Отчет о прохождении внешнего курса

Основы информационной безопасности

Выполнила: Пестова Ева Константиновна

Группа: НКАбд-03-23

Москва. Российский университет дружбы народов. 2025 год

Цель работы

Изучить основы кибербезопасности, с помощью курса на stepic и проверить свои знания с помощью контрольных вопросов.

Задание

- Пройти курс.
- Получить сертификат.
- Записать видео (с записью камерой лица) по прохождению контрольных мероприятий (тесты и задания) по каждому разделу + итоговая презентация по каждому этапу.
- Написать отчёт по прохождению контрольных мероприятий (тесты и задания) по каждому разделу.

Выполнение

2.1

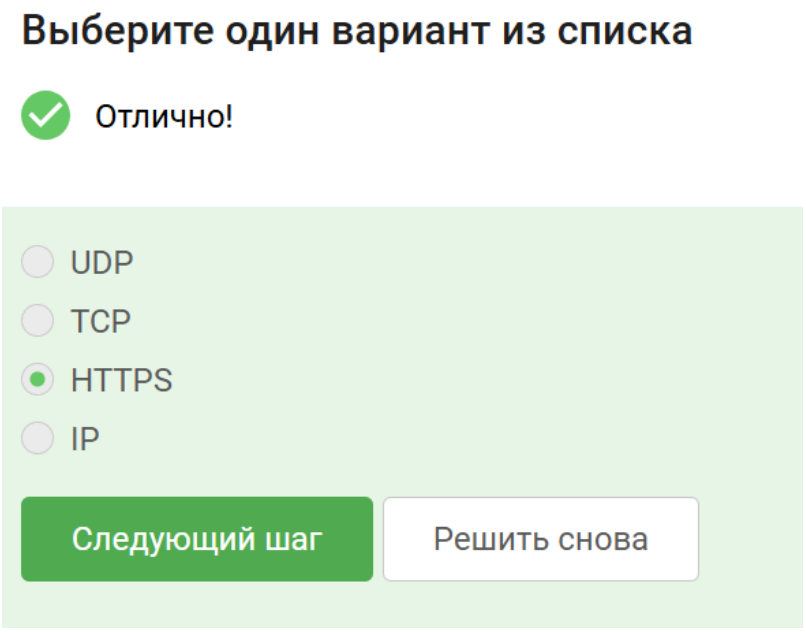

Рисунок 2.1-1

Комментарий: Протокол HTTPS используется для безопасной передачи данных — в отличие от HTTP, он шифрует трафик.

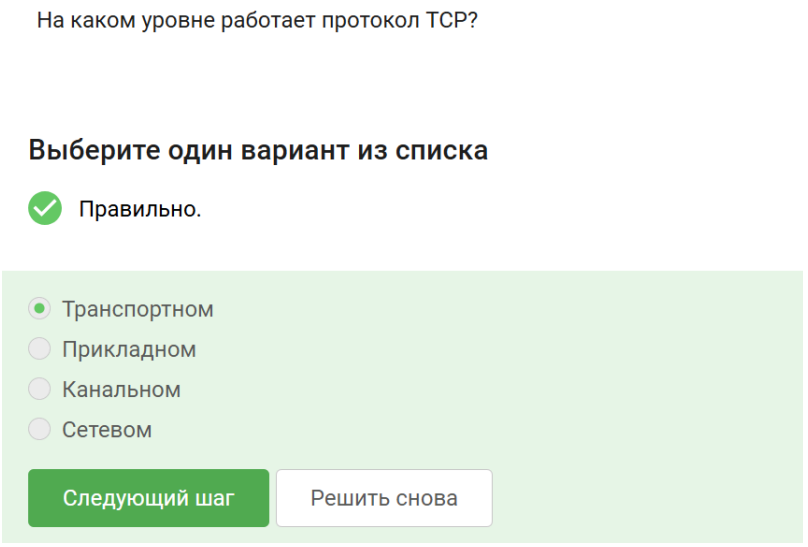

Рисунок 2.1-2

Комментарий: Протокол TCP работает на транспортном уровне, обеспечивая надёжную доставку данных.

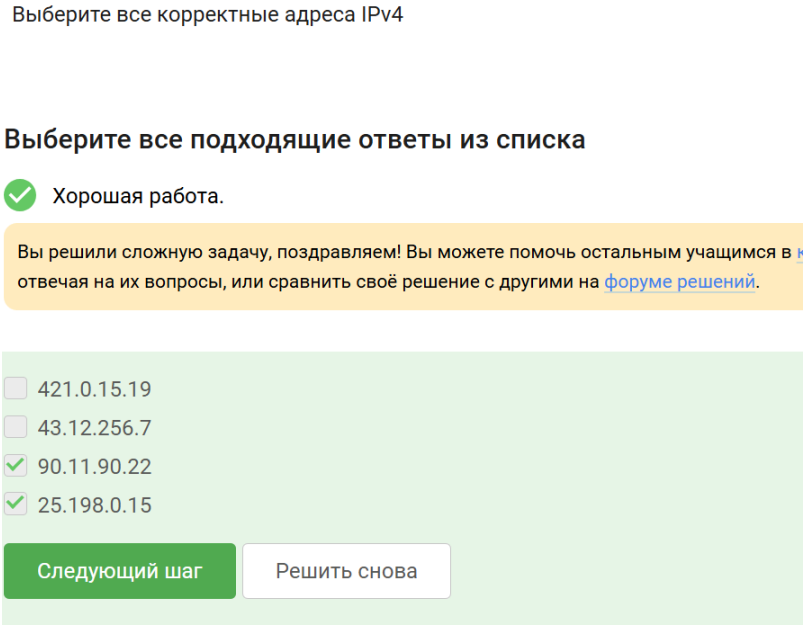

Рисунок 2.1-3

Комментарий: Корректные IPv4-адреса должны быть в диапазоне от 0.0.0.0 до 255.255.255.255 без некорректных значений (например, 421 или 256).

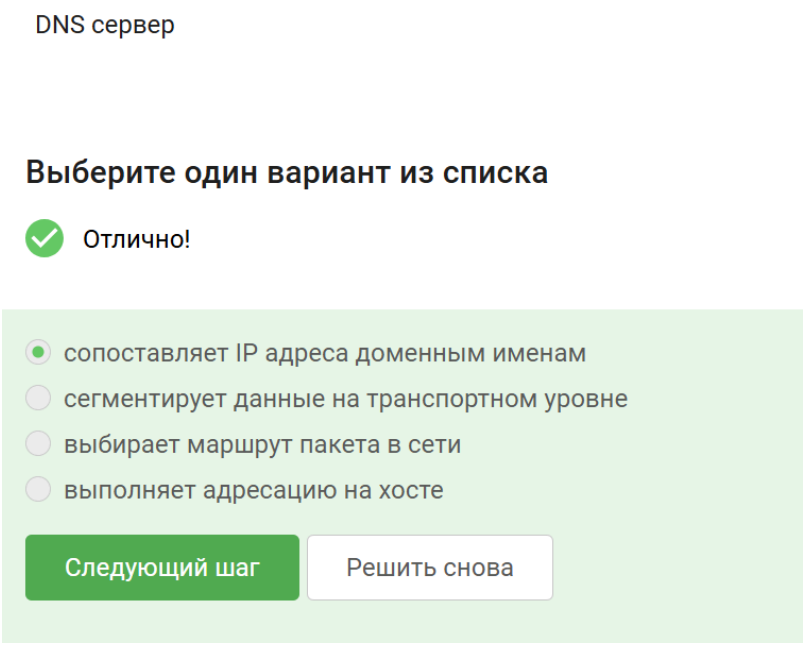

Рисунок 2.1-4

Комментарий: DNS-сервер сопоставляет доменные имена с IP-адресами — именно это его основная функция.

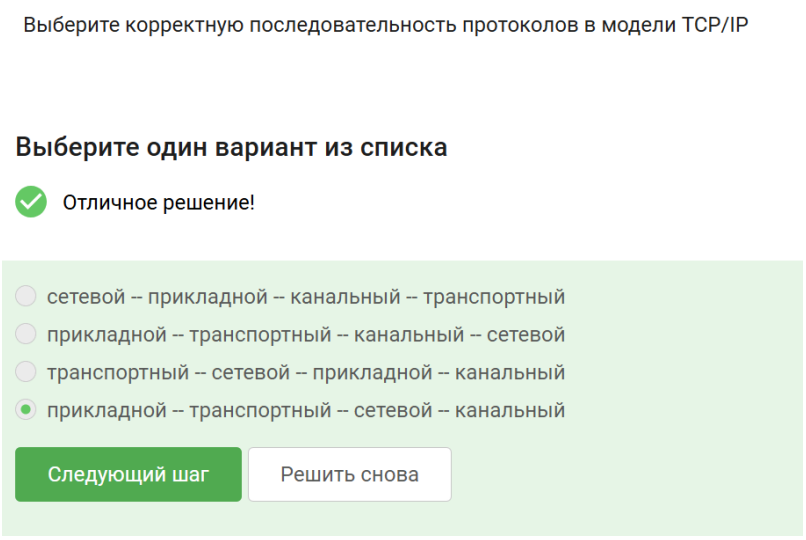

Рисунок 2.1-5

Комментарий: Правильная последовательность протоколов TCP/IP: прикладной → транспортный → сетевой → канальный.

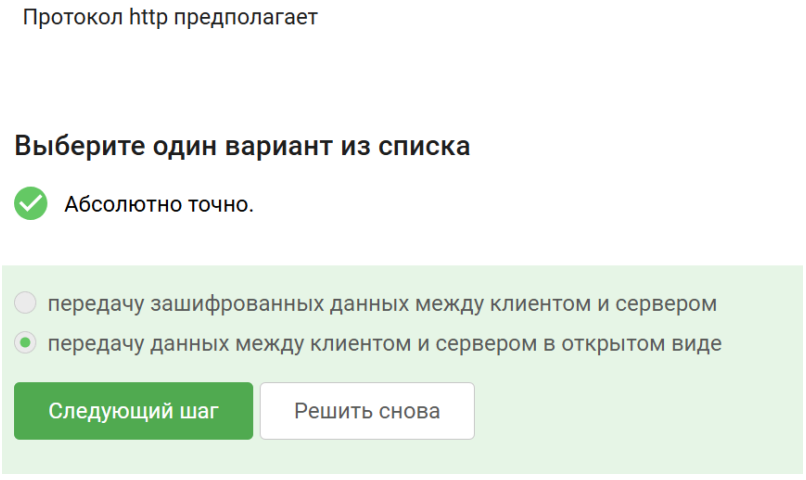

Рисунок 2.1-6

Комментарий: HTTP передаёт данные в открытом виде, без шифрования — это делает его небезопасным в публичных сетях.

