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 целессообразно 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. 3.1).

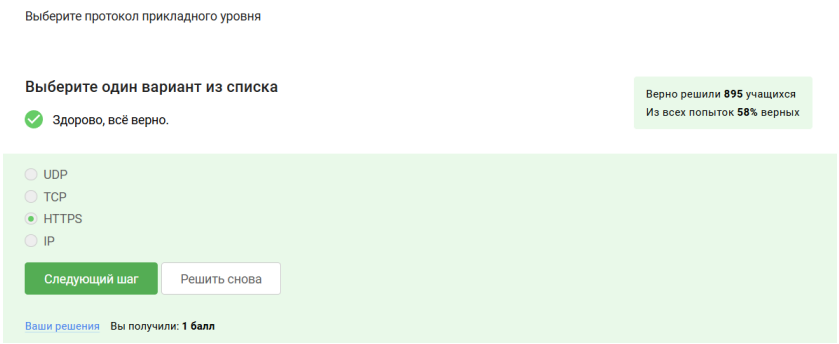

Рис. 3.1: Протокол прикладного уровня

Протокол TCP работает на транспортном уровне, поскольку определяет правила передачи пакетов (рис. 3.2).

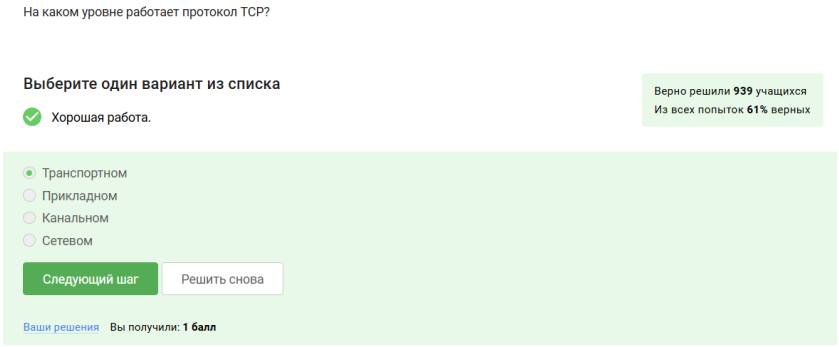

Рис. 3.2: Уровень работы протокола TCP

Валидными IP-адресами считаются адреса, содержащие 4 октета, каждый из которых состоит из чисел в диапазоне от 0 до 255 (рис. 3.3).

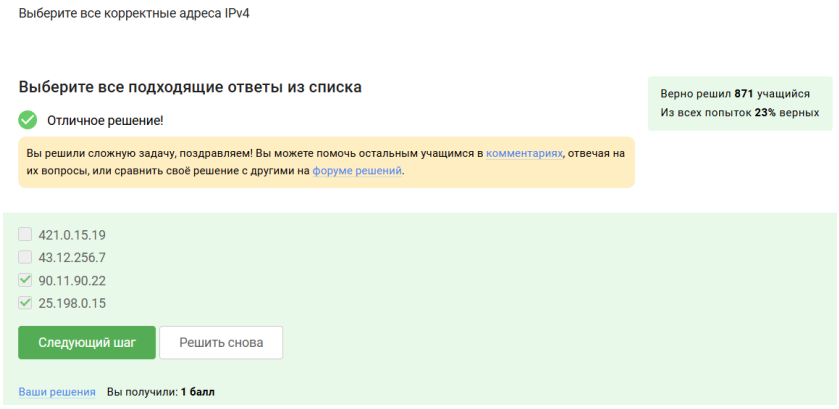

Рис. 3.3: Корректные IP

DNS - специальные сервера, которые сообщают устройству, какой IP привязан к домену (рис. 3.4).

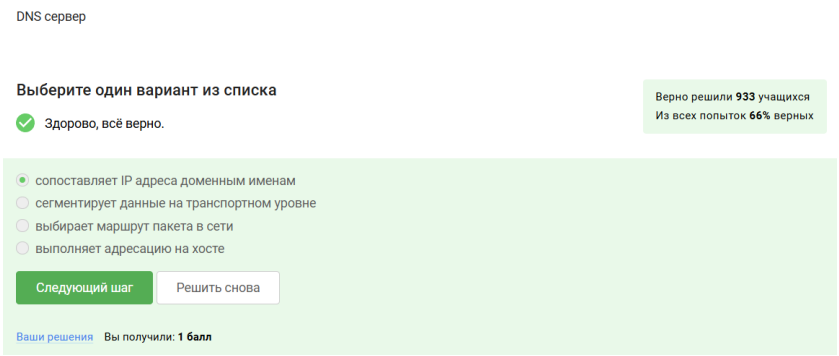

Рис. 3.4: Функция DNS

Последовательность протоколов определяется абстрактной моделью OSI (рис. 3.5).

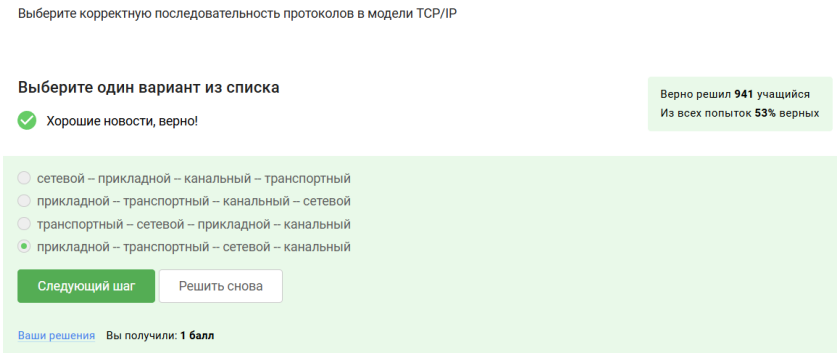

Рис. 3.5: Последовательность уровней TCP/IP

HTTP не шифрует данные (рис. 3.6).

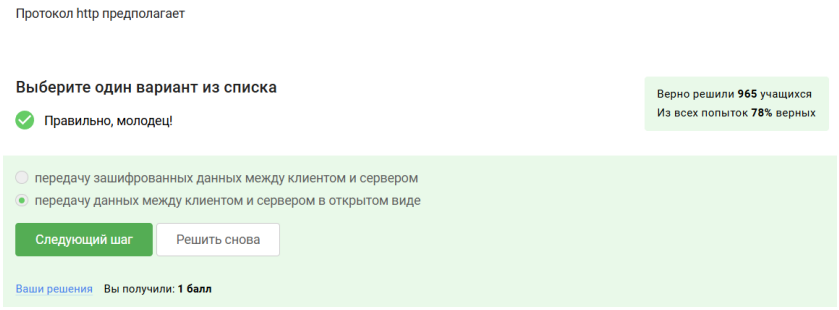

Рис. 3.6: HTTP

Для успешной передачи данных в протоколе HTTPS была реализована двухфазная передача, состоящая из рукопожатия и непосредственно передачи (рис. 3.7).

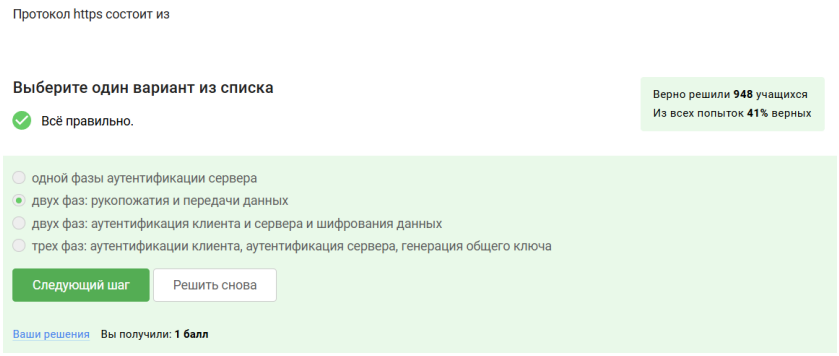

Рис. 3.7: HTTPS

В каждом устройстве определена своя версия протокола TLS. При общении выбирается наименьшая, поскольку присутствует поддержка обратной совместимости (рис. 3.8).

