

Внешний курс

Степик по основам безопасности

Прокопьева Марина Евгеньевна

Содержание

1	Цель работы	6
2	Выполнение	7
3	Выводы	35
	Список литературы	36

Список иллюстраций

2.1	нет названия	7
2.2	нет названия	8
2.3	нет названия	8
2.4	нет названия	9
2.5	нет названия	9
2.6	нет названия	10
2.7	нет названия	10
2.8	нет названия	11
2.9	нет названия	11
2.10	нет названия	12
2.11	нет названия	12
2.12	нет названия	13
2.13	нет названия	13
2.14	нет названия	14
2.15	нет названия	14
2.16	нет названия	15
2.17	нет названия	15
2.18	нет названия	16
2.19	нет названия	16
2.20	нет названия	17
2.21	нет названия	17
2.22	нет названия	18
2.23	нет названия	18
2.24	нет названия	19
2.25	нет названия	19
2.26	нет названия	20
2.27	нет названия	20
2.28	нет названия	21
2.29	нет названия	21
2.30	нет названия	22
2.31	нет названия	22
2.32	нет названия	23
2.33	нет названия	23
2.34	нет названия	24
2.35	нет названия	24
2.36	нет названия	25
2.37	нет названия	25

2.38 нет названия	26
2.39 нет названия	26
2.40 нет названия	27
2.41 нет названия	27
2.42 нет названия	28
2.43 нет названия	28
2.44 нет названия	29
2.45 нет названия	29
2.46 нет названия	30
2.47 нет названия	30
2.48 нет названия	31
2.49 нет названия	31
2.50 нет названия	32
2.51 нет названия	32
2.52 нет названия	33
2.53 нет названия	33
2.54 нет названия	34

