Внешний курс. Часть 1: Безопасность в сети

Основы информационной безопасности

Александрова У.В.

Содержание

1 Цель работы

Цель работы - выполнить контрольные задания первого раздела курса “Основы Кибербезопасности”

2 Выполнение заданий

2.1 Как работает интернет: базовые сетевые протоколы

HTTPS - протокол прикладного уровня (рис. 2.1).

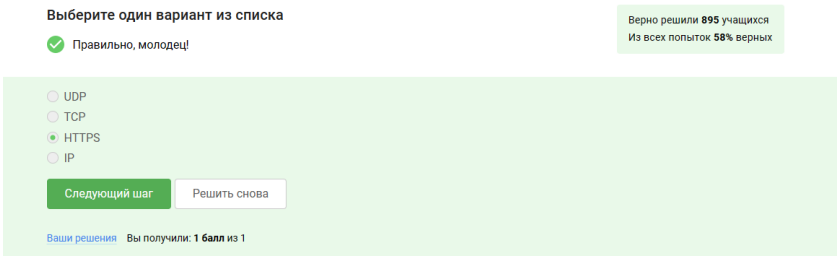

Рис. 2.1: Вопрос 2.1.1

Transmission control protocol работает на транспортном уровне (рис. 2.2).

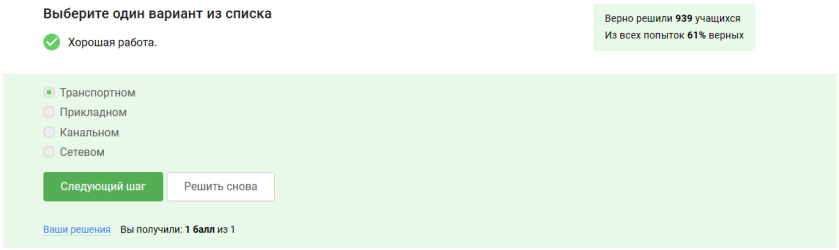

Рис. 2.2: Вопрос 2.1.2

В адресе типа IPv4 не может быть чисел больше 255 (рис. 2.3).

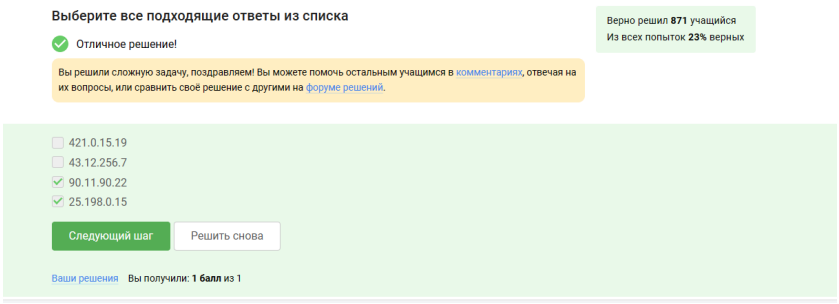

Рис. 2.3: Вопрос 2.1.3

DNS-сервер (рис. 2.4).

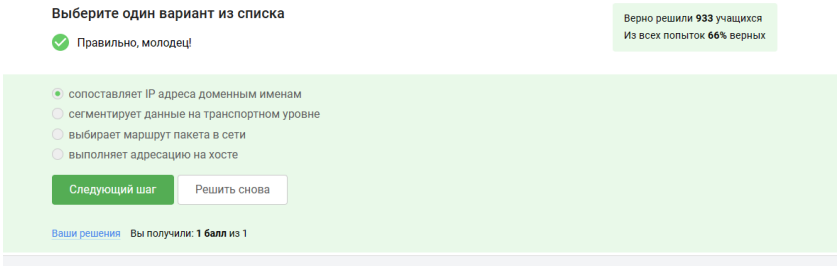

Рис. 2.4: Вопрос 2.1.4

Распределение протоколов в модели TCP/IP:

- Прикладной уровень: HTTP, RTSP, FTP, DNS.
- Транспортный уровень: TCP, UDP, SCTP, DCCP.
- Сетевой (Межсетевой) уровень: IP.
- Уровень сетевого доступа (Канальный): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring, ATM и MPLS. (рис. 2.5).

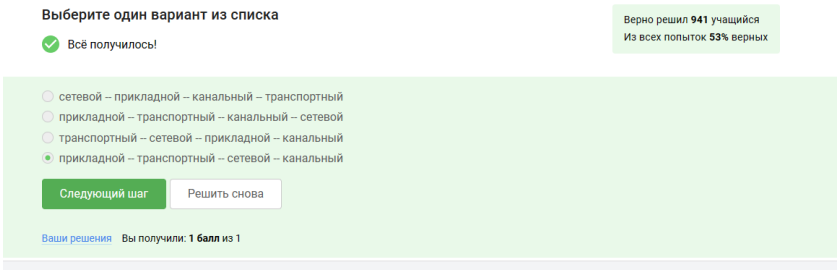

Рис. 2.5: Вопрос 2.1.5

Протокол http передает не зашифрованные данные (а https передает уже зашифрованные) (рис. 2.6).

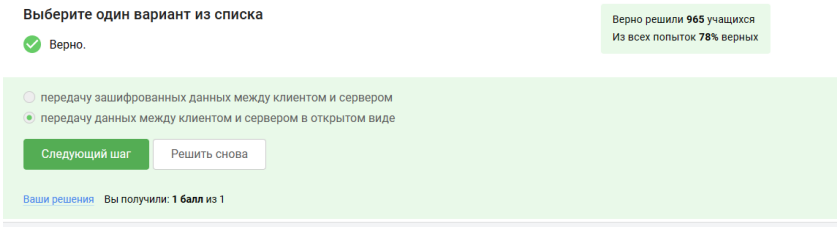

Рис. 2.6: Вопрос 2.1.6

Https передает зашифрованные данные, поэтому одна из фаз - передача данных, другая должна быть рукопожатием (рис. 2.7).

Рис. 2.7: Вопрос 2.1.7

TLS определяется как клиентом, так и сервером (рис. 2.8).

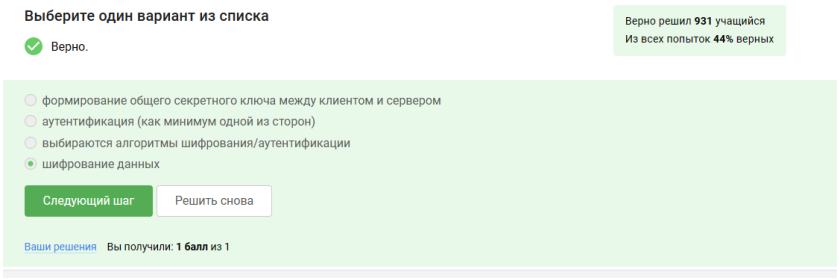

Рис. 2.8: Вопрос 2.1.8

Шифрование данных (рис. 2.9).