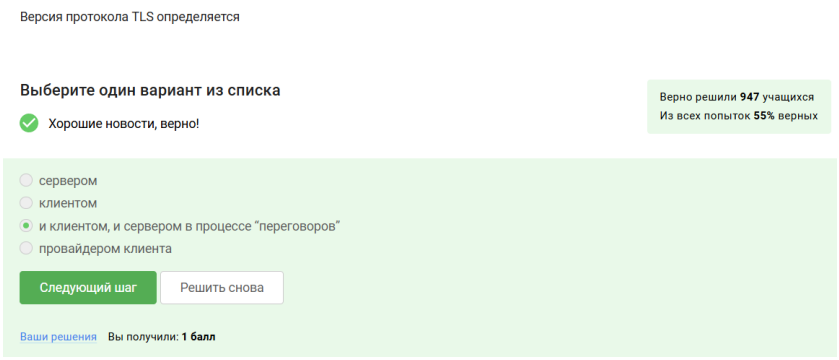

Рис. 3.8: TLS определяется всеми

Шифрование данных происходит после рукопожатия (рис. 3.9).

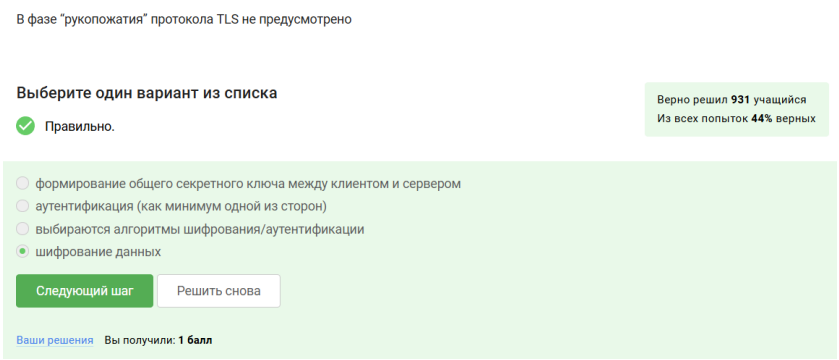

Рис. 3.9: TLS

Куки не хранят чувствительные данные, поскольку их не составляет труда перехватить (рис. 3.10).

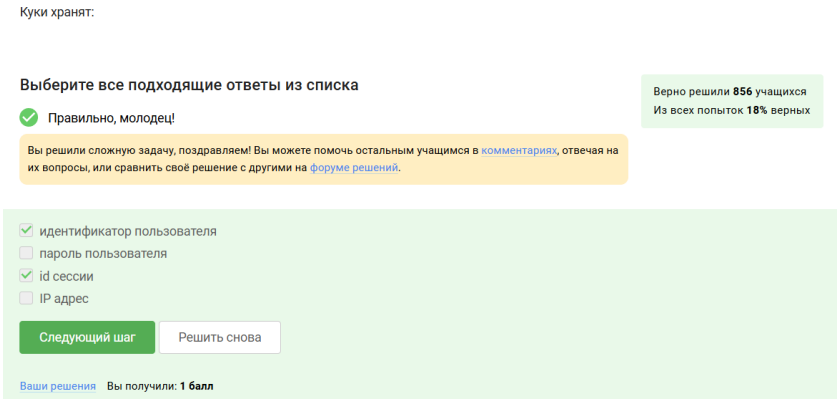

Рис. 3.10: Содержимое куки

Куки не используются для улучшения надёжности соединения, поскольку создавались с другой целью (рис. 3.11).

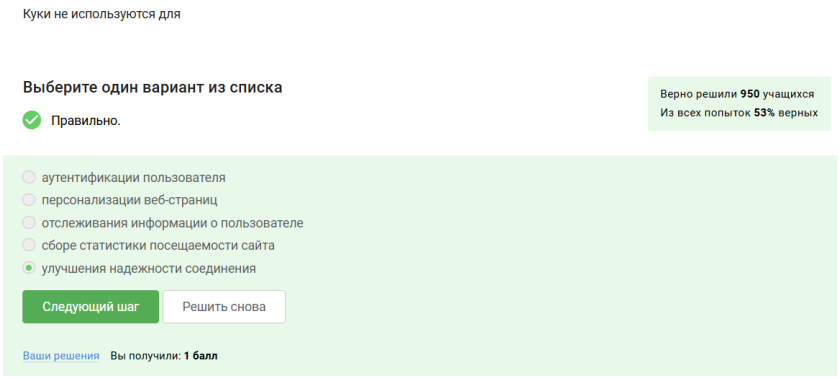

Рис. 3.11: Куки не используется для

Куки генерируются сервером в ходе общения с пользователем, затем отправляются этому пользователю и хранятся на его хосте (рис. 3.12).

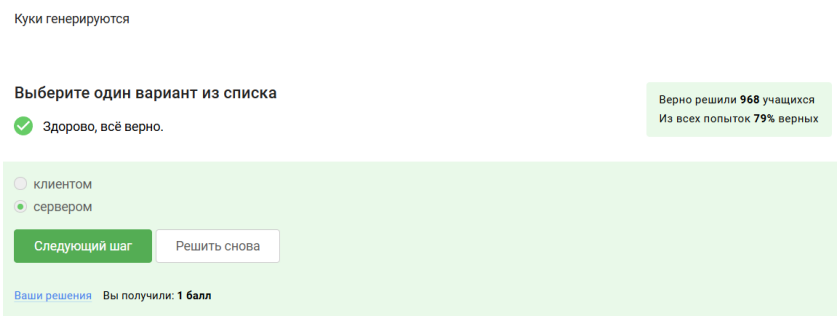

Рис. 3.12: Где генерируются куки

Сессионные куки хранятся до тех пор, пока эта сессия не завершится. Отсюда и название (рис. 3.13).

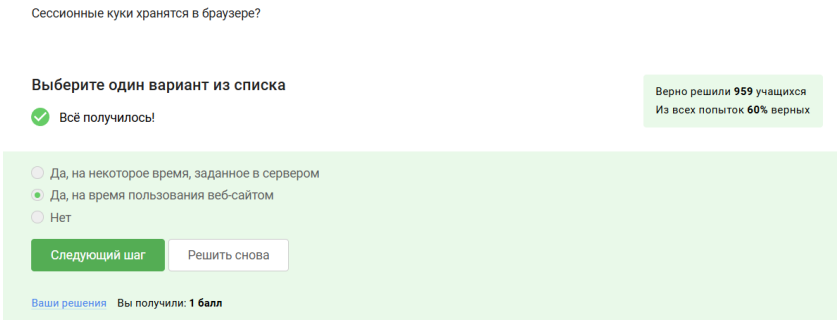

Рис. 3.13: Сессионные куки

В луковой маршрутизации используется 3 ноды (рис. 3.14).

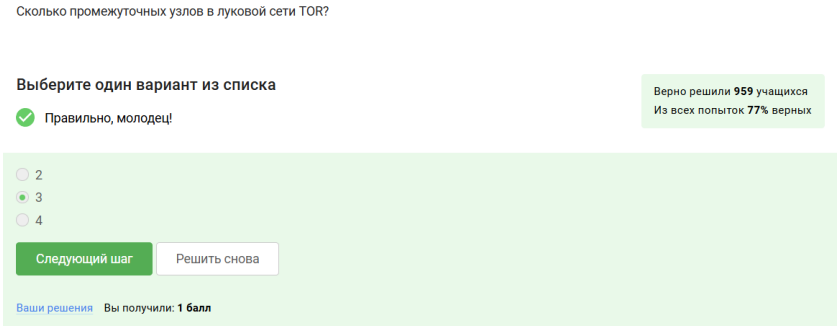

Рис. 3.14: Количество узлов TOR

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. 3.15 и рис. 3.16).