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

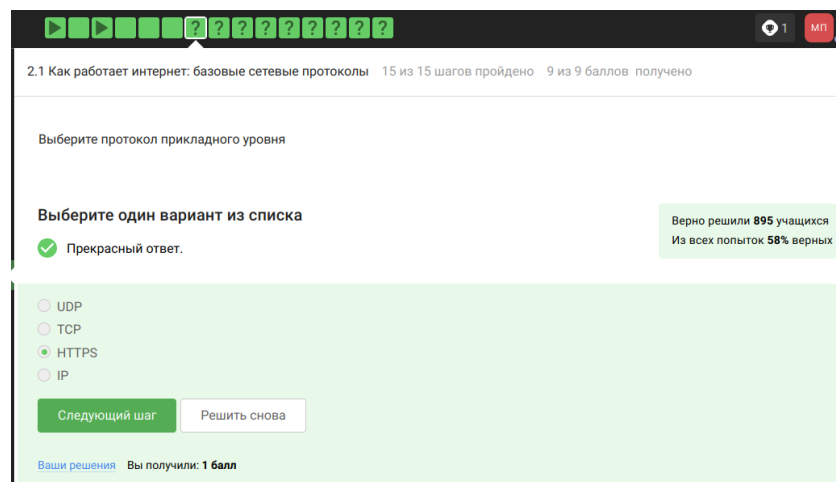


Рис. 2.1: нет названия

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

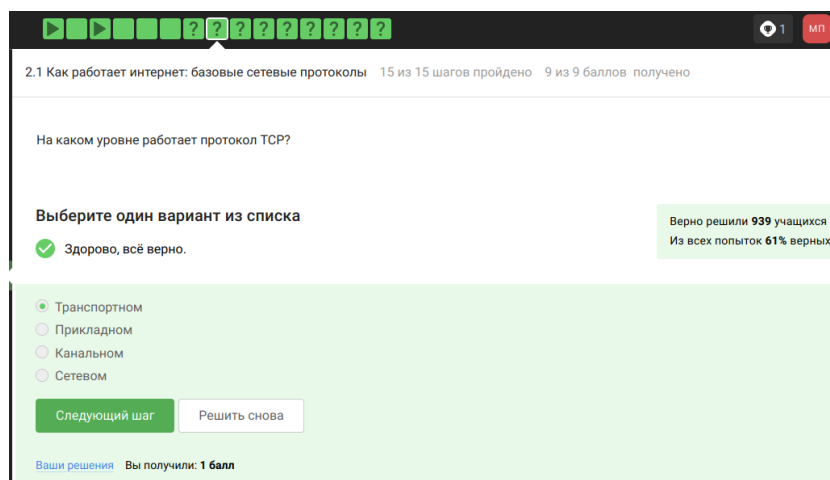


Рис. 2.2: нет названия

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

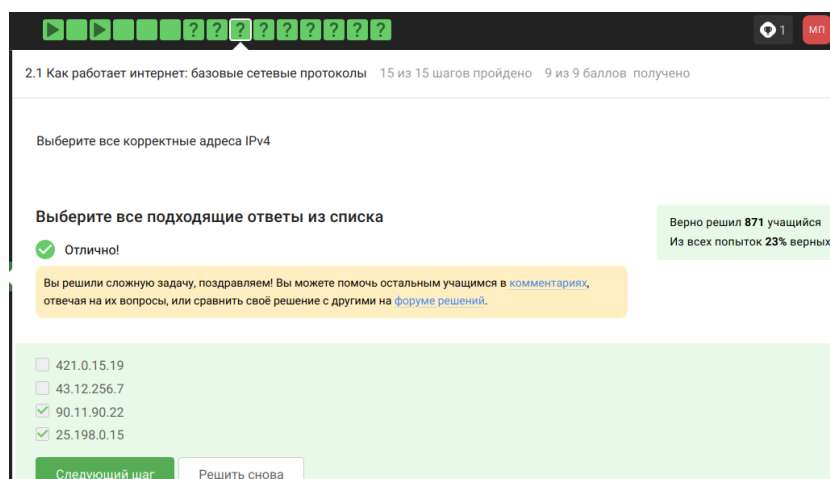


Рис. 2.3: нет названия

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

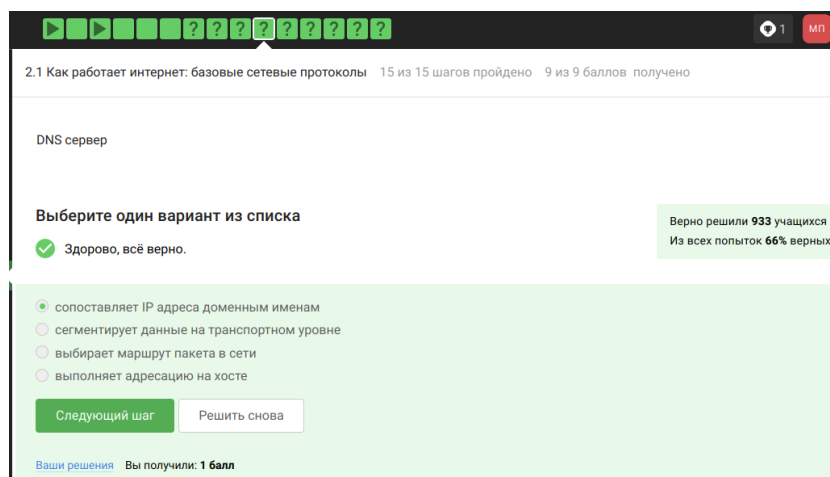


Рис. 2.4: нет названия

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

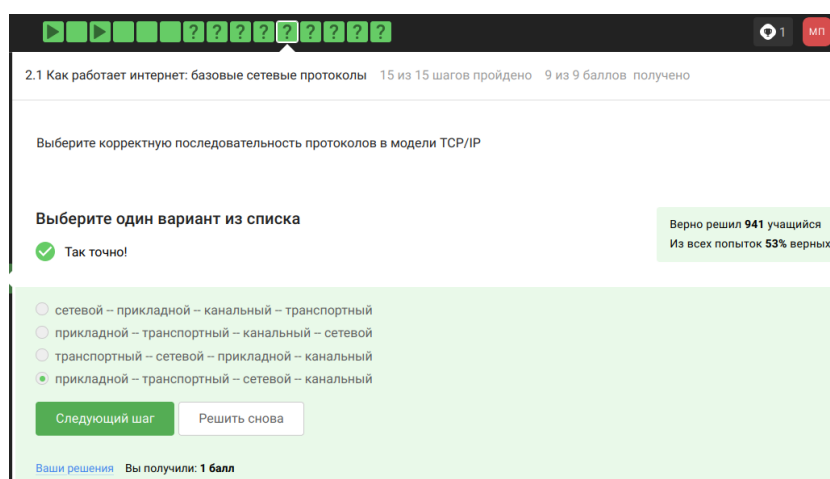


Рис. 2.5: нет названия

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

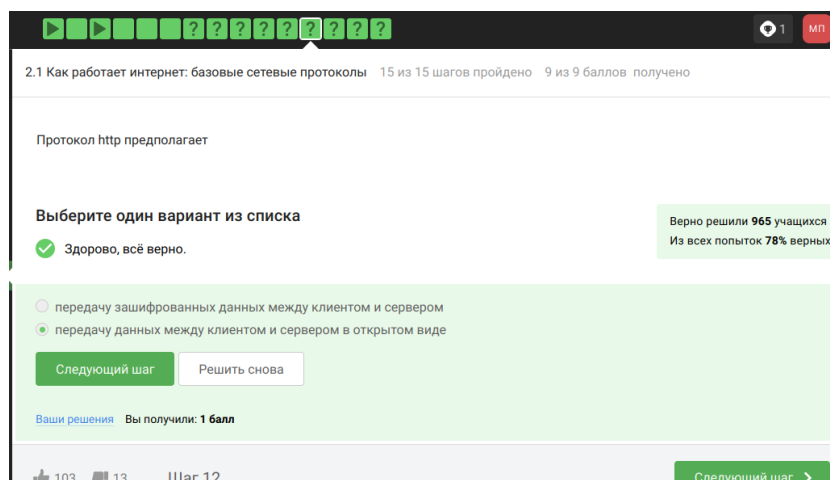


Рис. 2.6: нет названия

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

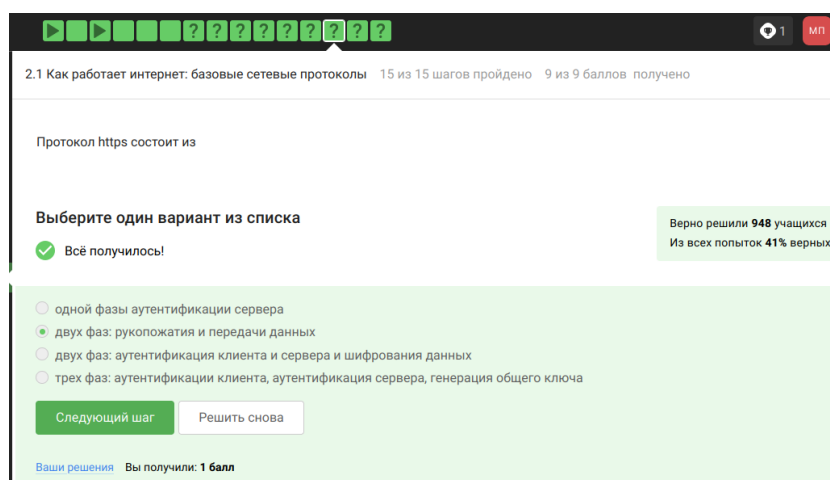


Рис. 2.7: нет названия

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

