Внешний курс на Stepik

Основы кибербезопасности

Хватов Максим Григорьевич

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

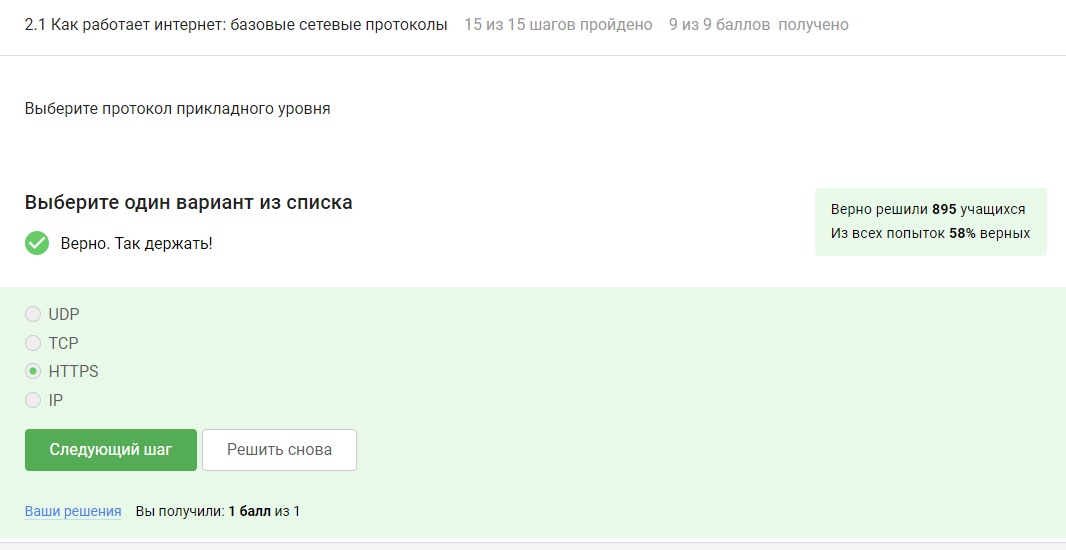


Рис. 1

На каком уровне работает протокол TCP?: транспортном

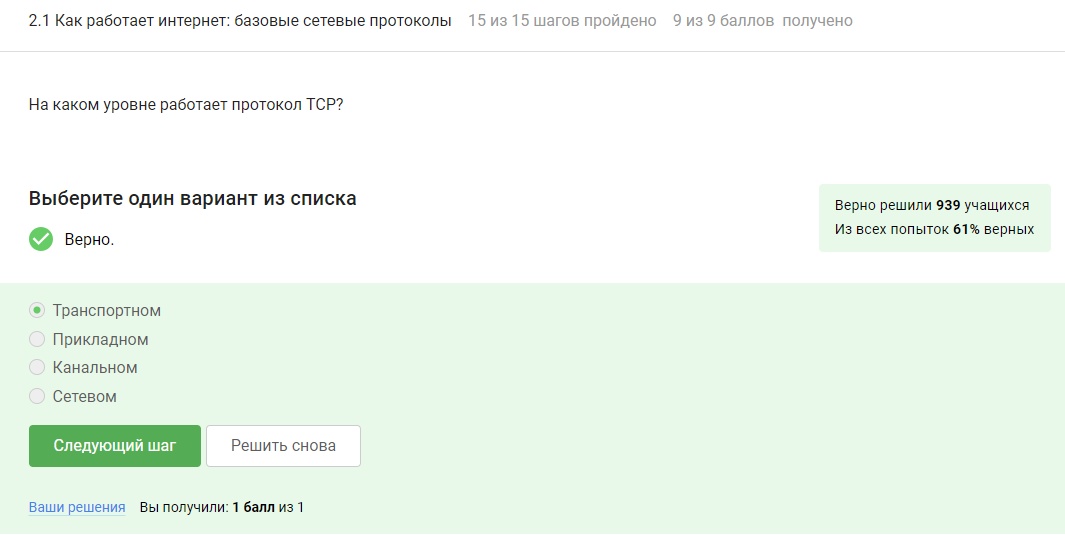


Рис. 2

Выберите все корректные адреса IPv4: 90.11.90.22, 25.198.0.15

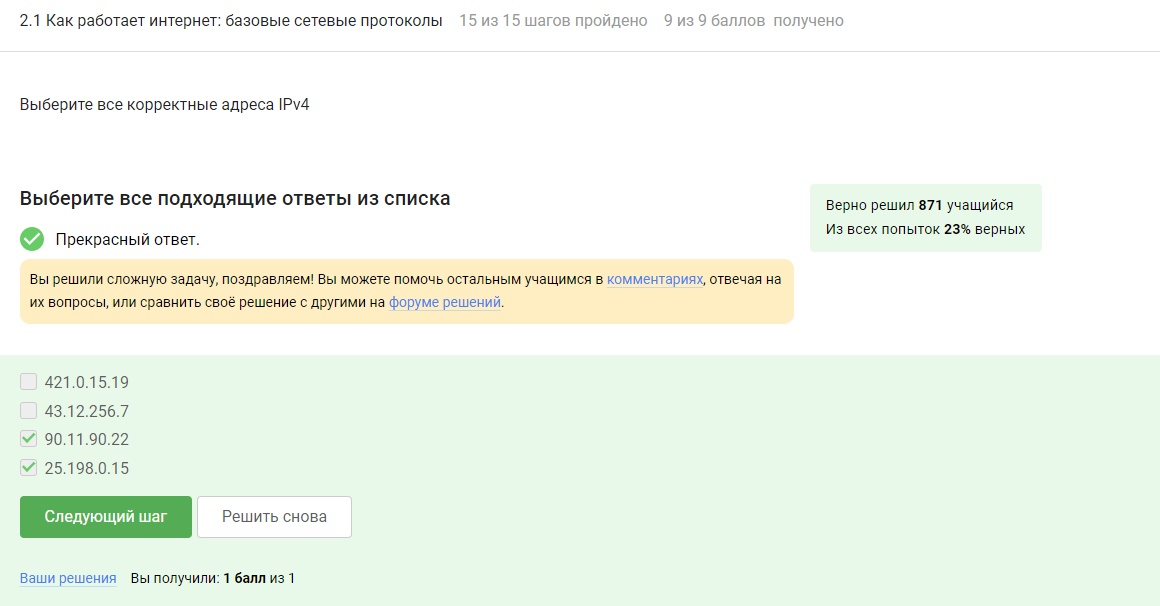


Рис. 3

DNS сервер: сопоставляет IP адреса доменным именам

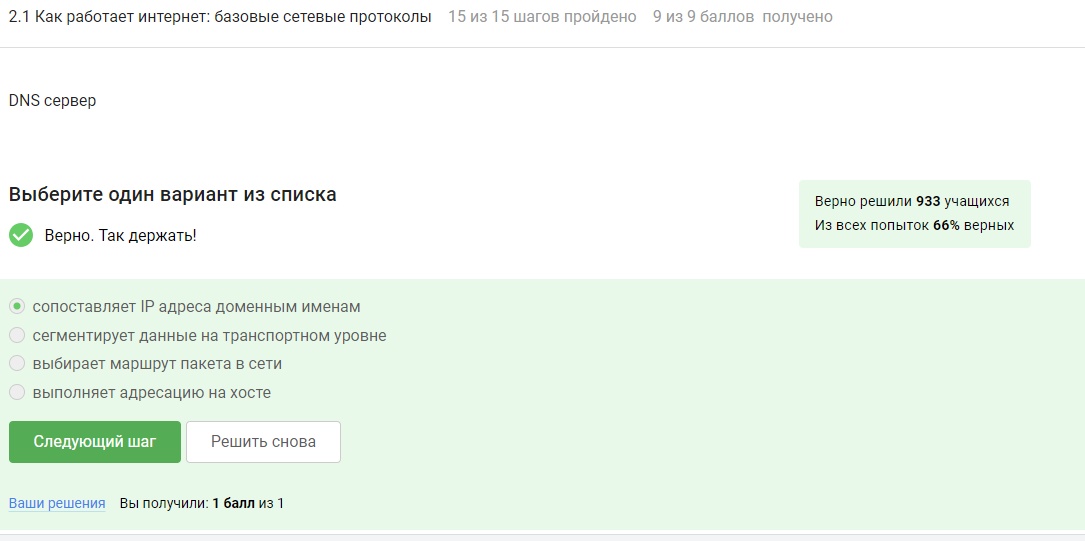


Рис. 4

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

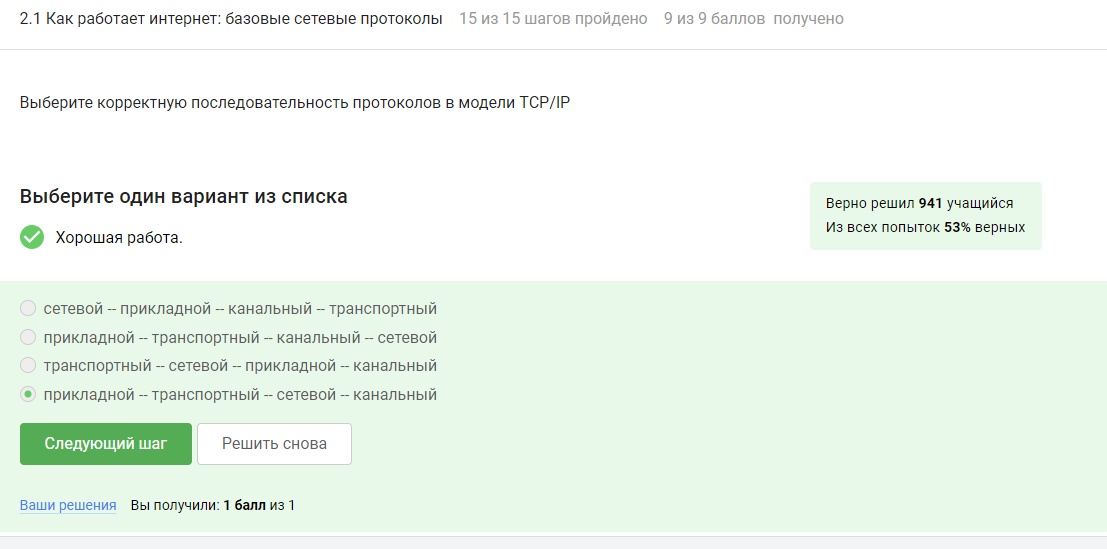


Рис. 5

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

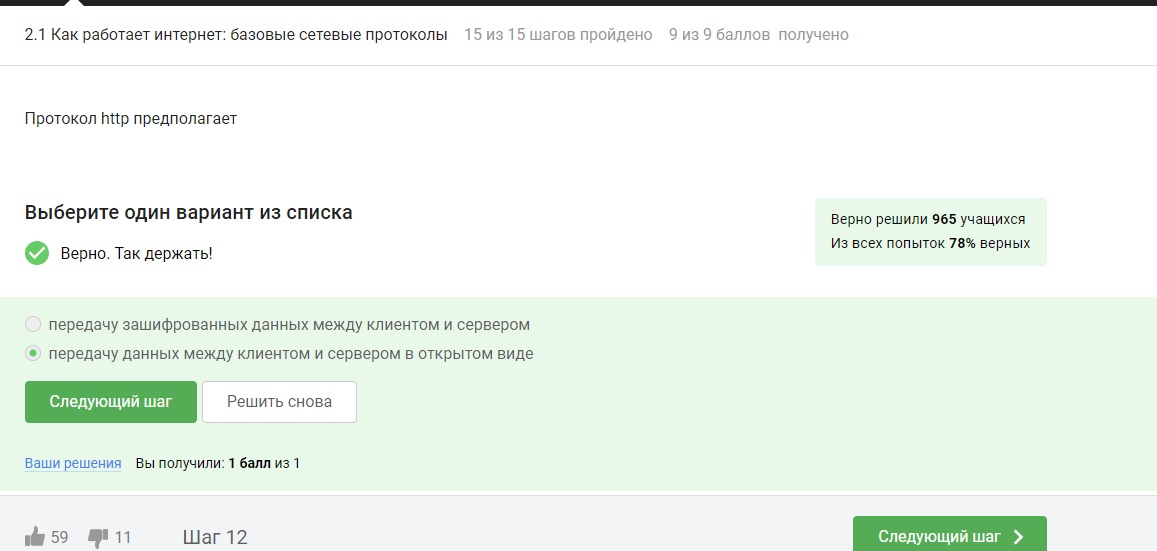


Рис. 6

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

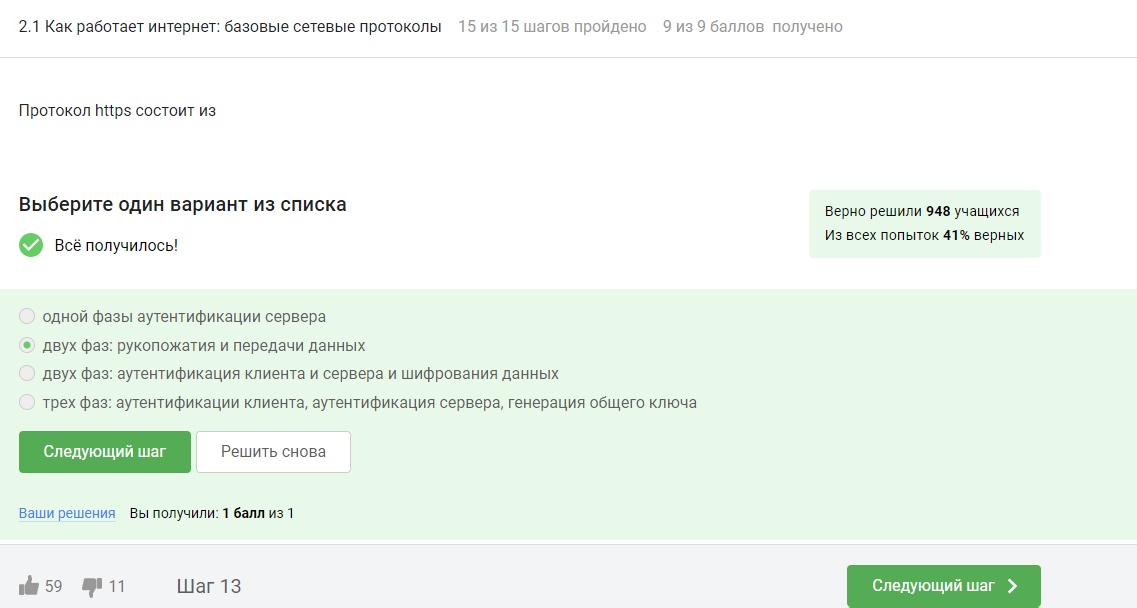


Рис. 7

