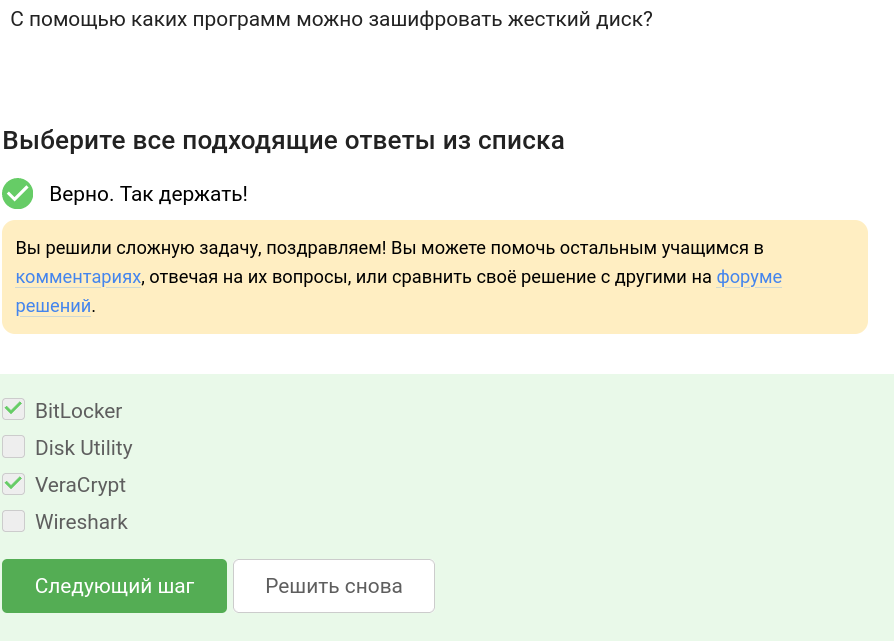


Рис. 25: Скриншот выполнения задания

## 2.2 Пароли

* Вопрос 1. Какие пароли можно отнести с стойким? (рис. 26)

Ответ: *UQr9@j4!S$*.

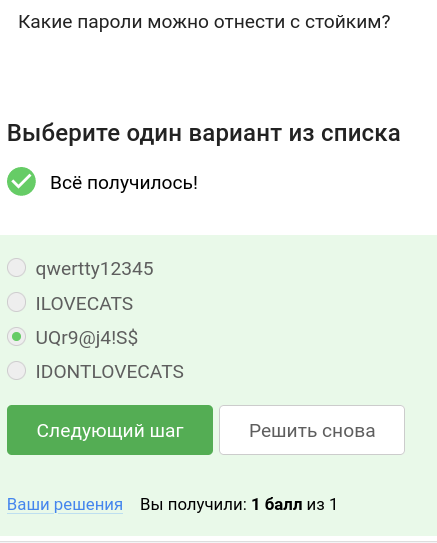


Рис. 26: Скриншот выполнения задания

* Вопрос 2. Где безопасно хранить пароли? (рис. 27)

Ответ: *В менеджерах паролей*.

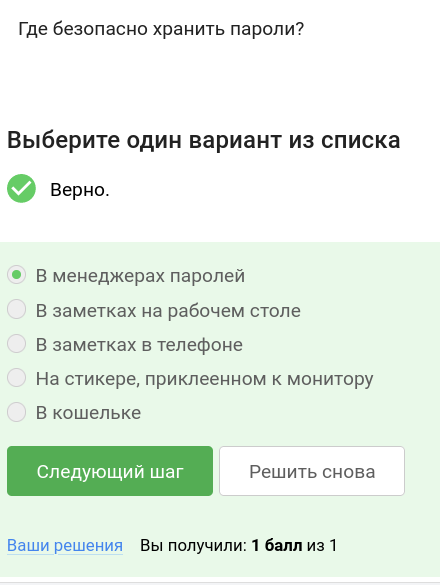


Рис. 27: Скриншот выполнения задания

* Вопрос 3. Зачем нужна капча? (рис. 28)

Ответ: *Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа*.

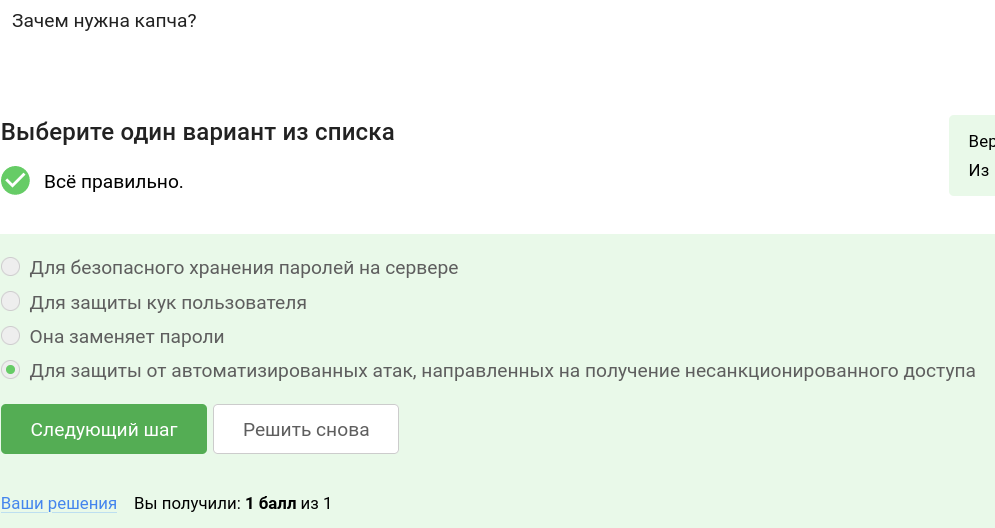


Рис. 28: Скриншот выполнения задания

* Вопрос 4. Для чего применяется хэширование паролей? (рис. 29)

Ответ: *Для того, чтобы не хранить пароли на сервере в открытом виде.*.