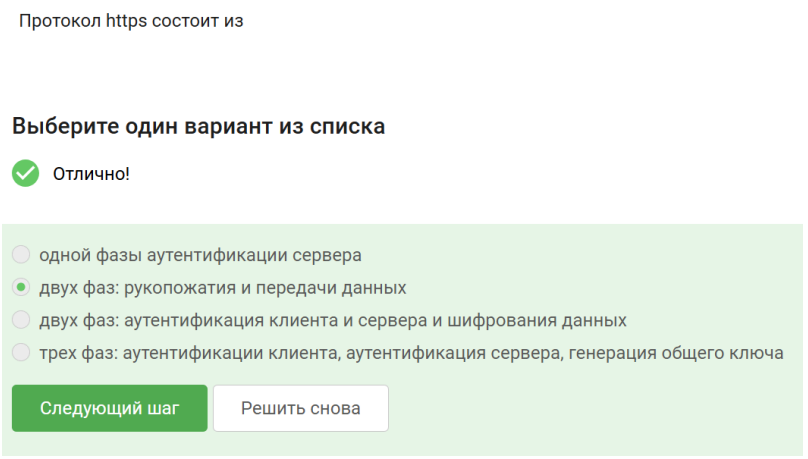

Рисунок 2.1-7

Комментарий: Протокол HTTPS состоит из двух фаз: рукопожатия и передачи данных — в первой фазе устанавливаются параметры безопасности.

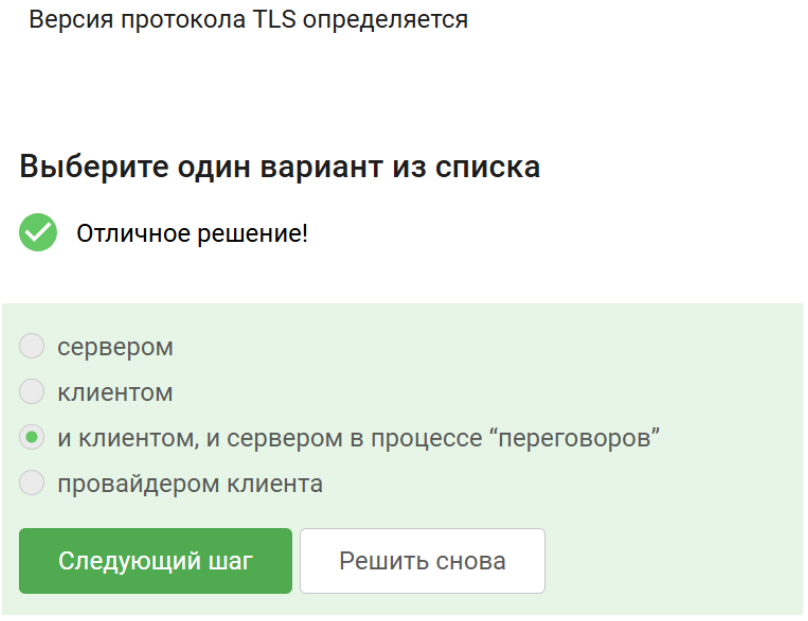

Рисунок 2.1-8

Комментарий: Версия TLS определяется в процессе переговоров между клиентом и сервером — это двусторонний процесс.

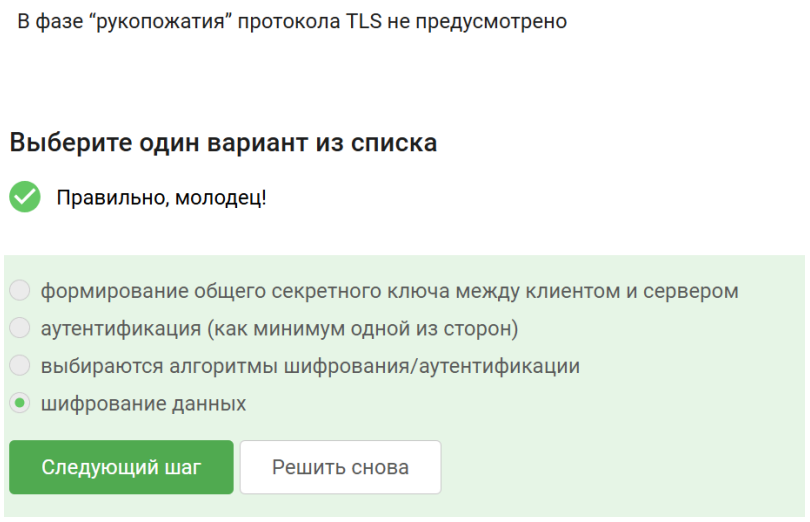

Рисунок 2.1-9

Комментарий: На этапе 'рукопожатия' TLS не происходит шифрования данных — только выбор параметров и аутентификация.

2.2

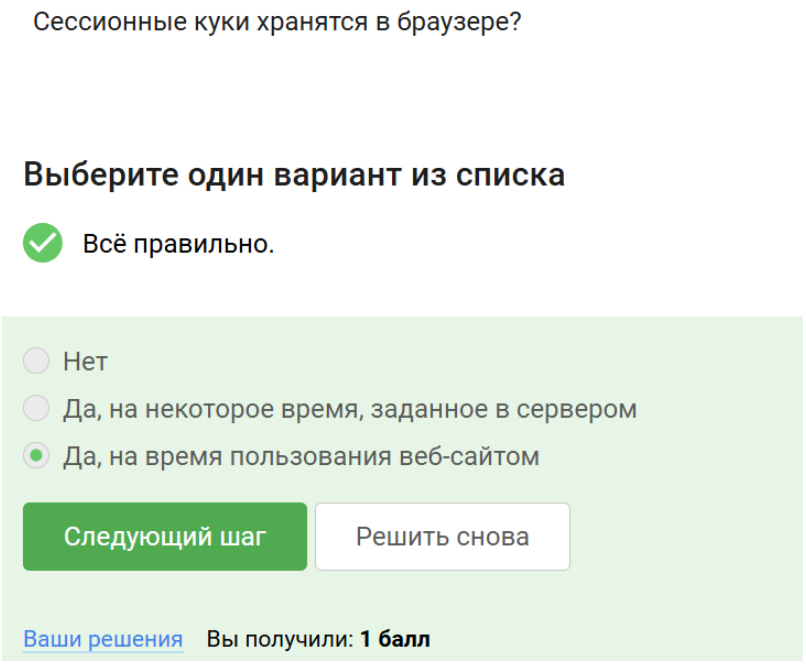

Рисунок 2.2-1

Комментарий: Сессионные куки действительно хранятся в браузере только на время активного взаимодействия с сайтом — после закрытия вкладки или браузера они удаляются.

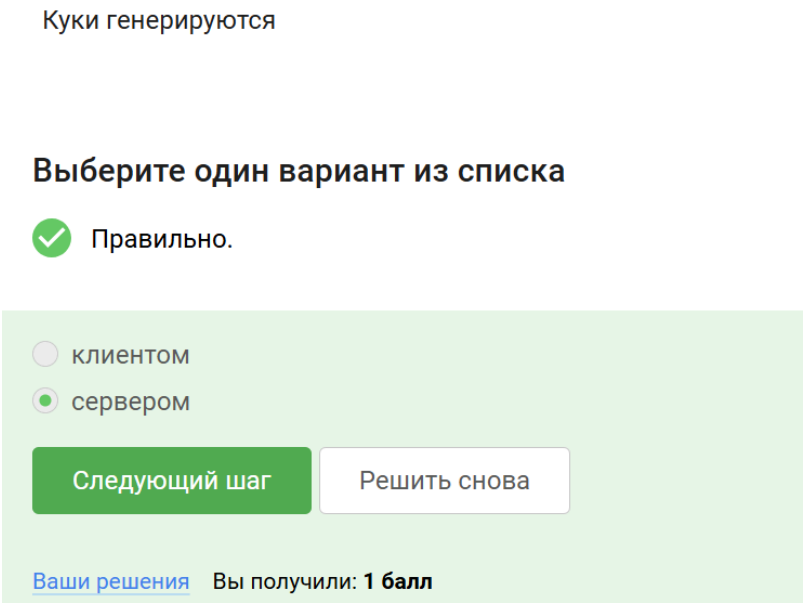

Рисунок 2.2-2

Комментарий: Куки создаются сервером, поскольку именно сервер управляет механизмом идентификации пользователя.

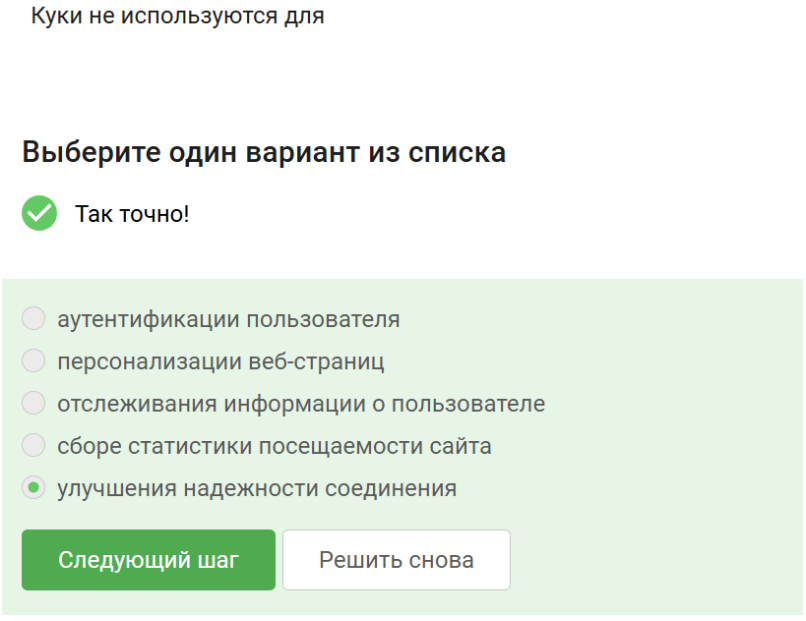

Рисунок 2.2-3

Комментарий: Куки не применяются для улучшения надёжности соединения — это задача других технологий, например, TCP и TLS.

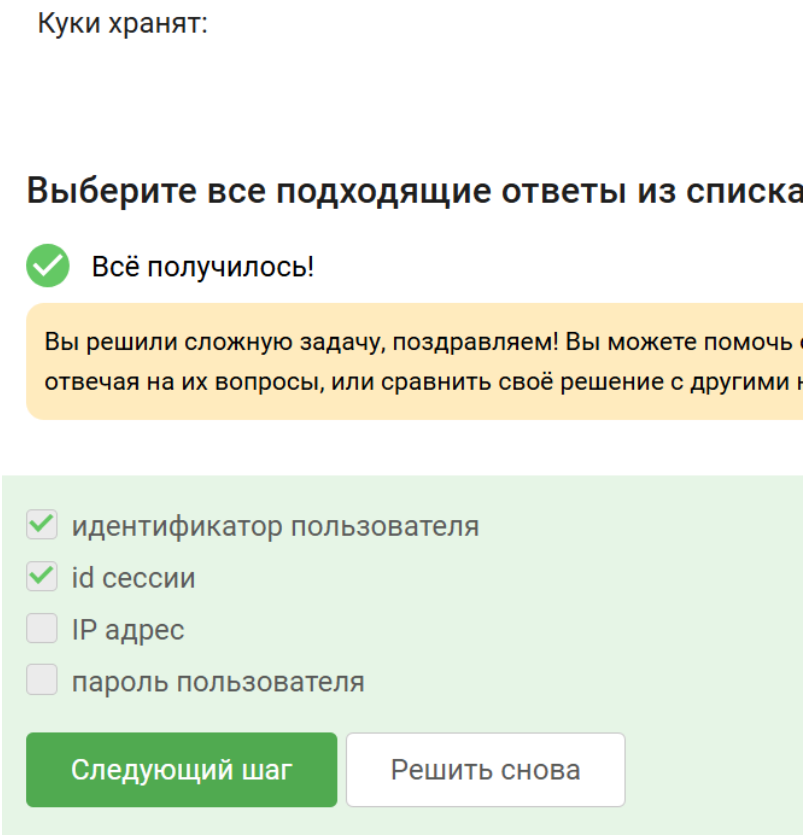

Рисунок 2.2-4

Комментарий: Куки используются для хранения информации об идентификаторе пользователя и сессии — это необходимо для аутентификации и сохранения состояния входа.

