Отчёт по прохождению внешнего курса

Основы информационной безопасности

Бережной Иван Александрович

Содержание

Список иллюстраций

# 1 Цель работы

Ознакомиться с основными понятиями информационной безопасности

# 2 Задание

Пройти все этапы курса

# 3 Выполнение тестов

Поскольку тестов в совокупности не так много, а на отдельных этапах их вообще мало, я решил, что более целессобразно будет сделать один отчёт по прохождению всего курса, нежели делать множество отчётов по каждому этапу.

## 3.1 Прохождение первого этапа

Протоколом прикладного уровня является HTTPS, поскольку он устанавливает правила общения с внешним ресурсом (рис. 1).

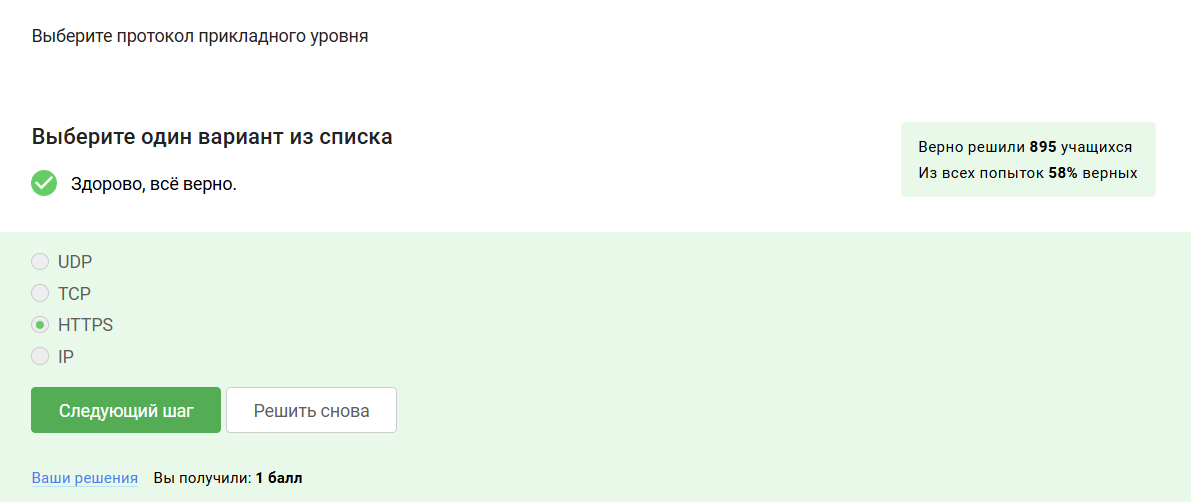


Рис. 1: Протокол прикладного уровня

Протокол TCP работает на транспортном уровне, поскольку определяет правила передачи пакетов (рис. 2).

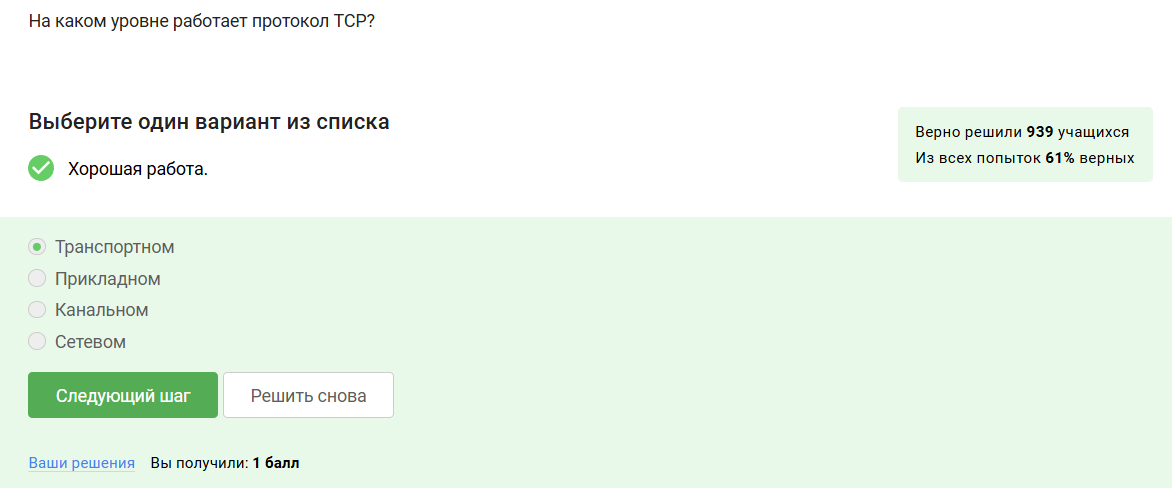


Рис. 2: Уровень работы протокола TCP

Валидными IP-адресами считаются адреса, содержащие 4 октета, каждый из которых состоит из чисел в диапазоне от 0 до 255 (рис. 3).

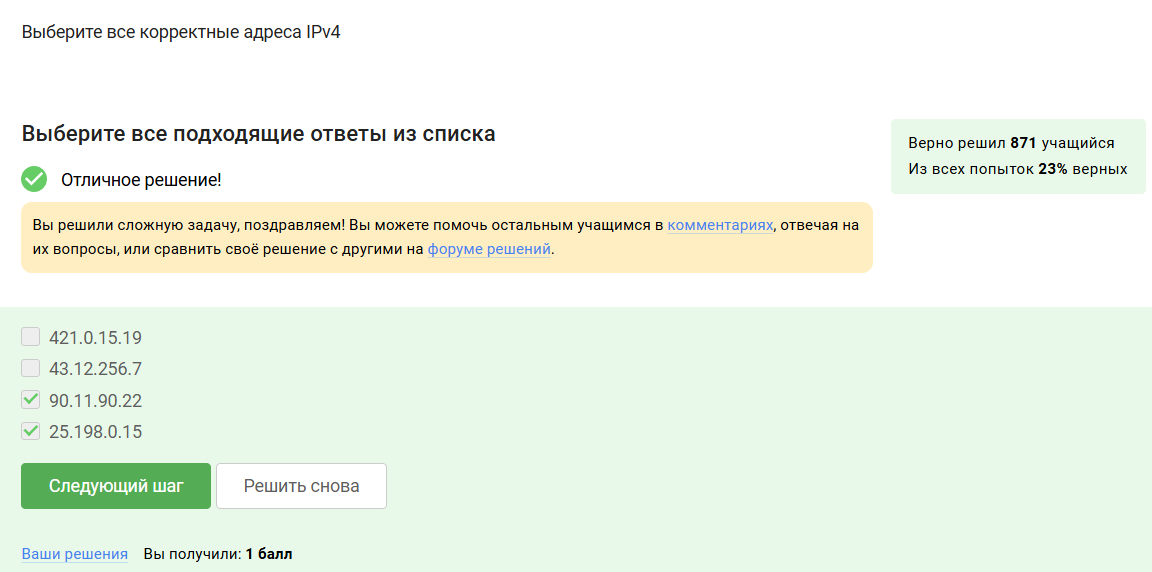


Рис. 3: Корректные IP

DNS - специальные сервера, которые сообщают устройству, какой IP привязан к домену (рис. 4).

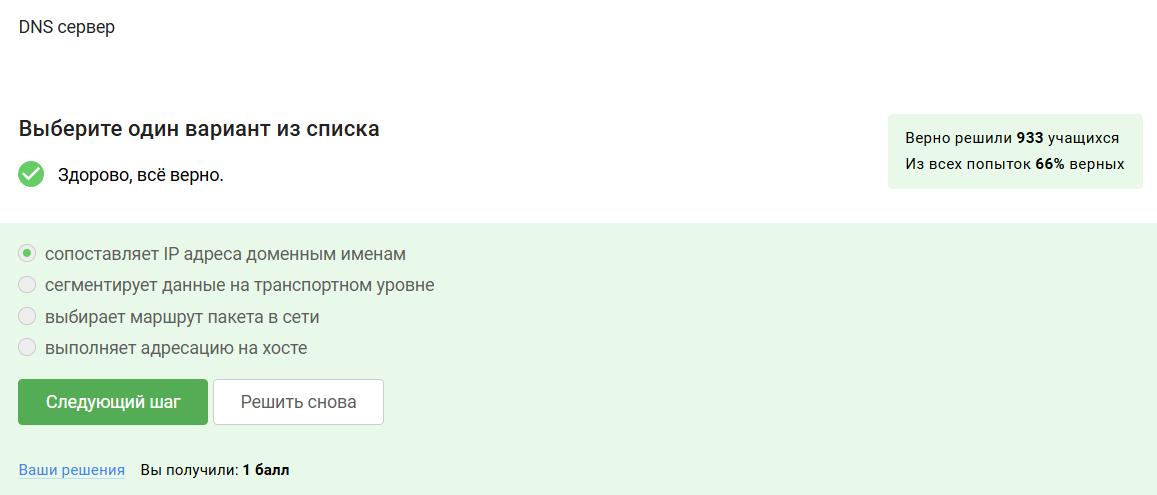


Рис. 4: Функция DNS

Последовательность протоколов определяется абстрактной моделью OSI (рис. 5).

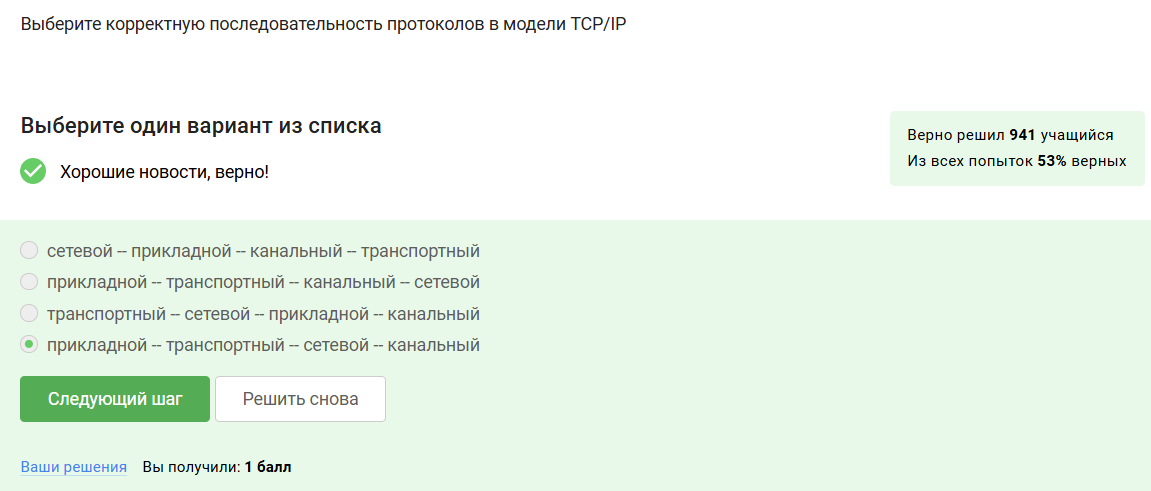


Рис. 5: Последовательность уровней TCP/IP

HTTP не шифрует данные (рис. 6).

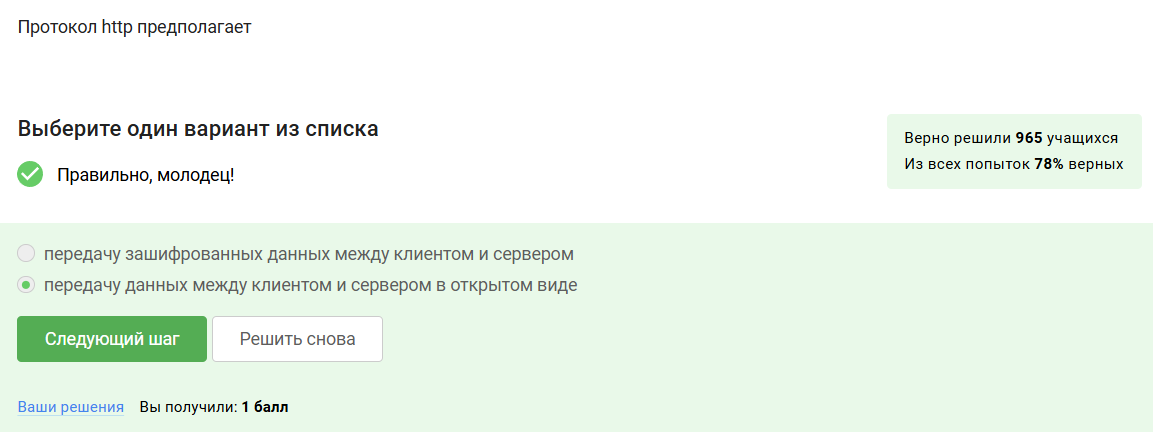


Рис. 6: HTTP

Для успешной передачи данных в протоколе HTTPS была реализована двухфазная передача, состоящая из рукопожатия и непосредственно передачи (рис. 7).

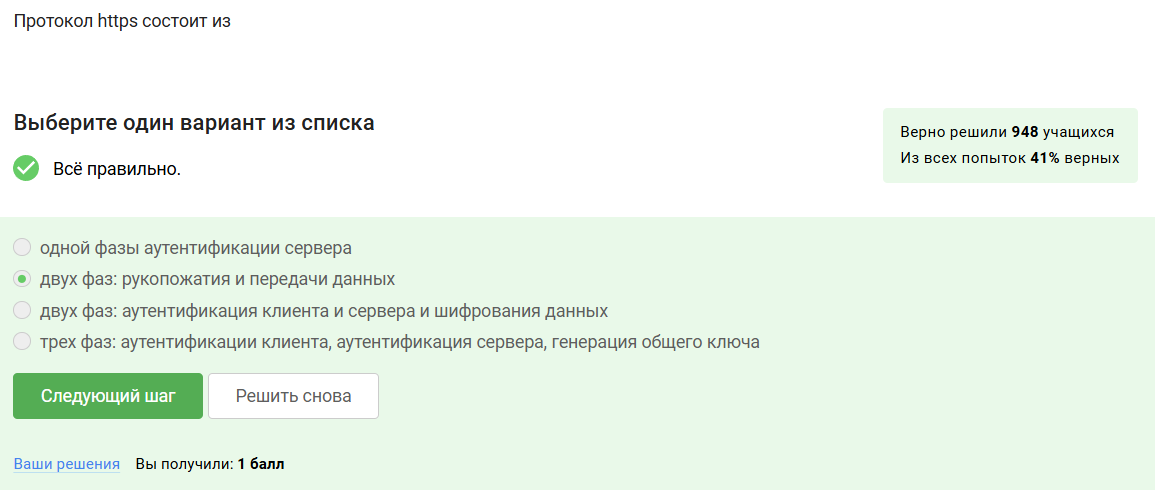


Рис. 7: HTTPS

В каждом устройстве определена своя версия протокола TLS. При общении выбирается наименьшая, поскольку присутствует поддержка обратной совместимости (рис. 8).