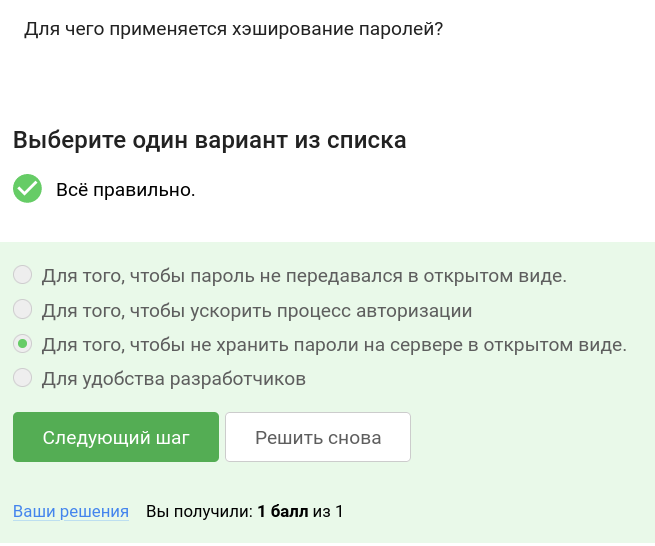


Рис. 29: Скриншот выполнения задания

* Вопрос 5. Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу? (рис. 30)

Ответ: *Нет*.

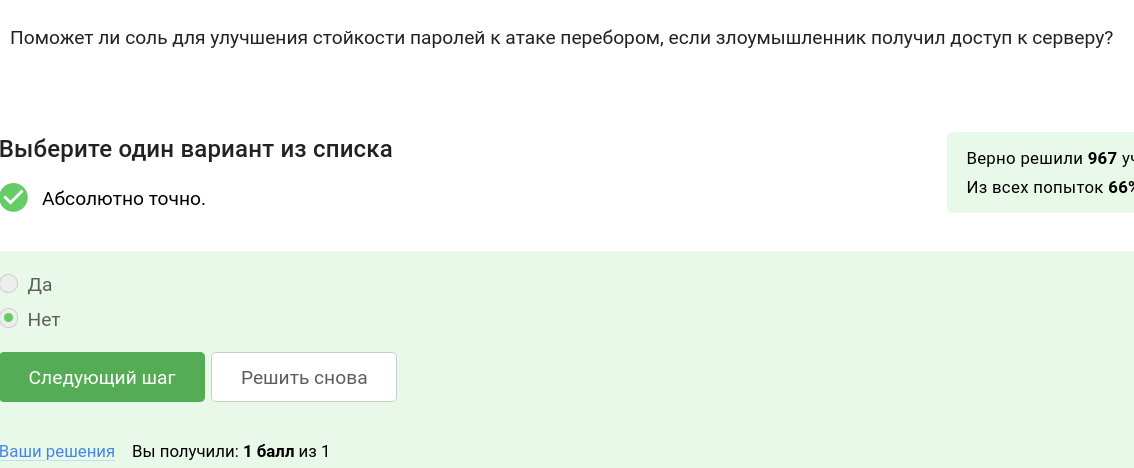


Рис. 30: Скриншот выполнения задания

* Вопрос 6. Какие меры защищают от утечек данных атакой перебором? (рис. 31)

Ответ: *разные пароли на всех сайтах, периодическая смена паролей, сложные(=длинные) пароли, капча*.

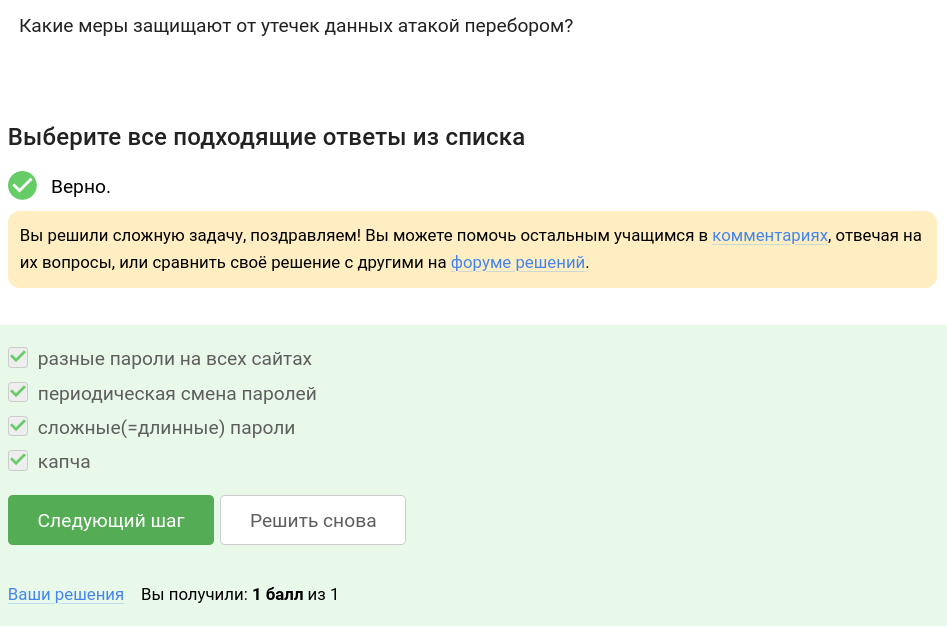


Рис. 31: Скриншот выполнения задания

## 2.3 Фишинг

* Вопрос 1. Какие из следующих ссылок являются фишинговыми? (рис. 32)

Ответ: *https://online.sberbank.wix.ru/CSAFront/index.do (вход в Сбербанк.Онлайн) и https://passport.yandex.ucoz.ru/auth?origin=home\_desktop\_ru (вход в аккаунт Яндекс)*.