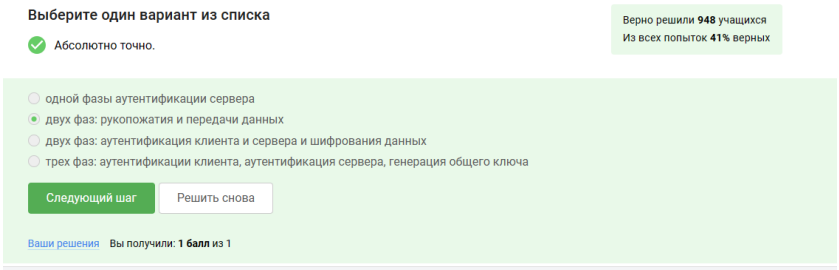

Рис. 2.9: Вопрос 2.1.9

2.2 Персонализация сети

Куки хранят ID сессии и идентификатор (рис. 2.10).

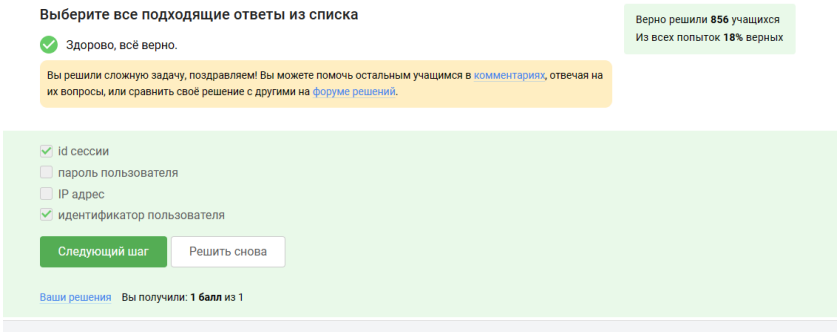

Рис. 2.10: Вопрос 2.2.1

Куки не делают соединение более надежным, даже наоборот (рис. 2.11).

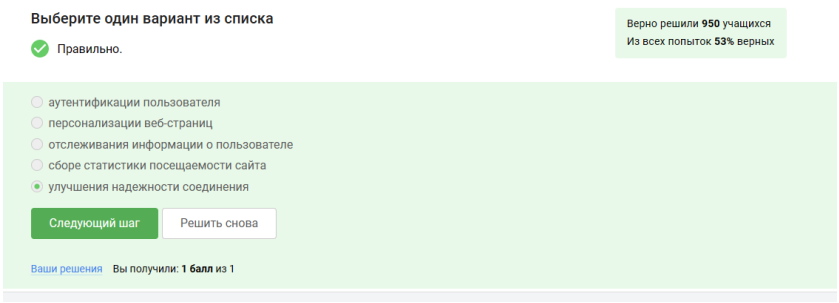

Рис. 2.11: Вопрос 2.2.2

Куки генерируются сервером (рис. 2.12).

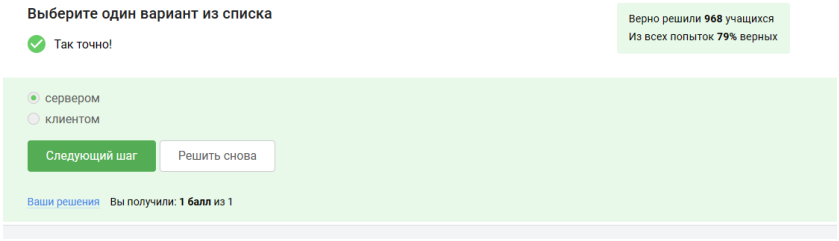

Рис. 2.12: Вопрос 2.2.3

Сессионные куки хранятся лишь в течение сессии (рис. 2.13).

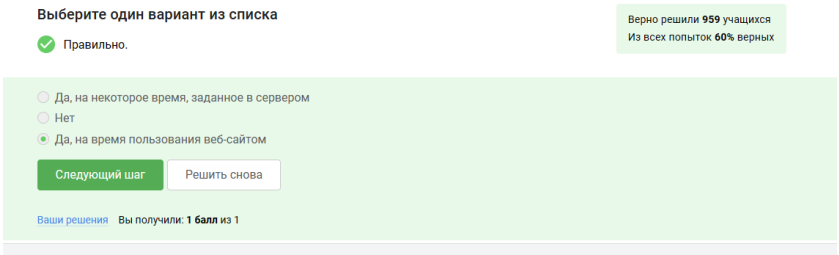

Рис. 2.13: Вопрос 2.2.4

2.3 Браузер TOR

Необходимо три узла: входной, промежуточный и выходной (рис. 2.14).

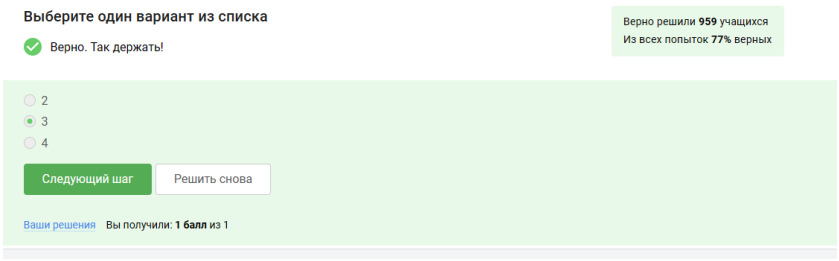

Рис. 2.14: Вопрос 2.3.1

IP-адрес не должен быть известен охранному и промежуточному узлам (рис. 2.15).

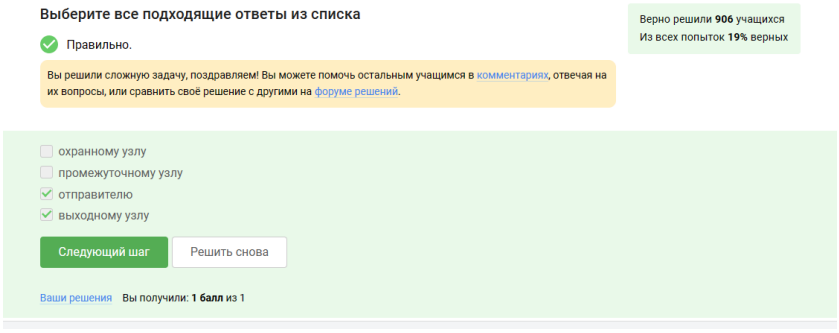

Рис. 2.15: Вопрос 2.3.2

Отправитель генерирует общий секретный ключ с узлами, через которые идет передача, то есть со всеми (рис. 2.16).

