Внешний курс

Степик по основам безопасности

Прокопьева Марина Евгеньевна

Содержание

Список иллюстраций

Список таблиц

# 1 Цель работы

Пройти курс на степике и узнать много нового (или нет)

# 2 Выполнение

UDP - протокол сетевого уровня TCP - протокол транспортного уровня HTTPS - протокол прикладного уровня IP - протокол сетевого уровня, поэтому ответ HTTPS

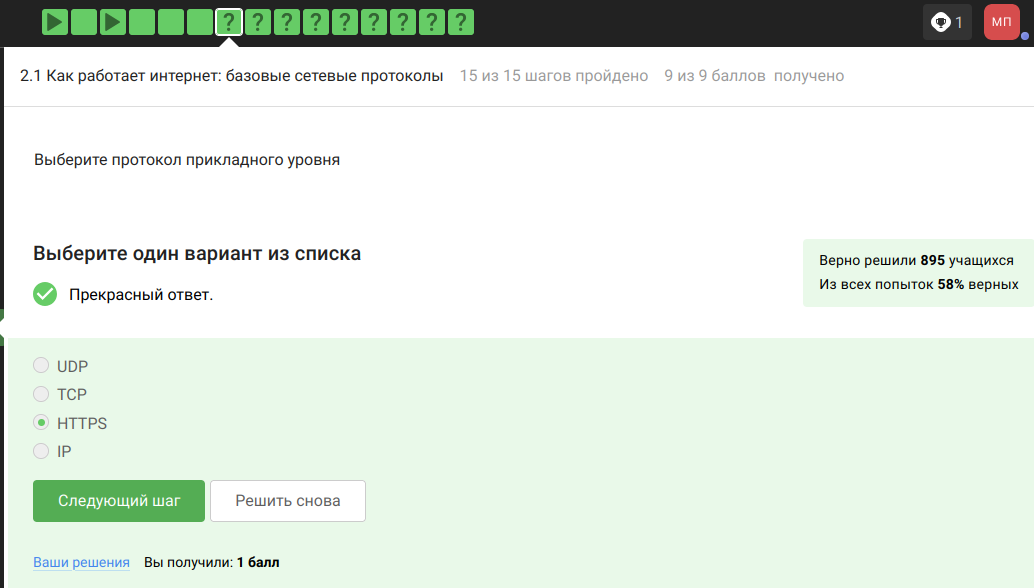


Рис. 1: нет названия

Ранее было упомянуто, что протокол TCP - transmission control protocol - работает на транспортном уровне

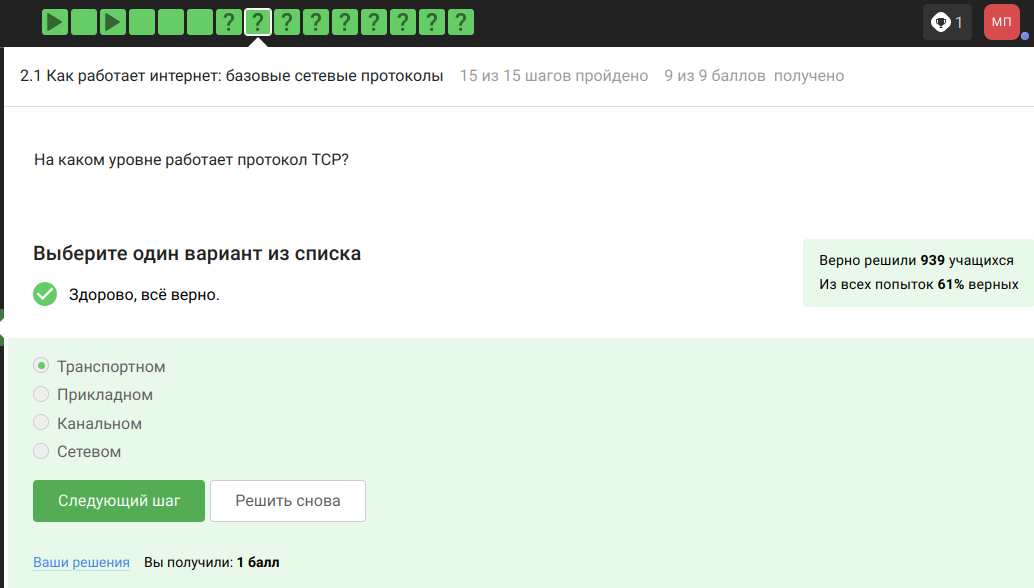


Рис. 2: нет названия

В адресе типа IPv4 не может быть чисел больше 255, поэтому первые два варианта не подходят

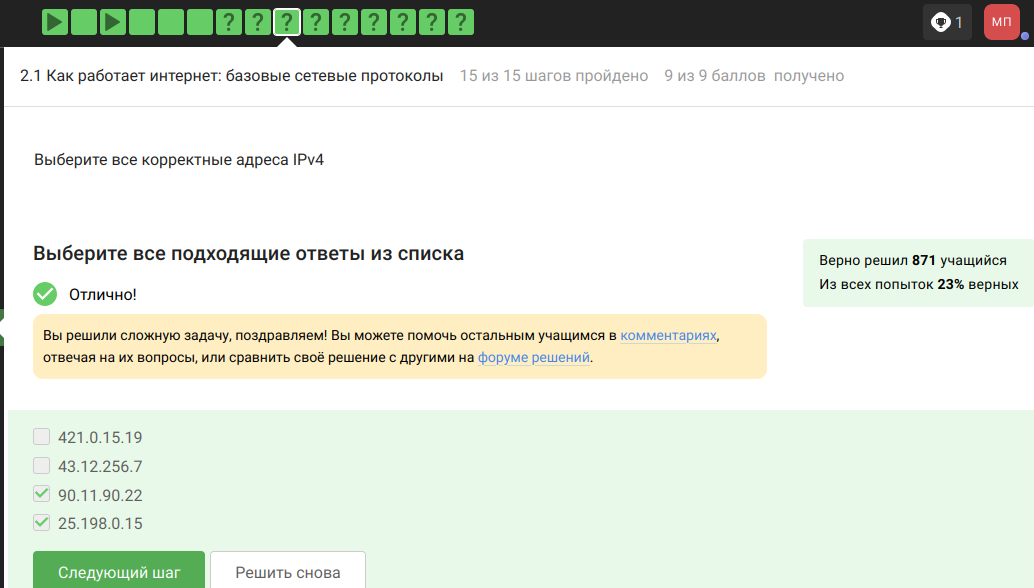


Рис. 3: нет названия

DNS-сервер, Domain name server — приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу Обязательное условие – Сопоставление сервером доменных имен доменного имени с IP-адресом называется разрешением имени и адреса

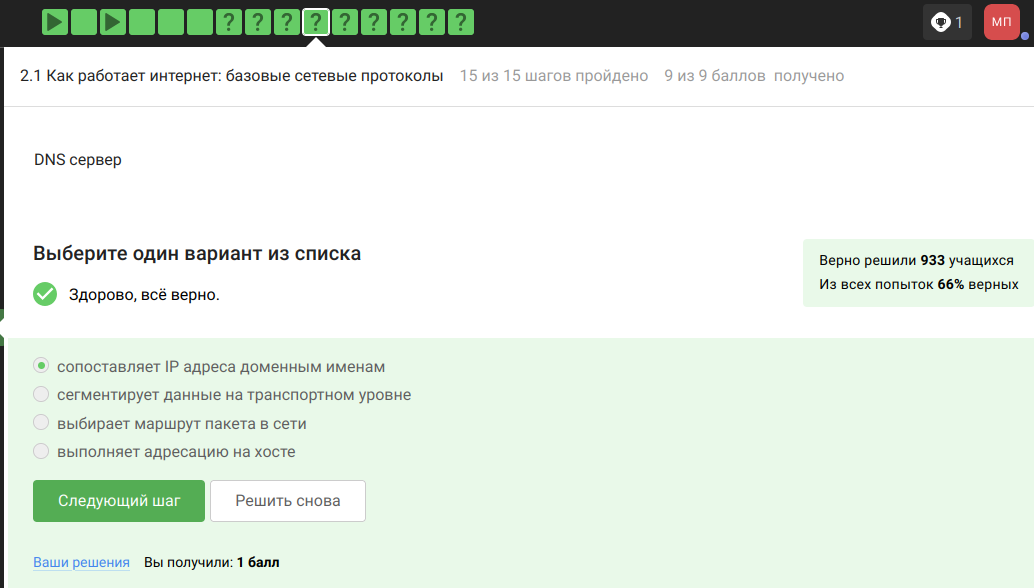


Рис. 4: нет названия

Распределение протоколов в модели TCP/IP:

* Прикладной уровень (Application Layer): HTTP, RTSP, FTP, DNS.
* Транспортный уровень (Transport Layer): TCP, UDP, SCTP, DCCP.
* Сетевой (Межсетевой) уровень (Network Layer): IP.
* Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring

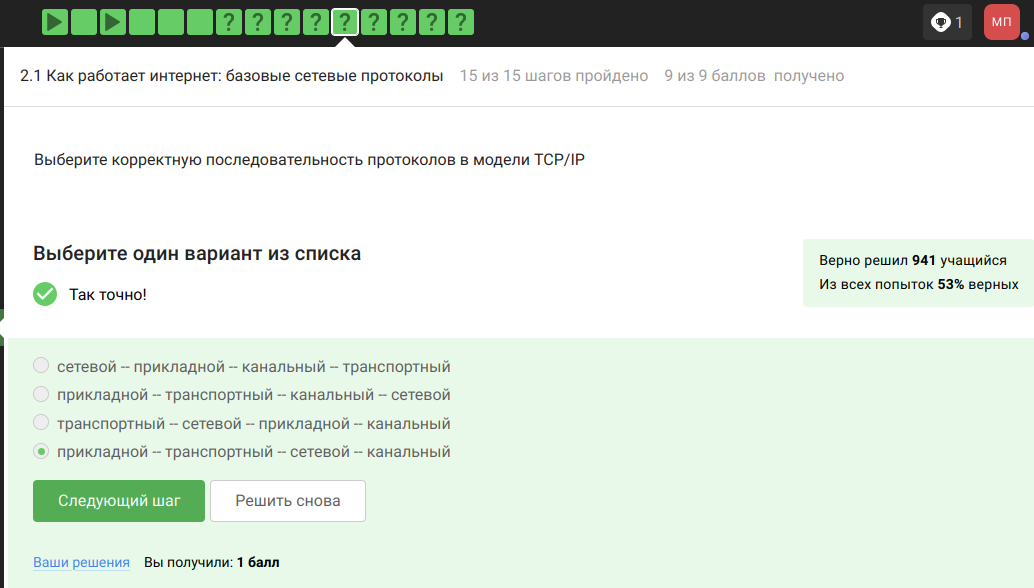


Рис. 5: нет названия

ротокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные

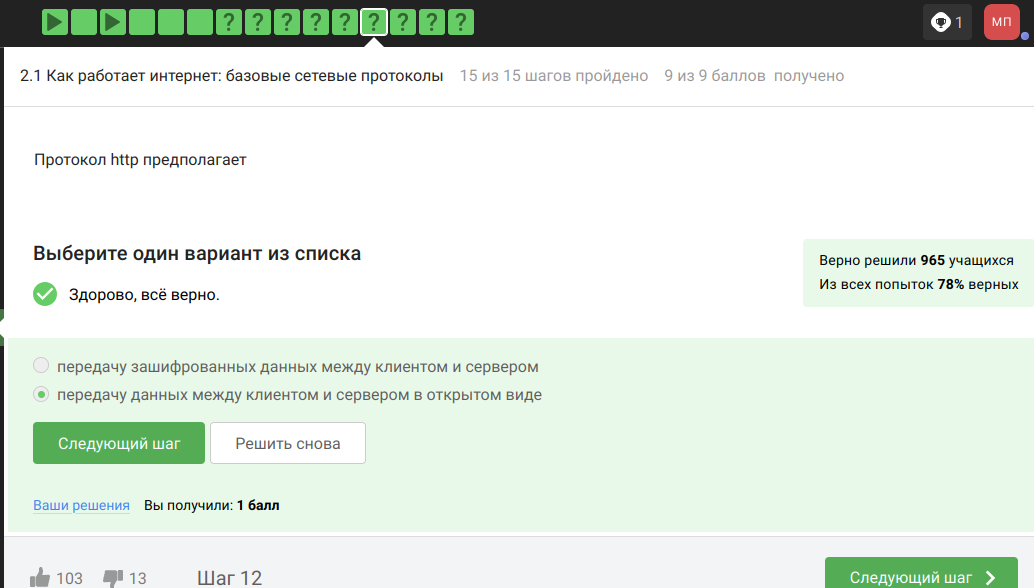


Рис. 6: нет названия

https передает зашифрованные данные, одна из фаз - передача данных, другая должна быть рукопожатием