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

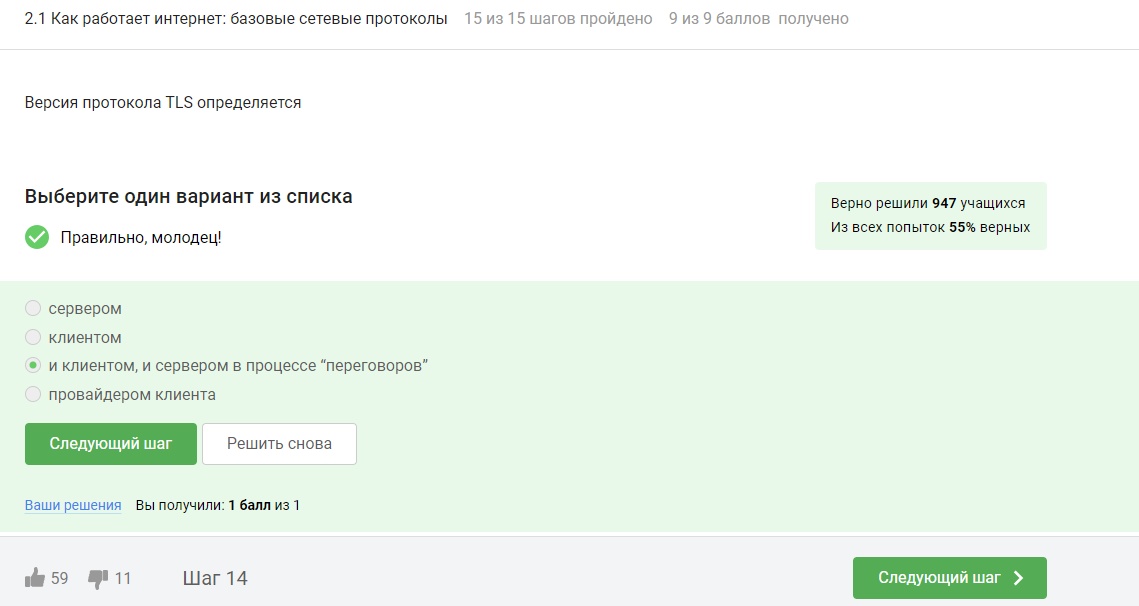


Рис. 8

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

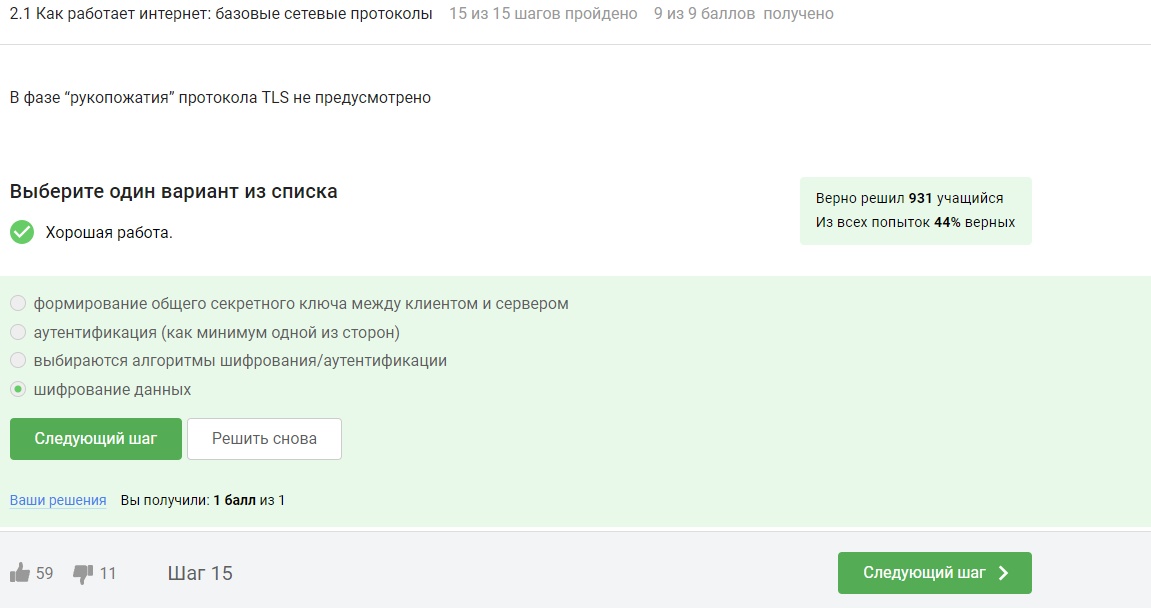


Рис. 9

# 3 Раздел 2.2

Куки хранят: id сессии, идентификатор пользователя

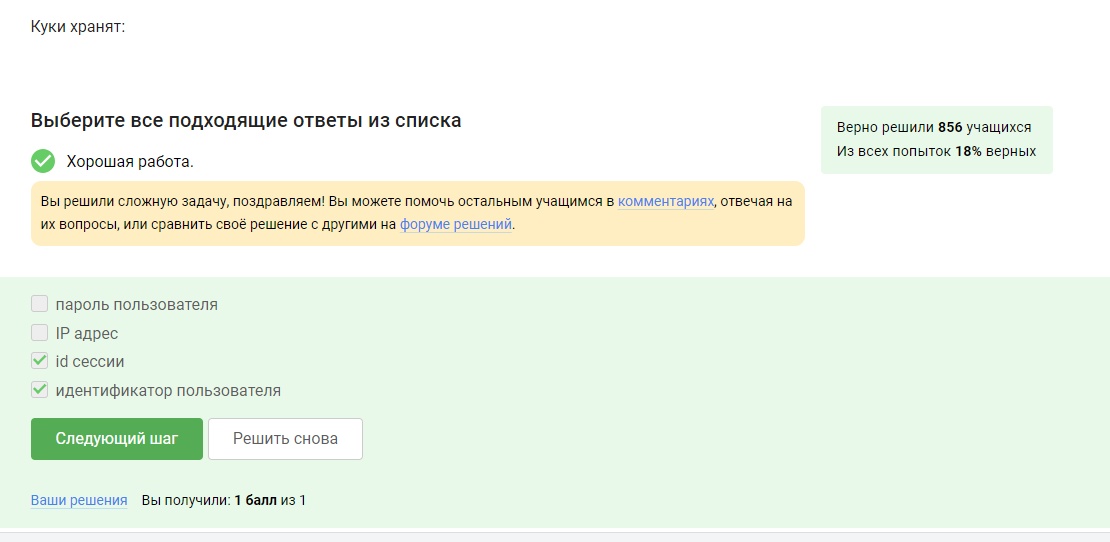


Рис. 1

Куки не используются для: улучшения надежности соединения

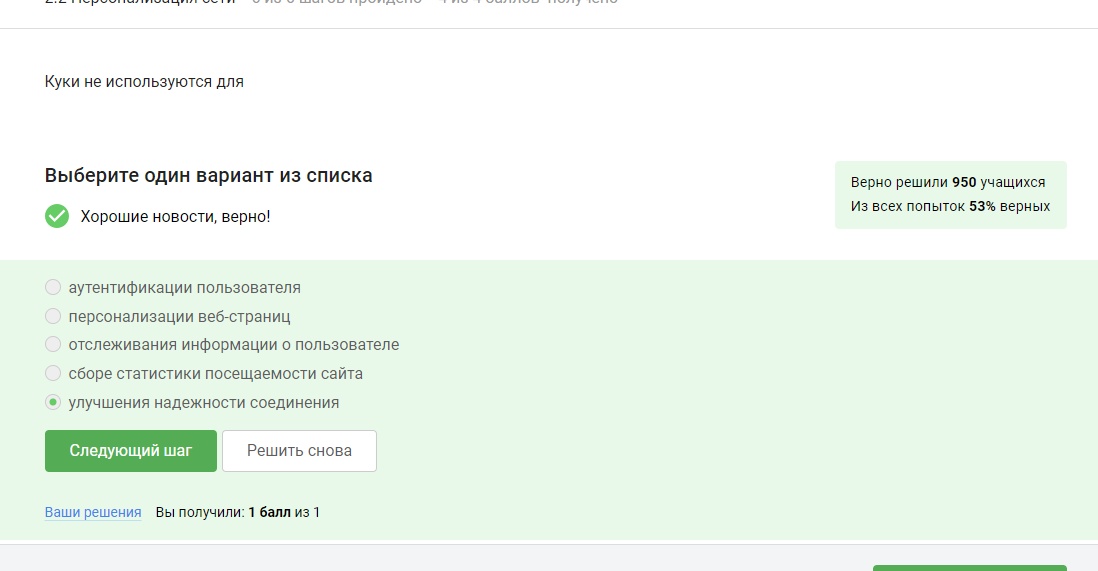


Рис. 2

Куки генерируются: сервером

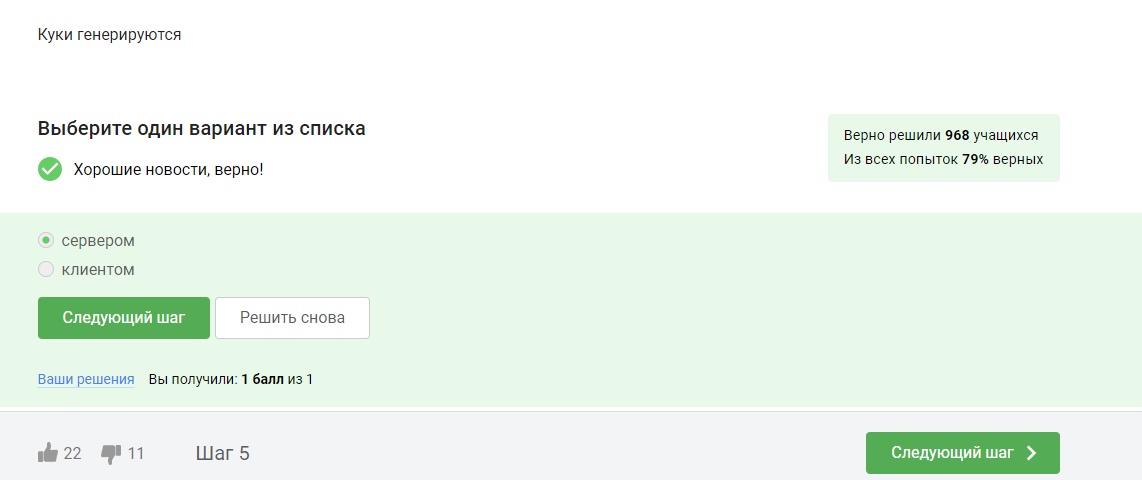


Рис. 3

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

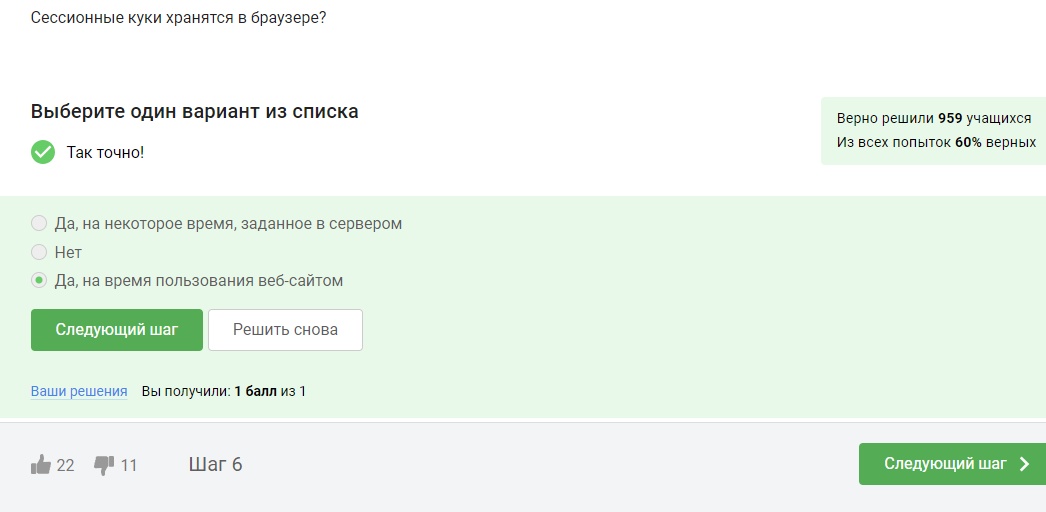


Рис. 4

# 4 Раздел 2.3

Сколько промежуточных узлов в луковой сети TOR? 3

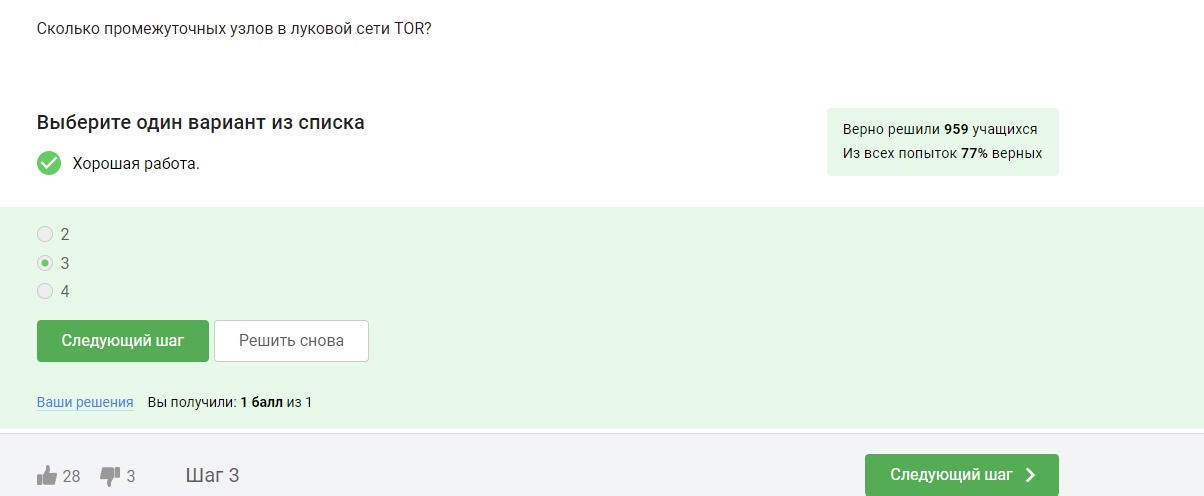


Рис. 1

IP-адрес получателя известен: отправителю, выходному узлу

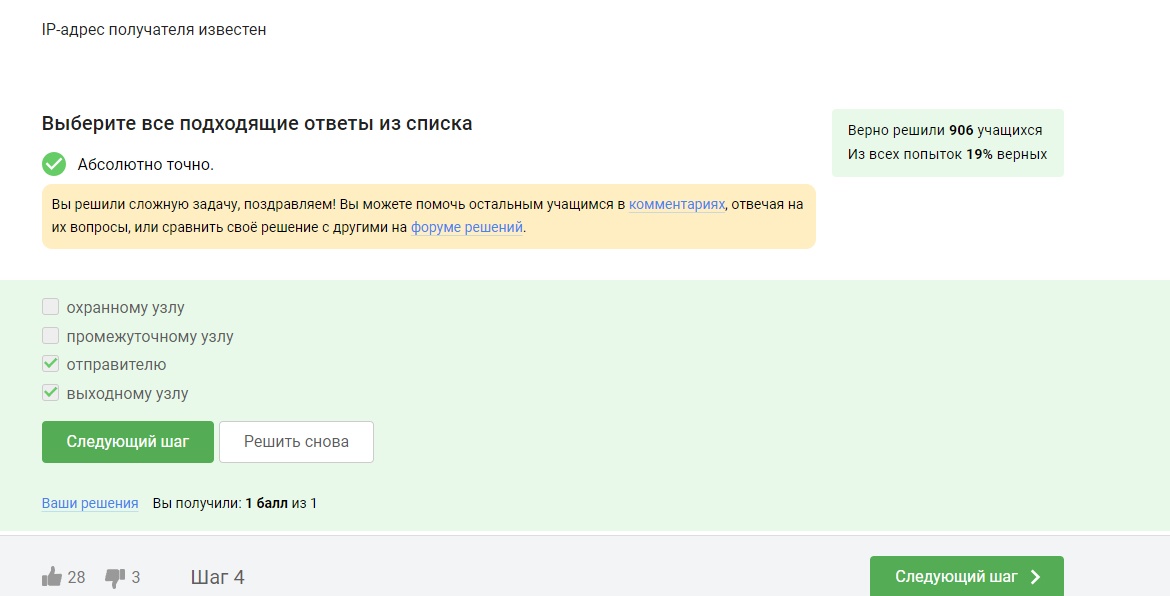


Рис. 2