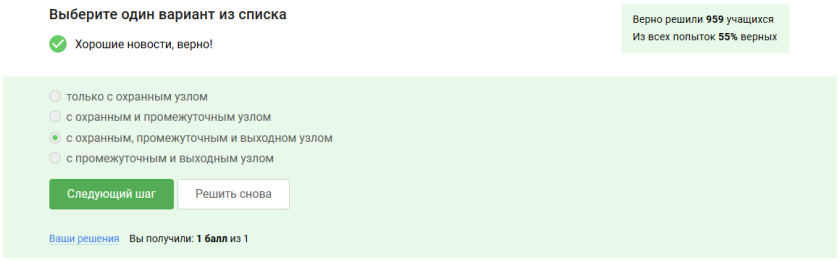

Рис. 2.16: Вопрос 2.3.3

Для получения пакетов не обязательно использовать TOR (рис. 2.17).

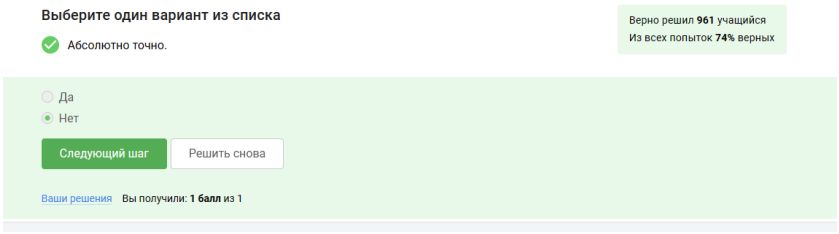

Рис. 2.17: Вопрос 2.3.4

2.4 Беспроводные сети Wi-fi

Wi-Fi (рис. 2.18).

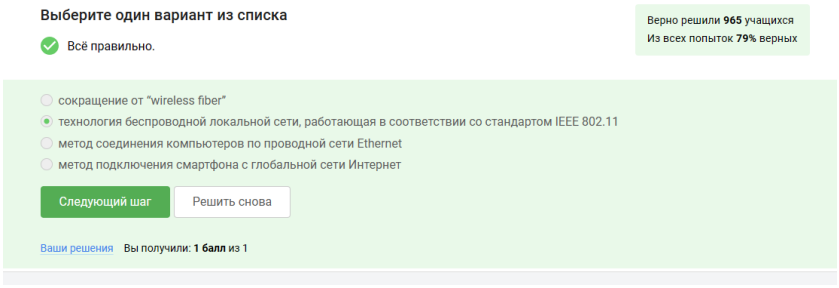

Рис. 2.18: Вопрос 2.4.1

Wi-Fi располагается как канальный уровень ниже интернет-уровня интернет-протокола (рис. 2.19).

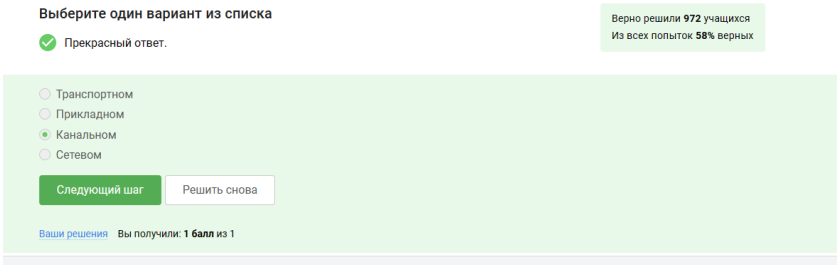

Рис. 2.19: Вопрос 2.4.2

WEP (Wired Equivalent Privacy) – устаревший и небезопасный метод проверки подлинности (рис. 2.20).

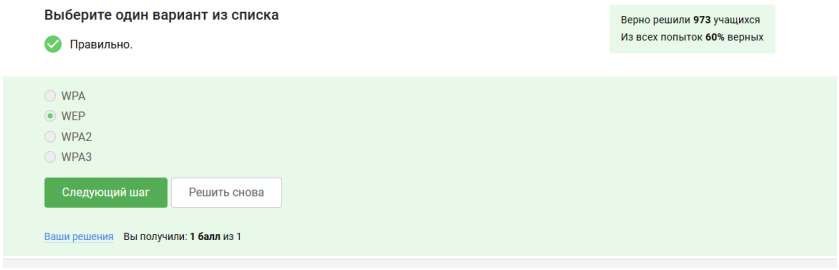

Рис. 2.20: Вопрос 2.4.3

Нужно аутентифицировать устройства, а потом передать зашифрованные данные (рис. 2.21).

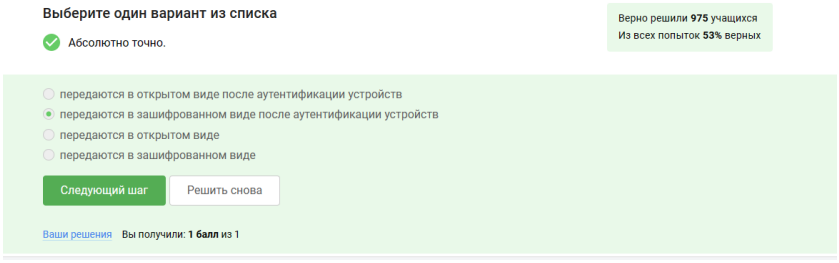

Рис. 2.21: Вопрос 2.4.4

WPA2 Personal для личного использования, a enterprise - для предпиятий (рис. 2.22).

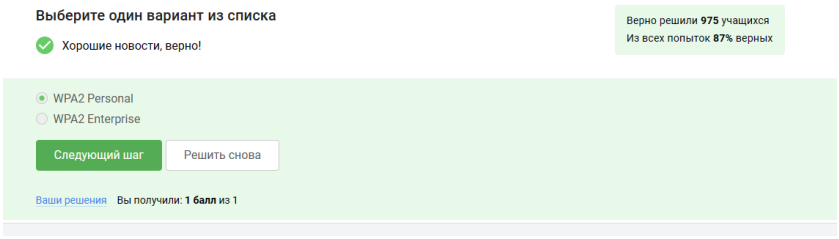

Рис. 2.22: Вопрос 2.4.5

3 Выводы

Я выполнила задания первого раздела внешнего курса и получила знания о работе базовых сетевых протоколов, куки сетей Wi-Fi и браузера TOR.

Внешний курс. Часть 2: Защита ПК/Телефона

Основы информационной безопасности

Александрова У.В.

Содержание

1 Цель работы

Цель работы - выполнение контрольных заданий второго раздела курса “Основы Кибербезопасности”.

2 Выполнение блока 2: Защита ПК/Телефона

2.1 Шифрование диска

Зашифровать загрузочный сектор диска можно (рис. 2.1).

