Внешний курс на Stepik

Основы кибербезопасности

Алади Принц Чисом

Содержание

# 1 Цель работы

Закончить курс с сертификатом и научиться базовым приемам и методам информационной безопсности.

# 2 Раздел 2.1

Выберите протокол прикладного уровня: HTTPS

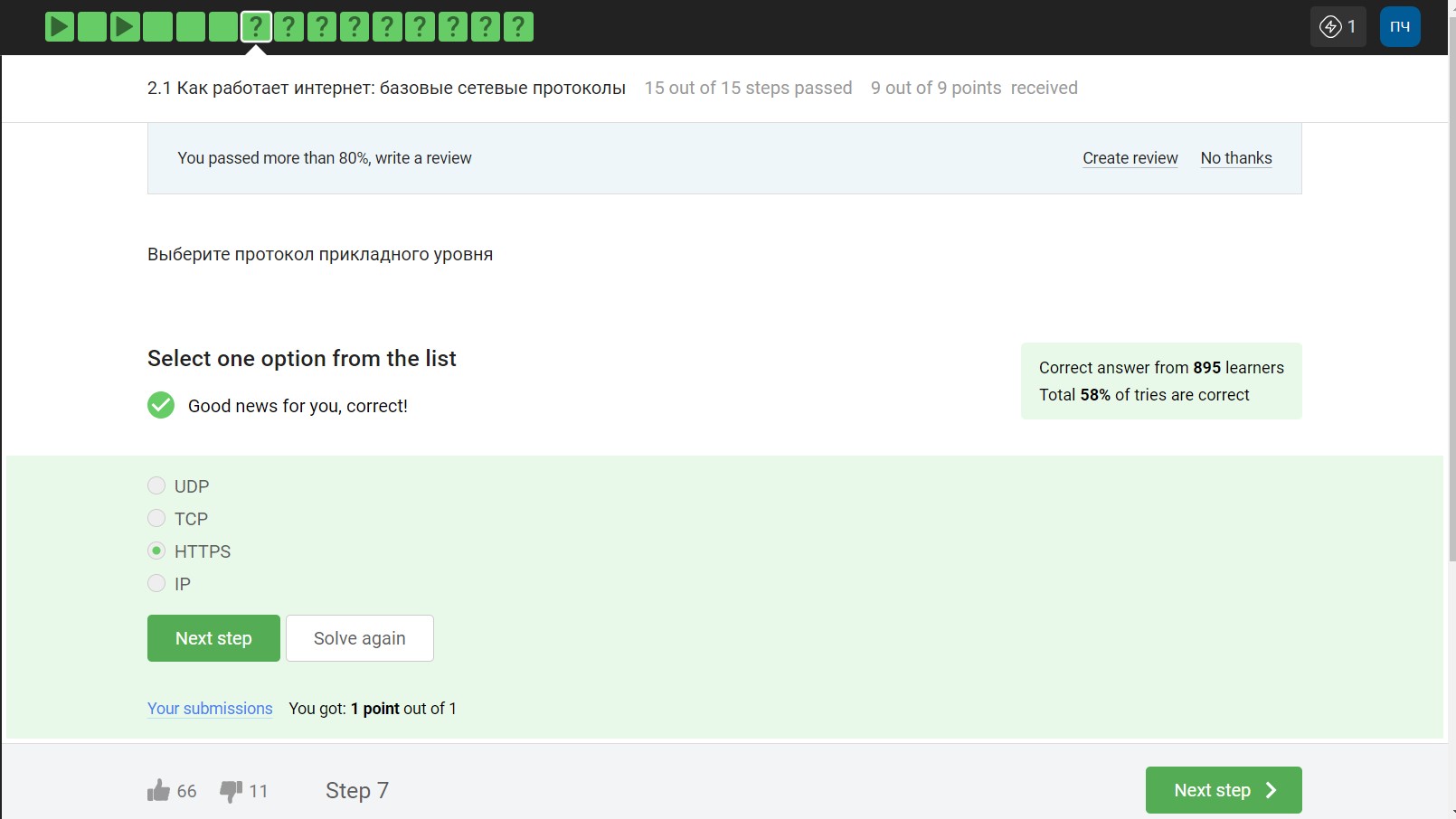


Рис. 1: Рис. 1

На каком уровне работает протокол TCP?: транспортном

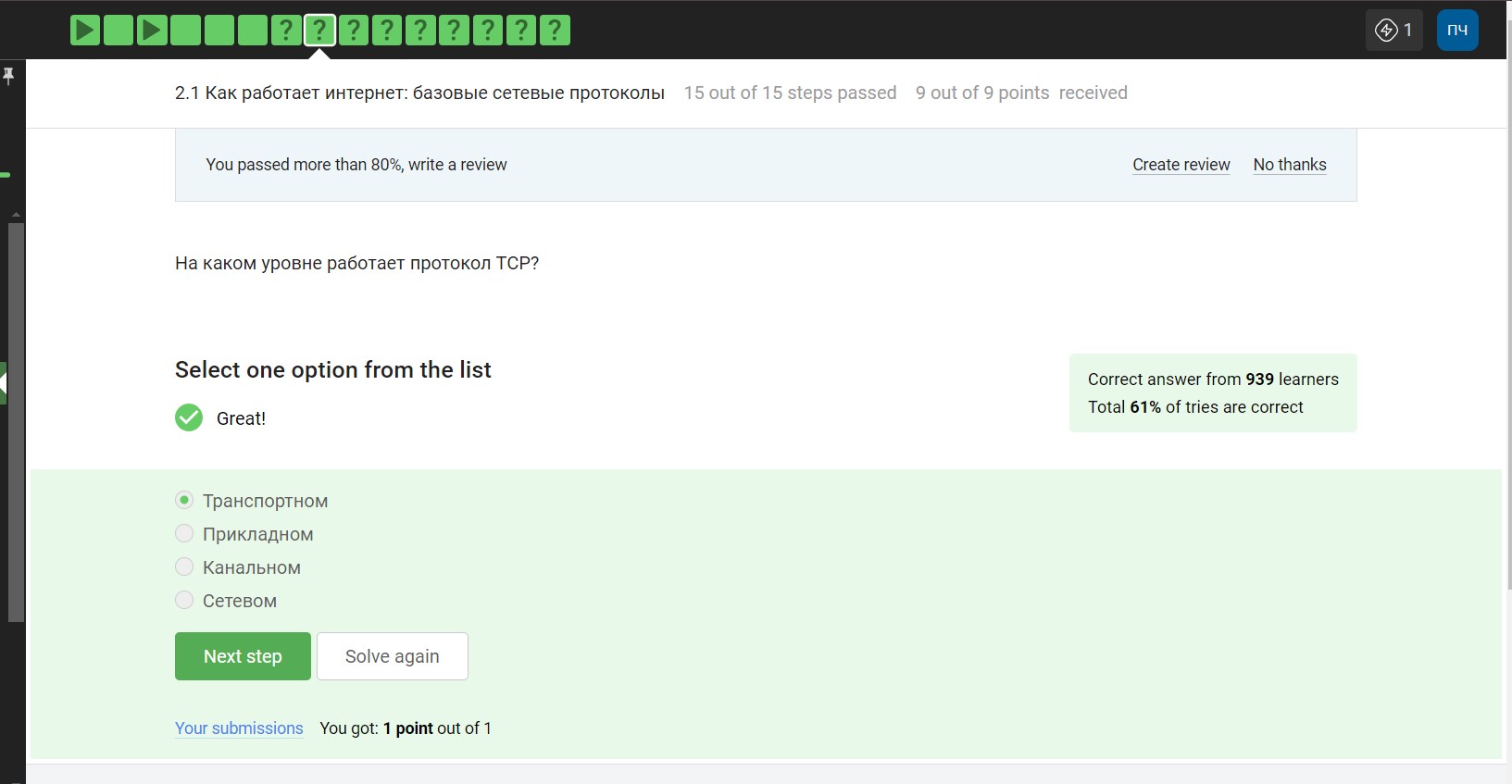


Рис. 2: Рис. 2

Выберите все корректные адреса IPv4: 90.11.90.22, 25.198.0.15

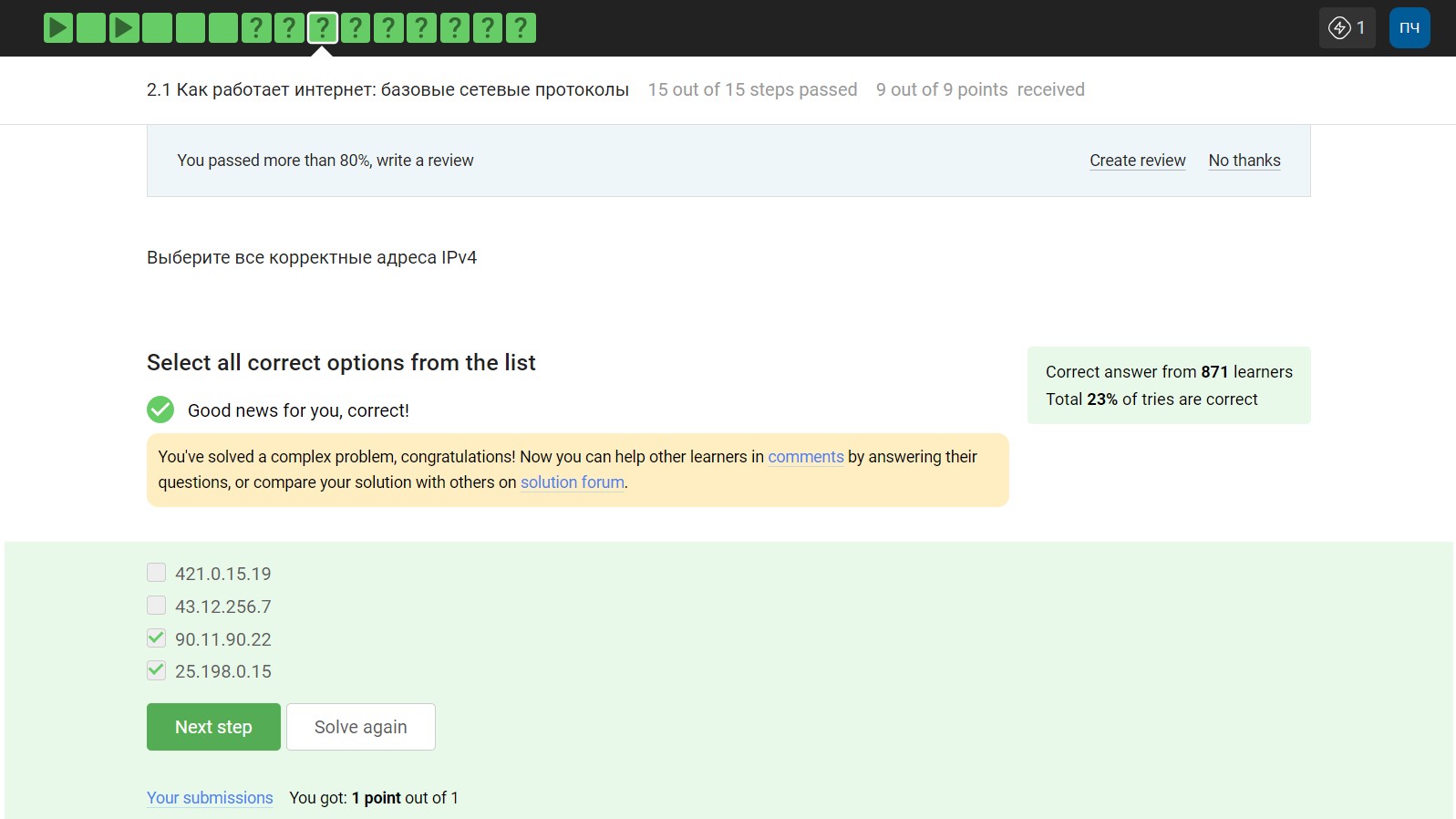


Рис. 3: Рис. 3

DNS сервер: сопоставляет IP адреса доменным именам

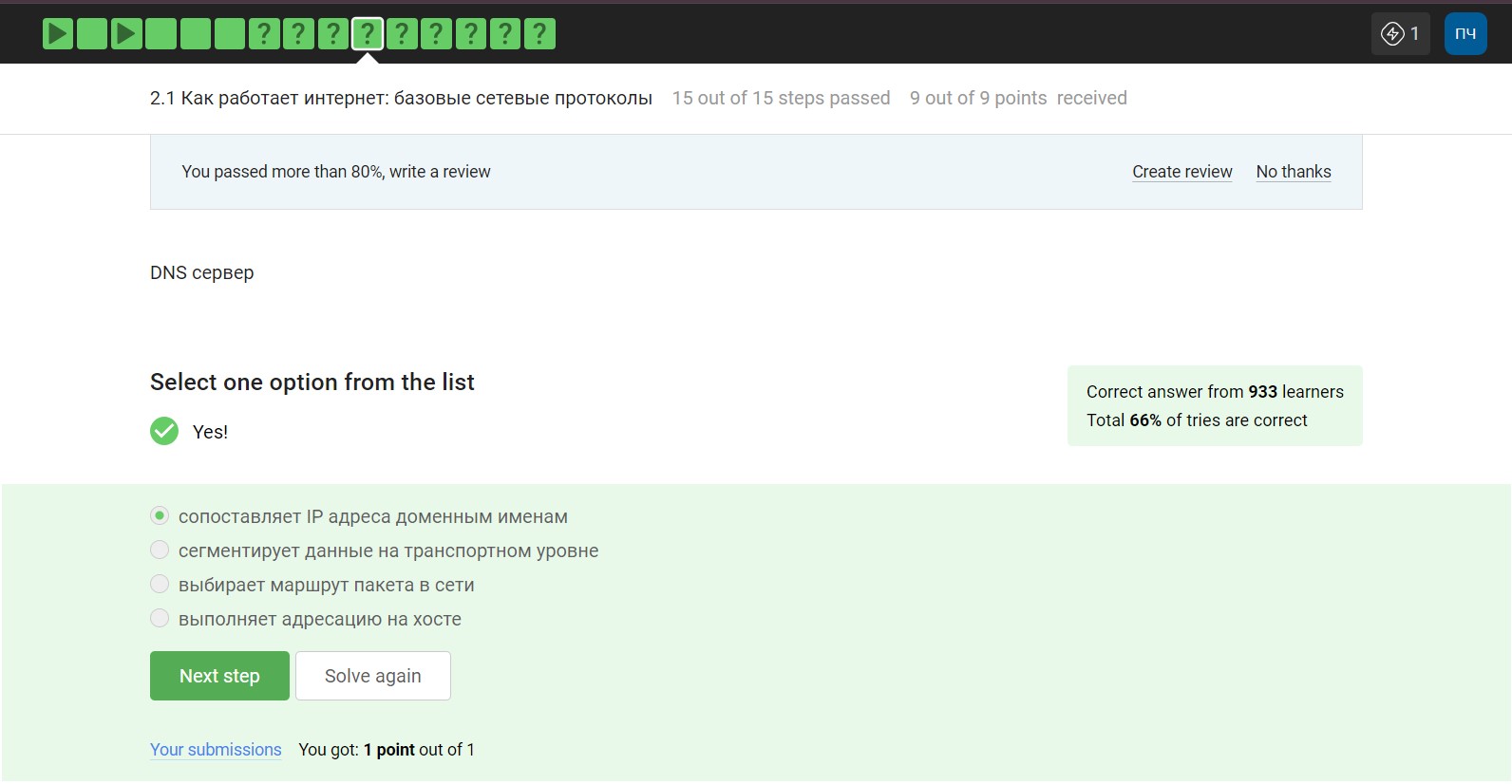


Рис. 4: Рис. 4

Выберите корректную последовательность протоколов в модели TCP/IP: прикладной – транспортный – сетевой – канальный

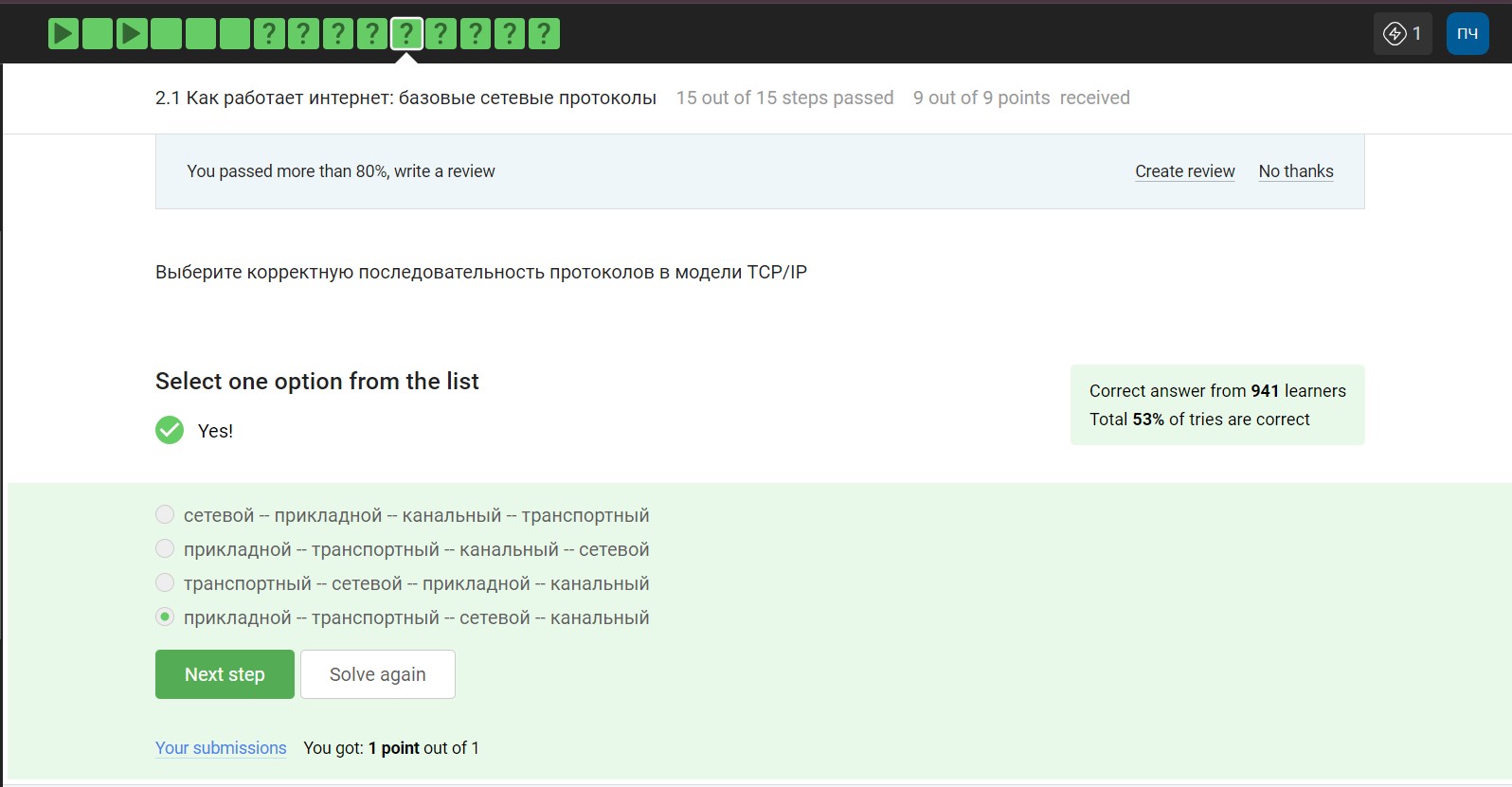


Рис. 5: Рис. 5

Протокол http предполагает: передачу данных между клиентом и сервером в открытом виде

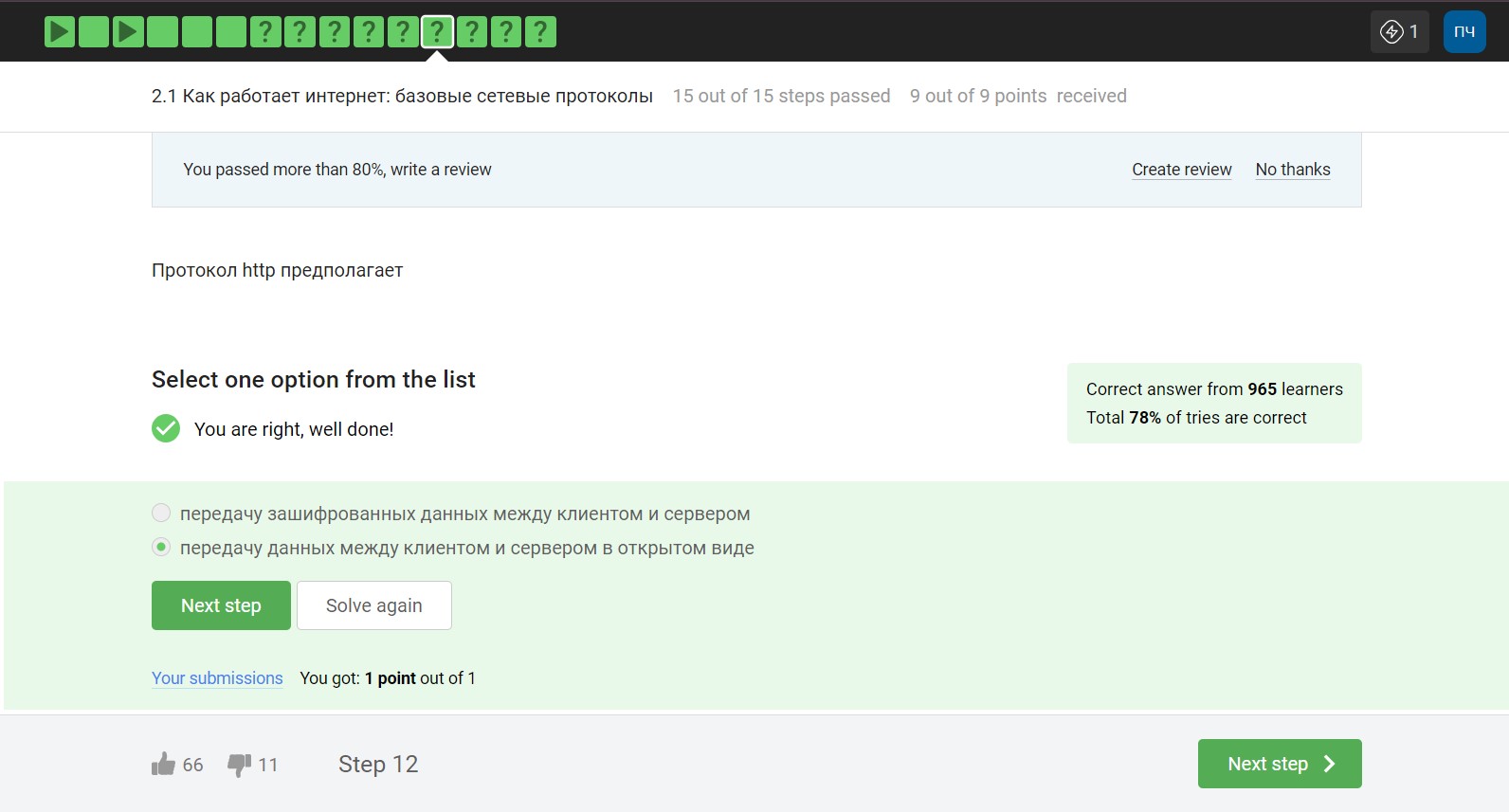


Рис. 6: Рис. 6

Протокол https состоит из: двух фаз: рукопожатия и передачи данных

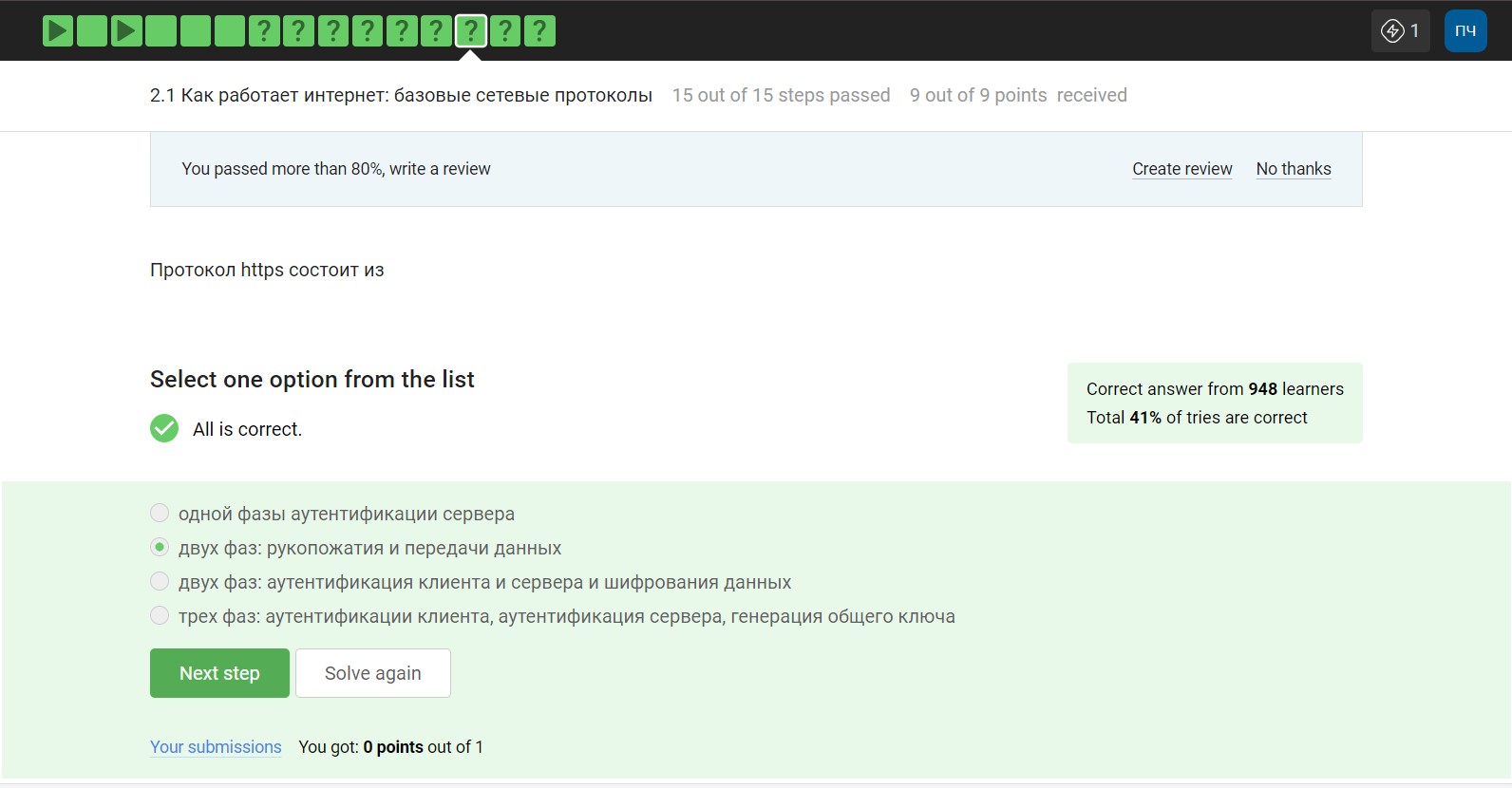


Рис. 7: Рис. 7

Версия протокола TLS определяется: и клиентом, и сервером в процессе “переговоров”