2.3

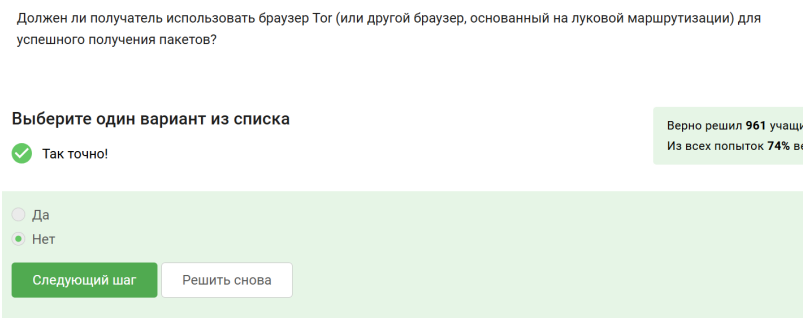

Рисунок 2.3-1

Комментарий: Получателю не обязательно использовать браузер Tor — он получает пакеты через обычный браузер, если они были отправлены с маршрутизацией по Tor.

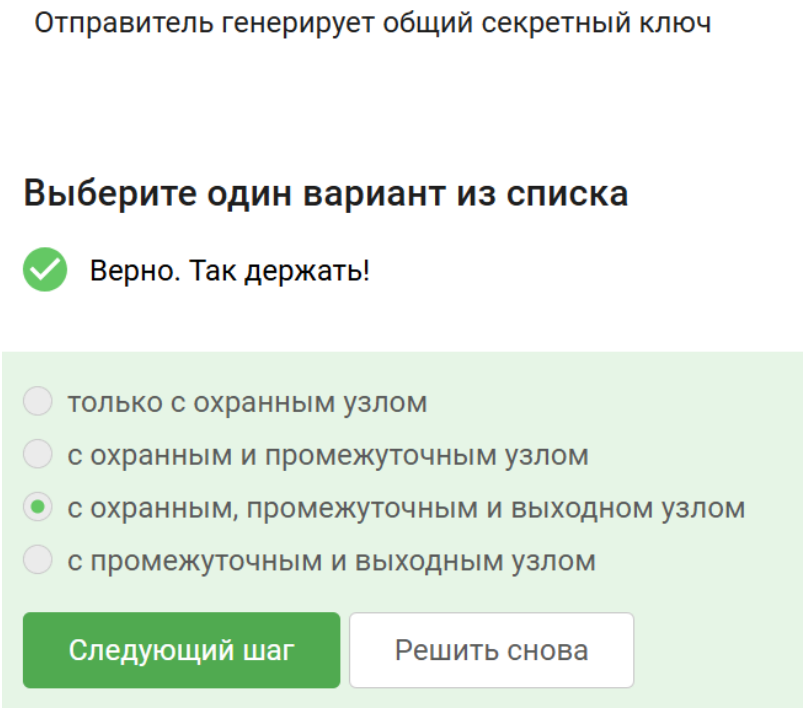

Рисунок 2.3-2

Комментарий: Общий секретный ключ генерируется отправителем для всех узлов маршрута (охранного, промежуточного и выходного), чтобы обеспечить шифрование на всём пути.

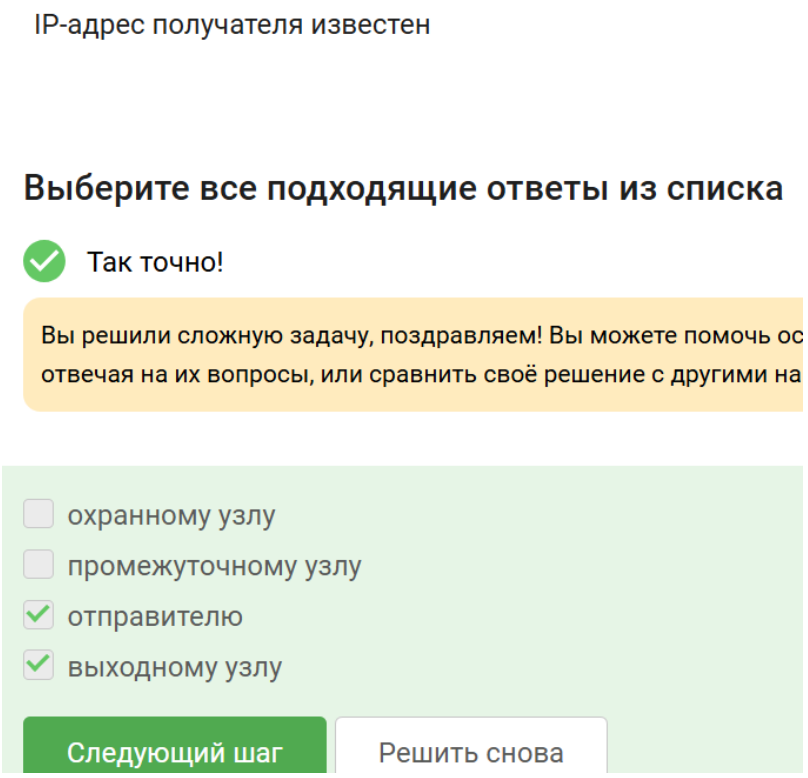

Рисунок 2.3-3

Комментарий: IP-адрес получателя известен только отправителю и выходному узлу — остальные узлы не имеют этой информации, что обеспечивает анонимность.

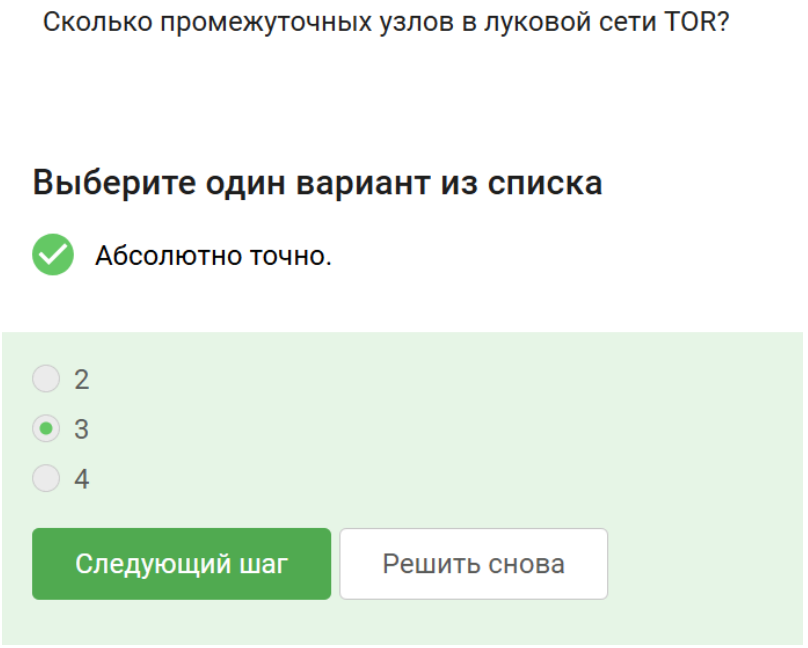

Рисунок 2.3-4

Комментарий: В луковой маршрутизации TOR используется 3 узла: охранный, промежуточный и выходной — они шифруют данные послойно, как "луковица".

2.4

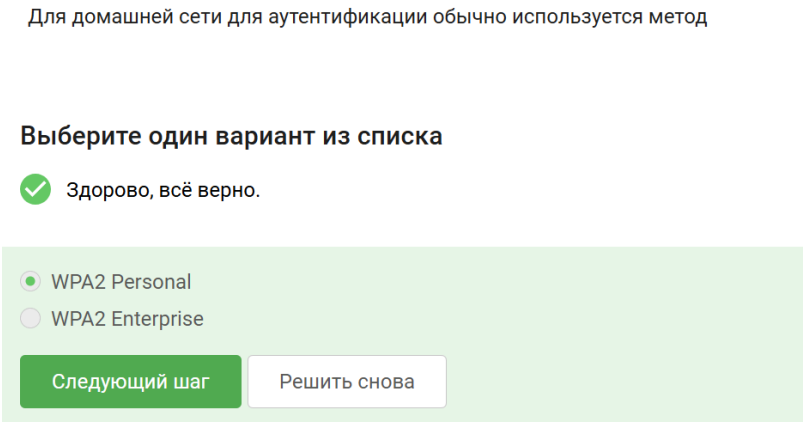

Рисунок 2.4-1

Комментарий: В домашних сетях чаще всего используется метод аутентификации WPA2 Personal, поскольку он основан на общем пароле и не требует сложной инфраструктуры.

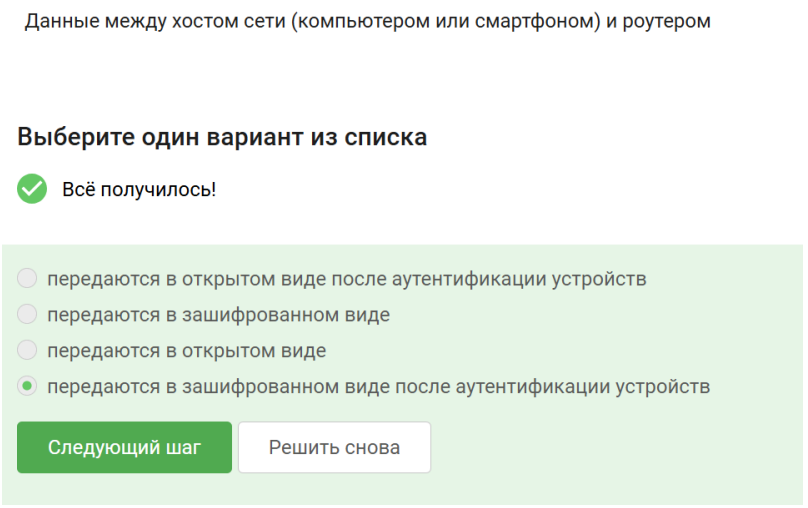

Рисунок 2.4-2

Комментарий: После успешной аутентификации устройства, данные между хостом и роутером передаются в зашифрованном виде — это основа безопасности беспроводных сетей.