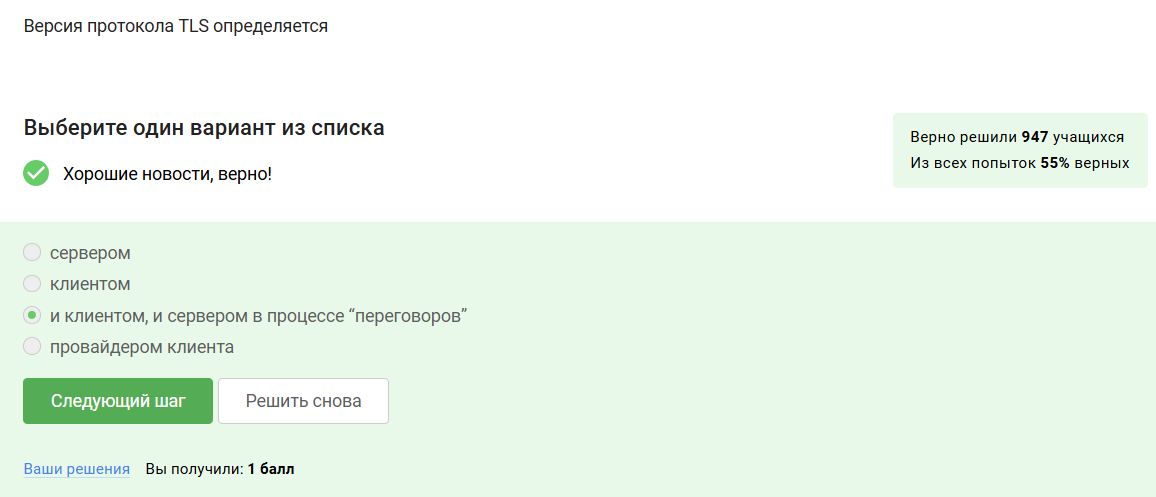


Рис. 8: TLS определяется всеми

Шифрование данных происходит после рукопожатия (рис. 9).

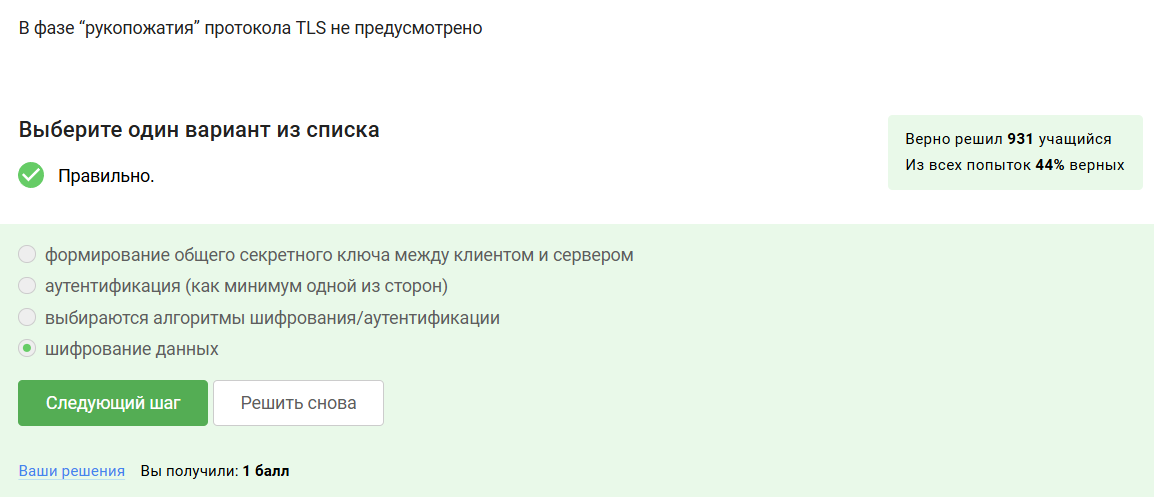


Рис. 9: TLS

Куки не хранят чувствительные данные, поскольку их не составляет труда перехватить (рис. 10).

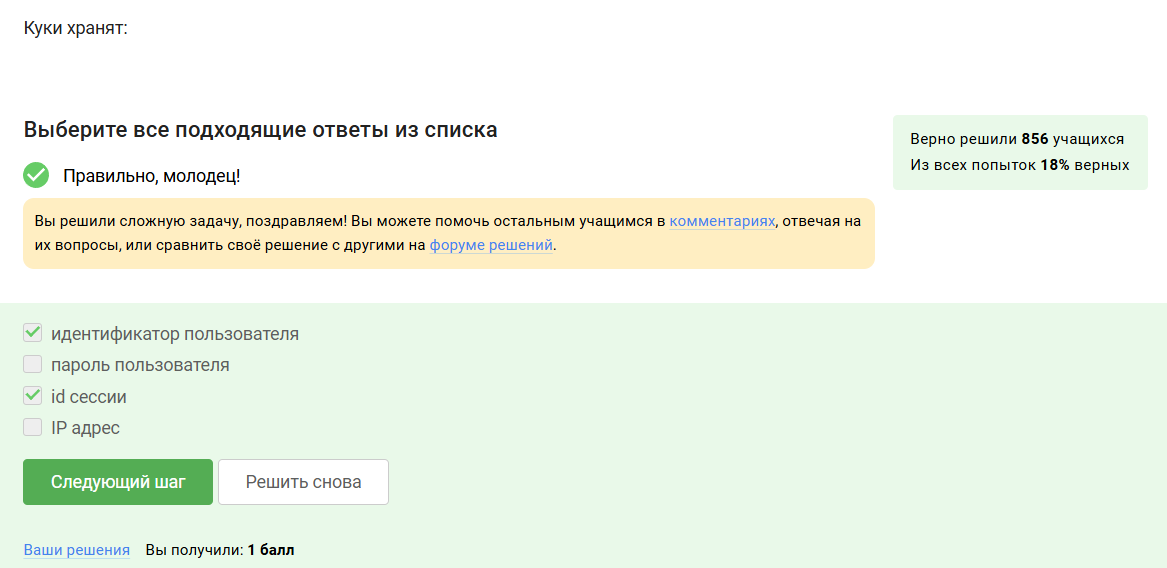


Рис. 10: Содержимое куки

Куки не используются для улучшения надёжности соединения, поскольку создавались с другой целью (рис. 11).

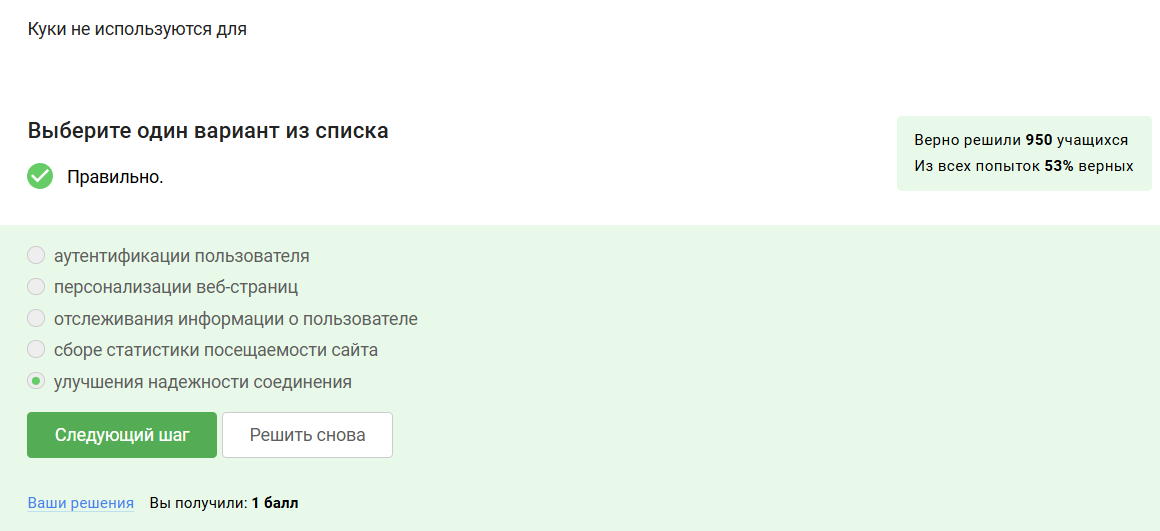


Рис. 11: Куки не используется для

Куки генерируются сервером в ходе общения с пользователем, затем отправляются этому пользователю и хранятся на его хосте (рис. 12).

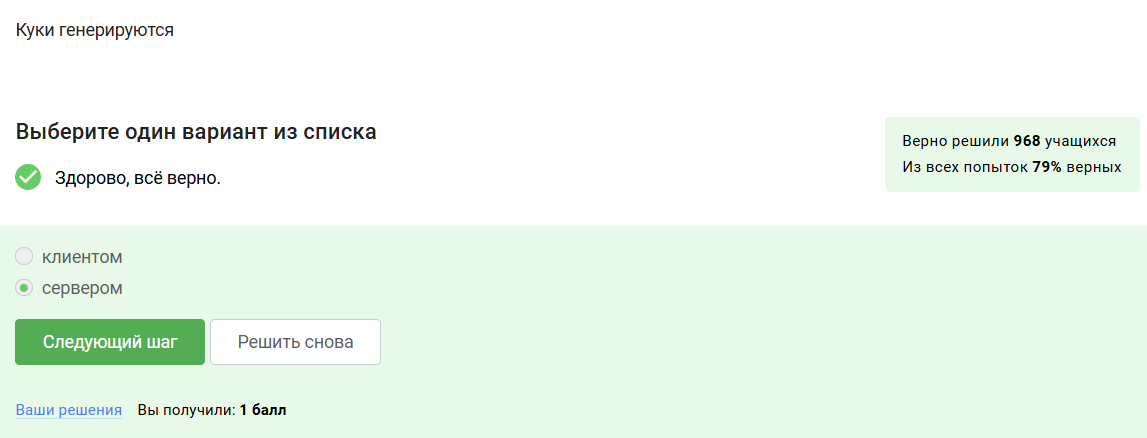


Рис. 12: Где генерируются куки

Сессионные куки хранятся до тех пор, пока эта сессия не завершится. Отсюда и название (рис. 13).

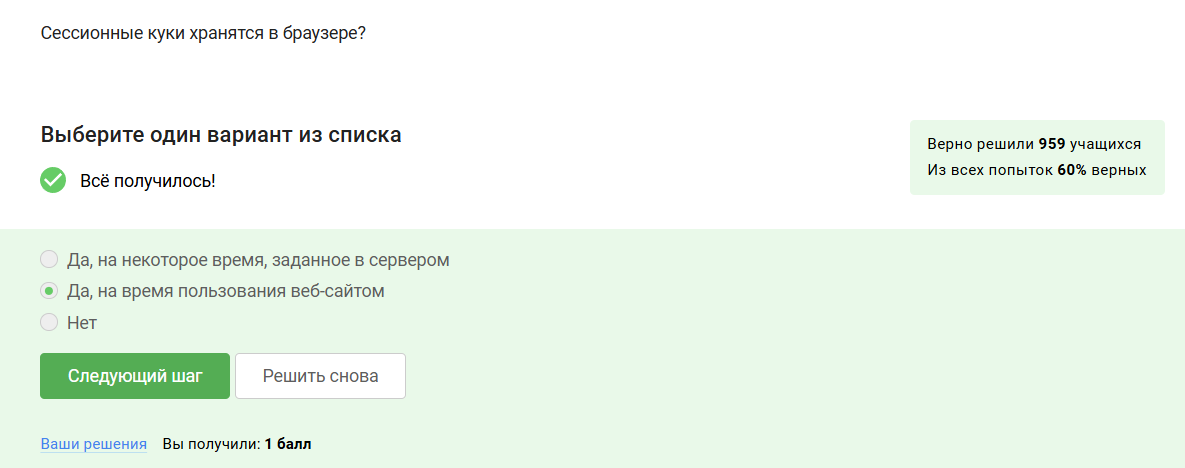


Рис. 13: Сессионные куки

В луковой маршрутизации используется 3 ноды (рис. 14).

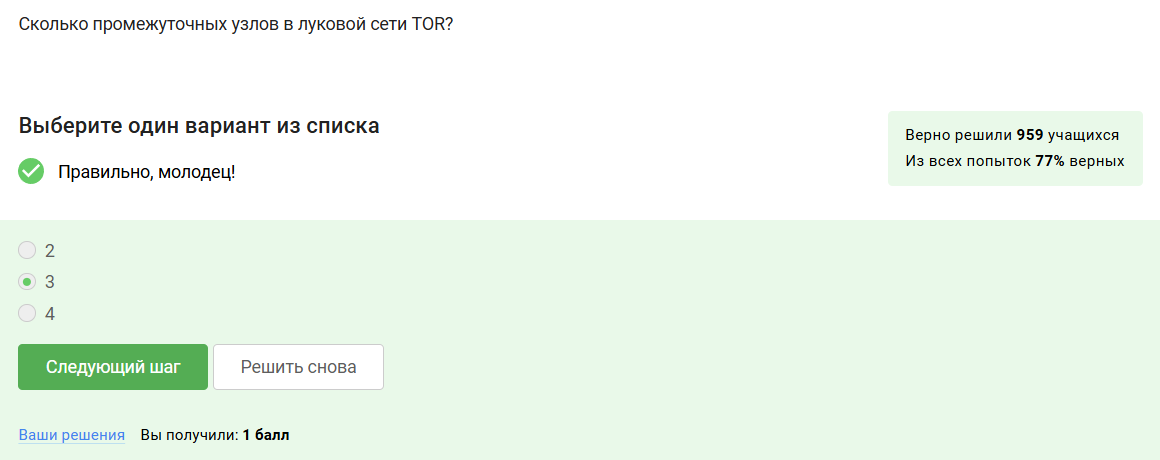


Рис. 14: Количество узлов TOR

Благодря тройному шифрованию адрес получателя известен только отправителю и выходной ноде. Таким образом ни одна нода не обладает полной информацией о всех участниках “общения” (рис. 15 и рис. 16).