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

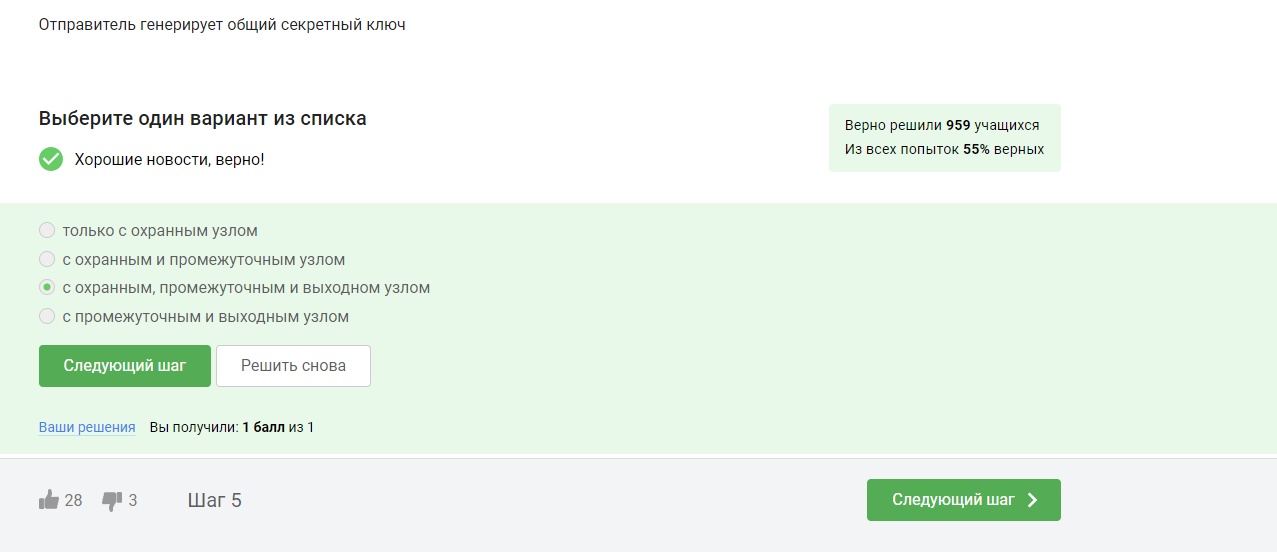


Рис. 3

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

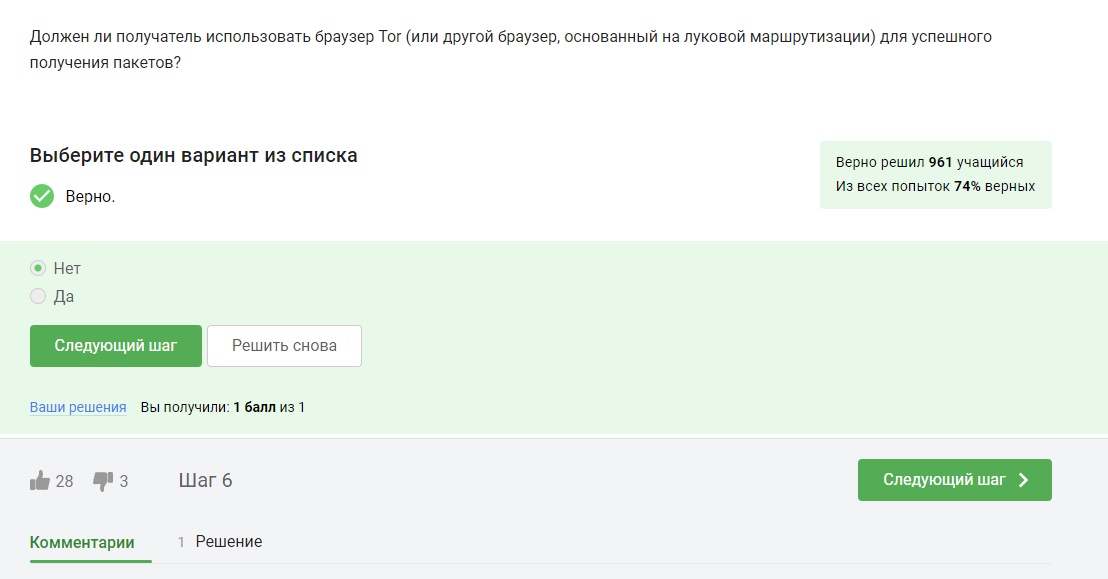


Рис. 4

# 5 Раздел 2.4

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

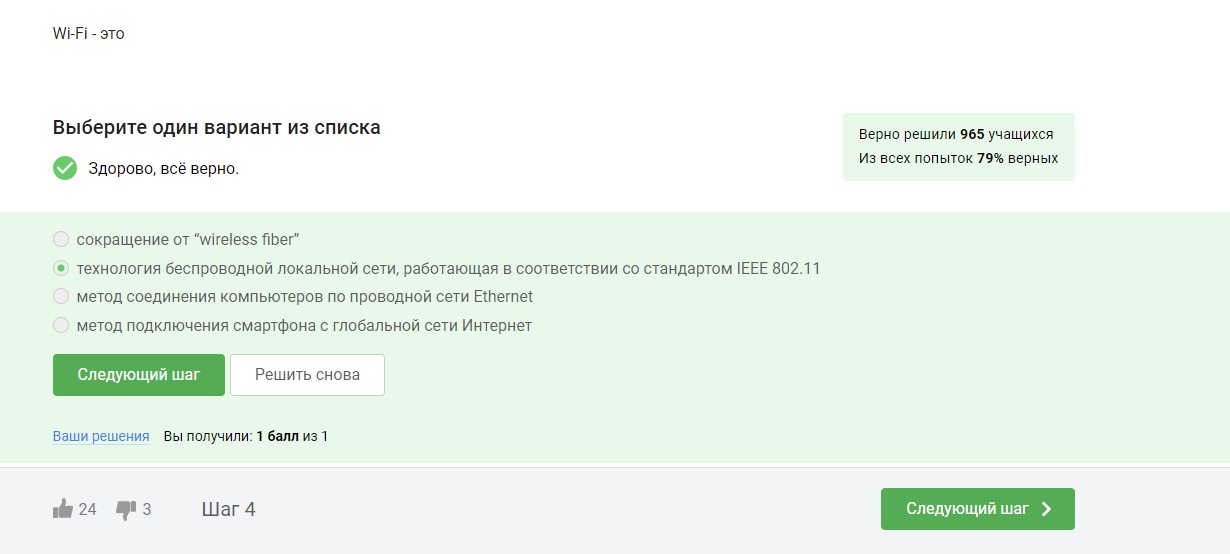


Рис. 1

На каком уровне работает протокол WiFi? Канальном

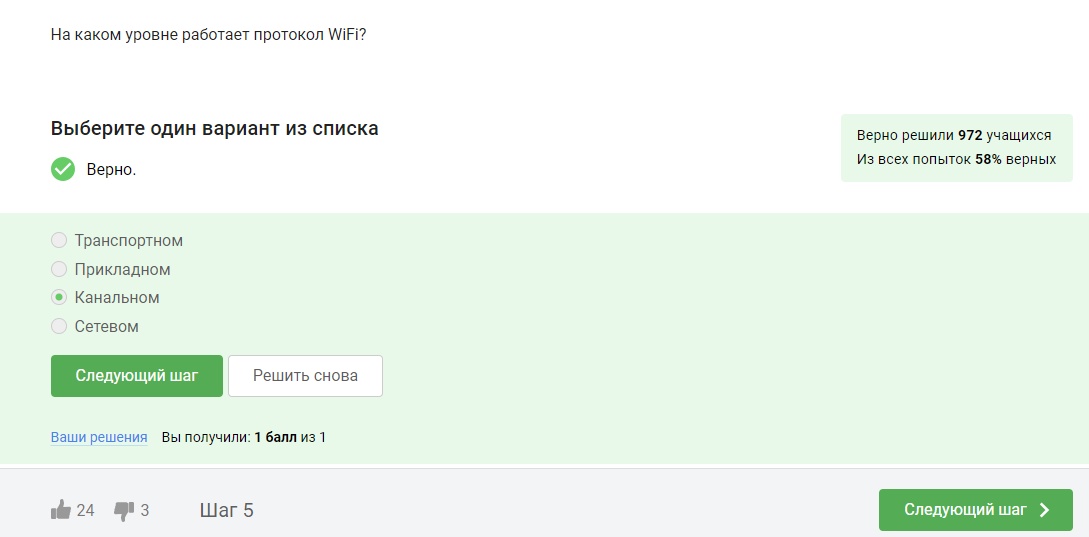


Рис. 2

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

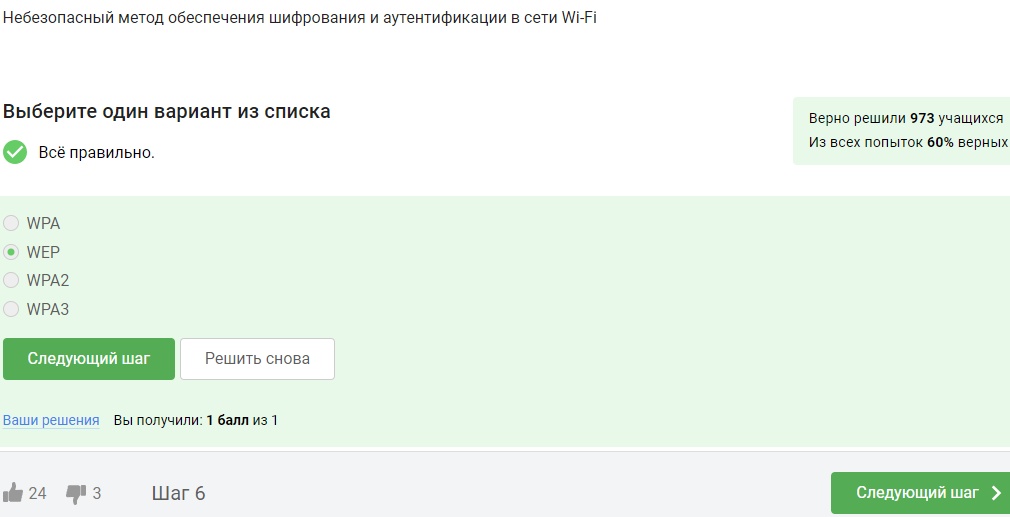


Рис. 3

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

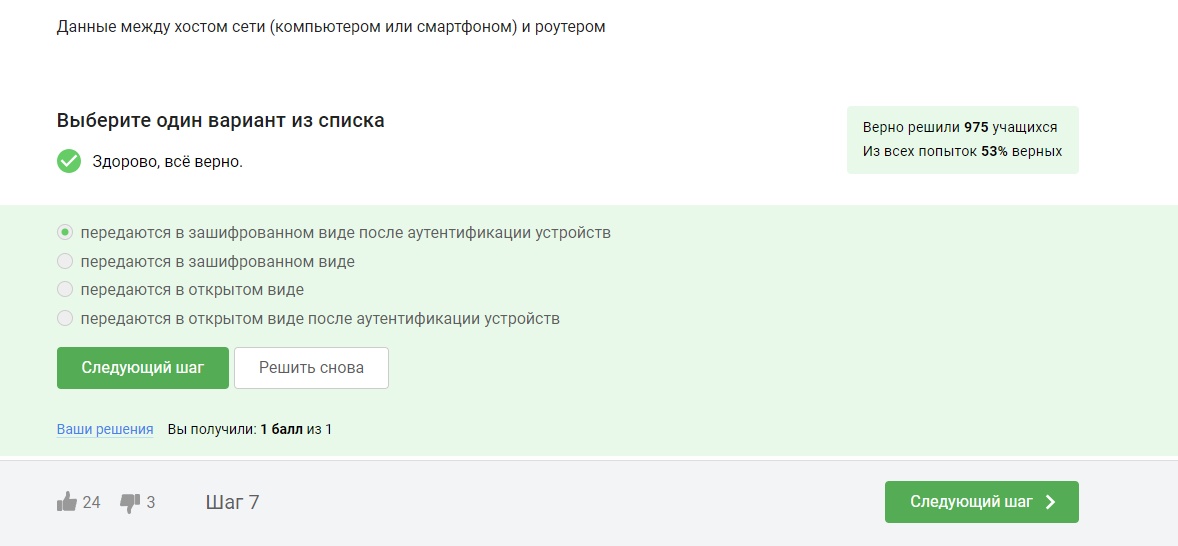


Рис. 4

Для домашней сети для аутентификации обычно используется метод: WPA2 Personal

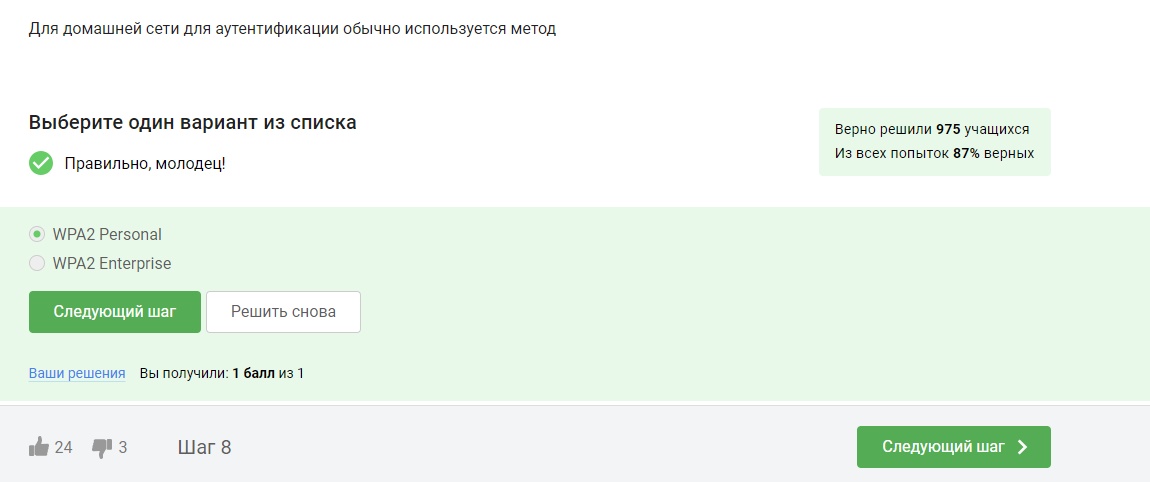


Рис. 5

# 6 Раздел 3.1. защита ПК и телефона

Можно ли зашифровать загрузочный сектор диска: да