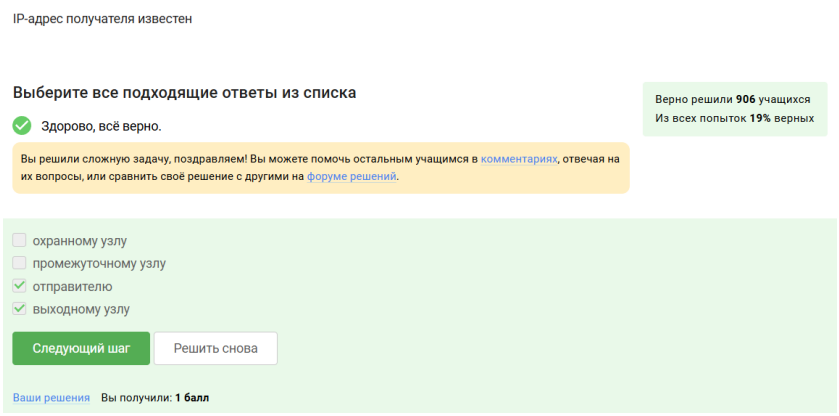

Рис. 3.15: Скрытие IP

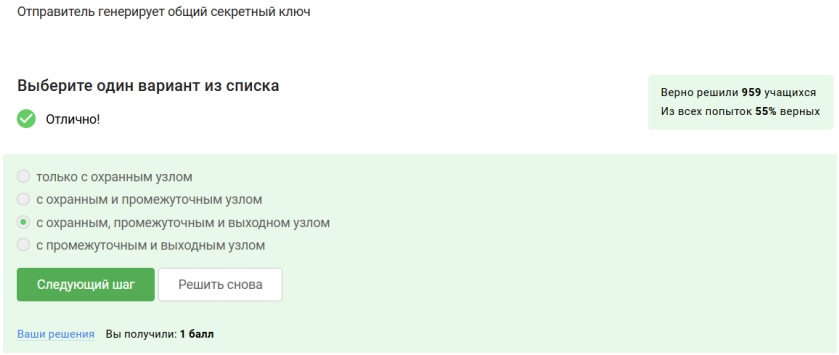

Рис. 3.16: Множественные ключи

Получателю необязательно использовать Tor при общении, поскольку всю дешифровку осуществляют ноды (рис. 3.17).

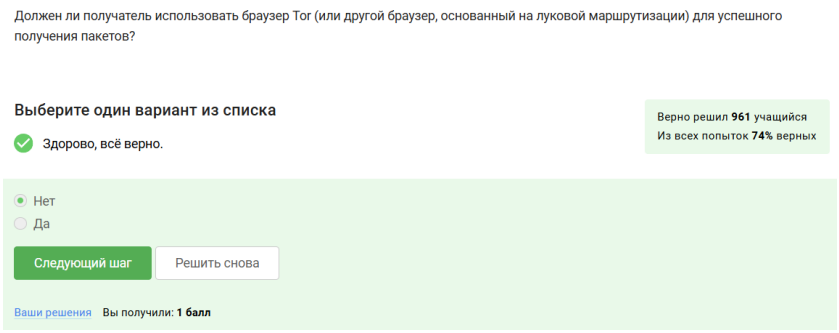

Рис. 3.17: Одностороннее использование TOR

Определение Wi-Fi (рис. 3.18).

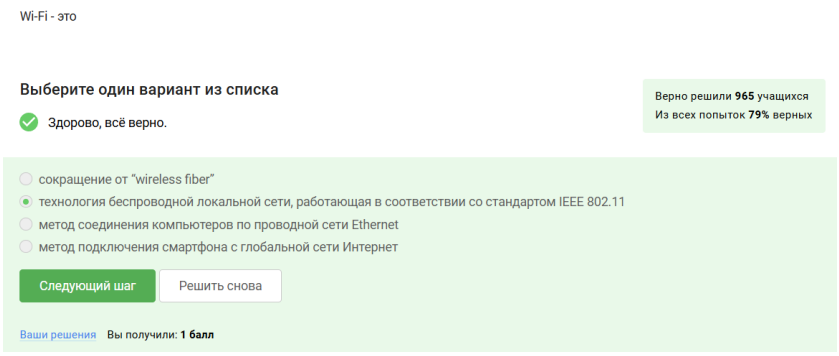

Рис. 3.18: Определение Wi-Fi

Wi-Fi работает на канальном уровне, поскольку связывает локальные устройства с интернетом (рис. 3.19).

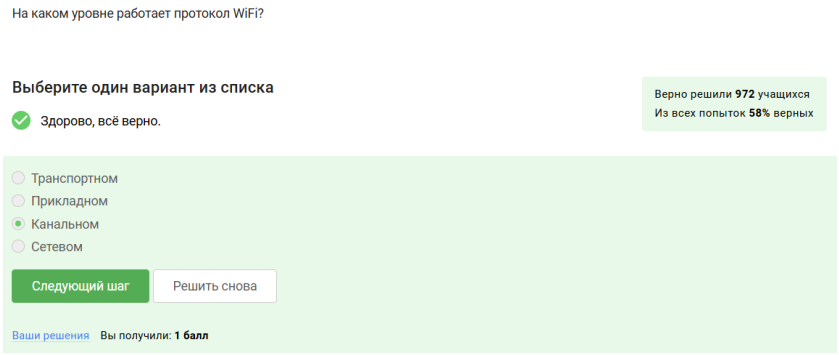

Рис. 3.19: Уровень работы Wi-Fi

WEP считается устаревшим и небезопасным, потому что его ключ шифрования ограничен 40 битами (рис. 3.20).

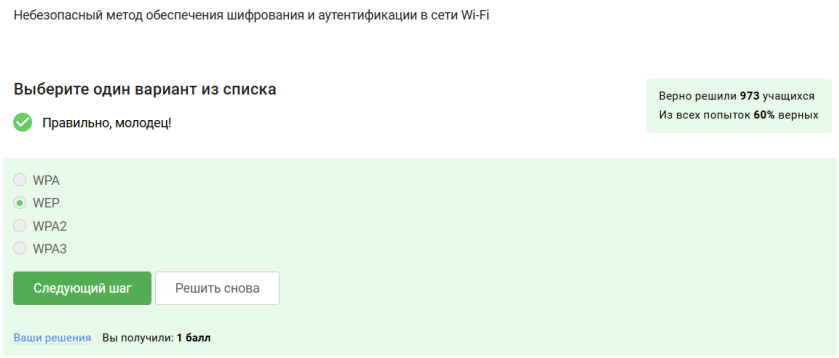

Рис. 3.20: Небезопасный метод шифрования

Данные между хостом и роутером передаются в зашифрованном виде, дабы исключлчить использование данных при перехвате (рис. 3.21).

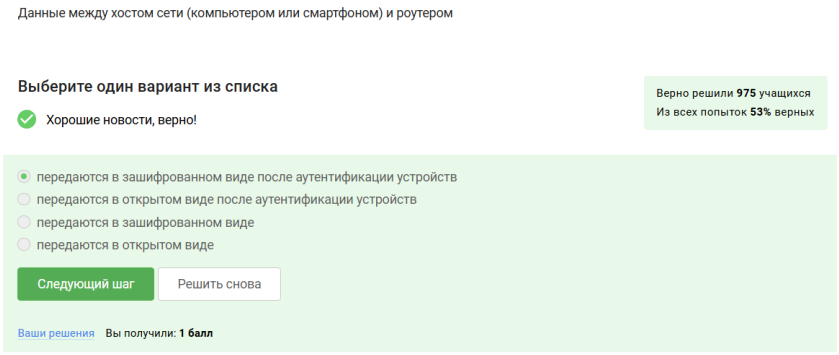

Рис. 3.21: Передача данных Wi-Fi

Для домашней сети используется WPA2 Personal, поскольку это удобнее для пользователей, ведь Enterprise использует динамические ключи (рис. 3.22).

