Прохождение внешних курсов

Дисциплина: Основы информационной безопасности

Дудырев Глеб Андреевич НПИбд-01-22

Содержание

1 Цель работы **6**

2 Безопасность в сети **7**
2.1 Как работает интернет базовые сетевые протоколы 7
2.2 Персонализация сети 11
2.3 Браузер TOR. Анонимизация 13
2.4 Беспроводные сети Wi-fi 15

3 Защита ПК/телефона **19**
3.1 Шифрование диска 19
3.2 Пароли 20
3.3 Фишинг 23
3.4 Вирусы. Примеры 24
3.5 Безопасность мессенджеров 25

4 Криптография на практике **26**
4.1 Введение в криптографию 26
4.2 Цифровая подпись 28
4.3 Электронные платежи 30
4.4 Блокчейн 31

5 Выводы **33**

Список иллюстраций

2.1 Задание 1.1.1 7
2.2 Задание 1.1.2 8
2.3 Задание 1.1.3 8
2.4 Задание 1.1.4 9
2.5 Задание 1.1.5 9
2.6 Задание 1.1.6 10
2.7 Задание 1.1.7 10
2.8 Задание 1.1.8 11
2.9 Задание 1.1.9 11
2.10 Задание 1.2.1 12
2.11 Задание 1.2.2 12
2.12 Задание 1.2.3 13
2.13 Задание 1.2.4 13
2.14 Задание 1.3.1 14
2.15 Задание 1.3.2 14
2.16 Задание 1.3.3 15
2.17 Задание 1.3.4 15
2.18 Задание 1.4.1 16
2.19 Задание 1.4.2 16
2.20 Задание 1.4.3 17
2.21 Задание 1.4.4 17
2.22 Задание 1.4.5 18

3.1 Задание 2.1.1 19
3.2 Задание 2.1.2 19
3.3 Задание 2.1.3 20
3.4 Задание 2.2.1 20
3.5 Задание 2.2.2 21
3.6 Задание 2.2.3 21
3.7 Задание 2.2.4 22
3.8 Задание 2.2.5 22
3.9 Задание 2.2.6 23
3.10 Задание 2.3.1 23
3.11 Задание 2.3.2 24
3.12 Задание 2.4.1 24
3.13 Задание 2.4.2 24
3.14 Задание 2.5.1 25

3.15 Задание 2.5.2 25

4.1 Задание 3.1.1 26
4.2 Задание 3.1.2 27
4.3 Задание 3.1.3 27
4.4 Задание 3.1.4 27
4.5 Задание 3.1.5 28
4.6 Задание 3.2.1 28
4.7 Задание 3.2.2 29
4.8 Задание 3.2.3 29
4.9 Задание 3.2.4 29
4.10 Задание 3.2.5 30
4.11 Задание 3.3.1 30
4.12 Задание 3.3.2 31
4.13 Задание 3.3.3 31
4.14 Задание 3.4.1 32
4.15 Задание 3.4.2 32
4.16 Задание 3.4.3 32

Список таблиц

1 Цель работы

Познакомиться с основами кибербезопасности

2 Безопасность в сети

2.1 Как работает интернет базовые сетевые протоколы

1. Протоколом прикладного уровня является протокол HTTPS, он отвечает за работу с приложениями. (рис. 2.1)

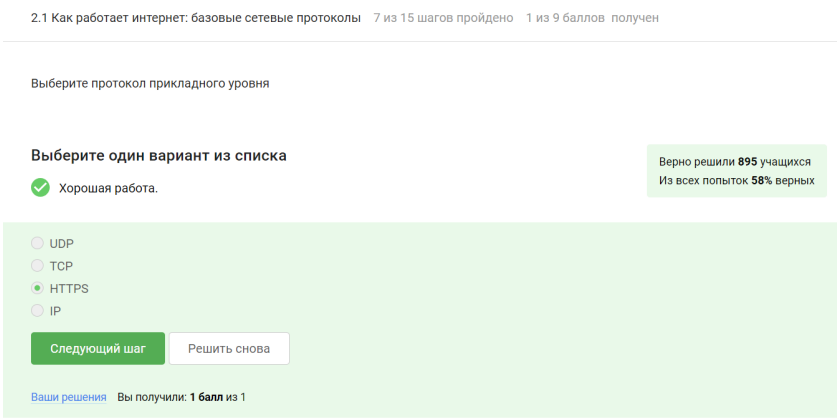

Рис. 2.1: Задание 1.1.1

2. Протокол TCP отвечает за передачу данных внутри одной машины, следовательно, он работает на транспортном уровне. (рис. 2.2)