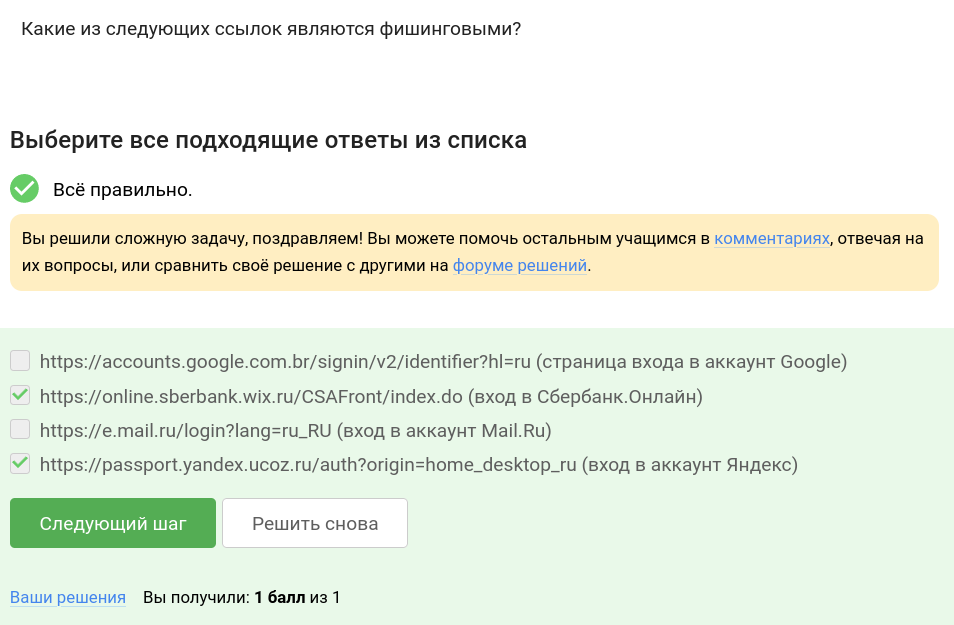


Рис. 32: Скриншот выполнения задания

* Вопрос 2. Может ли фишинговый имейл прийти от знакомого адреса? (рис. 33)

Ответ: *Да*.

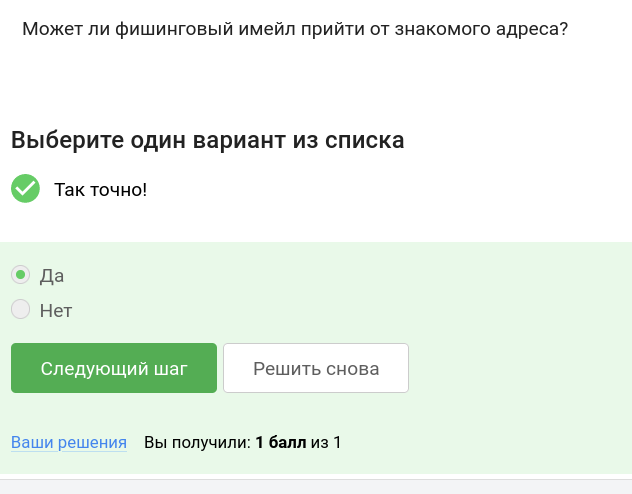


Рис. 33: Скриншот выполнения задания

## 2.4 Вирусы. Примеры

* Вопрос 1. Email Спуфинг – это (рис. 34)

Ответ: *подмена адреса отправителя в имейлах*.

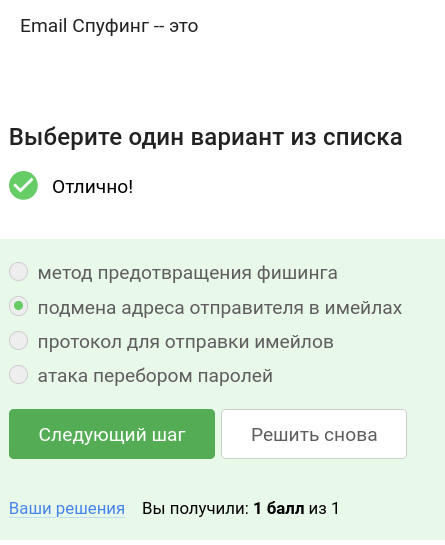


Рис. 34: Скриншот выполнения задания

* Вопрос 2. Вирус-троян (рис. 35)

Ответ: *маскируется под легитимную программу*.

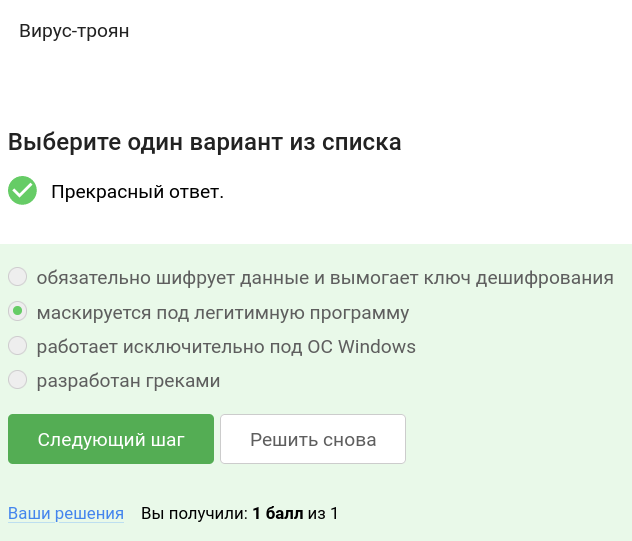


Рис. 35: Скриншот выполнения задания

## 2.5 Безопасность мессенджеров

* Вопрос 1. На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal? (рис. 36)

Ответ: *при генерации первого сообщения стороной-отправителем*.