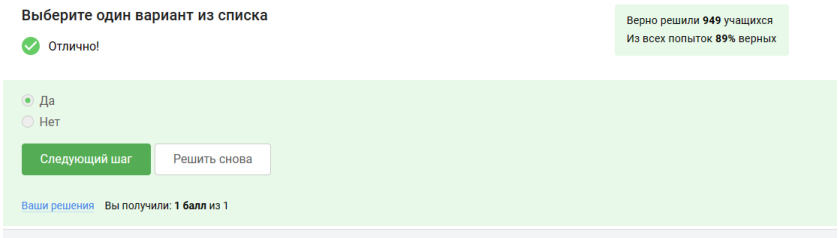

Рис. 2.1: Вопрос 3.1.1

Шифрование диска основано на симметричном шифровании (рис. 2.2).

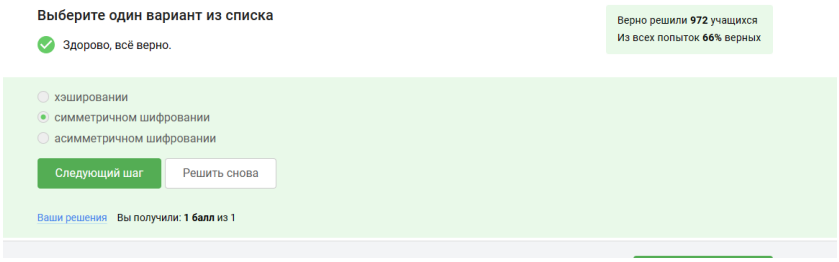

Рис. 2.2: Вопрос 3.1.2

С помощью этих пррограмм можно зашифровать жесткий диск (рис. 2.3).

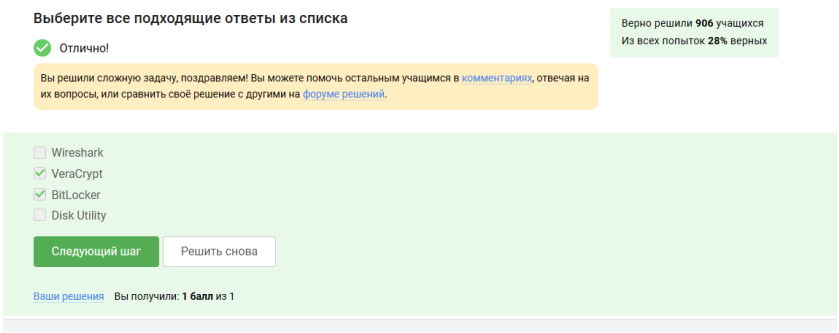

Рис. 2.3: Вопрос 3.1.3

2.2 Пароли

Стойкий пароль должен быть со специальными символами и достаточной длины (рис. 2.4).

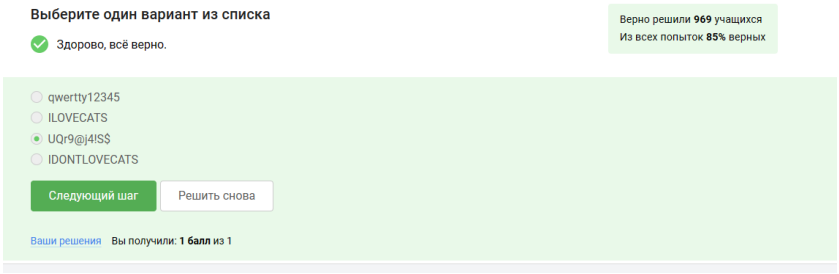

Рис. 2.4: Вопрос 3.2.1

Менеджер паролей - это самый безопасный вариант (рис. 2.5).

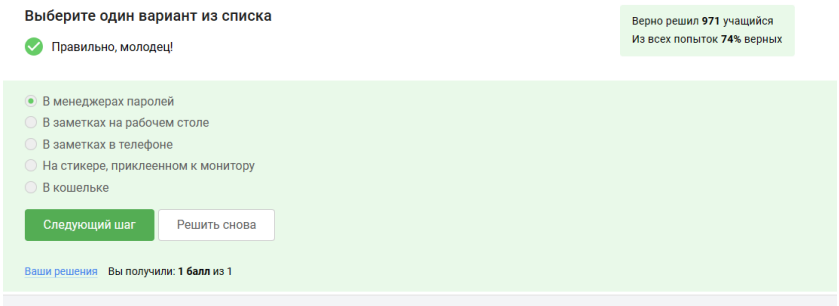

Рис. 2.5: Вопрос 3.2.2

Капча нужна для проверки на то, что за экраном не бот (рис. 2.6).

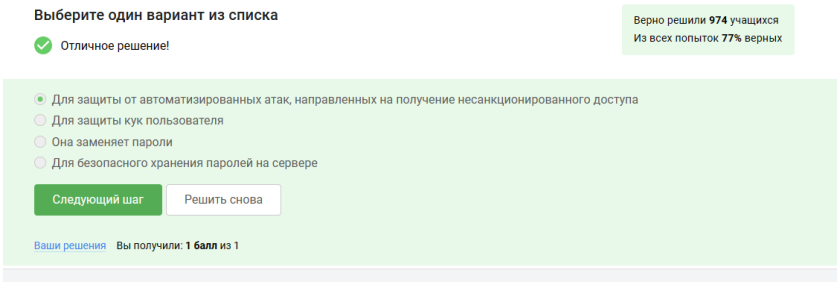

Рис. 2.6: Вопрос 3.2.3

Опасно хранить пароли в открытом виде, для этого есть хэши (рис. 2.7).

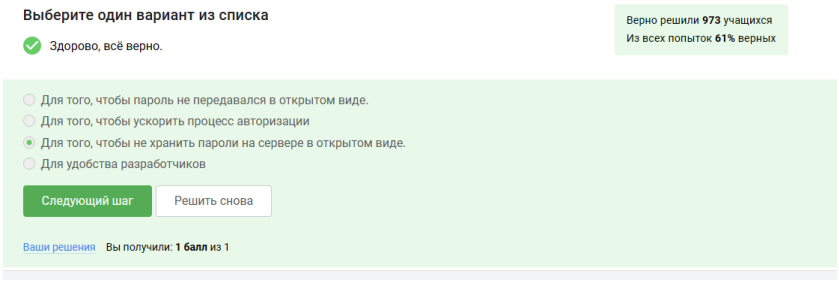

Рис. 2.7: Вопрос 3.2.4

Соль не может помочь для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу (рис. 2.8).