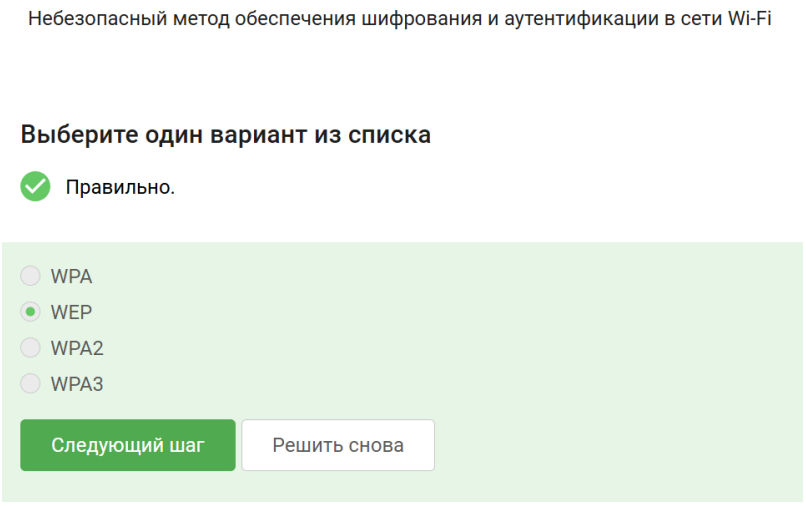

Рисунок 2.4-3

Комментарий: WEP — устаревший и уязвимый стандарт безопасности Wi-Fi, давно признан небезопасным, его использование не рекомендуется.

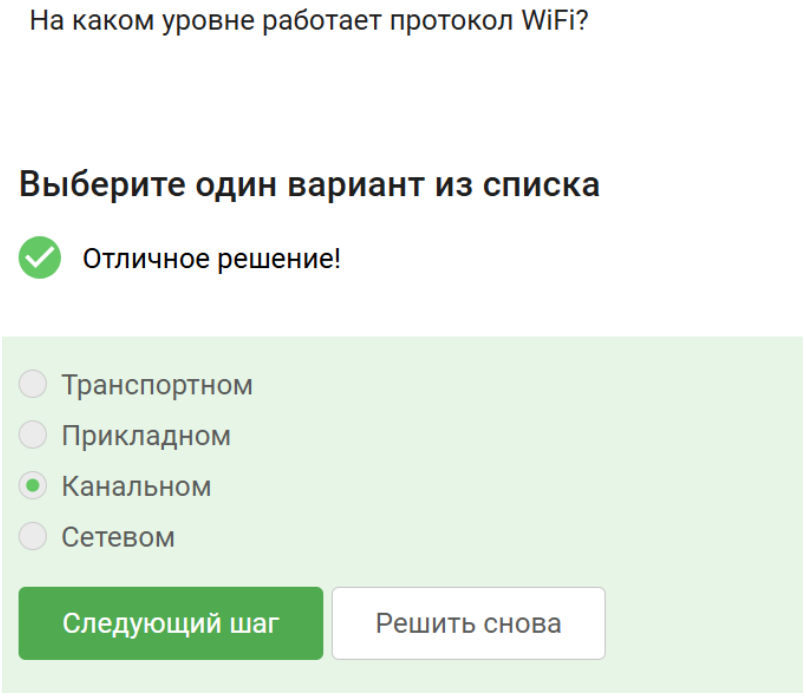

Рисунок 2.4-4

Комментарий: Протокол Wi-Fi работает на канальном уровне модели OSI, обеспечивая передачу кадров по беспроводному каналу.

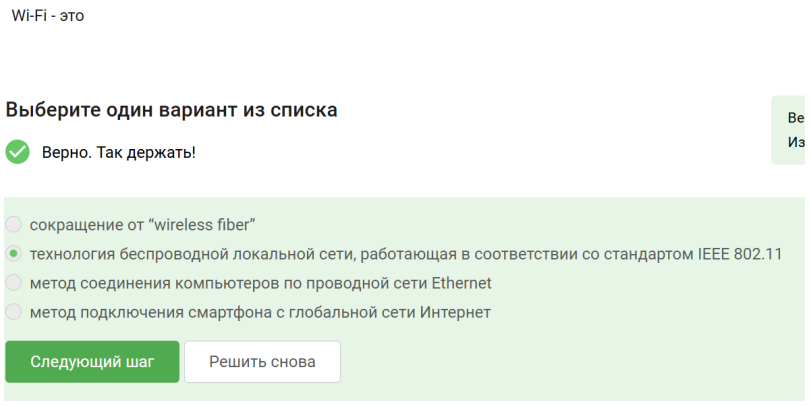

Рисунок 2.4-5

Комментарий: Wi-Fi — это технология беспроводной локальной сети (WLAN), работающая по стандарту IEEE 802.11.

3.1

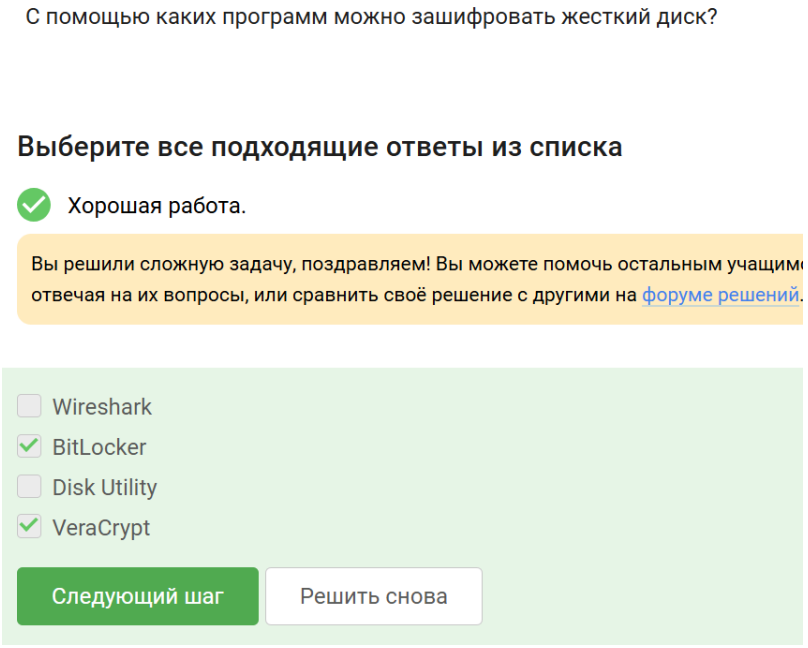

Рисунок 3.1-1

Комментарий: BitLocker, Disk Utility и VeraCrypt — это программы для шифрования жёстких дисков. Wireshark не подходит, так как используется для анализа сетевого трафика.

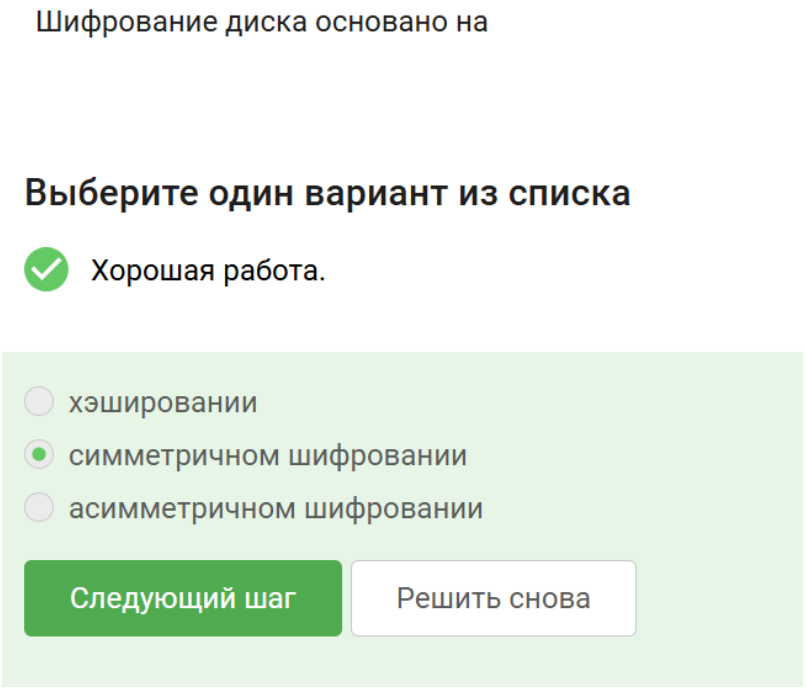

Рисунок 3.1-2

Комментарий: Шифрование диска обычно осуществляется с использованием симметричного шифрования — один ключ используется для шифрования и дешифрования данных.

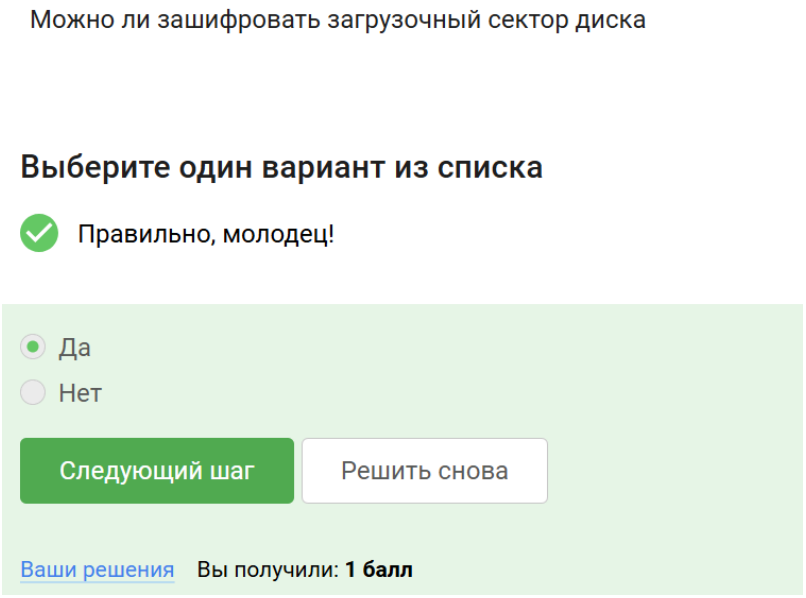

Рисунок 3.1-3

Комментарий: Загрузочный сектор диска может быть зашифрован — это делает всю систему защищённой, начиная с момента запуска.