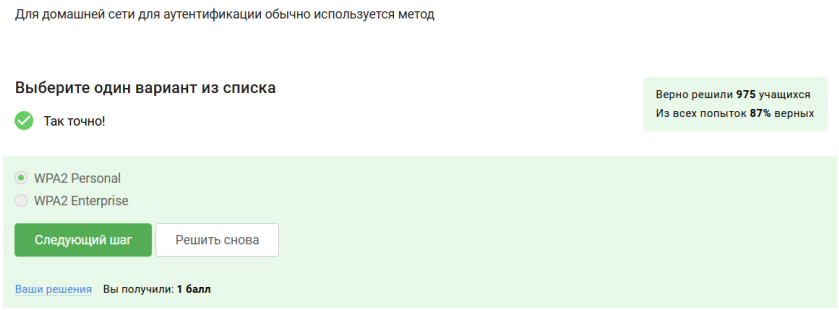

Рис. 3.22: Метод аутентификации в домашней сети

3.2 Прохождение второго этапа

Загрузочный сектор диска можно и рекомендуется шифровать (рис. 3.23).

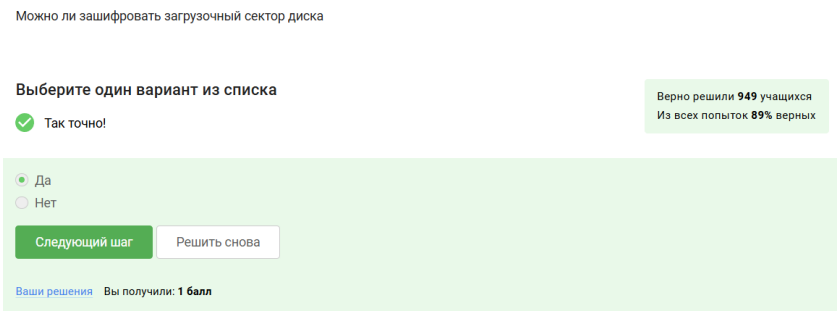

Рис. 3.23: Возможность шифровки загрузочного сектора диска

Шифрование дисков симметричное, поскольку оно гораздо быстрее асимметричного, что идёт в плюс пользователям (рис. 3.24).

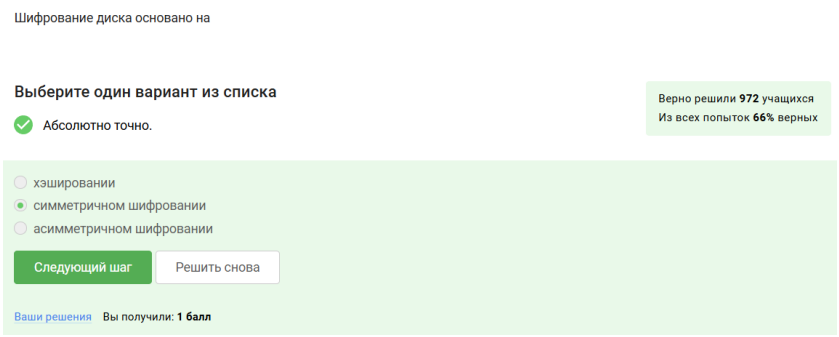

Рис. 3.24: Симметричное шифрование диска

BitLocker установлен в Windows по умолчанию, а VeraCrypt является наиболее популярной сторонней программой для шифрования дисков (рис. 3.25).

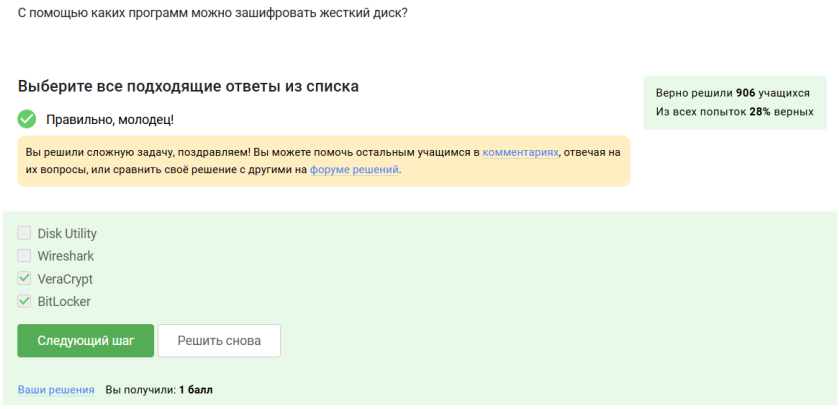

Рис. 3.25: Программы для шифрования диска

Пароли должны состоять из цифр, символов и спец. символов, чтобы подобрать было труднее (рис. 3.26).

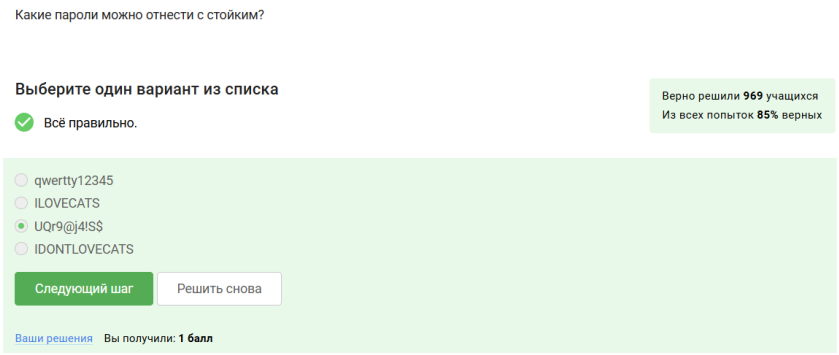

Рис. 3.26: Устойчивые к брутфорсу пароли

Пароли безопасно хранить в менеджере паролей, а пароль от него самого нужно хранить на нецифровом носителе или в голове (рис. 3.27).

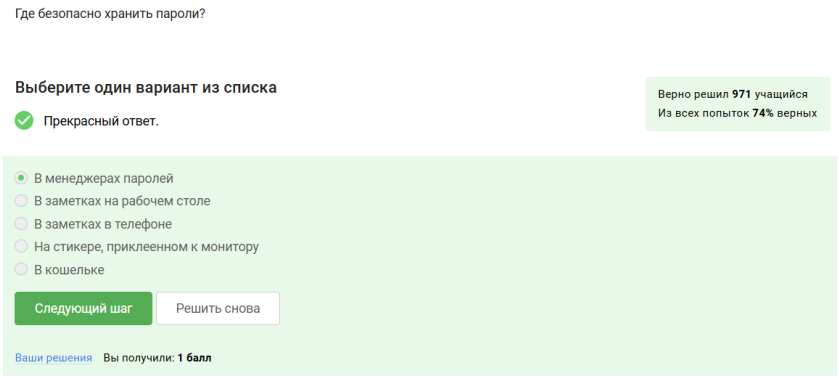

Рис. 3.27: Безопасное место для хранения паролей

Капча используется для защиты от брутфорса ботами (рис. 3.28).