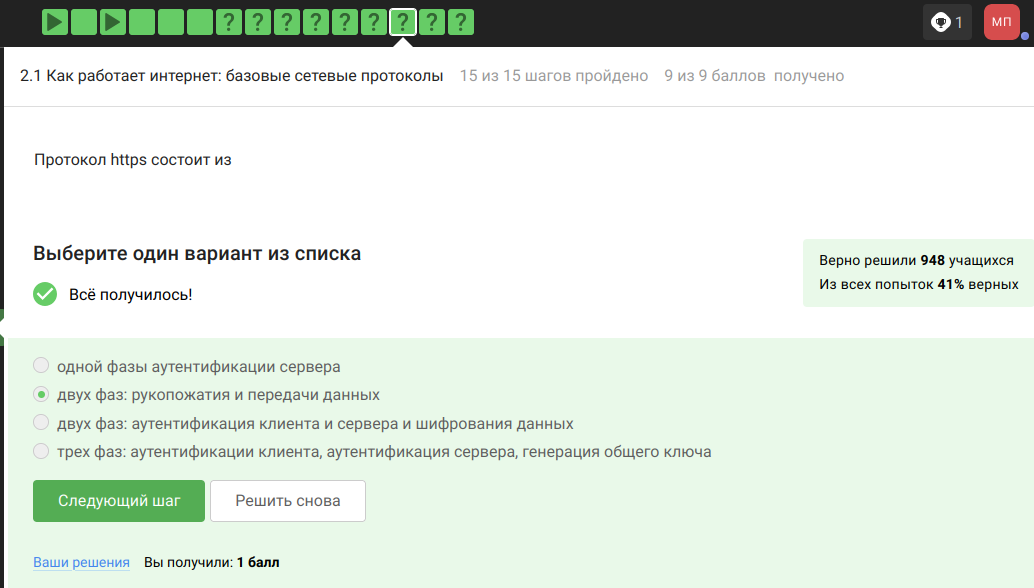


Рис. 7: нет названия

TLS определяется и клиентом, и сервером, чтобы было возможно подключиться

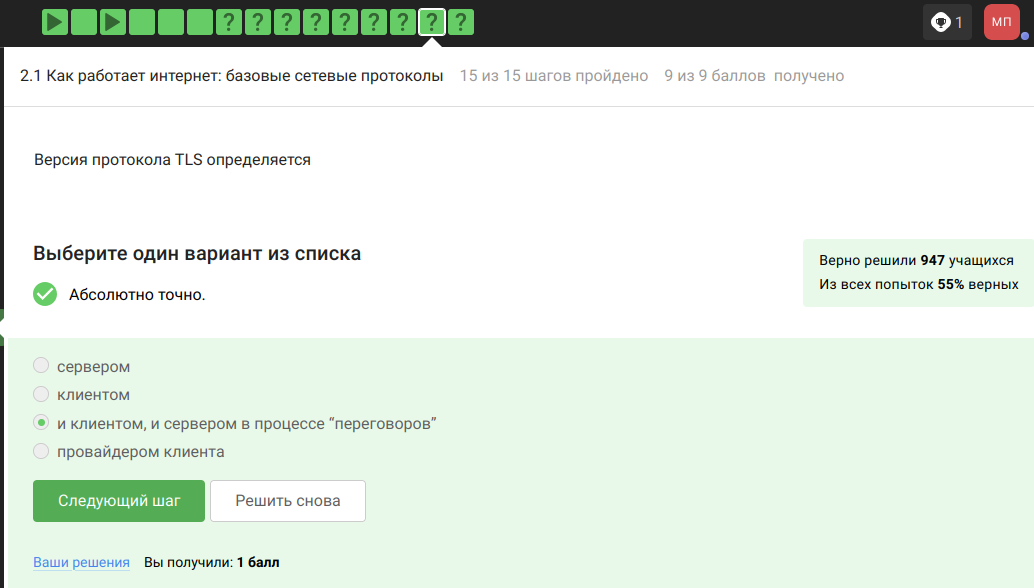


Рис. 8: нет названия

остальные варианты в протоколе предусмотрены

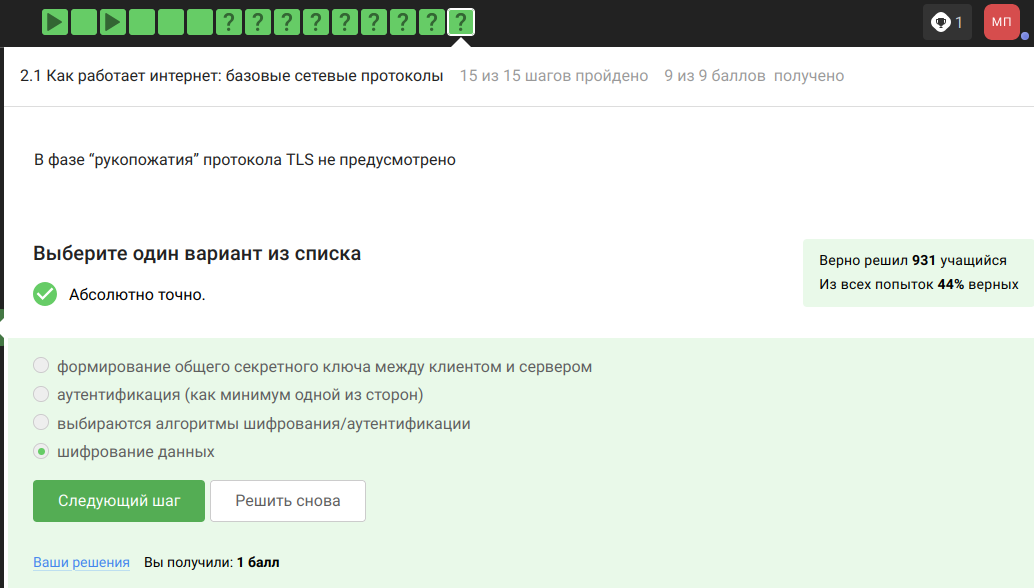


Рис. 9: нет названия

Куки точно не хранят пароли и IP-адреса, а id ceccии и идентификатор хранят

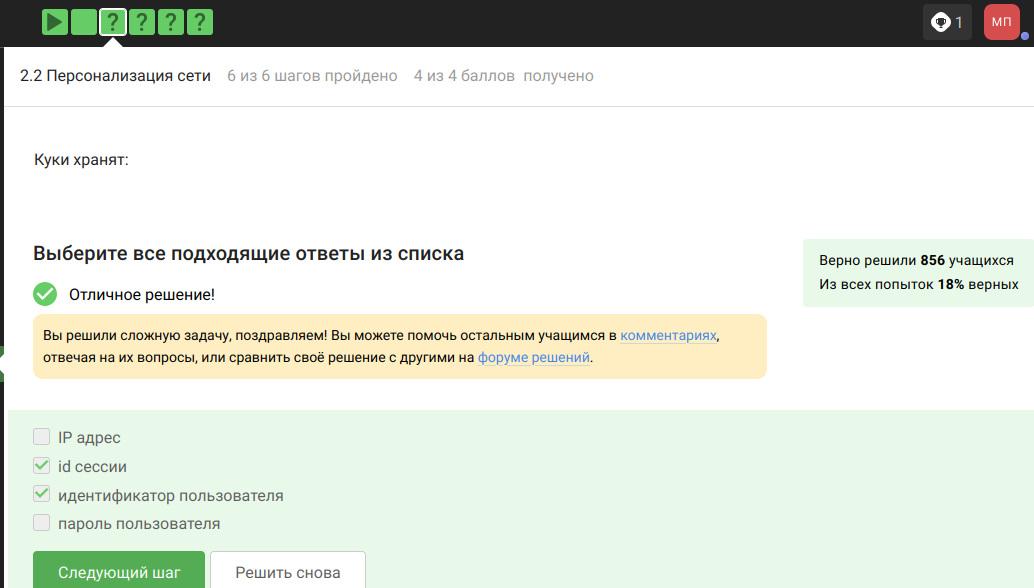


Рис. 10: нет названия

куки не делают соединение более надежным

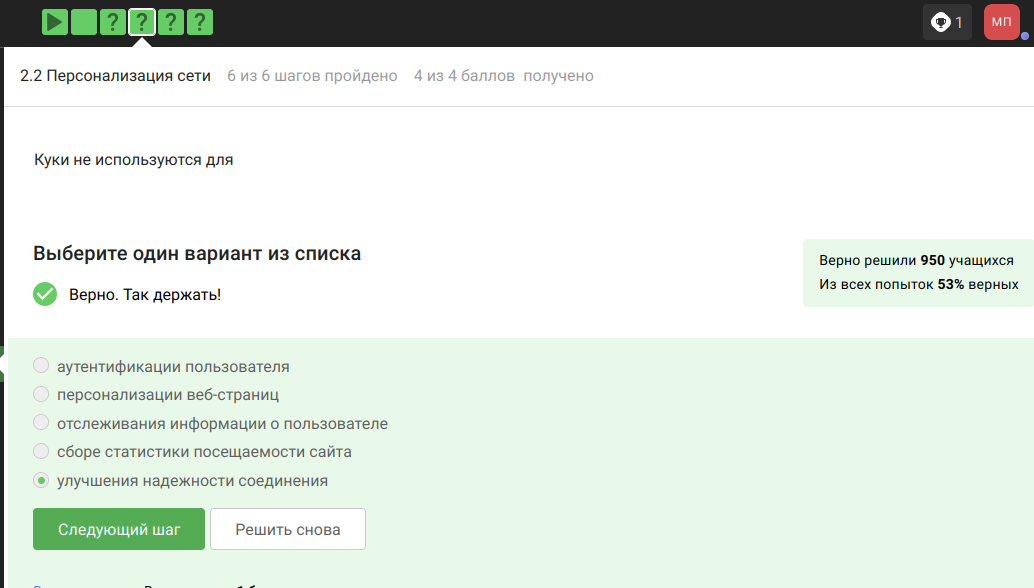


Рис. 11: нет названия

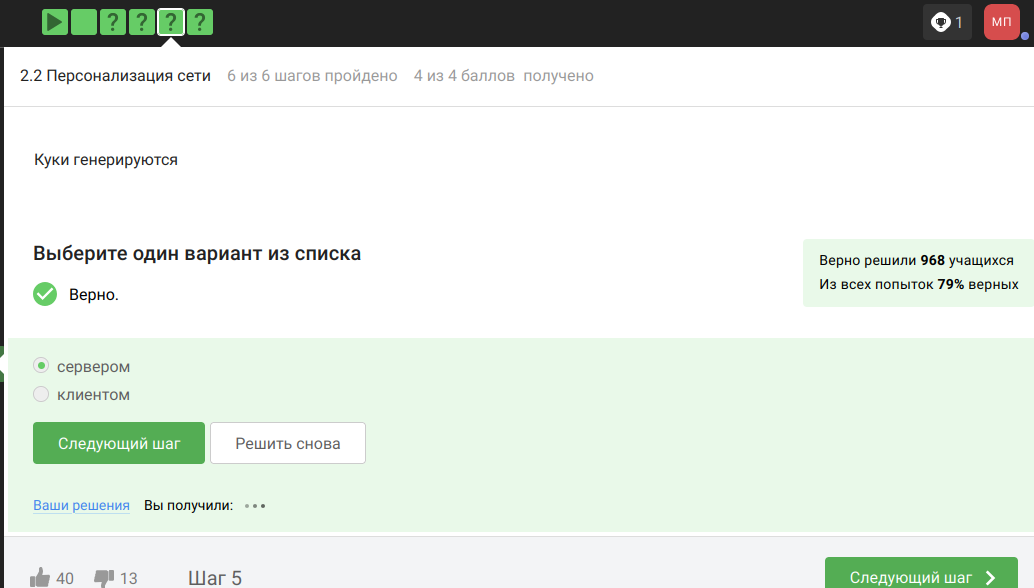


Рис. 12: нет названия

Сессионные куки хранятся в течение сессии, то есть пока используется веб-сайт

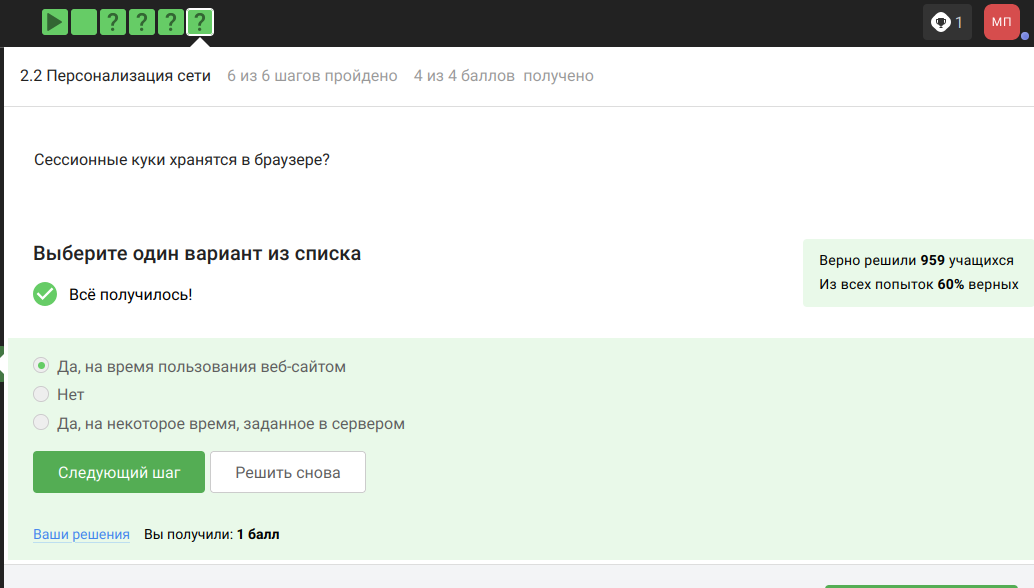


Рис. 13: нет названия

Необходимо три узла - входной, промежуточный и выходной