3.2

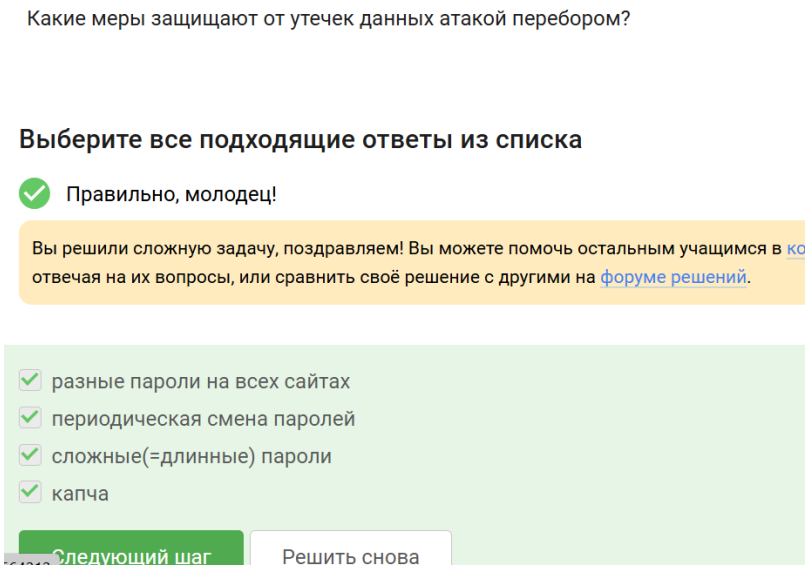

Рисунок 3.2-1

Комментарий: Все перечисленные меры — уникальные и сложные пароли, смена паролей и капча — эффективно защищают от атак методом перебора.

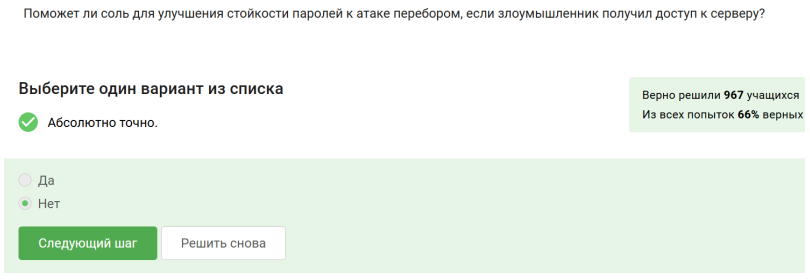

Рисунок 3.2-2

Комментарий: Соль не улучшает стойкость паролей при атаке перебором, если злоумышленник уже получил доступ к серверу. Она помогает против атак по словарю и радужных таблиц.

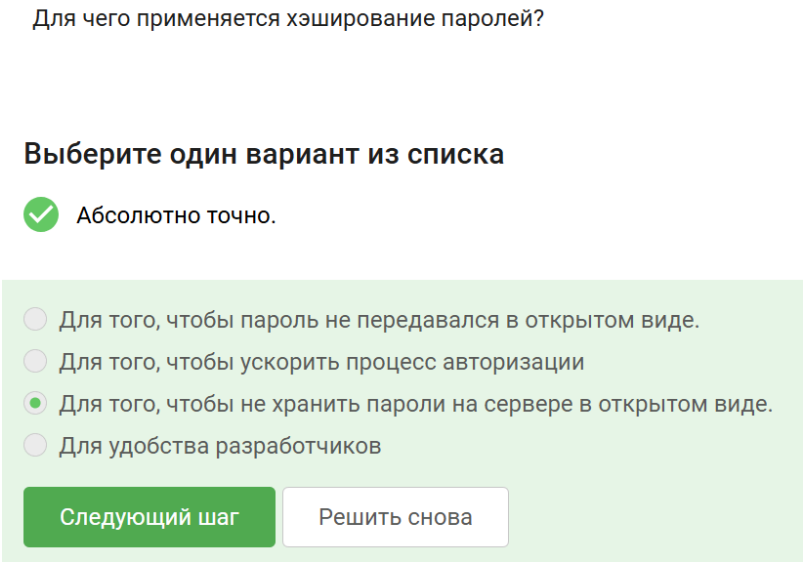

Рисунок 3.2-3

Комментарий: Хэширование паролей позволяет не хранить их в открытом виде — это критически важно для безопасности пользовательских данных.

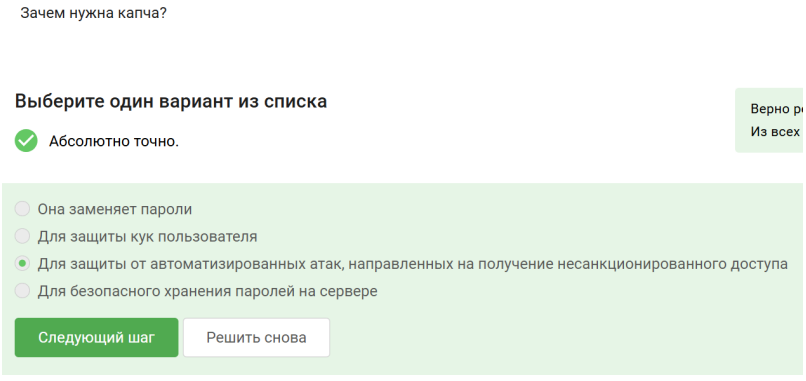

Рисунок 3.2-4

Комментарий: Капча используется для защиты от автоматизированных атак, предотвращая массовый перебор паролей ботами.

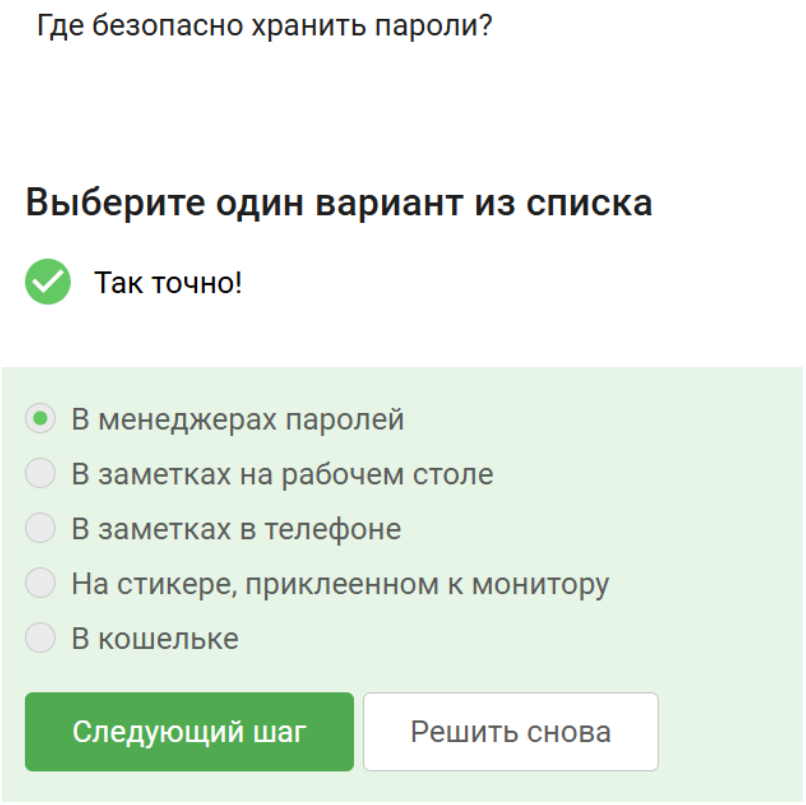

Рисунок 3.2-5

Комментарий: Пароли надёжнее всего хранить в специализированных менеджерах паролей, а не в заметках, файлах или на бумаге.

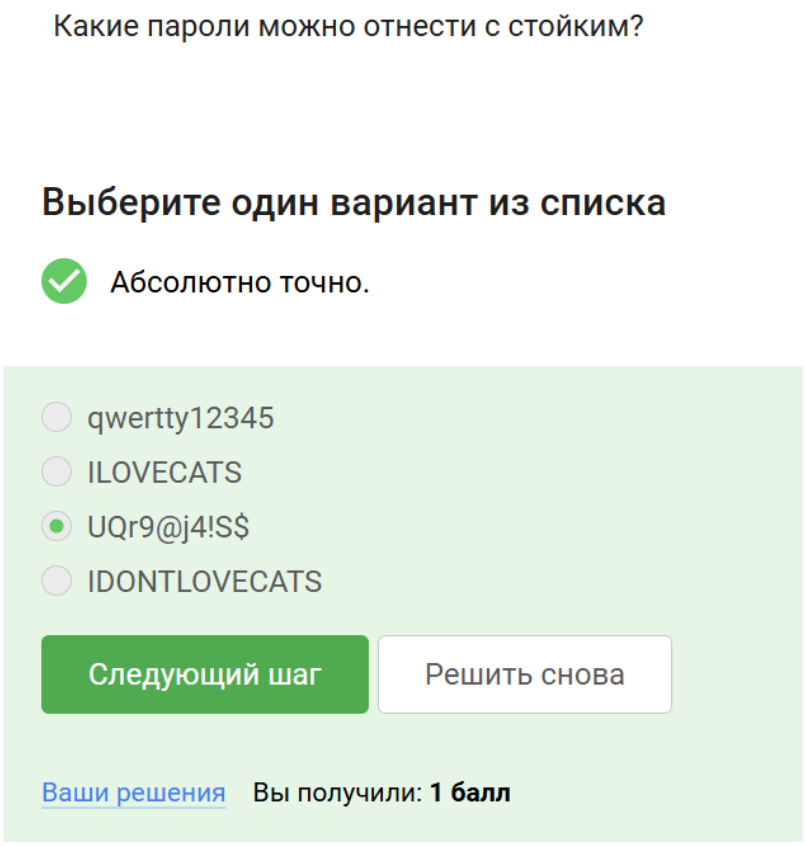

Рисунок 3.2-6

Комментарий: Стойкий пароль — это сложная комбинация символов, цифр и знаков. Пример `UQr9@j4!S$$` отвечает требованиям безопасности.

3.3

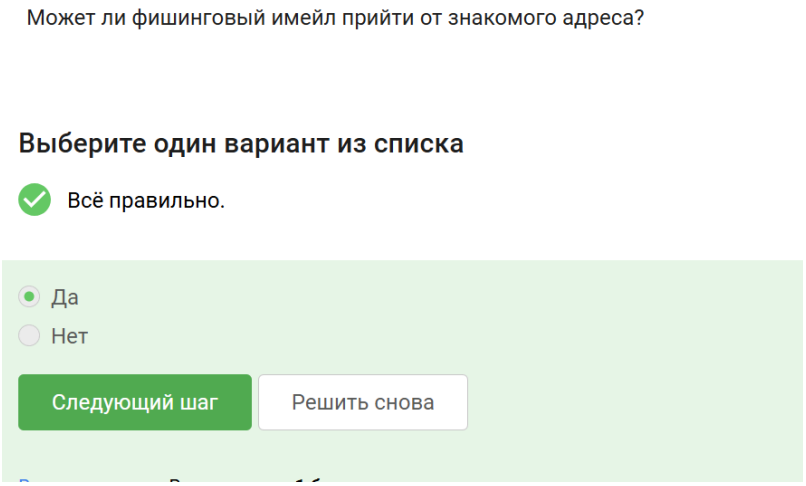

Рисунок 3.3-1

Комментарий: Фишинговый e-mail вполне может прийти от знакомого адреса — злоумышленники могут подделывать адрес отправителя (спуфинг) или взломать почту реального человека.