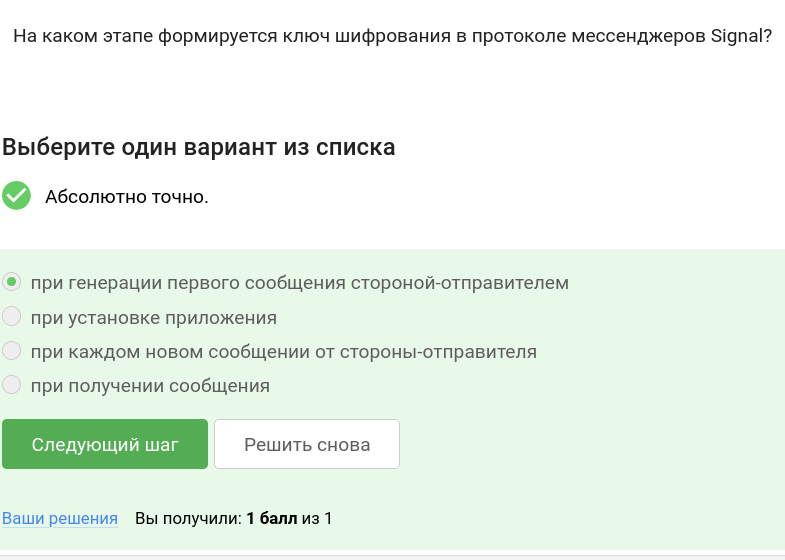


Рис. 36: Скриншот выполнения задания

* Вопрос 2. Суть сквозного шифрования состоит в том, что (рис. 37)

Ответ: *сообщения передаются по узлам связи (серверам) в зашифрованном виде*.

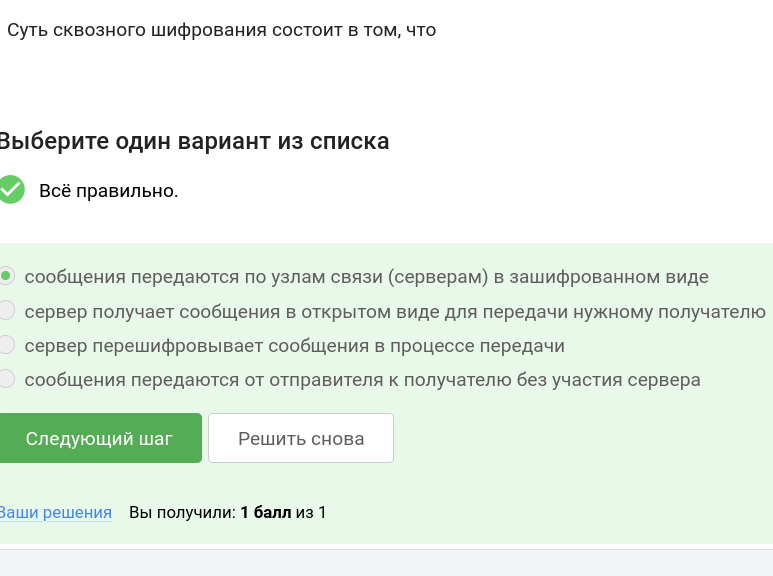


Рис. 37: Скриншот выполнения задания

# 3 Третий модуль. Криптография на практике.

## 3.1 Введение в криптографию

* Вопрос 1. В асимметричных криптографических примитивах (рис. 38):

Ответ: *обе стороны имеют пару ключей*.

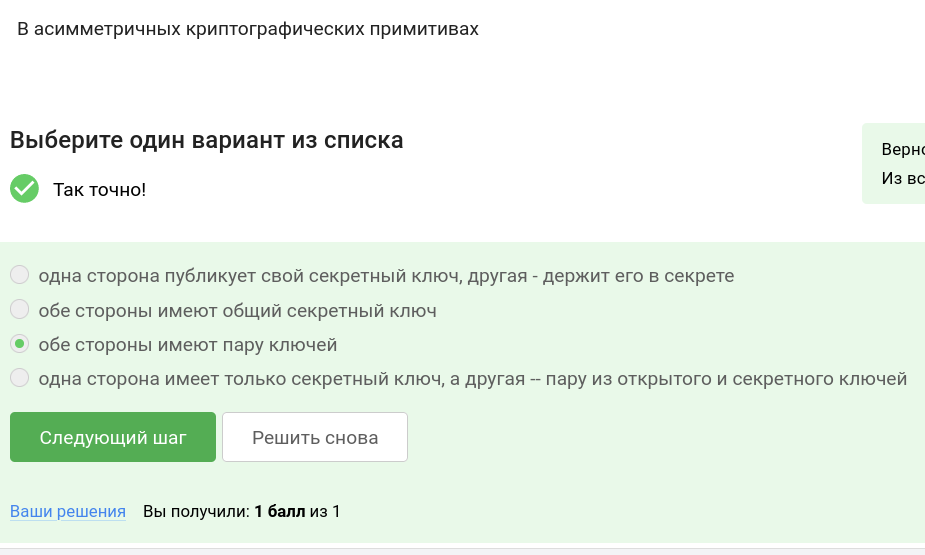


Рис. 38: Скриншот выполнения задания

* Вопрос 2. Криптографическая хэш-функция (рис. 39):

Ответ: *эффективно вычисляется, дает на выходе фиксированное число бит независимо от объема входных данных, стойкая к коллизиям*.

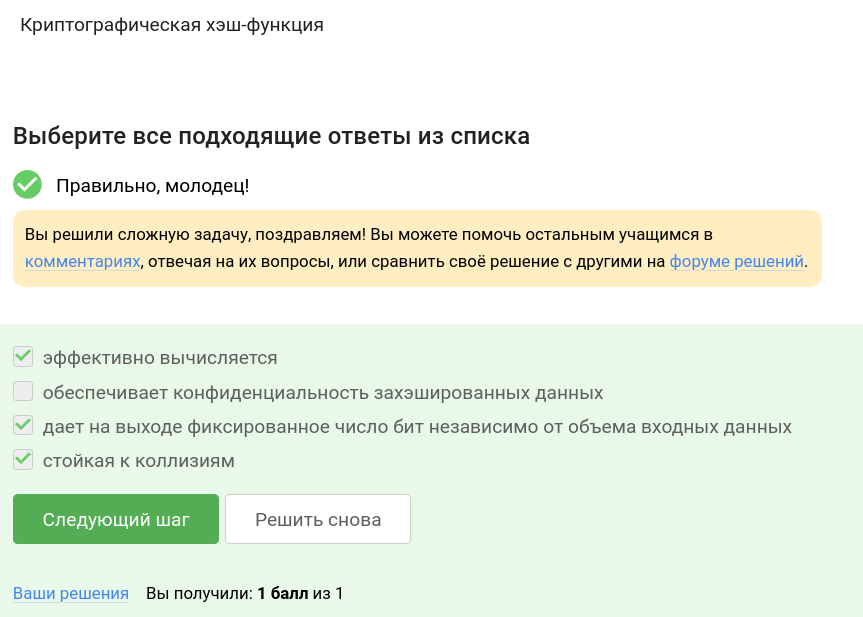


Рис. 39: Скриншот выполнения задания

* Вопрос 3. К алгоритмам цифровой подписи относятся (рис. 40):

Ответ: *RSA, ECDSA, ГОСТ Р 34.10-2012* .