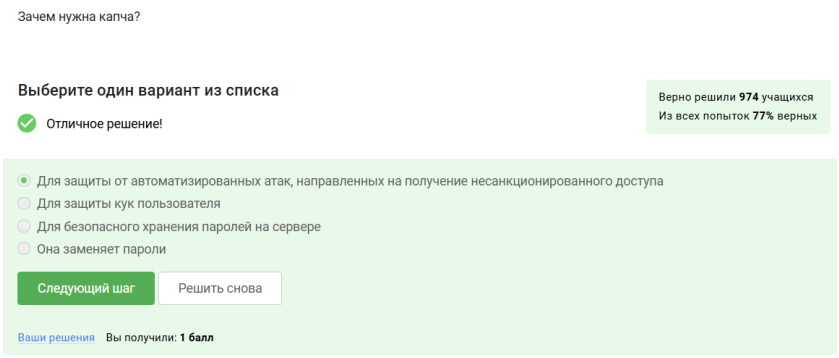

Рис. 3.28: Капча

Хэширование паролей нужно, чтобы сделать потенциальные утечки баз данных менее опасными (рис. 3.29).

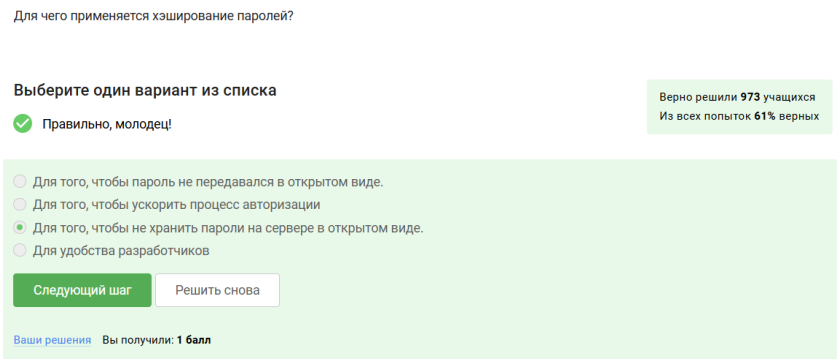

Рис. 3.29: Хэширование паролей

Соль помогает изменить хэш слабого пароля, но это не защищает от перебора (рис. 3.30).

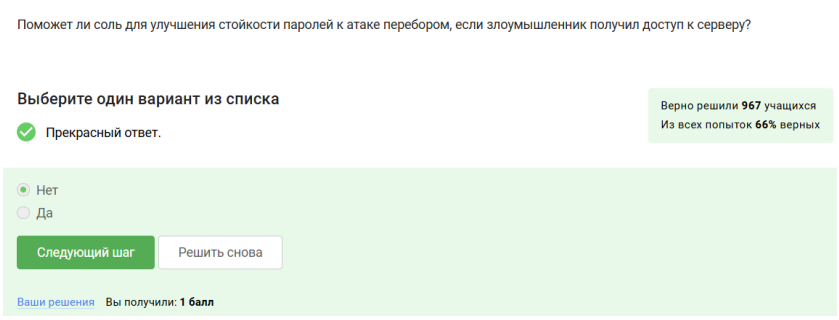

Рис. 3.30: Соль

Все методы, которые усложняют пароль или замедляют возможность перебора, помогут защитить от брутфорса (рис. 3.31).

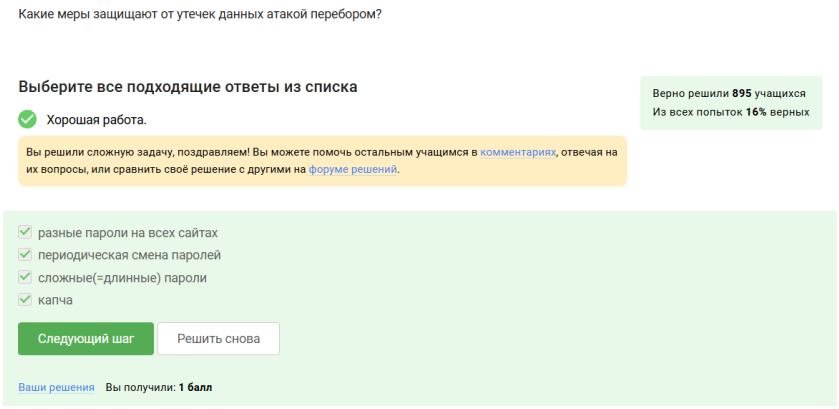

Рис. 3.31: Методы защиты данных от утечек

Фишинговые ссылки похожи на настоящие, но имеют в пути другие доменные зоны или как-то видоизменяют сам путь (рис. 3.32).

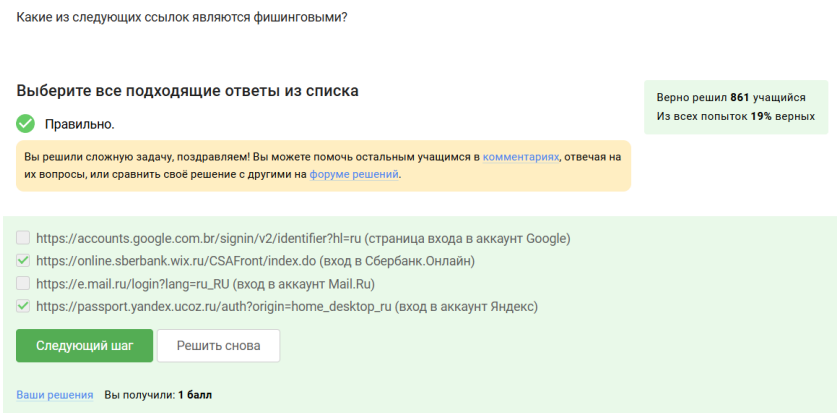

Рис. 3.32: Фишинговые ссылки

Фишинговый имейл может прийти от знакомого адреса, если используется слабый протокол почтового сервиса (рис. 3.33).

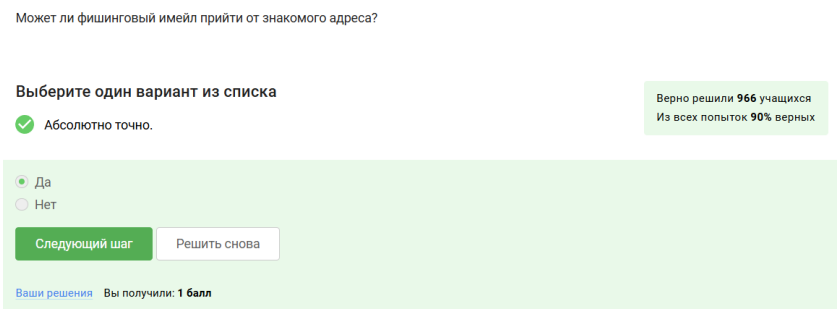

Рис. 3.33: Фишинговый имейл

Спуфинг уже практически неактуален, поскольку придуманы более защищённые протоколы отправки Email (рис. 3.34).

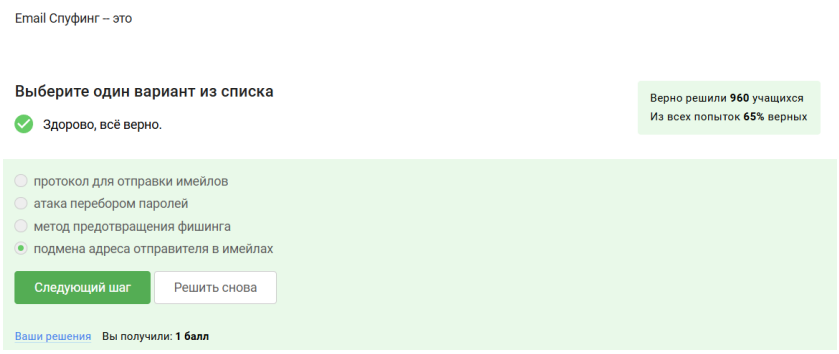

Рис. 3.34: Имейл спуфинг

Троян маскирутеся под легитимную программу и пытается получить контроль над устройством (рис. 3.35).