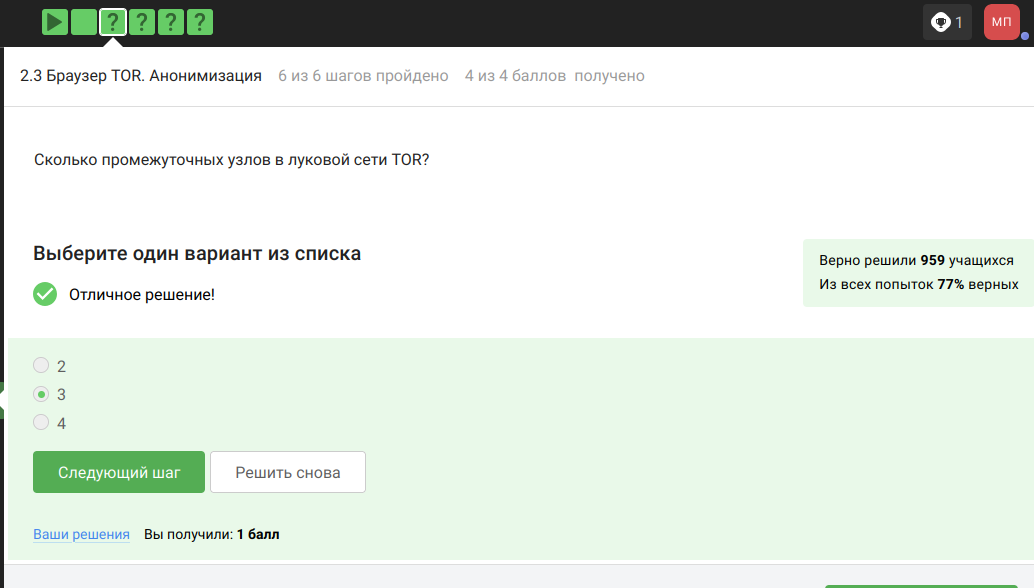


Рис. 14: нет названия

IP-адрес не должен быть известен охранному и промежуточному узлам

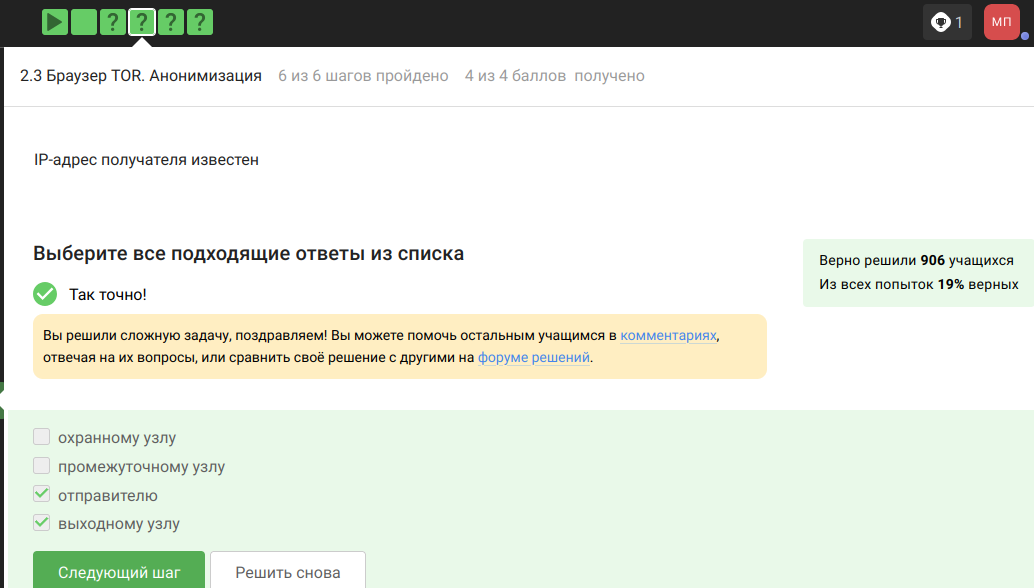


Рис. 15: нет названия

Отправитель генерирует общий секретный ключ со узлами, через которые идет передача, то есть со всеми

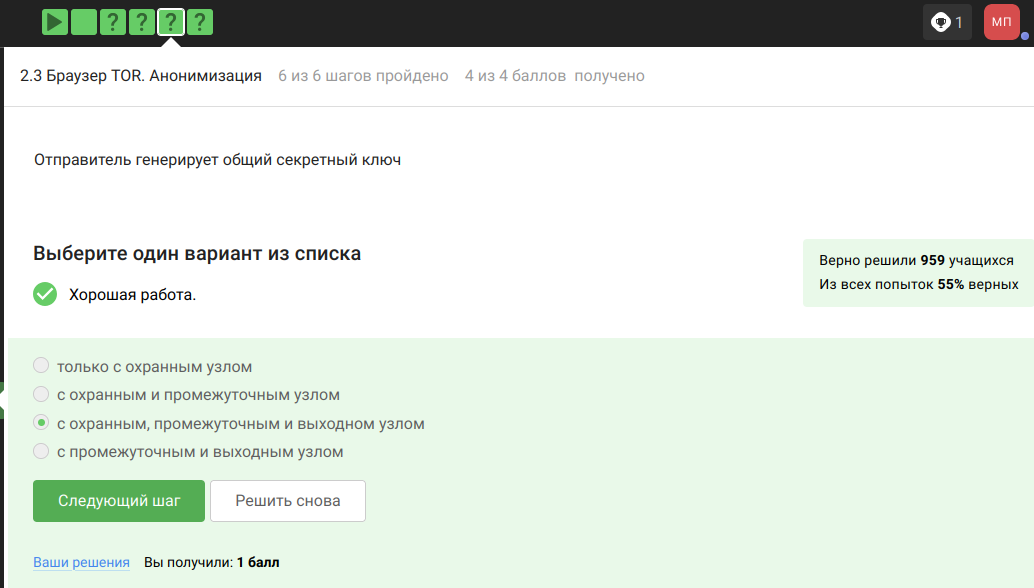


Рис. 16: нет названия

Для получаения пакетов не нужно использовать TOR

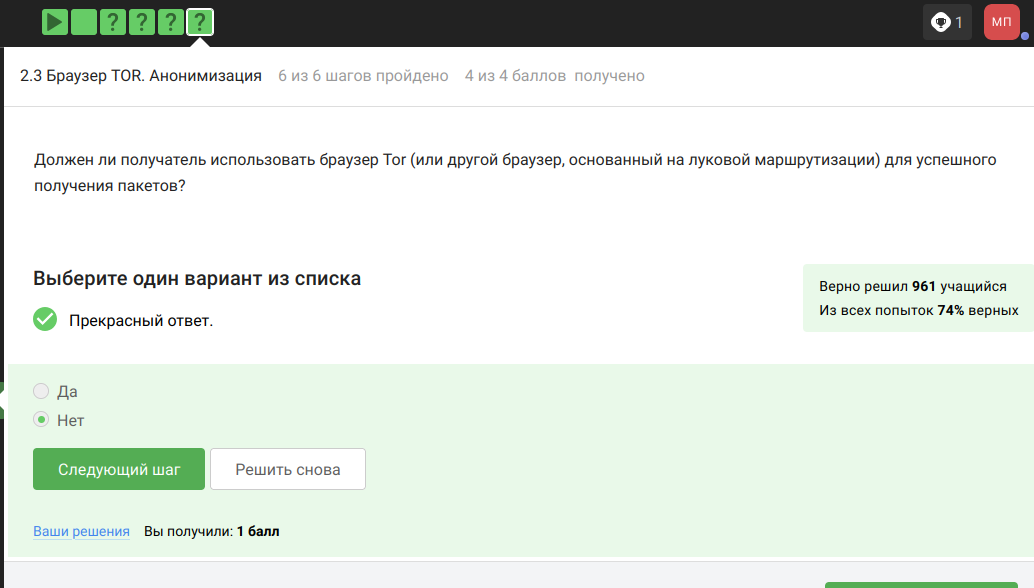


Рис. 17: нет названия

это определение Wi-Fi

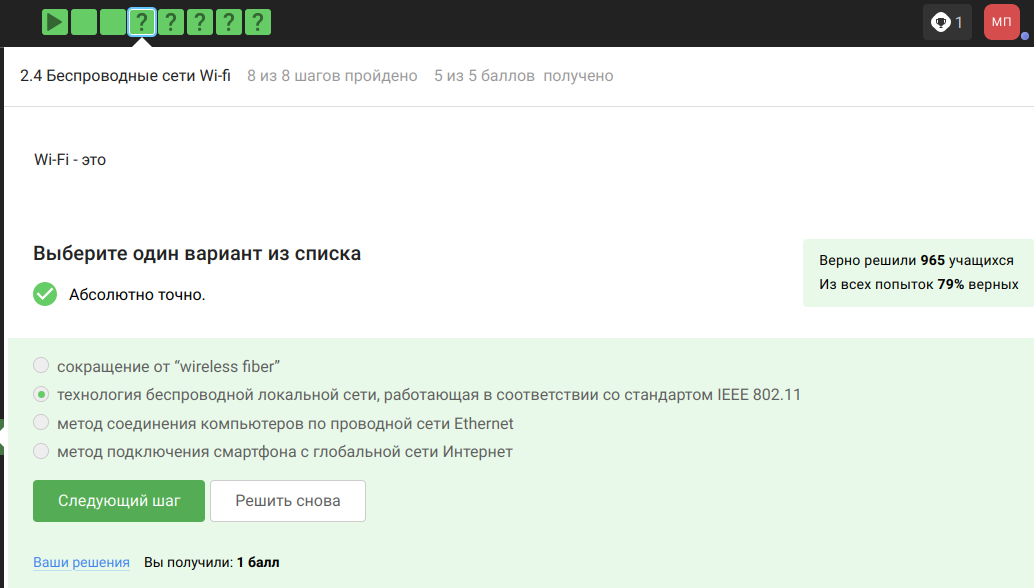


Рис. 18: нет названия

Для целей работы в Интернете Wi-Fi обычно располагается как канальный уровень

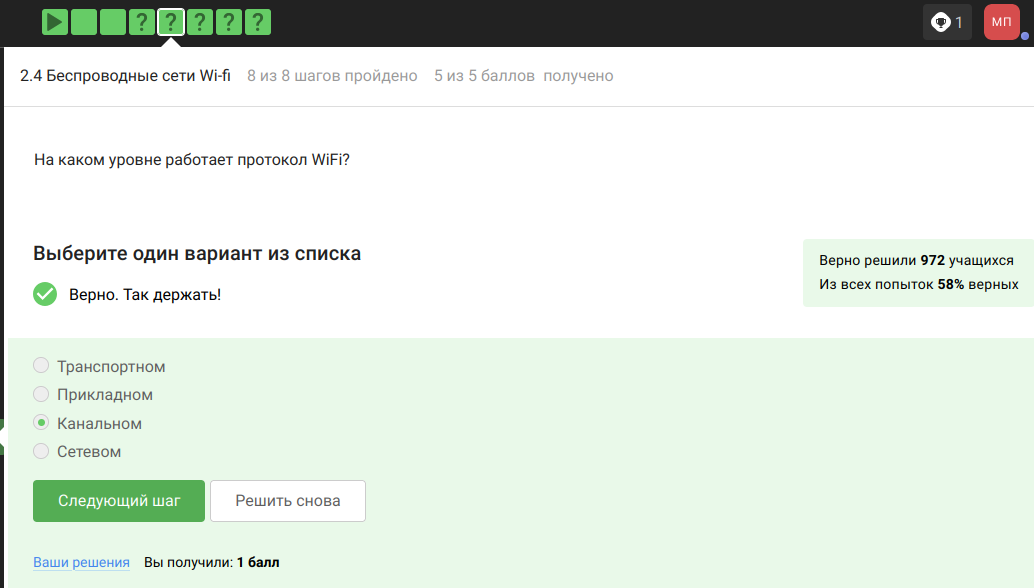


Рис. 19: нет названия

WEP (Wired Equivalent Privacy) – устаревший и небезопасный метод проверки подлинности