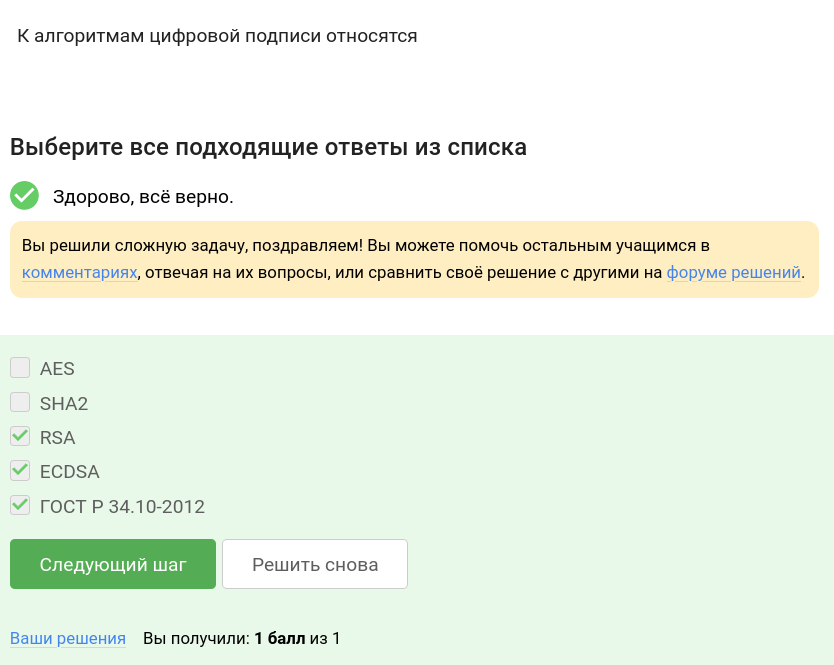


Рис. 40: Скриншот выполнения задания

* Вопрос 4. Код аутентификации сообщения относится к (рис. 41):

Ответ: *симметричным примитивам*.

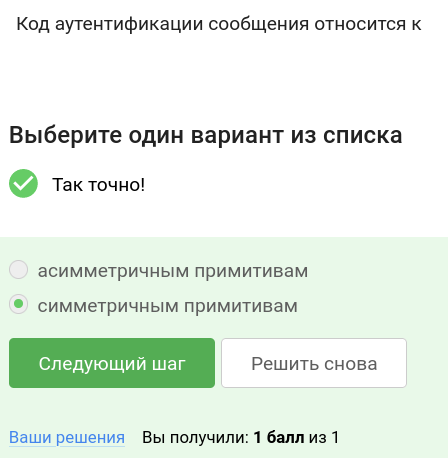


Рис. 41: Скриншот выполнения задания

* Вопрос 5. Обмен ключам Диффи-Хэллмана - это (рис. 42):

Ответ: *асимметричный примитив генерации общего секретного ключа*.

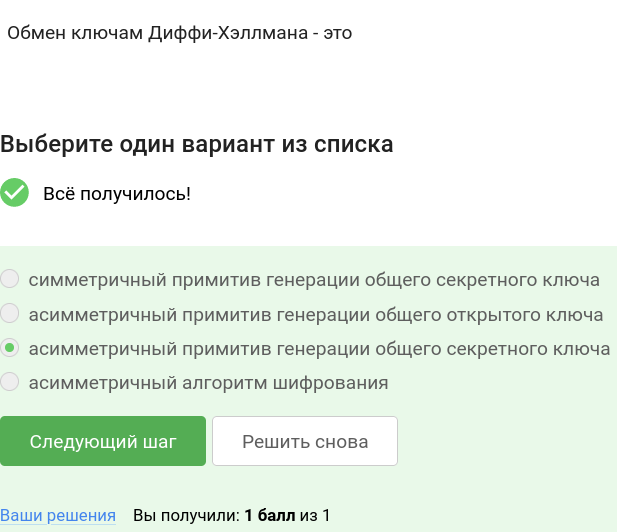


Рис. 42: Скриншот выполнения задания

## 3.2 Цифровая подпись

* Вопрос 1. Протокол электронной цифровой подписи относится к (рис. 43):

Ответ: *протоколам с публичным (или открытым) ключом*.

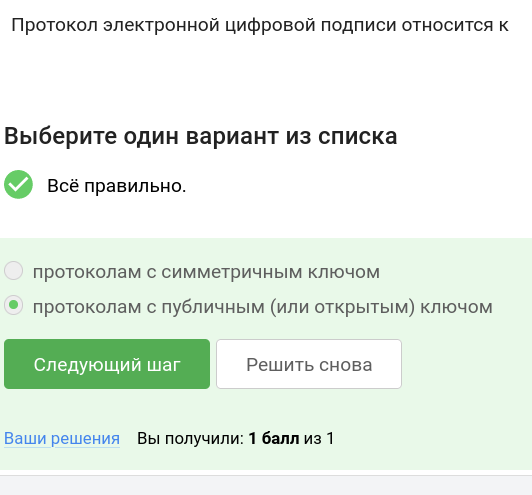


Рис. 43: Скриншот выполнения задания

* Вопрос 2. Алгоритм верификации электронной цифровой подписи требует на вход (рис. 44):

Ответ: *подпись, открытый ключ, сообщение*.