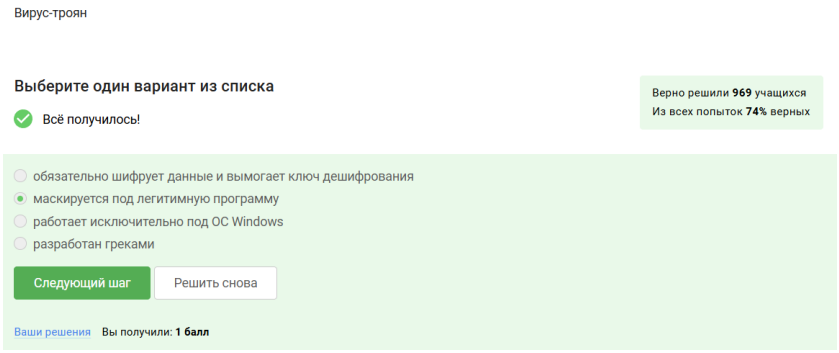

Рис. 3.35: Вирус-троян

Ключ шифрования в протоколе Signal генерируется при отправке первого со-

общения пользователем (рис. 3.36).

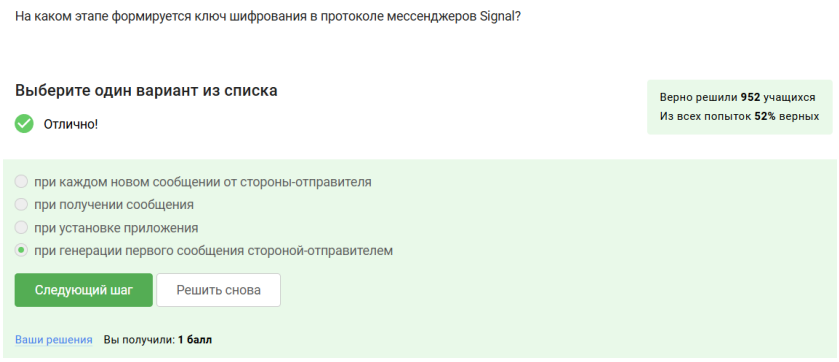

Рис. 3.36: Signal

Сквозное шифрование использует пару ключей для конфеденциального общения узлов (рис. 3.37).

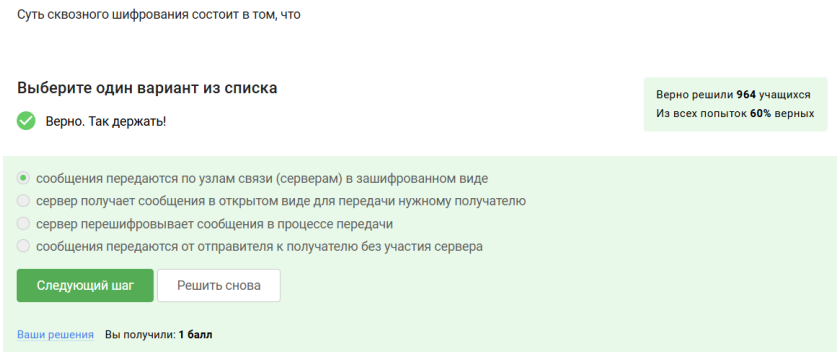

Рис. 3.37: Суть сквозного шифрования

Для правильной работы криптографических примитивов требуется наличие пары ключей у всех участников общения (рис. 3.38).

3.3 Прохождение третьего этапа

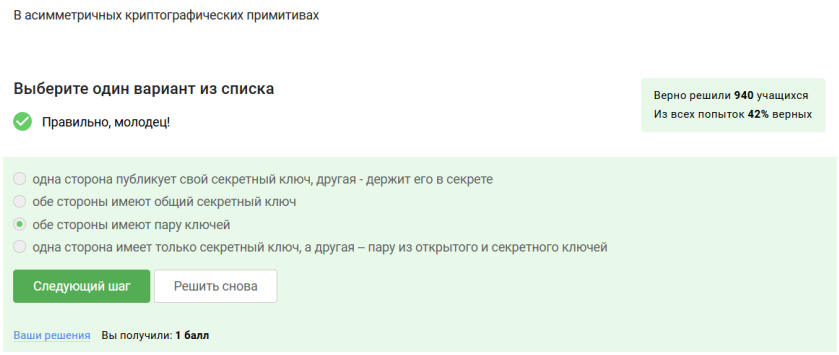

Рис. 3.38: Ассимитричные криптографические примитивы

Криптографическая хэш-функция не обеспечивает конфиденциальность захэшированных данных, поскольку её невозможно вычислить в обратном порядке (рис. 3.39).

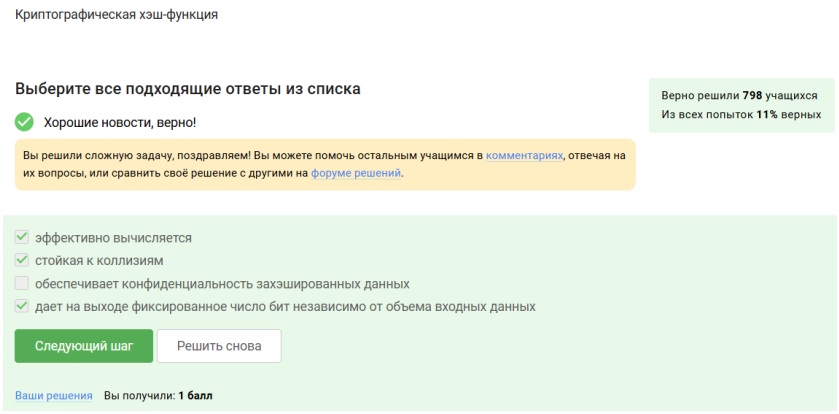

Рис. 3.39: Криптографическая хэш-функция

Перечисление алгоритмов цифровой подписи (рис. 3.40).

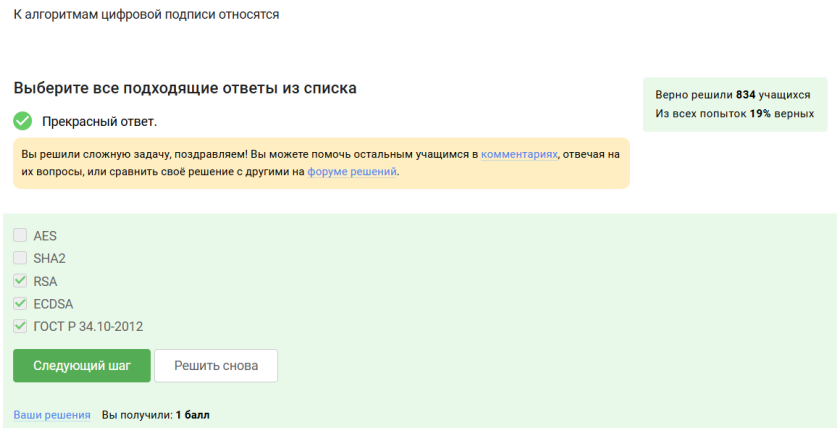

Рис. 3.40: Алгоритмы цифровой подписи

Код аутентификации сообщения относится к симметричным примитивам, поскольку используется симметричное шифрование (рис. 3.41).

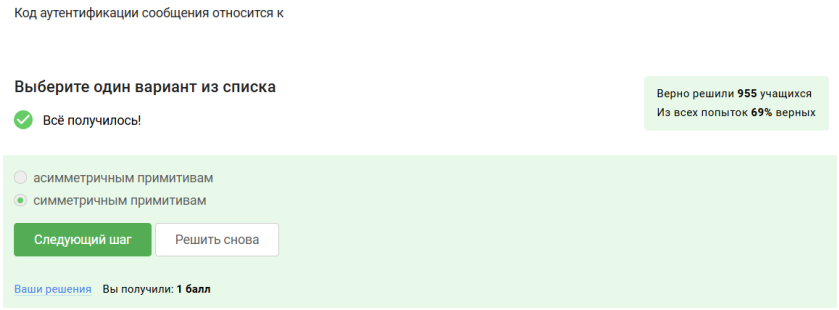

Рис. 3.41: Код аутентификации сообщения

Определение обмена ключами Диффи-Хеллмана (рис. 3.42).