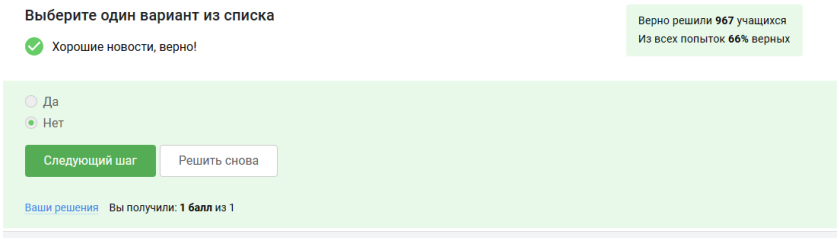

Рис. 2.8: Вопрос 3.2.5

Все приведенные меры верны (рис. 2.9).

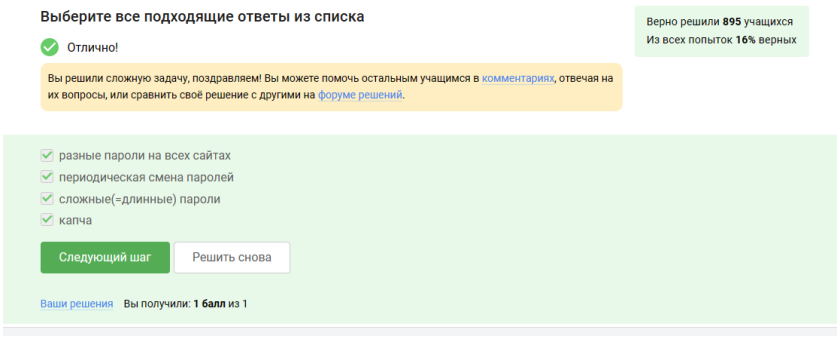

Рис. 2.9: НВопрос 3.2.6

2.3 Фишинг

В фишинговых ссылках есть отличия (рис. 2.10).

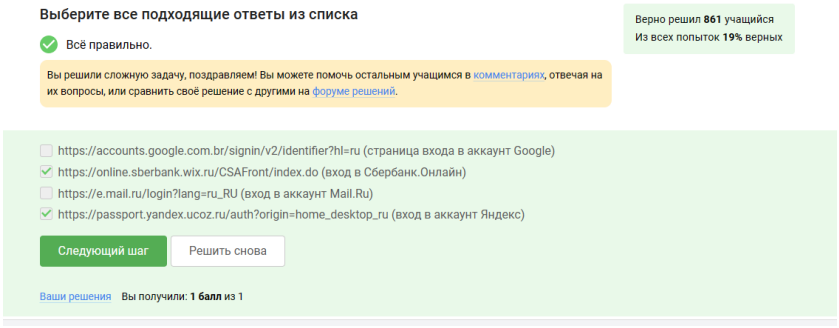

Рис. 2.10: Вопрос 3.3.1

Да, может, если пользователя со знакомым адресом взломали (рис. 2.11).

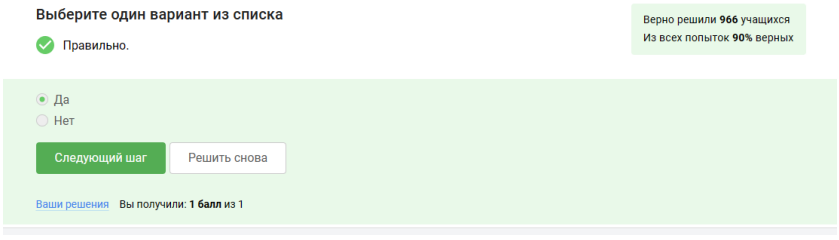

Рис. 2.11: Вопрос 3.3.2

2.4 Вирусы. Примеры

Email Спуфинг – это (рис. 2.12).

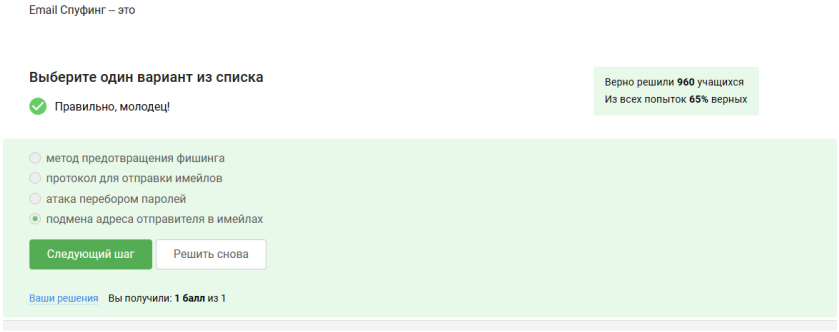

Рис. 2.12: Вопрос 3.4.1

Троян маскируется под обычную программу (рис. 2.13).

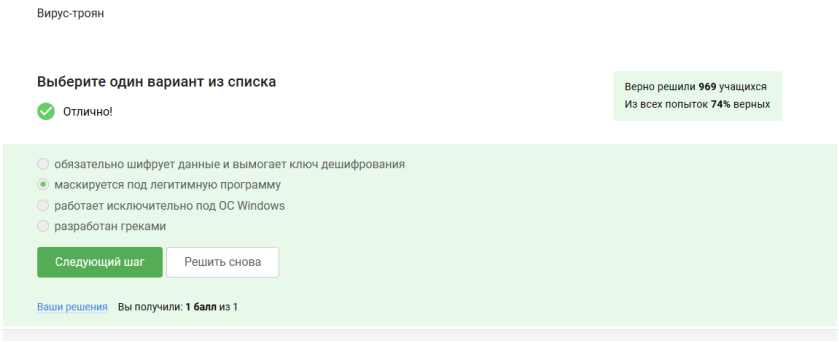

Рис. 2.13: Вопрос 3.4.2

2.5 Безопасность мессенджеров

При установке первого сообщения отправителем формируется ключ шифрования (рис. 2.14).

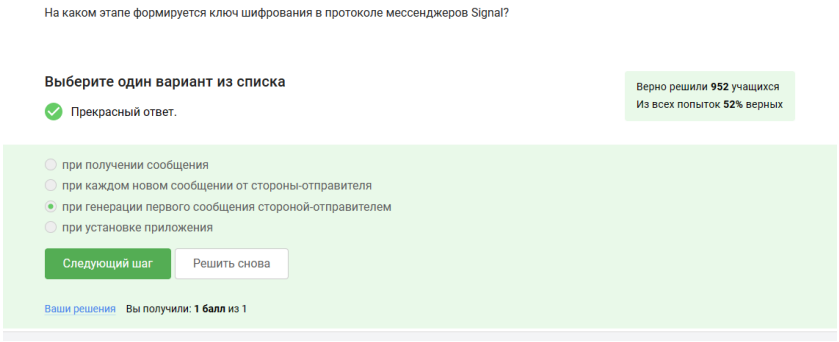

Рис. 2.14: Вопрос 3.5.1

Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде (рис. 2.15).