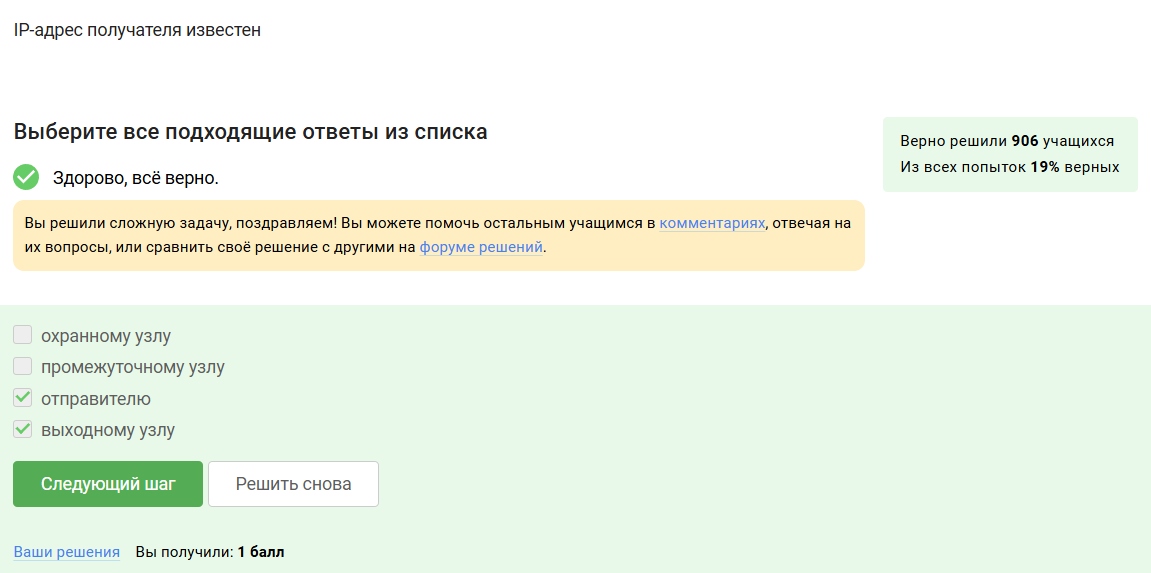


Рис. 15: Скрытие IP

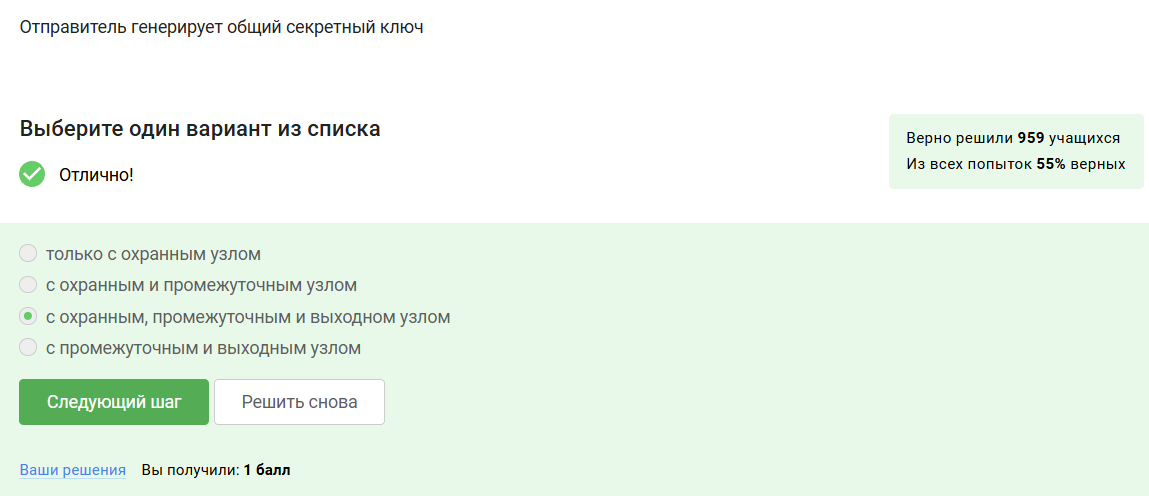


Рис. 16: Множественные ключи

Получателю необязательно использовать Tor при общении, поскольку всю дешифровку осуществляют ноды (рис. 17).

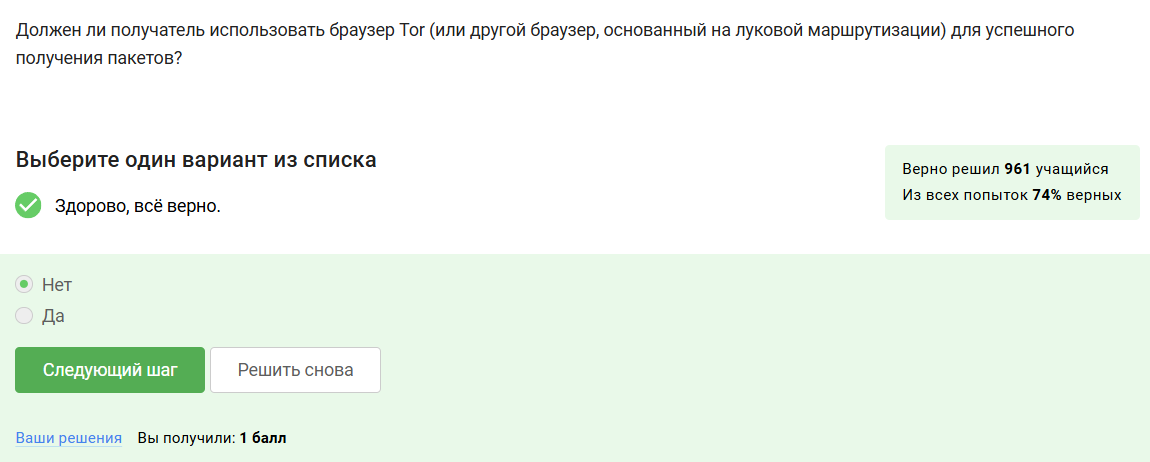


Рис. 17: Одностороннее использование TOR

Определение Wi-Fi (рис. 18).

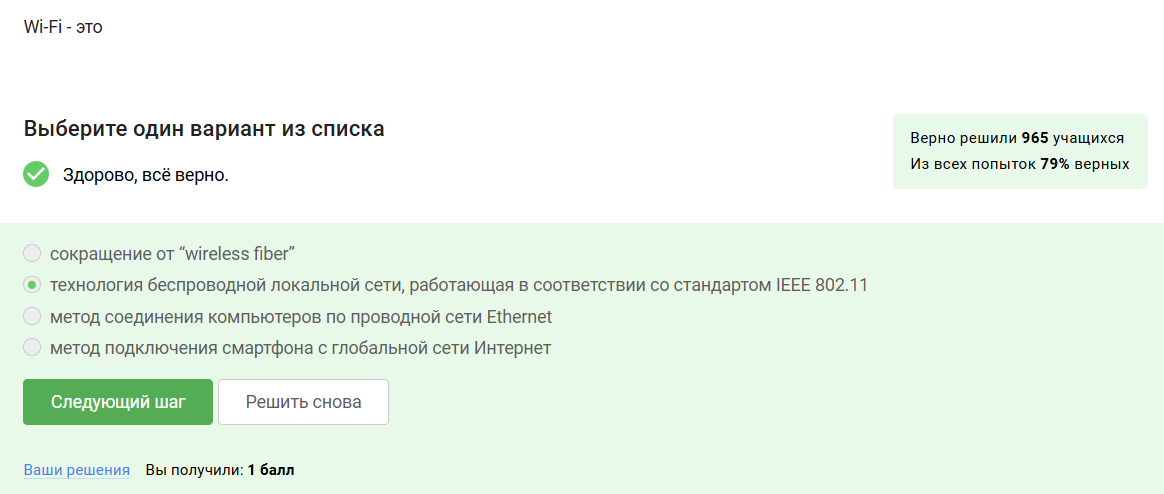


Рис. 18: Определение Wi-Fi

Wi-Fi работает на канальном уровне, поскольку связывает локальные устройства с интернетом (рис. 19).

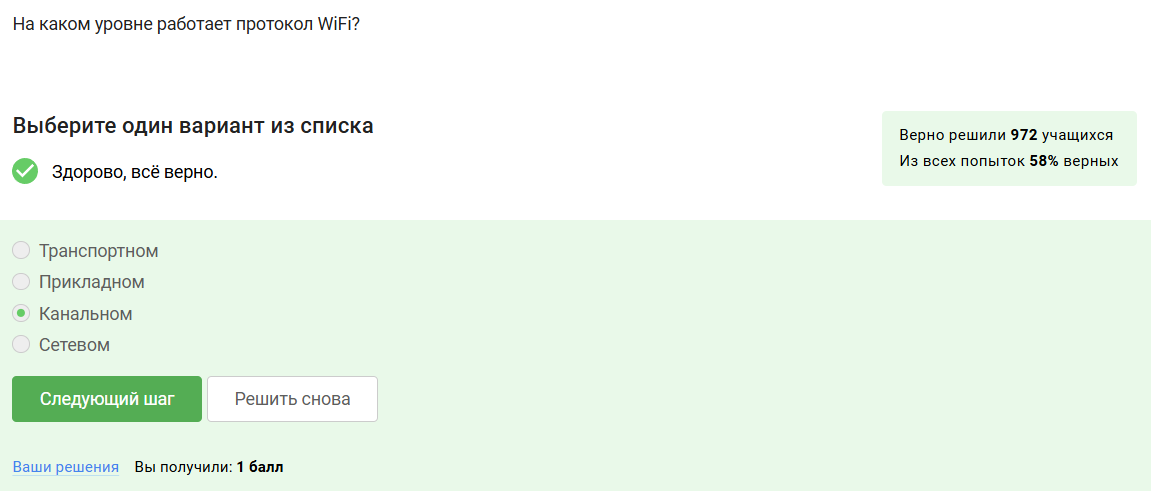


Рис. 19: Уровень работы Wi-Fi

WEP считается устаревшим и небезопасным, потому что его ключ шифрования ограничен 40 битами (рис. 20).

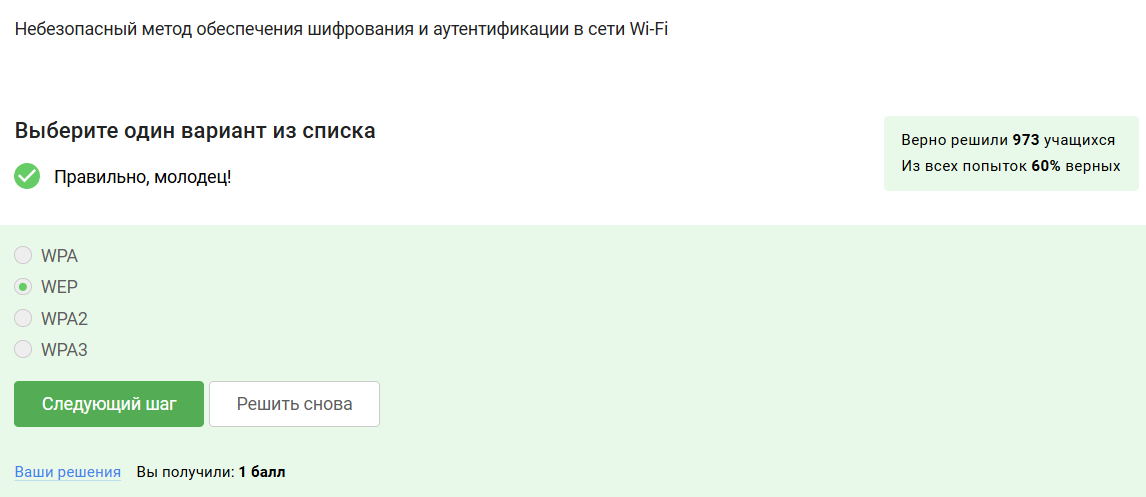


Рис. 20: Небезопасный метод шифрования

Данные между хостом и роутером передаются в зашифрованном виде, дабы исклюлчить использование данных при перехвате (рис. 21).

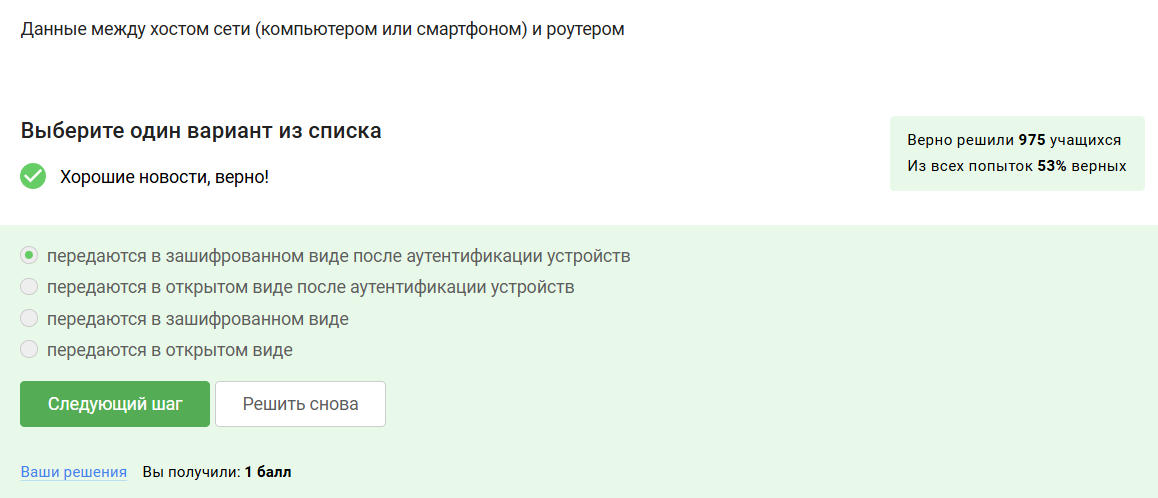


Рис. 21: Передача данных Wi-Fi

Для домашней сети используется WPA2 Personal, поскольку это удобнее для пользователей, ведь Enterprise использует динамические ключи (рис. 22).