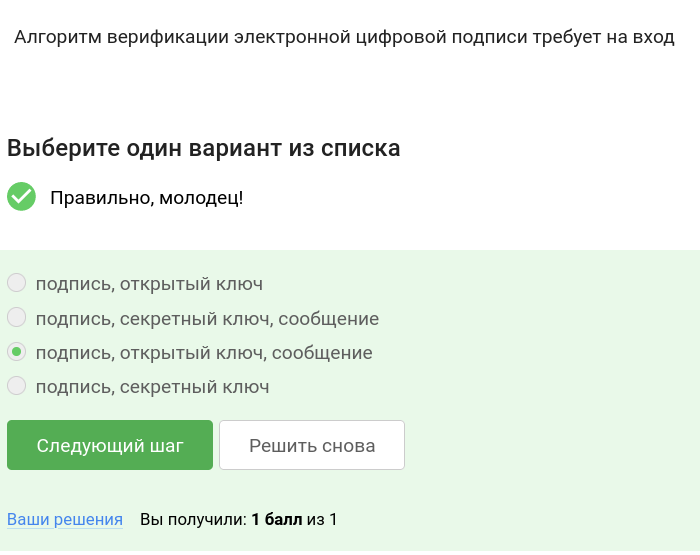


Рис. 44: Скриншот выполнения задания

* Вопрос 3. Электронная цифровая подпись не обеспечивает (рис. 45):

Ответ: *конфиденциальность*.

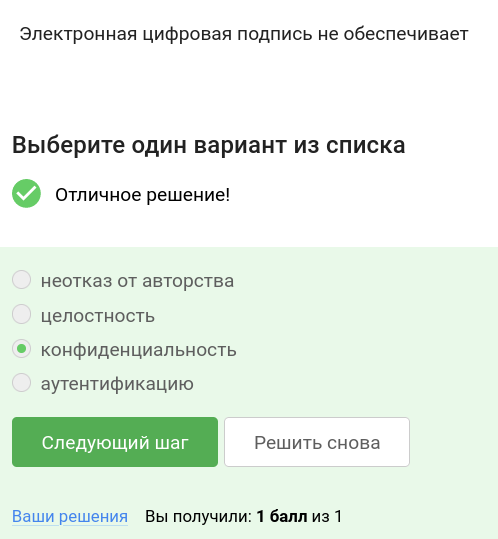


Рис. 45: Скриншот выполнения задания

* Вопрос 4. Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС? (рис. 46):

Ответ: *усиленная квалифицированная*.

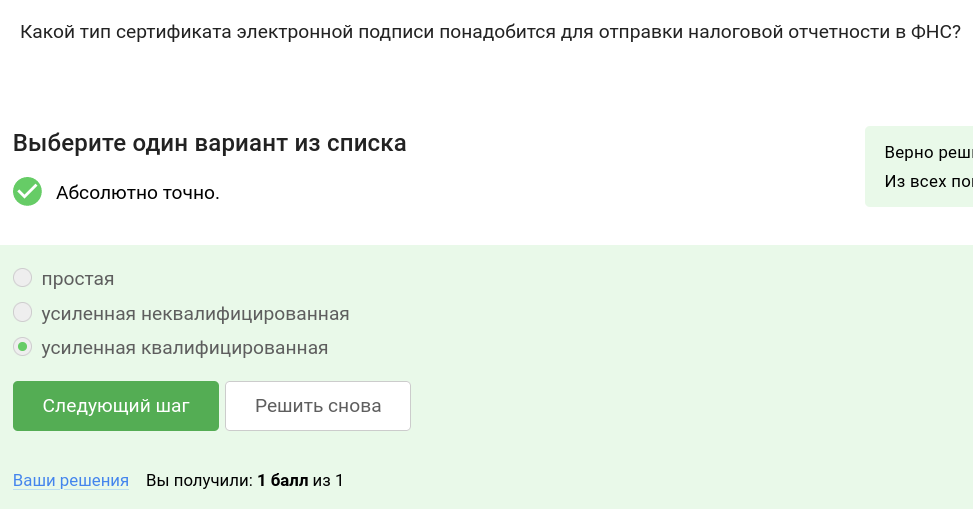


Рис. 46: Скриншот выполнения задания

* Вопрос 5. В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи? (рис. 47):

Ответ: *в удостоверяющем (сертификационном) центре*.

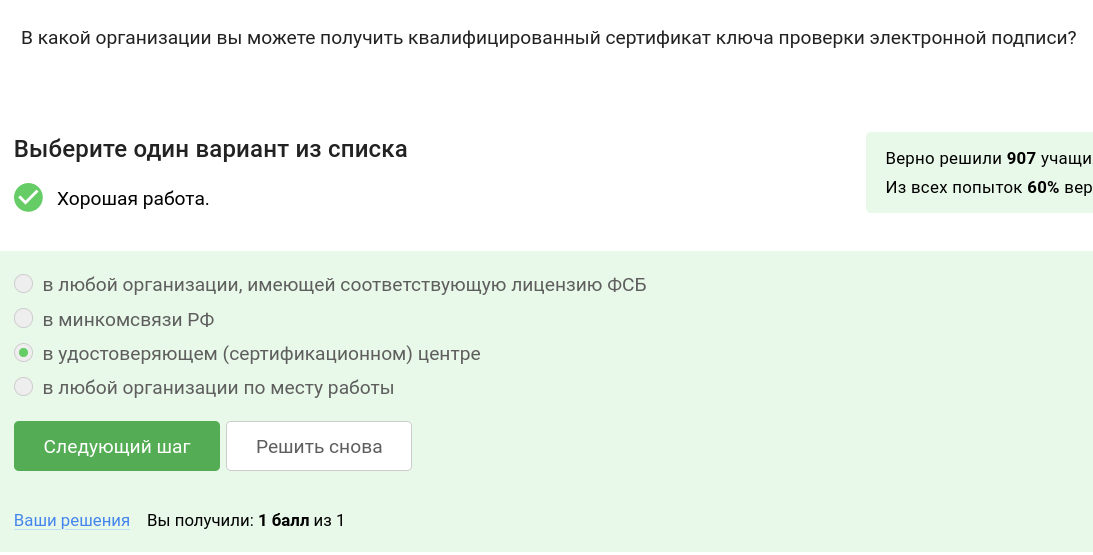


Рис. 47: Скриншот выполнения задания

## 3.3 Электронные платежи

* Вопрос 1. Выберите из списка все платежные системы. (рис. 48):

Ответ: *MasterCard, МИР*.