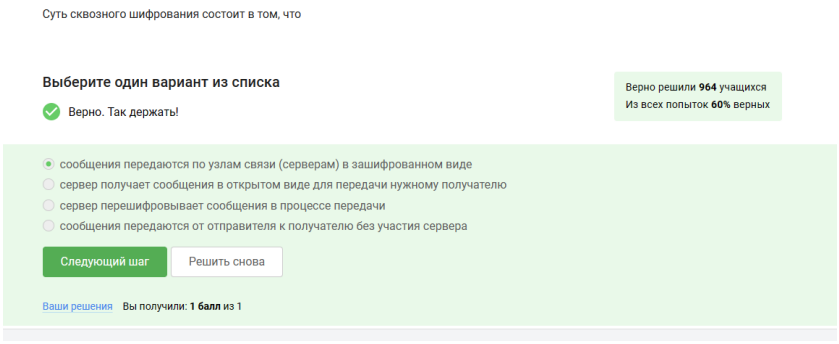

Рис. 2.15: Вопрос 3.5.2

3 Выводы

Я прошла второй раздел внешнего курса и получила знания о правилах хранения паролей и основную информацию о вирусах.

Внешний курс. Раздел 3: Криптография на практике

Основы информационной безопасности

Александрова У.В.

Содержание

1 Цель работы

Цель работы - выполнить контрольные задания третьего раздела курса “Основы Кибербезопасности”.

2 Выполнение блока 3: Криптография на практике

2.1 Введение в криптографию

Определение ассмиетричного шифрования с двумя ключами (рис. 2.1).

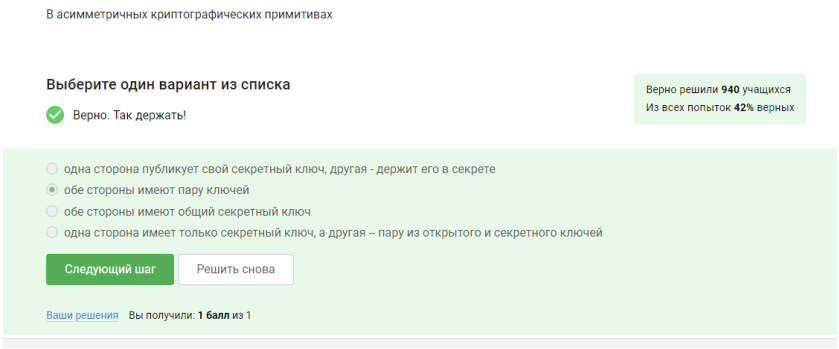

Рис. 2.1: Вопрос 4.1.1

Условия криптографической хэш-функции (рис. 2.2).

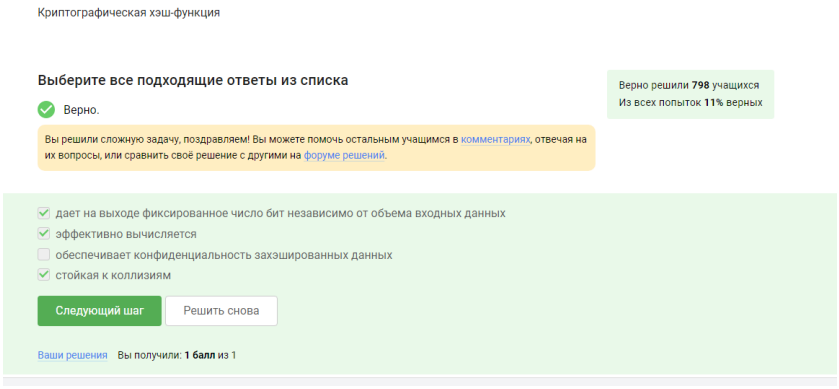

Рис. 2.2: Вопрос 4.1.2

Алгоритмы цифровой подписи (рис. 2.3).

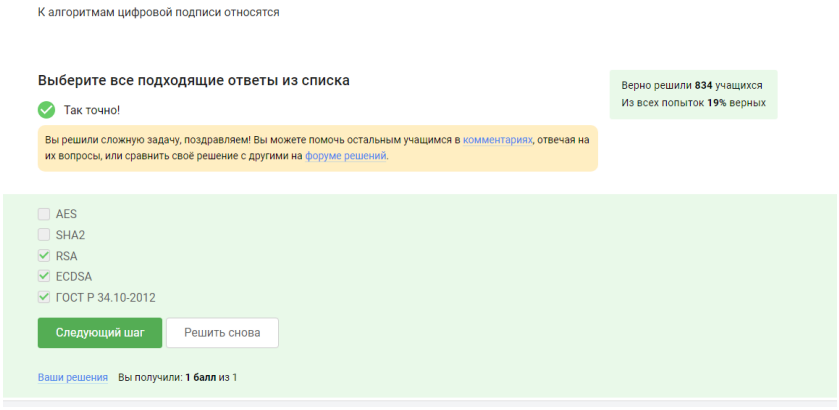

Рис. 2.3: Вопрос 4.1.3

Аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (рис. 2.4)

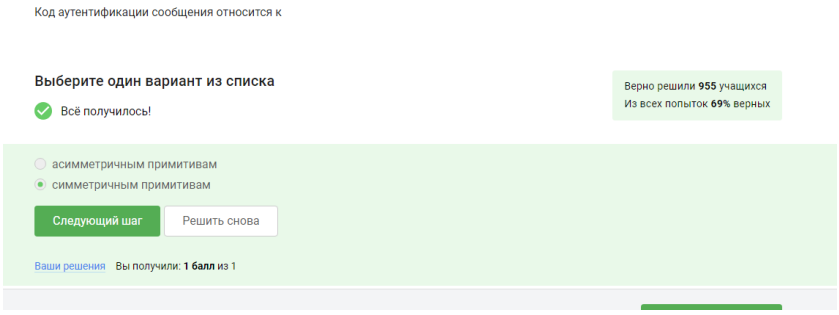

Рис. 2.4: Вопрос 4.1.4

Обмен ключам Диффи-Хэллмана - это (рис. 2.5).