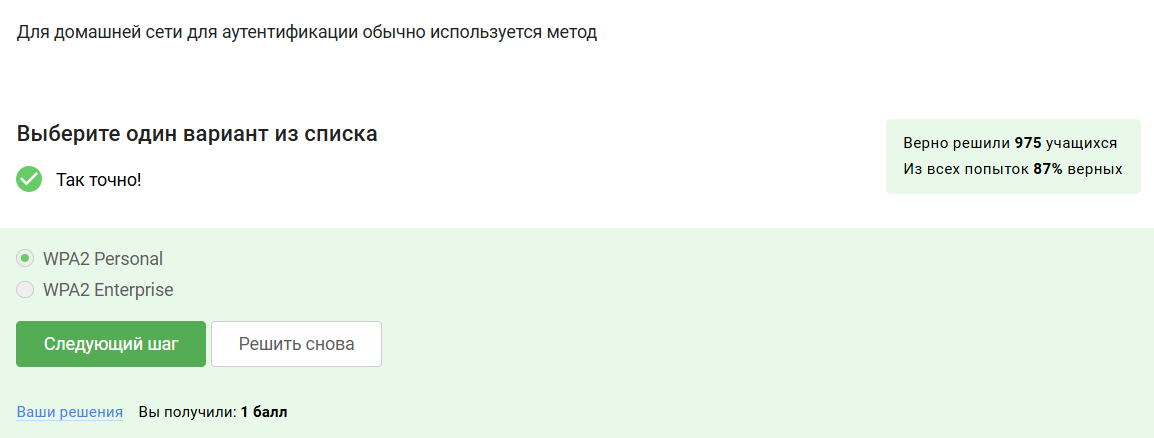


Рис. 22: Метод аутентификации в домашней сети

## 3.2 Прохождение второго этапа

Загрузочный сектор диска можно и рекомендуется шифровать (рис. 23).

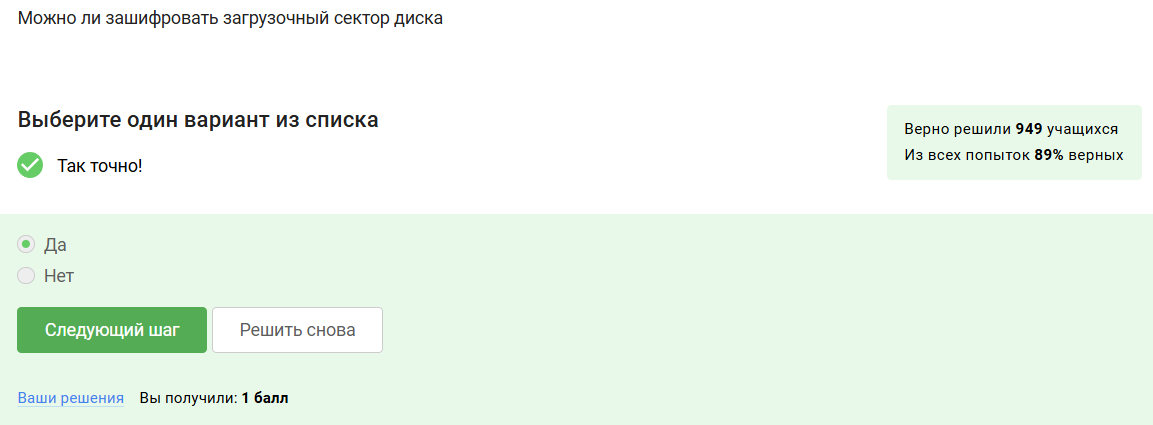


Рис. 23: Возможность шифровки загрузочного сектора диска

Шифрование дисков симметричное, поскольку оно гораздо быстрее асимметричного, что идёт в плюс пользователям (рис. 24).

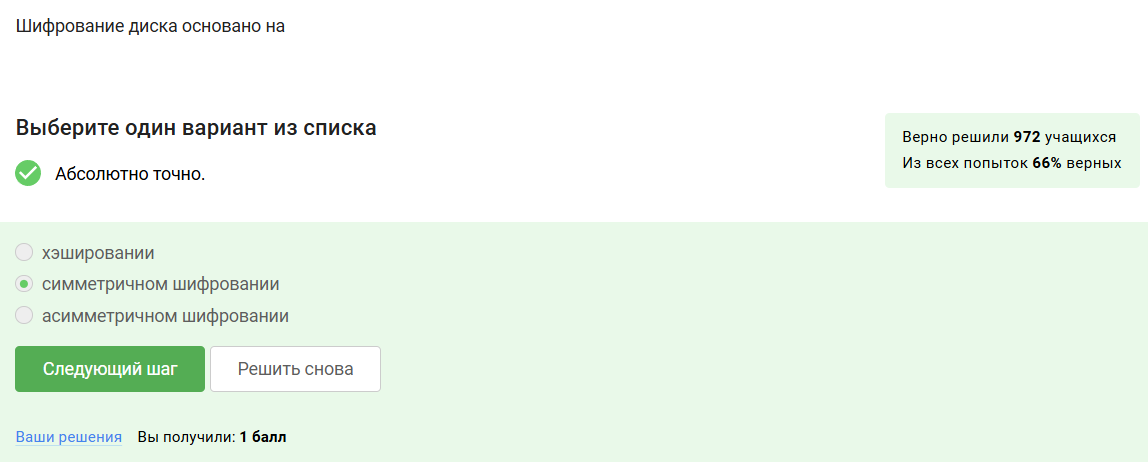


Рис. 24: Симметричное шифрование диска

BitLocker установлен в Windows по умолчанию, а VeraCrypt является наиболее популярной сторонней программой для шифрования дисков (рис. 25).

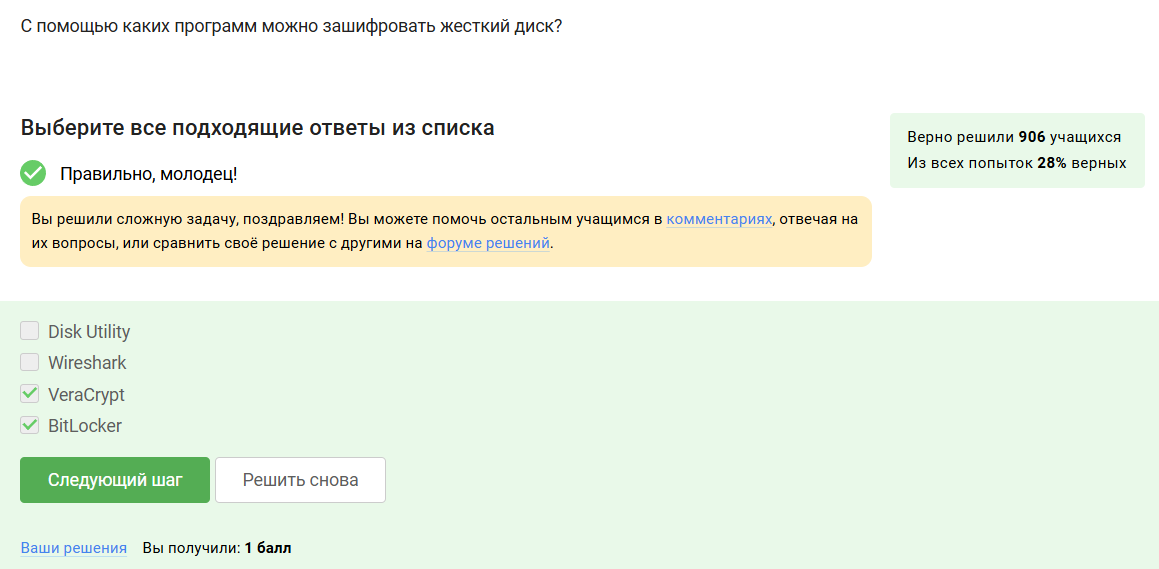


Рис. 25: Программы для шифрования диска

Пароли должны состоять из цифр, символов и спец. символов, чтобы подобрать было труднее (рис. 26).

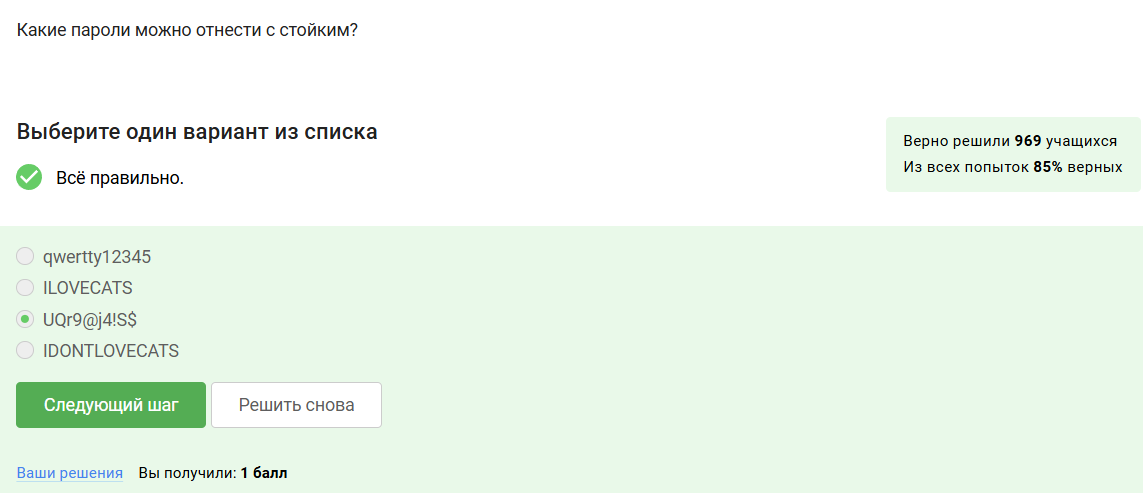


Рис. 26: Устойчивые к брутфорсу пароли

Пароли безопасно хранить в менеджере паролей, а пароль от него самого нужно хранить на нецифровом носителе или в голове (рис. 27).

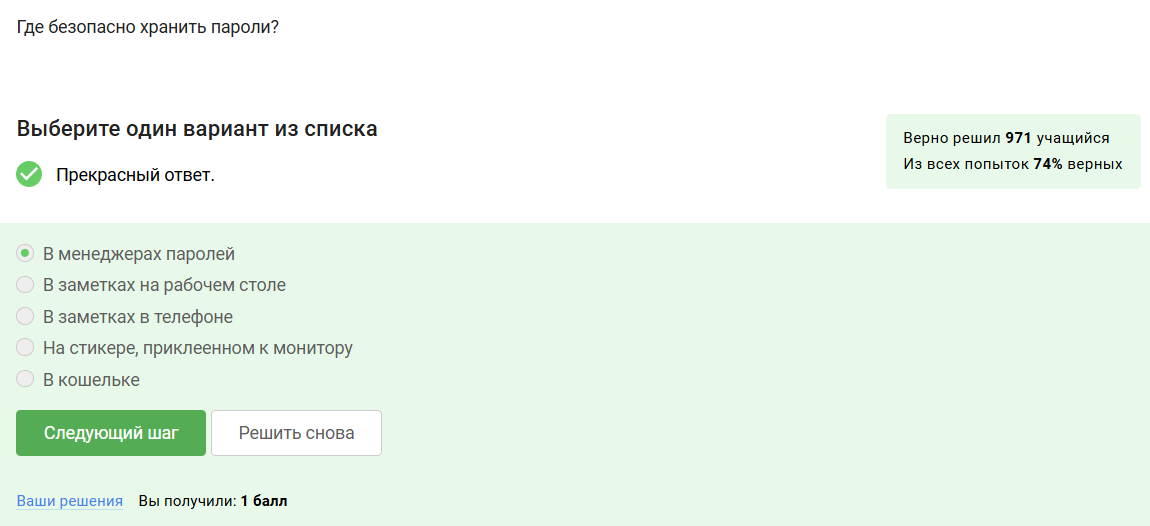


Рис. 27: Безопасное место для хранения паролей

Капча используется для защиты от брутфорса ботами (рис. 28).

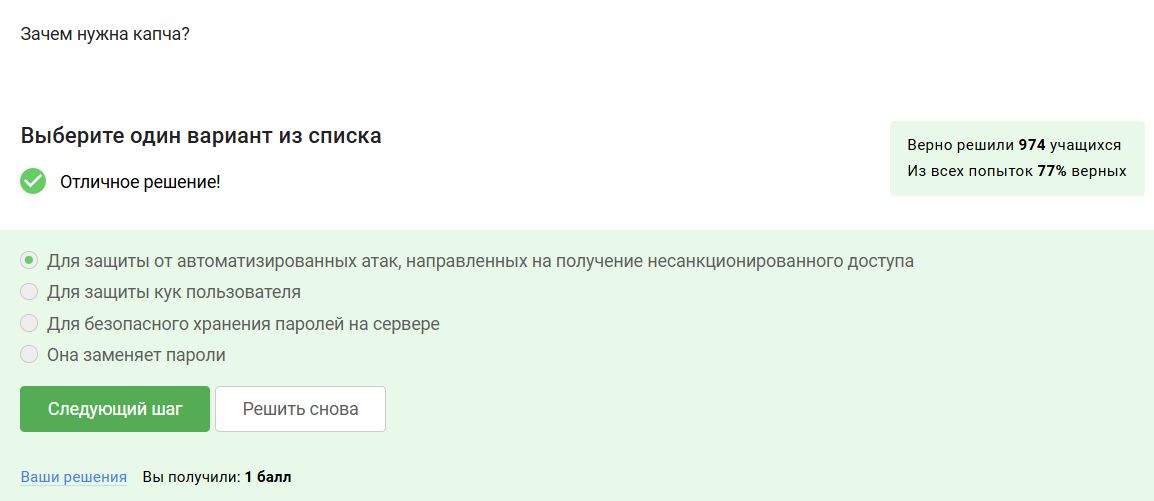


Рис. 28: Капча

Хэширование паролей нужно, чтобы сделать потенциальные утечки баз данных менее опасными (рис. 29).