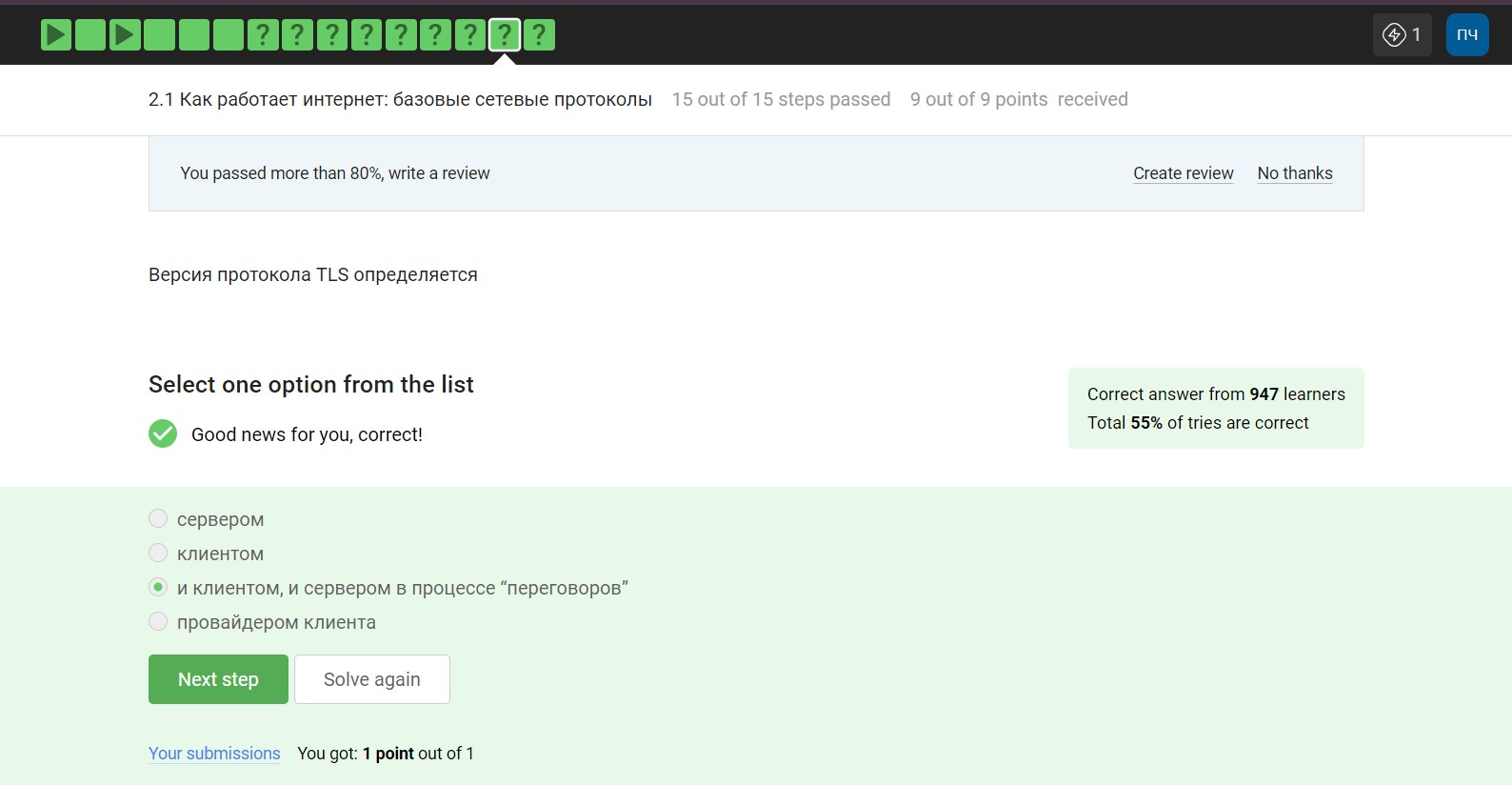


Рис. 8: Рис. 8

В фазе “рукопожатия” протокола TLS не предусмотрено: шифрование данных



Рис. 9: Рис. 9

# 3 Раздел 2.2

Куки хранят: id сессии, идентификатор пользователя

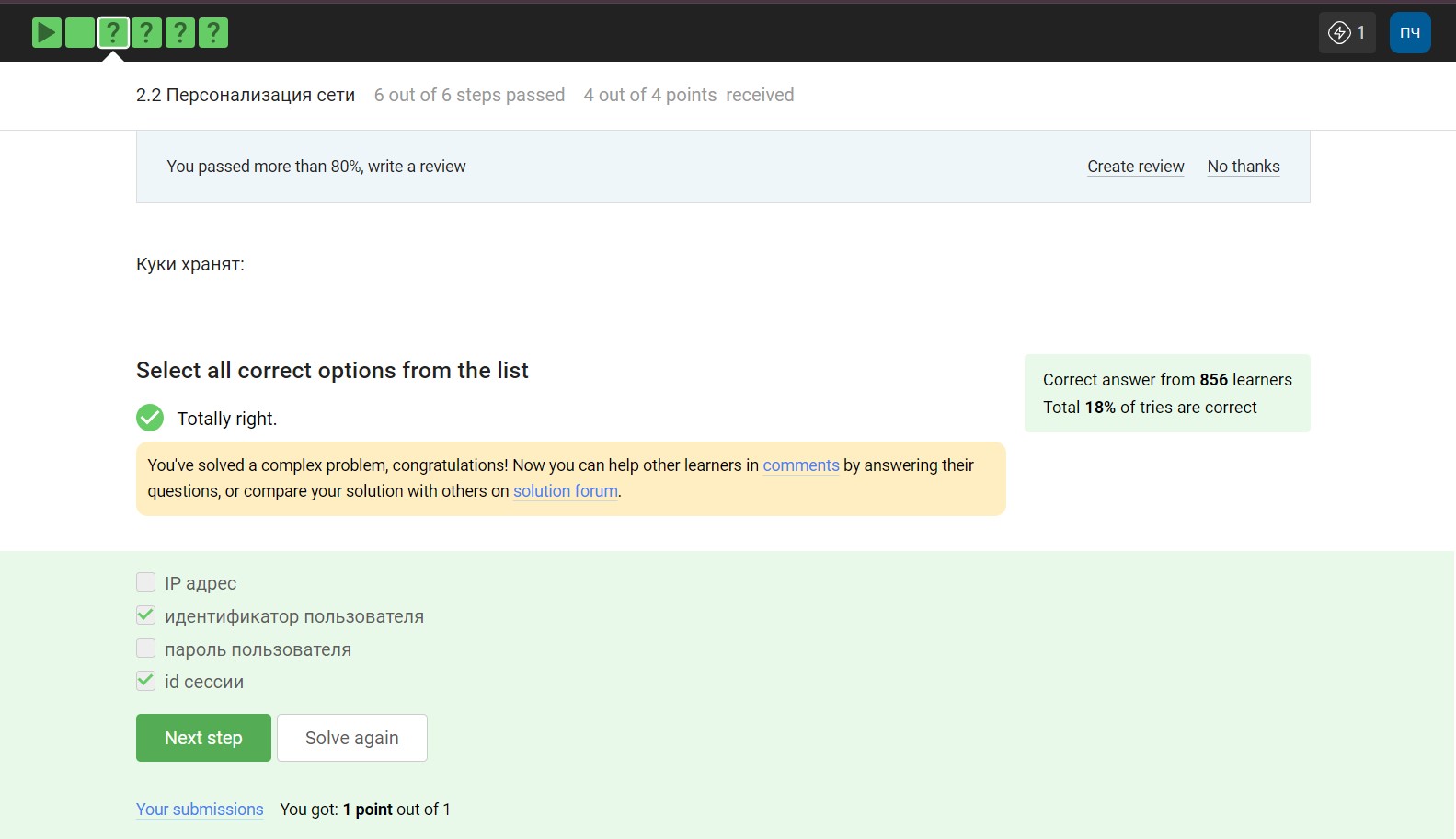


Рис. 10: Рис. 1

Куки не используются для: улучшения надежности соединения

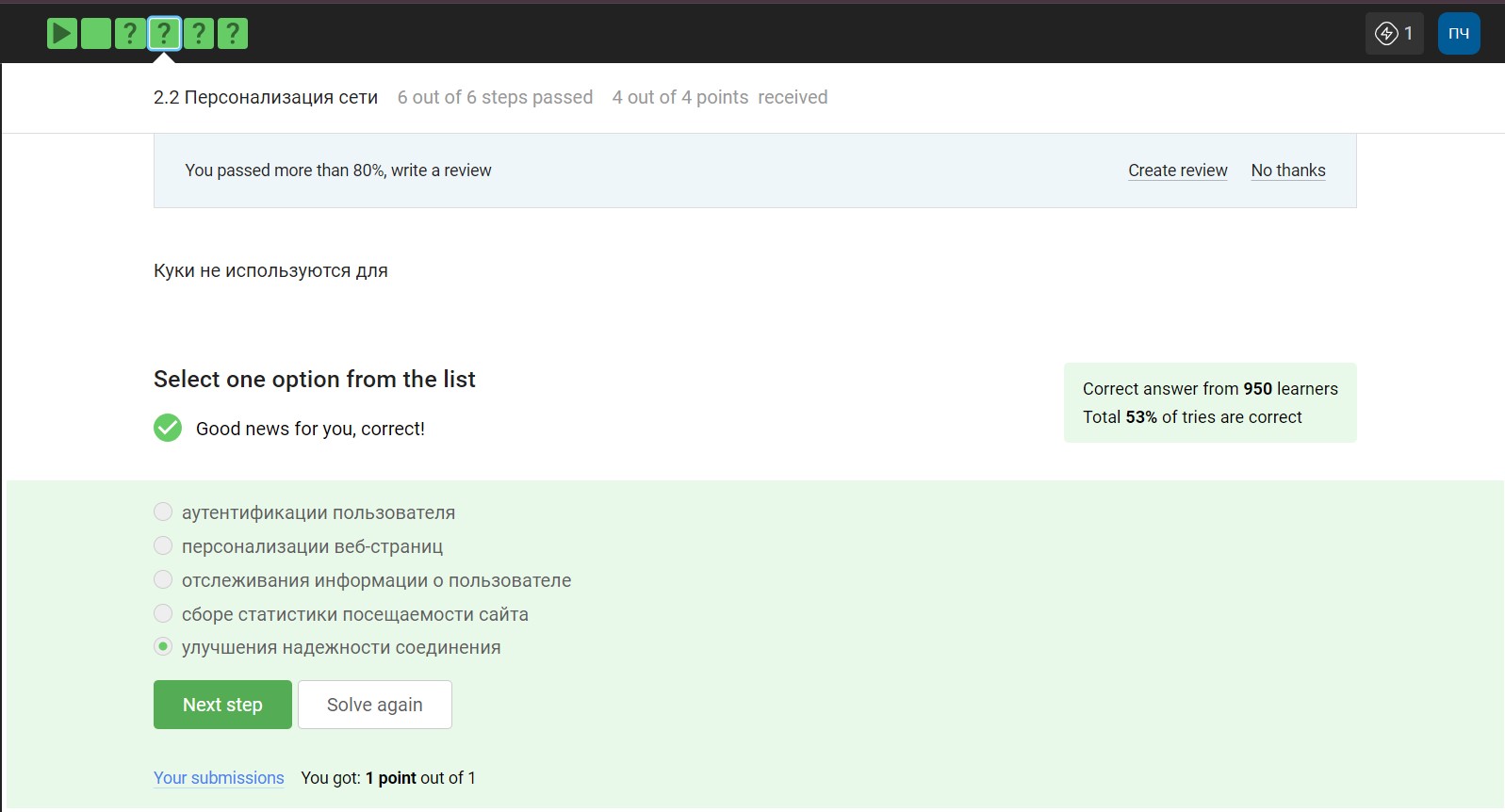


Рис. 11: Рис. 2

Куки генерируются: сервером

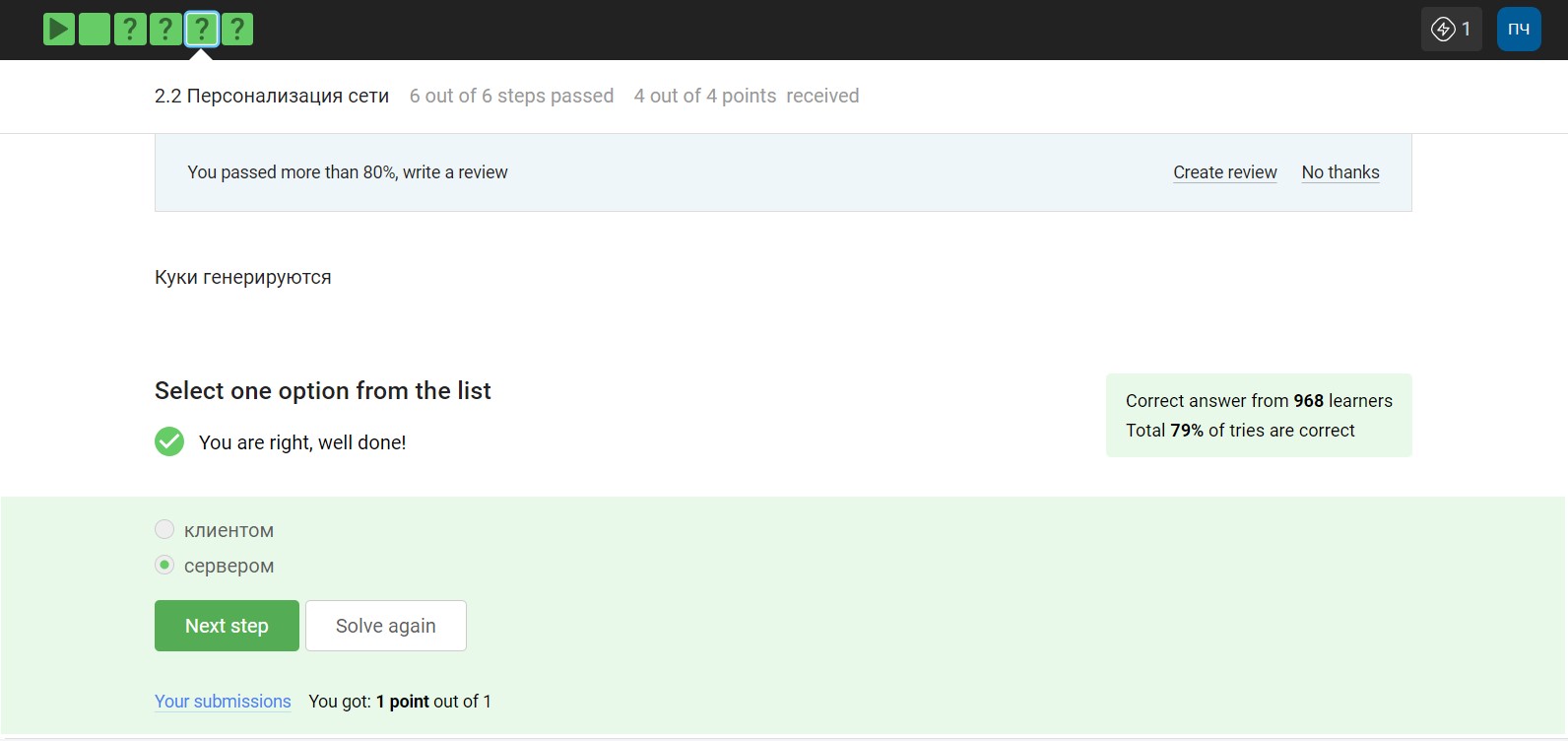


Рис. 12: Рис. 3

Сессионные куки хранятся в браузере? Да, на время пользования веб-сайтом

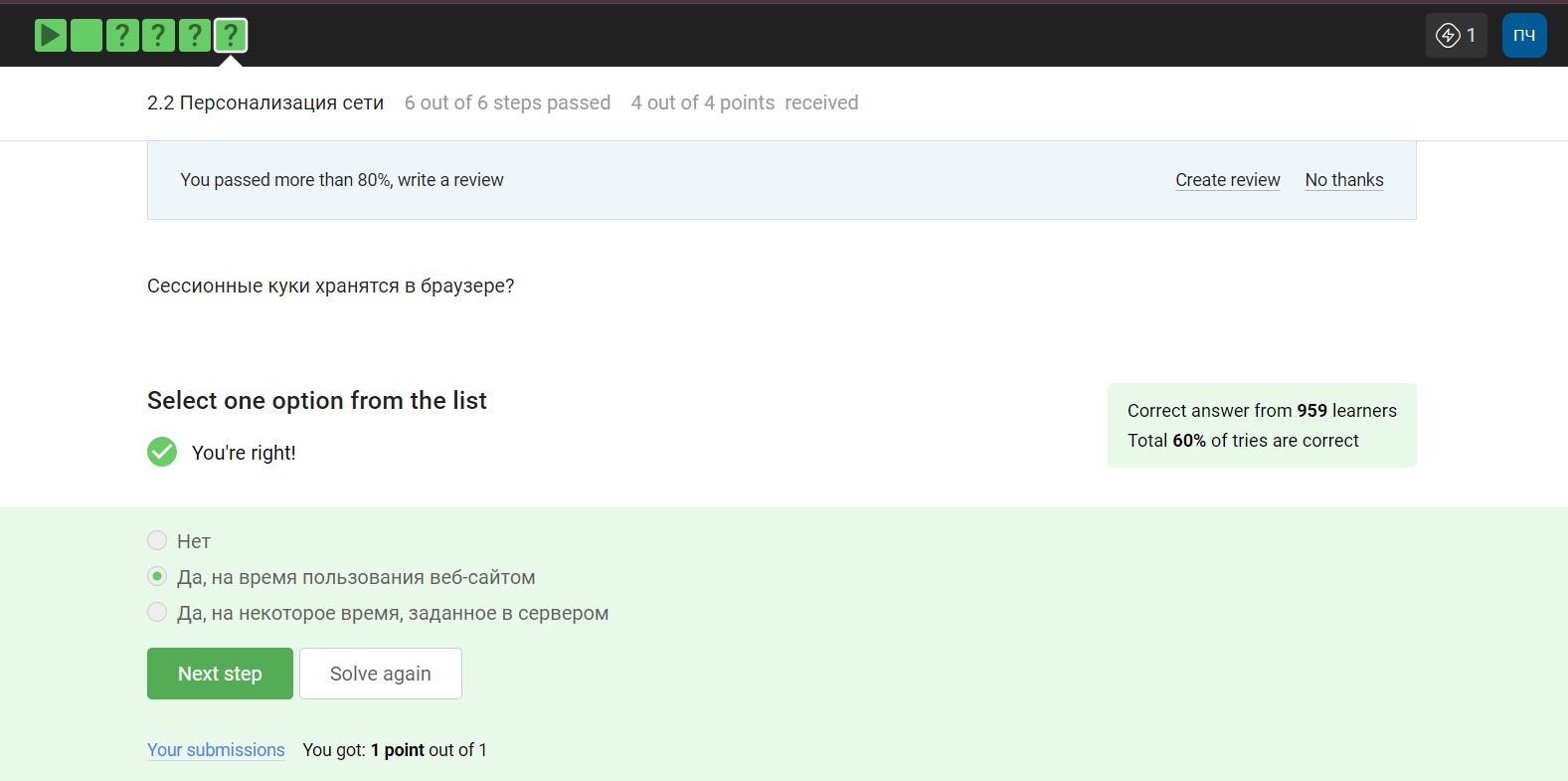


Рис. 13: Рис. 4

# 4 Раздел 2.3

Сколько промежуточных узлов в луковой сети TOR? 3

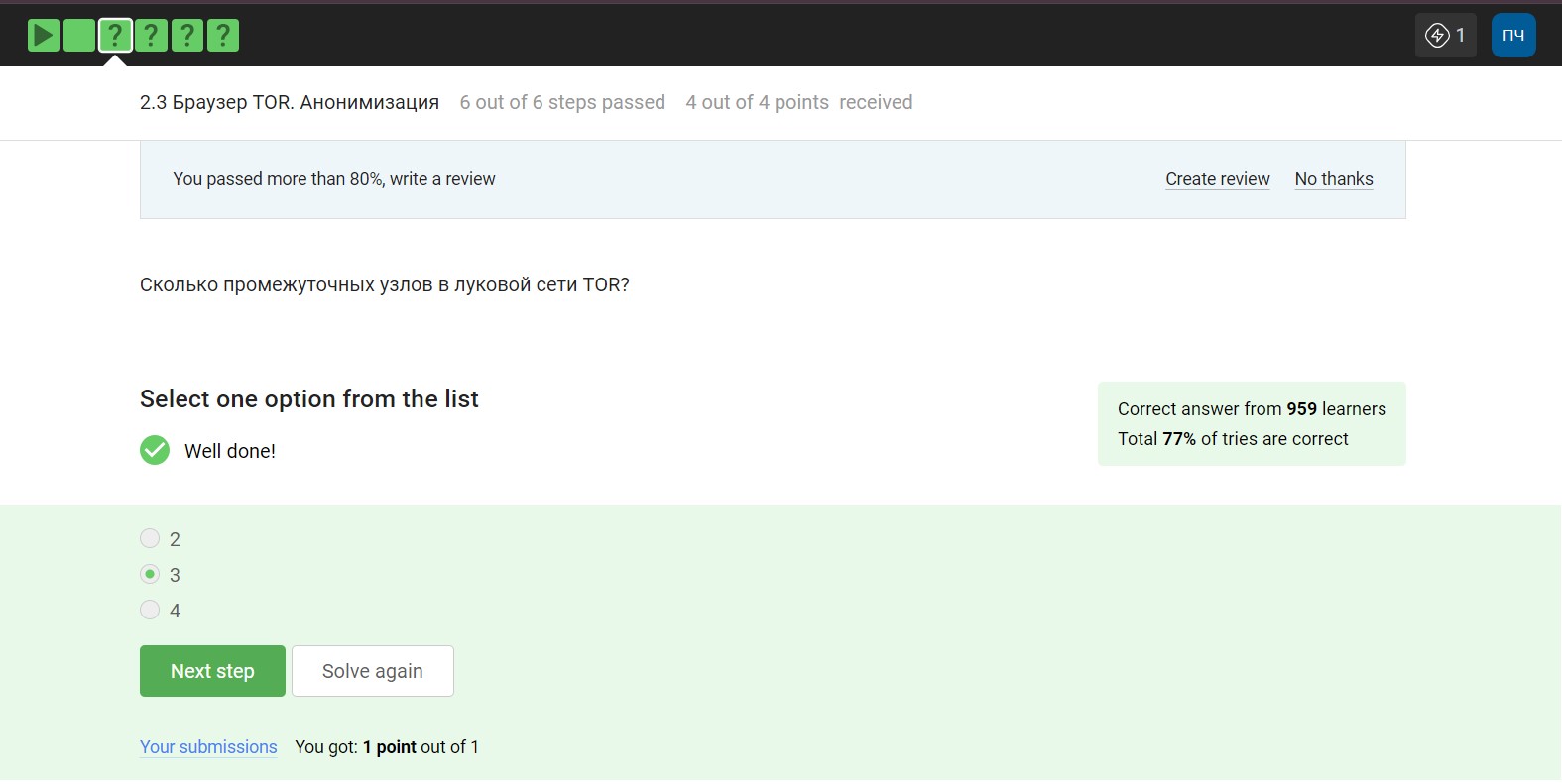


Рис. 14: Рис. 1

IP-адрес получателя известен: отправителю, выходному узлу