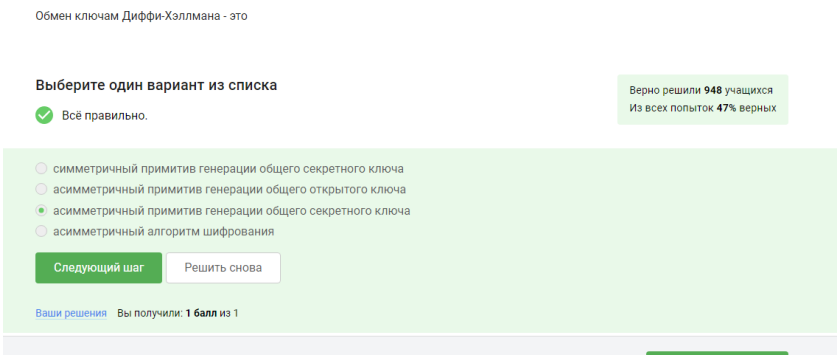

Рис. 2.5: Вопрос 4.1.5

2.2 Цифровая подпись

Протокол ЭЦП относится к протоколам с публичным ключом (рис. 2.6).

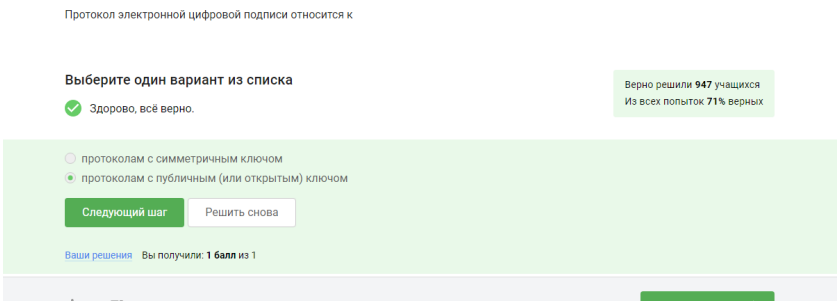

Рис. 2.6: Вопрос 4.2.1

Алгоритм верификации электронной цифровой подписи требует на вход подпись, открытый ключ и сообщение (рис. 2.7).

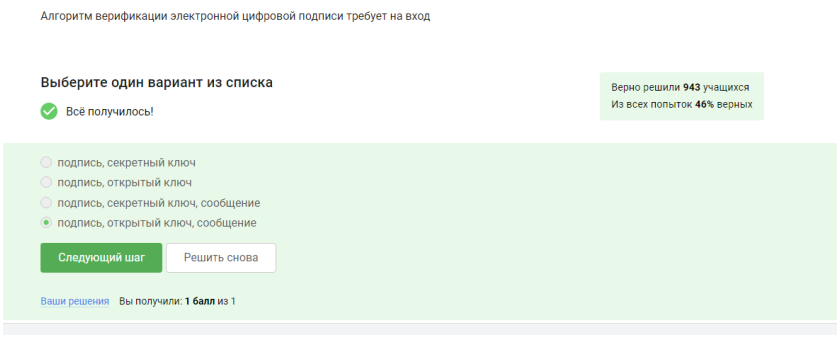

Рис. 2.7: Вопрос 4.2.2

Электронная подпись не обеспечивает обеспечивает конфиденциальность (рис. 2.8).

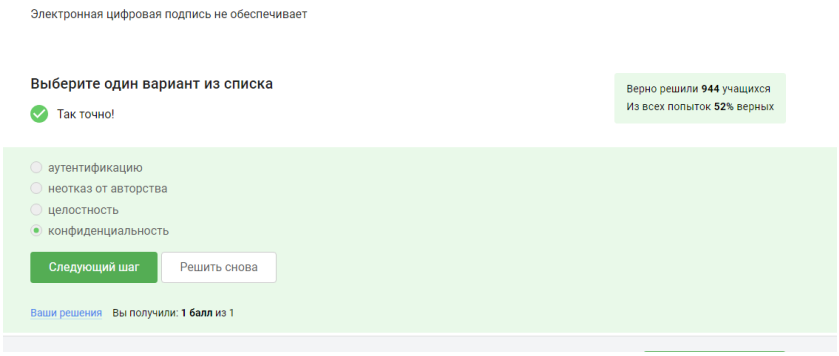

Рис. 2.8: Вопрос 4.2.3

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись (рис. 2.9).

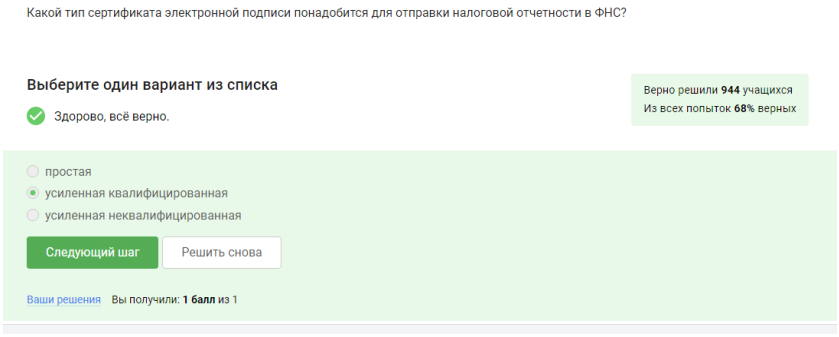

Рис. 2.9: Вопрос 4.2.4

В удостоверяющем (сертификационном) центре можно получить квалифицированный сертификат ключа проверки электронной подписи (рис. 2.10).

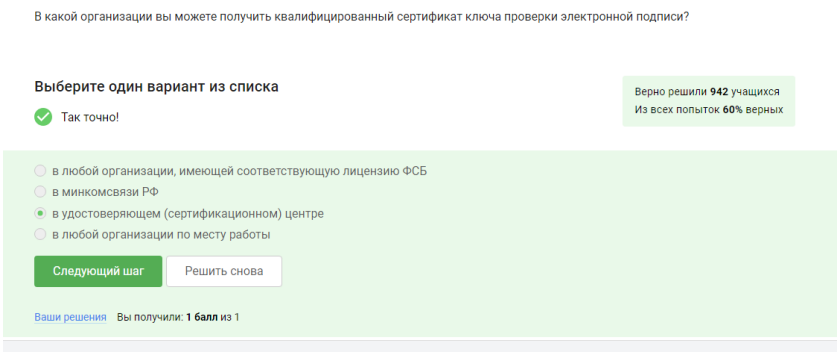

Рис. 2.10: Вопрос 4.2.5

2.3 Электронные платежи

MasterCard, МИР - платежные системы (рис. 2.11).