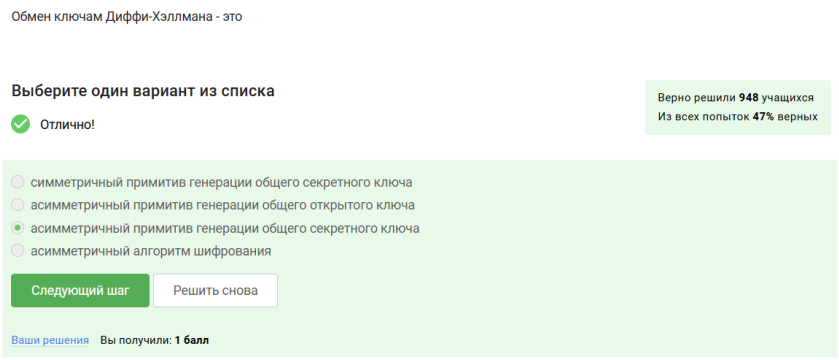

Рис. 3.42: Обмен ключами Диффи-Хеллмена

Протокол электронной цифровой подписи относится к протоколам с публичным ключом, ведь пользователи могут проверить подпись этим ключом (рис. 3.43).

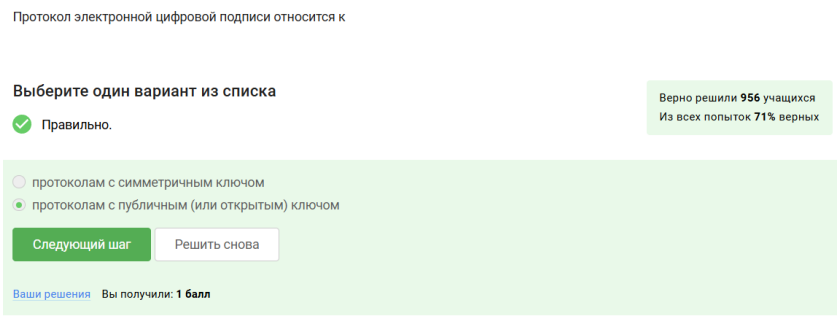

Рис. 3.43: Протокол электронной цифровой подписи

Механизм работы верификации ЭЦП (рис. 3.44).

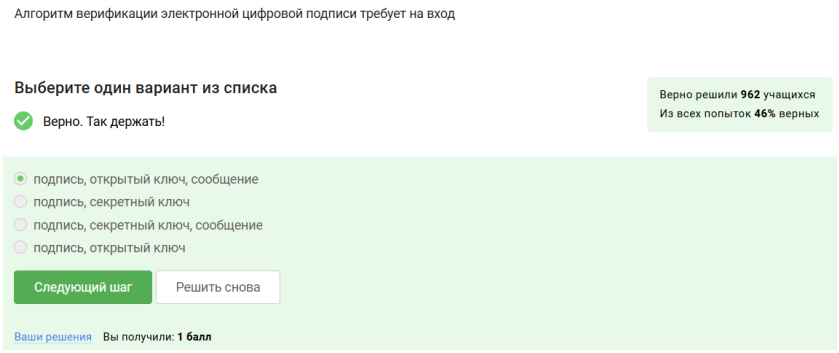

Рис. 3.44: Верификация ЭЦП

ЭПС не обеспечивает конфиденциальность, поскольку содержит информацию о пользователе, сделавшем эту подпись (рис. 3.45).

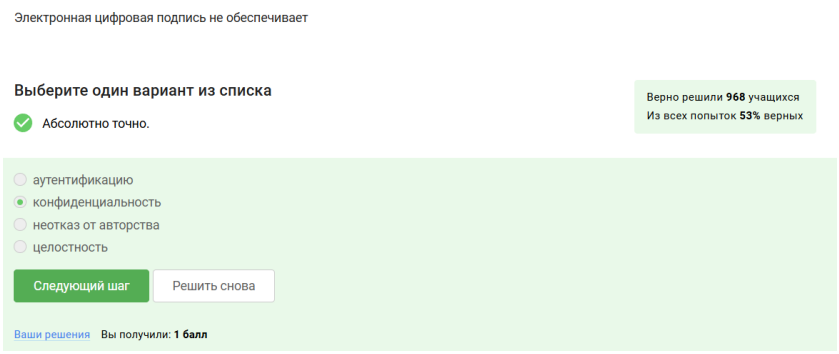

Рис. 3.45: ЭЦП не обеспечивает

Усиленная квалифицированная электронная подпись при отправки налоговой отчётности в ФНС требуется для обеспечения юридической значимости, безопасности и достоверности (рис. 3.46).

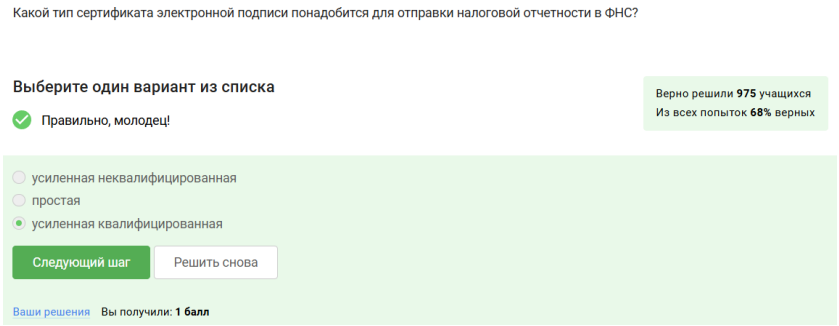

Рис. 3.46: Тип ЭЦП для отправки налоговой отчётности в ФНС

Сертификаты для доменов выдают сертифицированные центры (рис. 3.47).

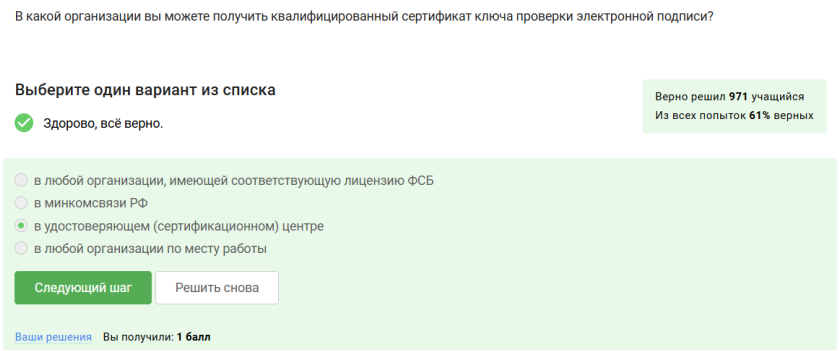

Рис. 3.47: СА

Список платёжных систем (рис. 3.48).

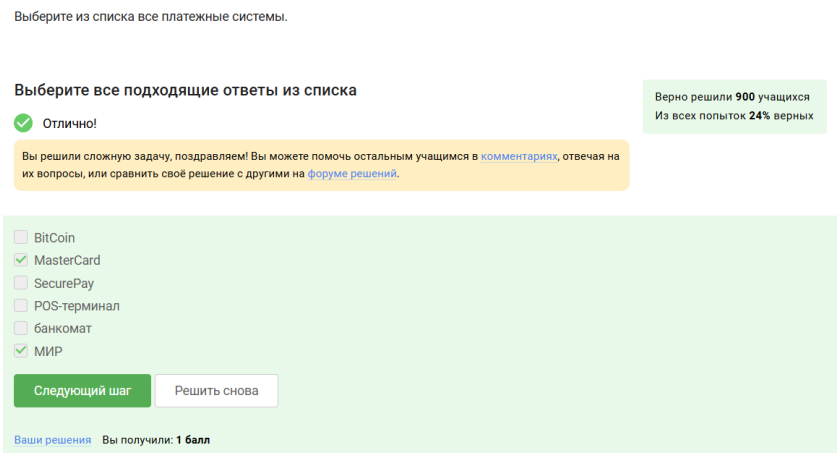

Рис. 3.48: Платёжные системы

Многофакторная аутентификация подразумевает собой ввод нескольких ключей для доступа к информации (рис. 3.49).