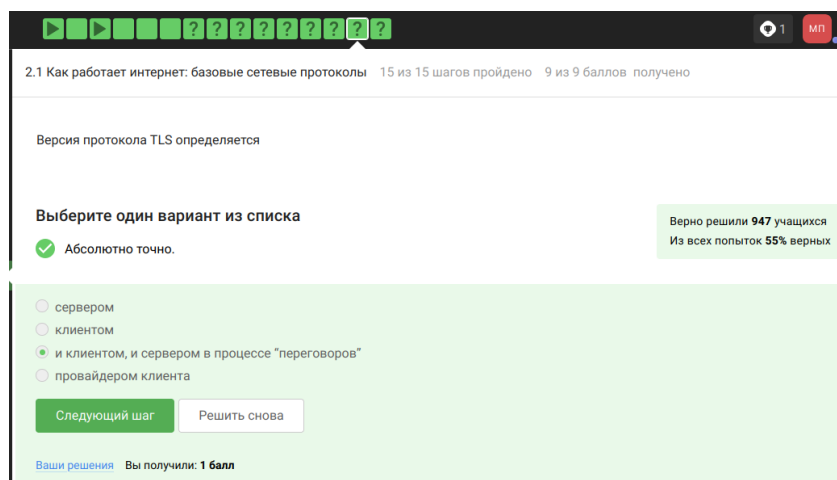


Рис. 2.8: нет названия

остальные варианты в протоколе предусмотрены

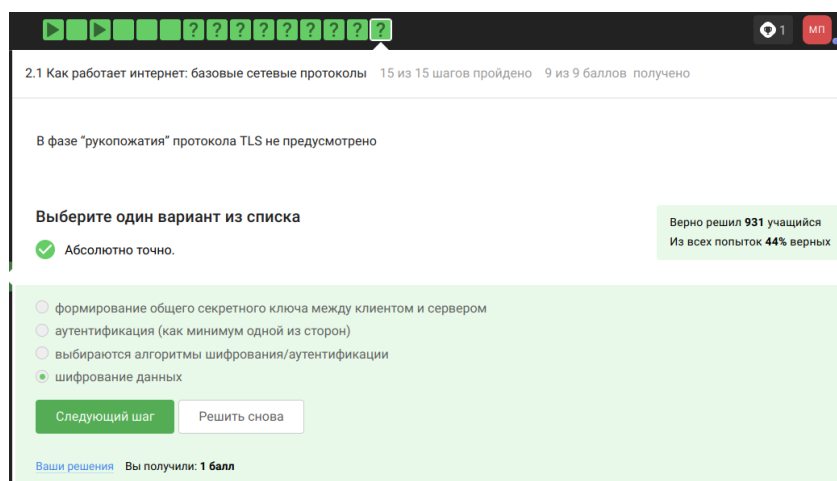


Рис. 2.9: нет названия

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

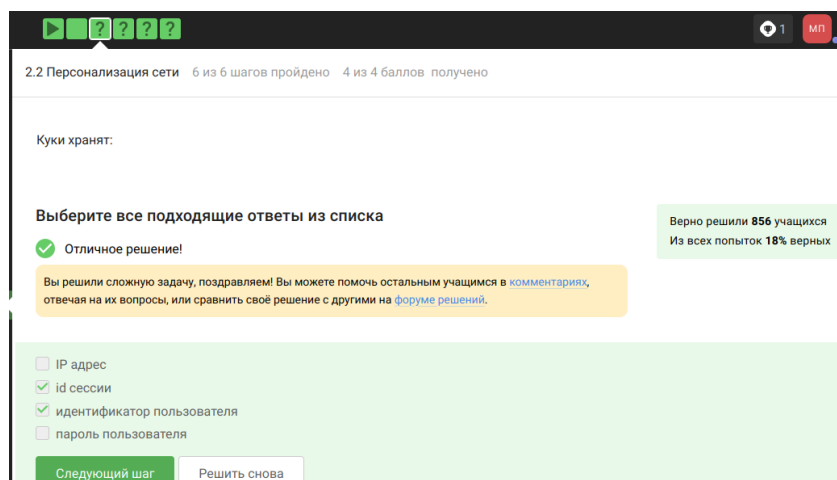


Рис. 2.10: нет названия

куки не делают соединение более надежным

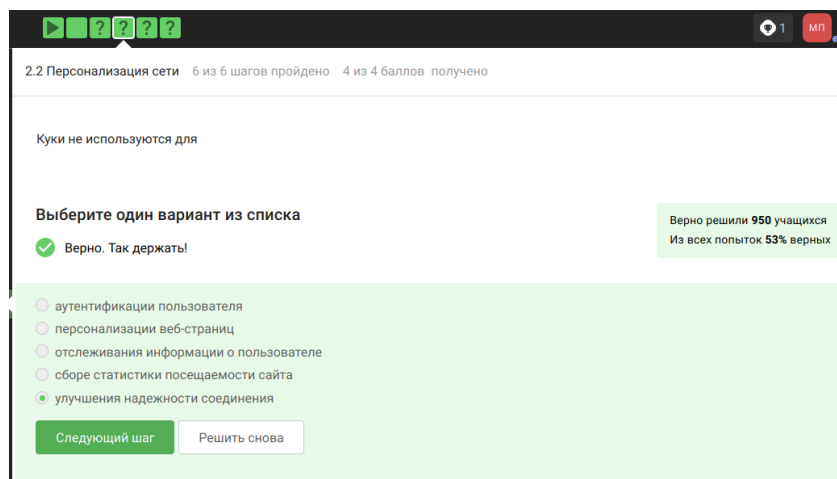


Рис. 2.11: нет названия

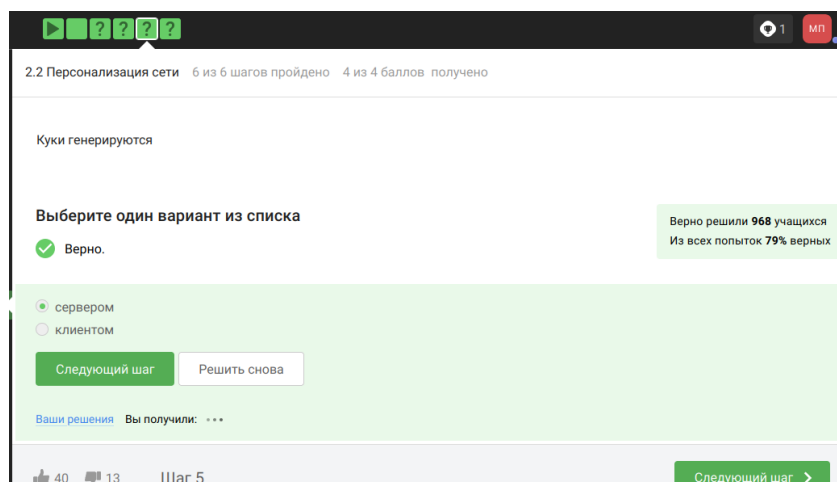


Рис. 2.12: нет названия

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

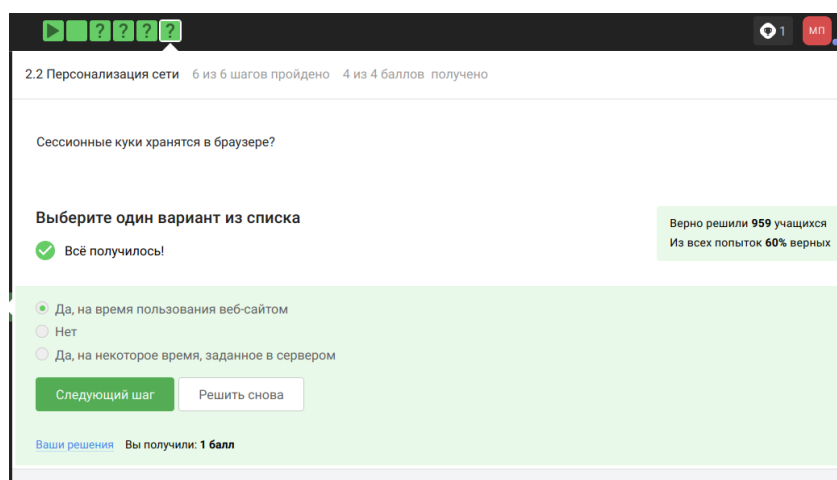


Рис. 2.13: нет названия

Необходимо три узла - входной, промежуточный и выходной

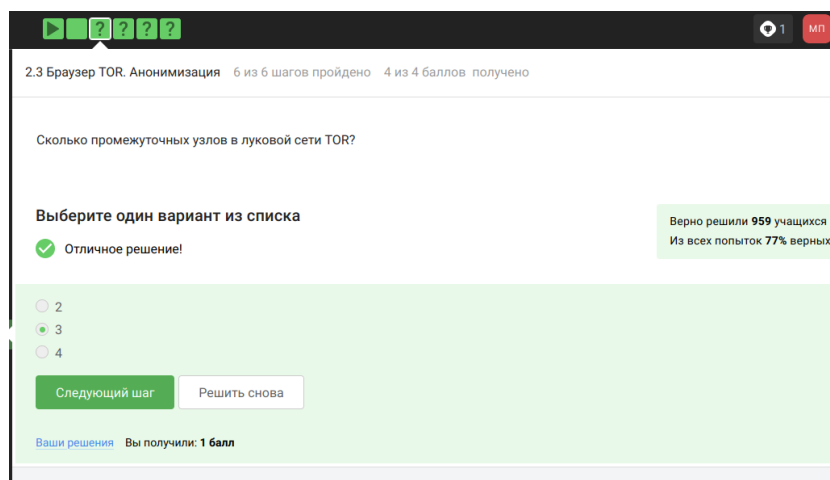


Рис. 2.14: нет названия

IP-адрес не должен быть известен охранному и промежуточному узлам

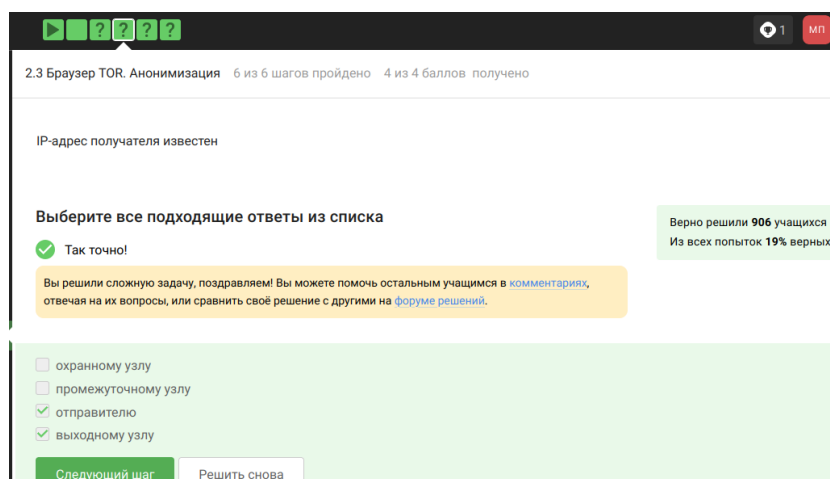


Рис. 2.15: нет названия

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