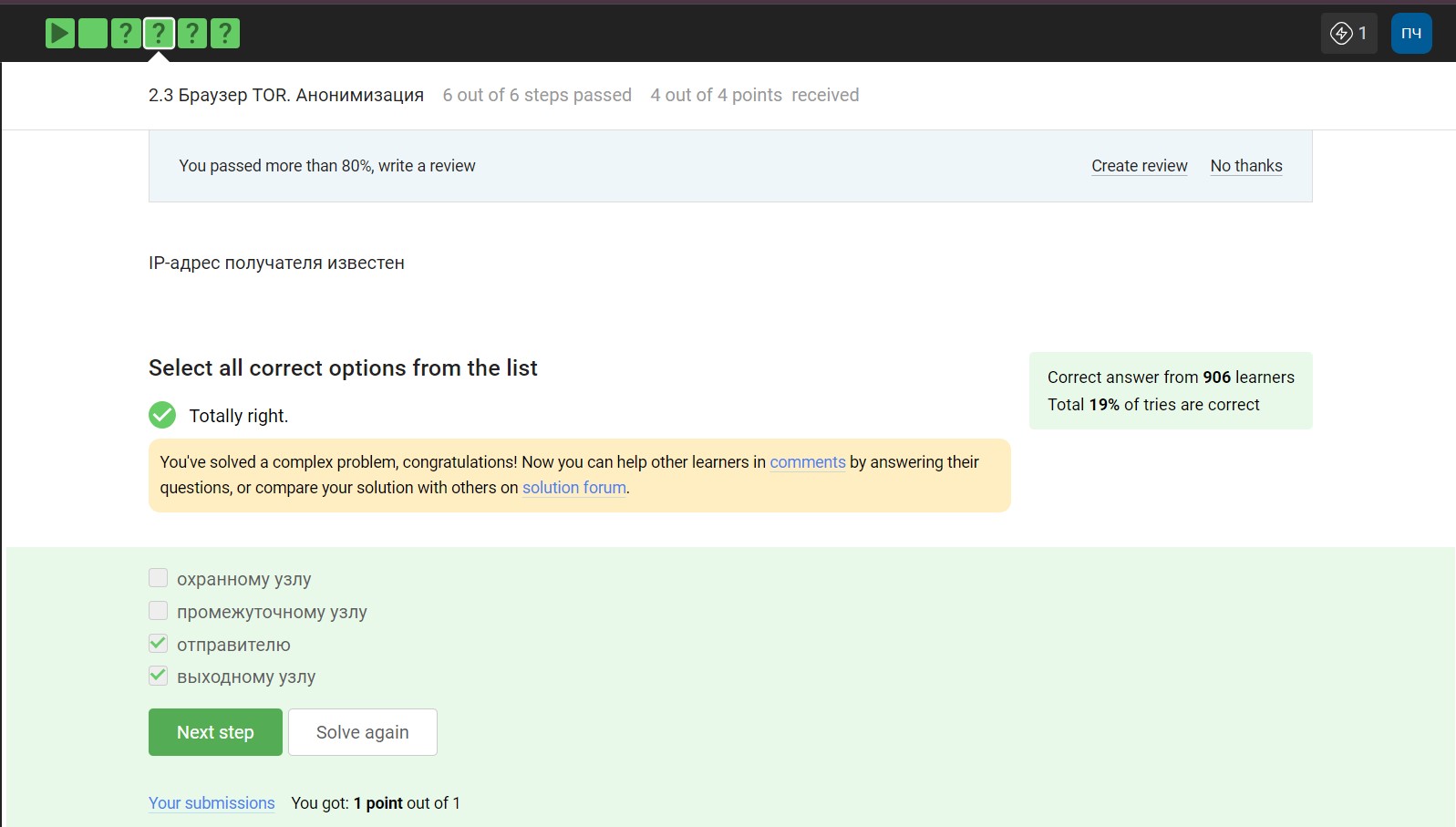


Рис. 15: Рис. 2

Отправитель генерирует общий секретный ключ: с охранным, промежуточным и выходном узлом

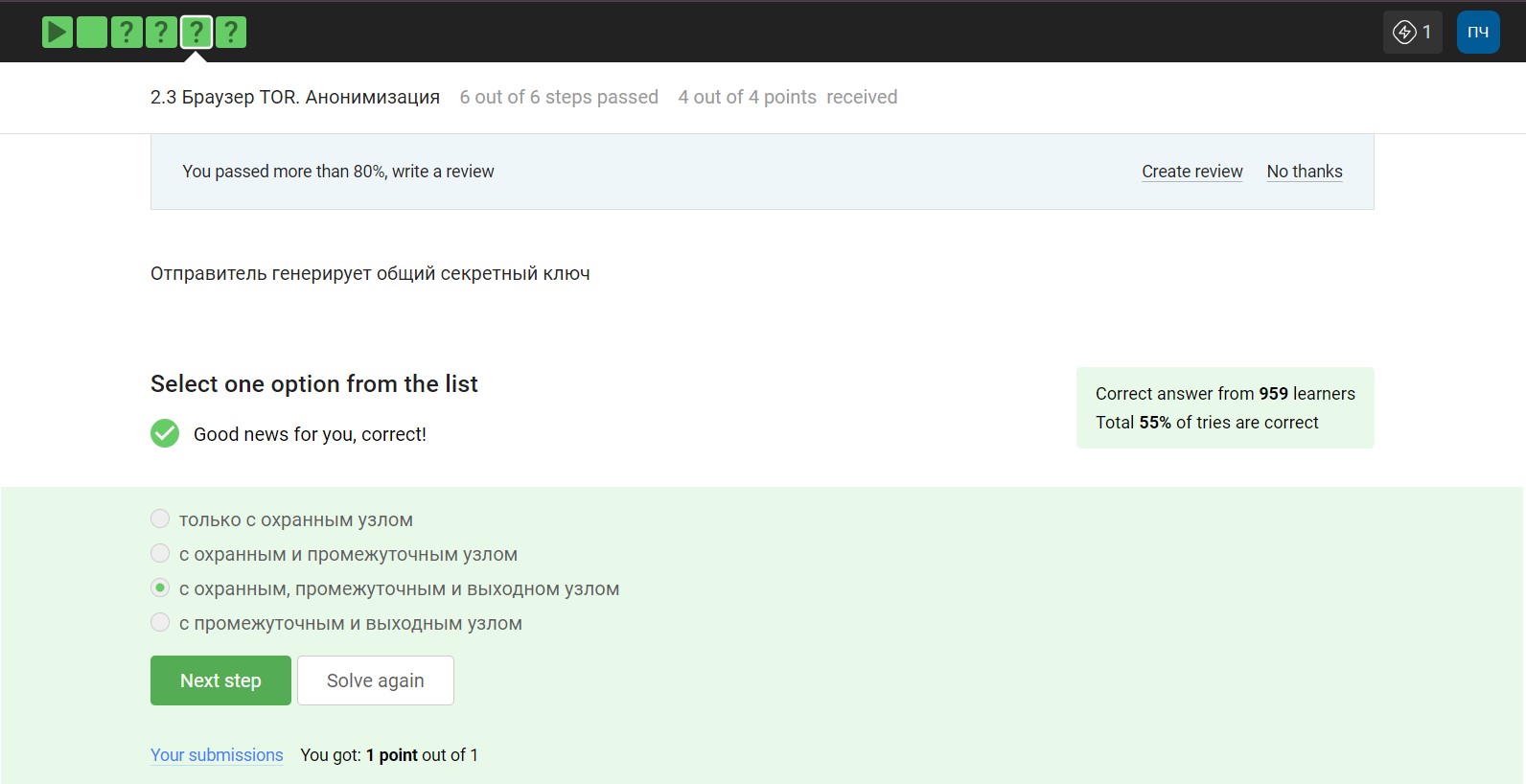


Рис. 16: Рис. 3

Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов? Нет

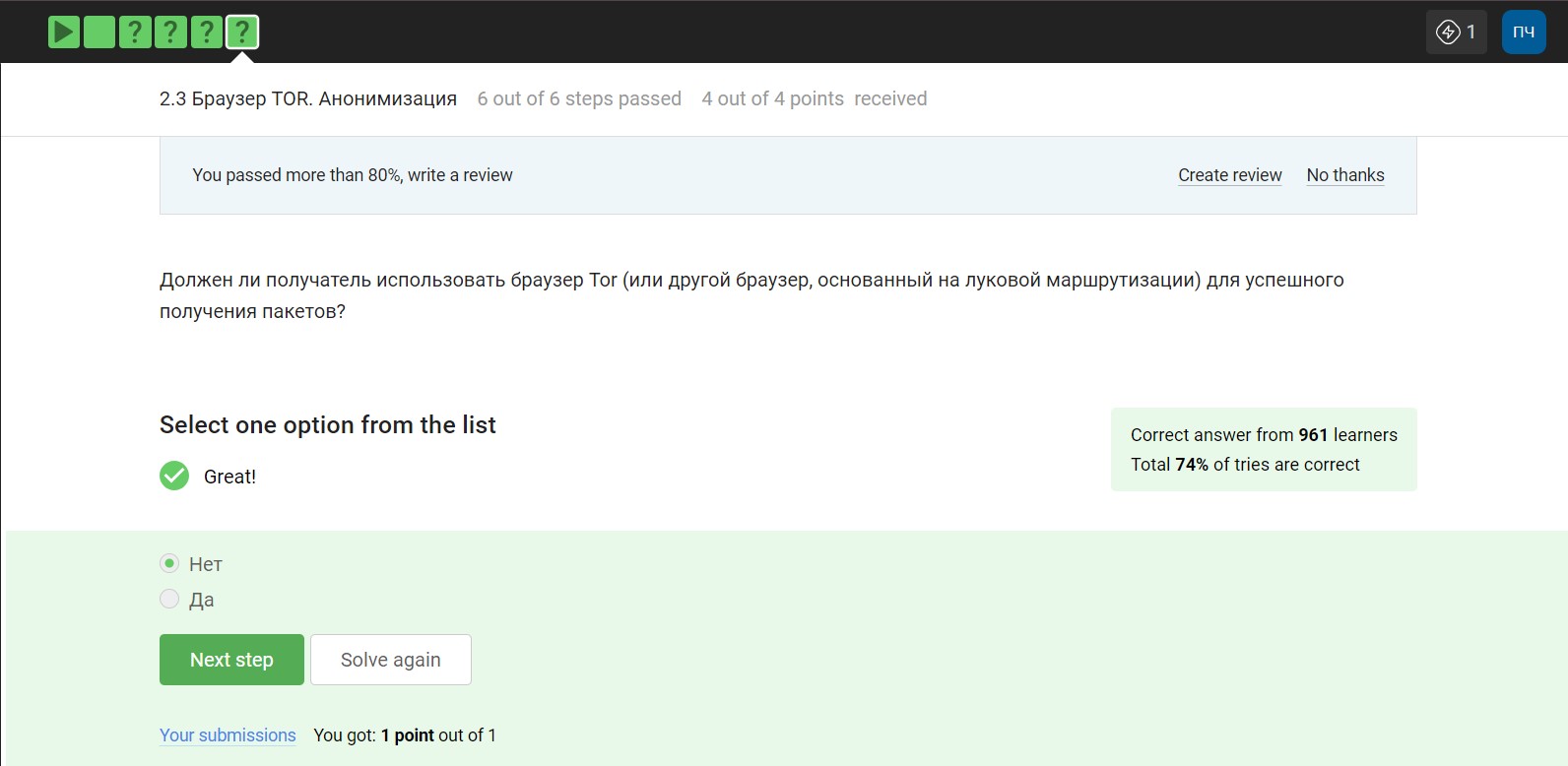


Рис. 17: Рис. 4

# 5 Раздел 2.4

Wi-Fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11



Рис. 18: Рис. 1

На каком уровне работает протокол WiFi? Канальном

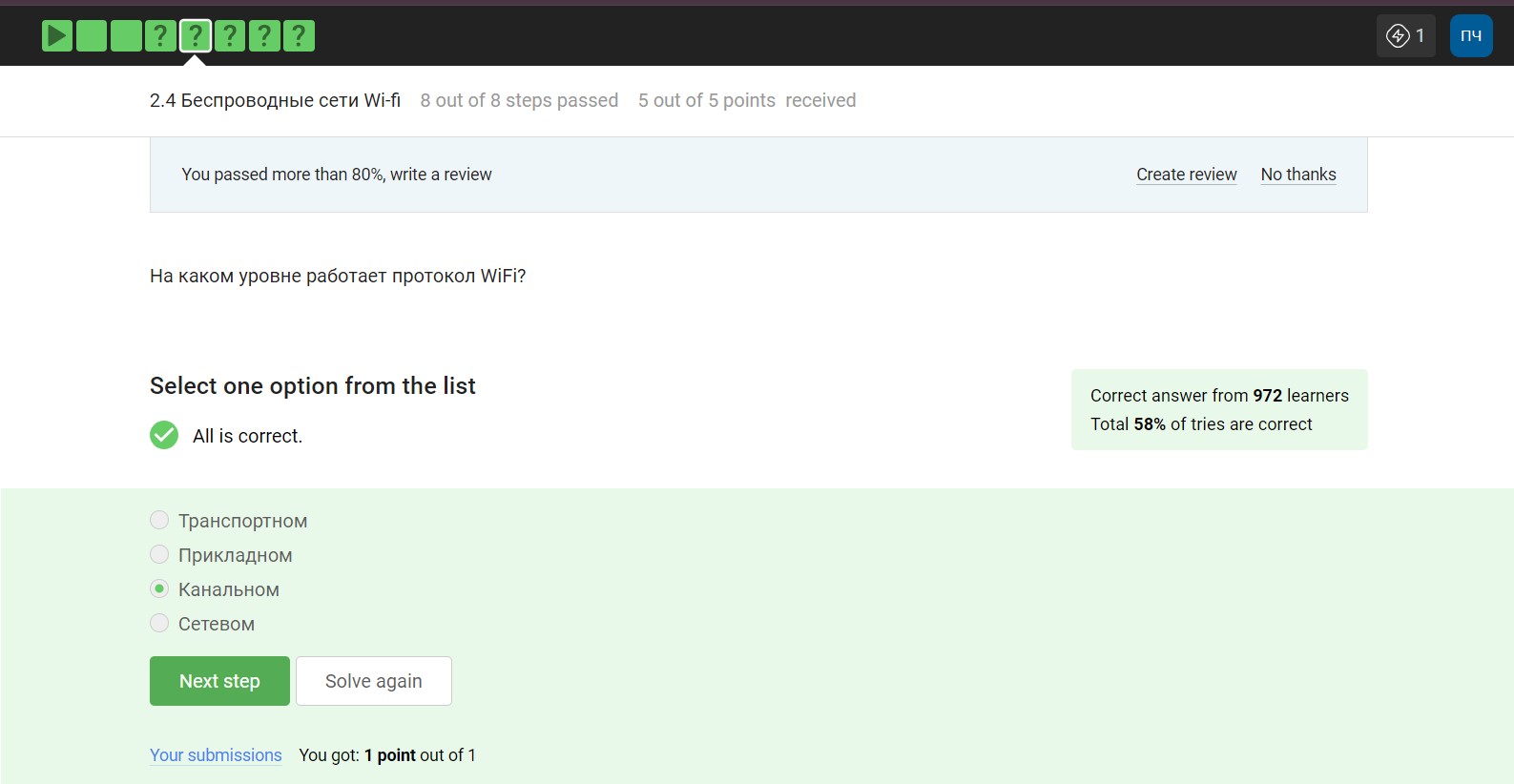


Рис. 19: Рис. 2

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi WEP

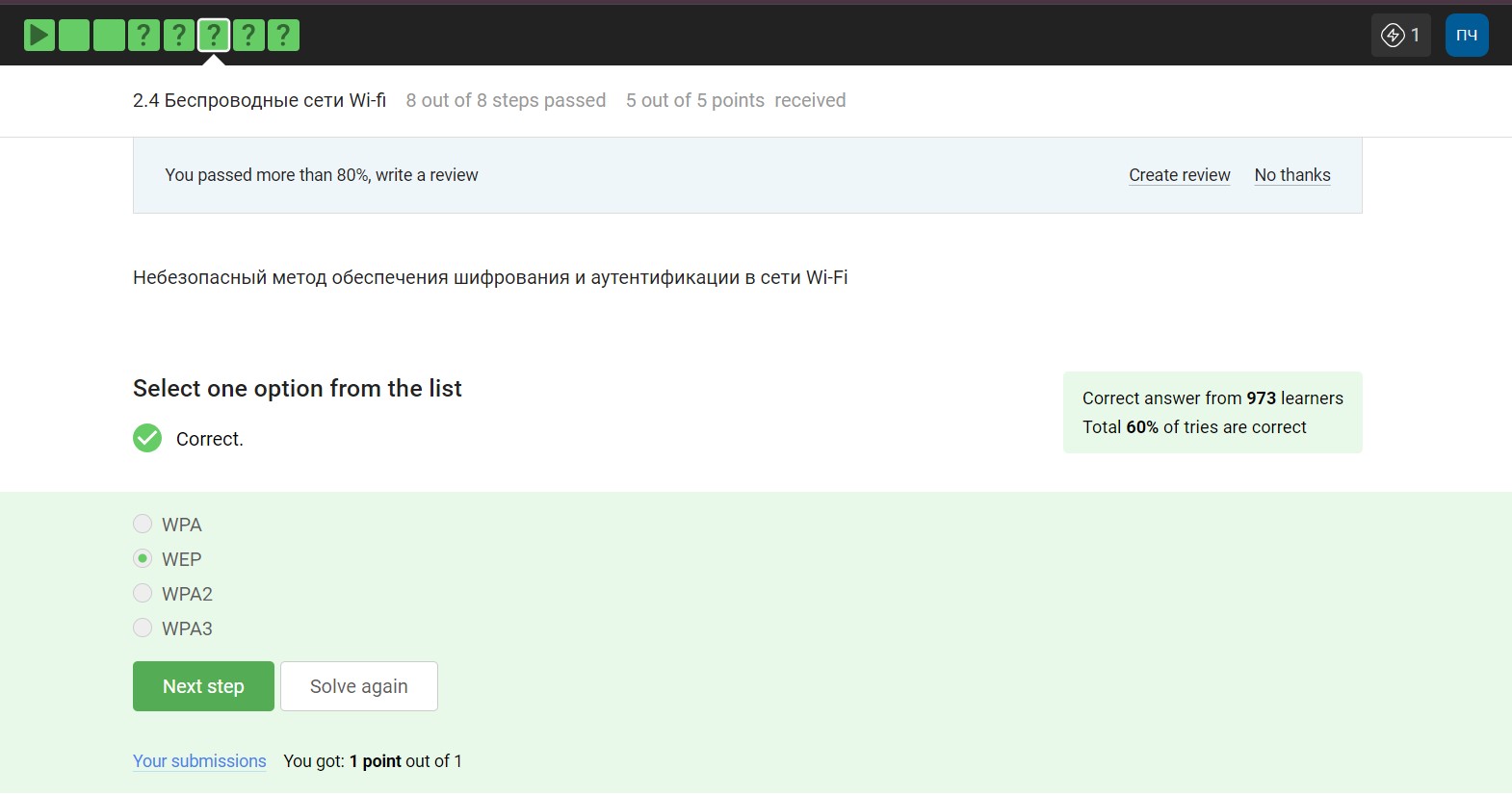


Рис. 20: Рис. 3

Данные между хостом сети (компьютером или смартфоном) и роутером: передаются в зашифрованном виде после аутентификации устройств