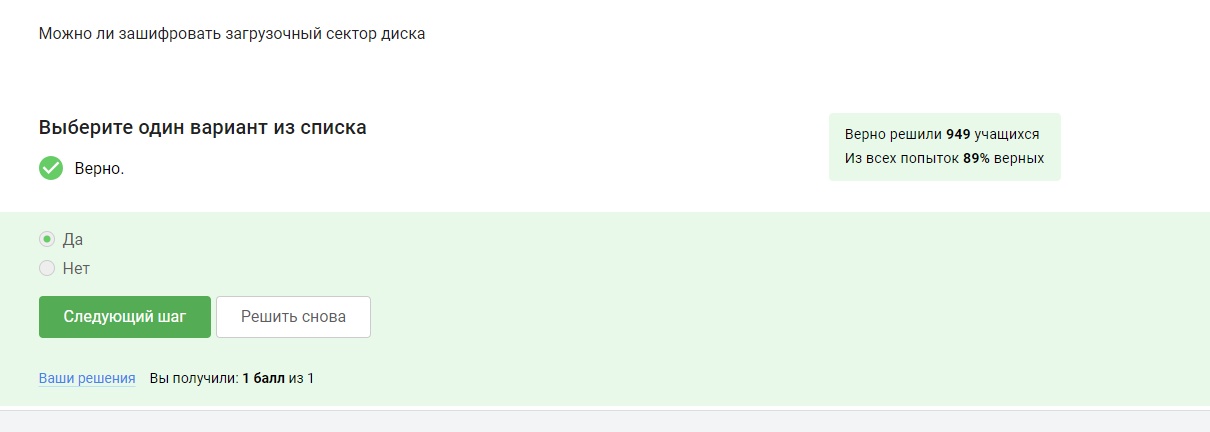


Рис. 1

Шифрование диска основано на: симметричном шифровании

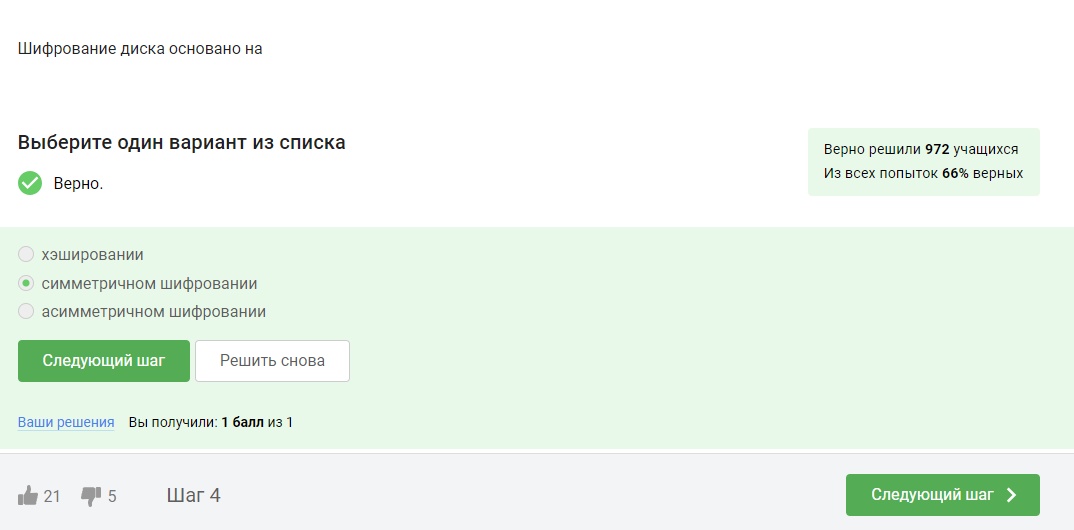


Рис. 2

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

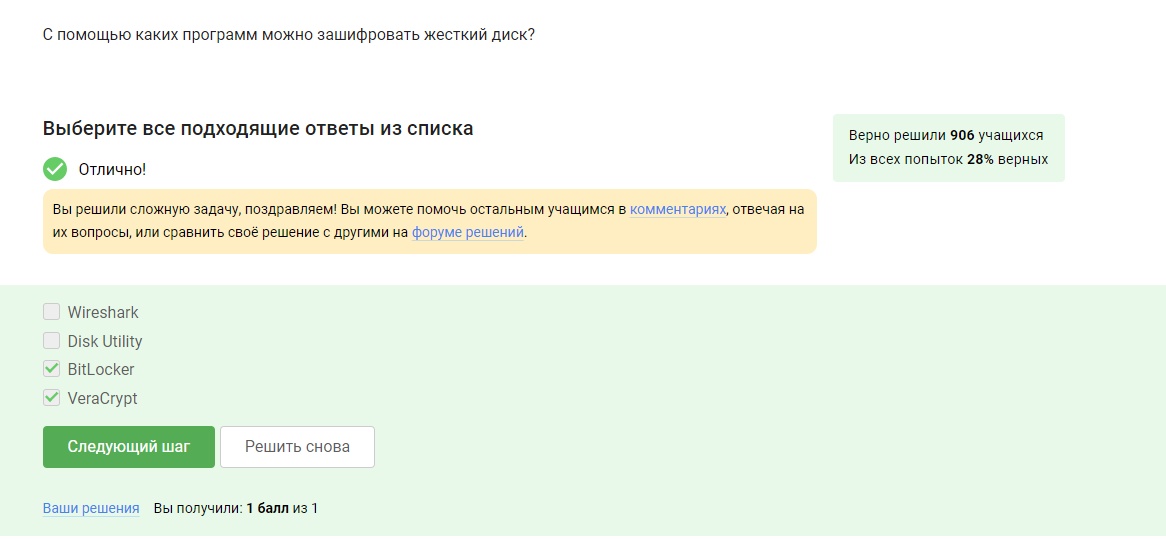
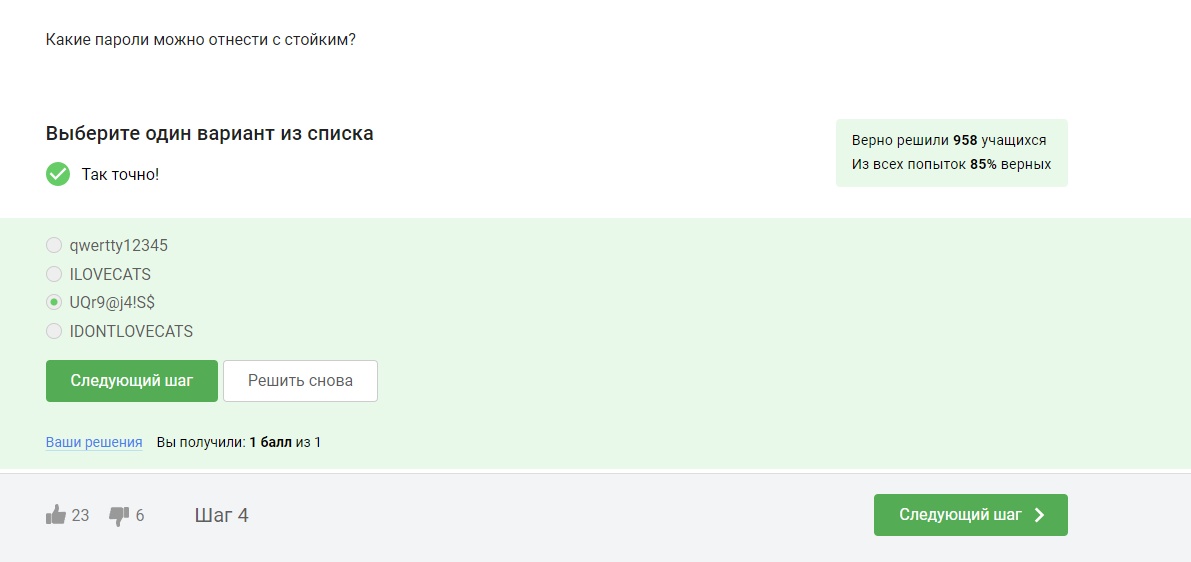
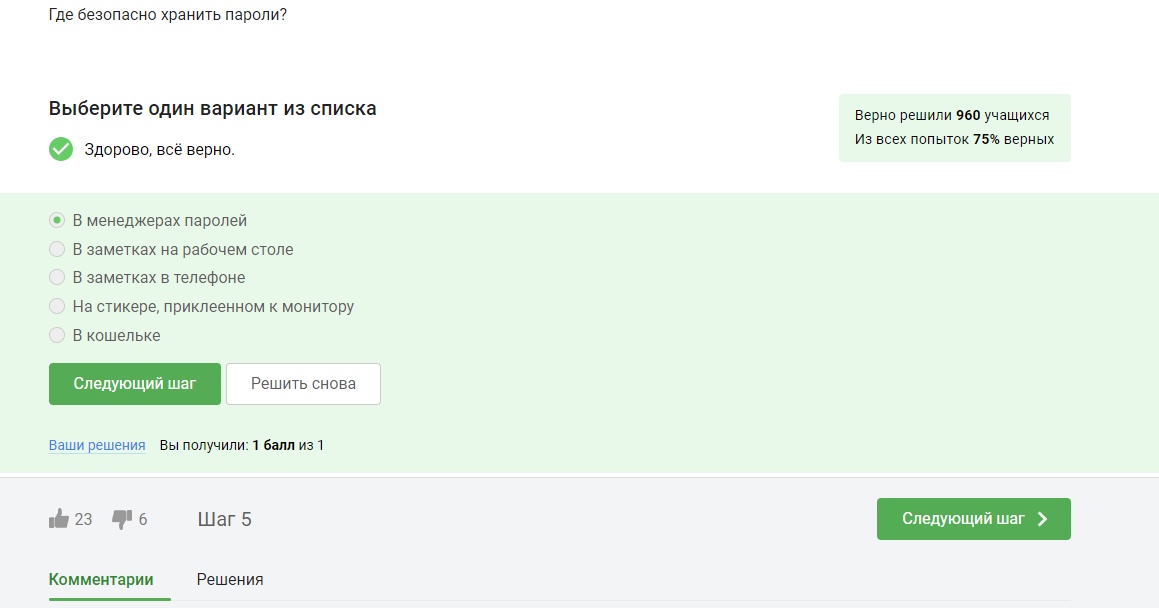
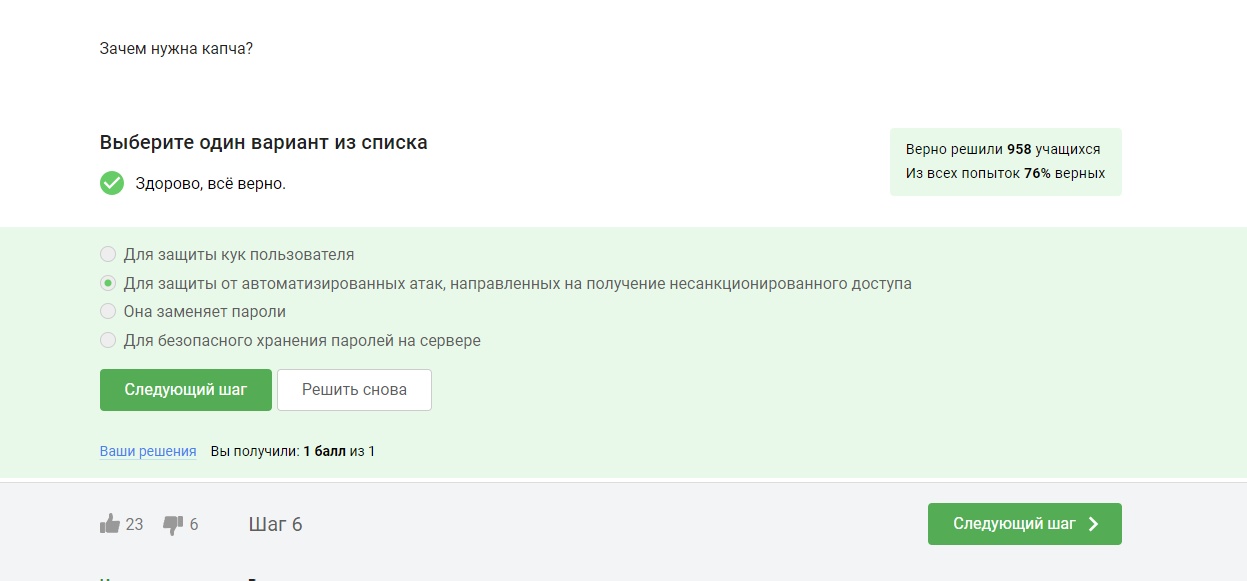


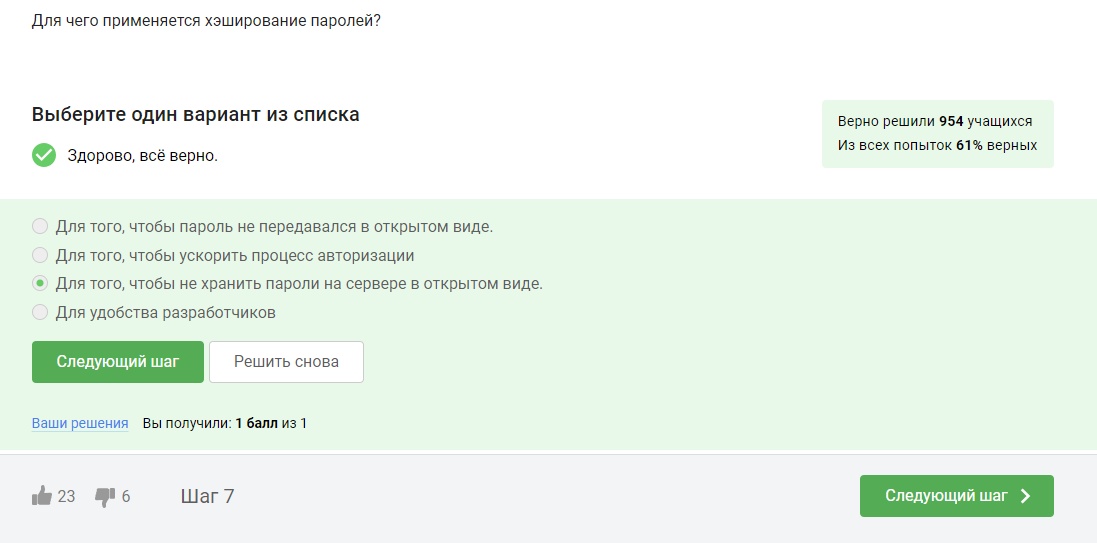
Рис. 3

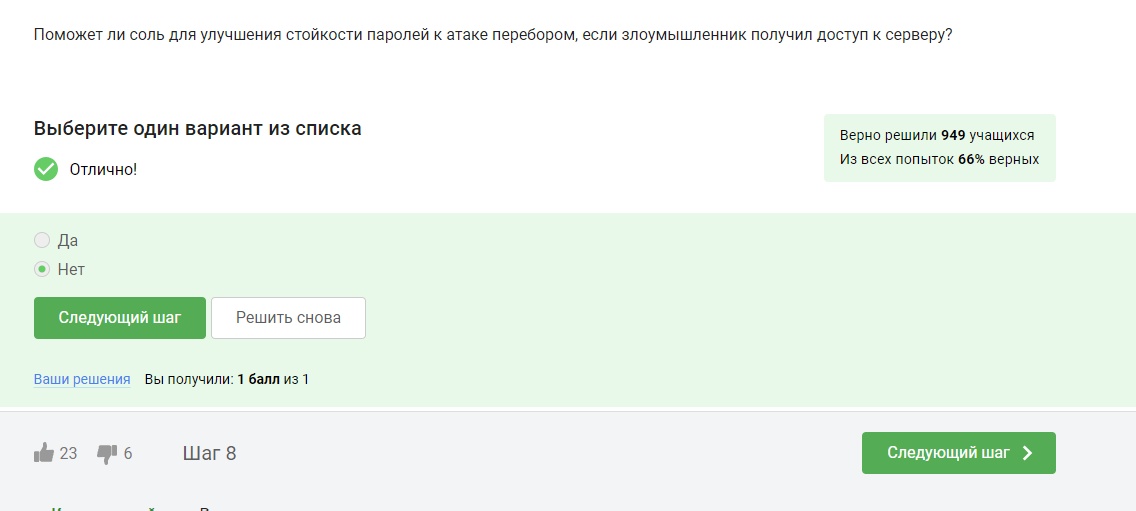
# 7 Раздел 3.2. Пароли

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

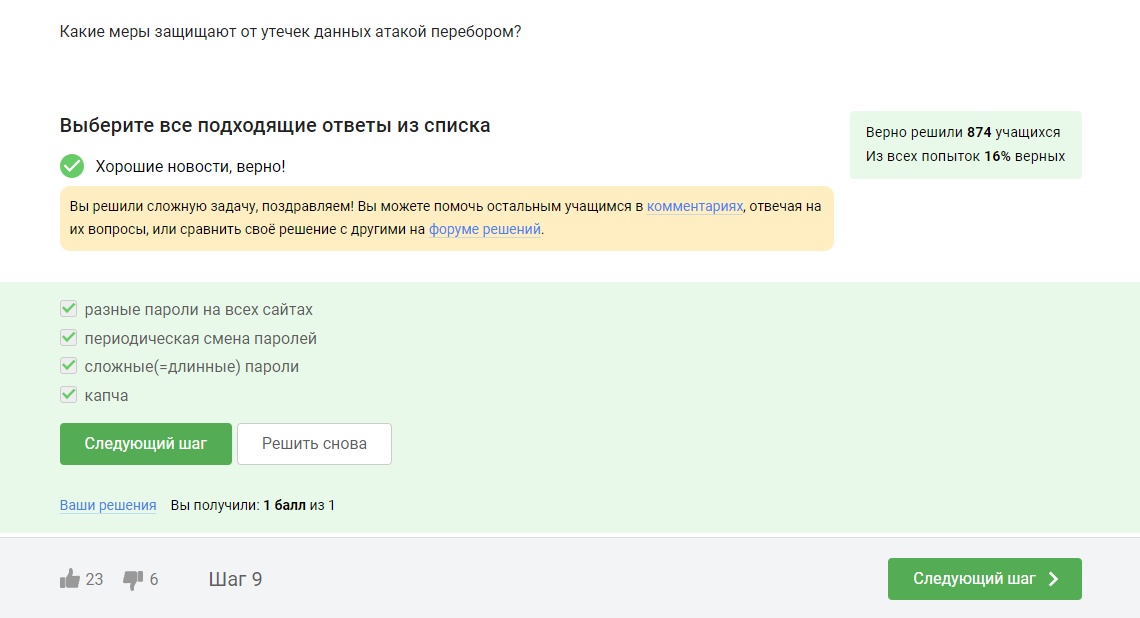
Где безопасно хранить пароли? В менеджерах паролей 

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

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 

Какие меры защищают от утечек данных атакой перебором?