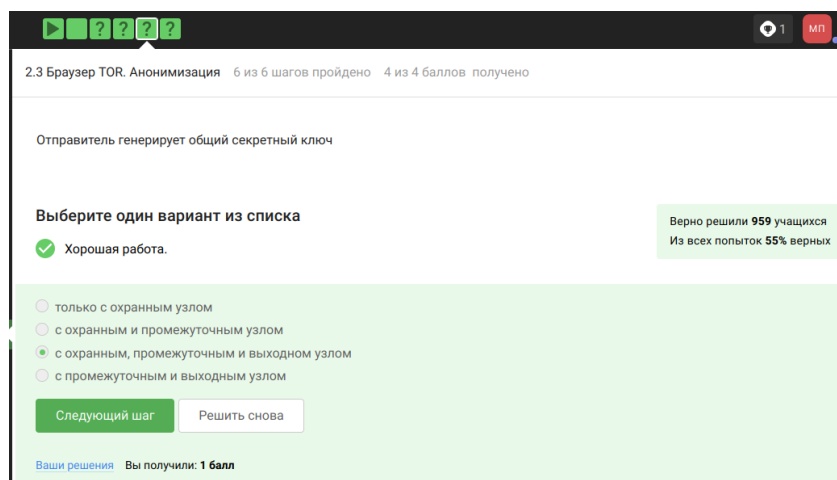


Рис. 2.16: нет названия

Для получения пакетов не нужно использовать TOR

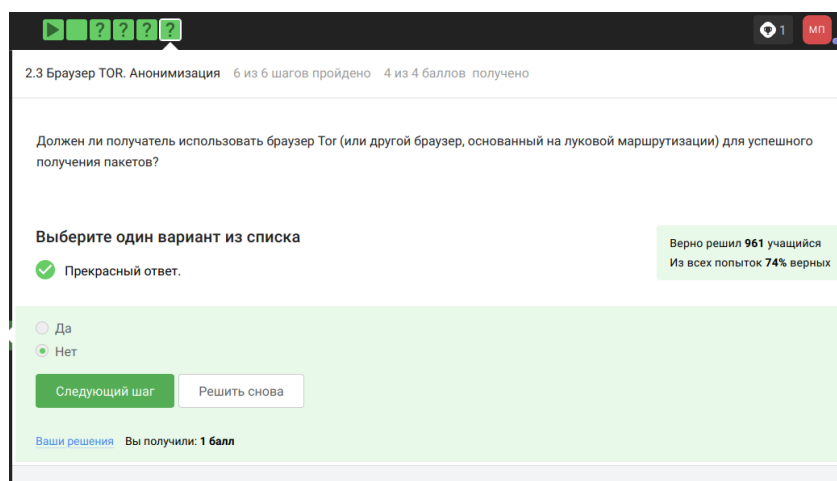


Рис. 2.17: нет названия

это определение Wi-Fi

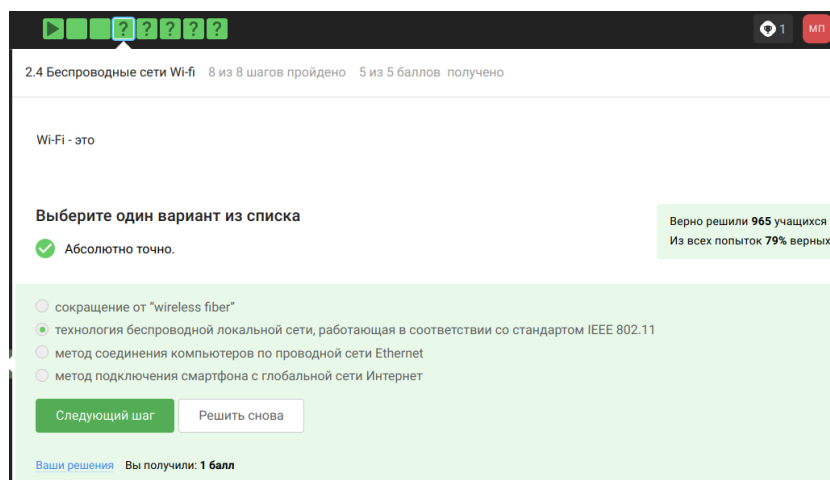


Рис. 2.18: нет названия

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

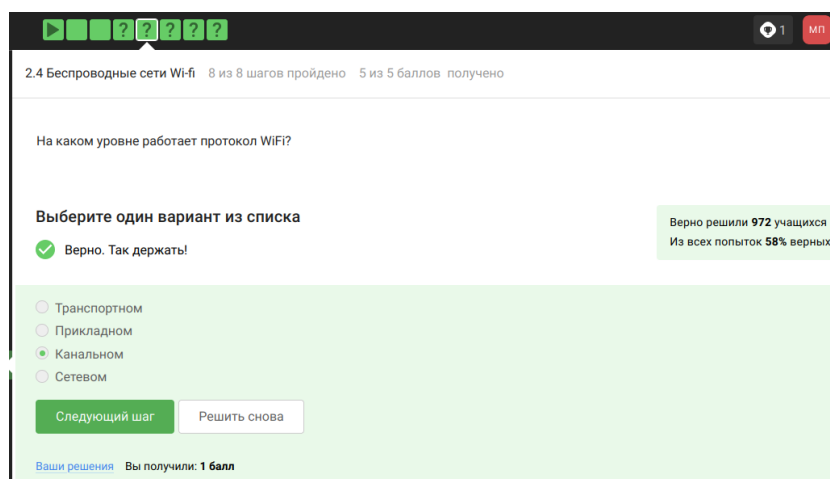


Рис. 2.19: нет названия

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

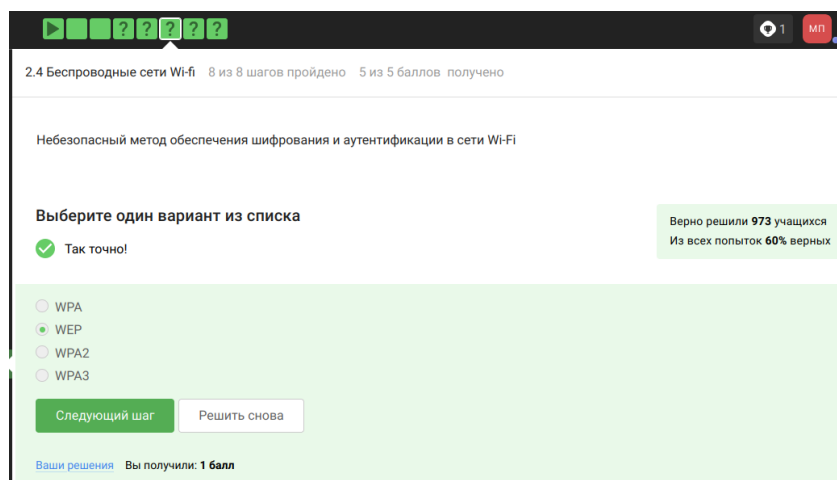


Рис. 2.20: нет названия

Нужно аутентифицировать устройства и позже передаются зашифрованные данные

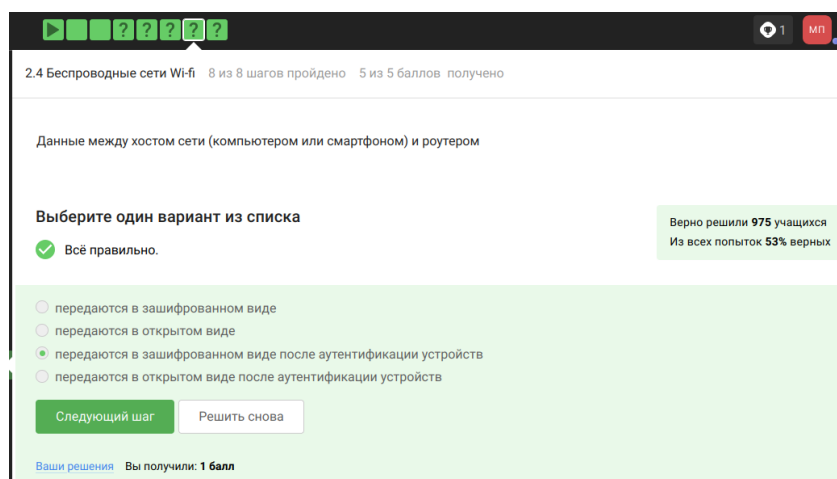


Рис. 2.21: нет названия

WPA2 Personal для личного использования

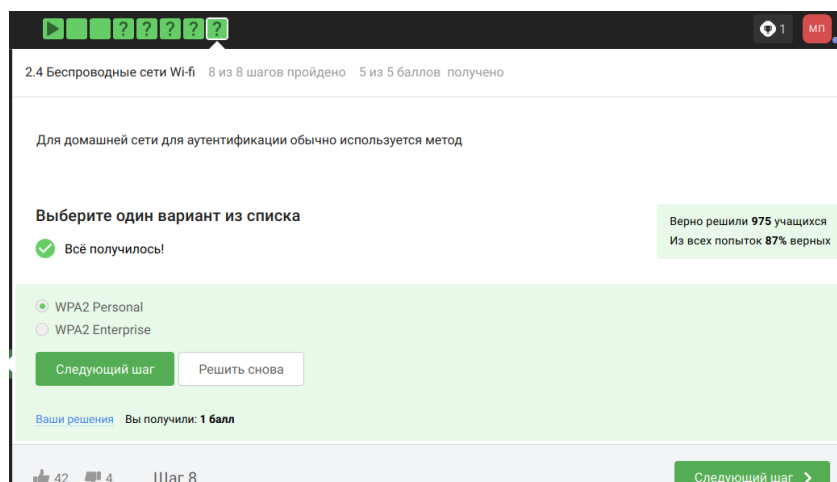


Рис. 2.22: нет названия

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

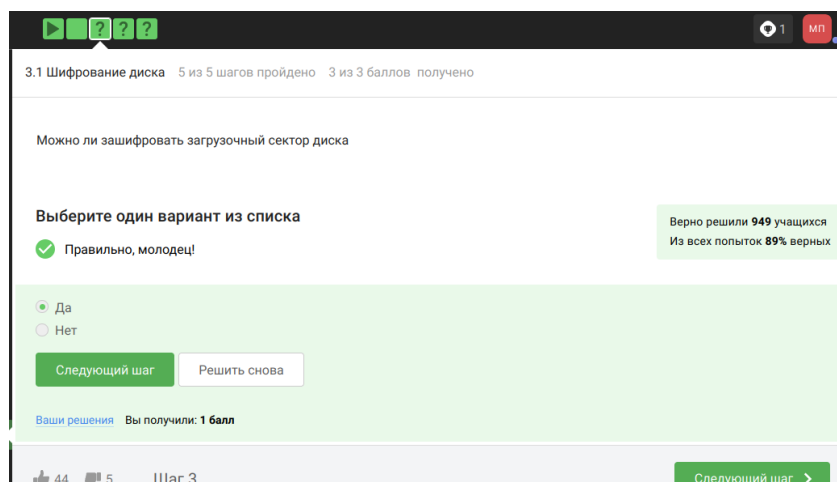