Рис. 21: Рис. 4

Для домашней сети для аутентификации обычно используется метод: WPA2 Personal

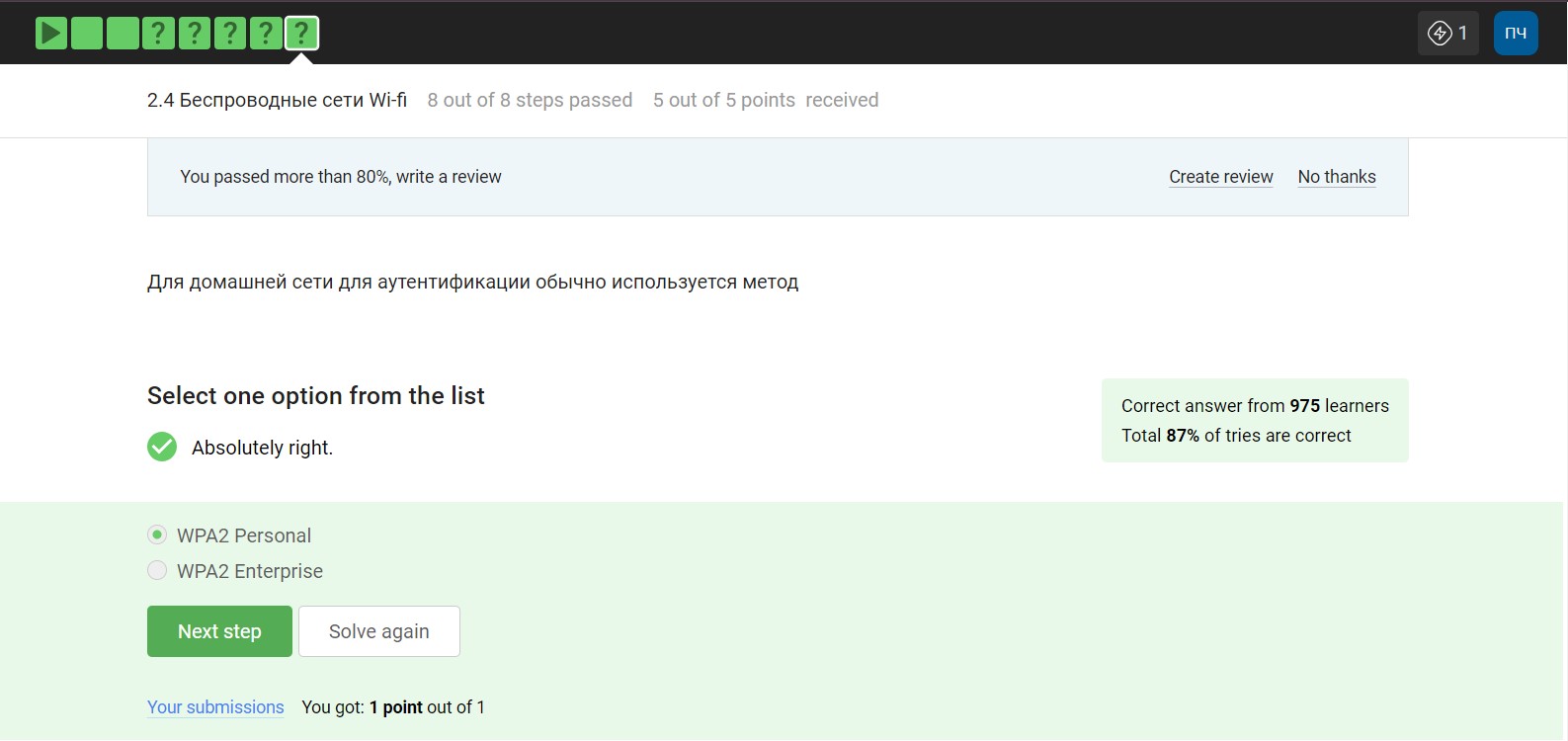


Рис. 22: Рис. 5

# 6 Раздел 3.1. защита ПК и телефона

Можно ли зашифровать загрузочный сектор диска: да

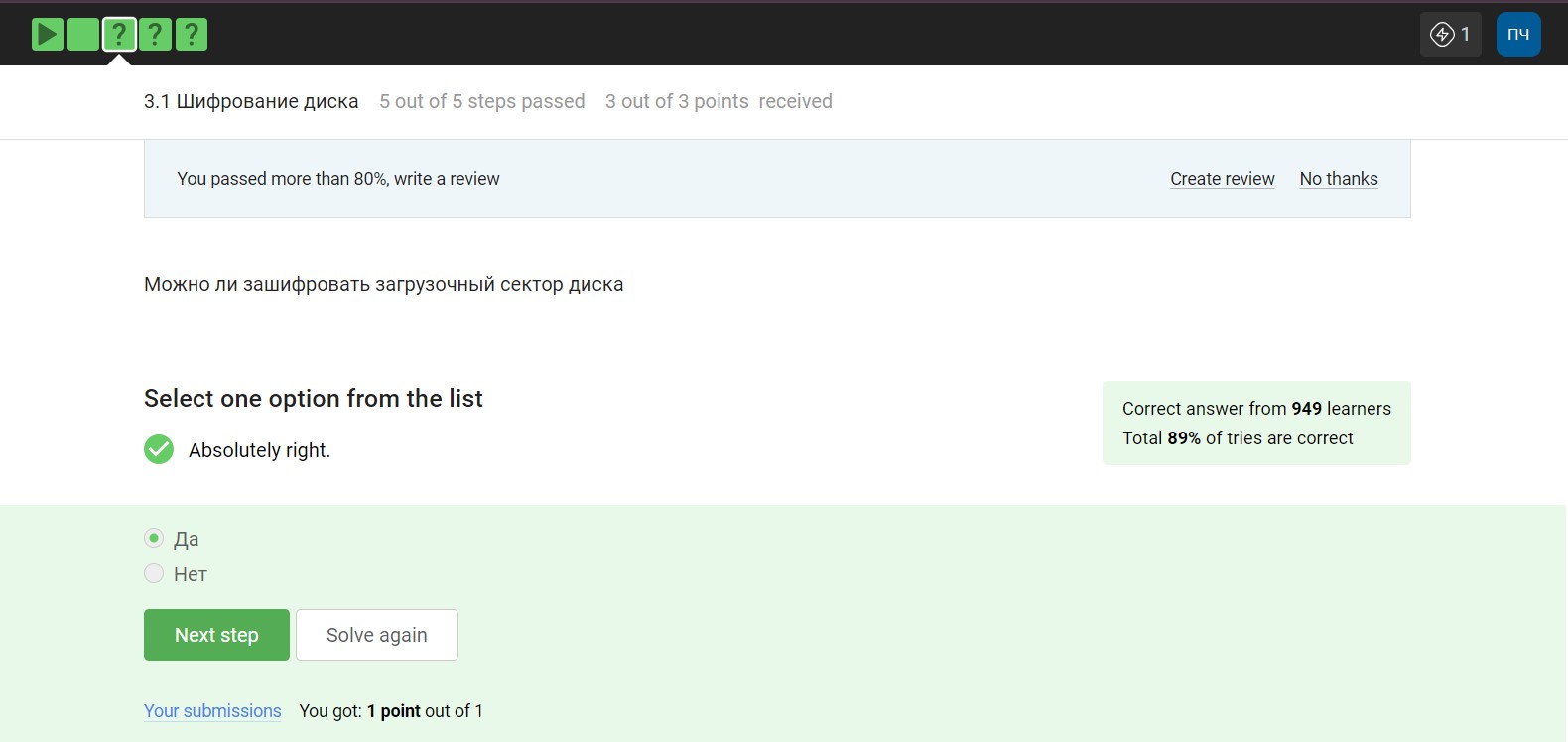


Рис. 23: Рис. 1

Шифрование диска основано на: симметричном шифровании

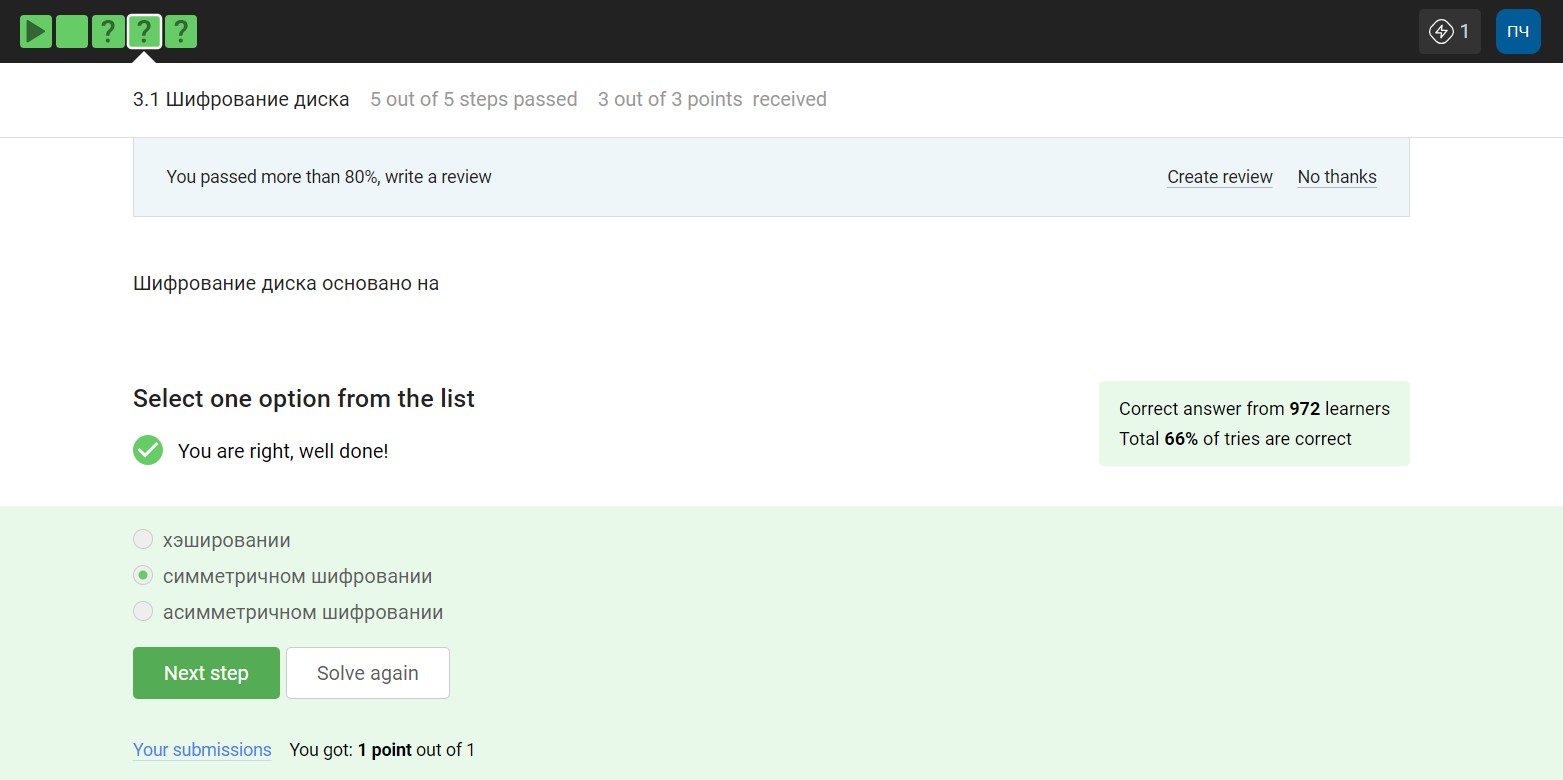


Рис. 24: Рис. 2

С помощью каких программ можно зашифровать жесткий диск?:BitLocker, VeraCrypt

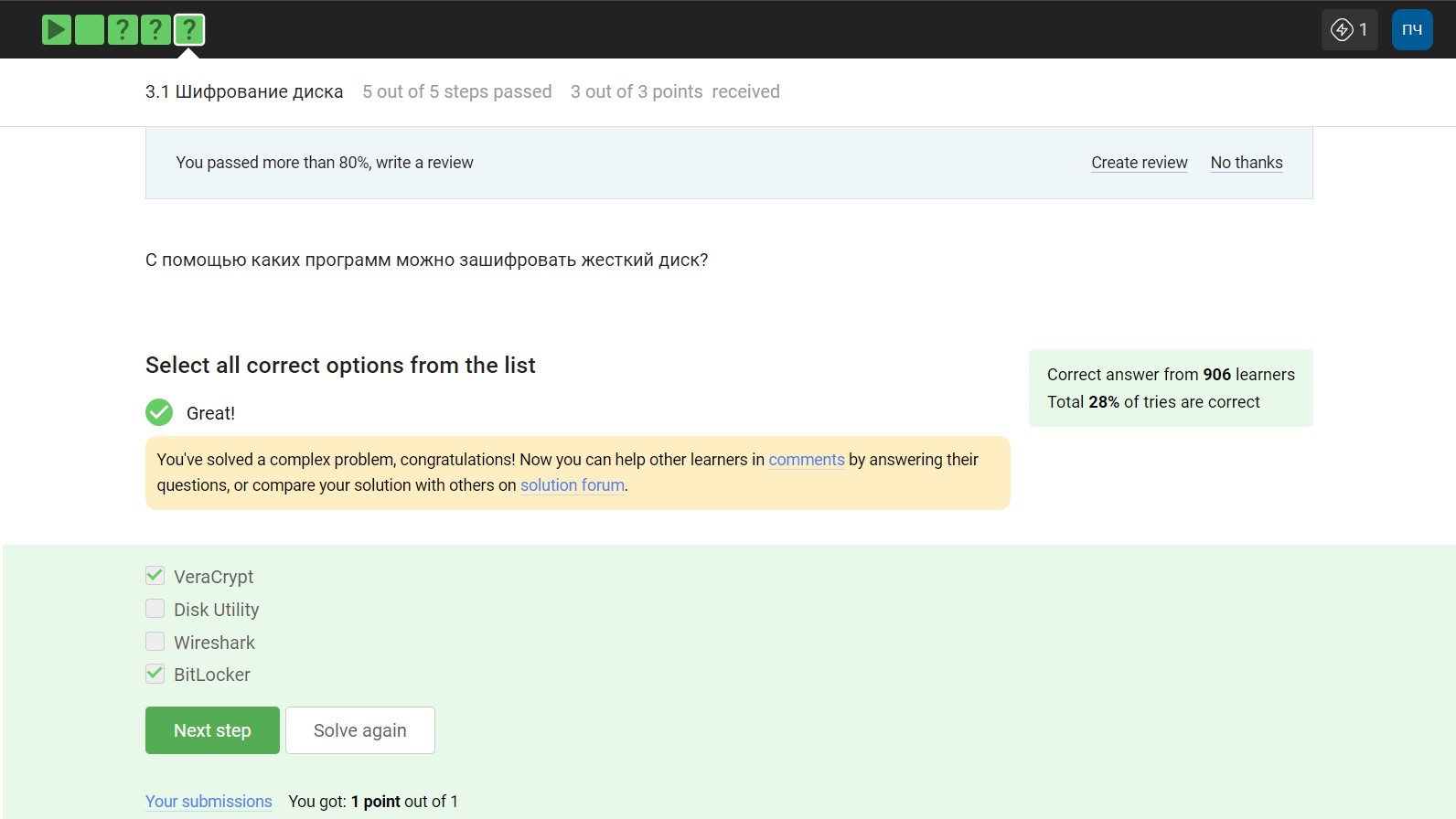


Рис. 25: Рис. 3

# 7 Раздел 3.2. Пароли

Какие пароли можно отнести с стойким? UQr9@j4!S$



Рис. 26: Рис. 1

Где безопасно хранить пароли? В менеджерах паролей

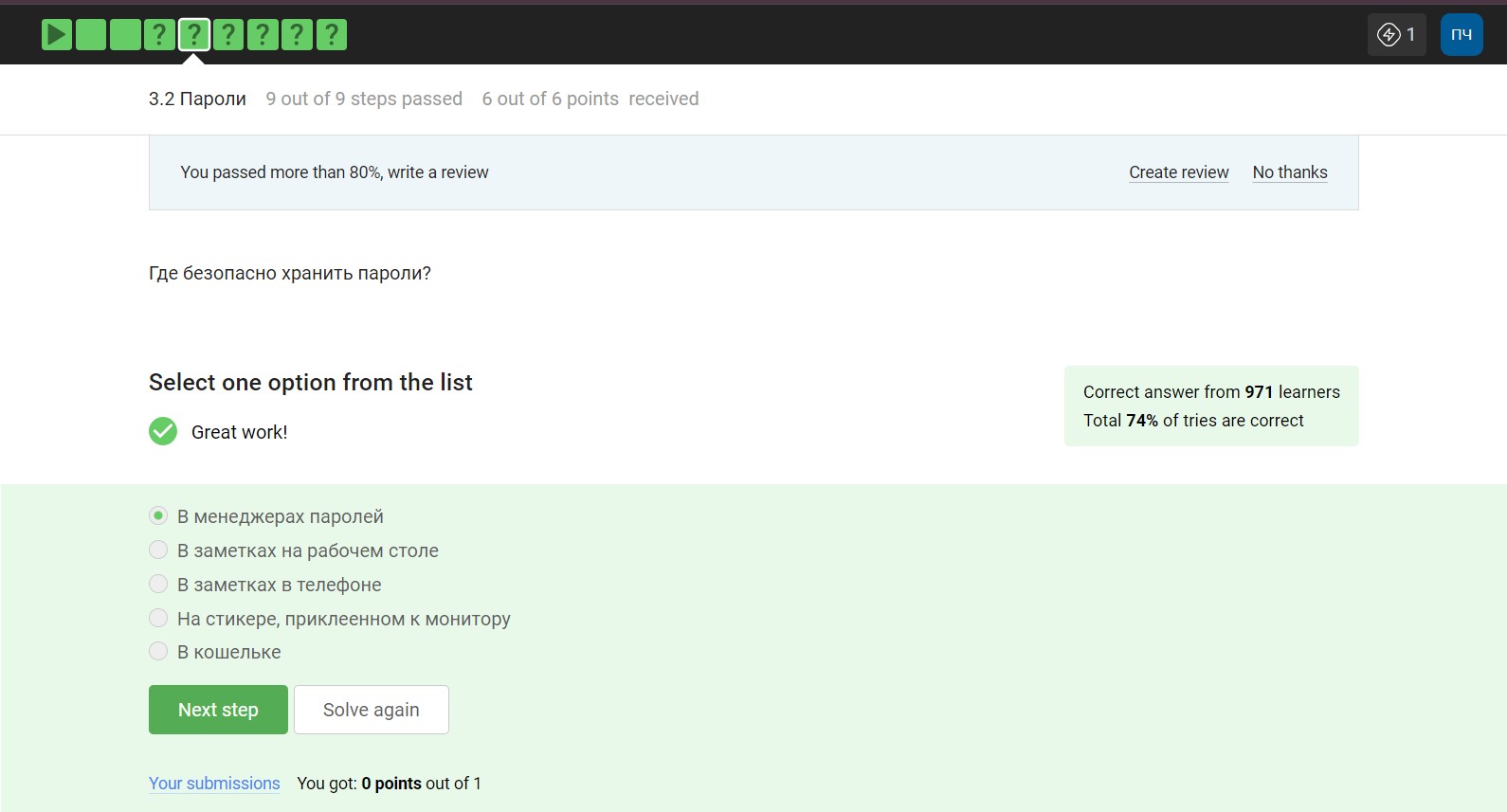


Рис. 27: Рис. 2

Зачем нужна капча?Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

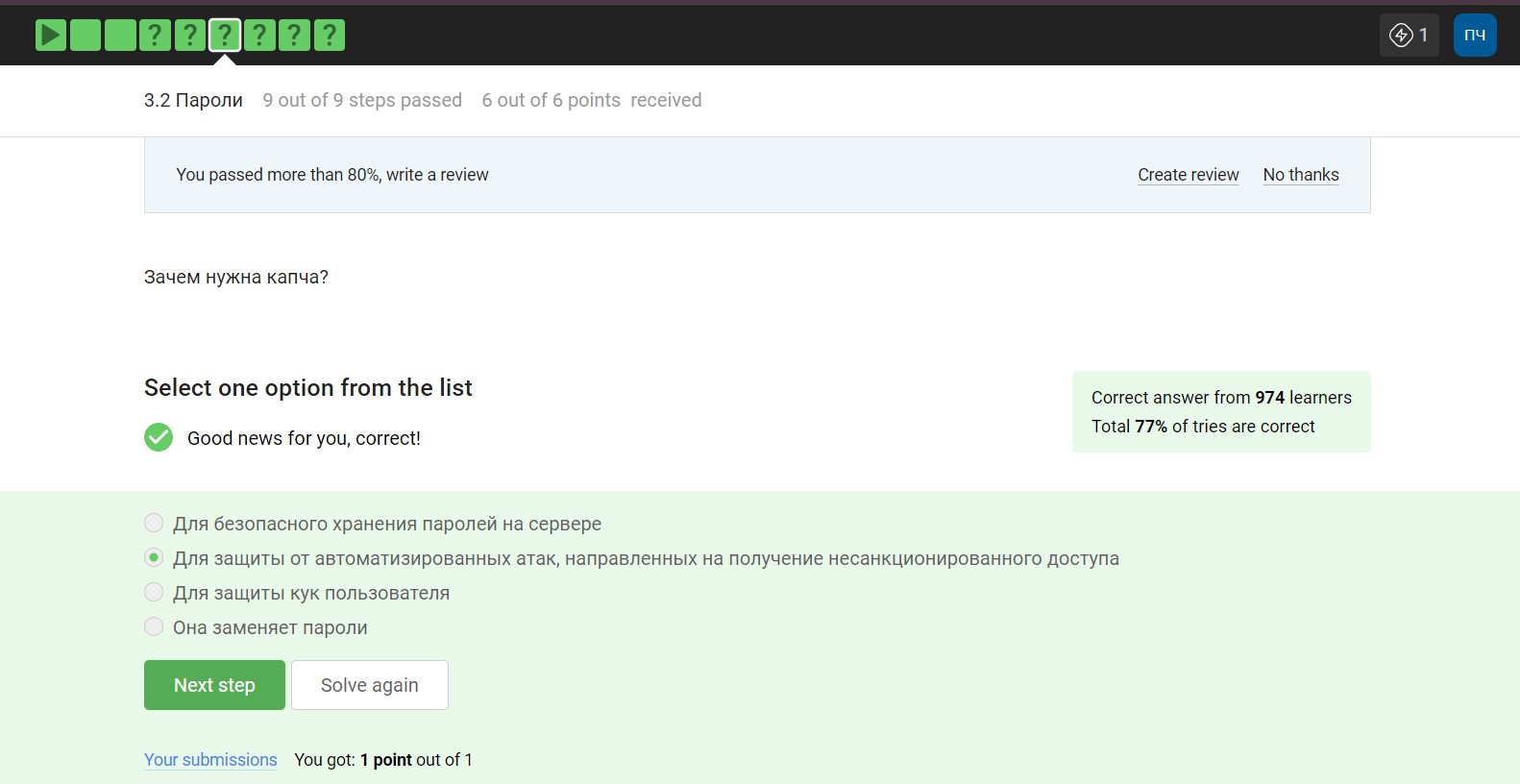
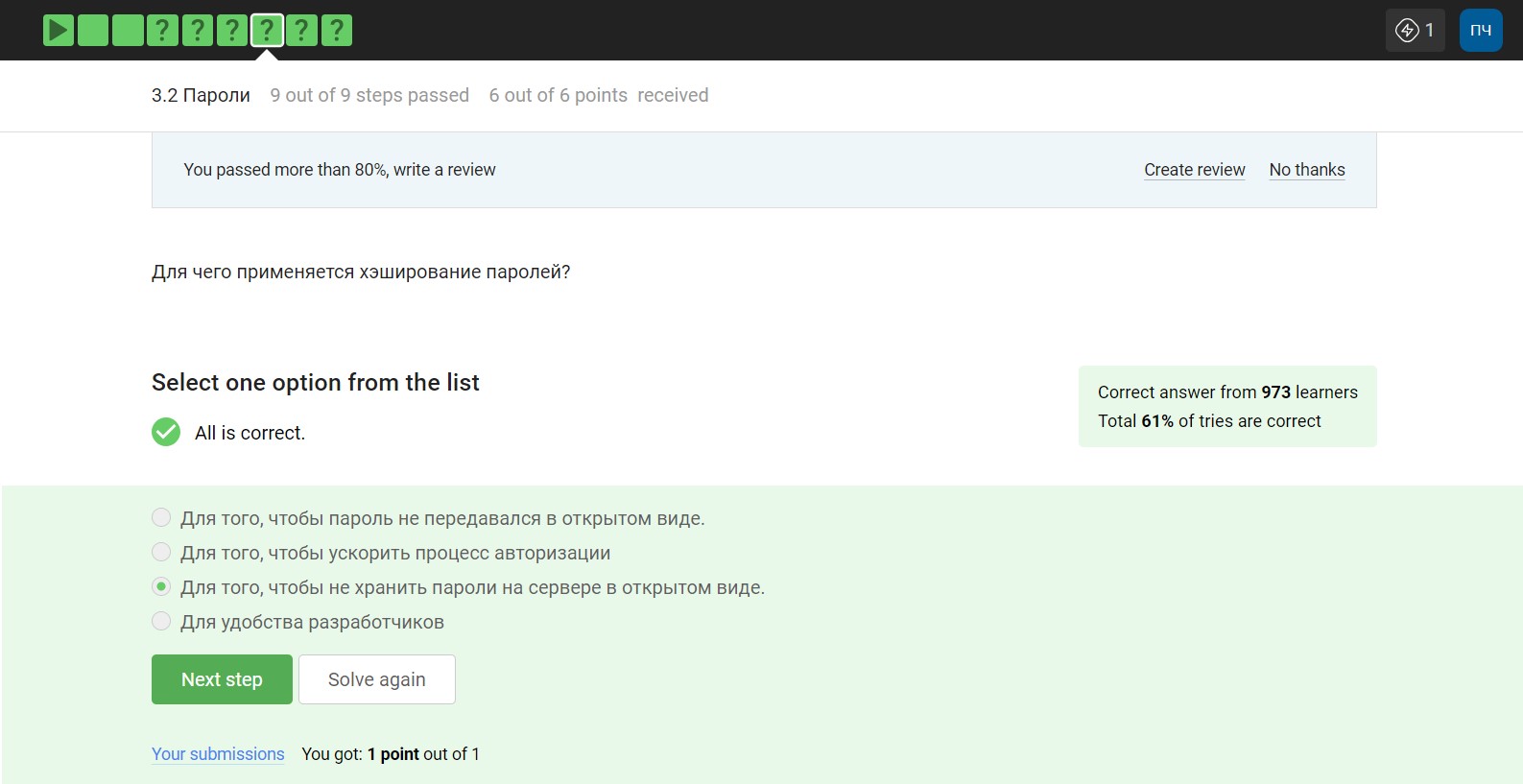


Рис. 28: Рис. 3

Для чего применяется хэширование паролей?Для того, чтобы не хранить пароли на сервере в открытом виде. 

Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу? Нет

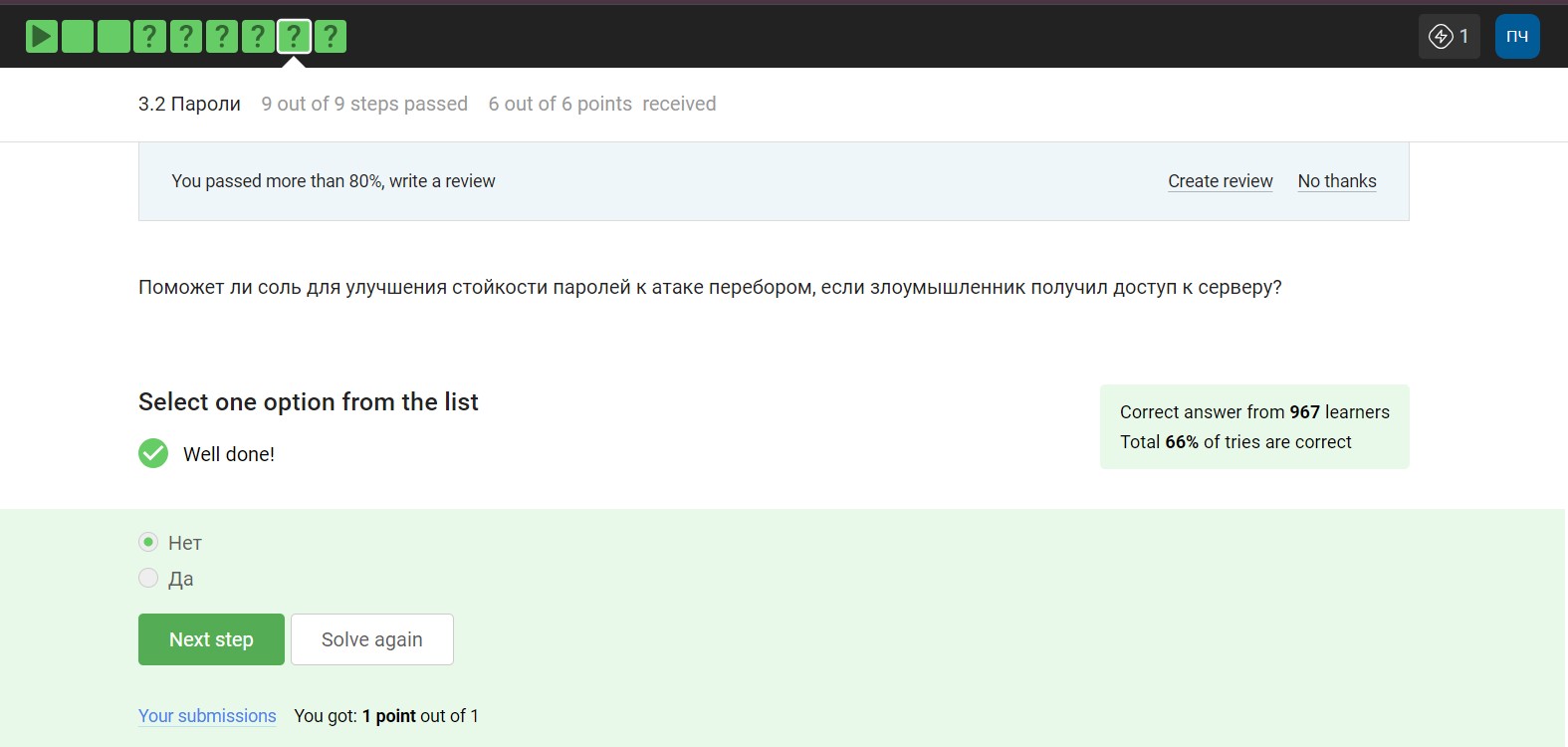


Рис. 29: Рис. 5

Какие меры защищают от утечек данных атакой перебором?

* разные пароли на всех сайтах
* периодическая смена паролей
* сложные(=длинные) пароли
* капча

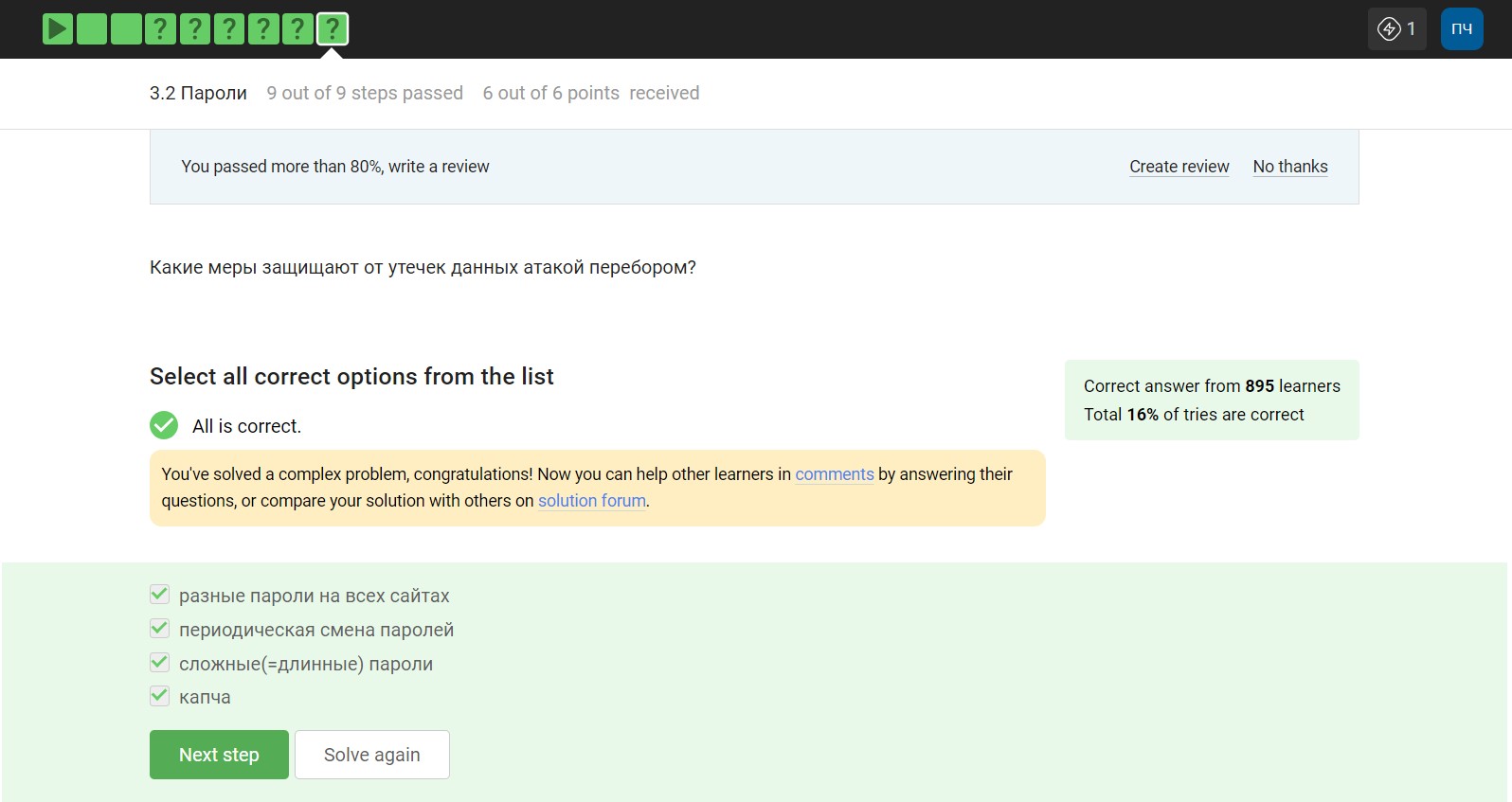


Рис. 30: Рис. 6

# 8 Раздел 3.3. Фишинг

Какие из следующих ссылок являются фишинговыми? - https://online.sberbank.wix.ru/CSAFront/index.do (вход в Сбербанк.Онлайн) - https://passport.yandex.ucoz.ru/auth?origin=home\_desktop\_ru (вход в аккаунт Яндекс)