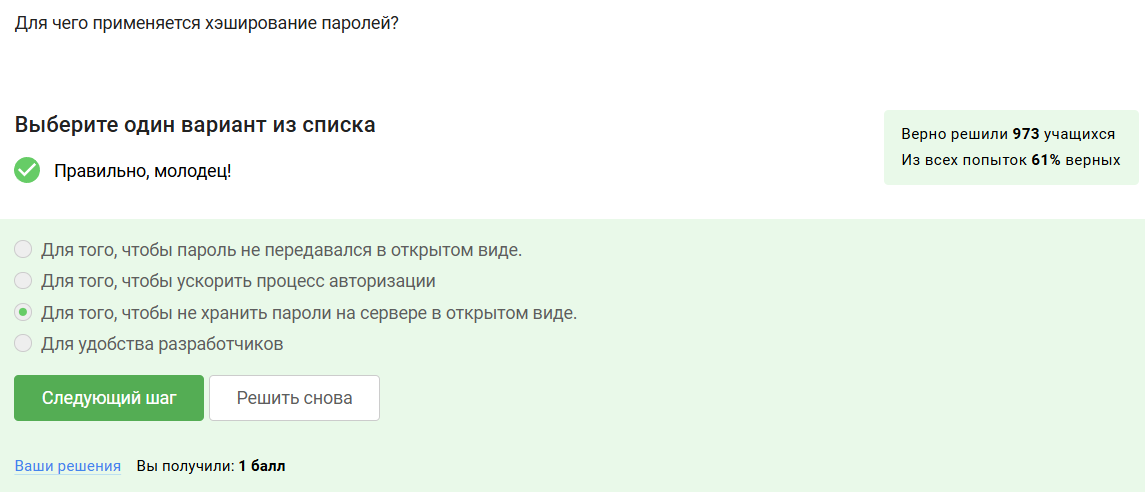


Рис. 29: Хэширование паролей

Соль помогает изменить хэш слабого пароля, но это не защищает от перебора (рис. 30).

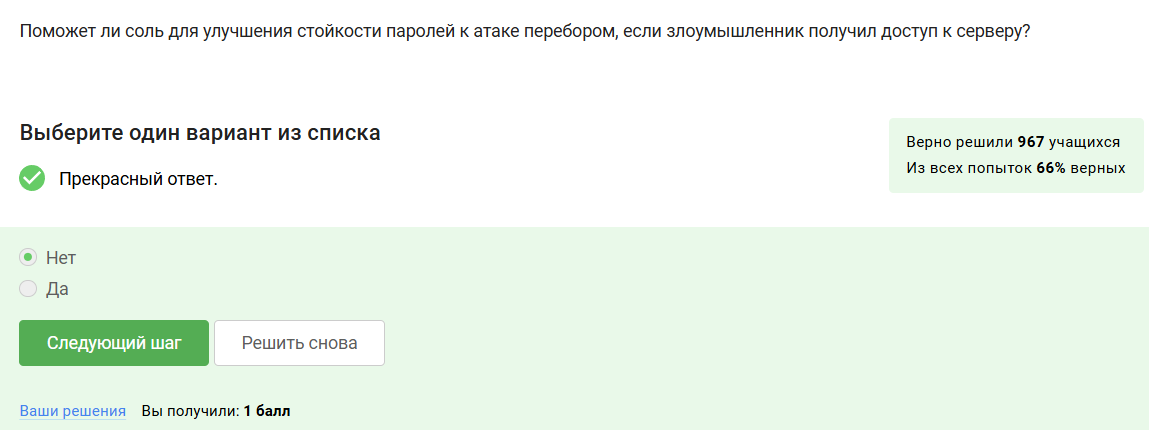


Рис. 30: Соль

Все методы, которые усложняют пароль или замедляют возможность перебора, помогут защитить от брутфорса (рис. 31).

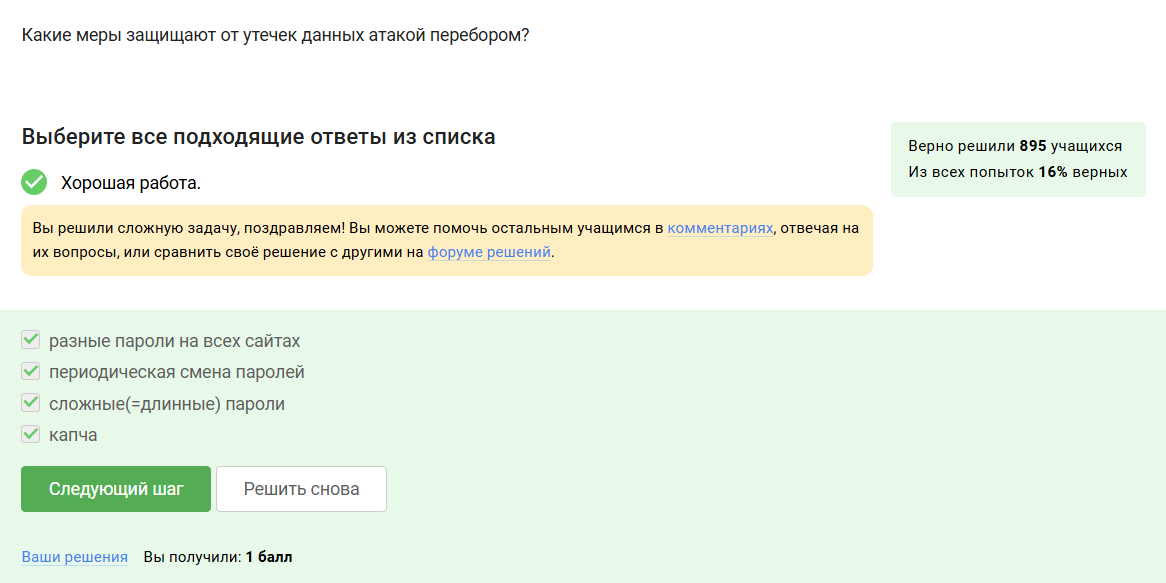


Рис. 31: Методы защиты данных от утечек

Фишинговые ссылки похожи на настоящие, но имеют в пути другие доменные зоны или как-то видоизменяют сам путь (рис. 32).

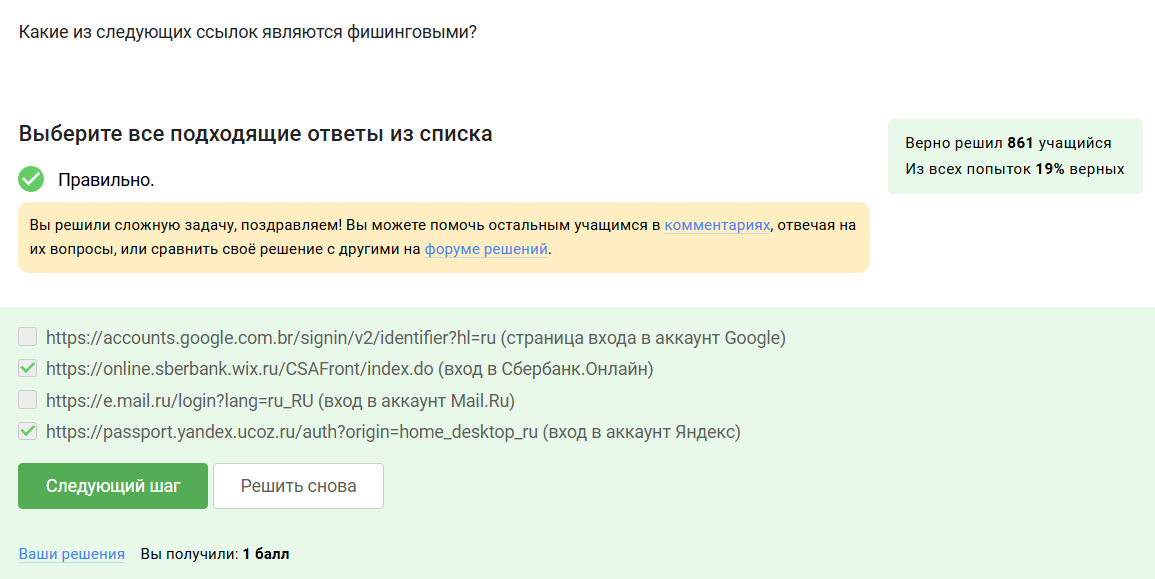


Рис. 32: Фишинговые ссылки

Фишинговый имейл может прийти от знакомого адреса, если используется слабый протокол почтового сервиса (рис. 33).

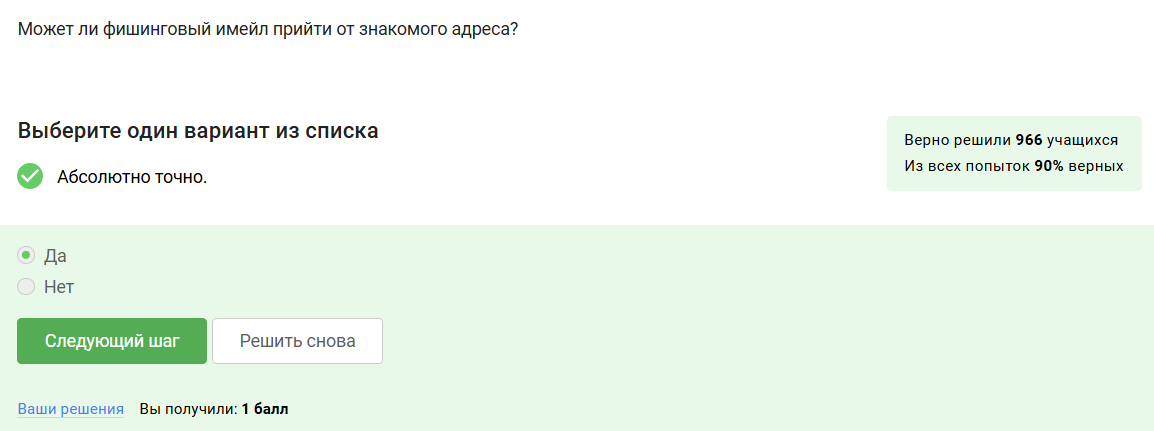


Рис. 33: Фишинговый имейл

Спуфинг уже практически неактуален, поскольку придуманы более защищённые протоколы отправки Email (рис. 34).

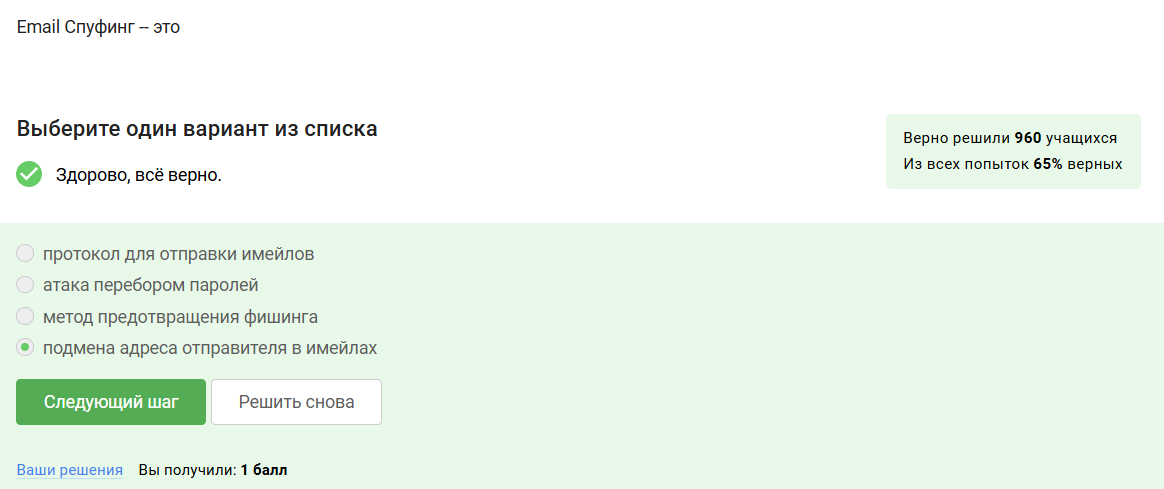


Рис. 34: Имейл спуфинг

Троян маскирутеся под легитимную программу и пытается получить контроль над устройством (рис. 35).

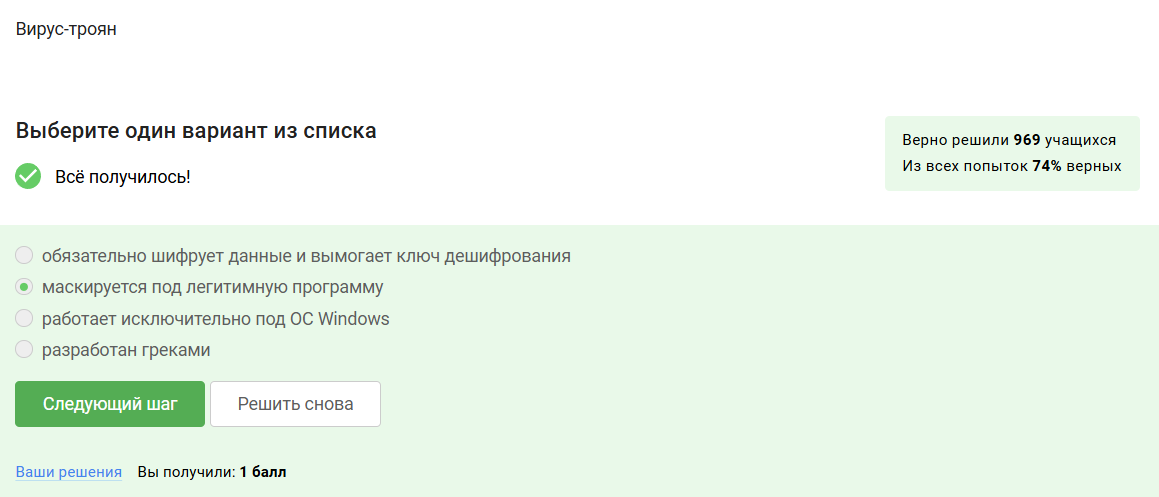


Рис. 35: Вирус-троян

Ключ шифрования в протоколе Signal генерируется при отправке первого сообщения пользователем (рис. 36).