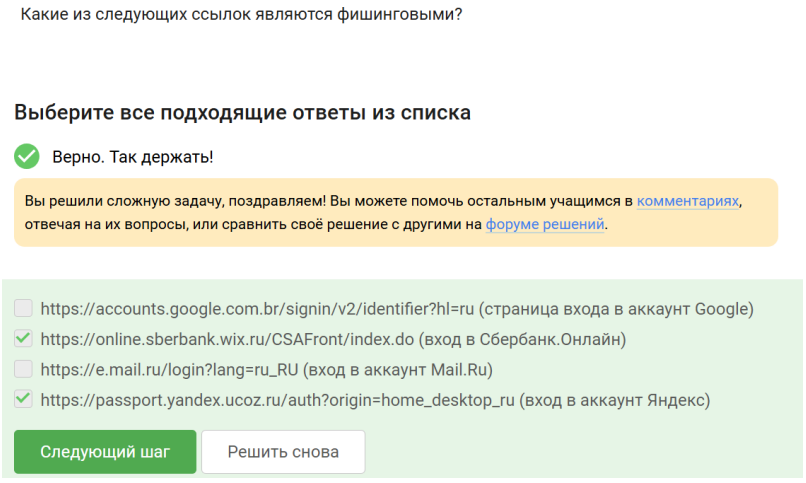

Рисунок 3.3-2

Комментарий: Ссылки с поддоменами известных компаний на чужих доменах (например, `wix.ru`, `ucoz.ru`) являются фишинговыми — они маскируются под легитимные сервисы, но ведут на сторонние ресурсы.

3.4

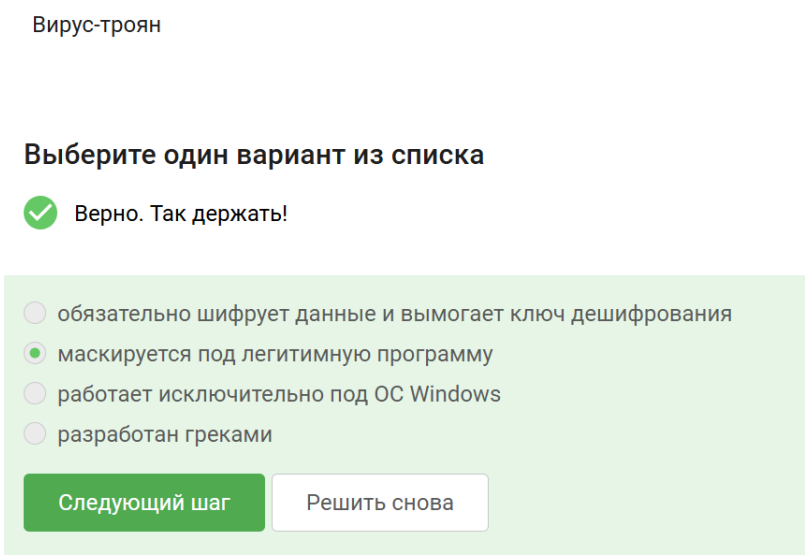

Рисунок 3.4-1

Комментарий: Троян — это тип вредоносного ПО, которое маскируется под легитимную программу, чтобы обманом заставить пользователя установить его на устройство.

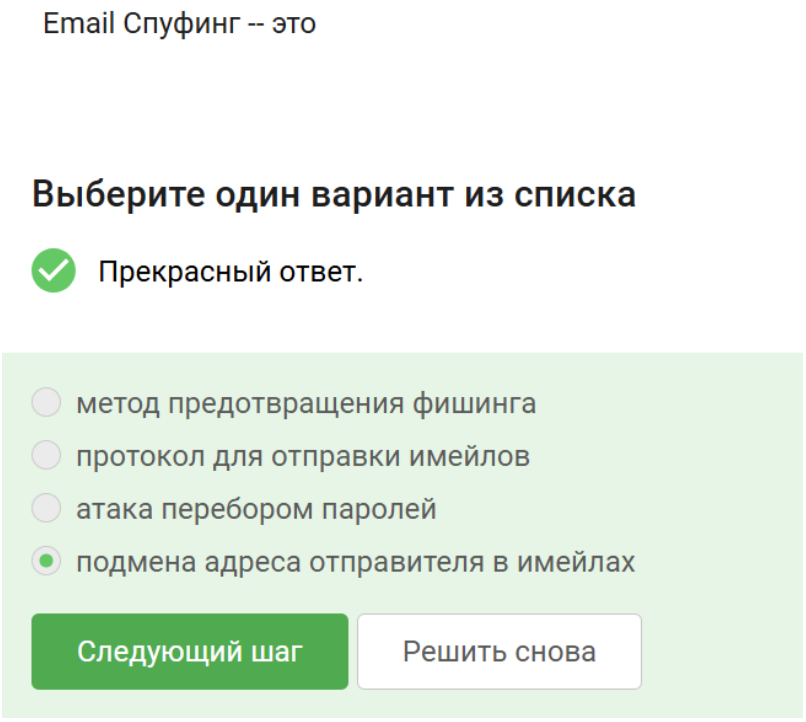

Рисунок 3.4-2

Комментарий: Email спуфинг — это подмена адреса отправителя, при которой письмо выглядит как отправленное с доверенного источника. Этот метод используется в фишинговых атаках для повышения доверия к письму.

3.5

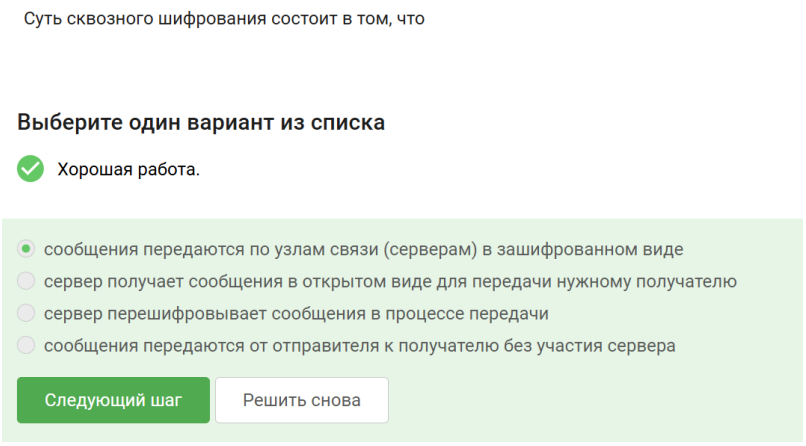

Рисунок 3.5-1

Комментарий: Суть сквозного шифрования (end-to-end encryption) заключается в том, что сообщение передаётся в зашифрованном виде через все промежуточные узлы, и только конечный получатель может его расшифровать.

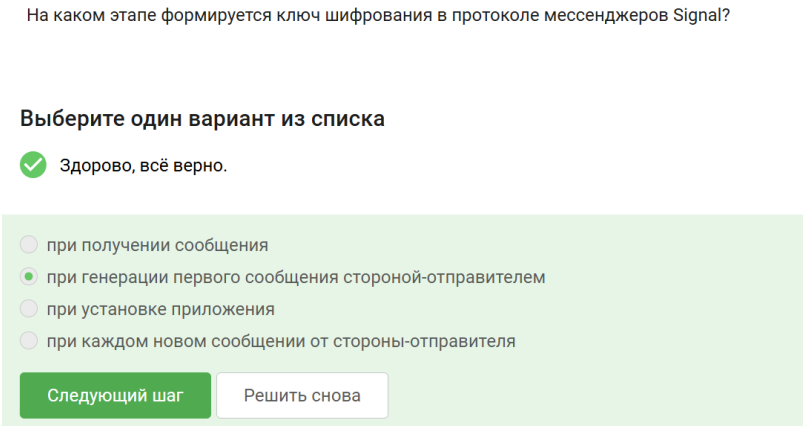

Рисунок 3.5-2

Комментарий: В протоколе Signal ключ шифрования формируется при генерации первого сообщения отправителем. Это позволяет обеспечить защиту информации с самого начала общения.

4.1

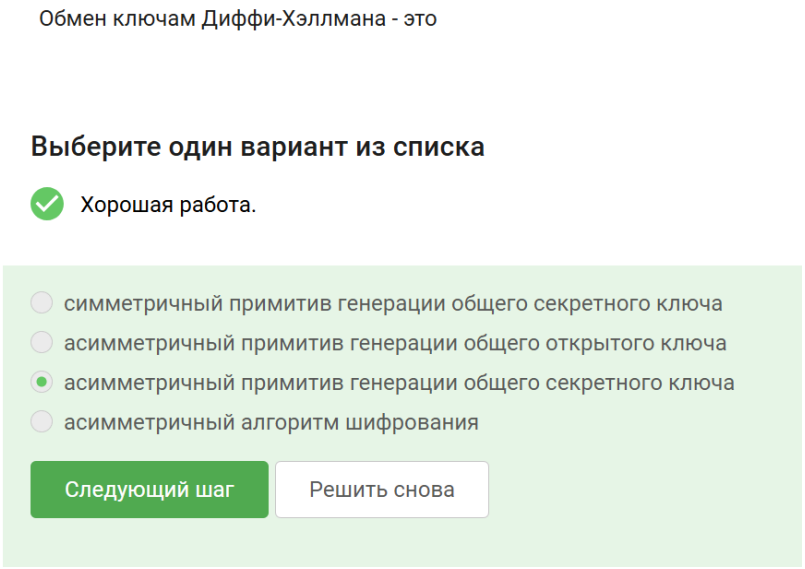

Рисунок 4.1-1

Комментарий: Диффи-Хеллман используется для генерации общего секретного ключа между двумя сторонами по открытому каналу. Поэтому правильный ответ — *асимметричный примитив генерации общего секретного ключа*.

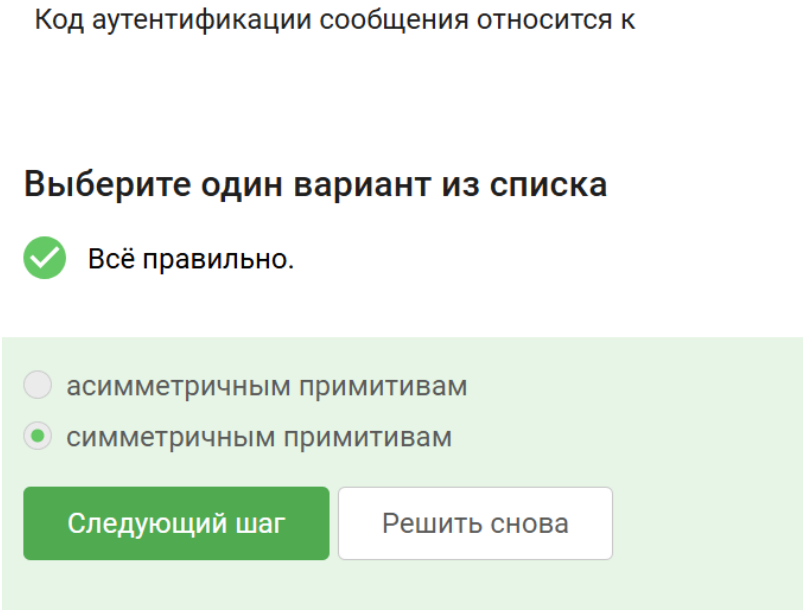

Рисунок 4.1-2

Комментарий: Код аутентификации сообщения (MAC) строится на основе симметричных криптографических примитивов, где используется общий секретный ключ.