Рис. 2.23: нет названия

Шифрование диска основано на симметричном шифровании

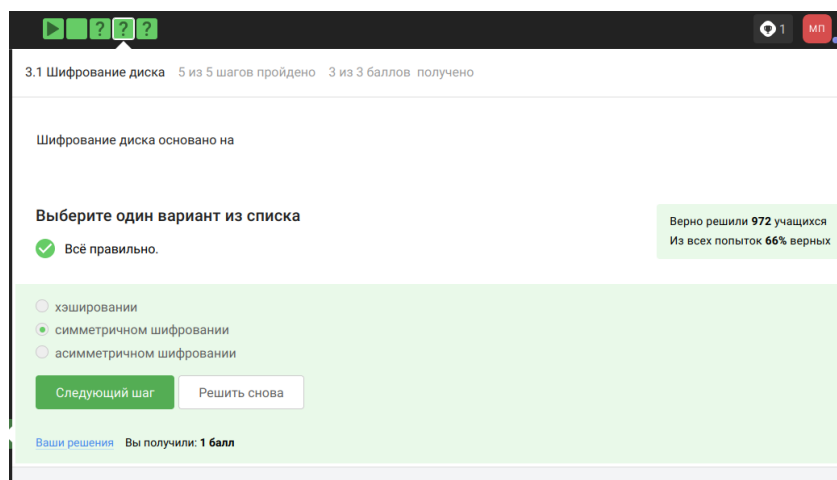


Рис. 2.24: нет названия

Отмечены программы, с помощью которых можно зашифровать жетский диск

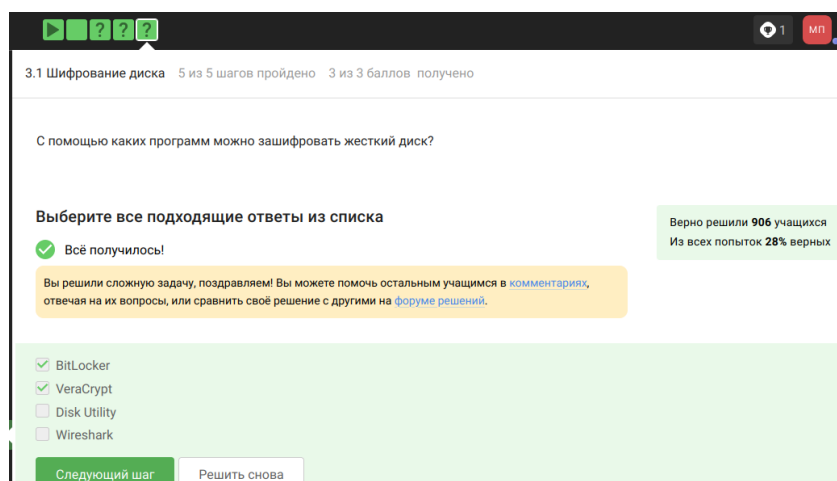


Рис. 2.25: нет названия

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

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 969 учащихся
Из всех попыток 85% верных

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQr9@j4!S\$
- ☐ IDONTLOVECATS

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.26: нет названия

Все варианты, кроме менеджера паролей, совершенно не надежные

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Отлично!

Верно решил 971 учащихся
Из всех попыток 74% верных

- ☒ В менеджерах паролей
- ☐ В заметках на рабочем столе
- ☐ В заметках в телефоне
- ☐ На стикере, приклеенном к монитору
- ☐ В кошельке