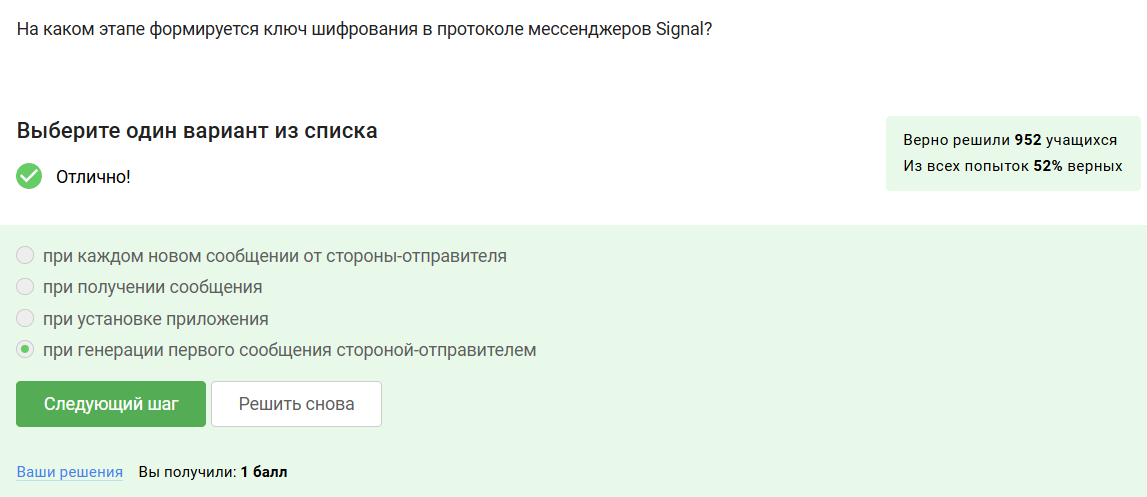


Рис. 36: Signal

Сквозное шифрование использует пару ключей для конфеденциального общения узлов (рис. 37).

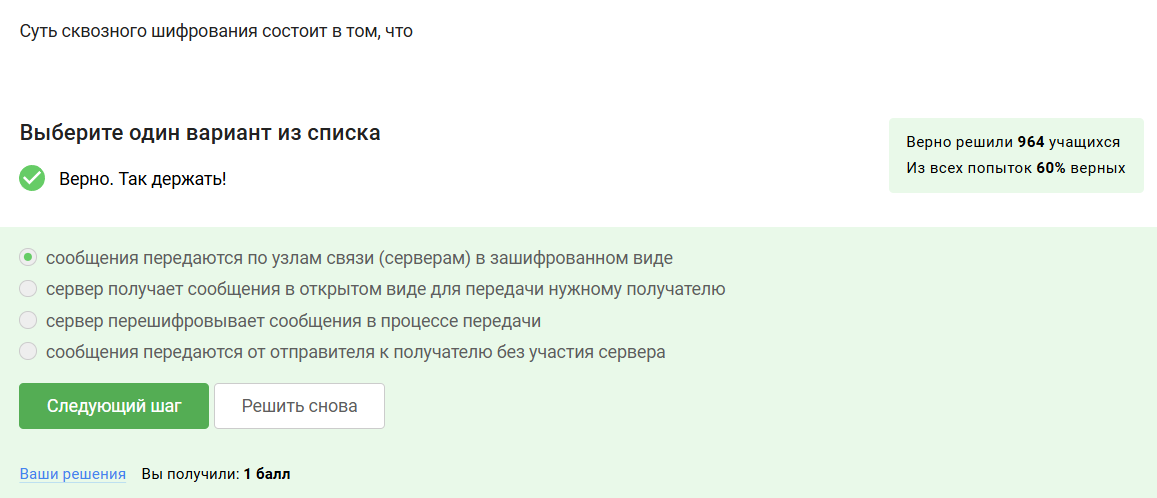


Рис. 37: Суть сквозного шифрования

Для правильной работы криптографических примитивов требуется наличие пары ключей у всех участников общения (рис. 38).

## 3.3 Прохождение третьего этапа

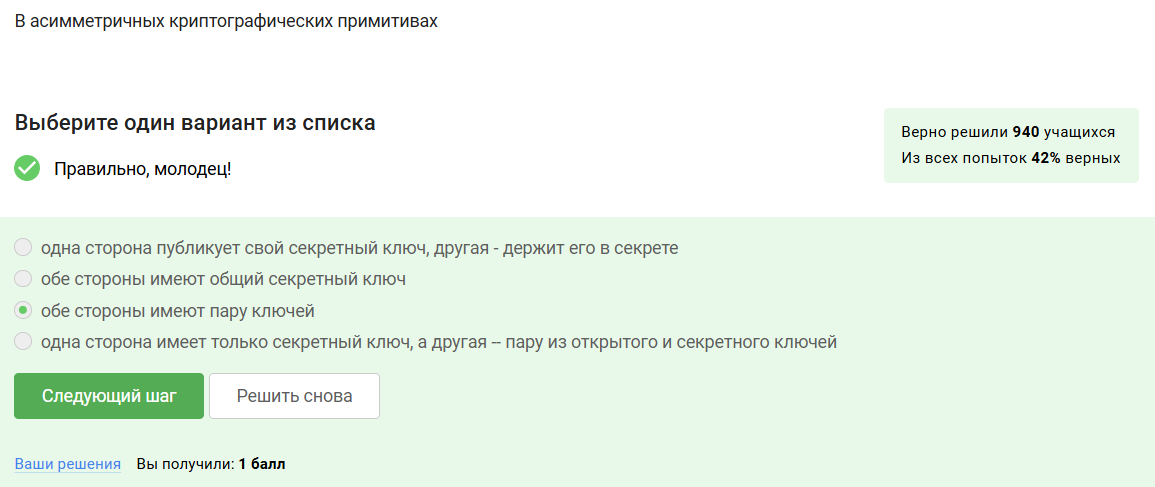


Рис. 38: Ассимитричные криптографические примитивы

Криптографическая хэш-функция не обеспечивает конфиденциальность захэшированных данных, поскольку её невозможно вычислить в обратном порядке (рис. 39).

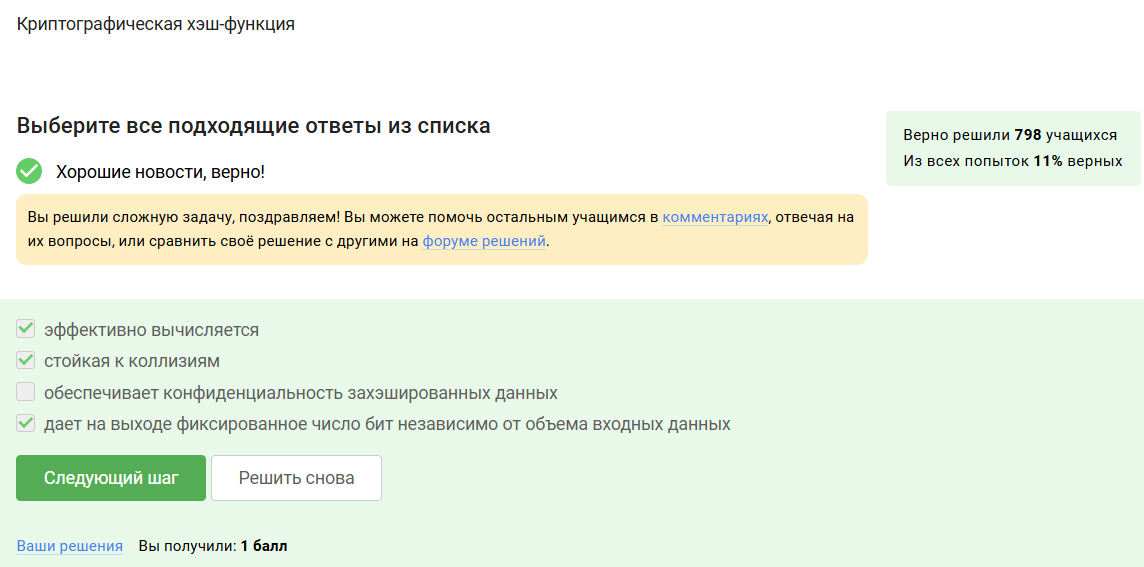


Рис. 39: Криптографическая хэш-функция

Перечисление алгоритмов цифровой подписи (рис. 40).

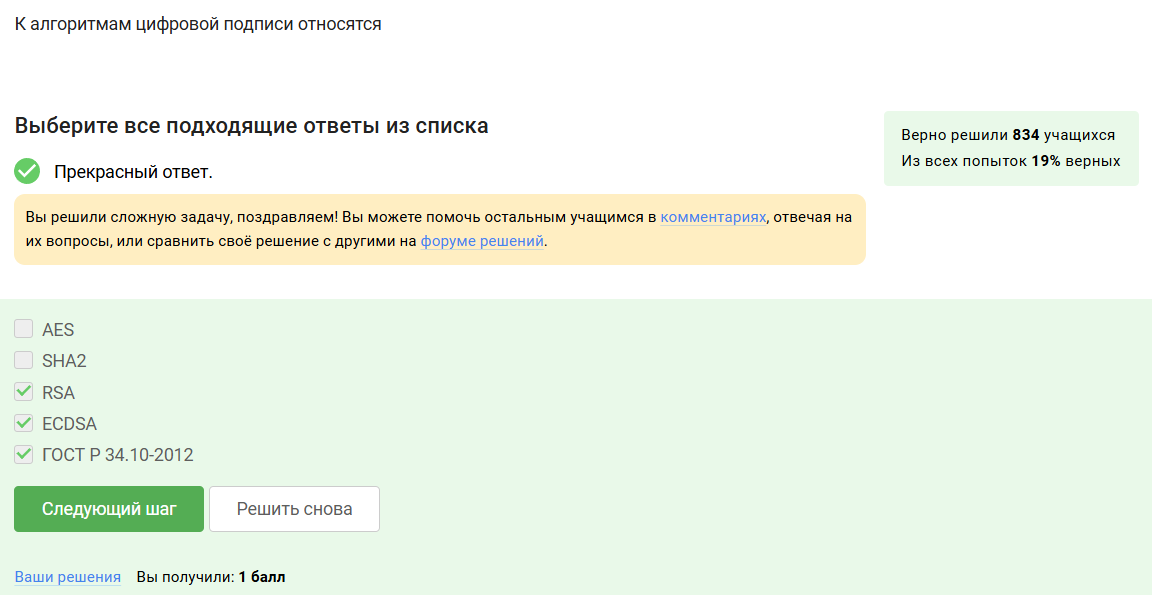


Рис. 40: Алгоритмы цифровой подписи

Код аутентификации сообщения относится к симметричным примитивам, поскольку используется симметричное шифрование (рис. 41).

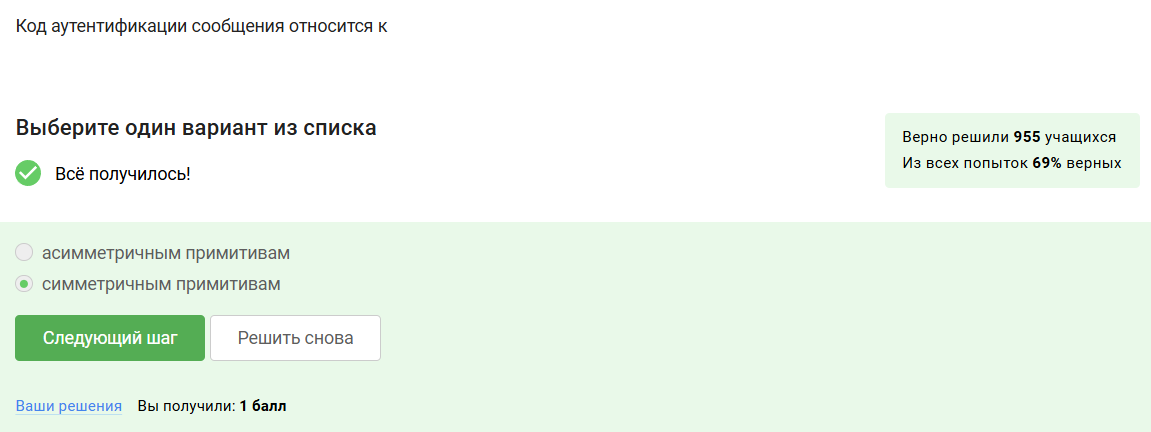


Рис. 41: Код аутентификации сообщения

Определение обмена ключами Диффи-Хеллмана (рис. 42).