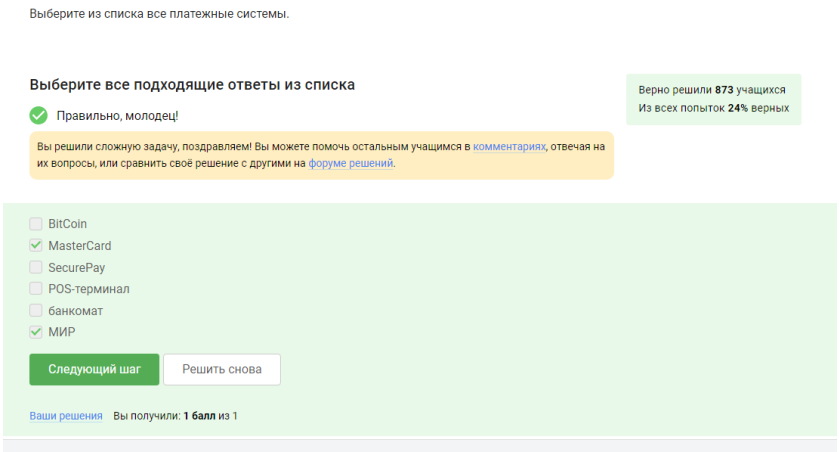

Рис. 2.11: Вопрос 4.3.1

Примеры многофакторной аутентификации (рис. 2.12).

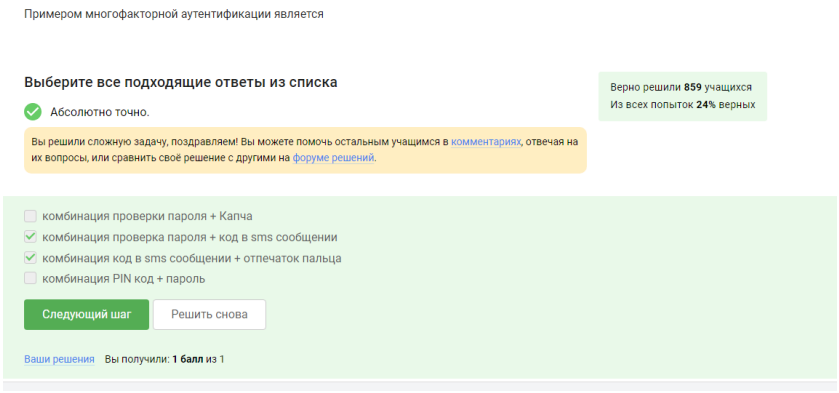

Рис. 2.12: Вопрос 4.3.2

При онлайн платежах используется многофакторная аутентификация (рис. 2.13).

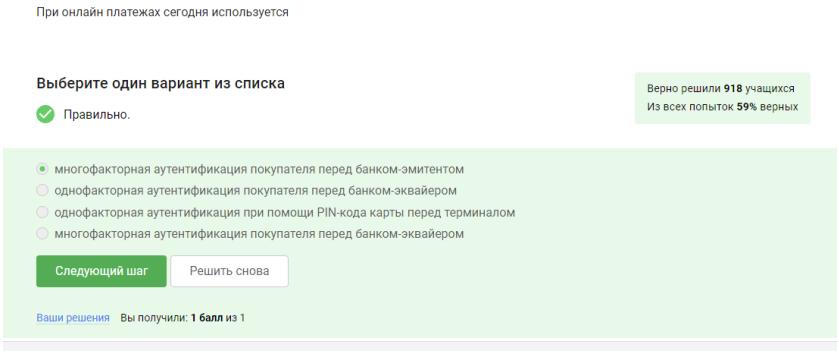

Рис. 2.13: Вопрос 4.3.3

2.4 Блокчейн

PoW (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне (рис. 2.14).

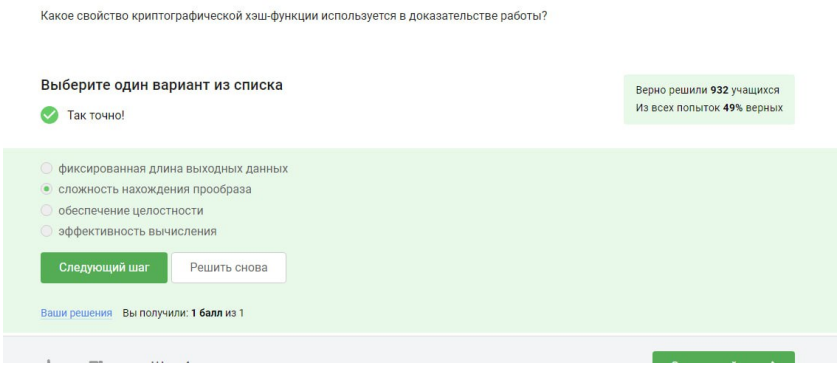

Рис. 2.14: Вопрос 4.4.1

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети (рис. 2.15).

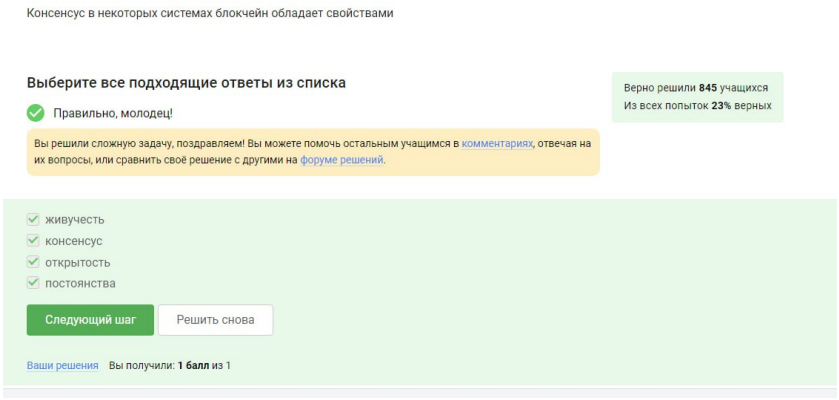

Рис. 2.15: Вопрос 4.4.2

Цифровая подпись (рис. 2.16).

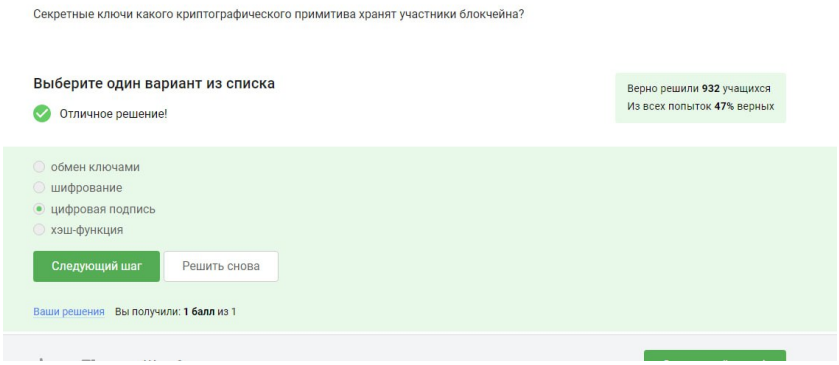

Рис. 2.16: Вопрос 4.4.3

3 Выводы

Я прошла третий раздел внешнего курса и получила полезные знания.