Следующий шаг Решить снова

Рис. 2.27: нет названия

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

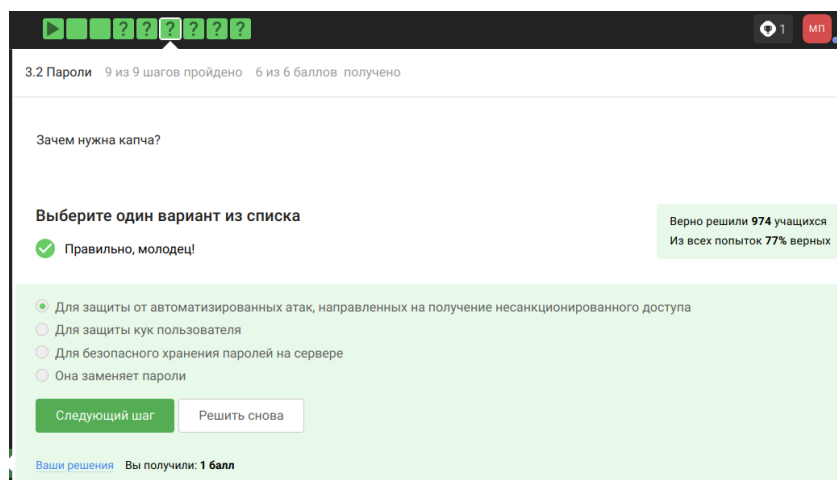


Рис. 2.28: нет названия

Опасно хранить пароли в открытом виде, поэтому хранят их хэши

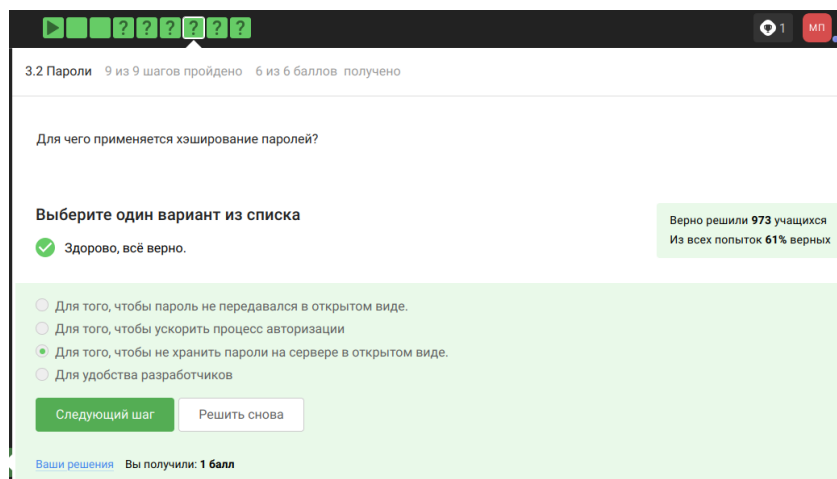


Рис. 2.29: нет названия

Соль не поможет

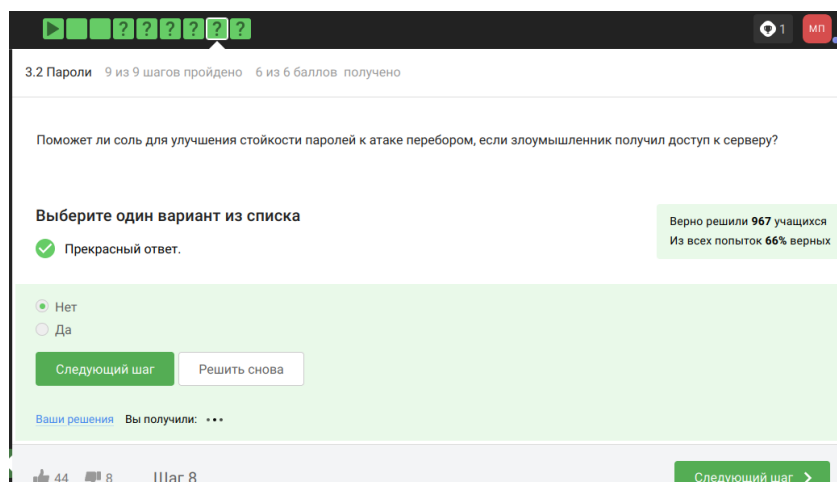


Рис. 2.30: нет названия

Все приведенные меры защищают от утечек данных

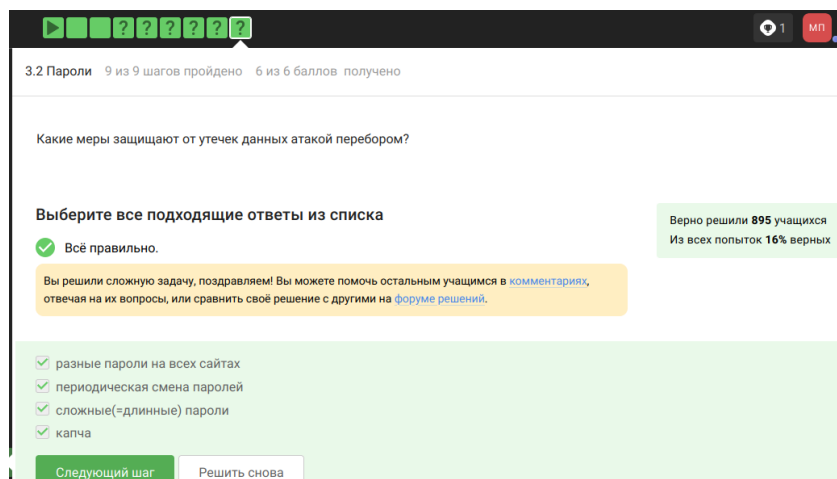


Рис. 2.31: нет названия

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

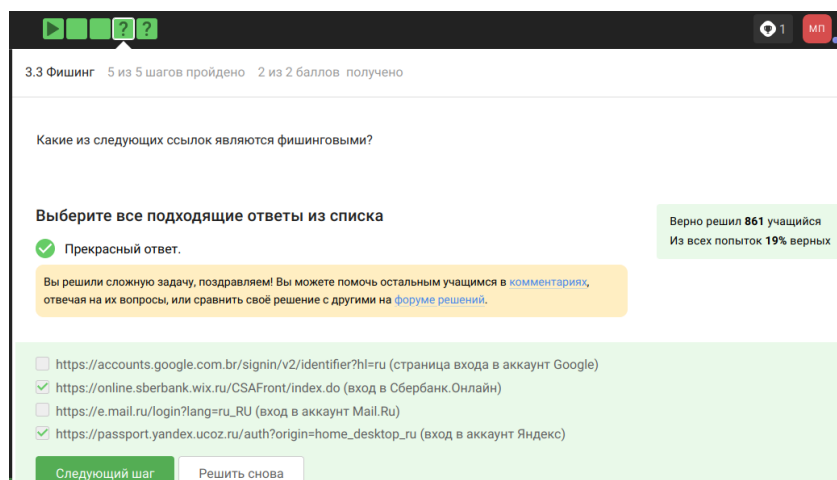


Рис. 2.32: нет названия

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

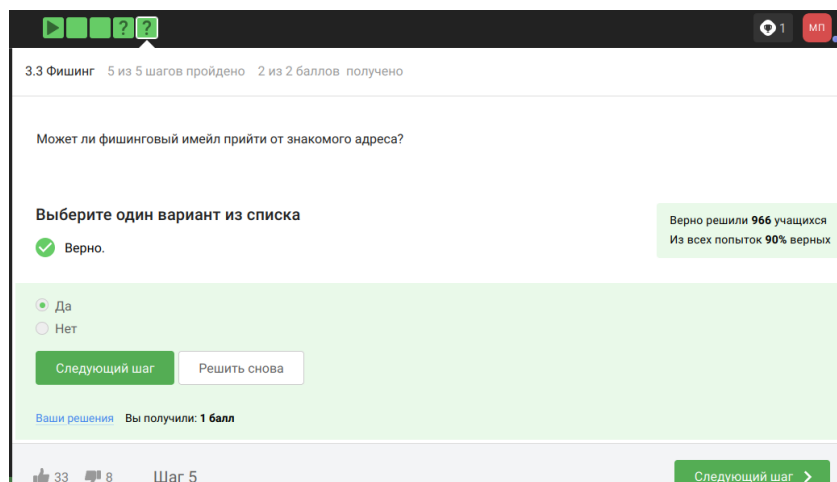


Рис. 2.33: нет названия

Ответ дан в соответствии с определением

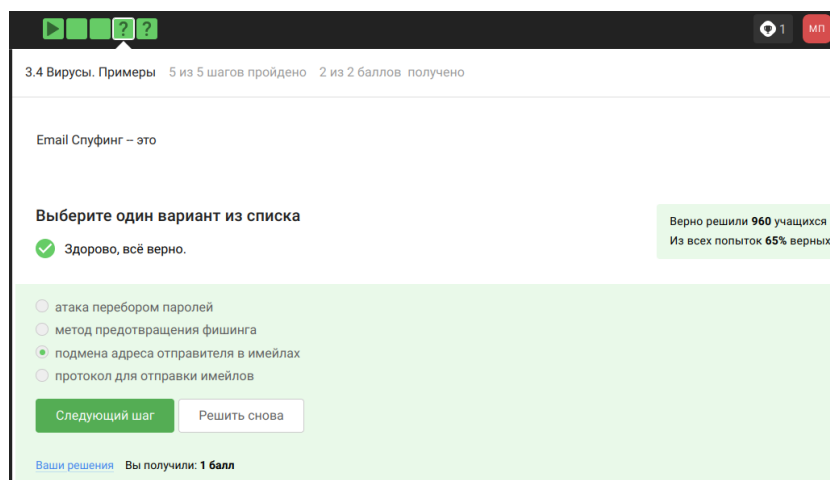


Рис. 2.34: нет названия