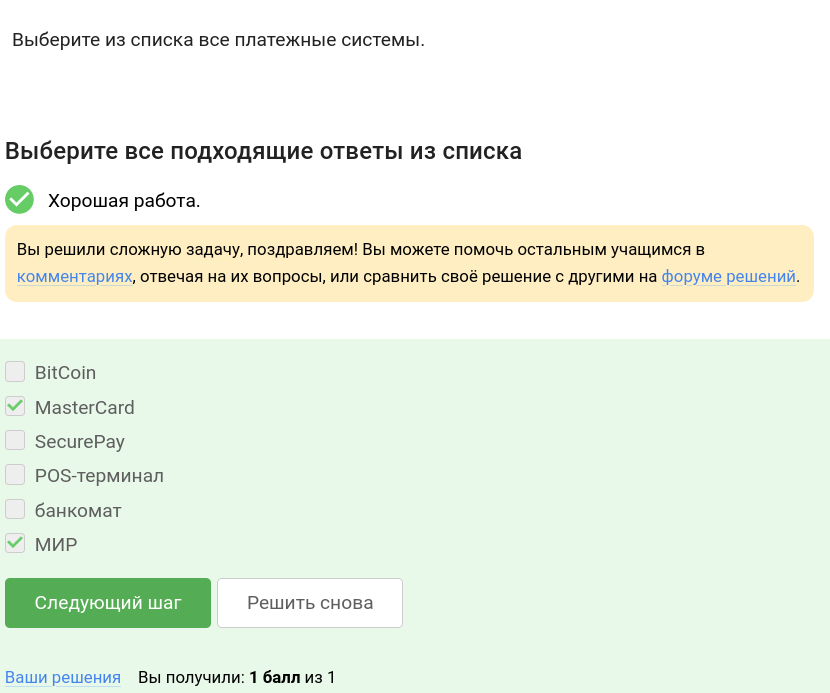


Рис. 48: Скриншот выполнения задания

* Вопрос 2. Примером многофакторной аутентификации является (рис. 49):

Ответ: *комбинация проверка пароля + код в sms сообщении, комбинация код в sms сообщении + отпечаток пальца* .

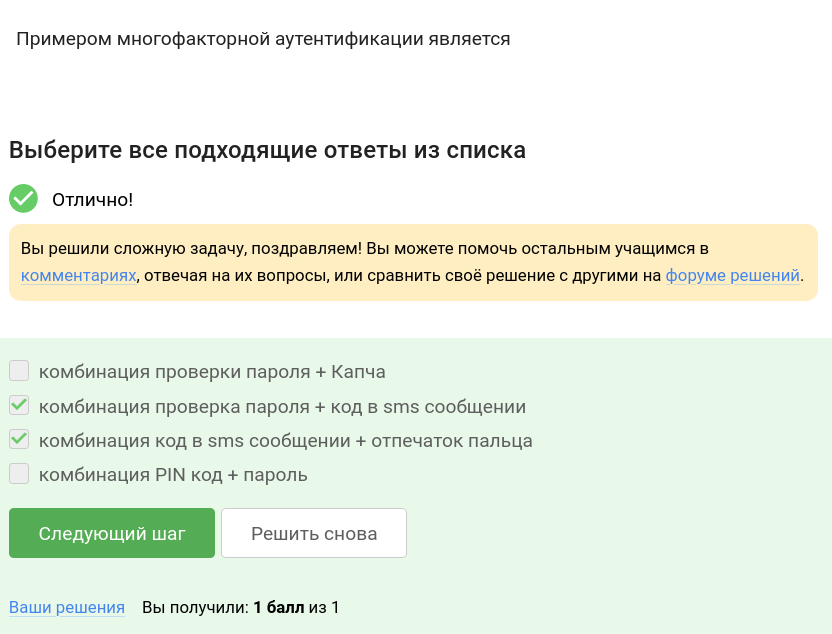


Рис. 49: Скриншот выполнения задания

* Вопрос 3. При онлайн платежах сегодня используется (рис. 50):

Ответ: *многофакторная аутентификация покупателя перед банком-эмитентом*.

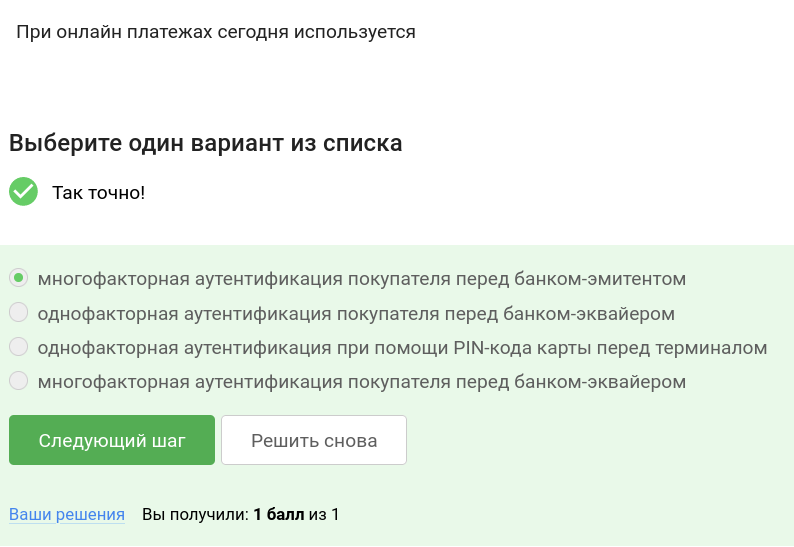


Рис. 50: Скриншот выполнения задания

## 3.4 Блокчейн

* Вопрос 1. Какое свойство криптографической хэш-функции используется в доказательстве работы? (рис. 51):

Ответ: *сложность нахождения прообраза*.