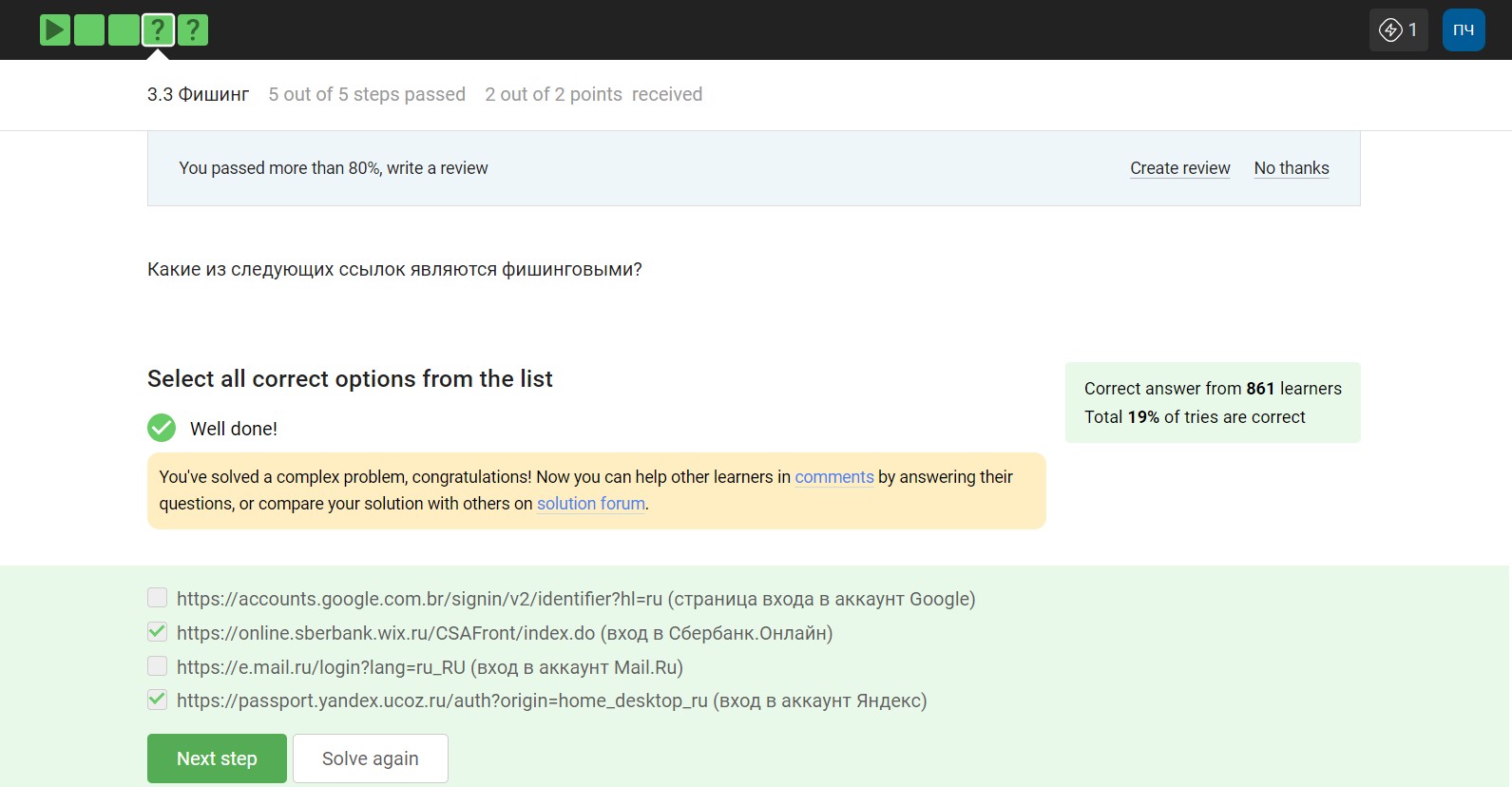


Рис. 31: Рис. 1

Может ли фишинговый имейл прийти от знакомого адреса? да

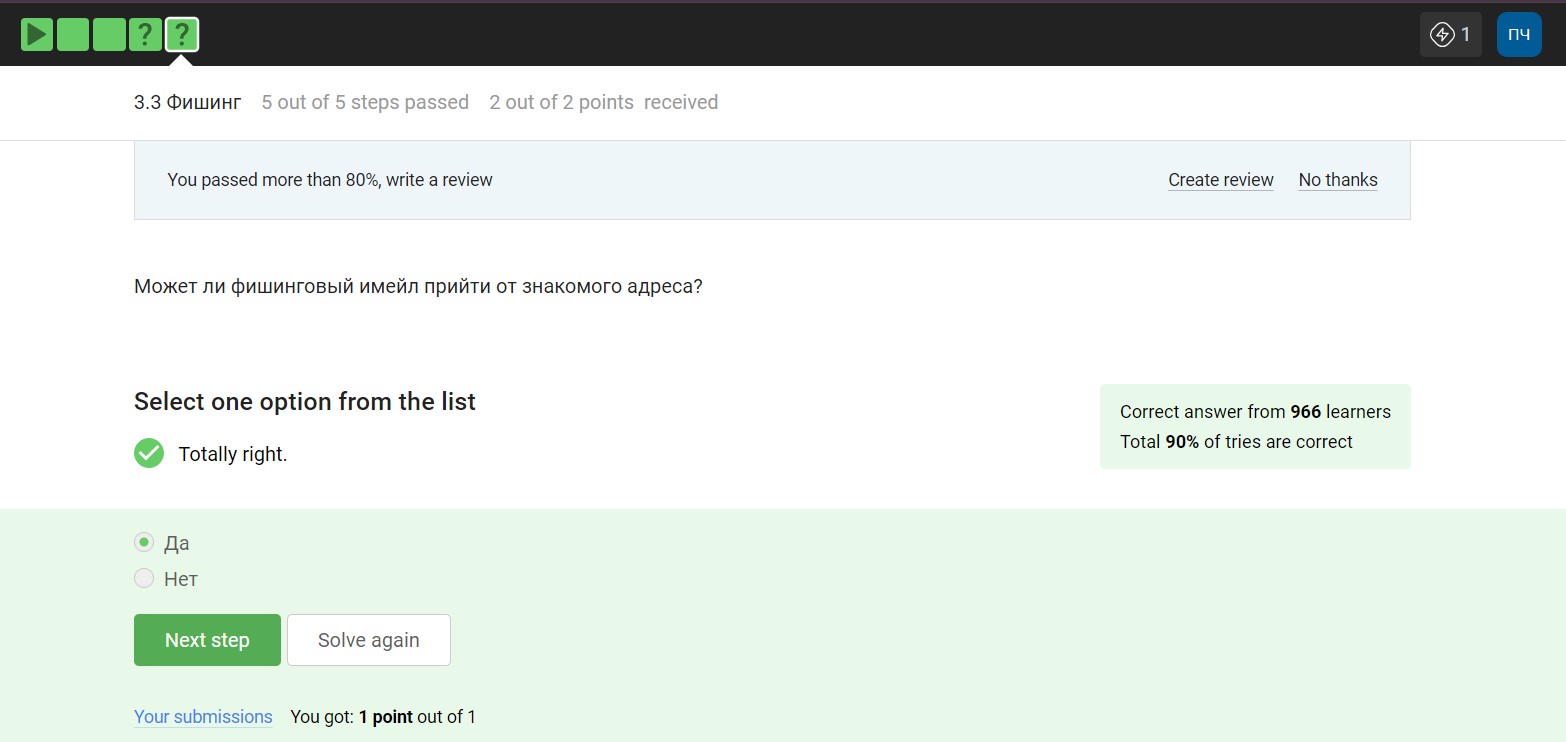


Рис. 32: Рис. 2

# 9 Раздел 3.3. Вирусы. Примеры

Email Спуфинг – это подмена адреса отправителя в имейлах

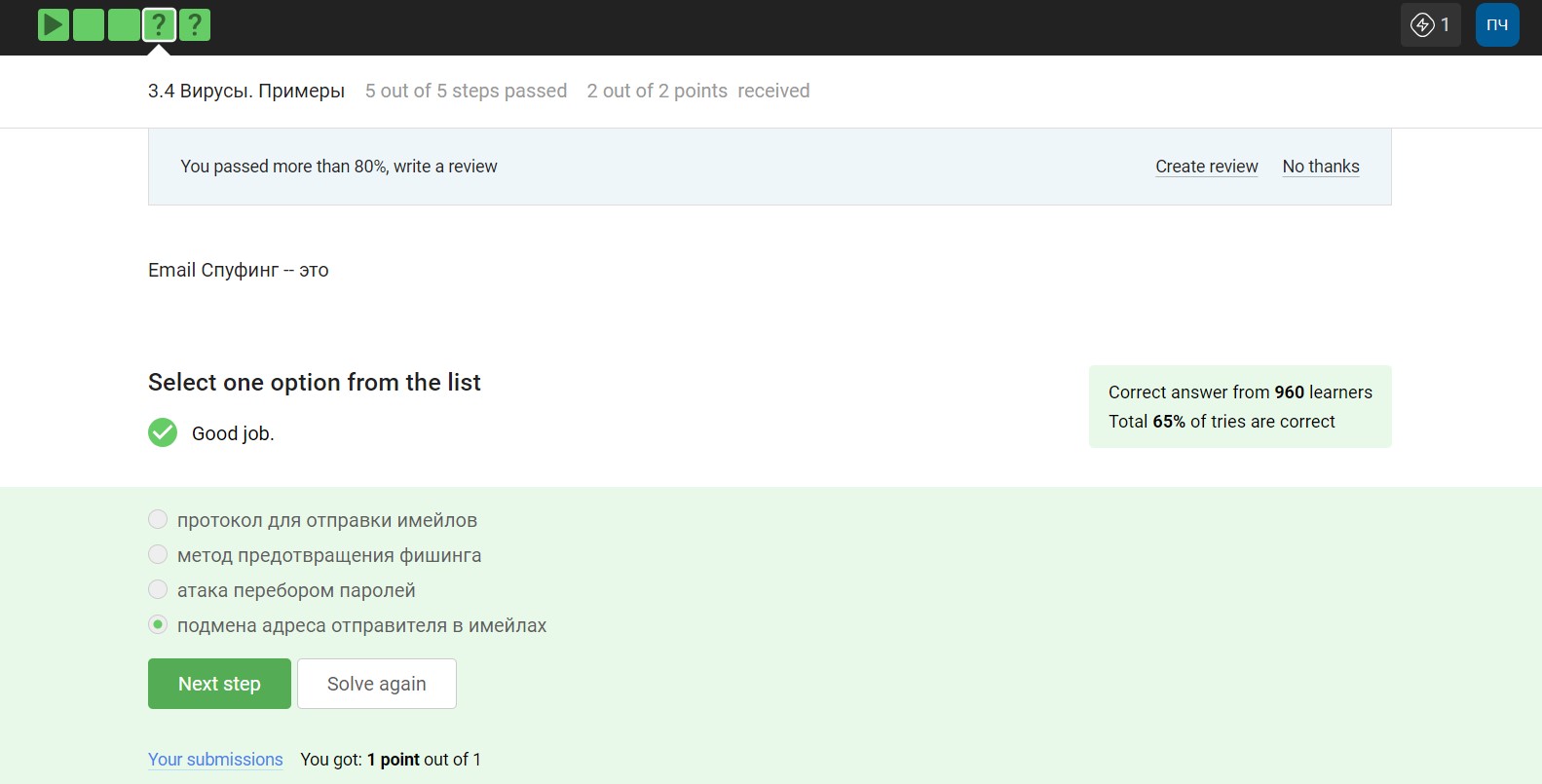


Рис. 33: Рис. 1

Вирус-троян маскируется под легитимную программу

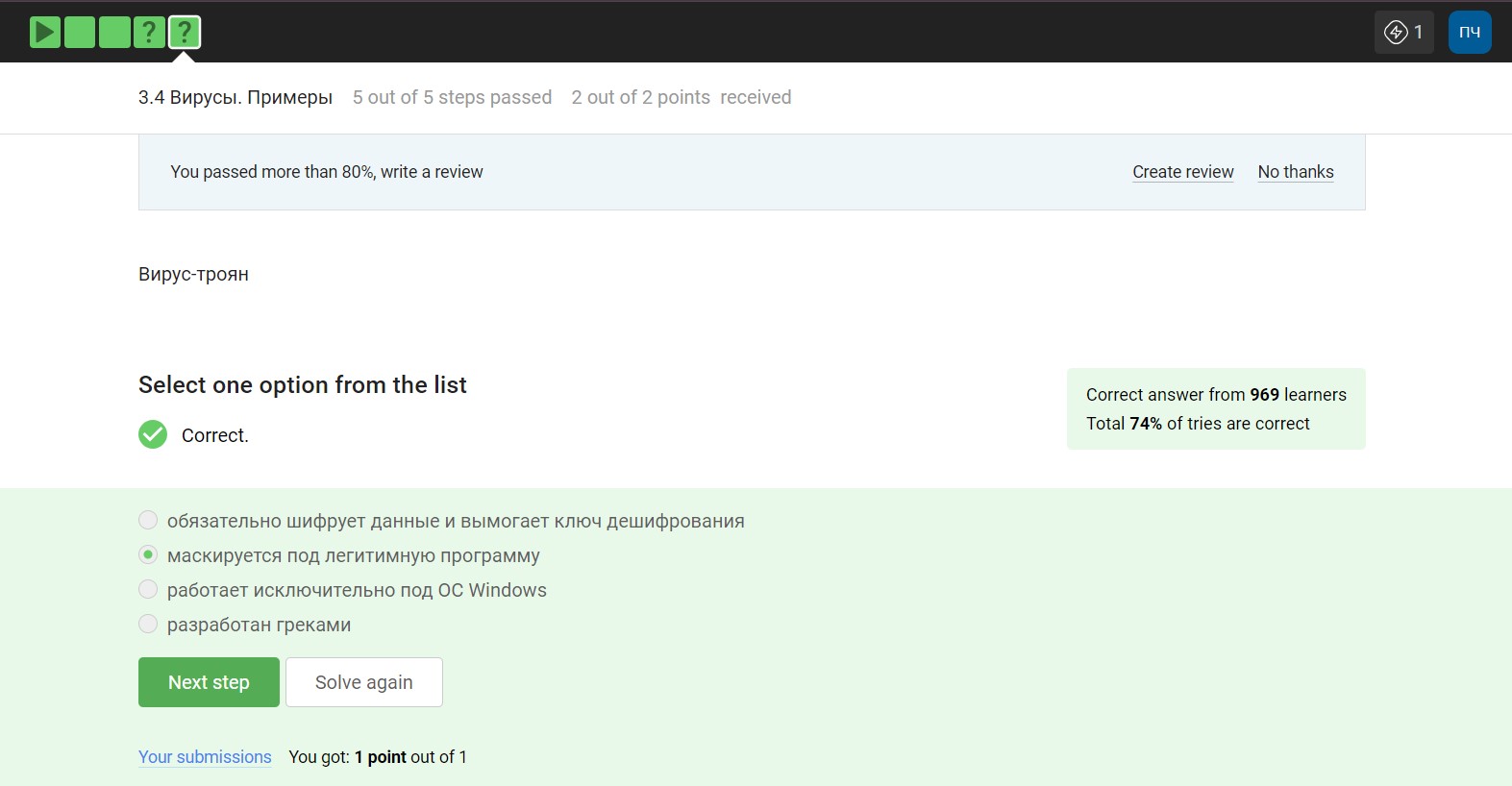


Рис. 34: Рис. 2

# 10 Раздел 3.5. Безопасность мессенджеров

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

* при генерации первого сообщения стороной-отправителем

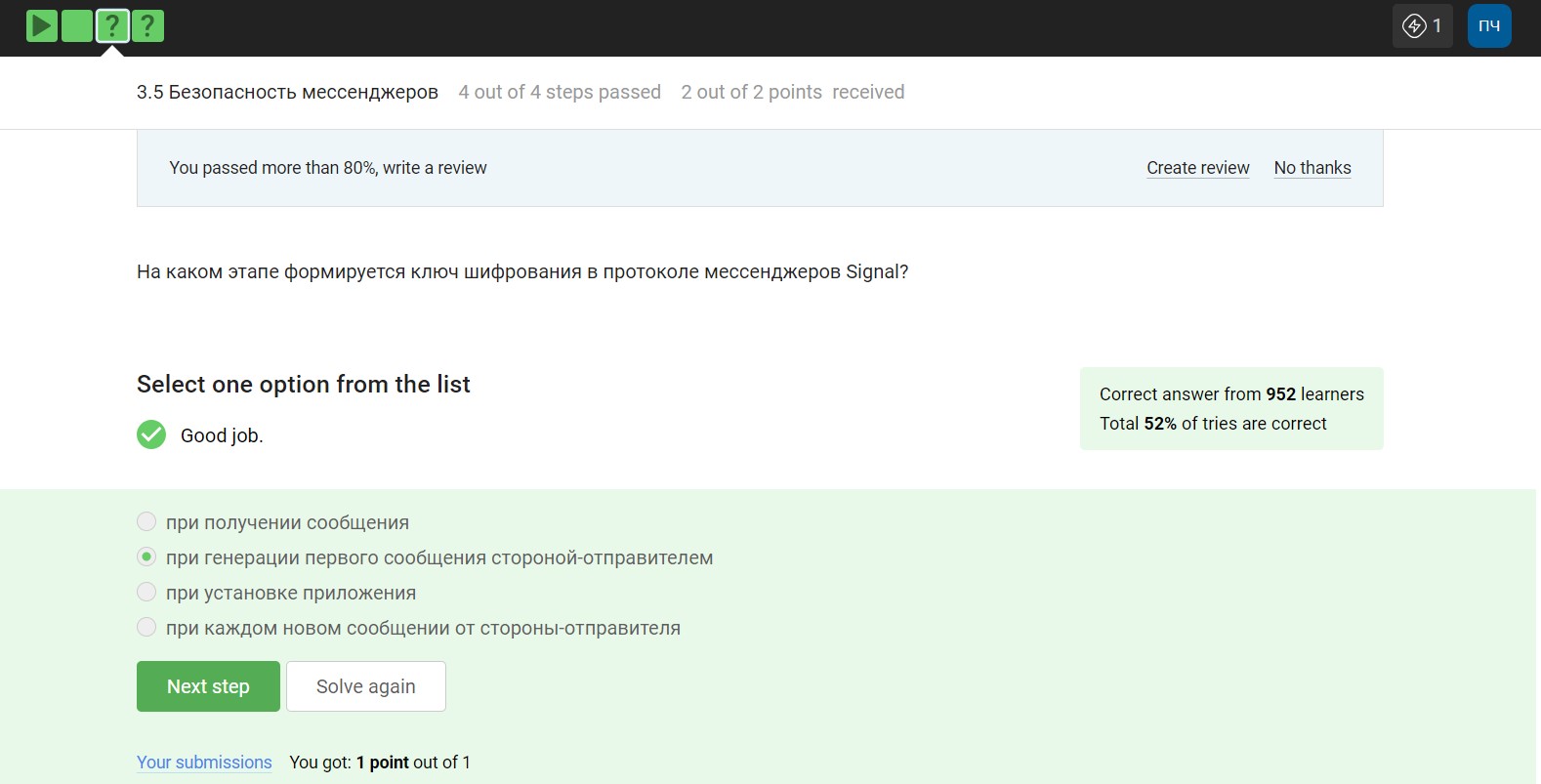
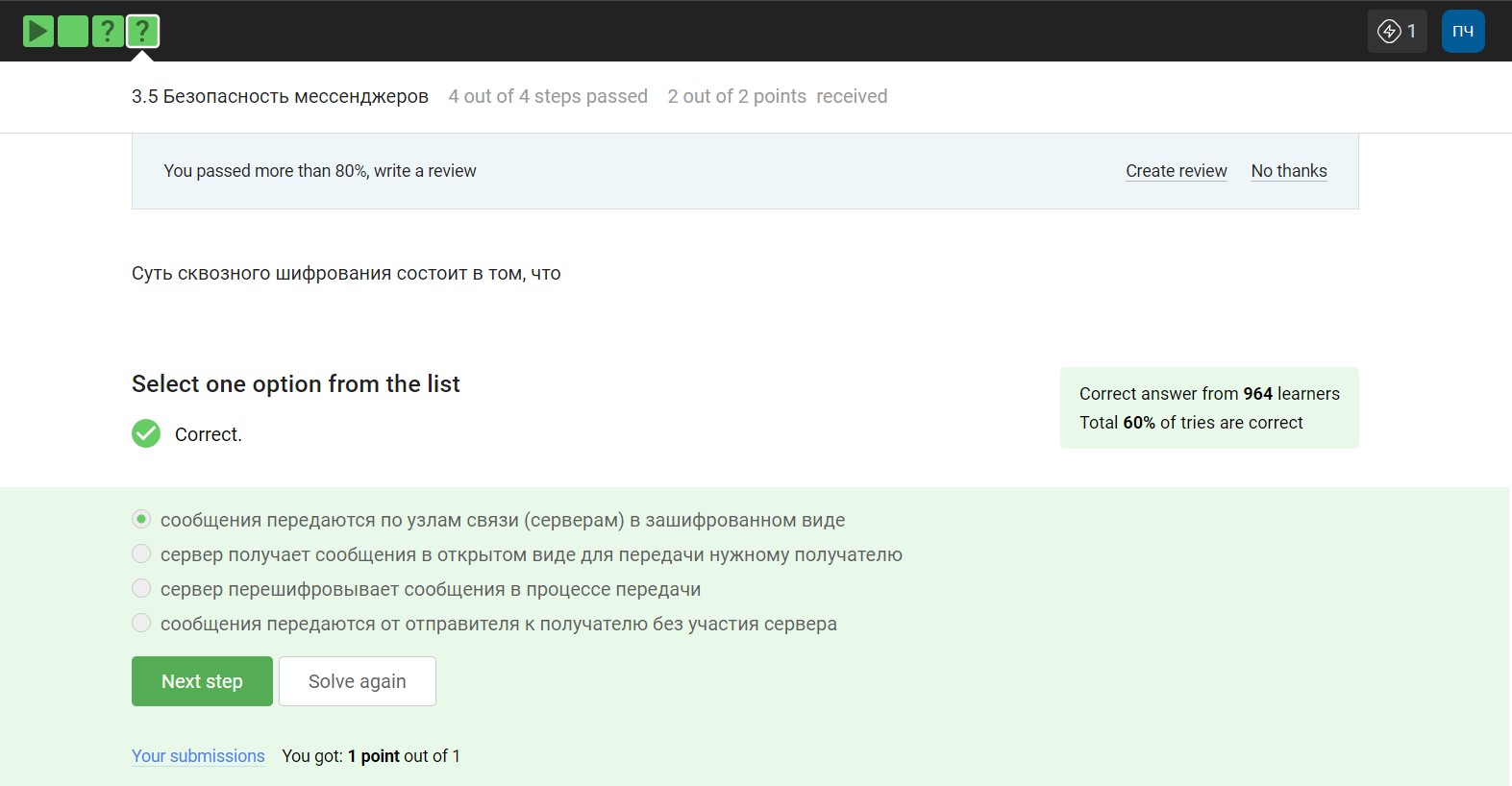


Рис. 35: Рис. 1

Суть сквозного шифрования состоит в том, что

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

# 11 Раздел 4.1 Введение в криптографию

В асимметричных криптографических примитивах - обе стороны имеют пару ключей

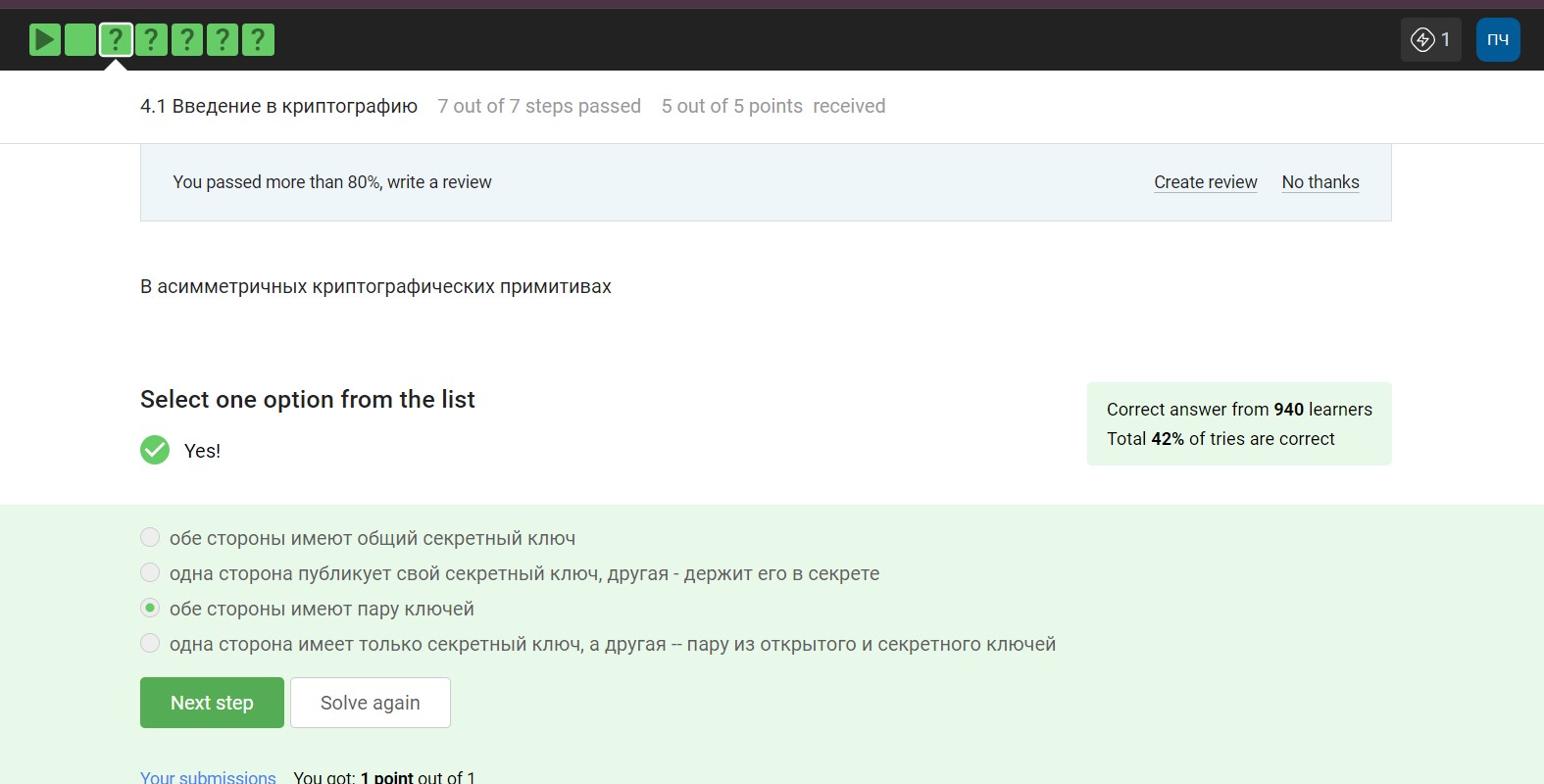


Рис. 36: Рис. 1

Криптографическая хэш-функция - стойкая к коллизиям - дает на выходе фиксированное число бит независимо от объема входных данных - эффективно вычисляется

К алгоритмам цифровой подписи относятся - RSA - ECDSA - ГОСТ Р 34.10-2012.

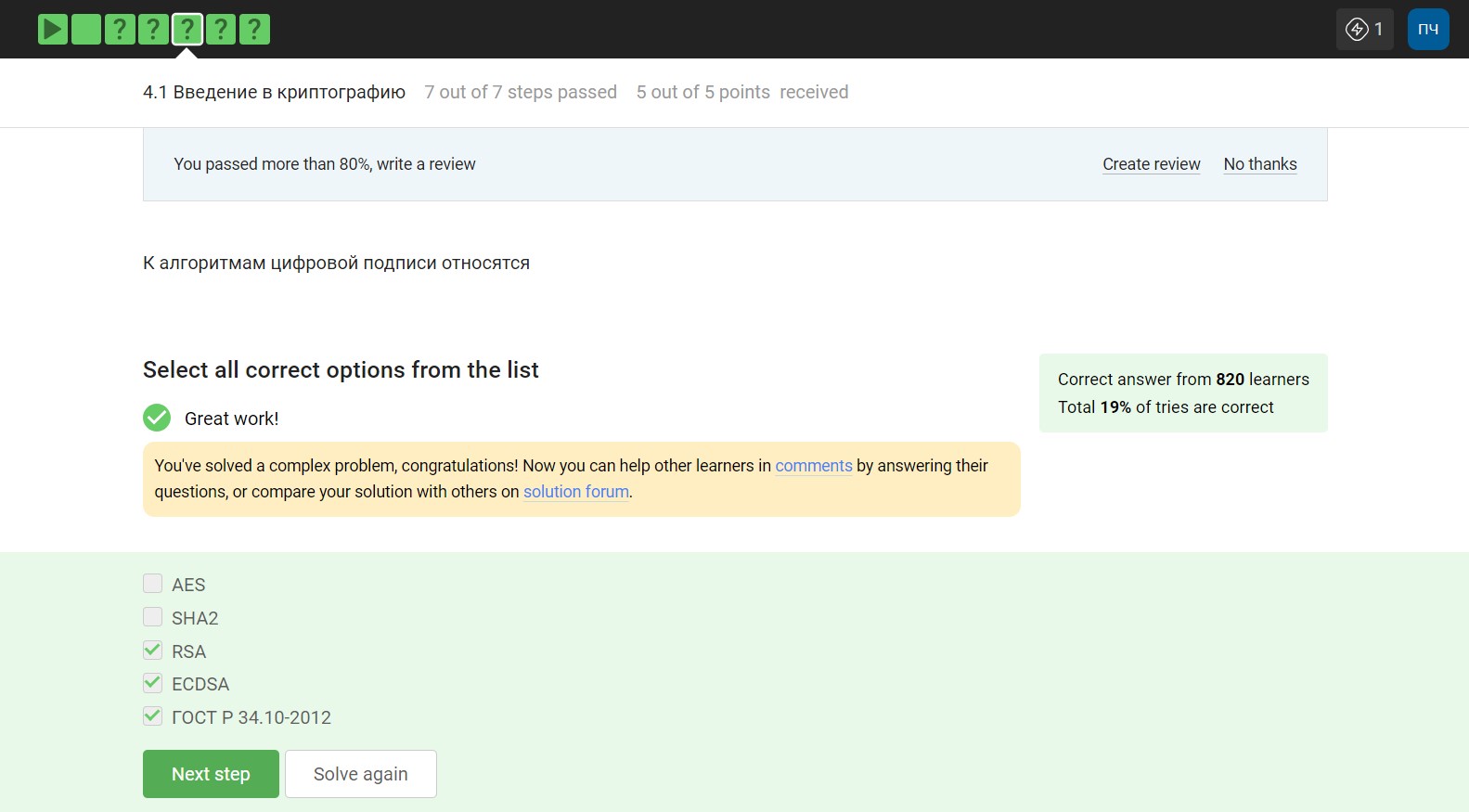


Рис. 37: Рис. 3

Код аутентификации сообщения относится к - симметричным примитивам

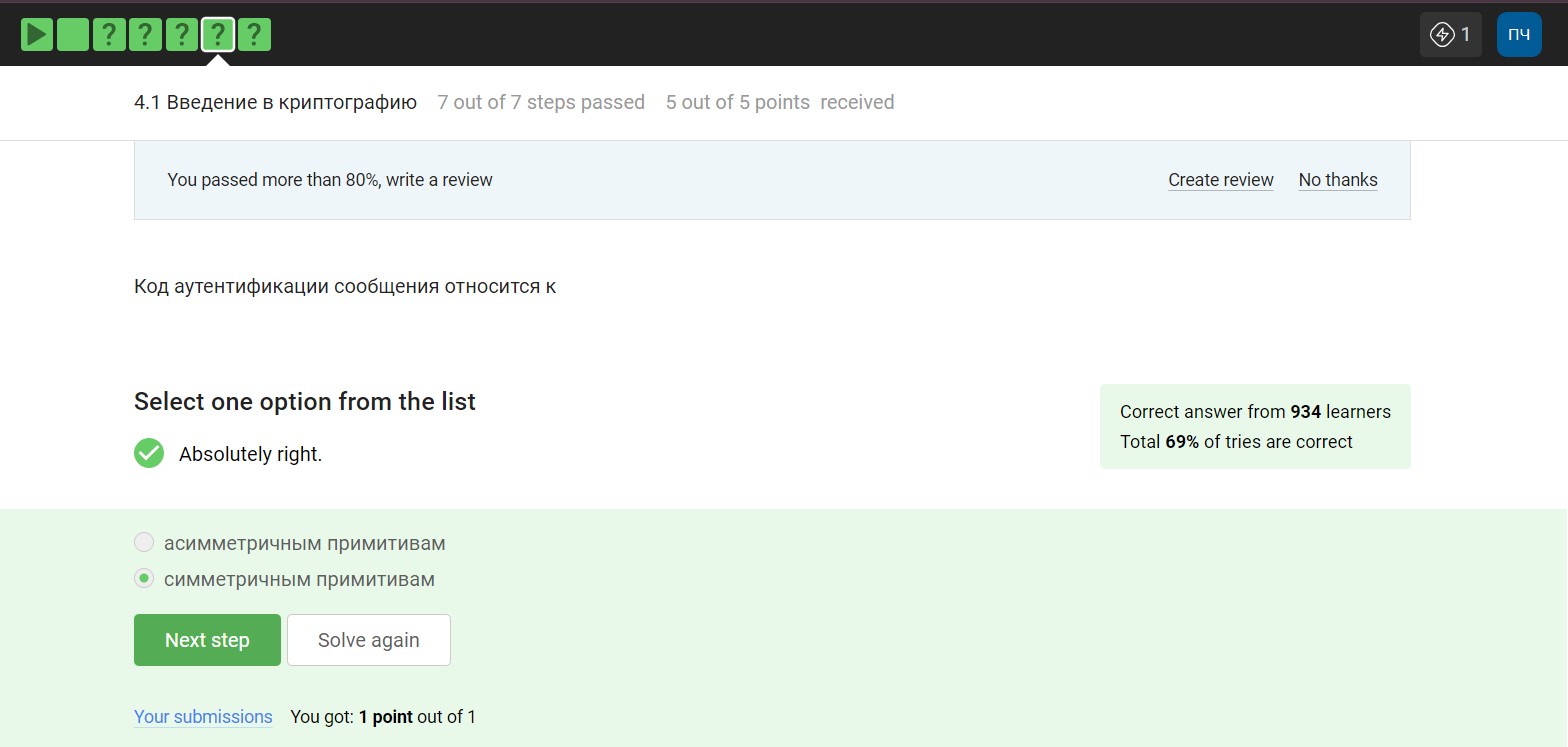


Рис. 38: Рис. 4

Обмен ключам Диффи-Хэллмана - это -асимметричный примитив генерации общего секретного ключа

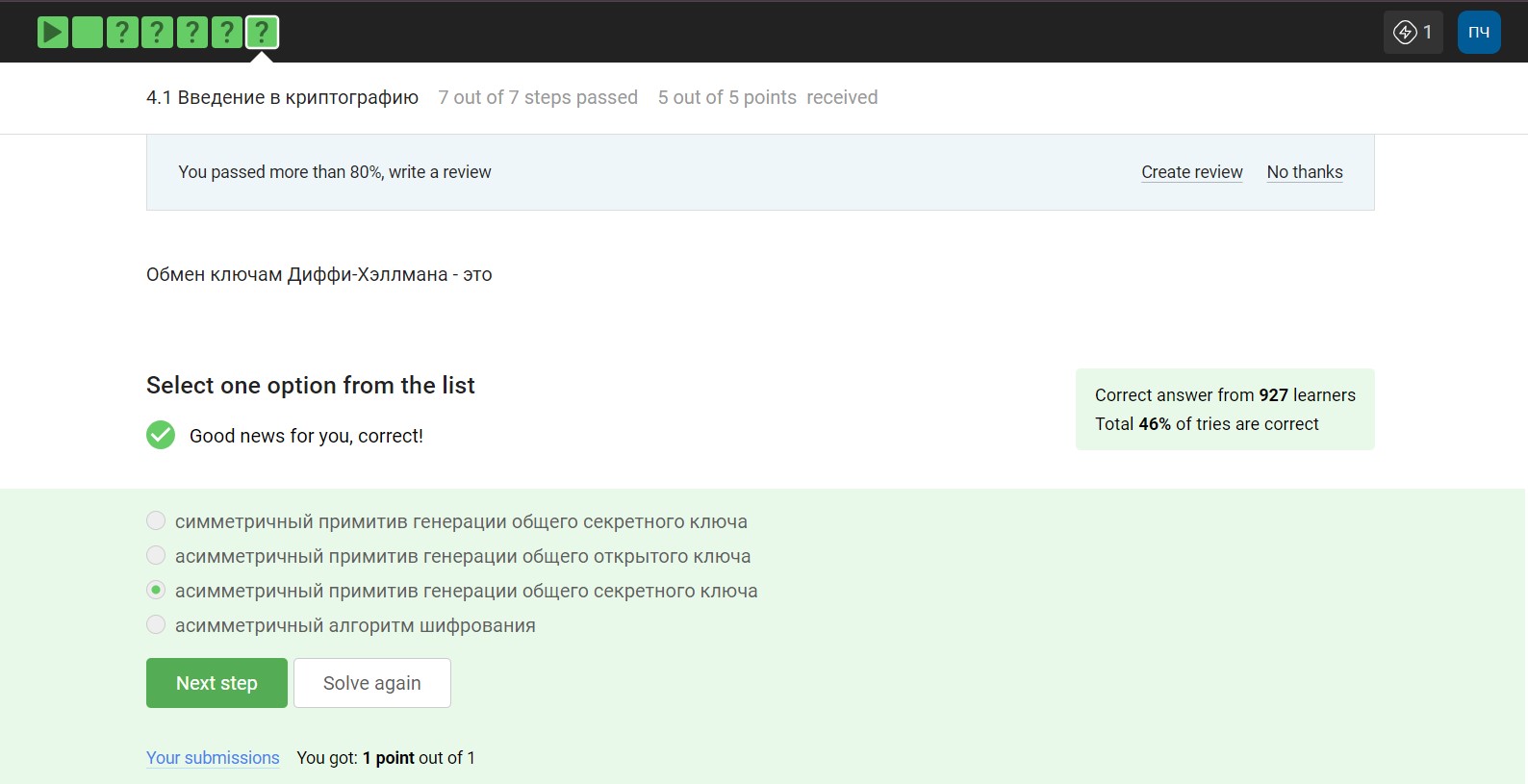


Рис. 39: Рис. 5

# 12 Раздел 4.2 Цифровая подпись

Протокол электронной цифровой подписи относится к - протоколам с публичным (или открытым) ключом