Троян маскируется под обычную программу

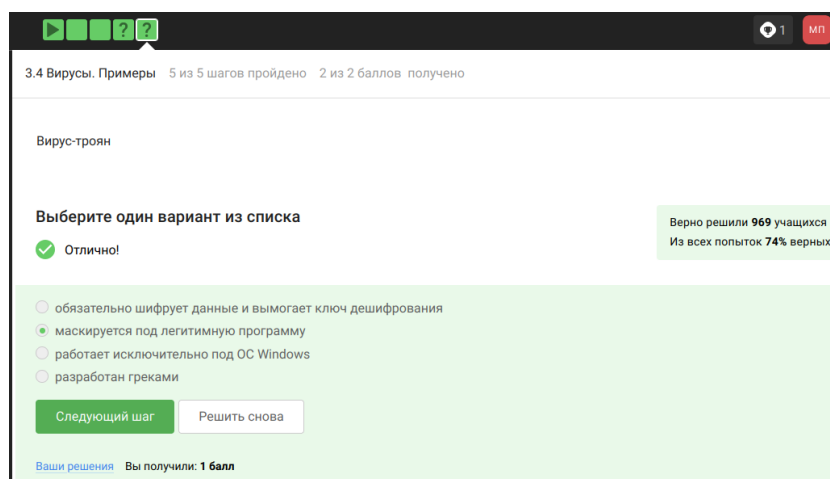


Рис. 2.35: нет названия

При установке первого сообщения отправителем формируется ключ шифрования

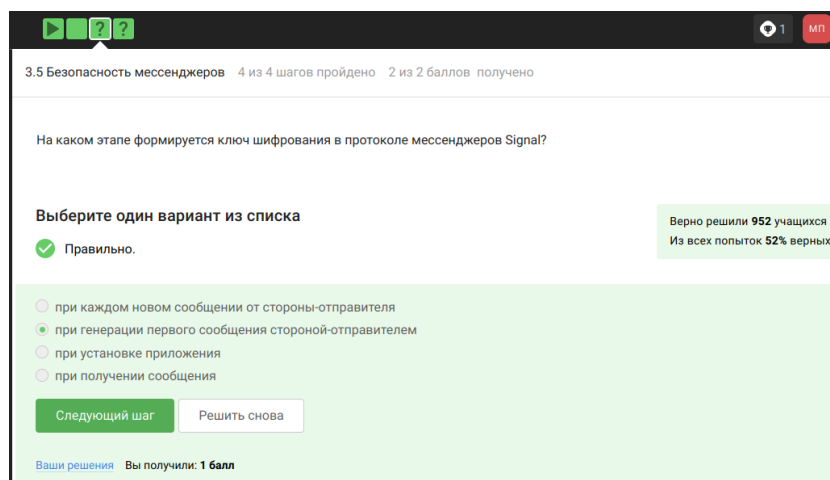


Рис. 2.36: нет названия

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

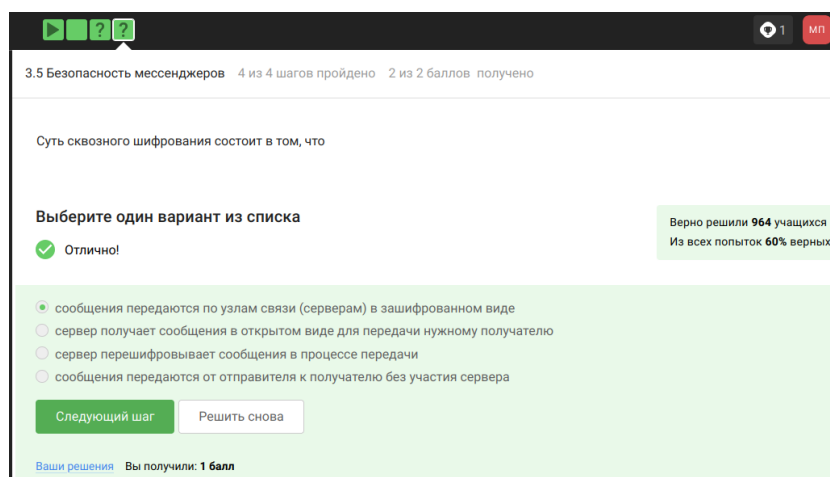


Рис. 2.37: нет названия

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами

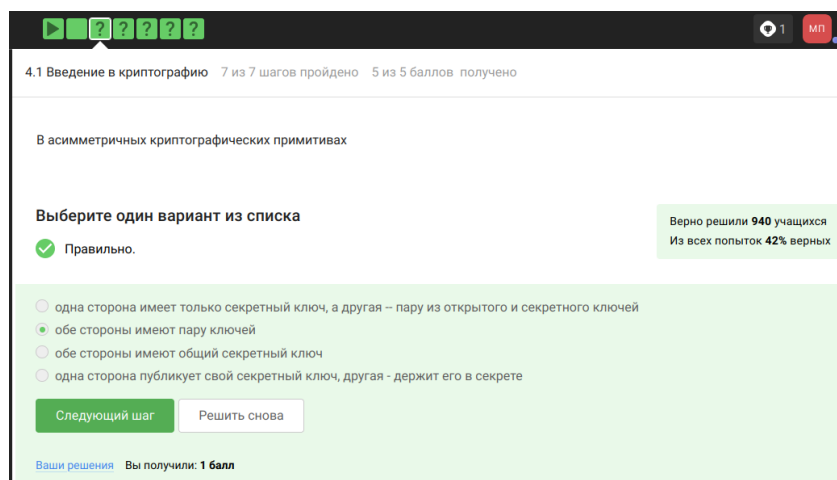


Рис. 2.38: нет названия

Отмечены основные условия для криптографической хэш-функции

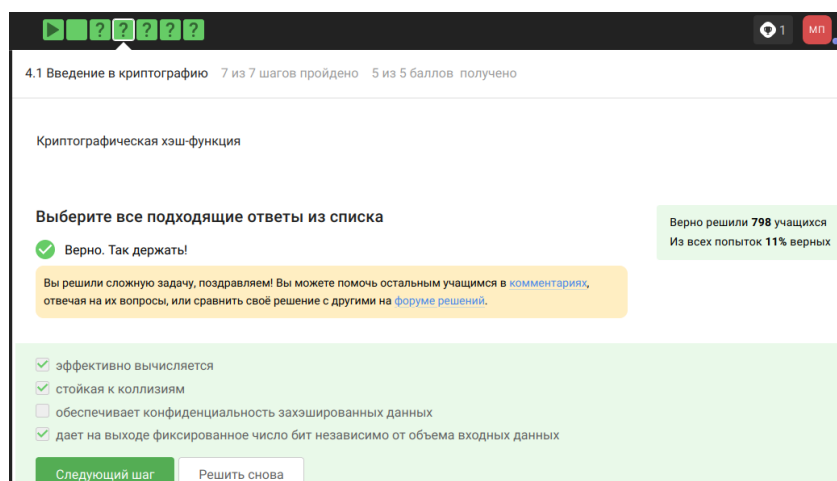


Рис. 2.39: нет названия

Отмечены алгоритмы цифровой подписи

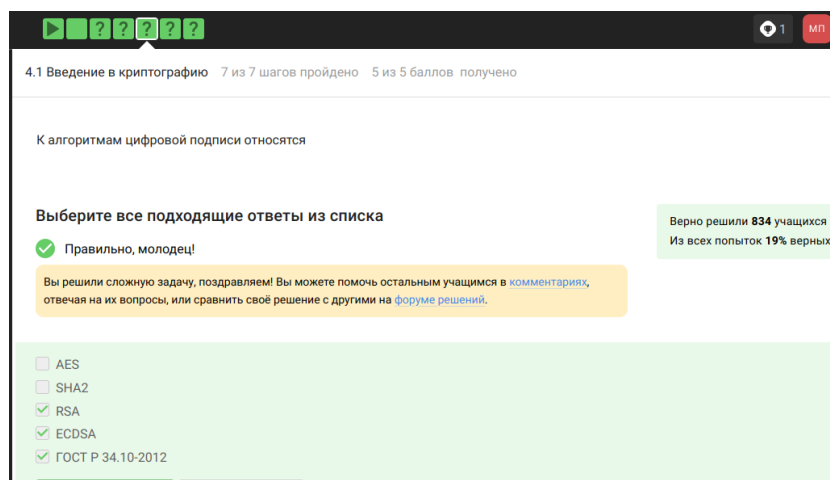


Рис. 2.40: нет названия

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

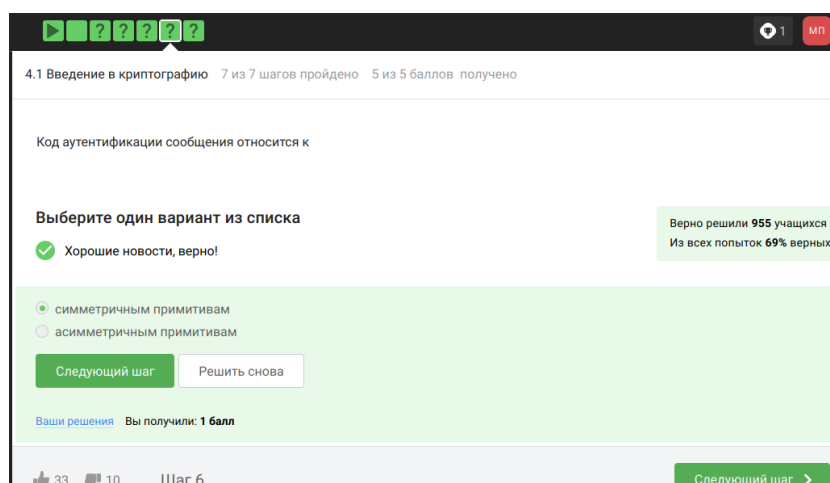


Рис. 2.41: нет названия

Определение обмена ключами Диффи-Хэллмана.