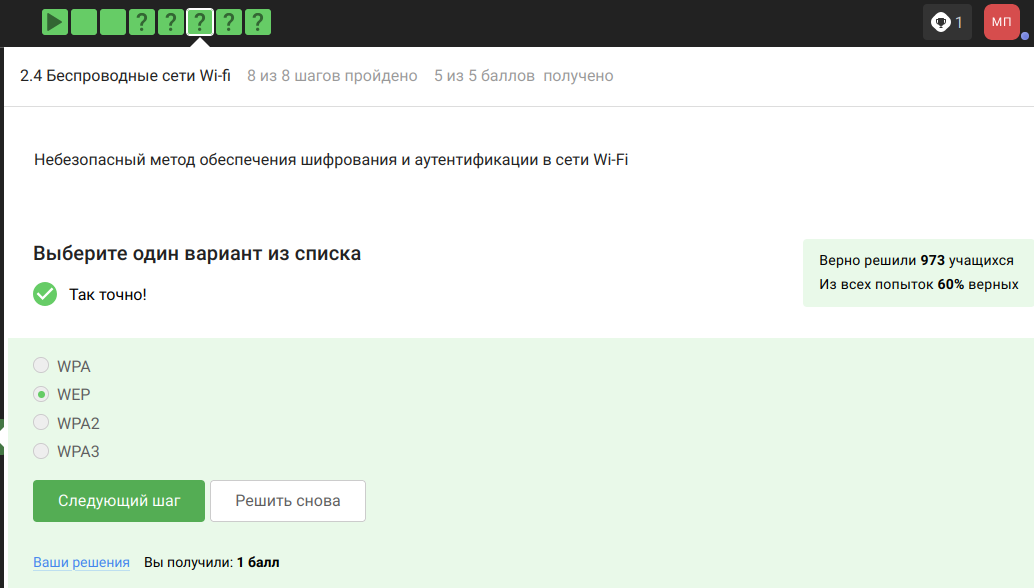


Рис. 20: нет названия

Нужно аутентифицировать устройства и позже передаются зашифрованные данные

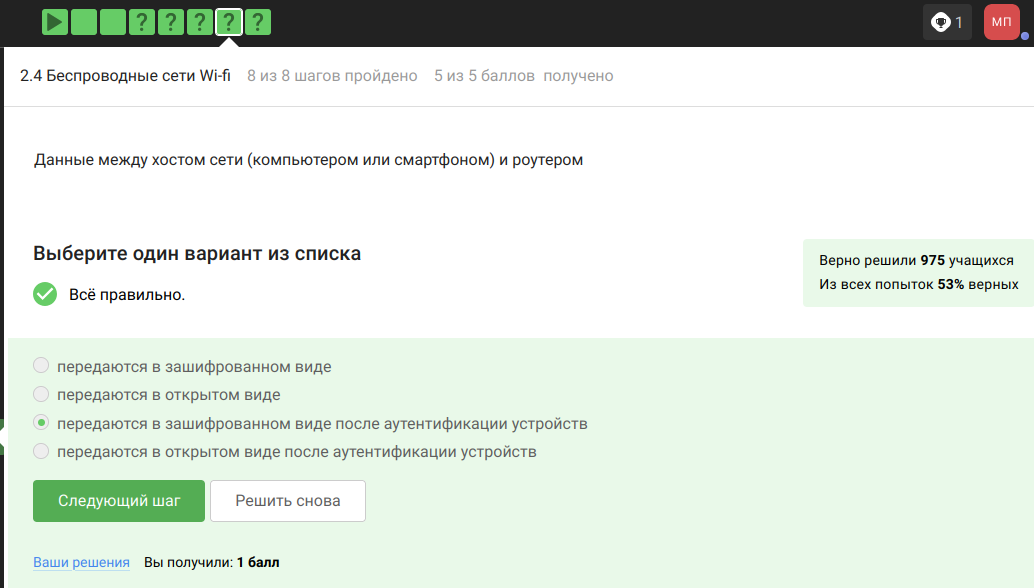


Рис. 21: нет названия

WPA2 Personal для личного использования

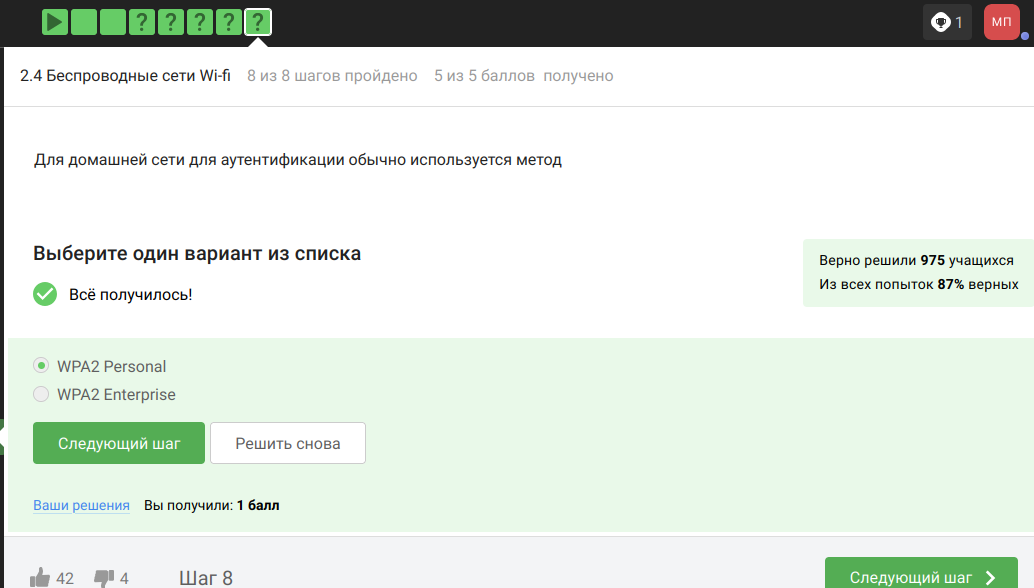


Рис. 22: нет названия

Шифрование диска — технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать.

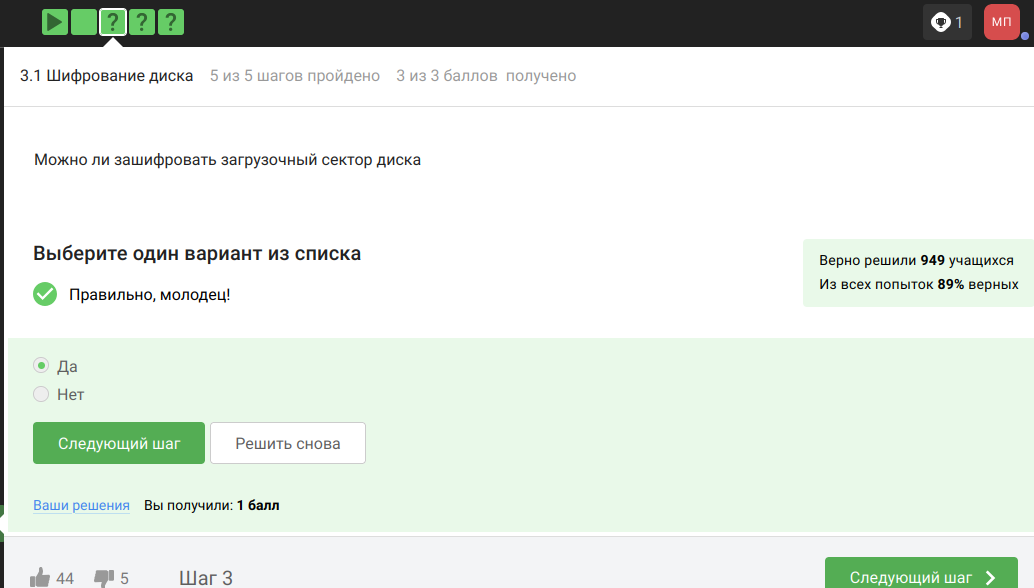


Рис. 23: нет названия

Шифрование диска основано на симметричном шифровании

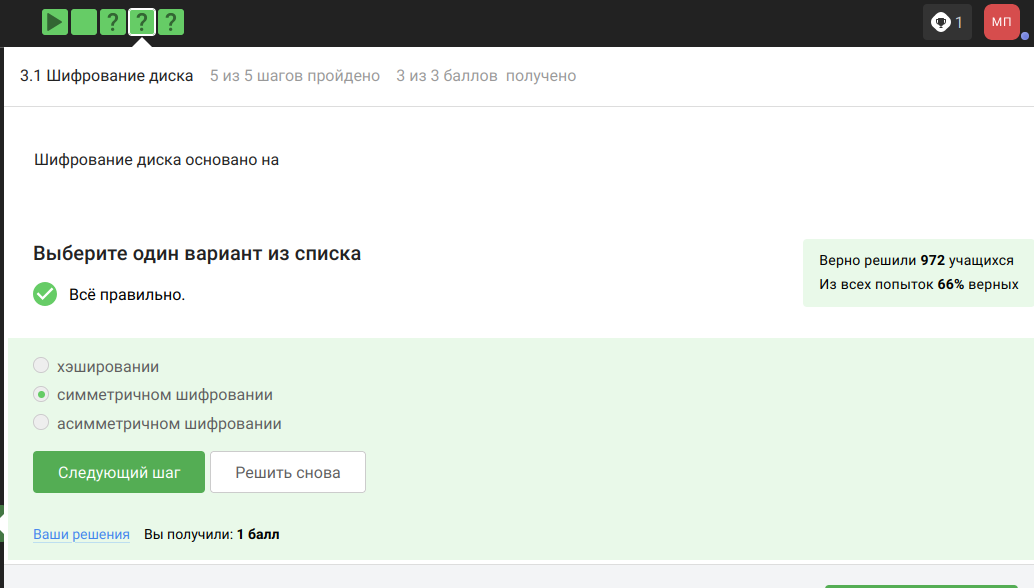


Рис. 24: нет названия

Отмечены программы, с помощью которых можно зашифровать жетский диск

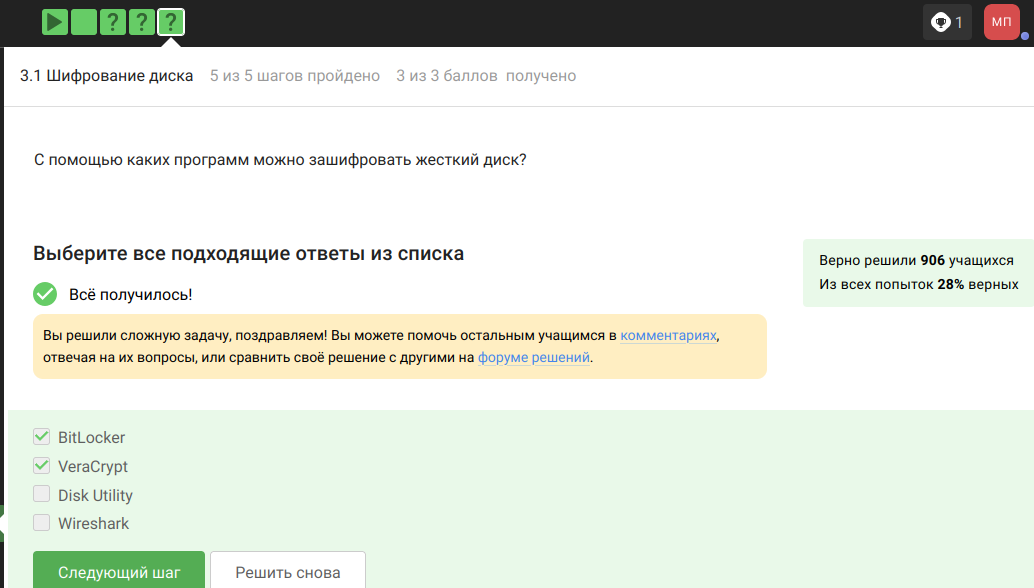


Рис. 25: нет названия

Стойкий пароль - тот, который тяжлее подобрать, он должен быть со спец. символами и длинный

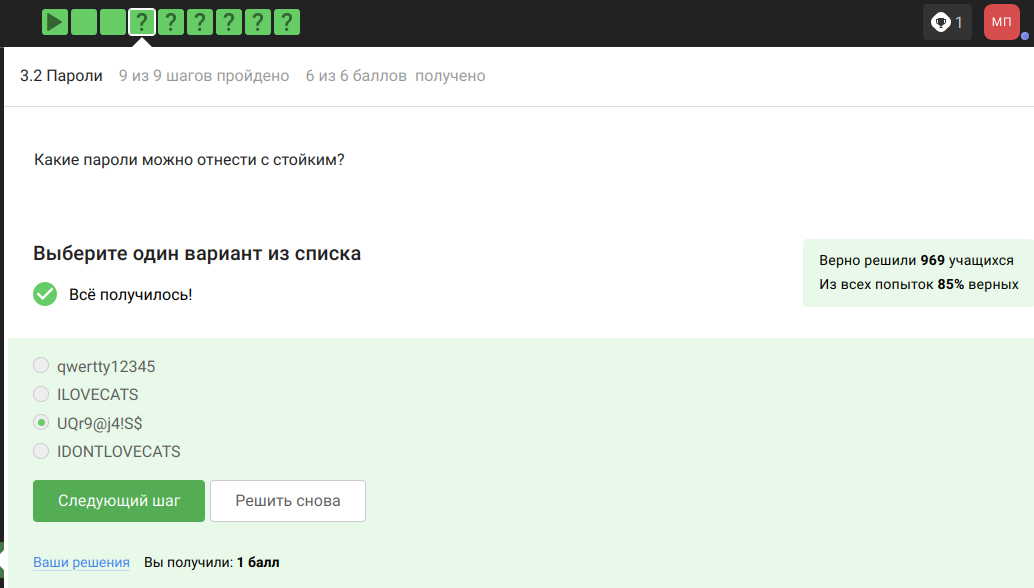


Рис. 26: нет названия

Все варианты, кроме менеджера паролей, совершенно не надежные

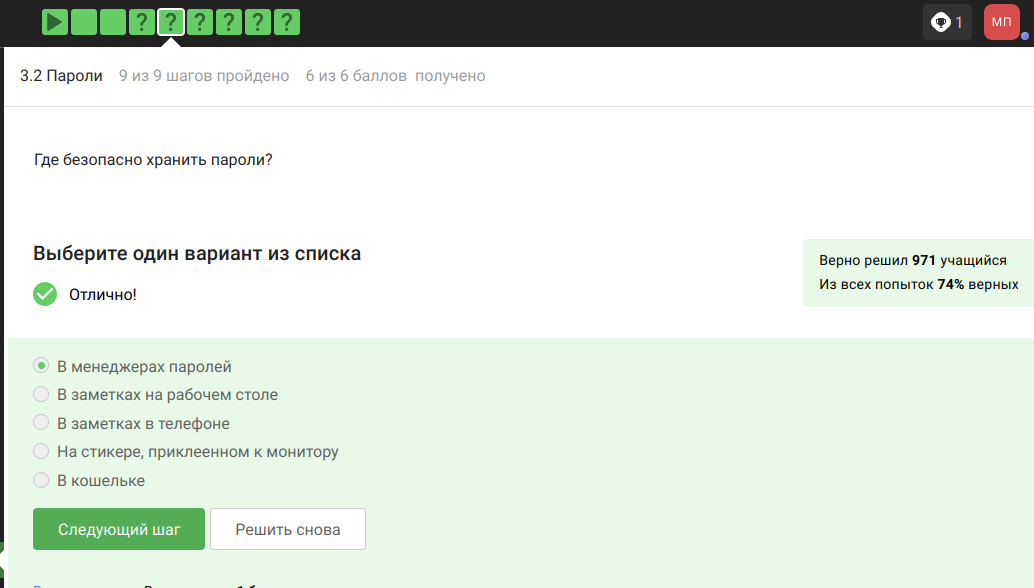


Рис. 27: нет названия

Капча нужна для проверки на то, что за экраном “не робот”