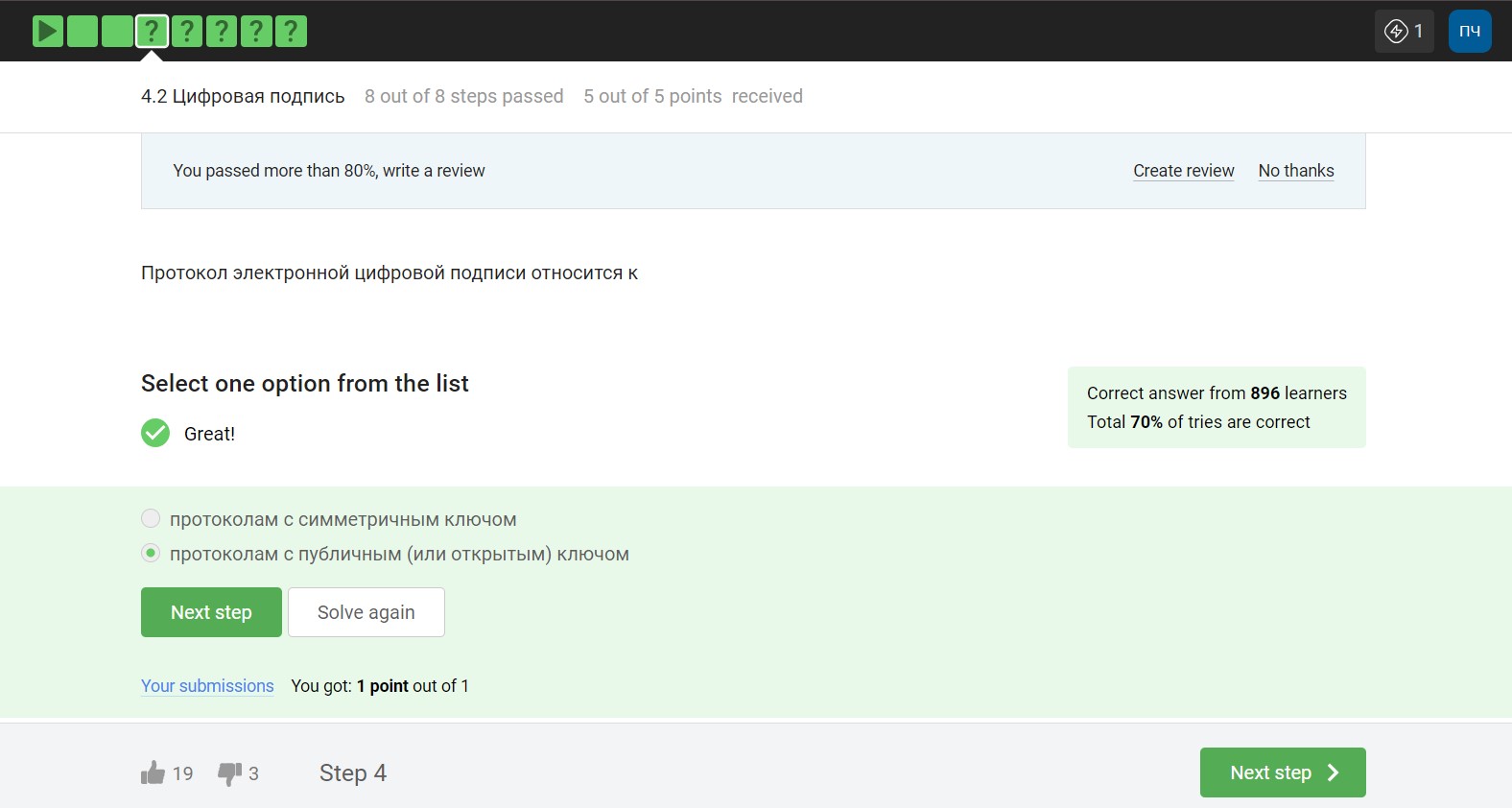
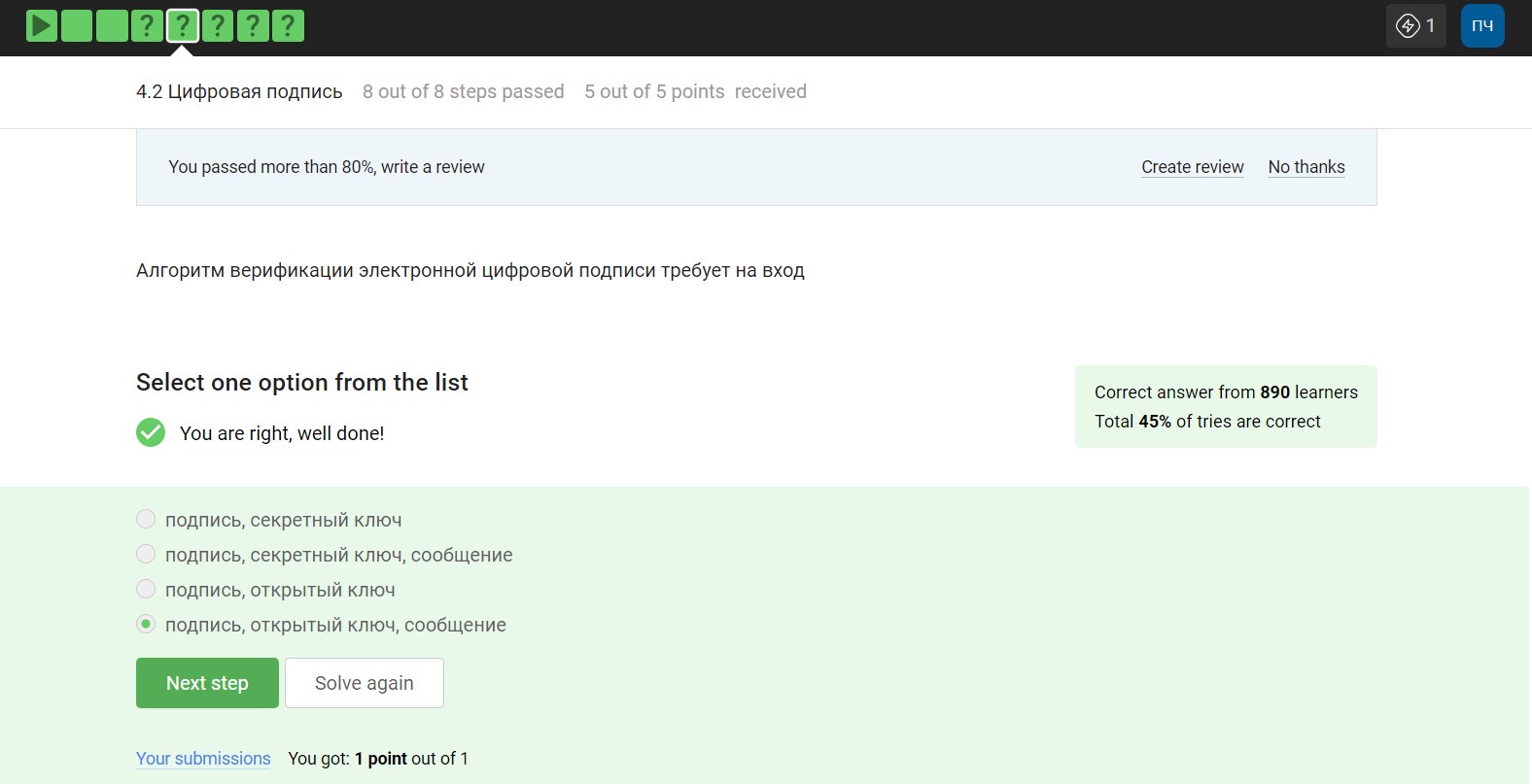


Рис. 40: Рис. 1

Алгоритм верификации электронной цифровой подписи требует на вход - подпись, открытый ключ, сообщение 

Электронная цифровая подпись не обеспечивает -конфиденциальность

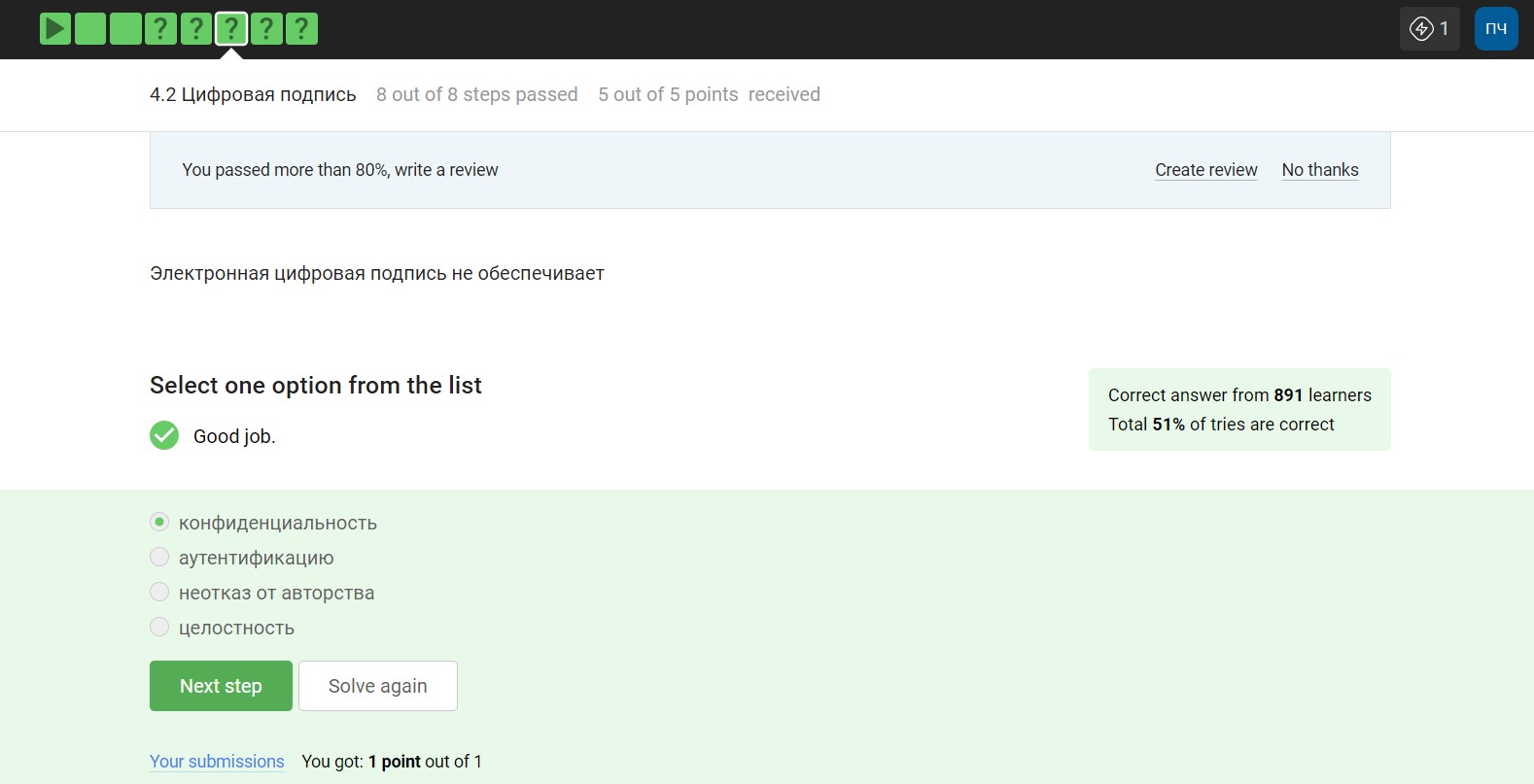


Рис. 41: Рис. 3

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС? -усиленная квалифицированная

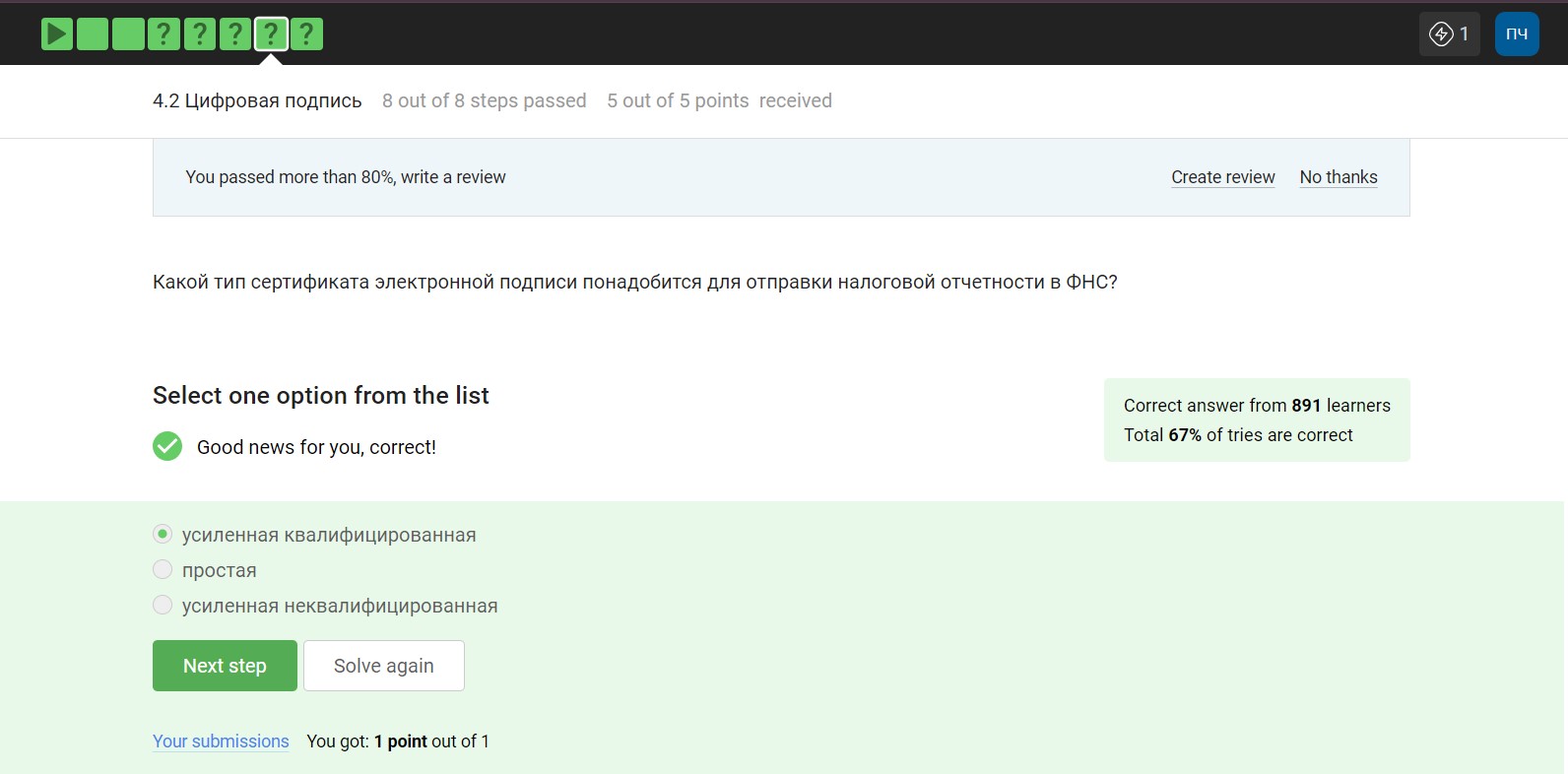


Рис. 42: Рис. 4

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи? -в удостоверяющем (сертификационном) центре

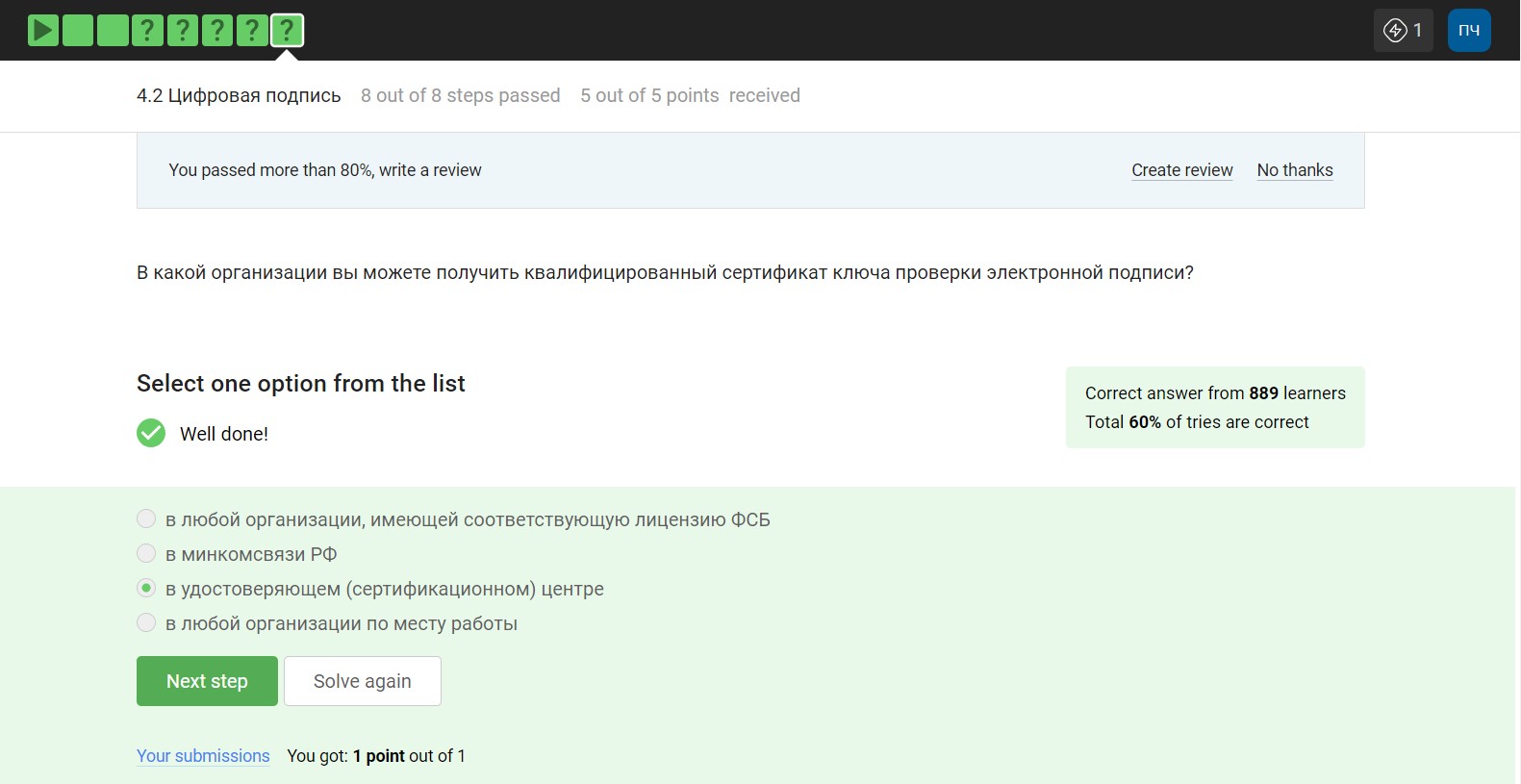


Рис. 43: Рис. 5

# 13 Раздел 4.3 Электронные платежи

Выберите из списка все платежные системы. - MasterCard - МИР

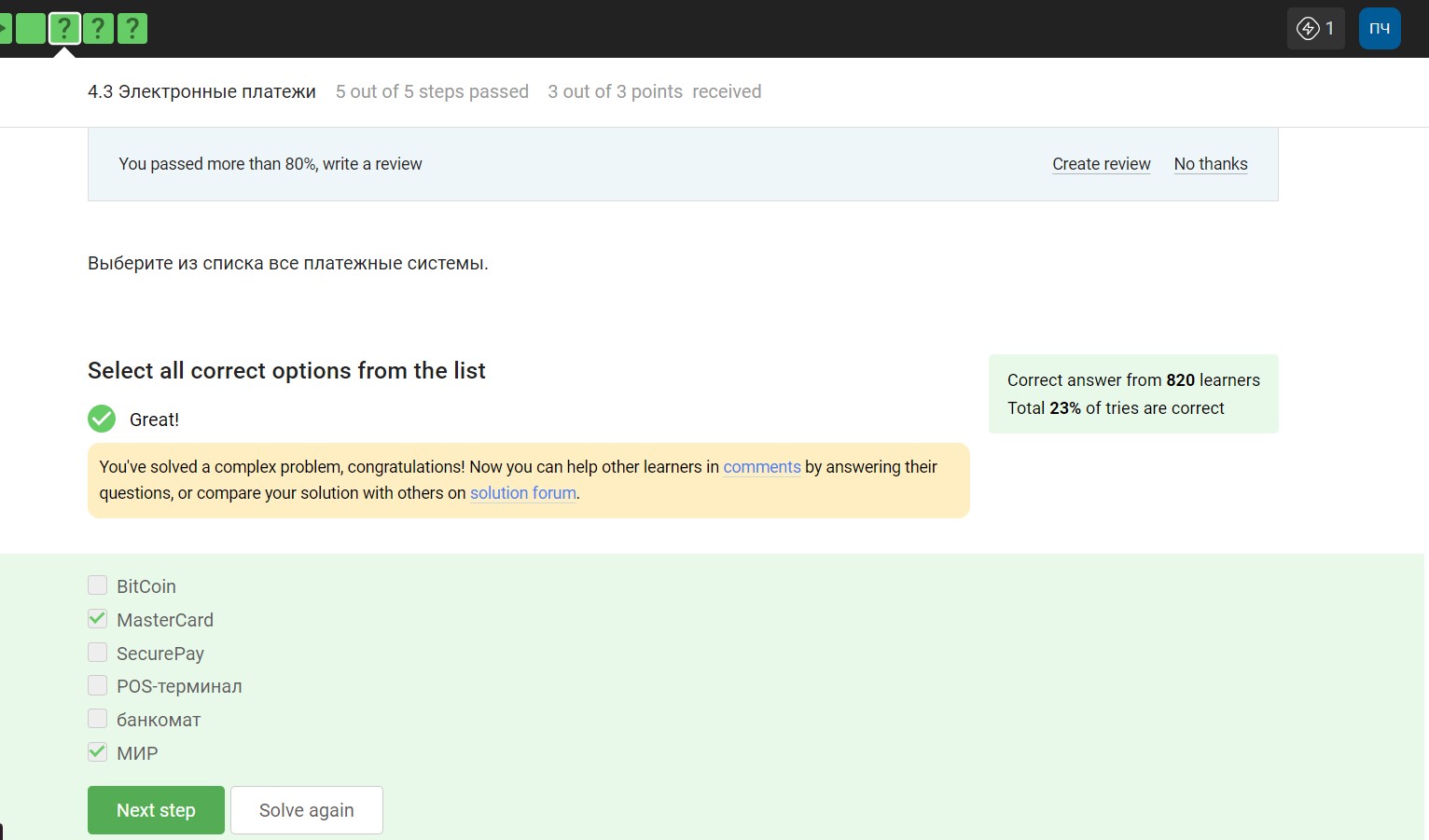


Рис. 44: Рис. 1

Примером многофакторной аутентификации является - комбинация проверка пароля + код в sms сообщении - комбинация код в sms сообщении + отпечаток пальца