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

# 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)

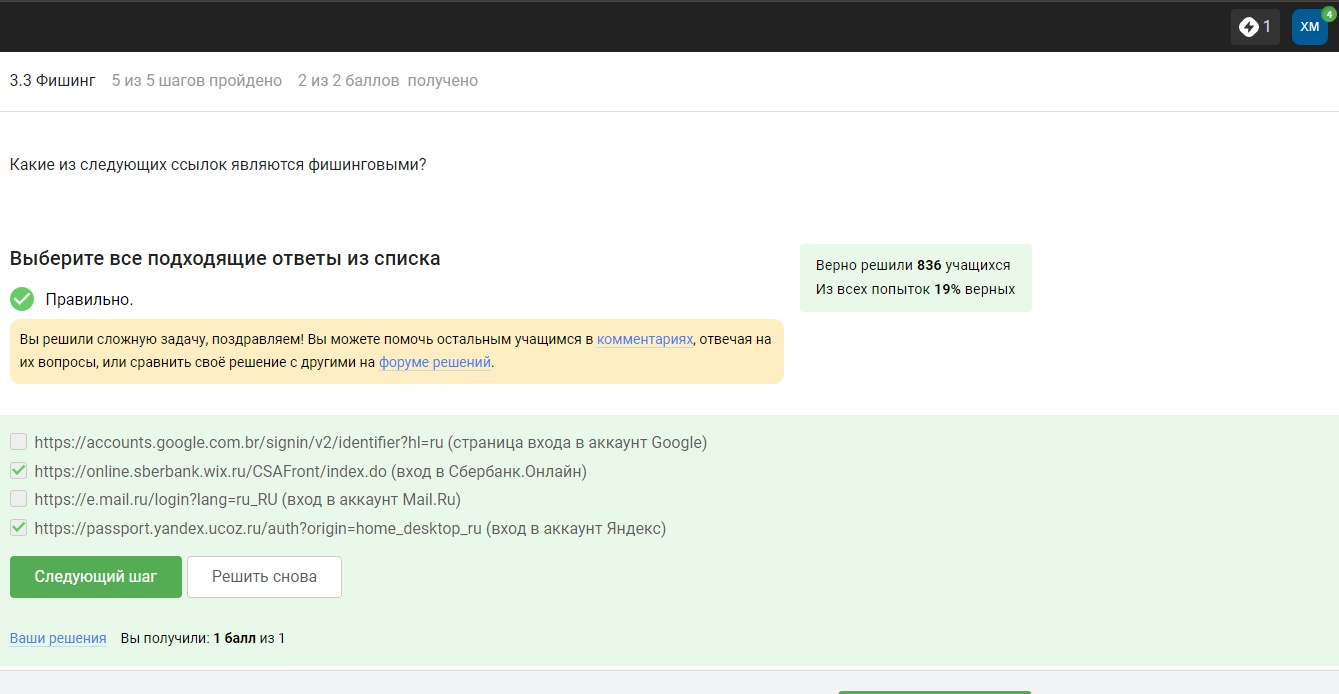
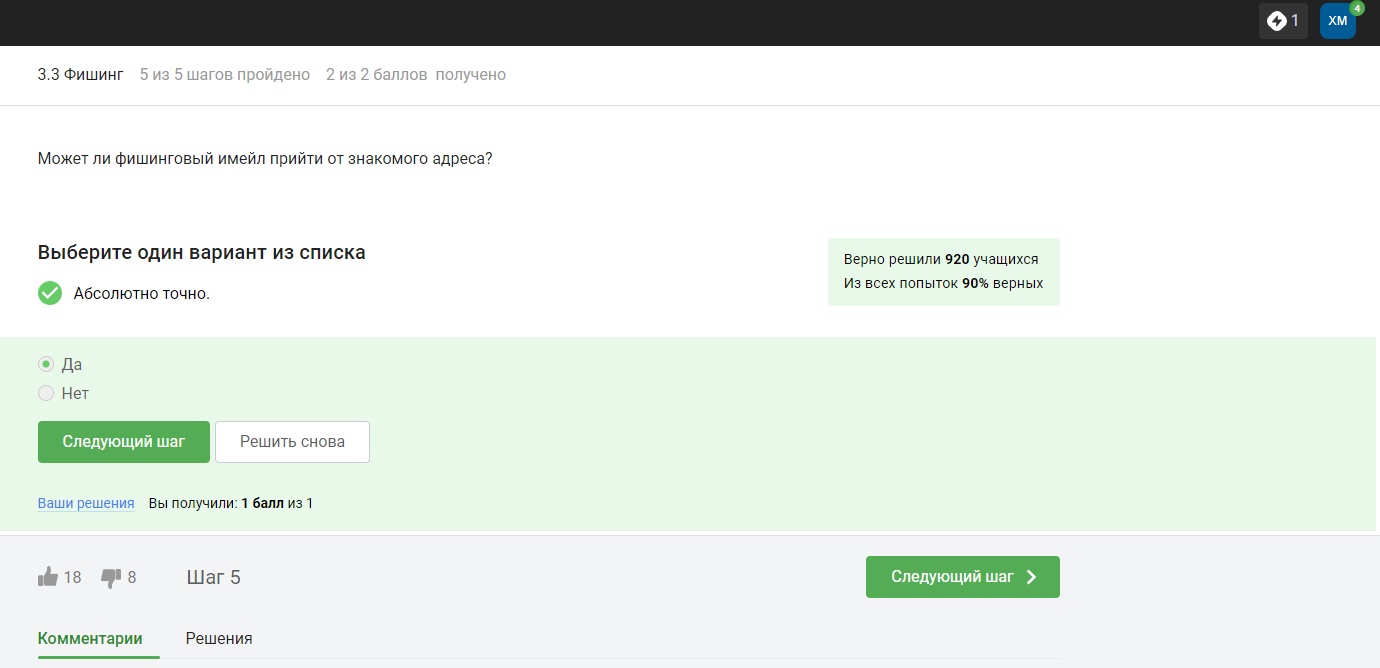
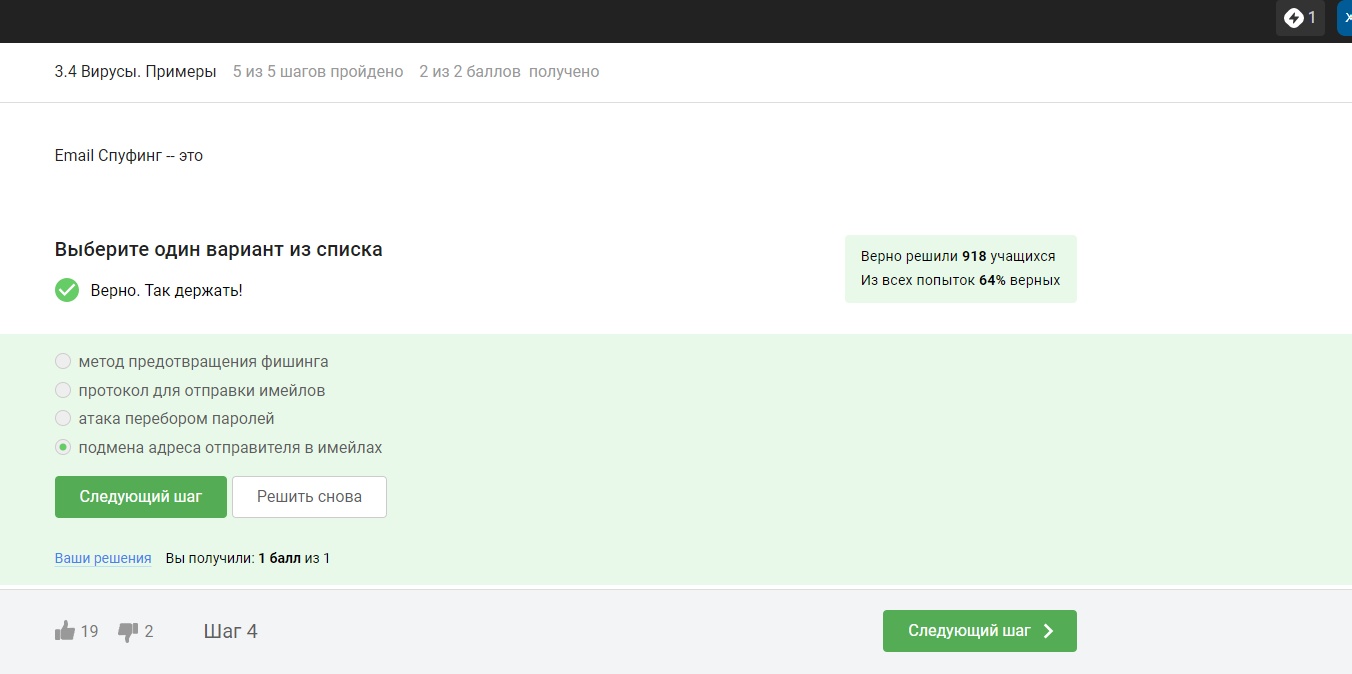
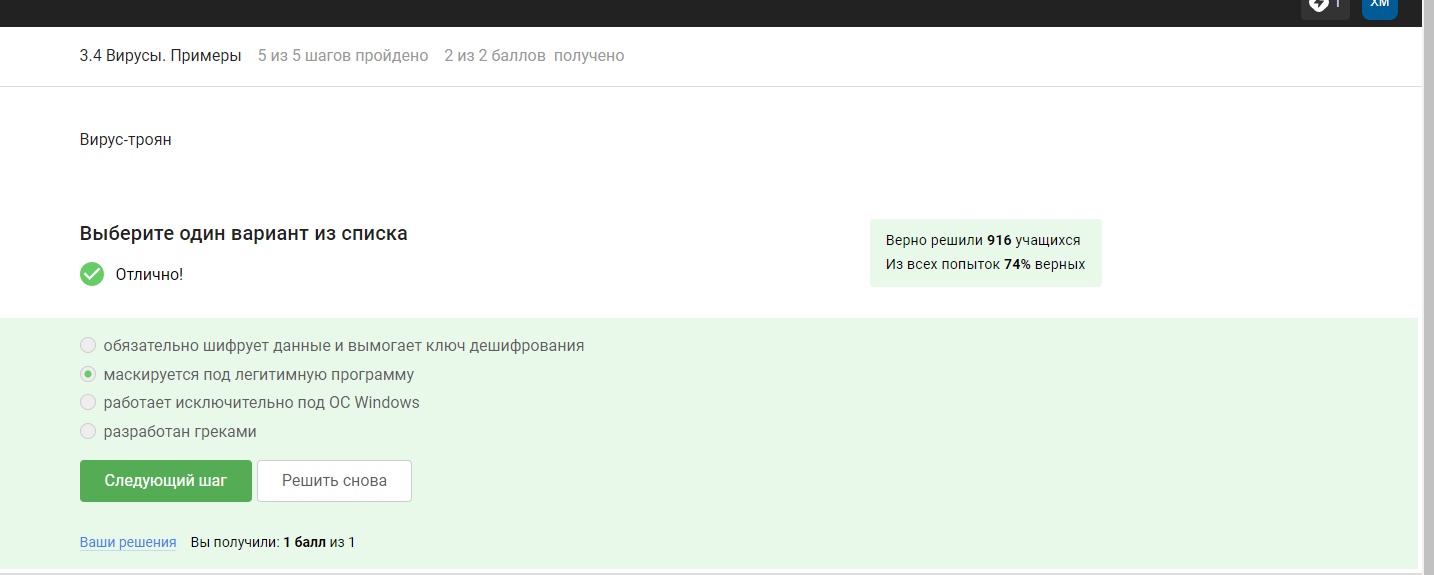


Рис. 1

Может ли фишинговый имейл прийти от знакомого адреса? да 

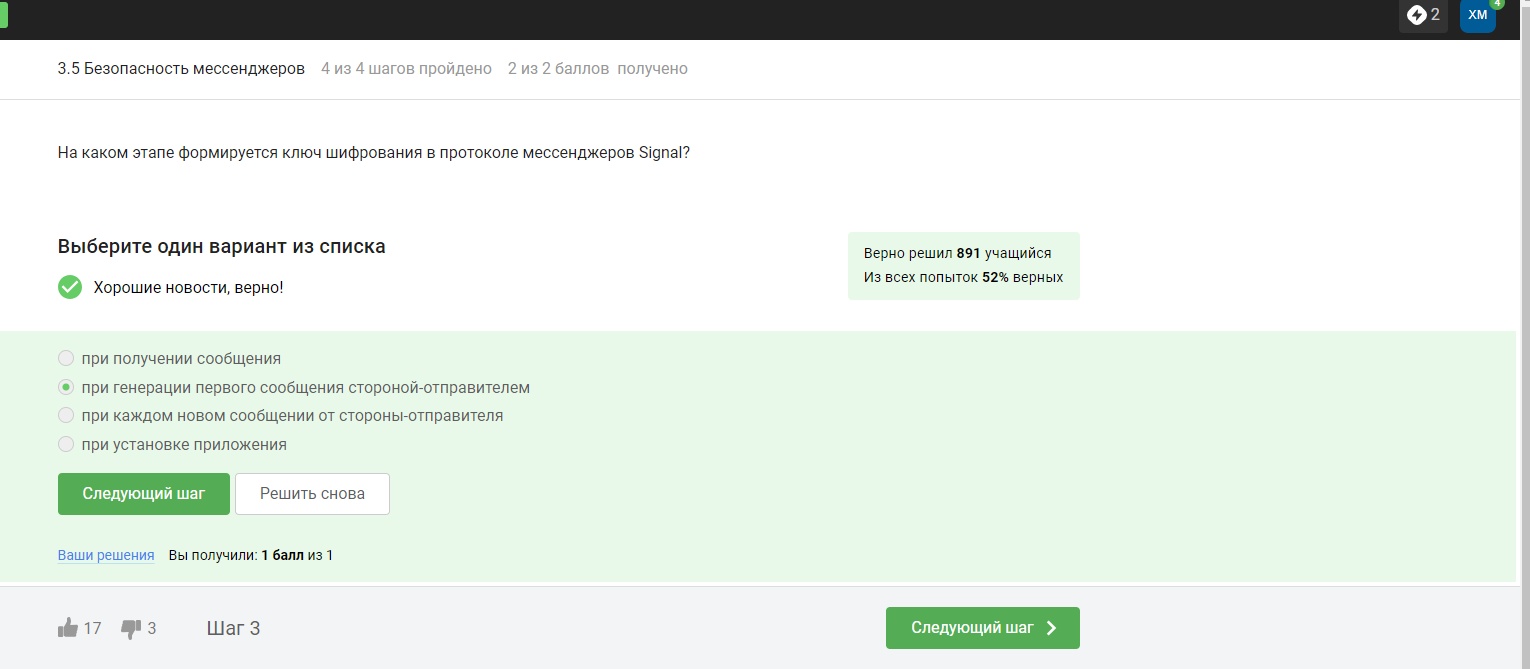
# 9 Раздел 3.3. Вирусы. Примеры

Email Спуфинг – это подмена адреса отправителя в имейлах 

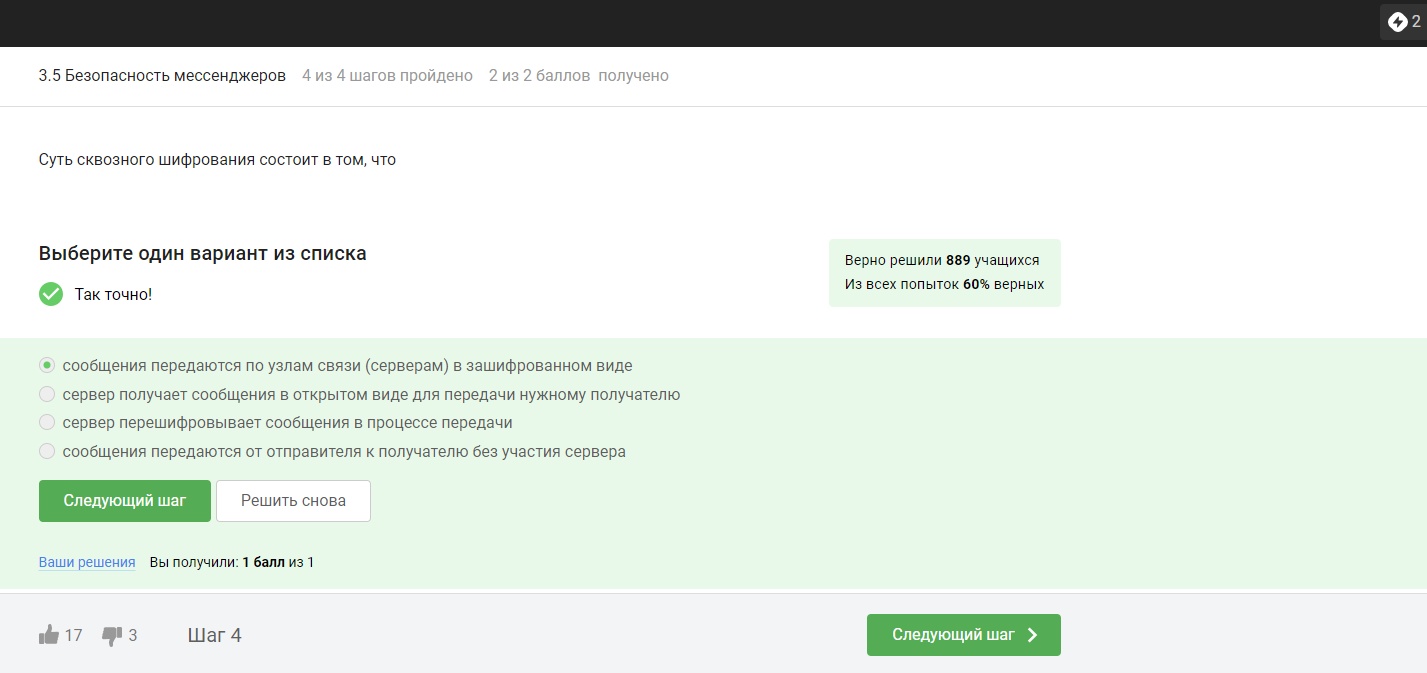
Вирус-троян маскируется под легитимную программу 

# 10 Раздел 3.5. Безопасность мессенджеров

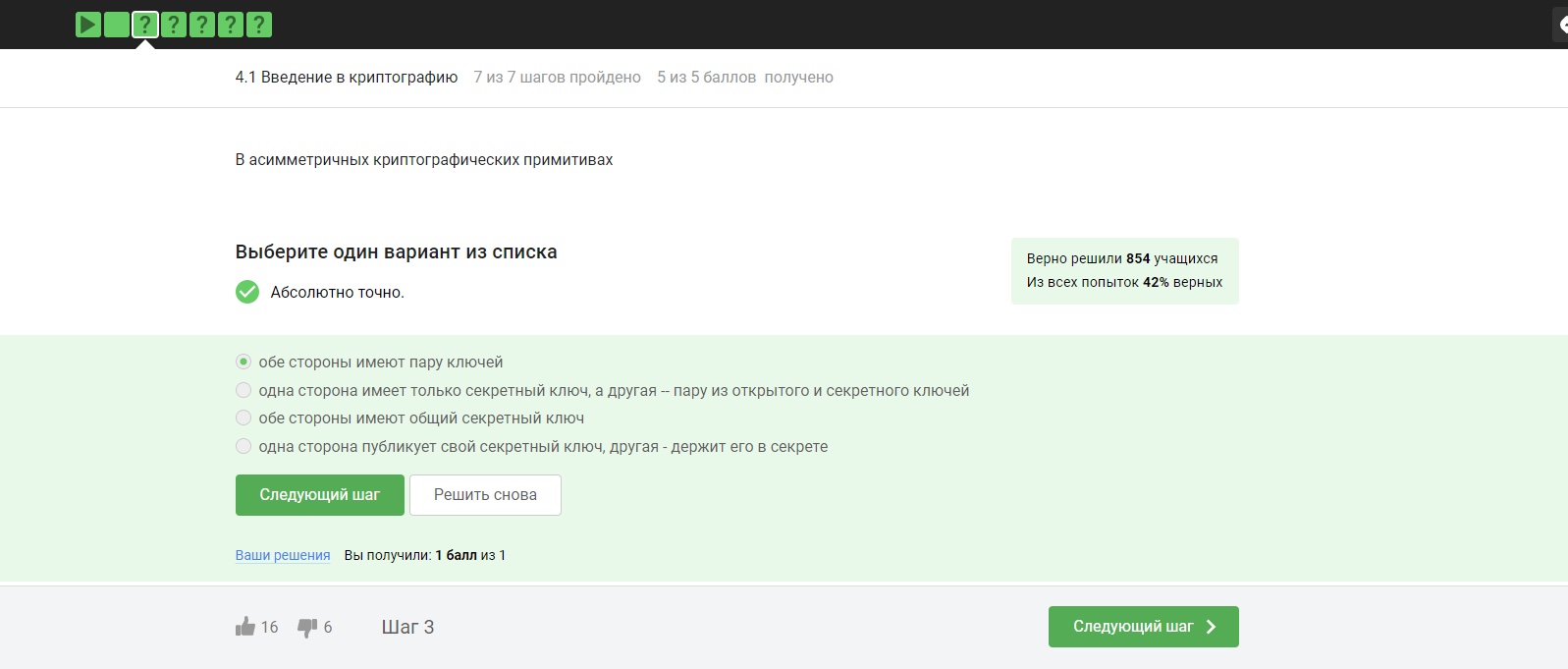
На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