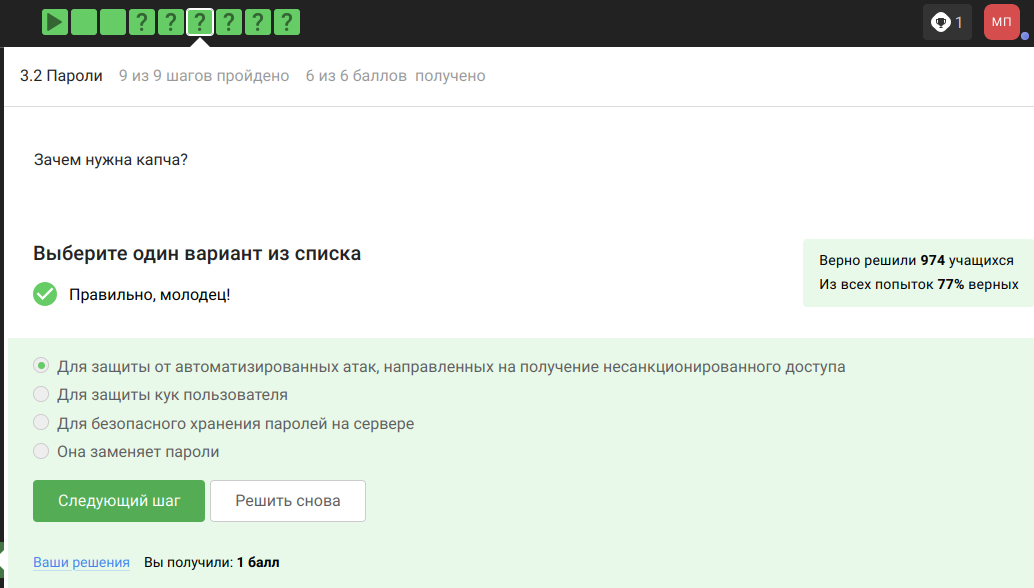


Рис. 28: нет названия

Опасно хранить пароли в открытом виде, поэтому хранят их хэши

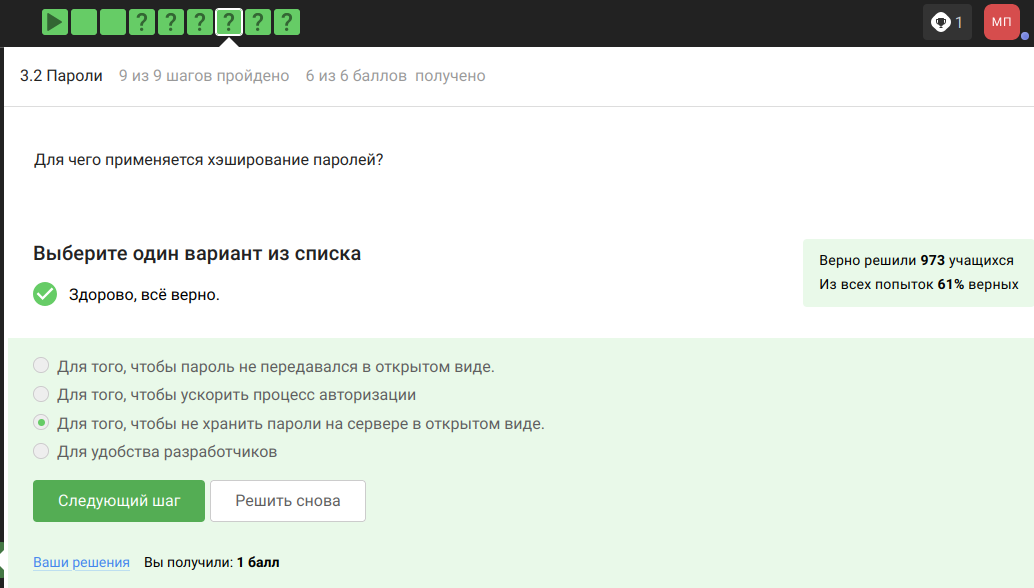


Рис. 29: нет названия

Соль не поможет

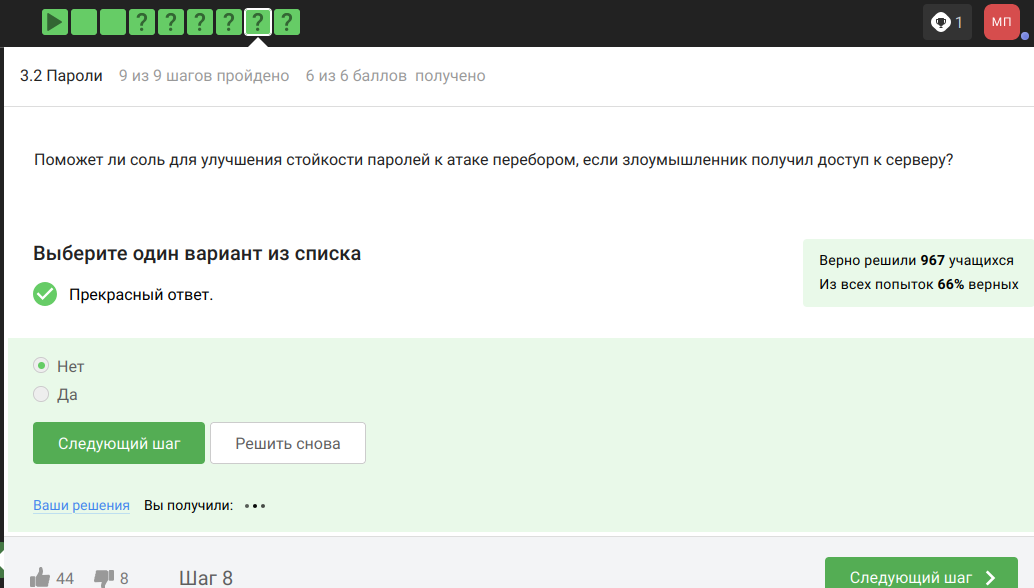


Рис. 30: нет названия

Все приведенные меры защищают от утечек данных

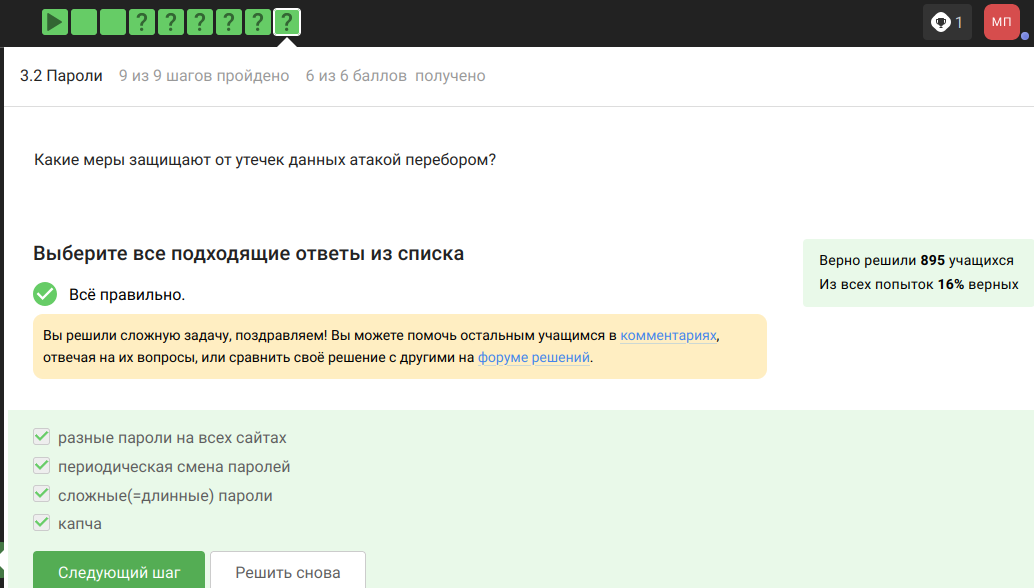


Рис. 31: нет названия

Фишинговые ссылки очень похожи на ссылки известных сервисов, но с некоторыми отличиями