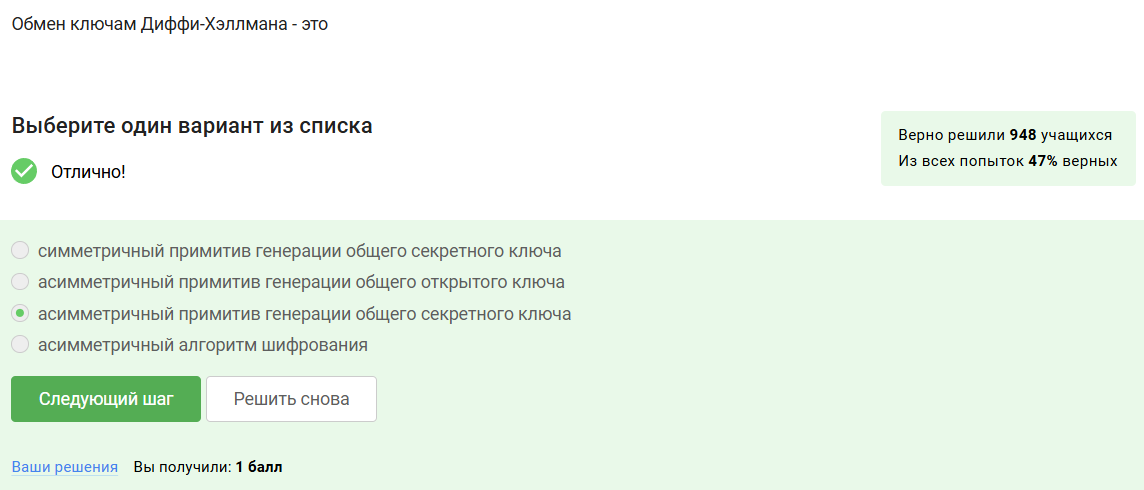


Рис. 42: Обмен ключами Диффи-Хеллмена

Протокол электронной цифровой подписи отностися к протоколам с публичным ключом, ведь пользователи могут проверить подпись этим ключом (рис. 43).

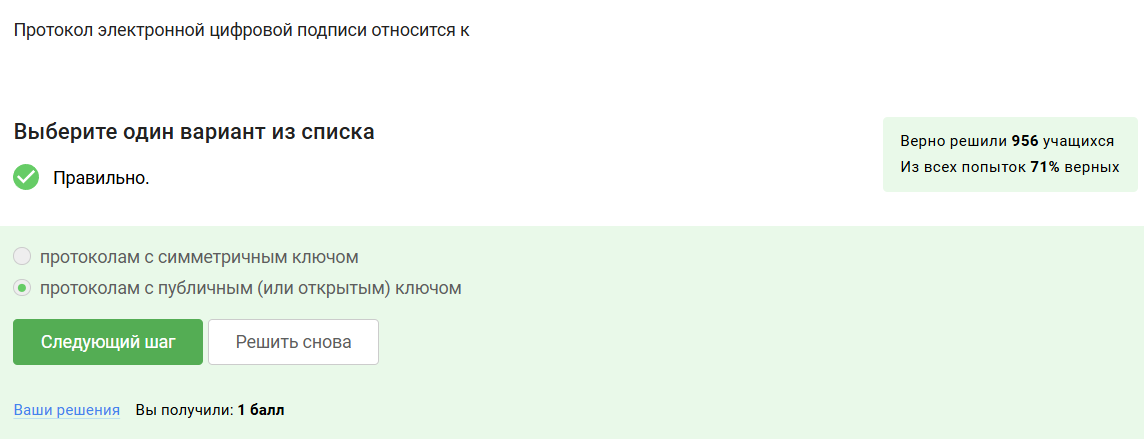


Рис. 43: Протокол электронной цифровой подписи

Механизм работы верификации ЭЦП (рис. 44).

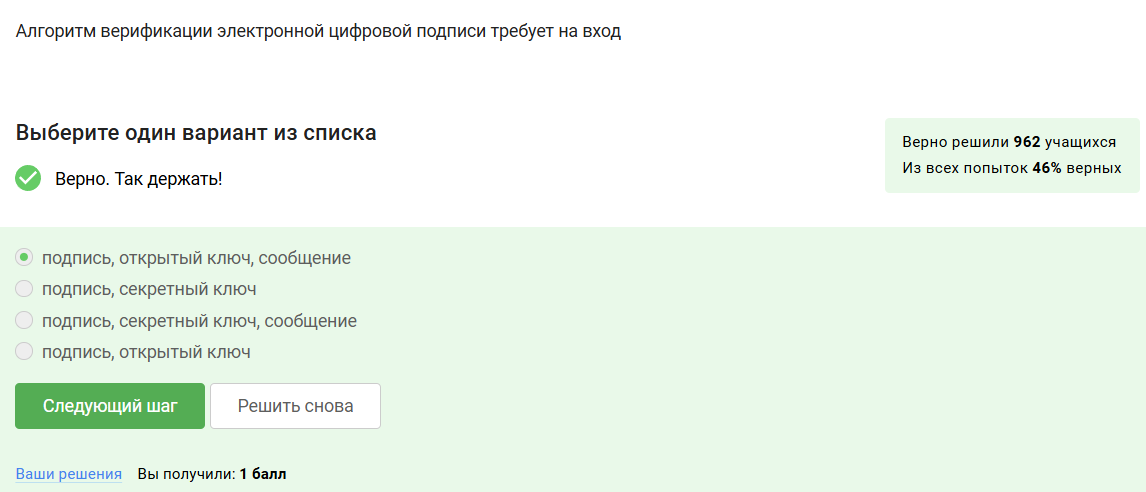


Рис. 44: Верификация ЭЦП

ЭПС не обеспечивает конфиденциальность, поскольку содержит информацию о пользователе, сделавшем эту подпись (рис. 45).

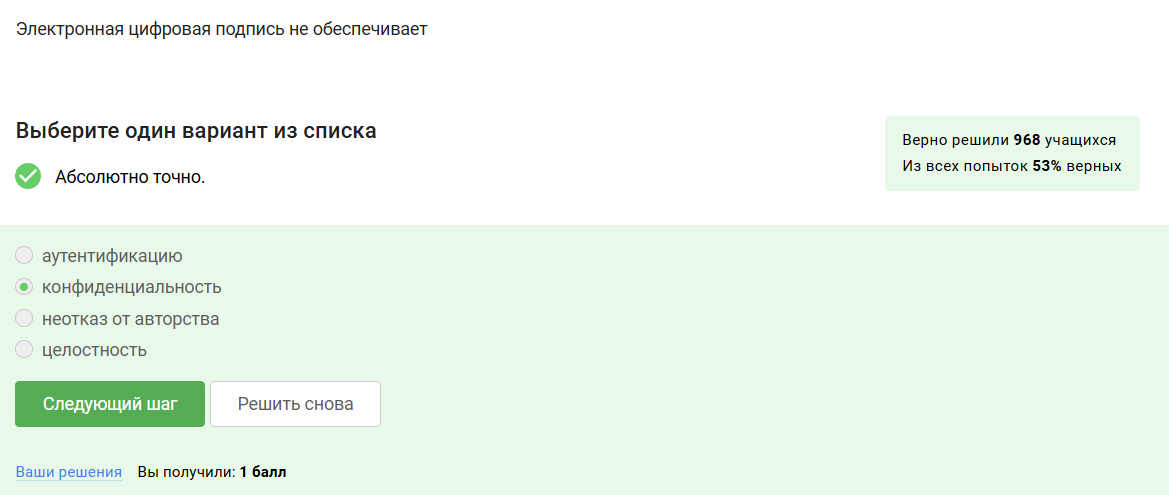


Рис. 45: ЭЦП не обеспечивает

Усиленная квалифицированная электронная подпись при отправки налоговой отчётности в ФНС требуется для обеспечения юридической значимости, безопасности и достоверности (рис. 46).

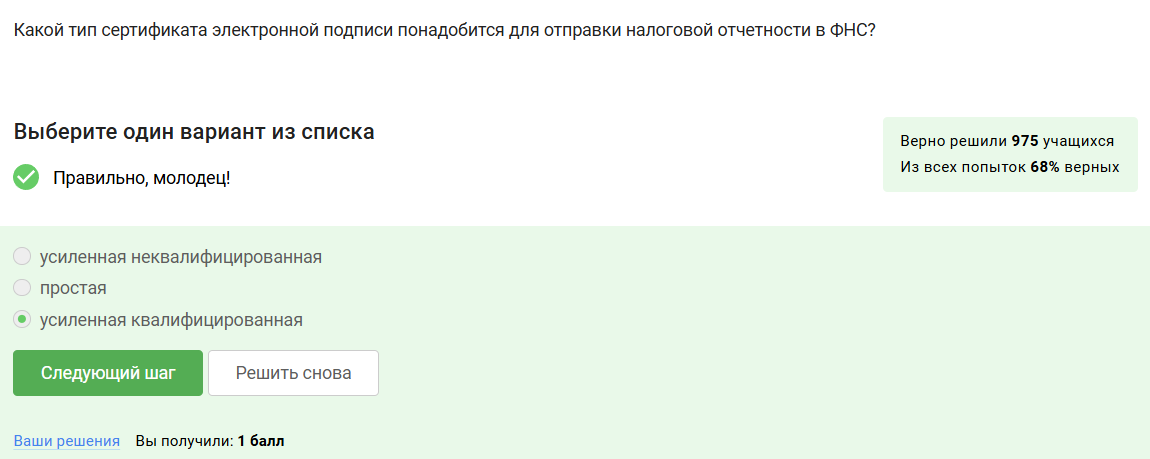


Рис. 46: Тип ЭЦП для отправки налоговой отчётности в ФНС

Сертификаты для доменов выдают сертифицированные центры (рис. 47).

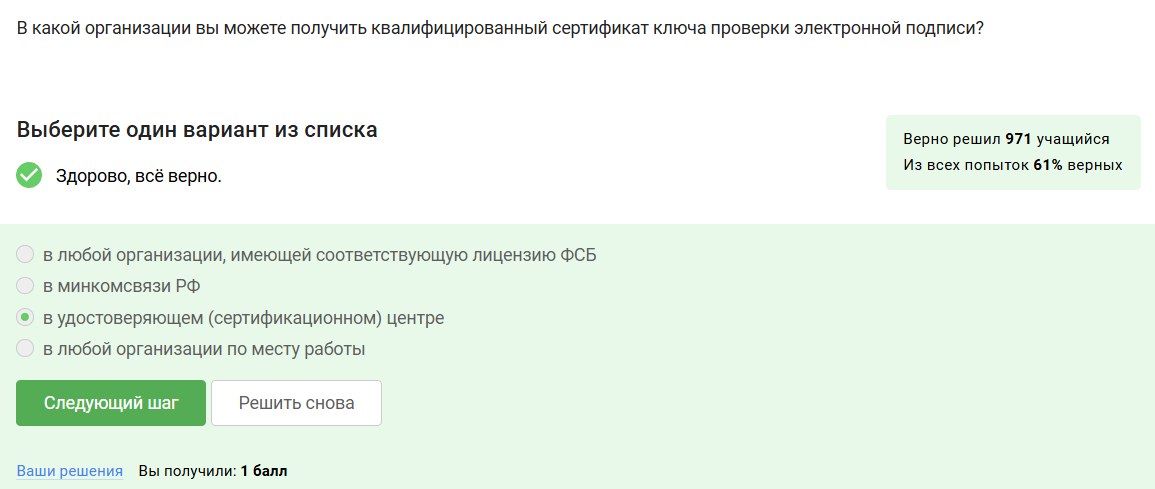


Рис. 47: CA

Список платёжных систем (рис. 48).

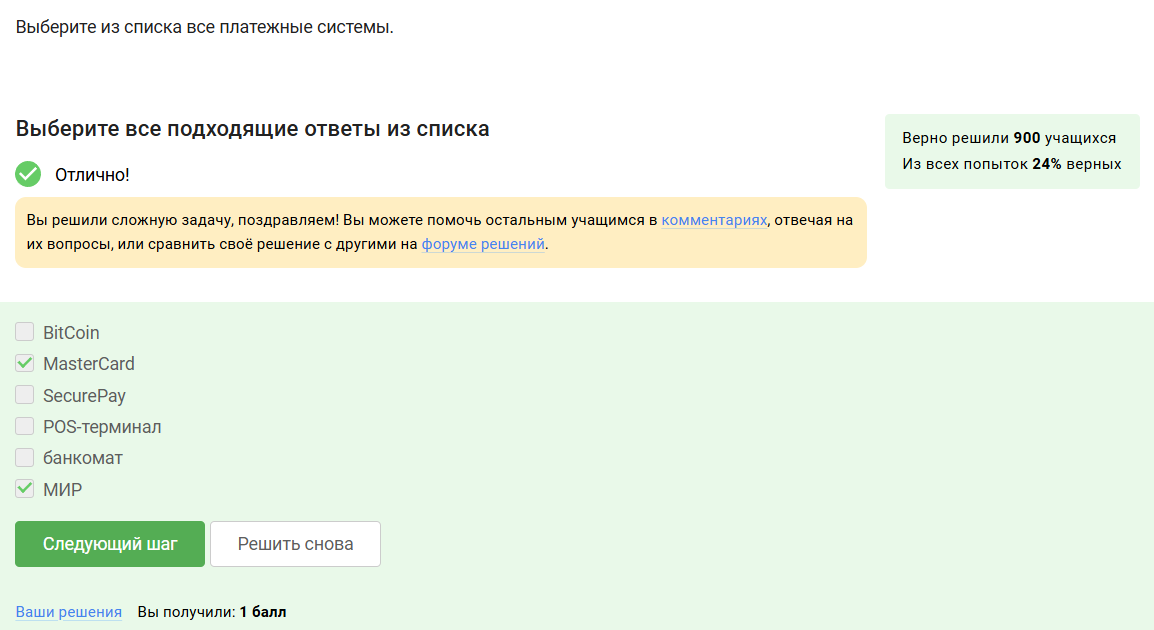


Рис. 48: Платёжные системы

Многофакторная аутентификация подразумевает собой ввод нескольких ключей для доступа к информации (рис. 49).