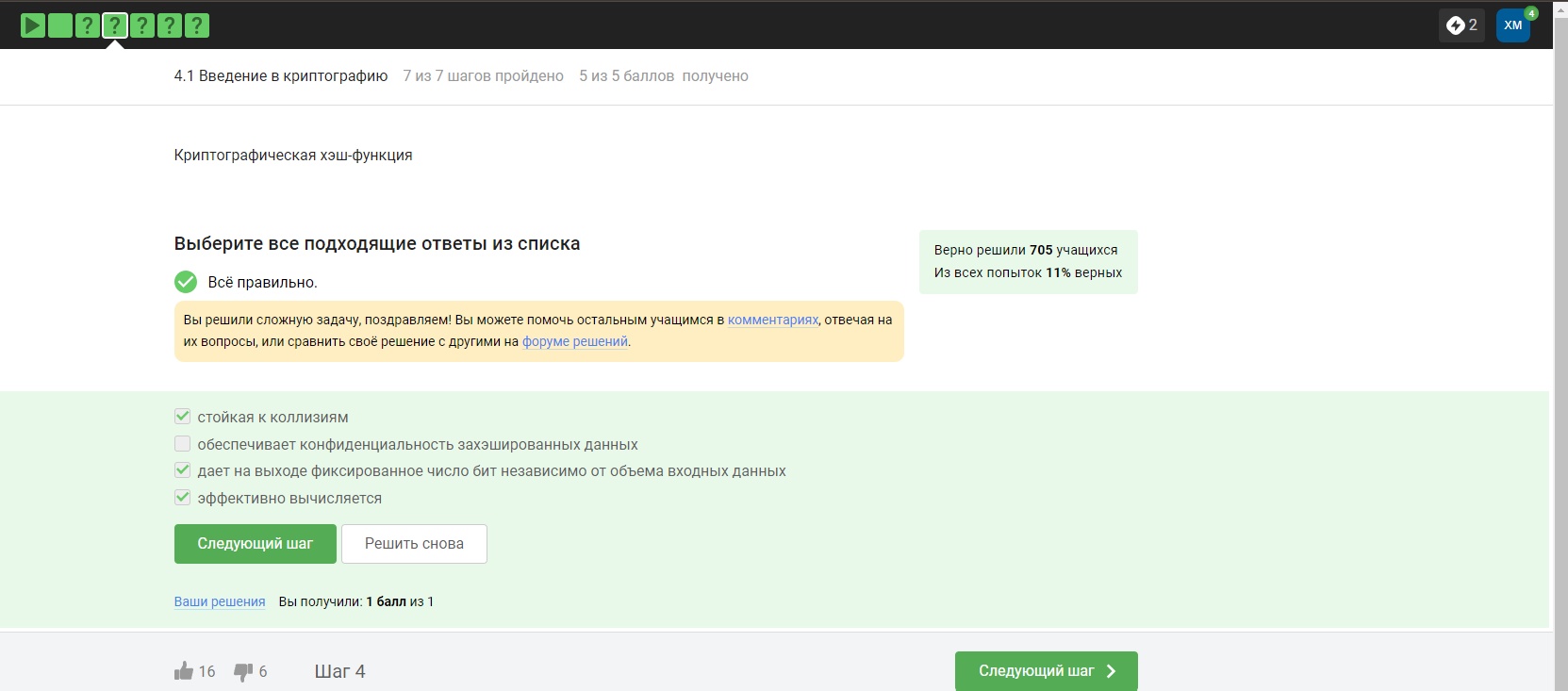
* при генерации первого сообщения стороной-отправителем 

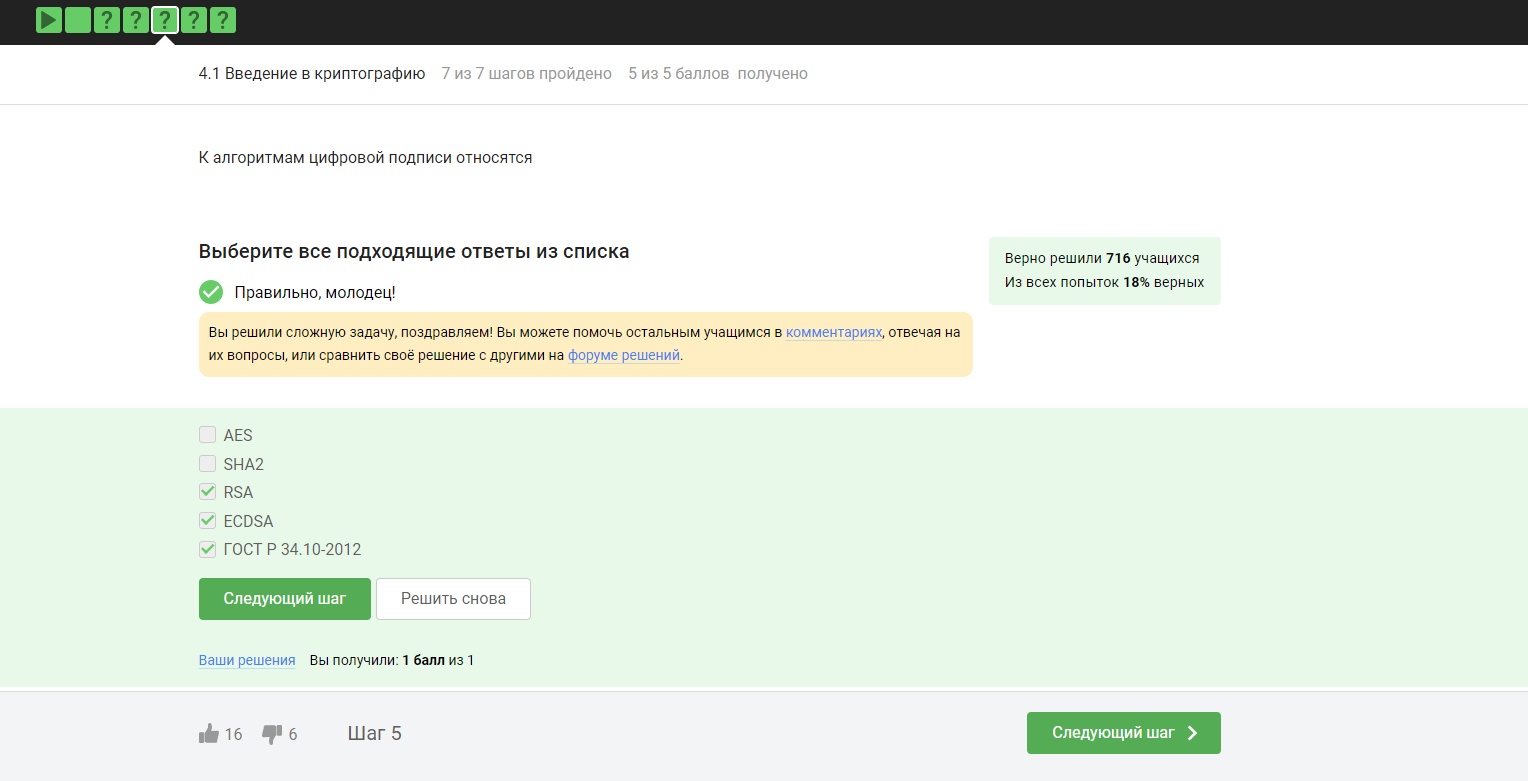
Суть сквозного шифрования состоит в том, что

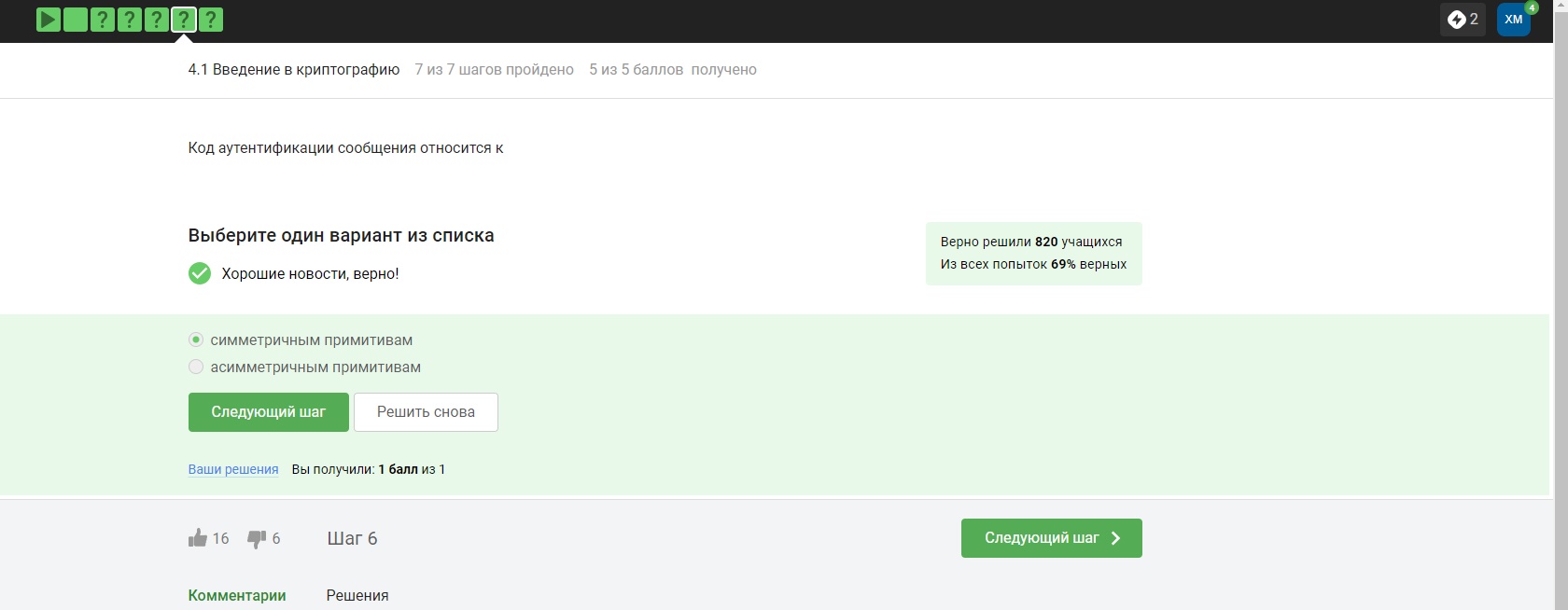
* сообщения передаются по узлам связи (серверам) в зашифрованном виде 

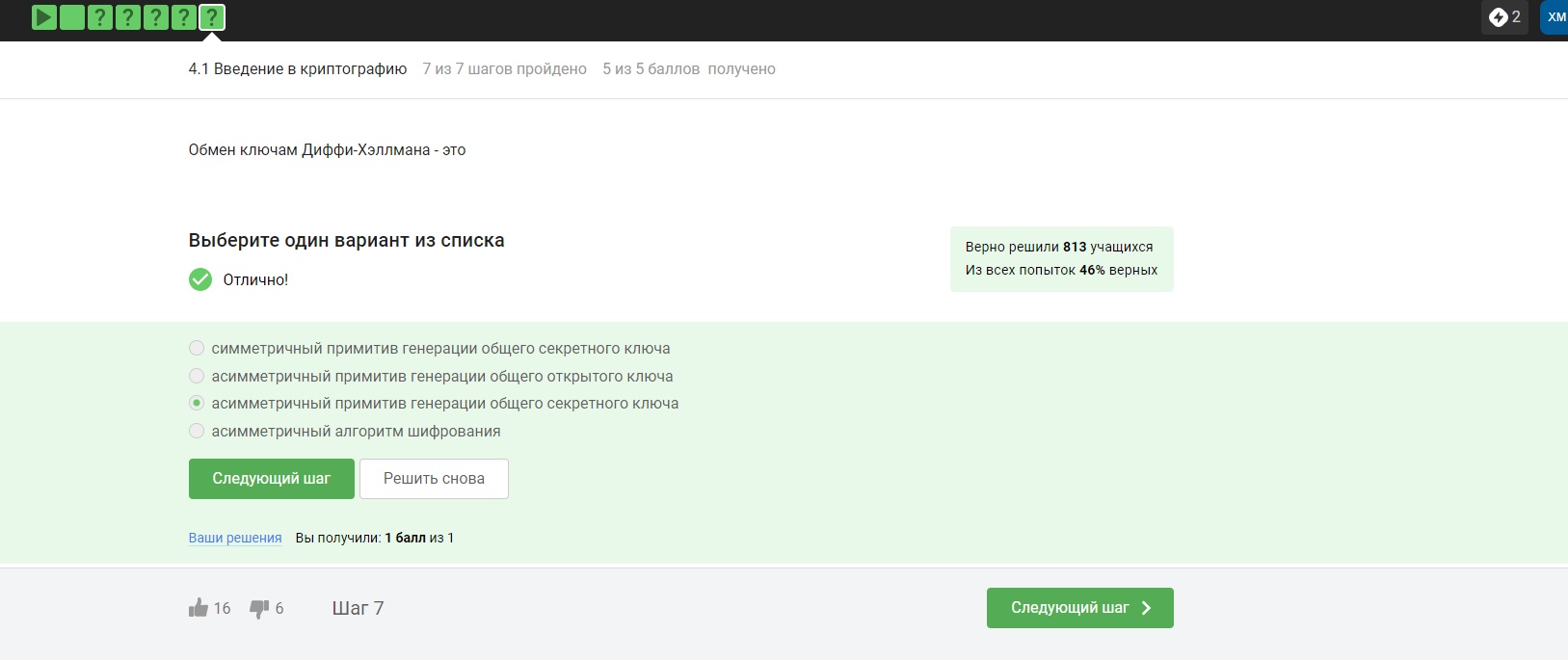
# 11 Раздел 4.1 Введение в криптографию

В асимметричных криптографических примитивах - обе стороны имеют пару ключей 

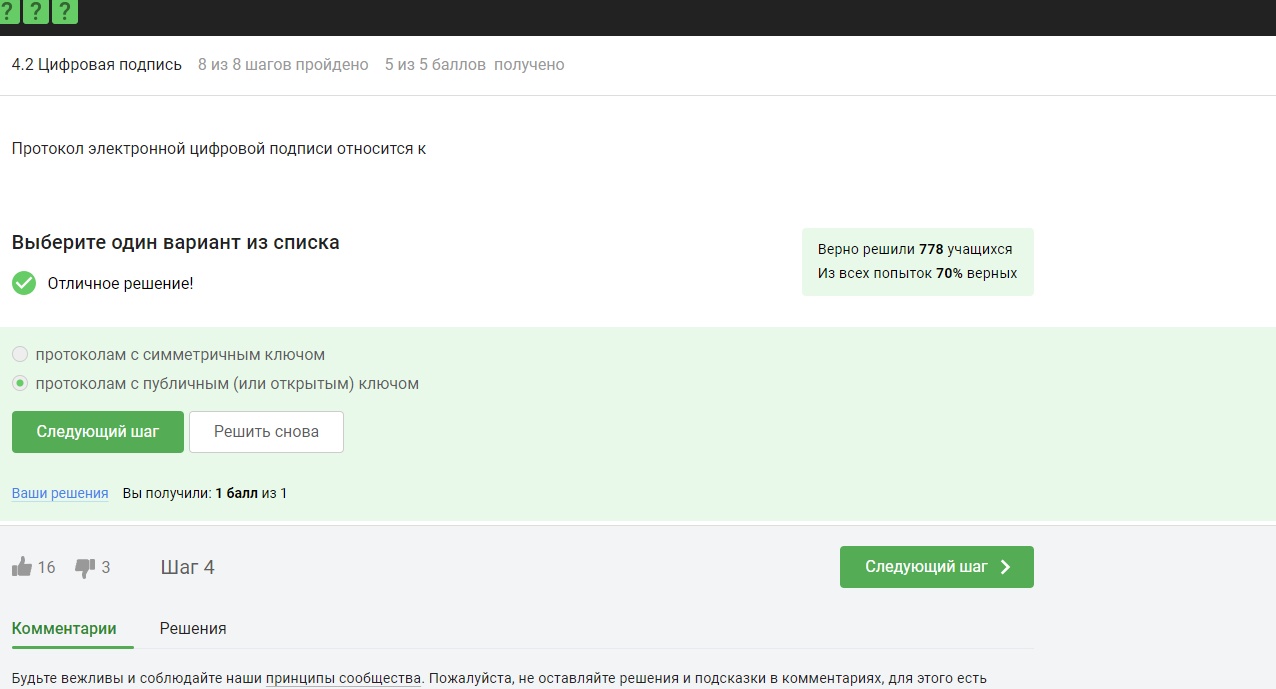
Криптографическая хэш-функция - стойкая к коллизиям - дает на выходе фиксированное число бит независимо от объема входных данных - эффективно вычисляется 