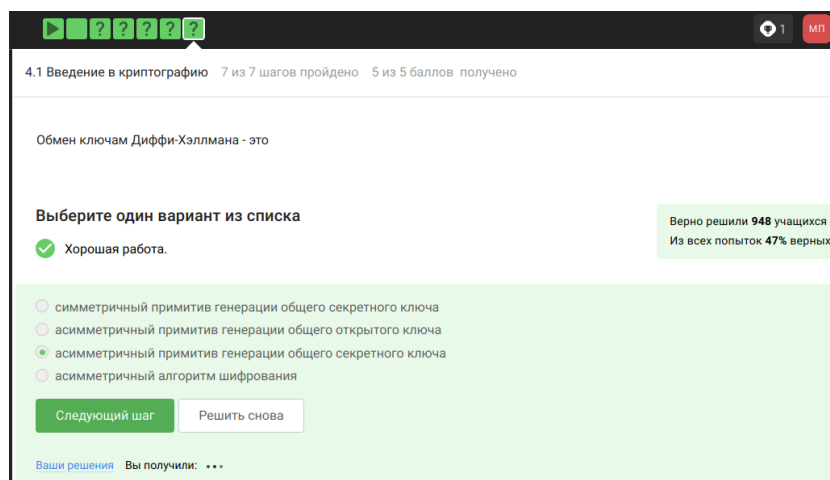


Рис. 2.42: нет названия

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

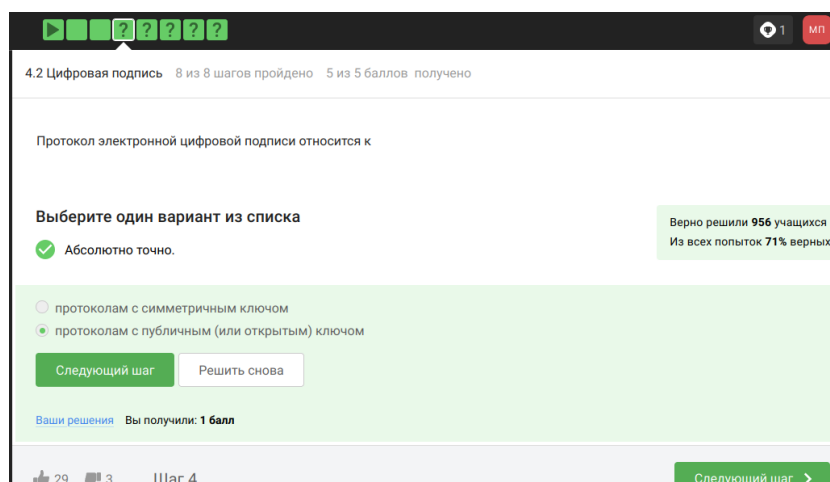


Рис. 2.43: нет названия

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

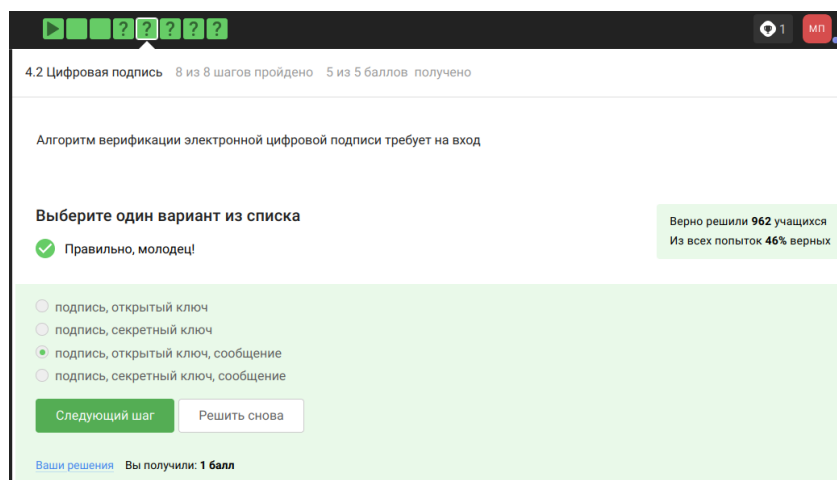


Рис. 2.44: нет названия

Электронная подпись обеспечивает все указанное, кроме конфиденциально-

СТИ

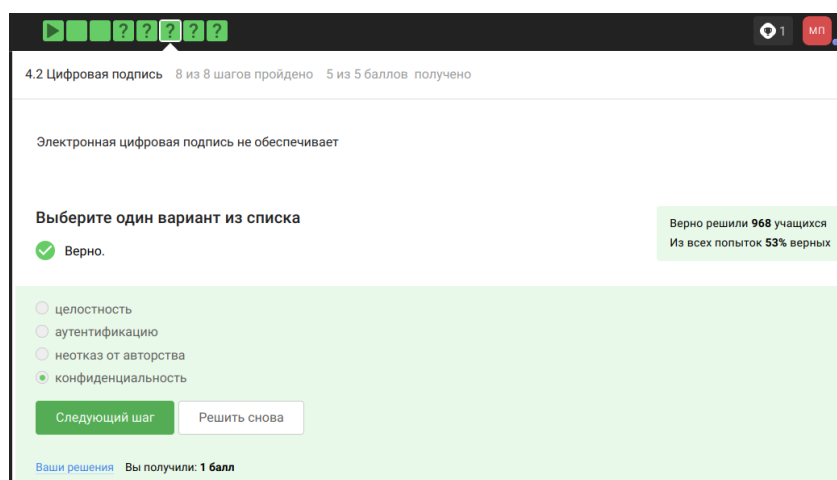


Рис. 2.45: нет названия

Для отправки налоговой отчетности в ФНС используется усиленная квалифи-

цированная электронная подпись

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

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

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 975 учащихся
Из всех попыток 68% верных

- ☐ усиленная неквалифицированная
- ☒ усиленная квалифицированная
- ☐ простая

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.46: нет названия

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант из списка

✓ Прекрасный ответ.

Верно решил 971 учащихся
Из всех попыток 61% верных

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Следующий шаг Решить снова

Ваши решения Вы получили: ...

Рис. 2.47: нет названия

Известные платежные системы - Visa, MasterCard, МИР

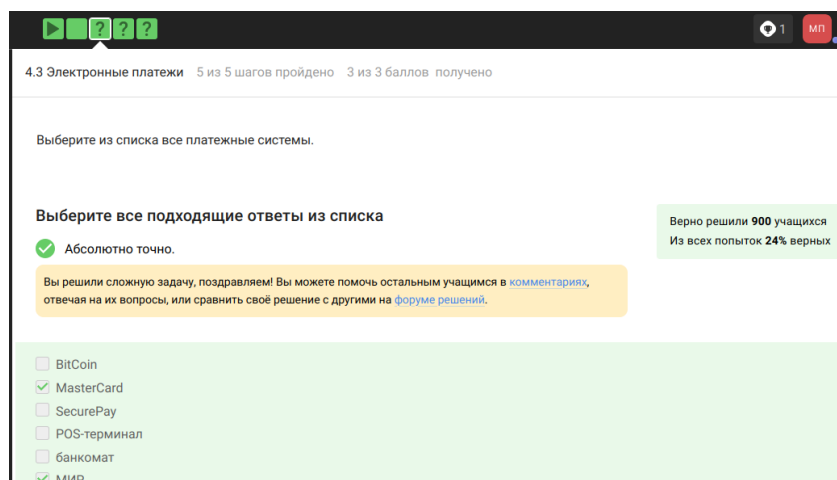


Рис. 2.48: нет названия

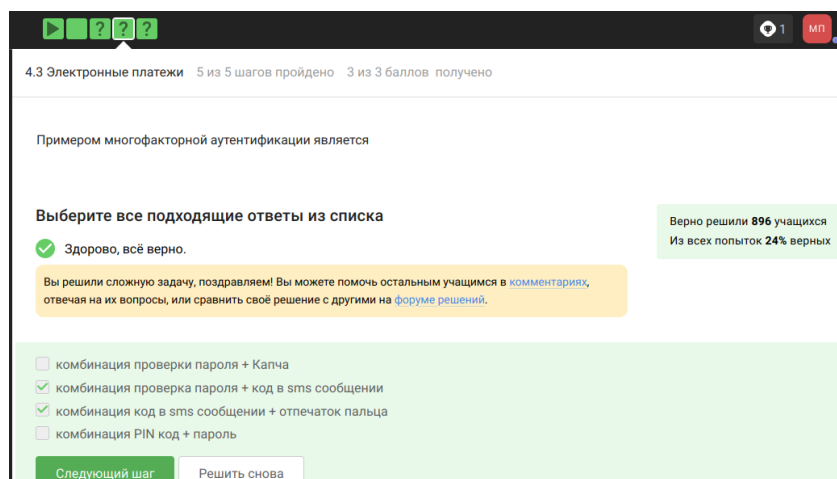


Рис. 2.49: нет названия

При онлайн платежах используется многофакторная аутентификация

4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено

При онлайн платежах сегодня используется

Выберите один вариант из списка

✓ Правильно.

Верно решили 957 учащихся
Из всех попыток 59% верных

- ☒ многофакторная аутентификация покупателя перед банком-эмитентом
- ☐ однофакторная аутентификация покупателя перед банком-эквайером
- ☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом
- ☐ многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.50: нет названия

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

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓ Хорошая работа.

Верно решили 932 учащихся
Из всех попыток 49% верных

- ☐ фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ эффективность вычисления

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2.51: нет названия

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

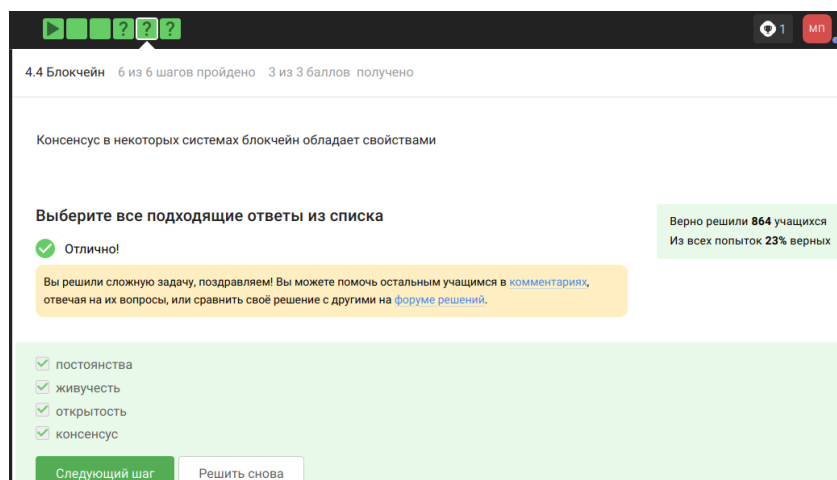


Рис. 2.52: нет названия

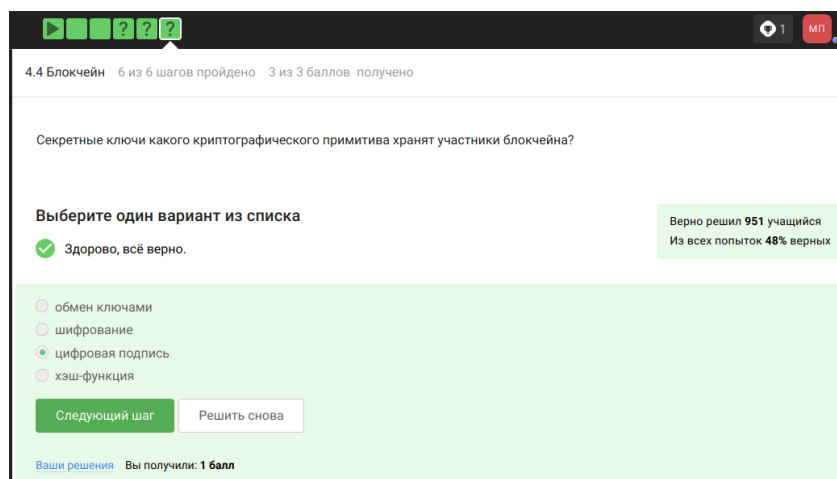


Рис. 2.53: нет названия

Прошла курс на степике



Основы кибербезопасности

100% материалов пройдено

53/53 баллов получено

Описание

Содержание

Новости

Комментарии

Отзывы

Рис. 2.54: нет названия

3 Выводы

Прошла курс на степике

Список литературы