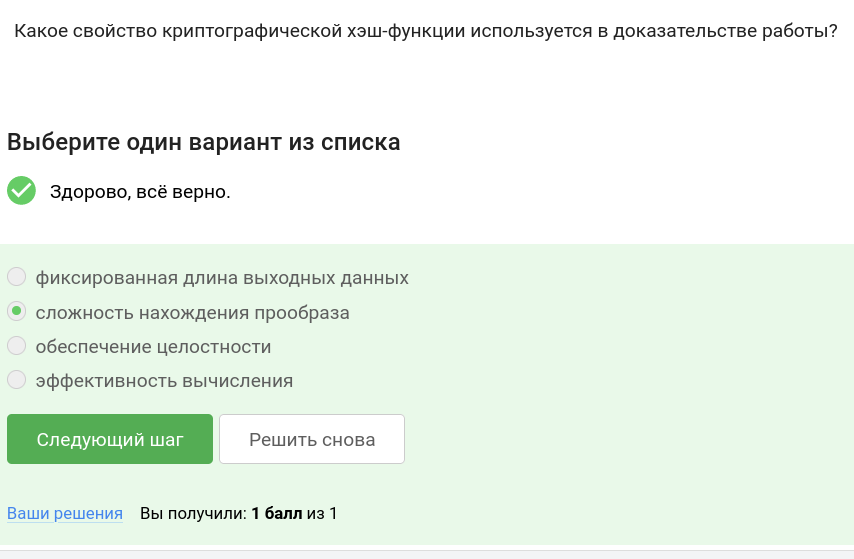


Рис. 51: Скриншот выполнения задания

* Вопрос 2. Консенсус в некоторых системах блокчейн обладает свойствами (рис. 52):

Ответ: *постоянства, консенсус, живучесть, открытость*.

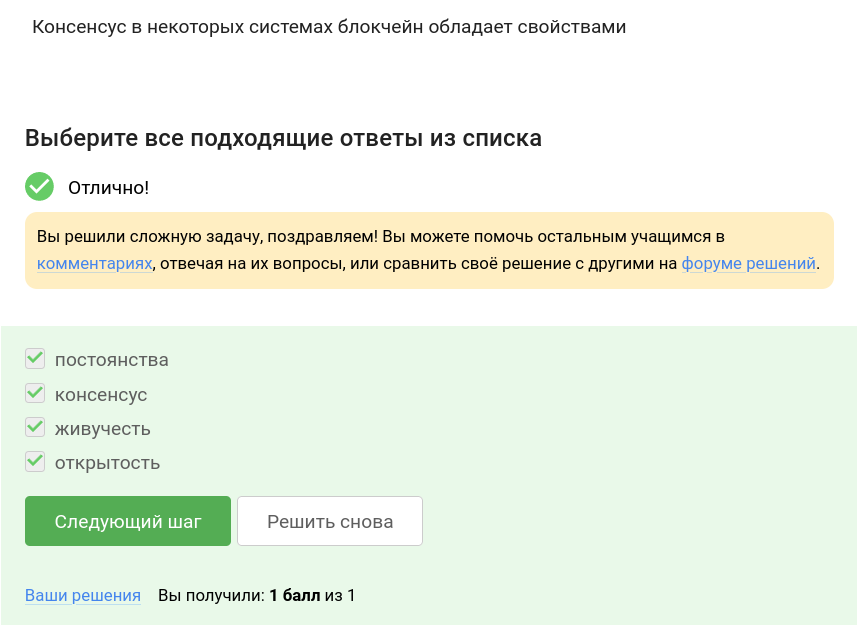


Рис. 52: Скриншот выполнения задания

* Вопрос 3. Секретные ключи какого криптографического примитива хранят участники блокчейна? (рис. 53):

Ответ: *цифровая подпись*.

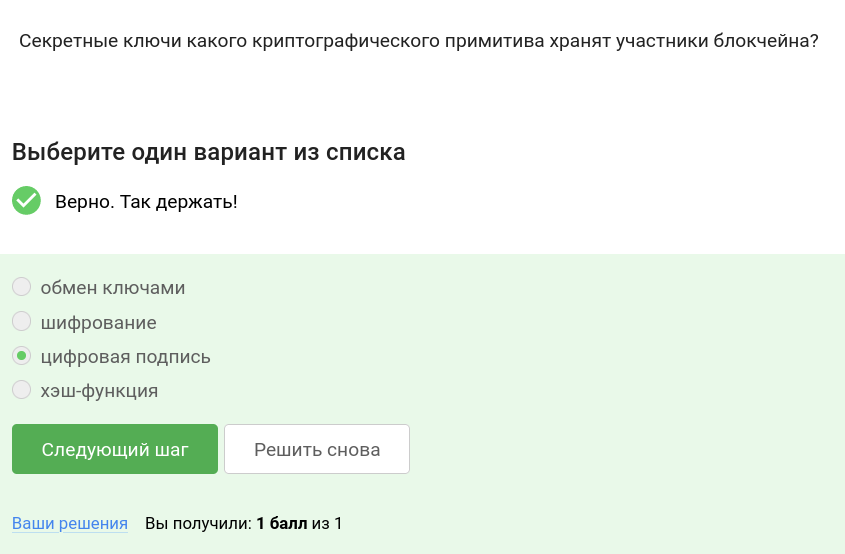


Рис. 53: Скриншот выполнения задания

# 4 Выводы

В рамках прохождения курса разобрались в схеме передачи данных через Интернет, их шифровании. Получили практические советы по выбору более качественного пароля. Научились отличать шифрование от цифровой подписи, поняли, как работают системы электронных платежей.