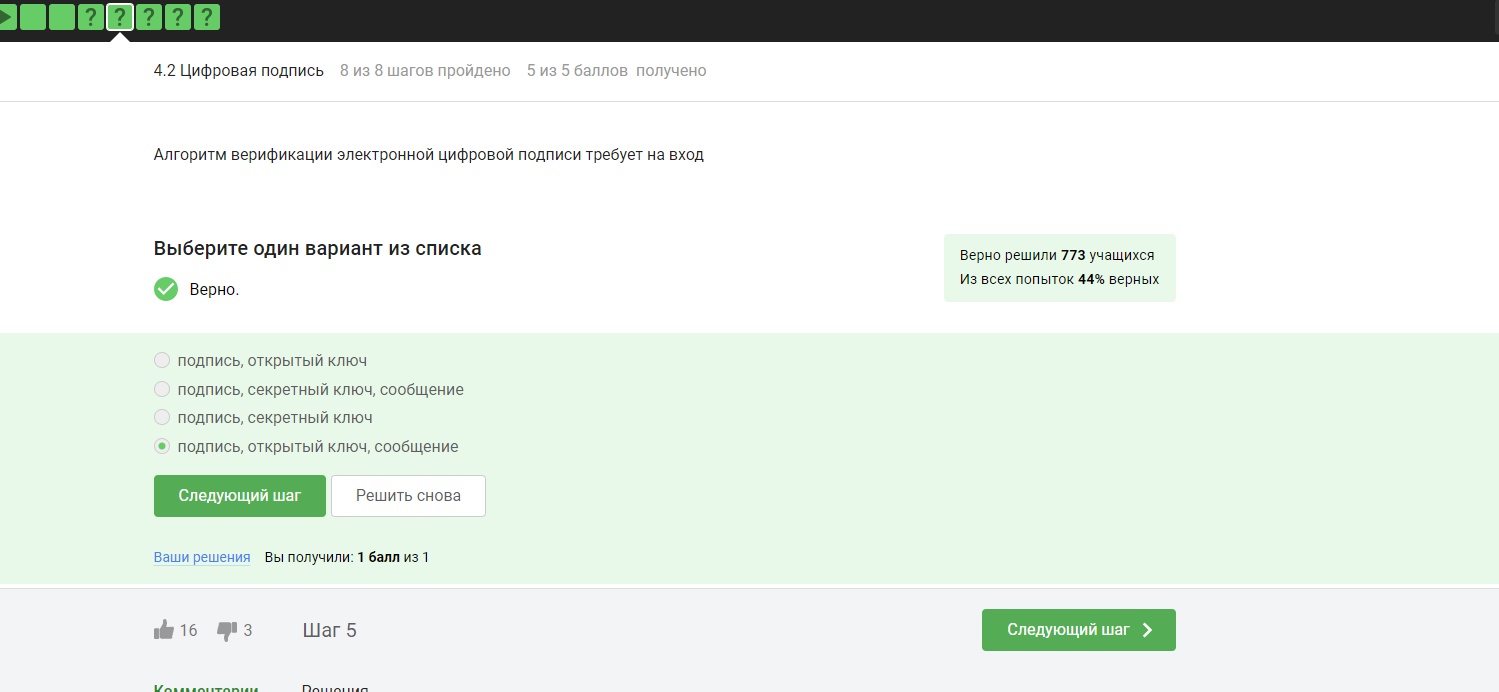
К алгоритмам цифровой подписи относятся - RSA - ECDSA - ГОСТ Р 34.10-2012. 

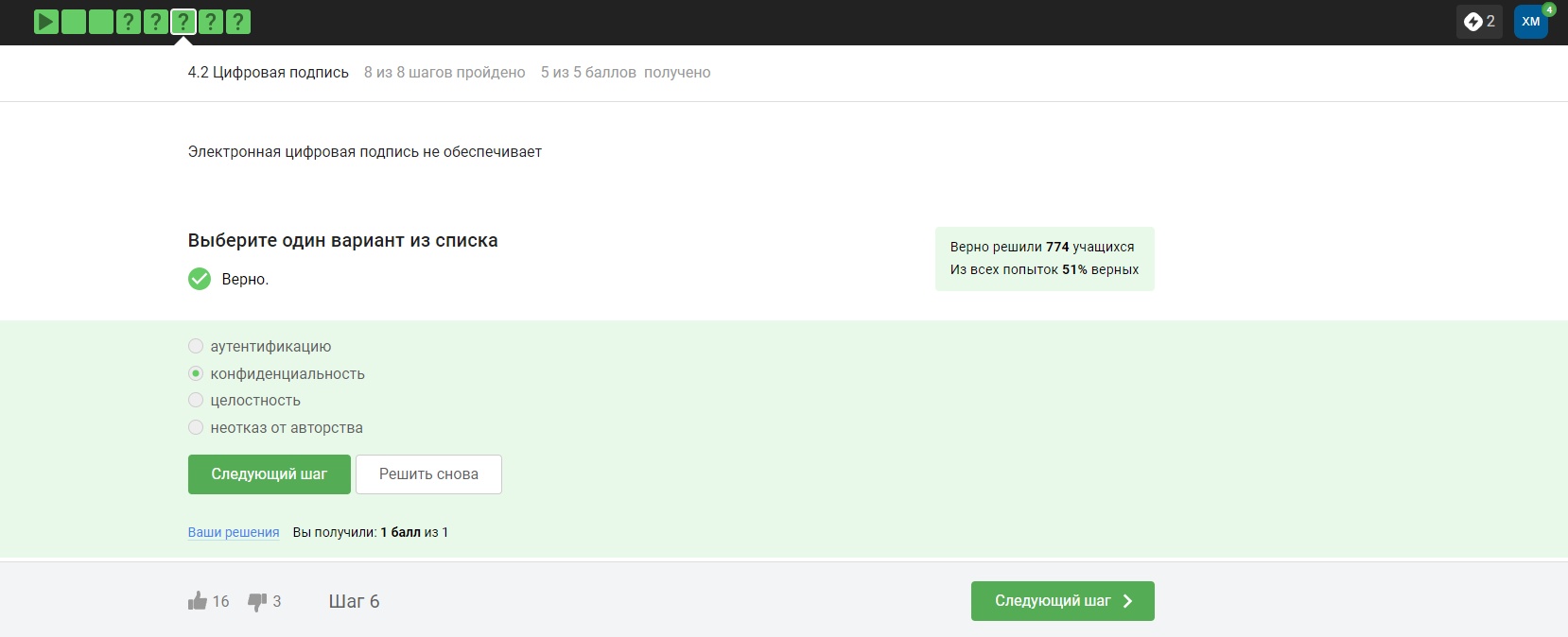
Код аутентификации сообщения относится к - симметричным примитивам 

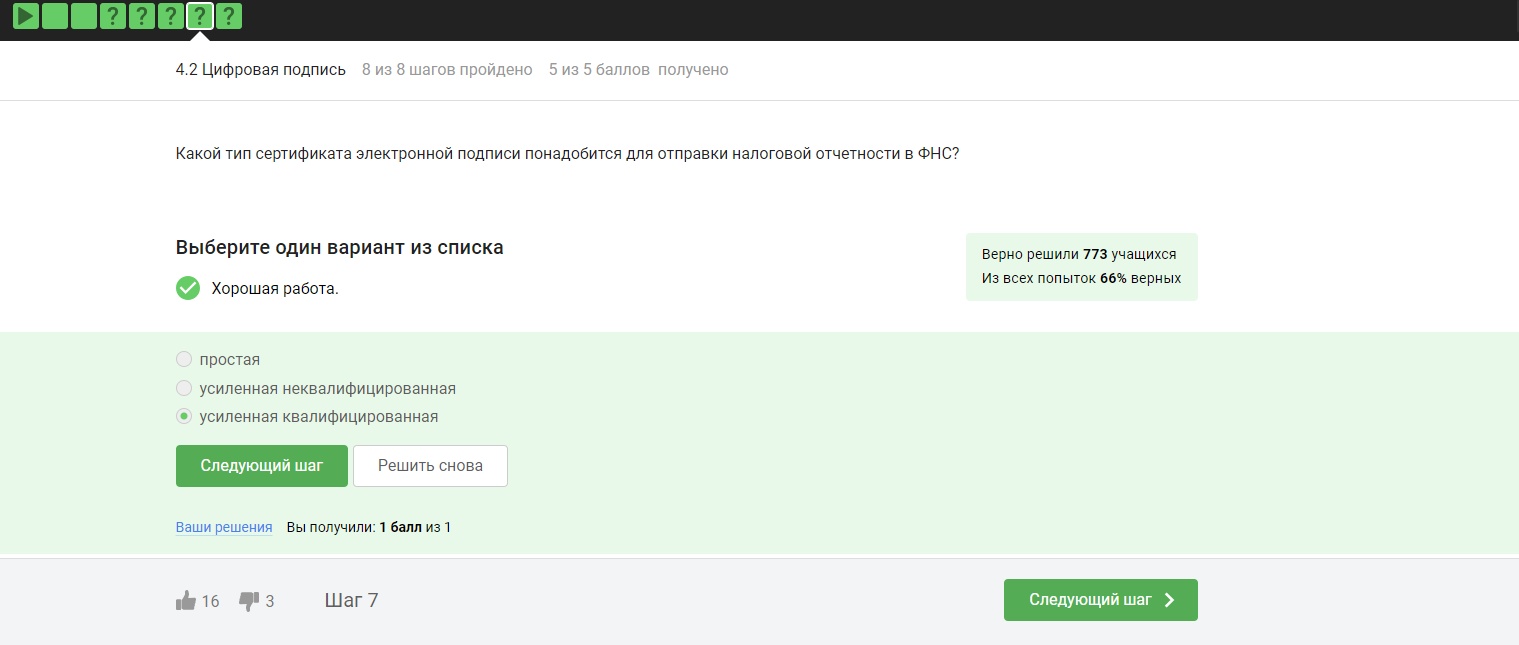
Обмен ключам Диффи-Хэллмана - это -асимметричный примитив генерации общего секретного ключа 

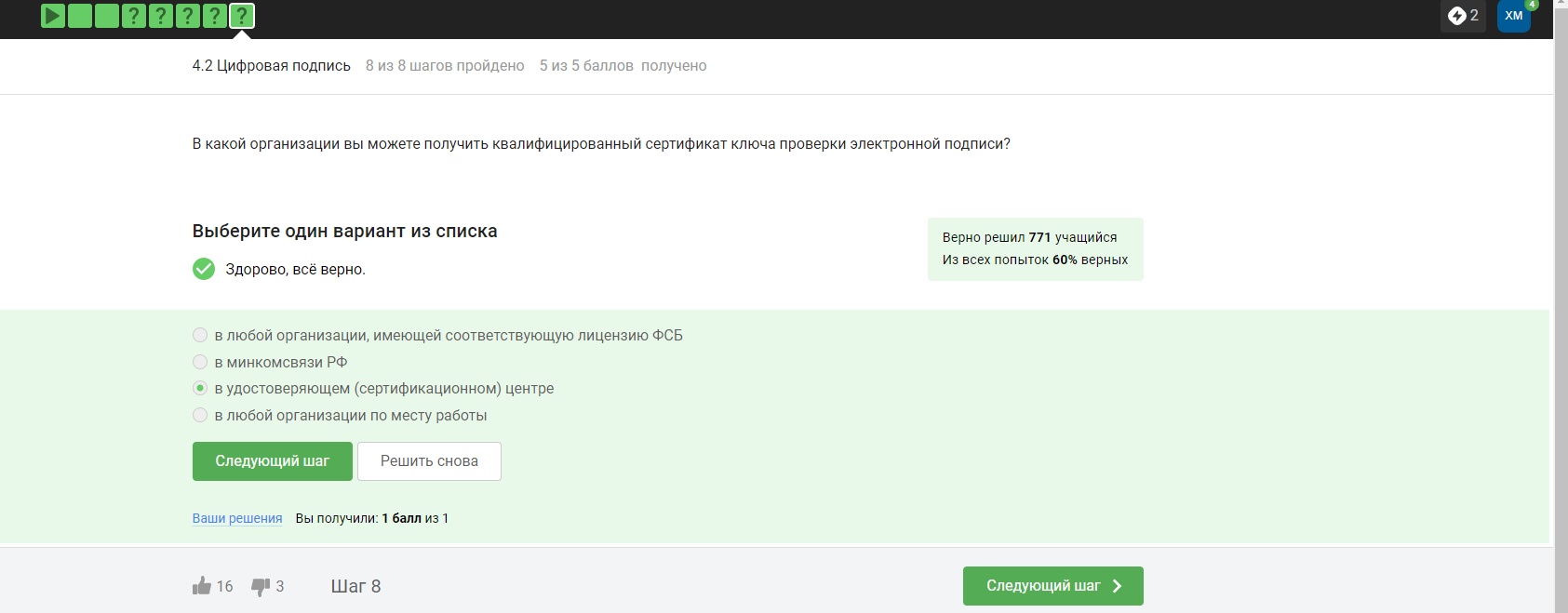
# 12 Раздел 4.2 Цифровая подпись

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

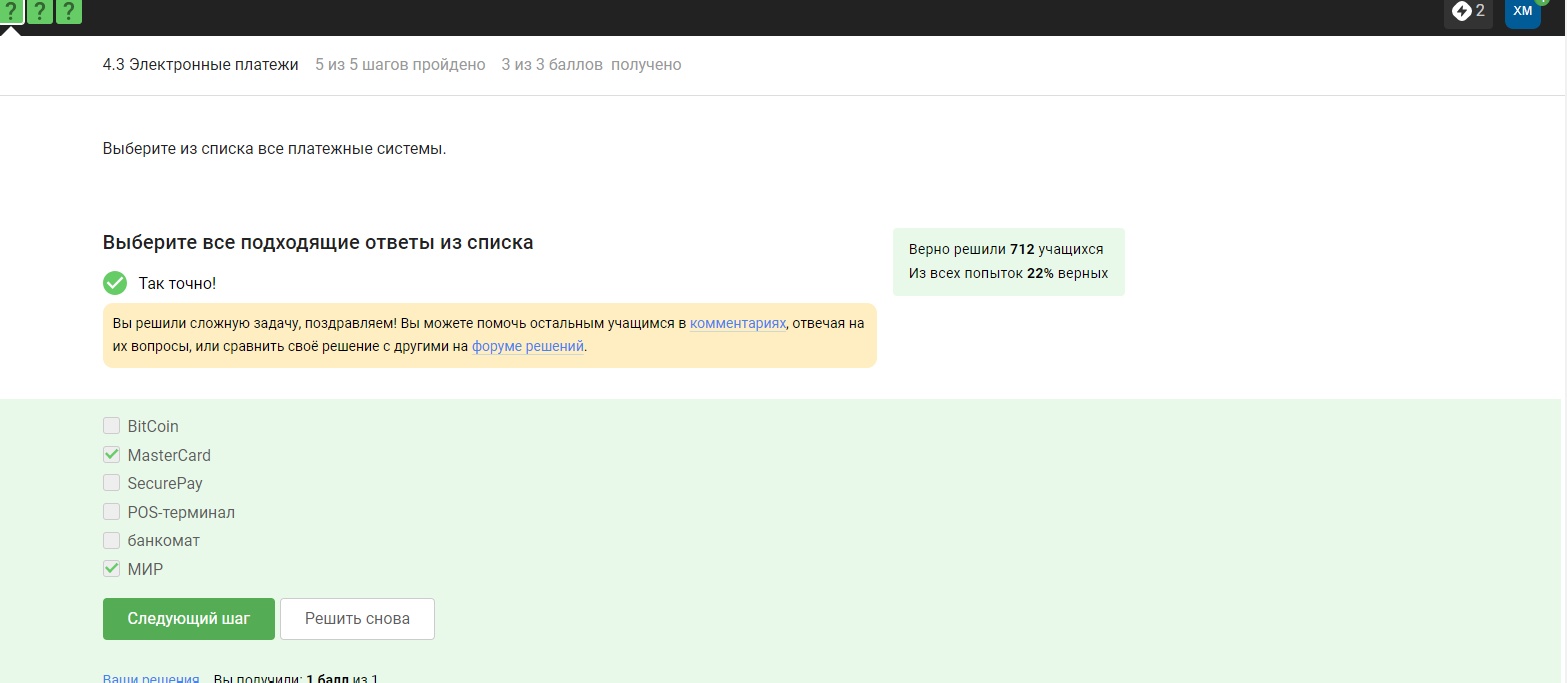
Алгоритм верификации электронной цифровой подписи требует на вход - подпись, открытый ключ, сообщение 