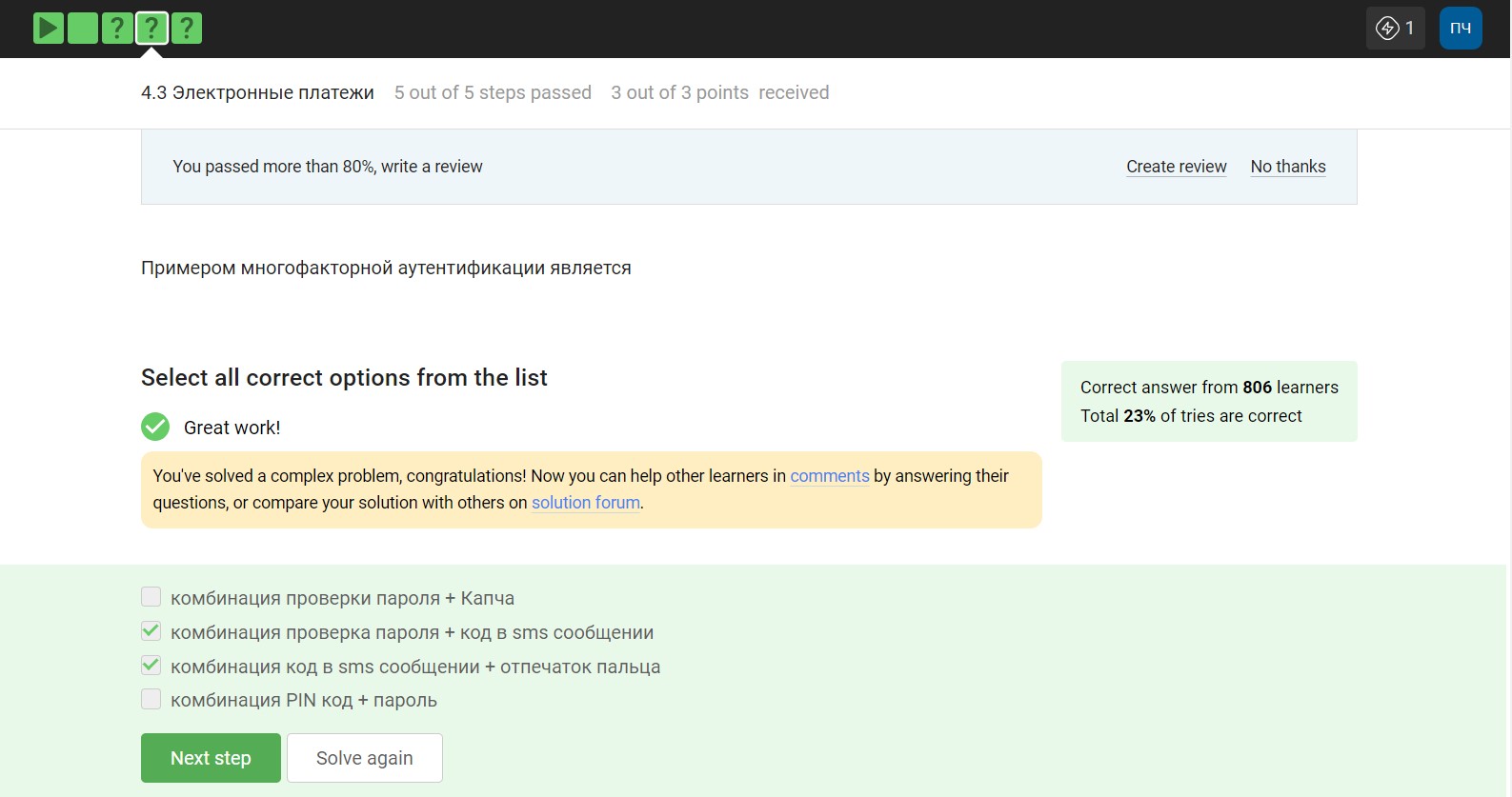


Рис. 45: Рис. 2

При онлайн платежах сегодня используется - многофакторная аутентификация покупателя перед банком-эмитентом

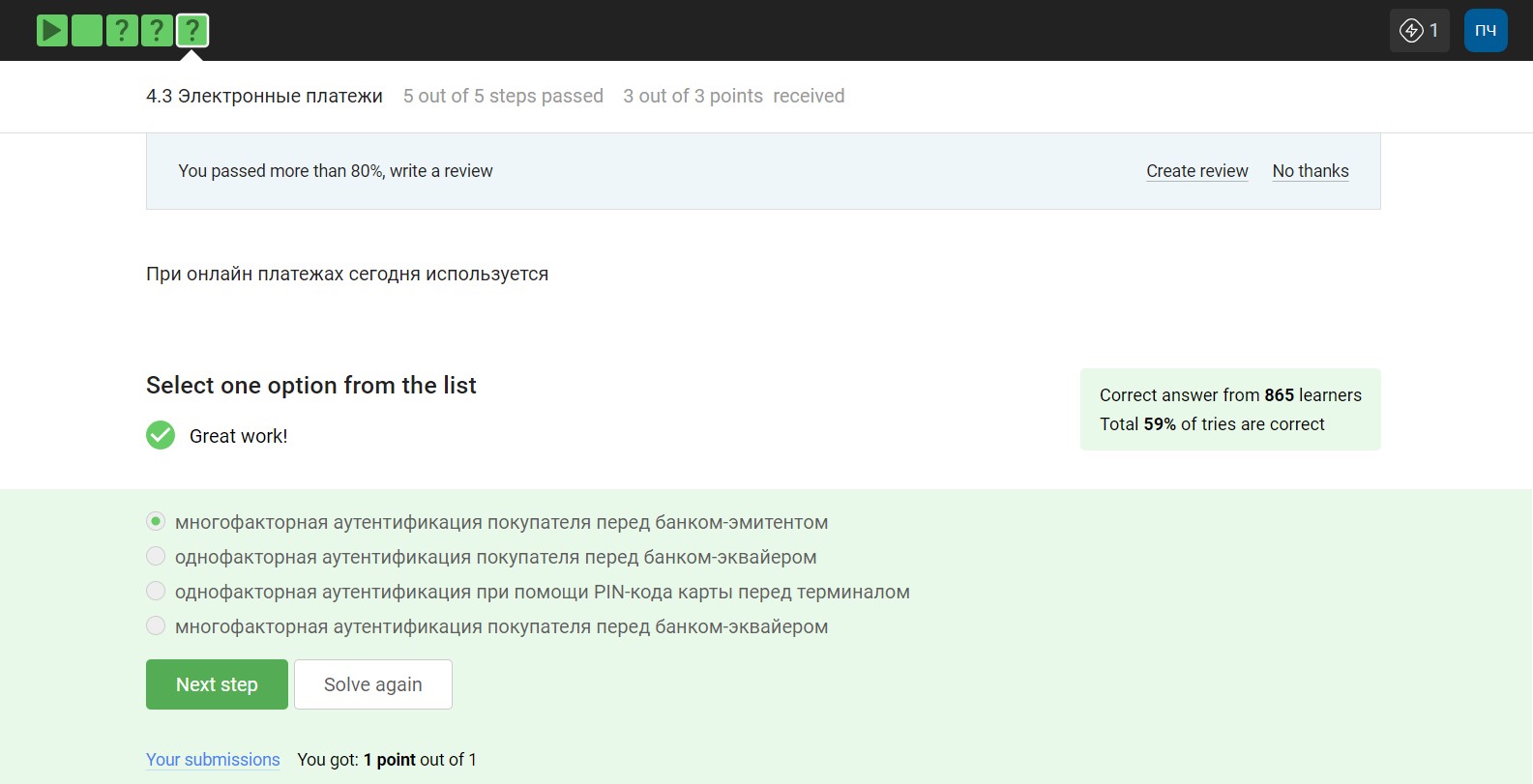


Рис. 46: Рис. 3

# 14 Раздел 4.4 Блокчейн

Какое свойство криптографической хэш-функции используется в доказательстве работы? - сложность нахождения прообраза

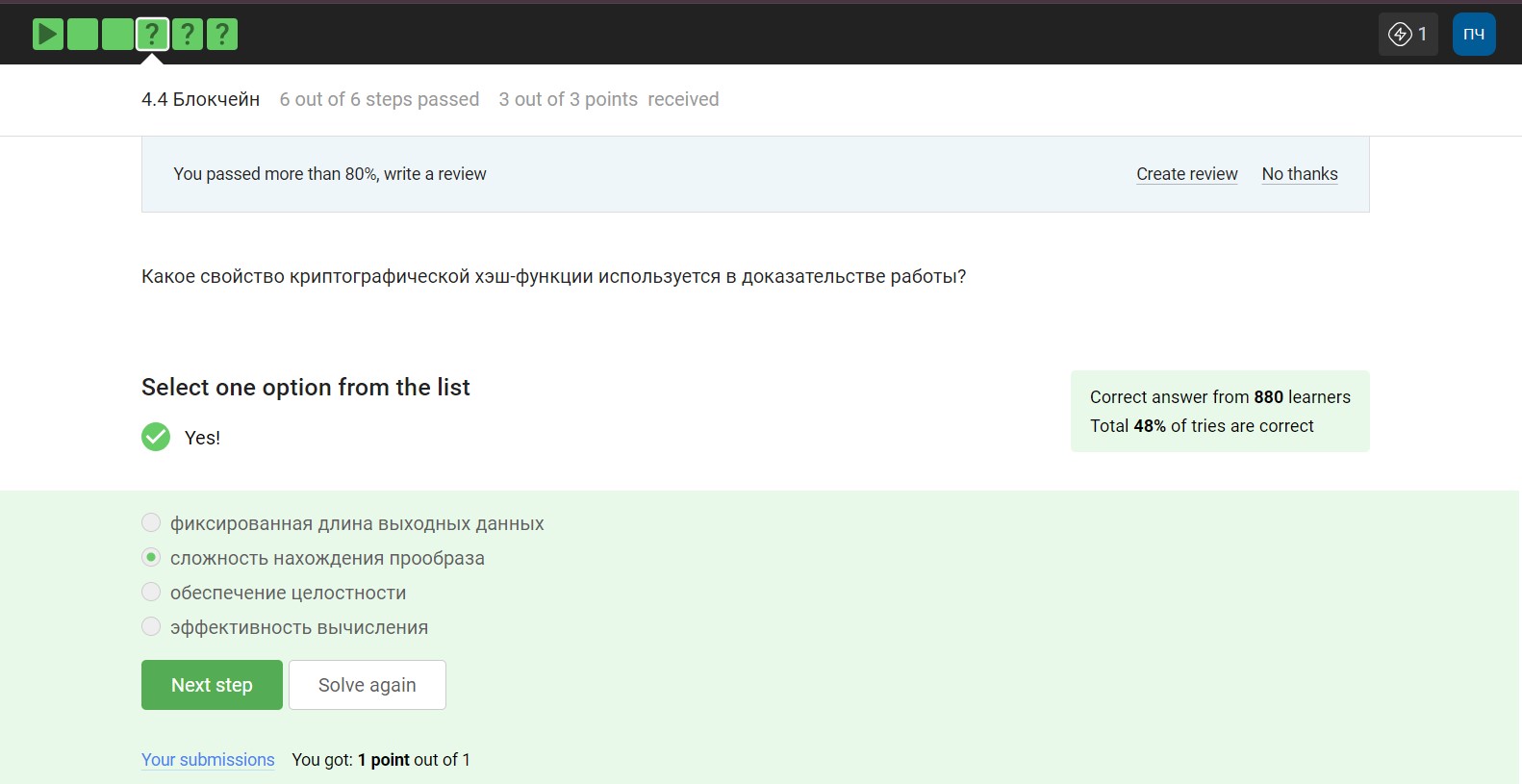


Рис. 47: Рис. 1

Консенсус в некоторых системах блокчейн обладает свойствами - открытость - консенсус - постоянства - живучесть

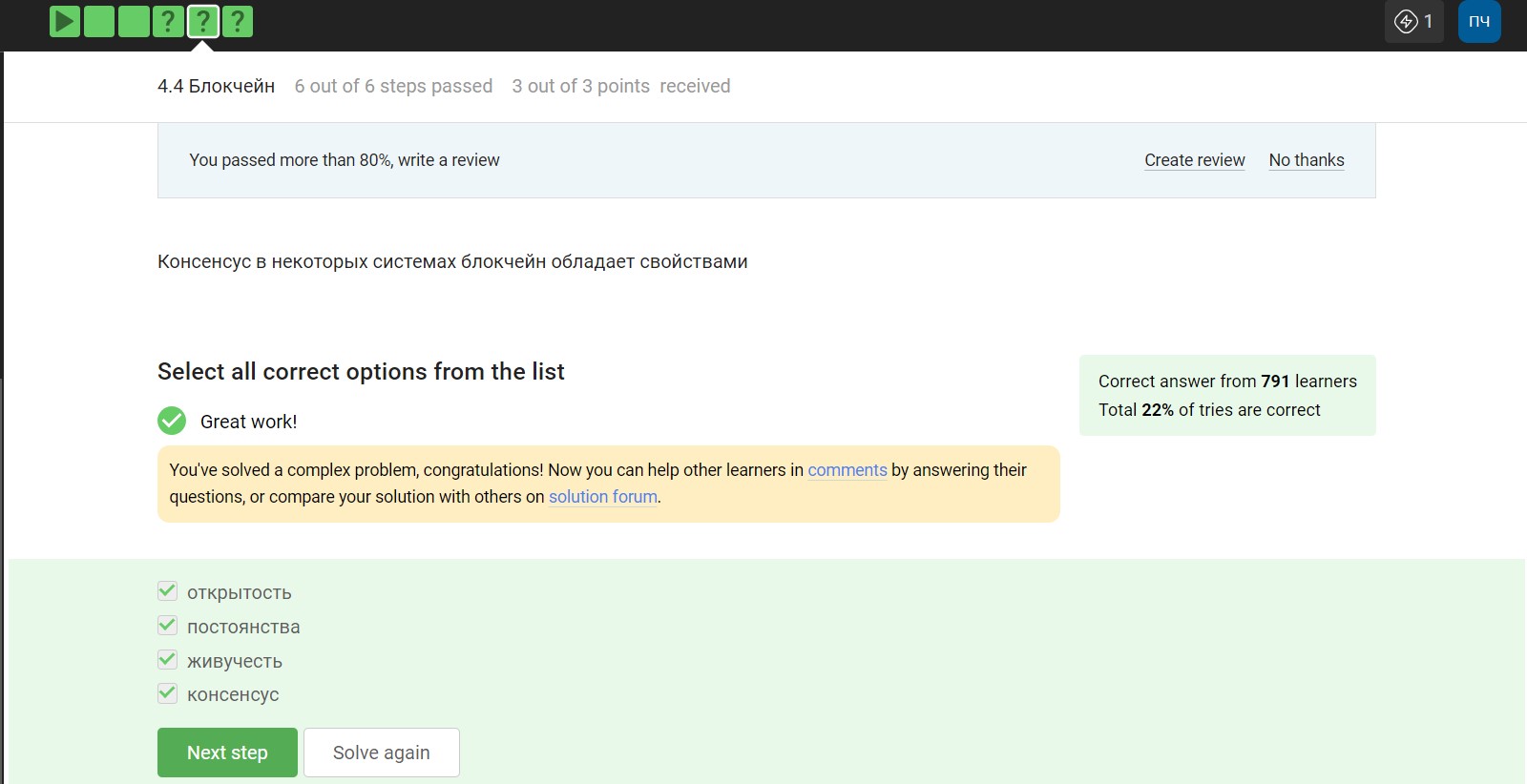


Рис. 48: Рис. 2

Секретные ключи какого криптографического примитива хранят участники блокчейна? - цифровая подпись

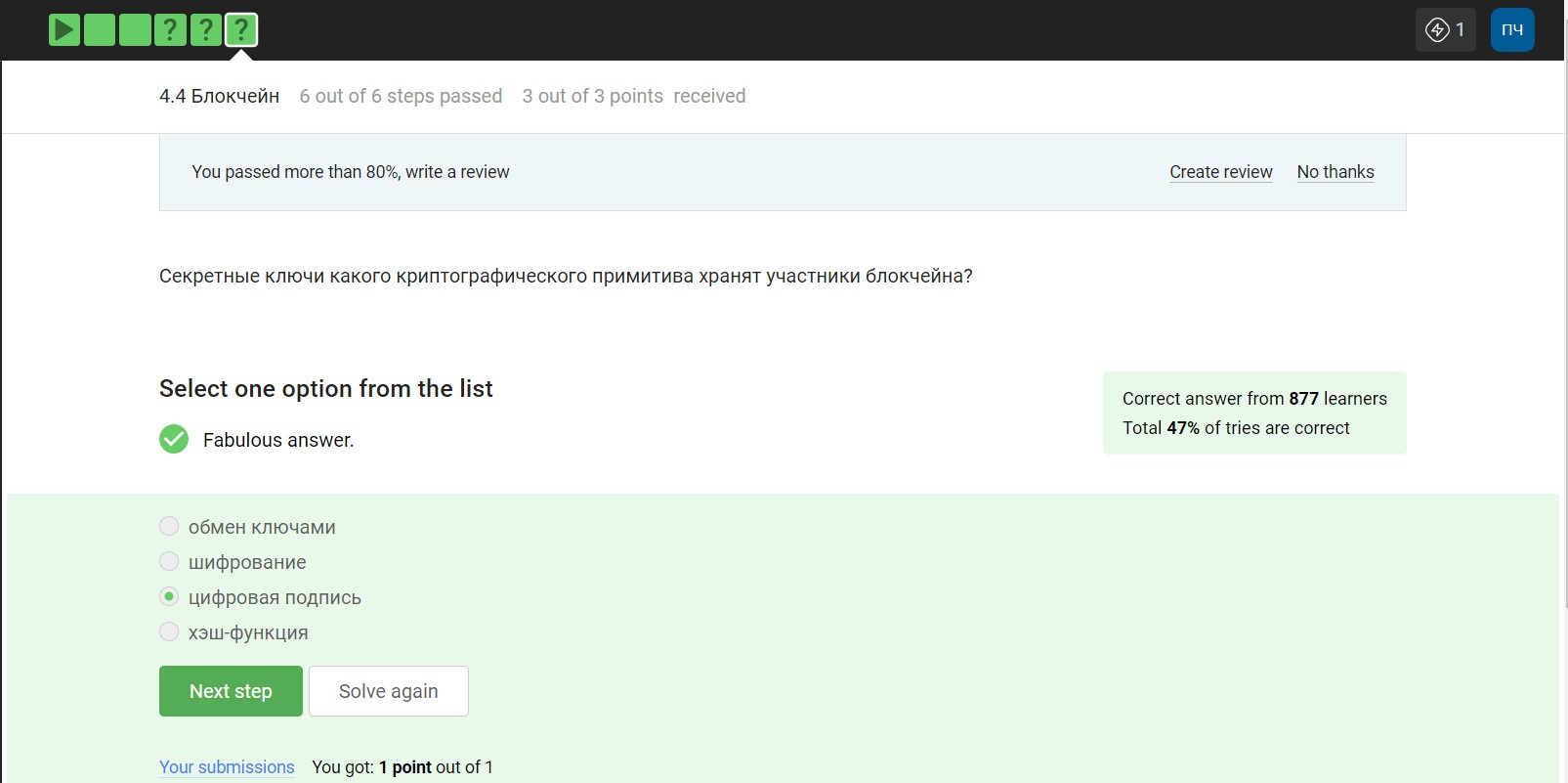


Рис. 49: Рис. 3

# 15 Вывод

Курс пройден, сертификат не выдаётся на этом курсе. Я научился основным методам информационной безопасности

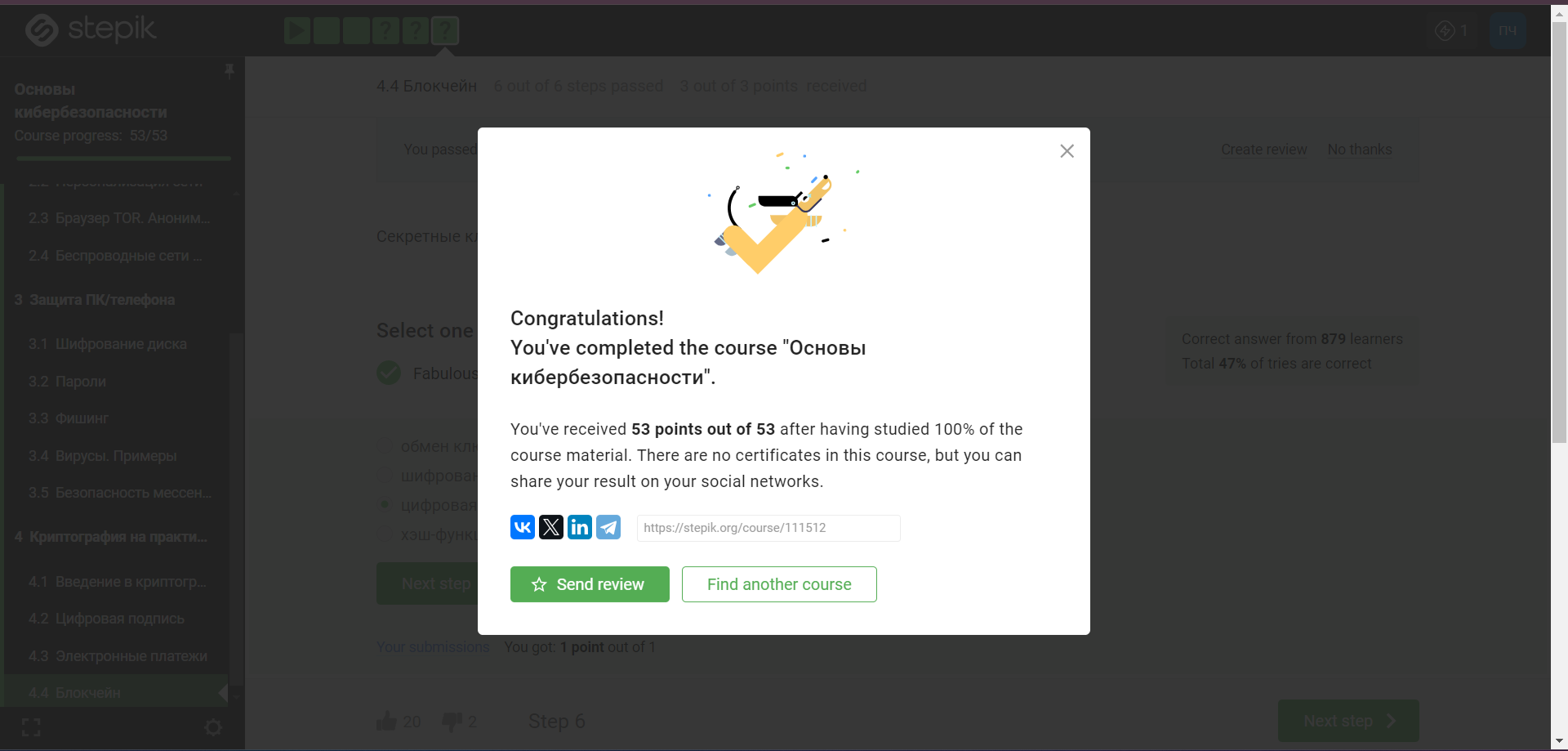


Рис. 50: Прохождение курса