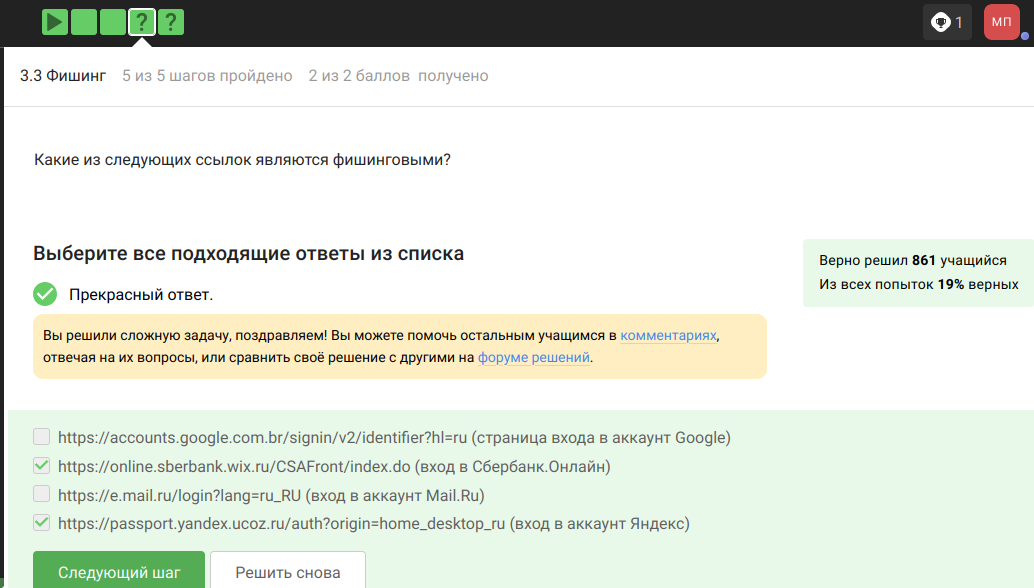


Рис. 32: нет названия

Да, может, например, если пользователя со знакомым адресом взломали

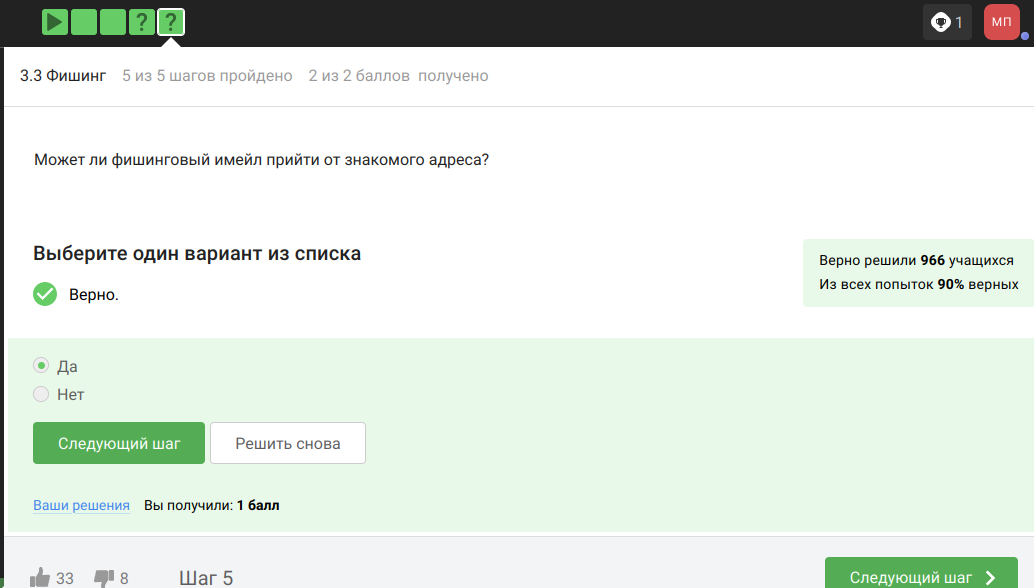


Рис. 33: нет названия

Ответ дан в соответствии с определением

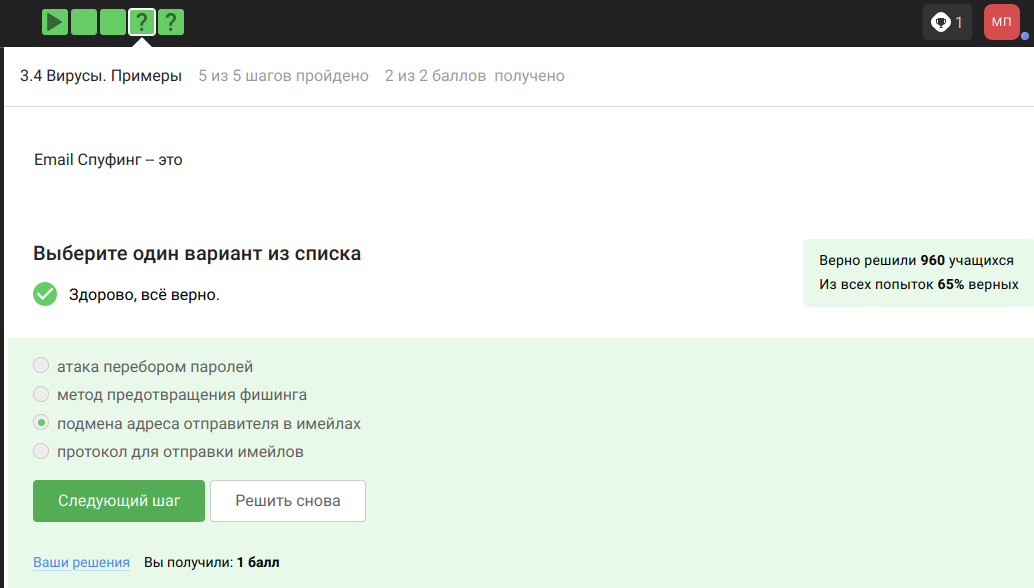


Рис. 34: нет названия

Троян маскируется под обычную программу

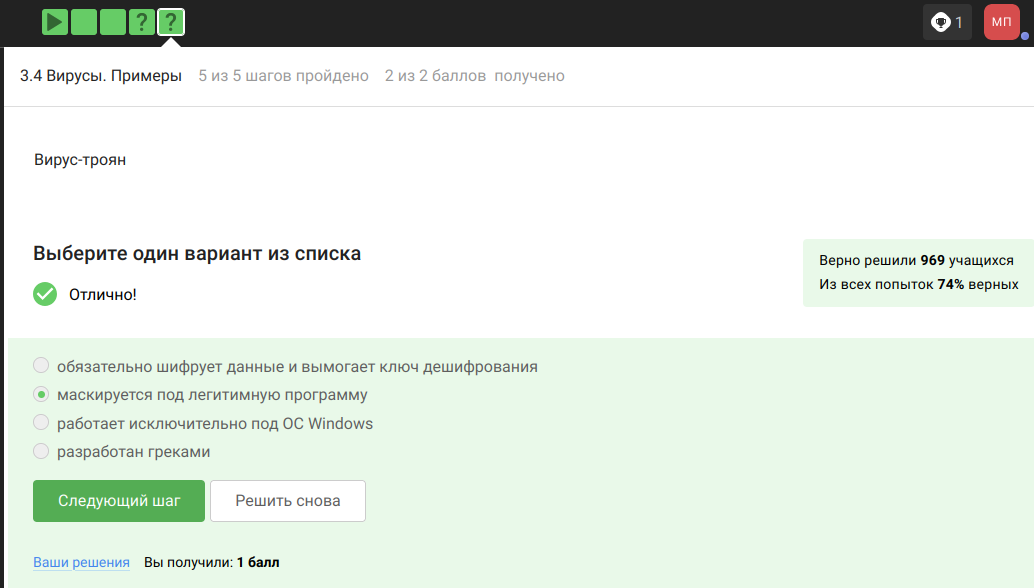


Рис. 35: нет названия

При установке первого сообщения отправителем формируется ключ шифрования

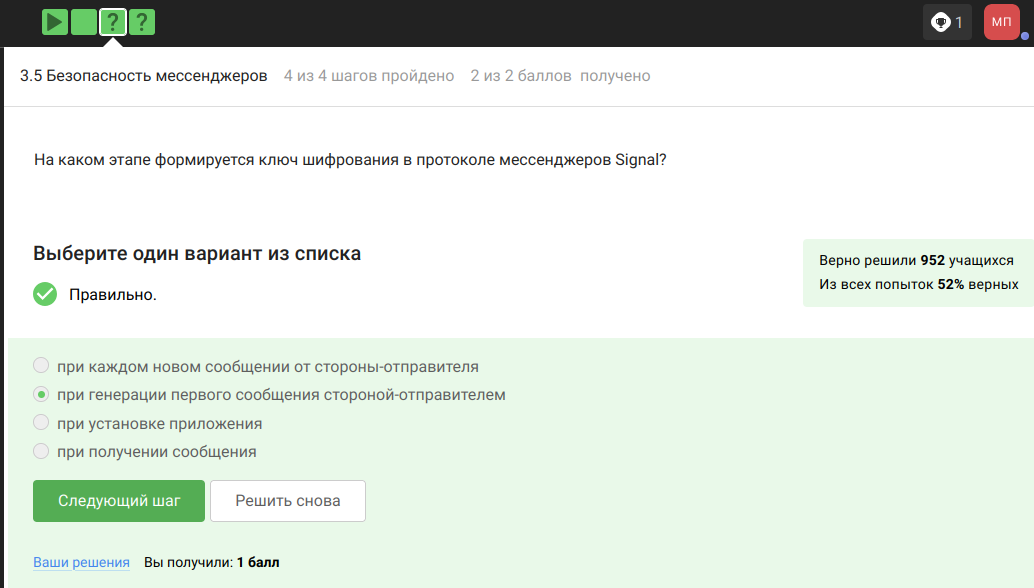


Рис. 36: нет названия

Суть сквозного шифрования состоит в том, что сообзения передаются по узлам связи в зашифрованном виде

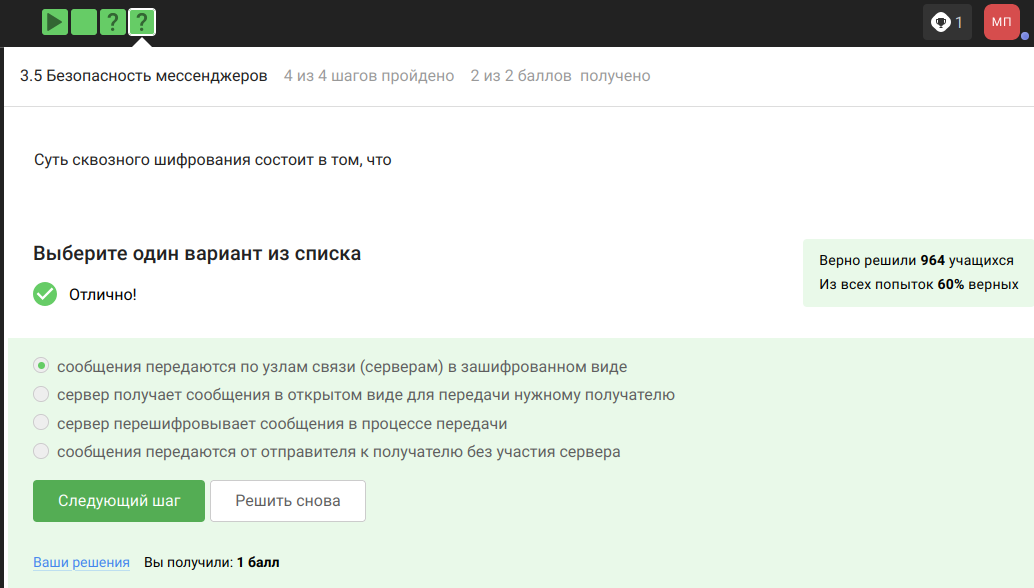


Рис. 37: нет названия

Для ответа на вопрос используется определение ассмиетричного шифрования с двумя ключами

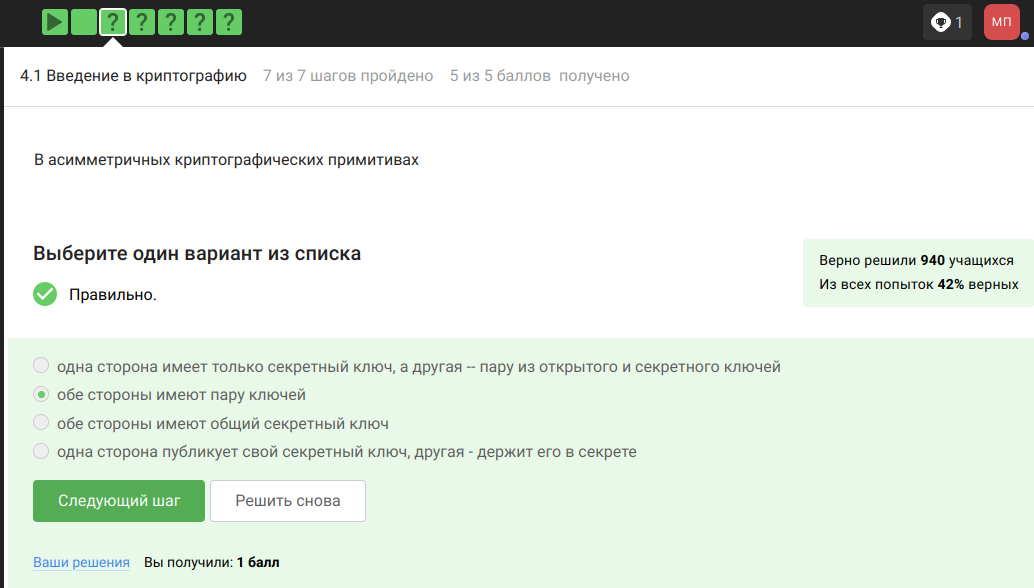


Рис. 38: нет названия

Отмечены основные условия для криптографической хэш-функции

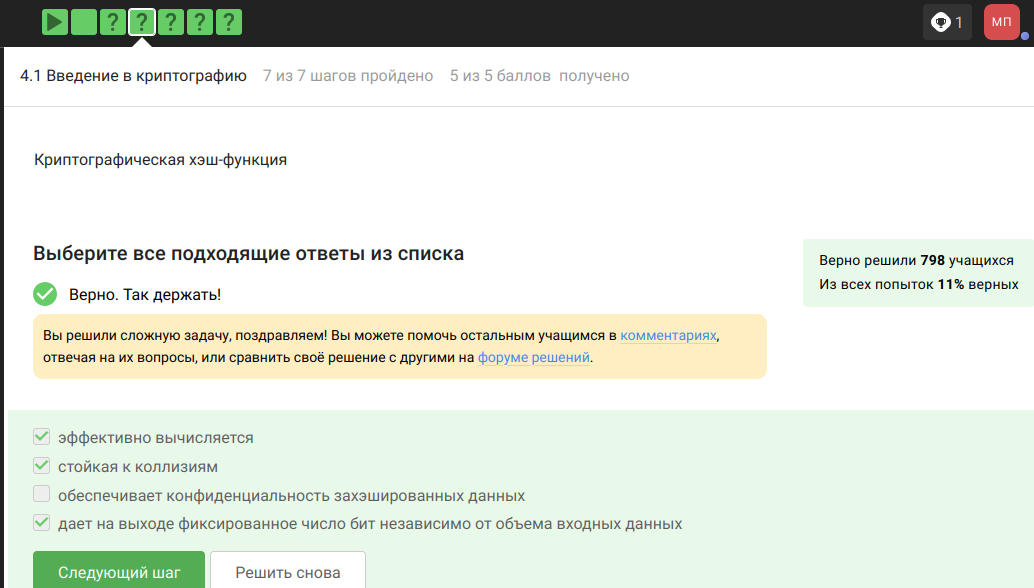


Рис. 39: нет названия

Отмечены алгоритмы цифровой подписи

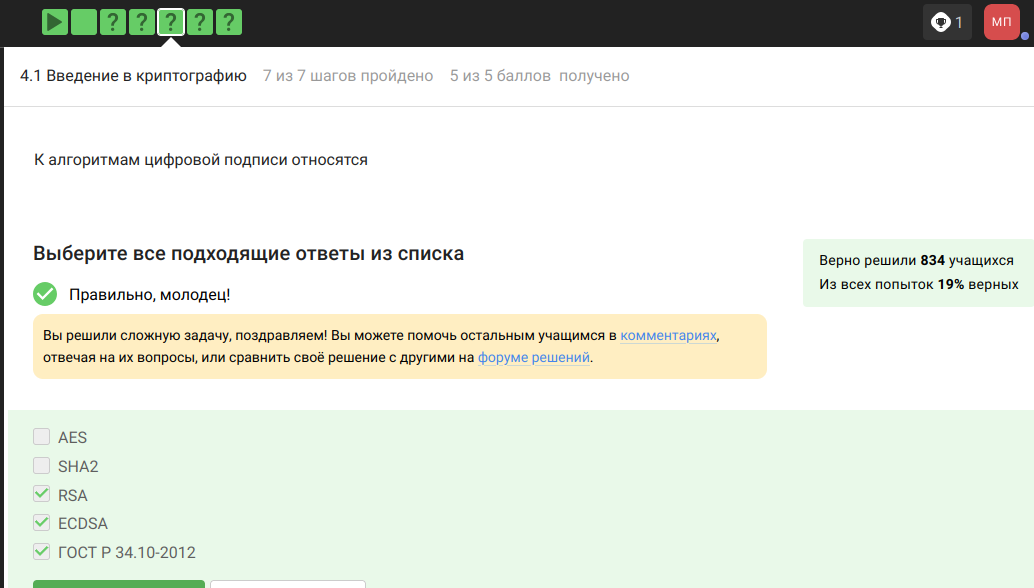


Рис. 40: нет названия

В информационной безопасности аутентификация сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения