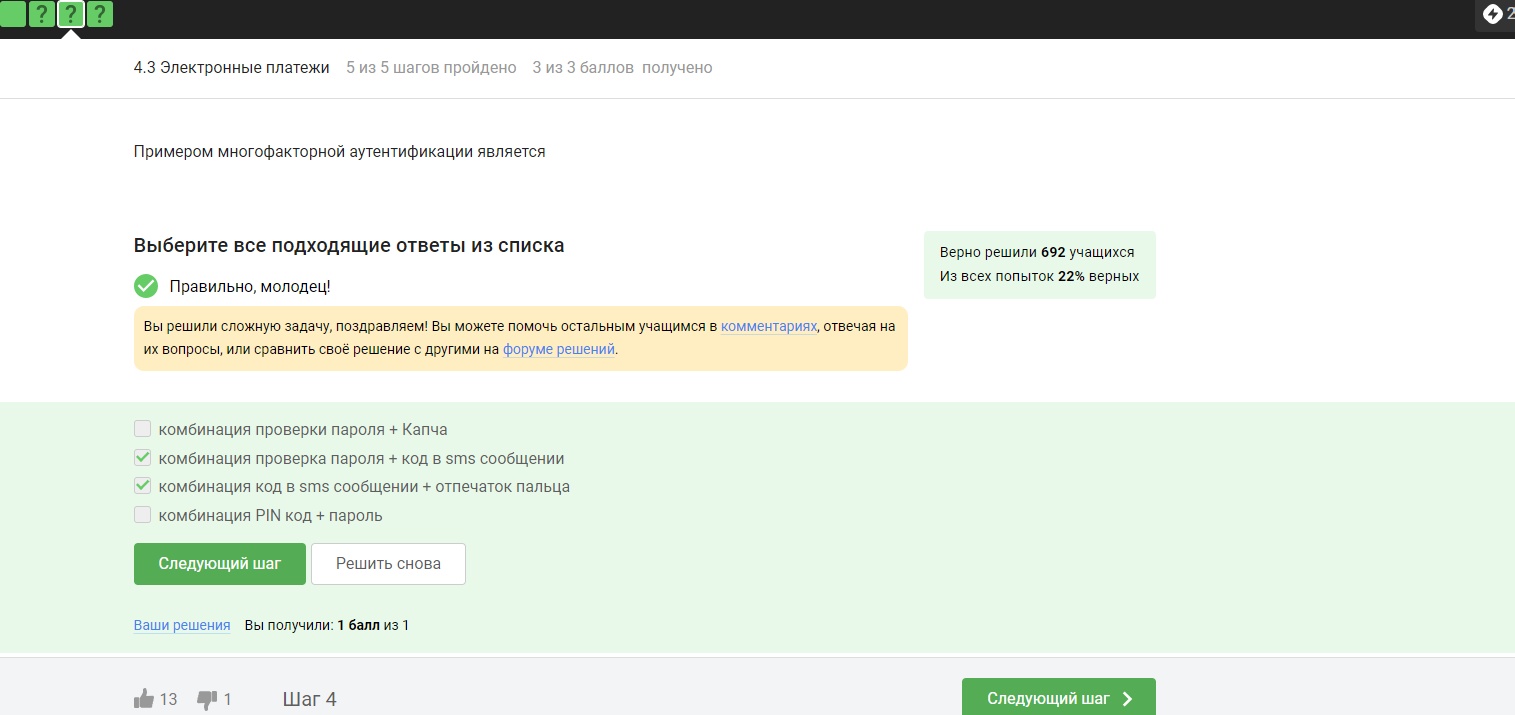
Электронная цифровая подпись не обеспечивает -конфиденциальность 

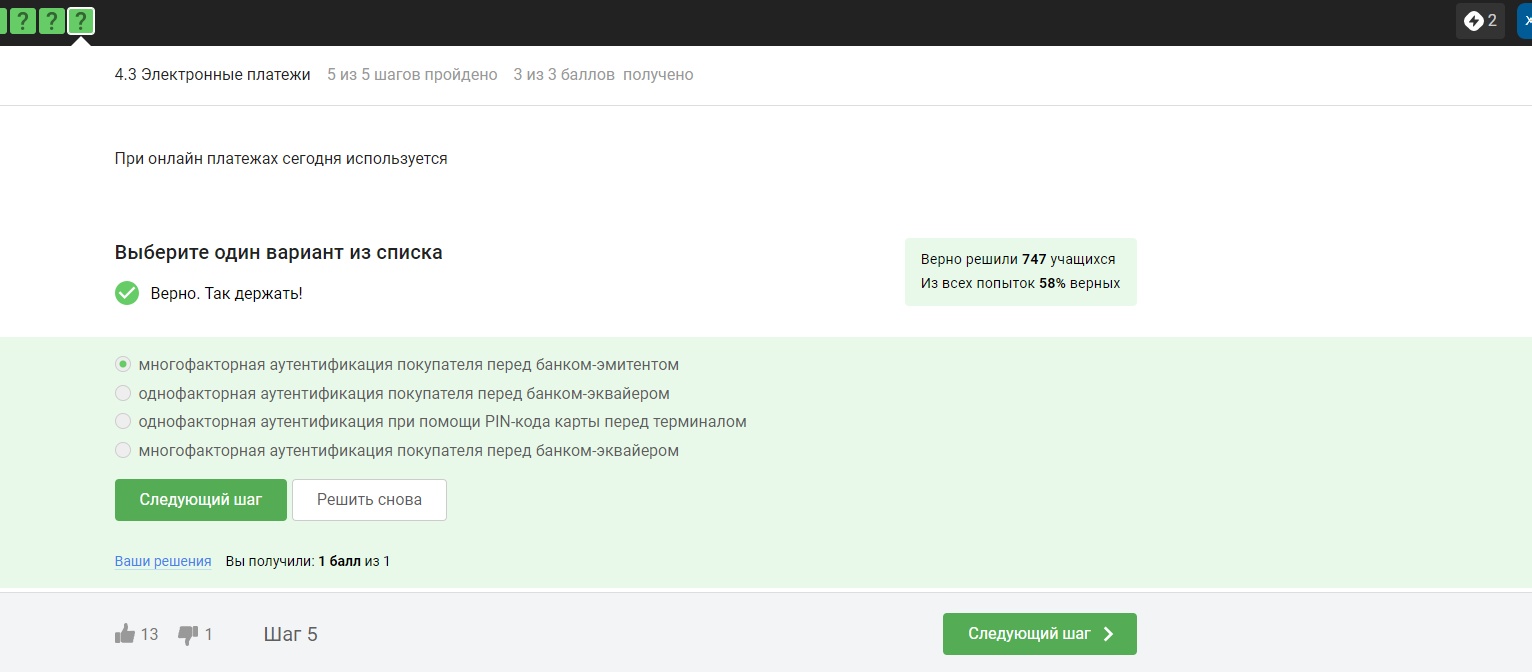
Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС? -усиленная квалифицированная 

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

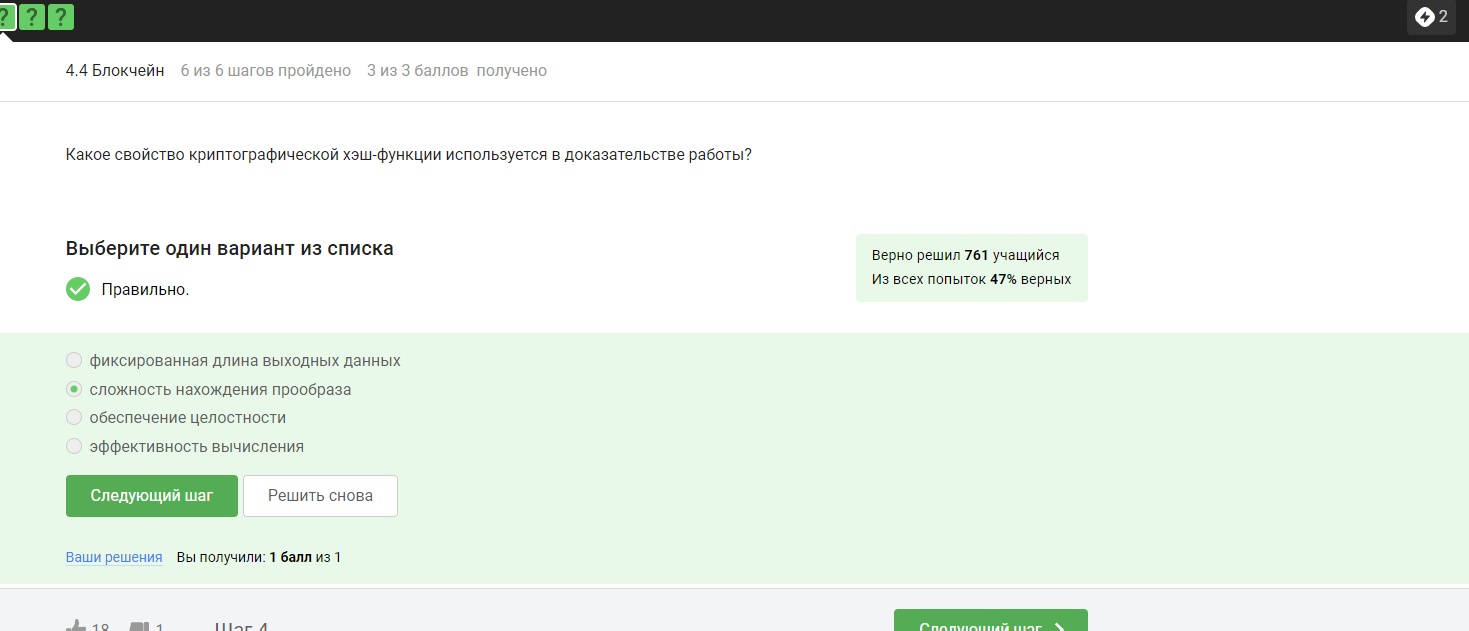
# 13 Раздел 4.3 Электронные платежи

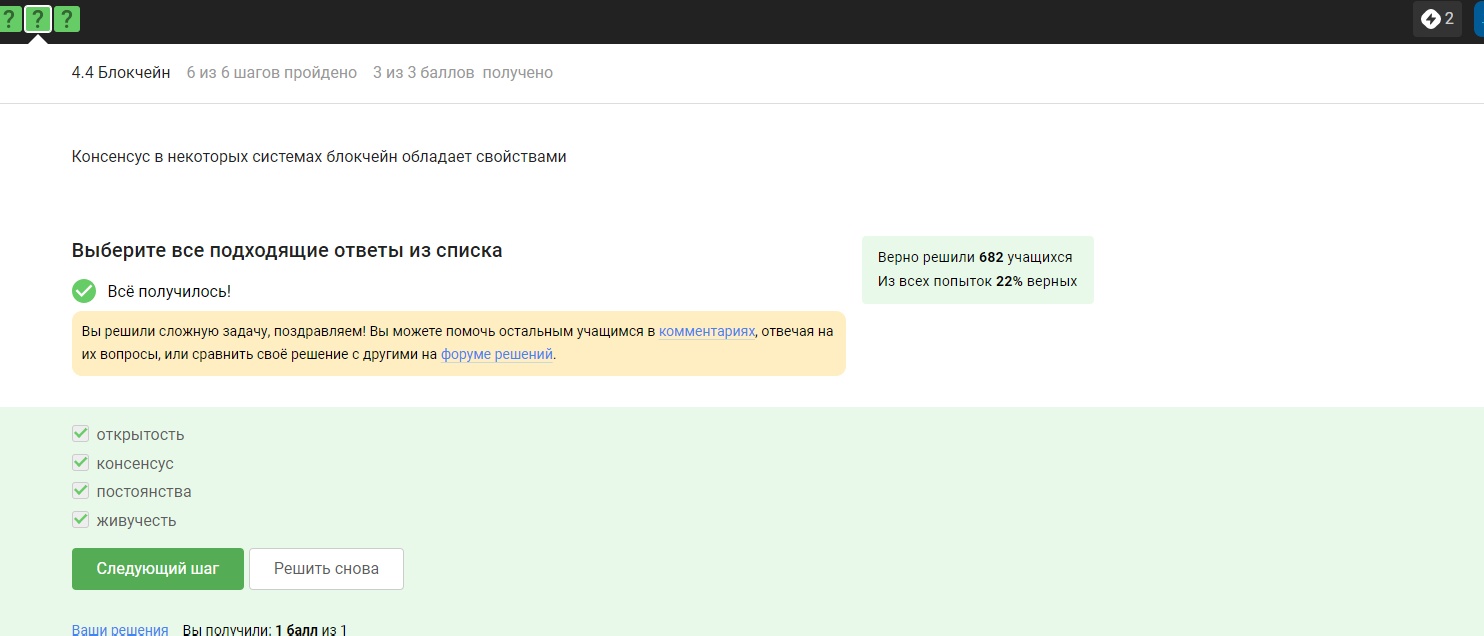
Выберите из списка все платежные системы. - MasterCard - МИР 

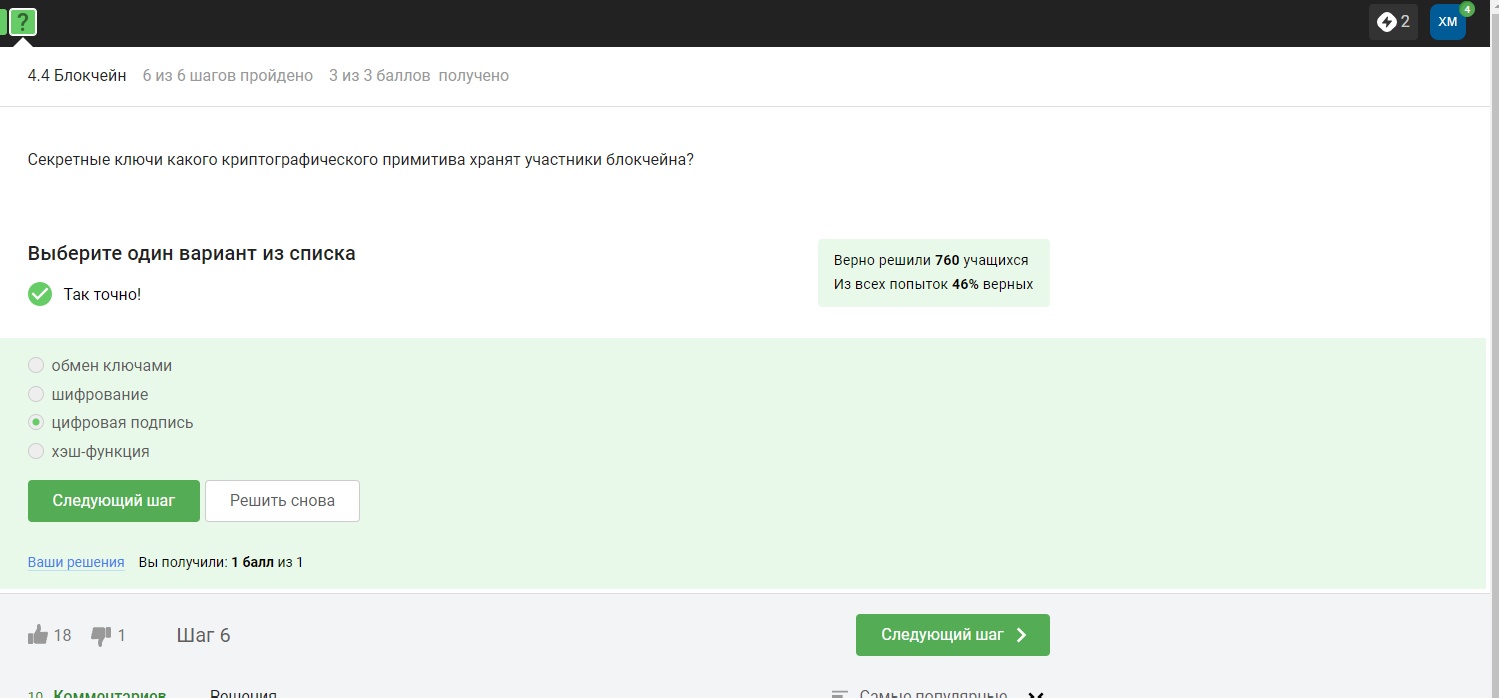
Примером многофакторной аутентификации является - комбинация проверка пароля + код в sms сообщении - комбинация код в sms сообщении + отпечаток пальца 

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

# 14 Раздел 4.4 Блокчейн

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

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

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

# 15 Вывод

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