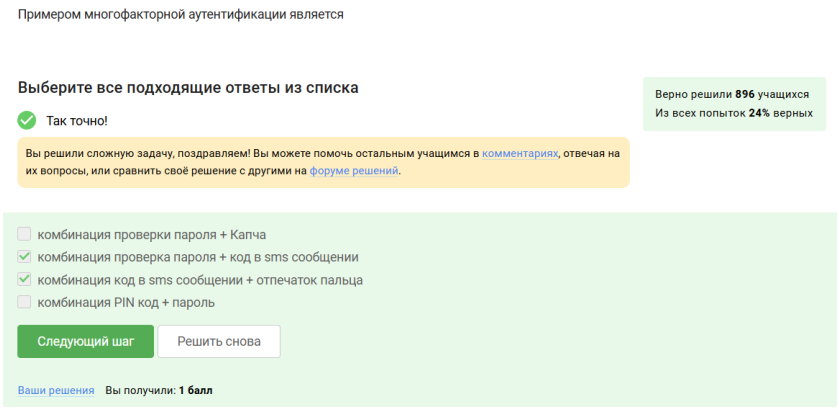

Рис. 3.49: Примеры многофакторной аутентификации

Для безопасности платёжных счетов пользователей при онлайн оплатах сегодня используется многофакторная аутентификация перед банком-эмитентом (рис. 3.50).

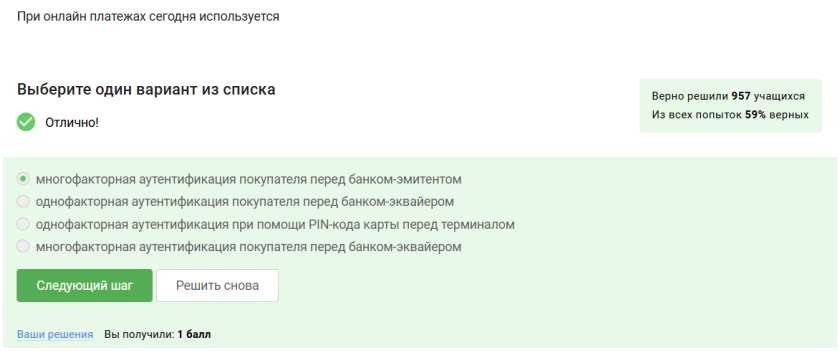

Рис. 3.50: Аутентификация при онлайн платежах

Устройство proof of work (рис. 3.51).

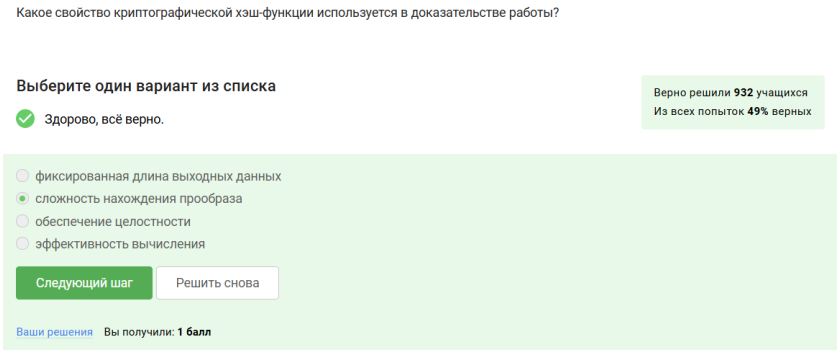

Рис. 3.51: Proof of work

Консенсус позволяет участникам блокчейна согласовывать операции без доверия друг к другу (рис. 3.52).

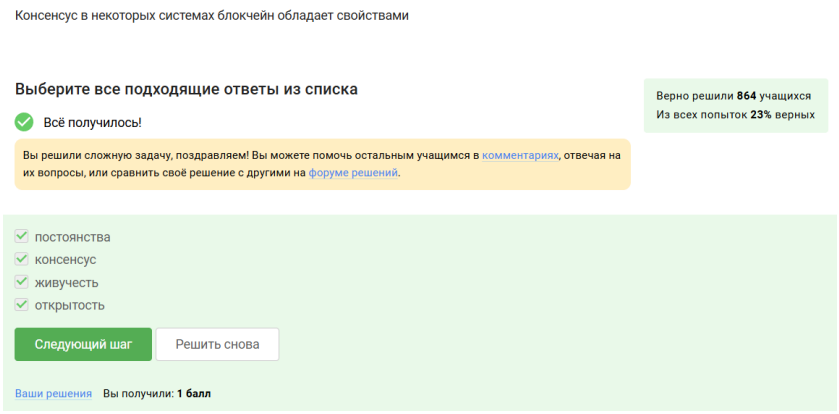

Рис. 3.52: Consensus

Все участники блокчейна хранят цифровую подпись (рис. 3.53).

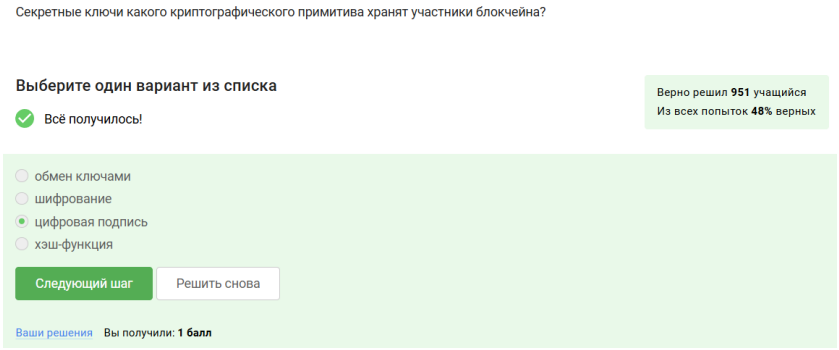

Рис. 3.53: Что хранят участники блокчейна

Данный курс не предусматривает выдачу сертификатов, поэтому прикладываю скриншот-доказательство прохождения курса (рис. 3.54).

3.4 Сертификат

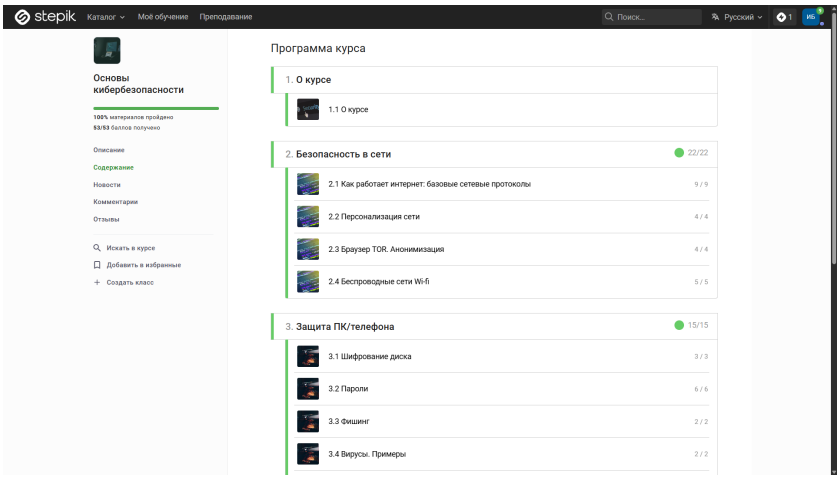

Рис. 3.54: “Сертификат”

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.