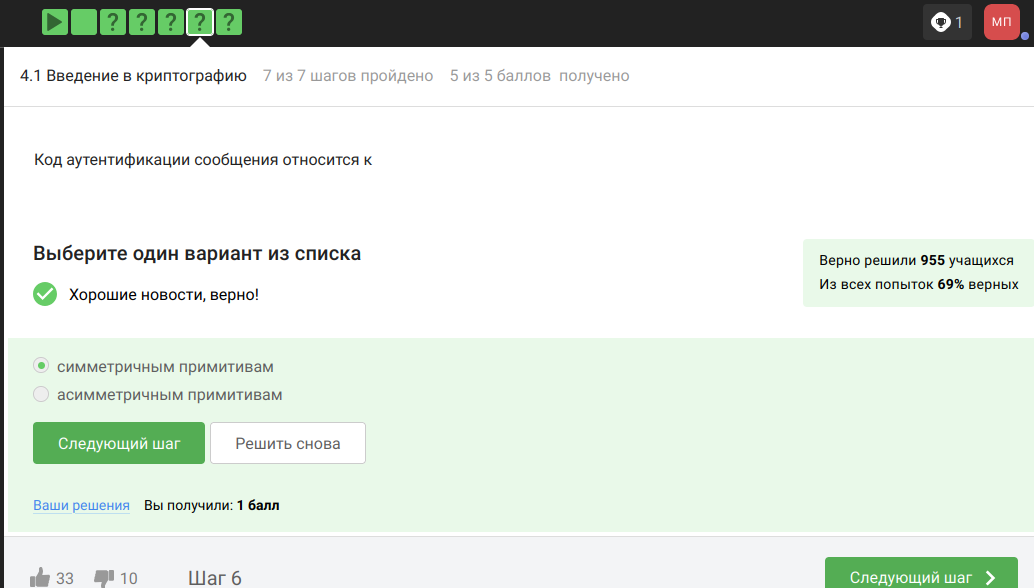


Рис. 41: нет названия

Определение обмена ключами Диффи-Хэллмана.

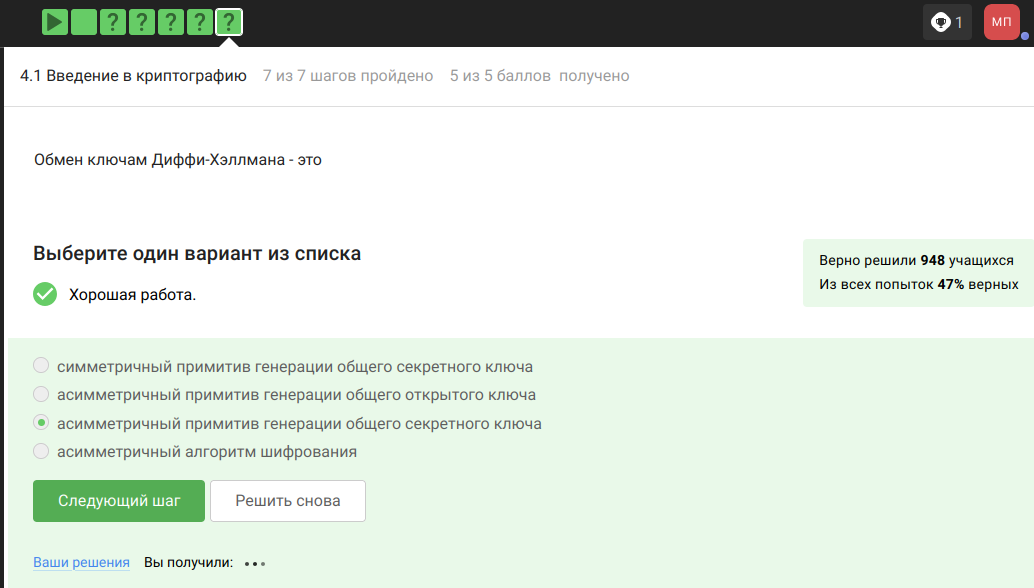


Рис. 42: нет названия

По определению цифровой подписи протокол ЭЦП относится к протоколам с публичным ключом

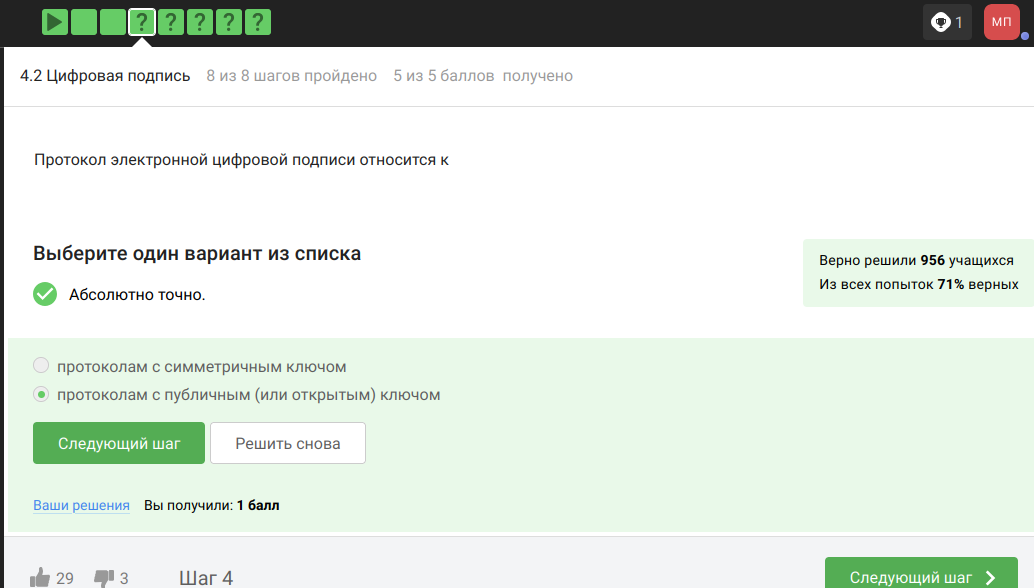


Рис. 43: нет названия

На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш- функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства