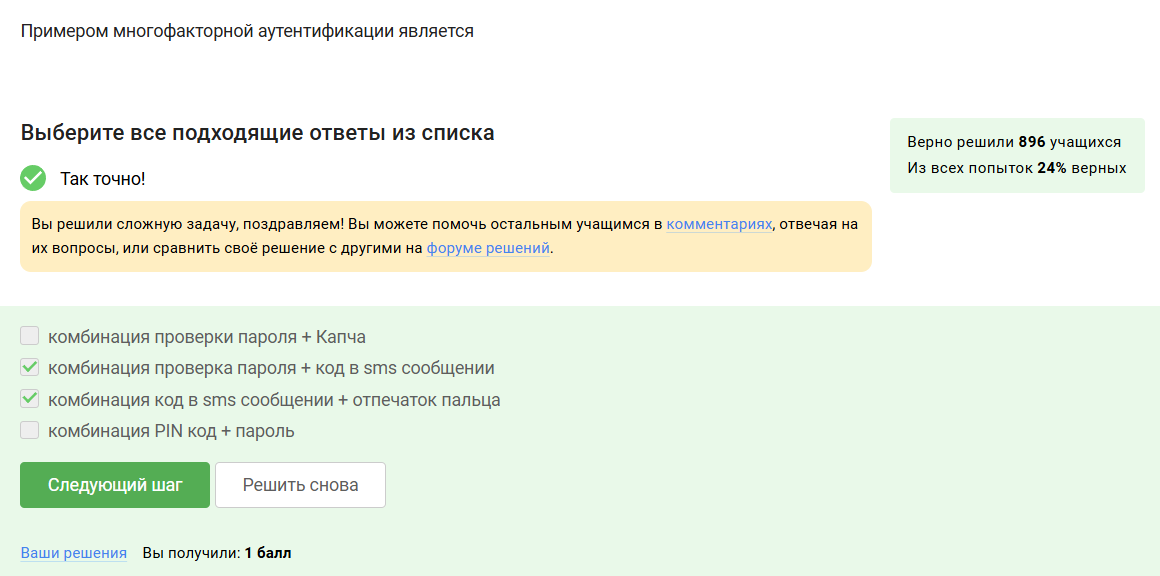


Рис. 49: Примеры многофакторной аутентификации

Для безопасности платёжных счетов пользователей при онлайн оплатах сегодня используется многофакторная аутентификация перед банком-эмитентом (рис. 50).

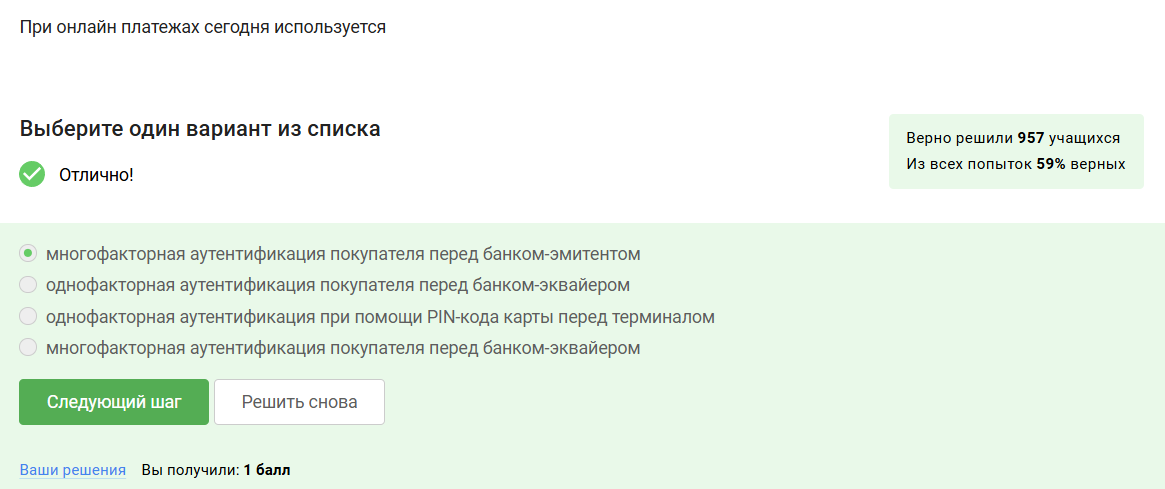


Рис. 50: Аутентификация при онлайн платежах

Устройство proof of work (рис. 51).

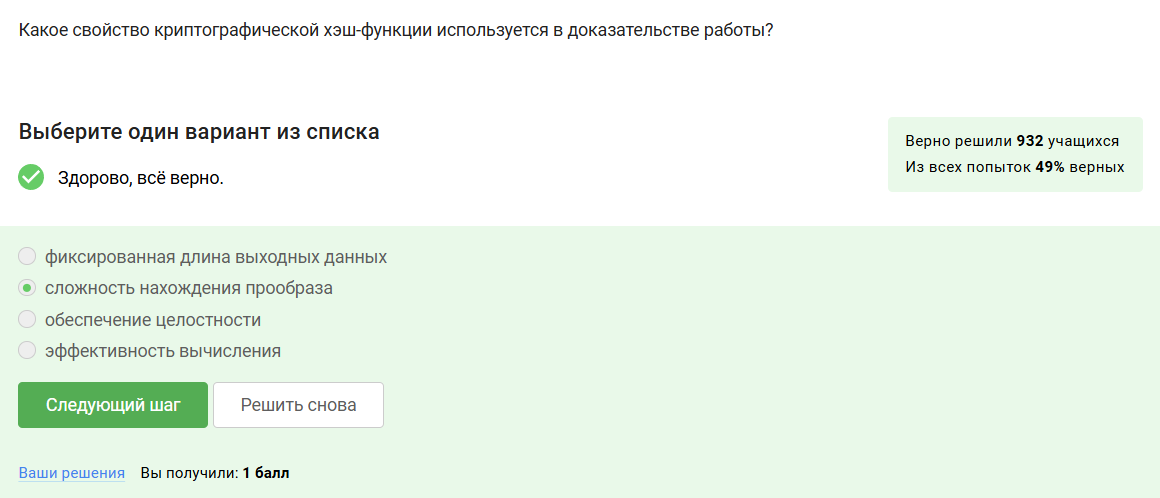


Рис. 51: Proof of work

Консенсус позволяет участникам блокчейна согласовывать операции без доверия друг к другу (рис. 52).

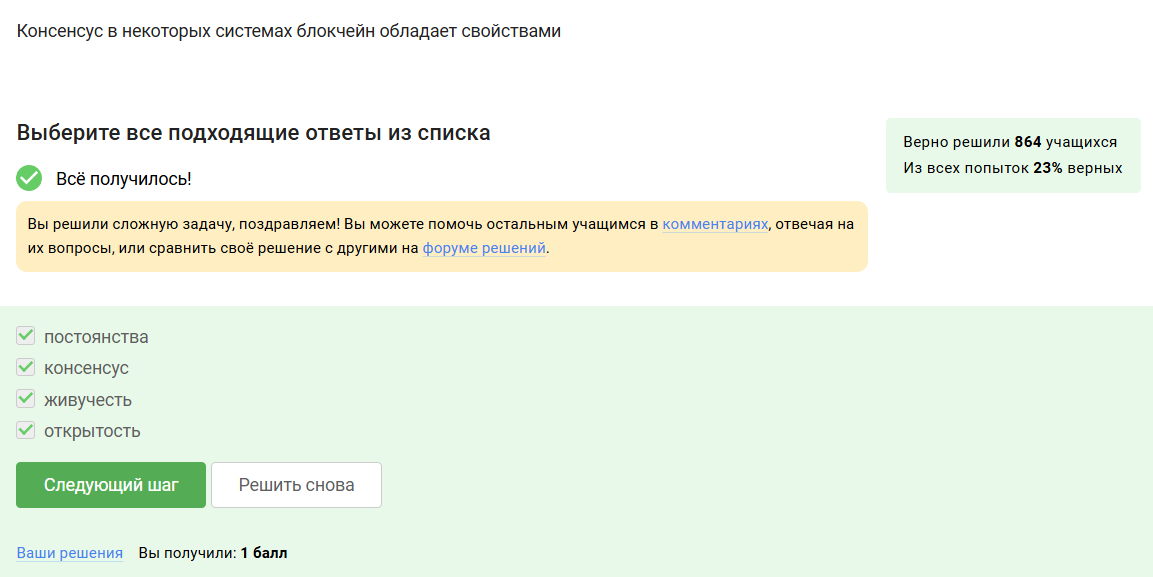


Рис. 52: Consensus

Все участники блокчейна хранят цифровую подпись (рис. 53).

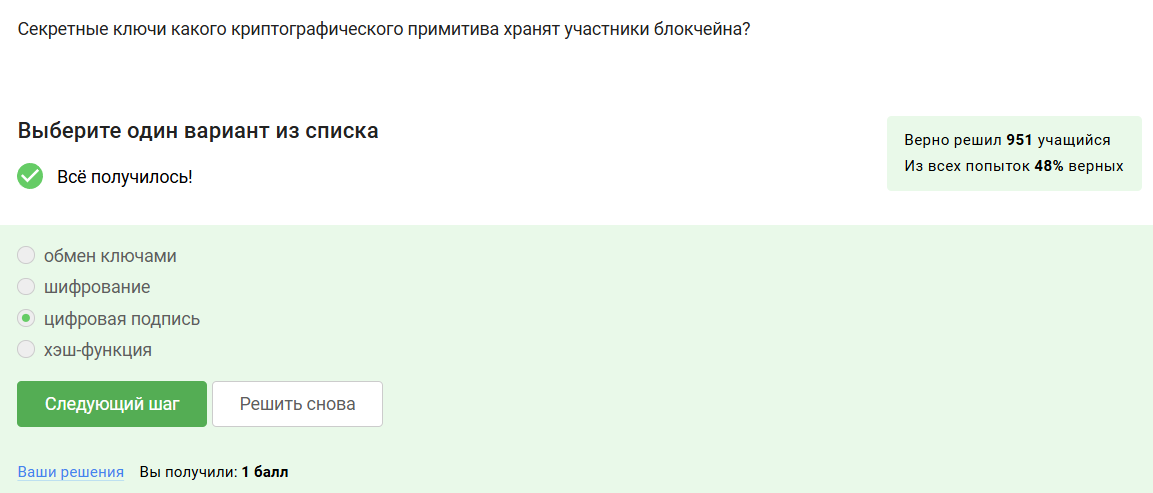


Рис. 53: Что хранят участники блокчейна

Данный курс не предусматривает выдачу сертификатов, поэтому прикладываю скриншот-доказательство прохождения курса (рис. 54).

## 3.4 Сертификат

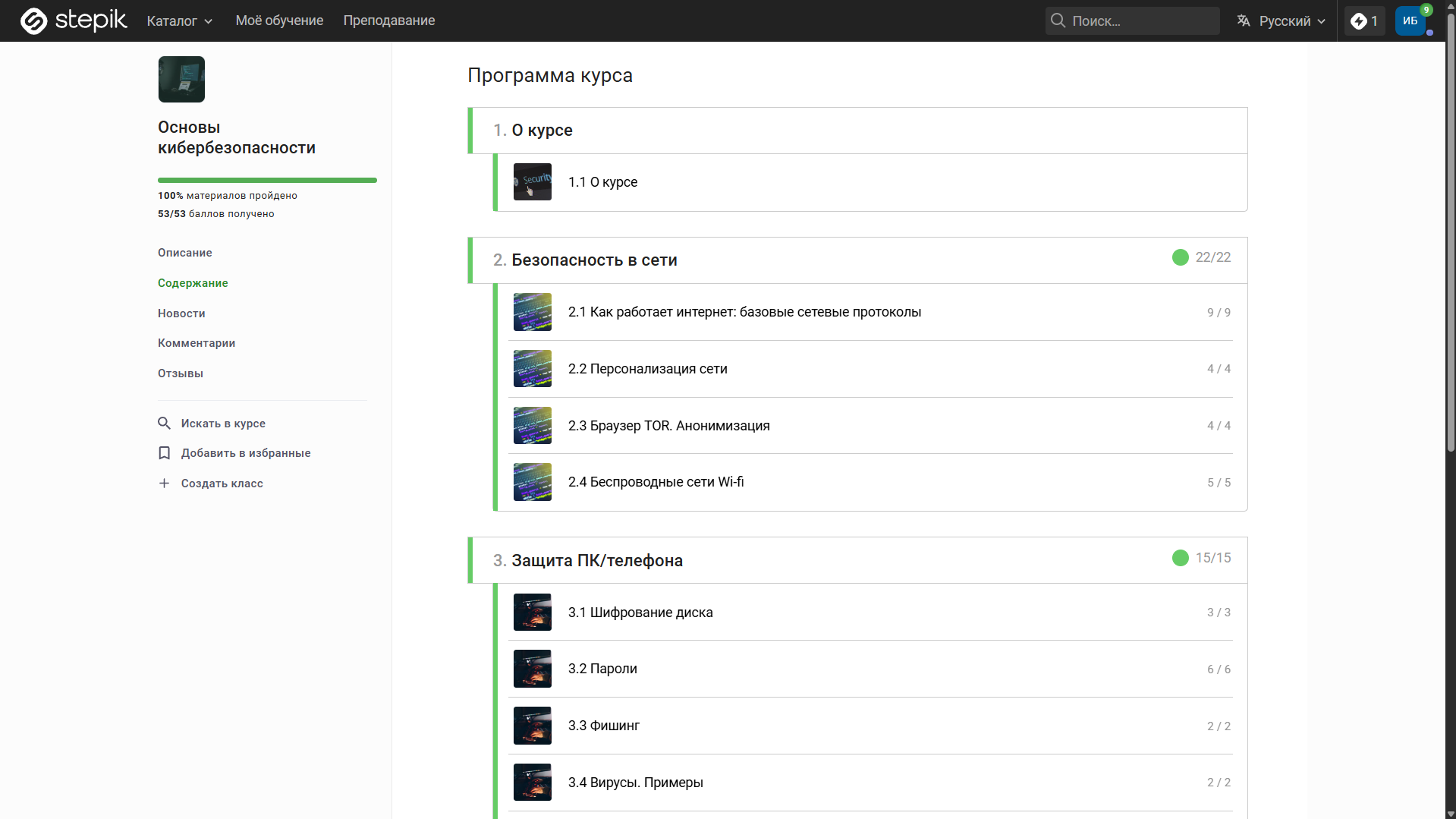


Рис. 54: “Сертификат”

# 4 Выводы

В результате прохождения внешнего курса мы узнали, как обеспечивается безопасность в сети, с помощью каких протоколов общаются устройства в ней, как защитить свои устройства и аккаунты от злоумышленников, а также рассмотрели криптографическую составляющую сети.