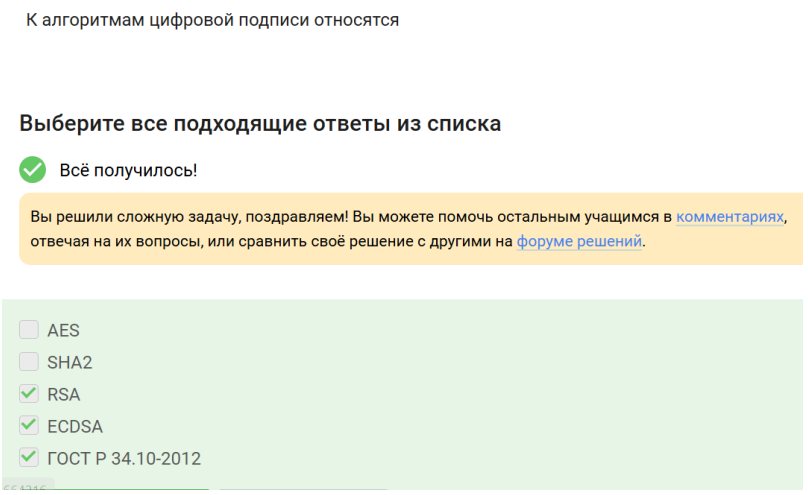

Рисунок 4.1-3

Комментарий: Алгоритмы RSA, ECDSA и ГОСТ Р 34.10-2012 являются стандартными схемами цифровой подписи. AES и SHA2 не относятся к цифровым подписям: AES — алгоритм шифрования, SHA2 — хеш-функция.

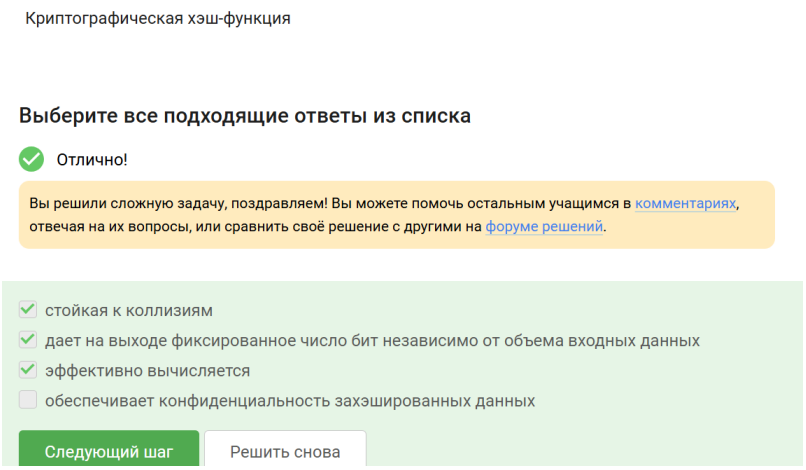

Рисунок 4.1-4

Комментарий: Хеш-функция должна быть стойкой к коллизиям, давать фиксированную длину хеша и эффективно вычисляться. Конфиденциальность данных — задача шифрования, а не хеширования.

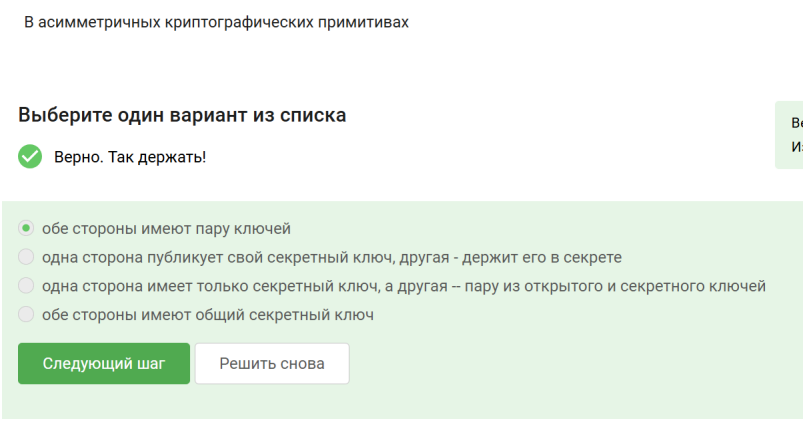

Рисунок 4.1-5

Комментарий: В асимметричной криптографии каждая сторона имеет пару ключей (открытый и закрытый), что позволяет безопасно обмениваться информацией и проверять подписи.

4.2

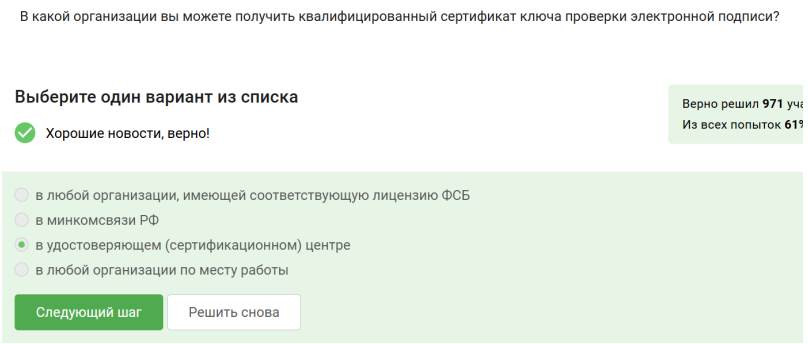

Рисунок 4.2-1

Комментарий: Квалифицированный сертификат ключа проверки электронной подписи можно получить только в удостоверяющем центре, так как именно он аккредитован для выпуска таких сертификатов в соответствии с законодательством.

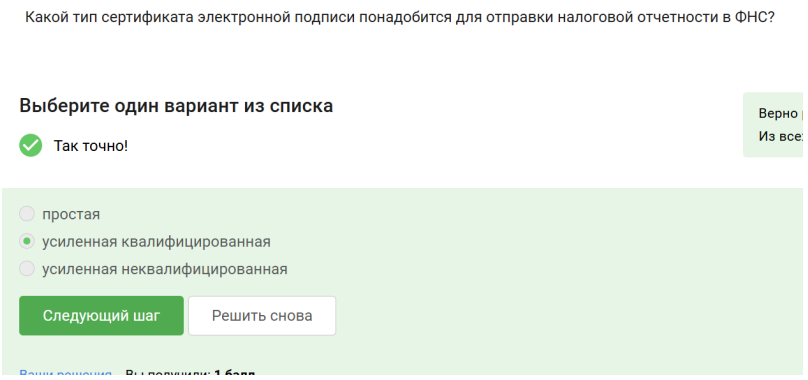

Рисунок 4.2-2

Комментарий: Для отправки отчётности в ФНС требуется усиленная квалифицированная электронная подпись, так как она имеет юридическую силу и соответствует требованиям к защите информации.

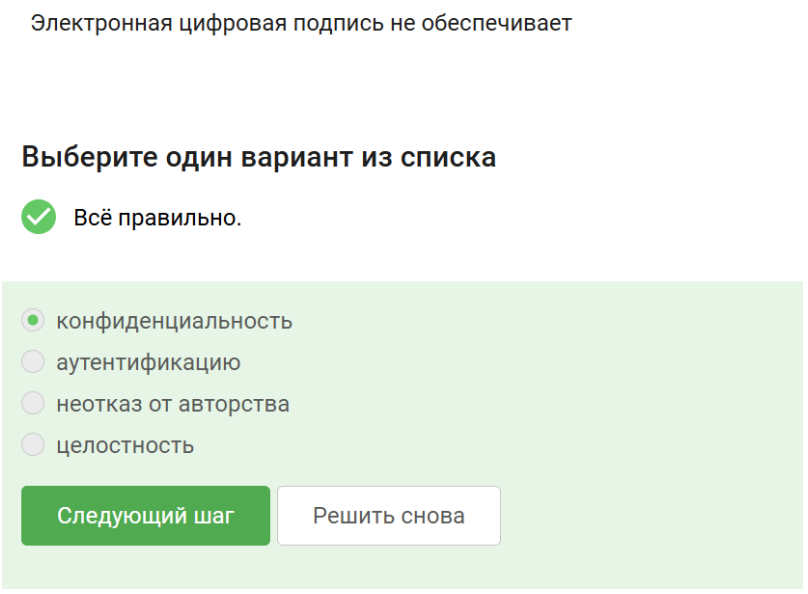

Рисунок 4.2-3

Комментарий: Электронная подпись не обеспечивает конфиденциальность, она используется для аутентификации, целостности и невозможности отказа от авторства, но не шифрует передаваемые данные.

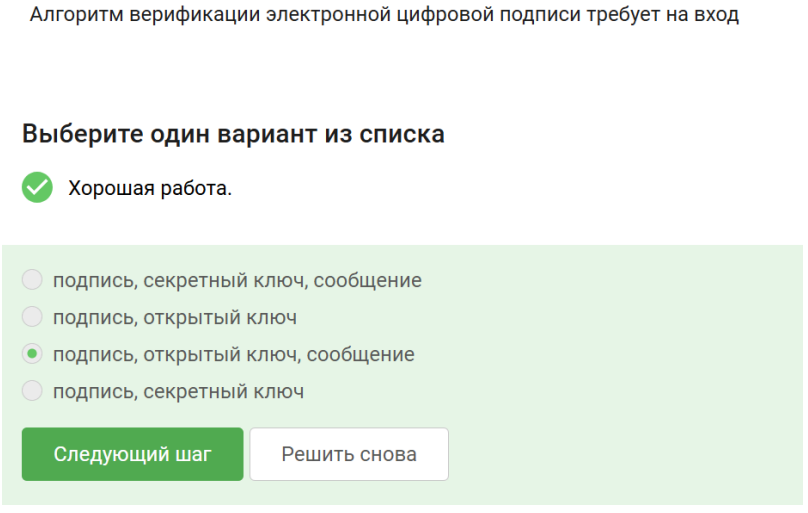

Рисунок 4.2-4

Комментарий: Для верификации электронной подписи необходимо использовать саму подпись, открытый ключ и сообщение — это позволяет проверить подлинность без знания закрытого ключа.