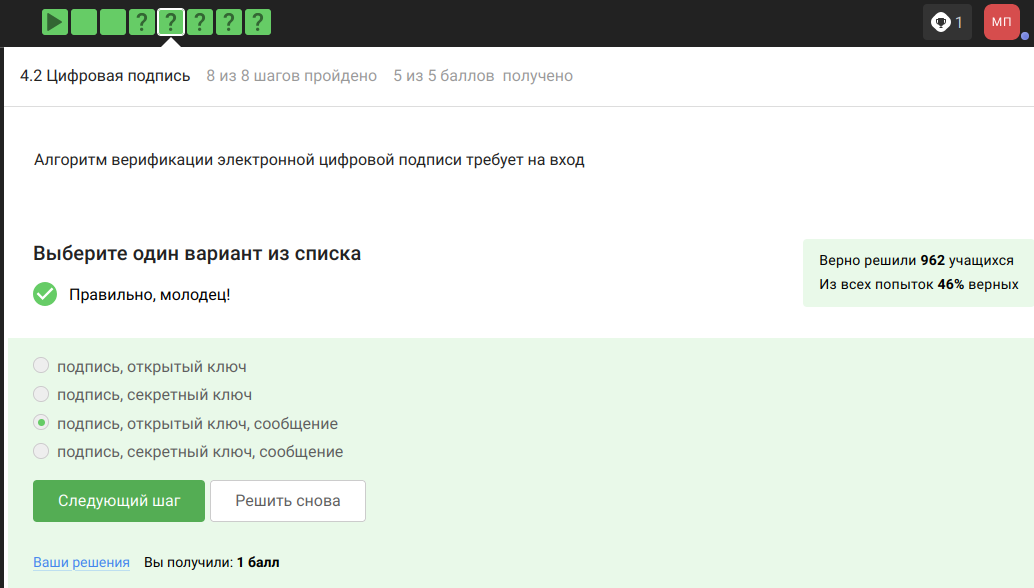


Рис. 44: нет названия

Электронная подпись обеспечивает все указанное, кроме конфиденциальности

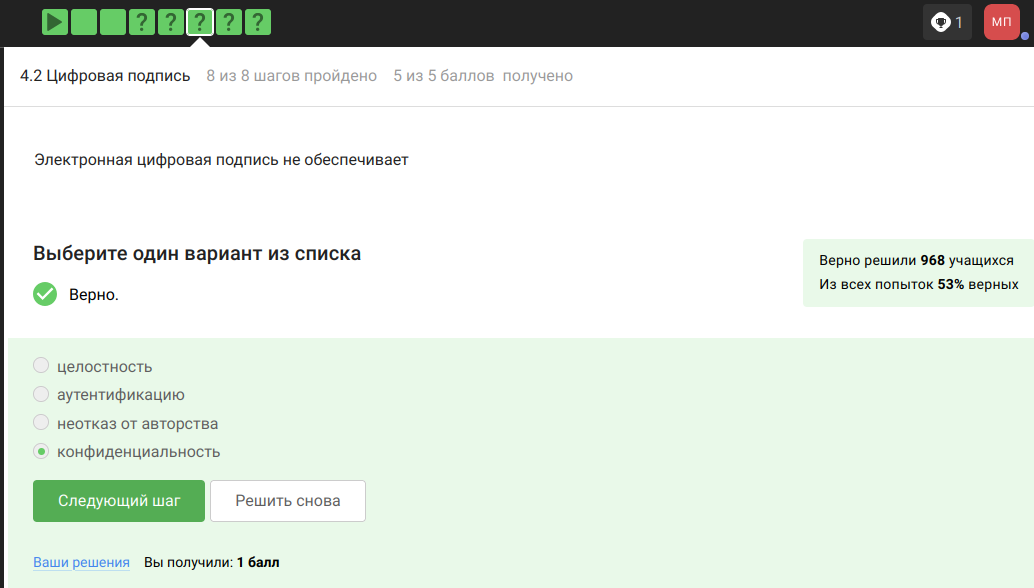


Рис. 45: нет названия

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись

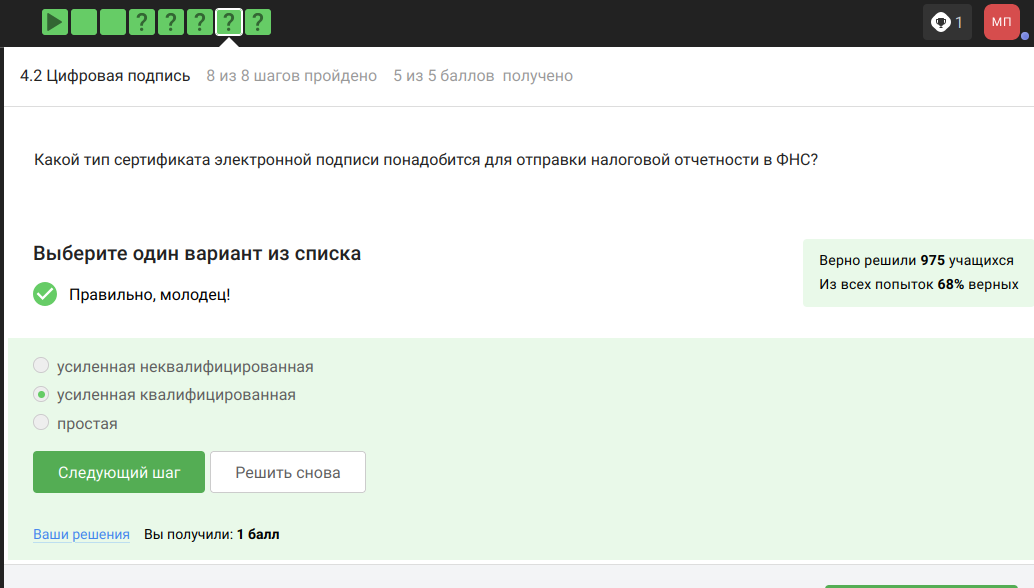


Рис. 46: нет названия

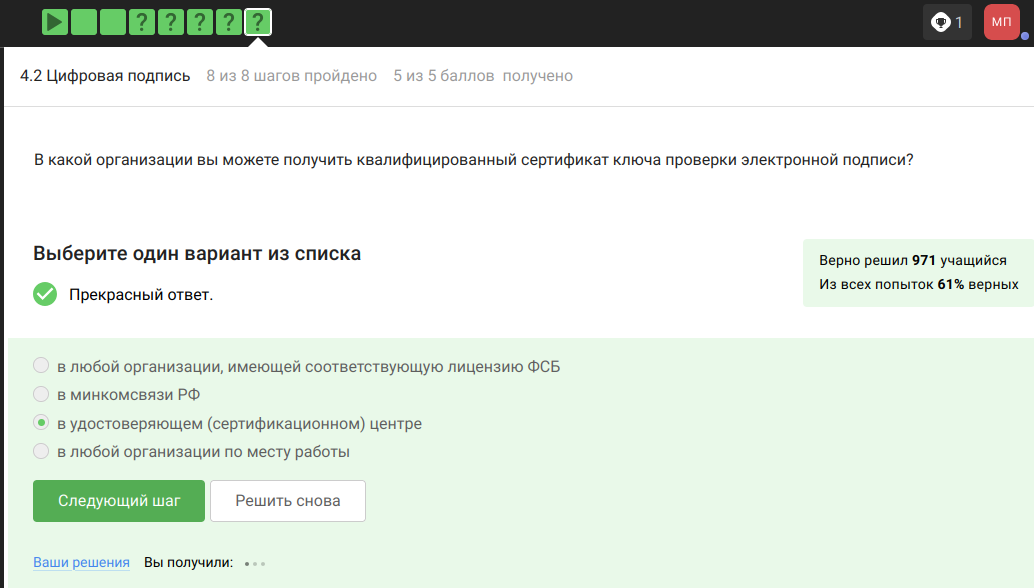


Рис. 47: нет названия

Известные платежные системы - Visa, MasterCard, МИР

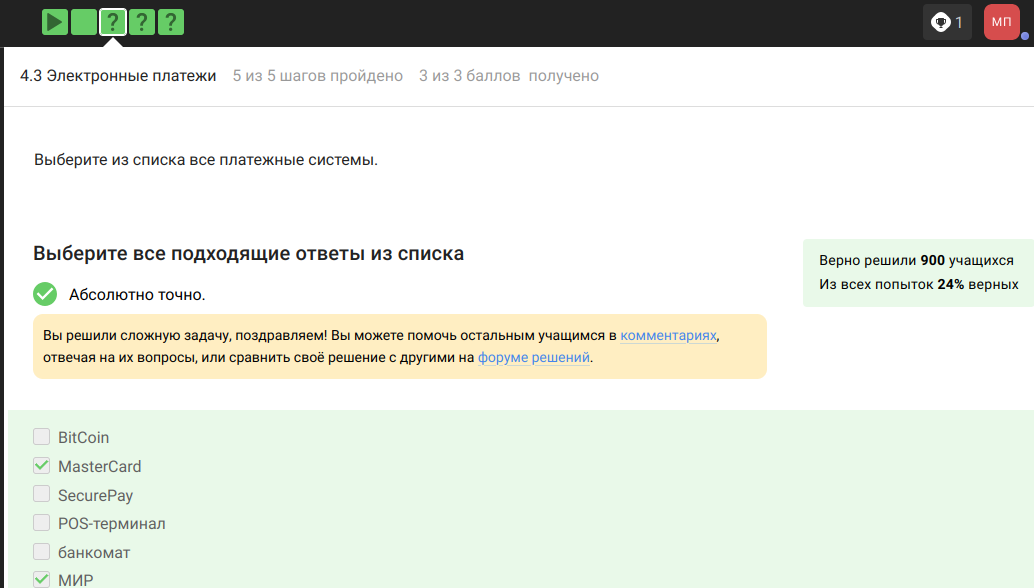


Рис. 48: нет названия

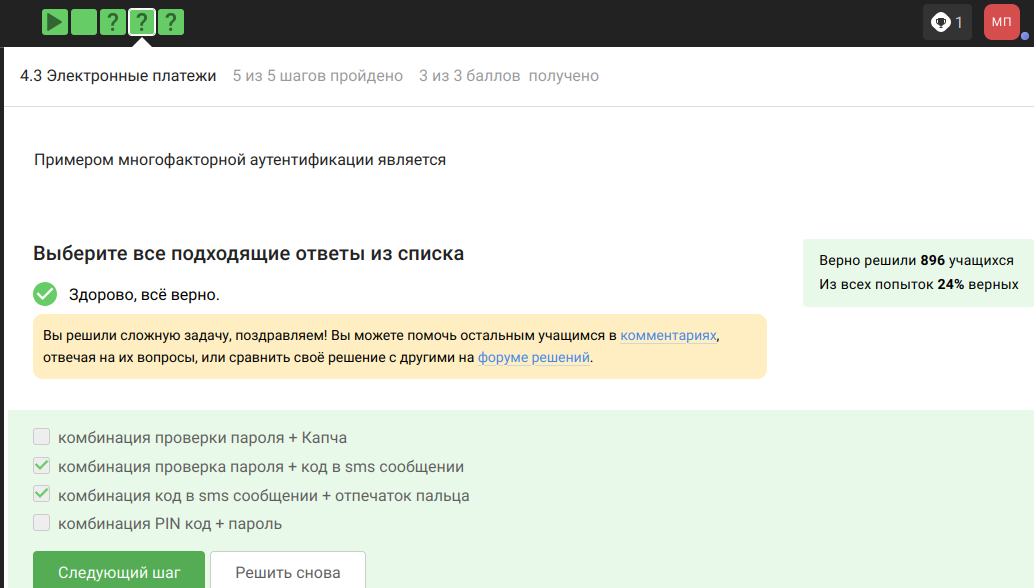


Рис. 49: нет названия

При онлайн платежах используется многофакторная аутентификация

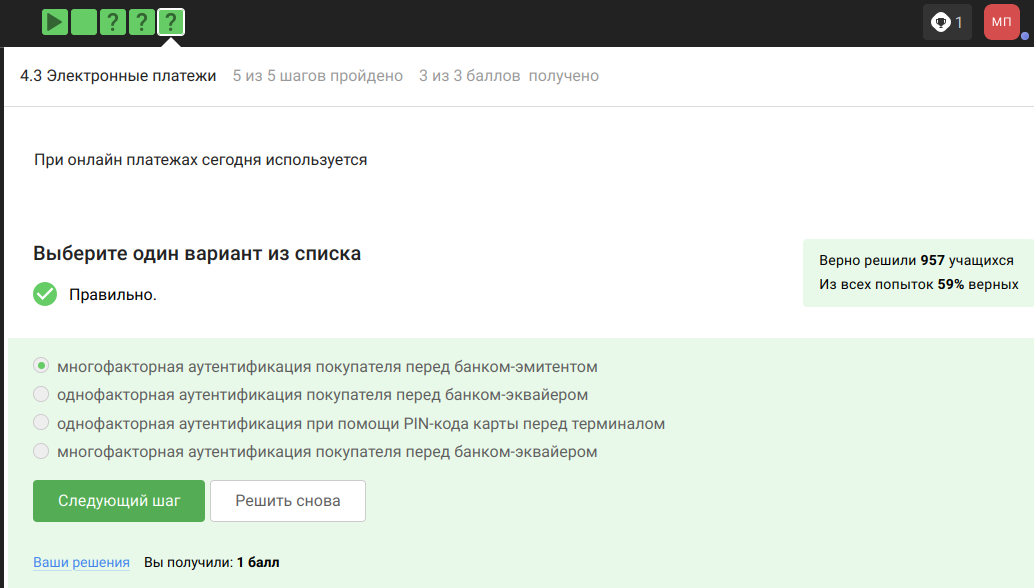


Рис. 50: нет названия

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне

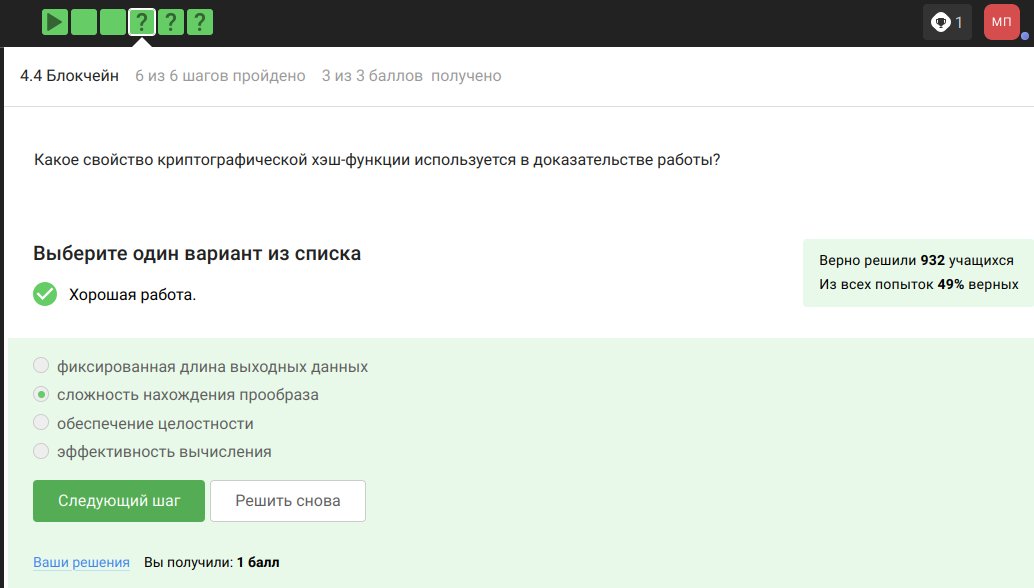


Рис. 51: нет названия

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети

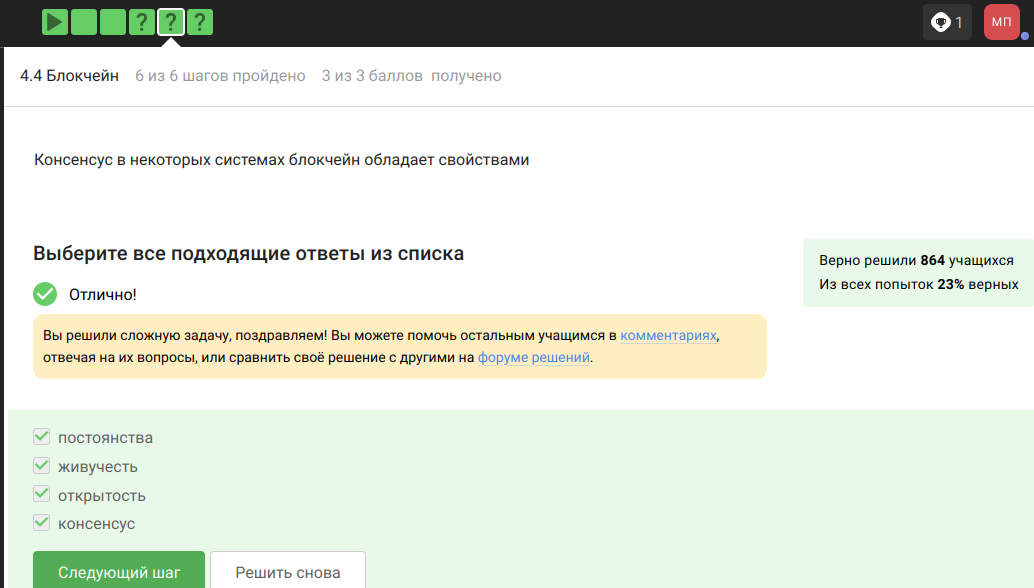


Рис. 52: нет названия

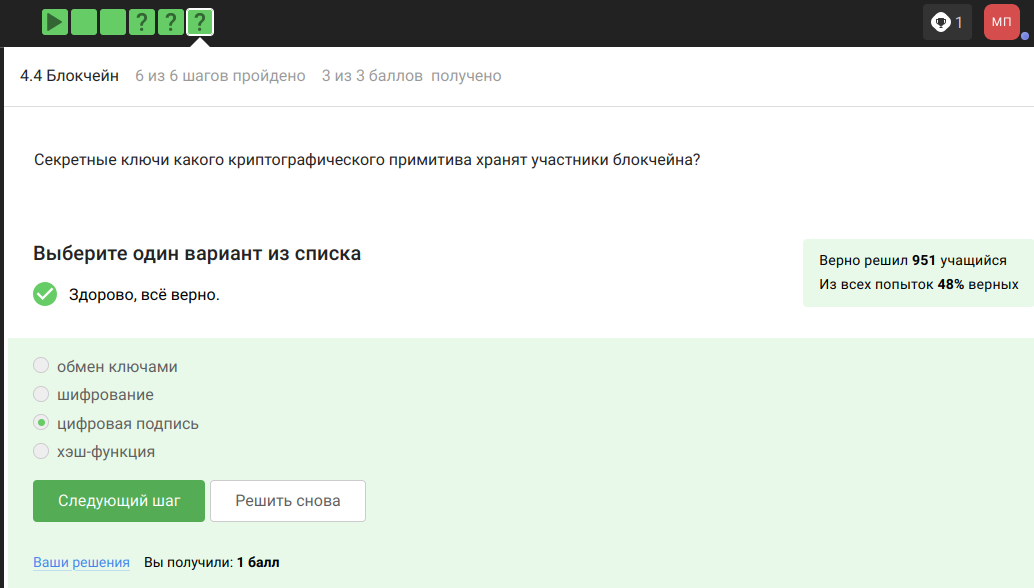


Рис. 53: нет названия

Прошла курс на степике

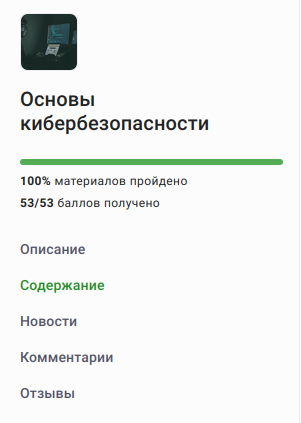


Рис. 54: нет названия

# 3 Выводы

Прошла курс на степике

# Список литературы