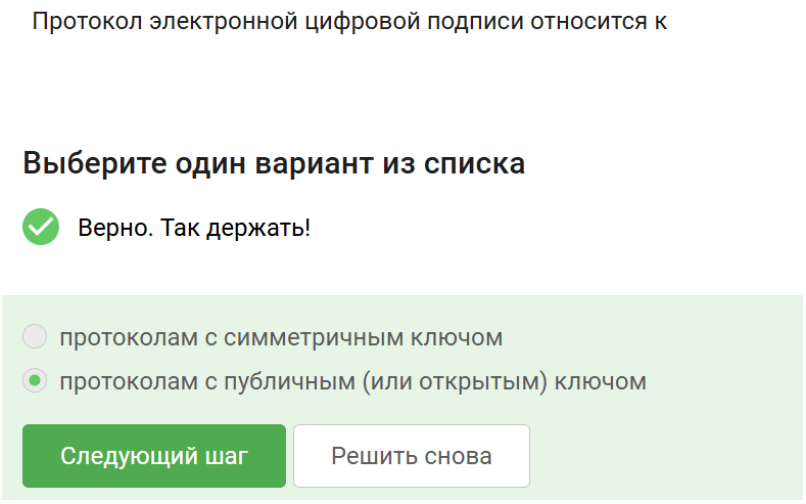

Рисунок 4.2-5

Комментарий: Протокол ЭЦП использует криптографию с открытым (публичным) ключом — именно эта модель обеспечивает проверку подписи без раскрытия закрытого ключа.

4.3

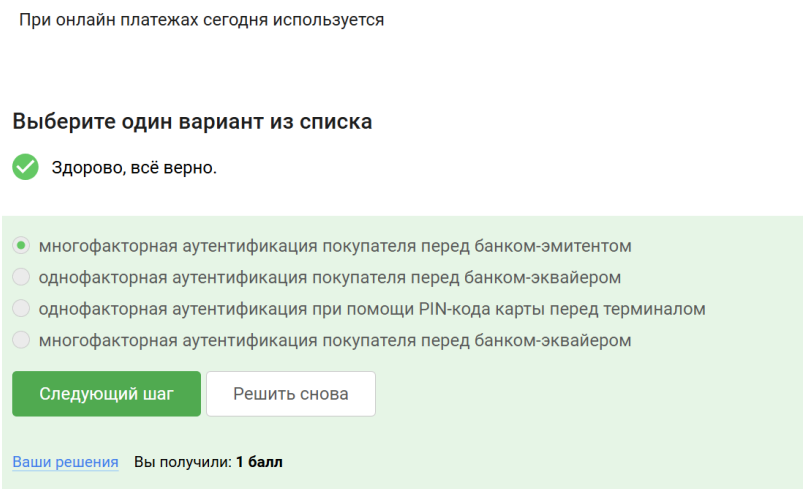

Рисунок 4.3-1

Комментарий: Сегодня при онлайн-платежах чаще всего используется многофакторная аутентификация перед банком-эмитентом — например, подтверждение через приложение или код из SMS, что позволяет надёжно идентифицировать пользователя.

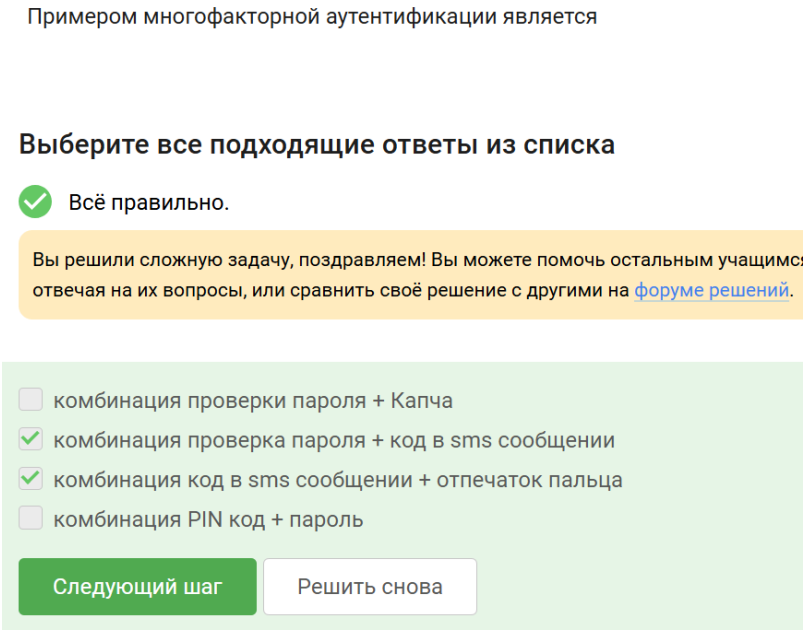

Рисунок 4.3-2

Комментарий: Многофакторная аутентификация — это сочетание разных факторов: знания (пароль), владения (смартфон с SMS), биометрии (отпечаток пальца). Поэтому комбинации пароля и кода, а также кода и отпечатка — корректные примеры.

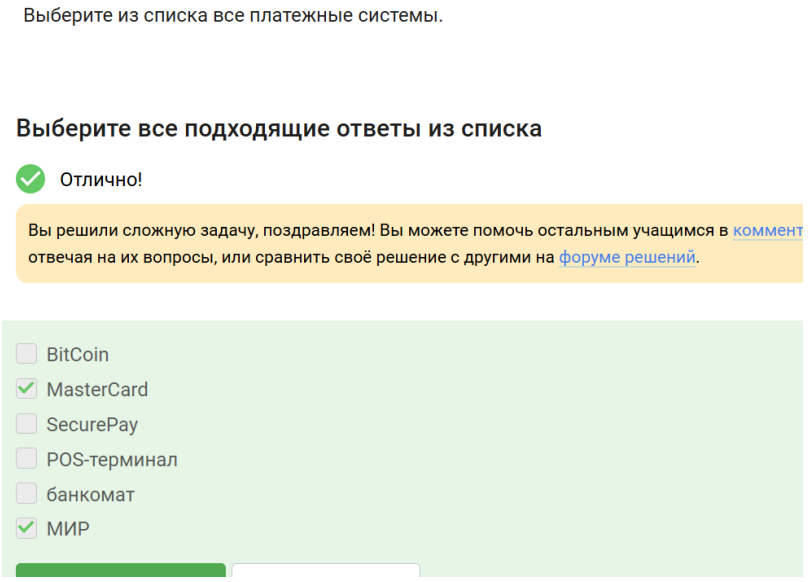

Рисунок 4.3-3

Комментарий: Платёжными системами являются именно сети и организации, обрабатывающие транзакции — например, MasterCard и МИР. Bitcoin — криптовалюта, а не платёжная система в традиционном смысле, POS-терминал и банкомат — устройства, а не системы.

4.4

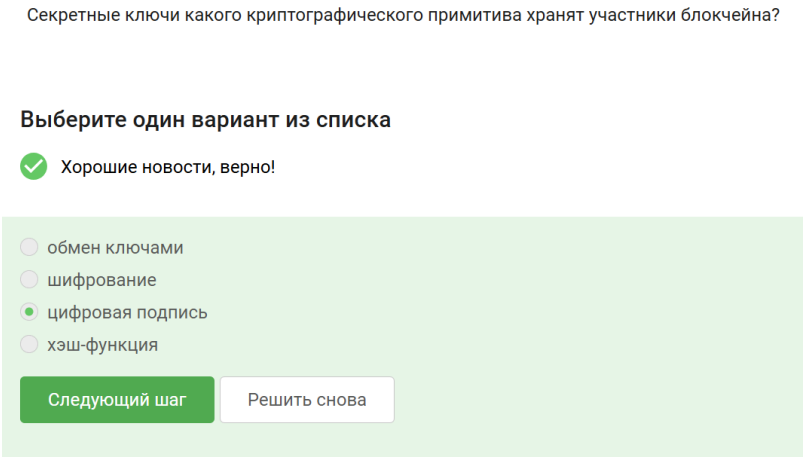

Рисунок 4.4-1

Комментарий: В блокчейне используются цифровые подписи, для которых участники хранят секретные ключи. Это необходимо для подтверждения подлинности транзакций и авторизации действий пользователя.

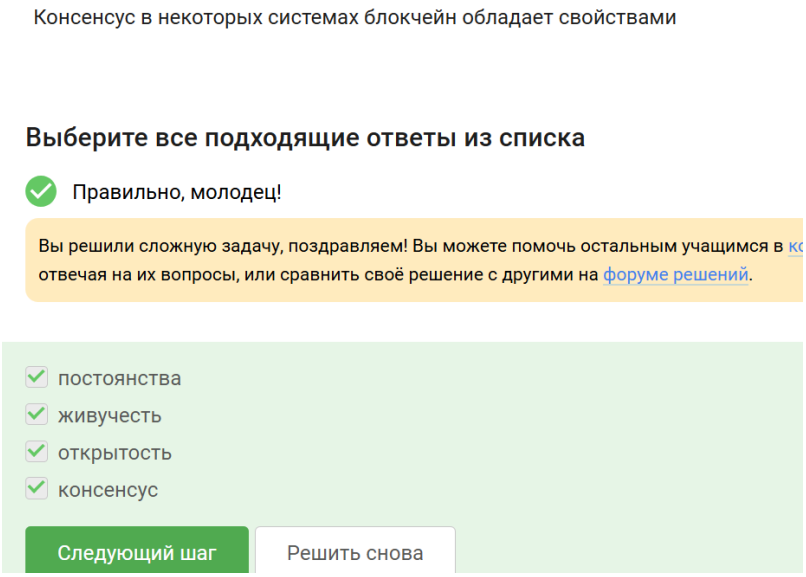

Рисунок 4.4-2

Комментарий: Консенсус в блокчейн-системах обладает такими свойствами, как постоянство (данные не меняются), живучесть (система продолжает работу), открытость (участие доступно всем) и сам консенсус — достижение единства между узлами.

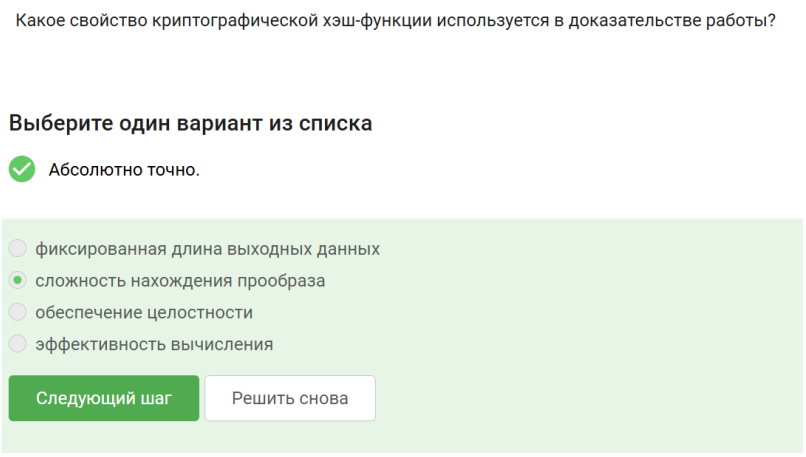

Рисунок 4.4-3

Комментарий: Свойство криптографической хэш-функции, критически важное для доказательства работы (Proof of Work), — это сложность нахождения прообраза. Она обеспечивает необходимую вычислительную нагрузку для подтверждения блока.

Выводы

В результате прохождения курса я получила базовые и прикладные знания в области информационной безопасности. Разобралась в принципах работы электронной подписи, видах сертификатов и ключей, а также в способах защиты от основных угроз. Курс оказался полезным и дал понимание, как безопасно работать с электронными документами и защищать свои данные.

Список литературы

1. https://stepik.org/course/111512