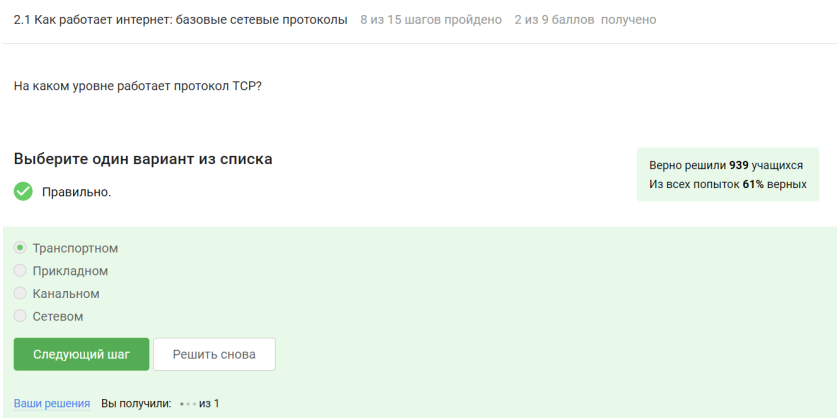

Рис. 2.2: Задание 1.1.2

3. Адреса IPv4 состает из 4 чисел от 0 до 255. (рис. 2.3)

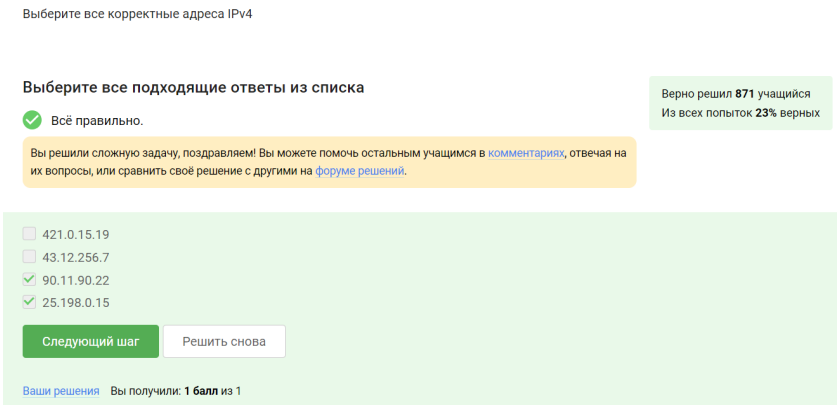

Рис. 2.3: Задание 1.1.3

4. Функцие DNS сервера является: соспоставить доменный и IP адреса. (рис. 2.4)

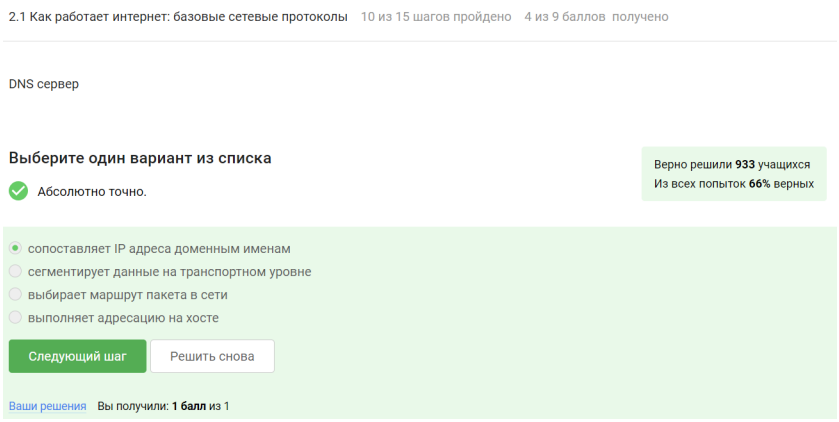

Рис. 2.4: Задание 1.1.4

5. Модель TCP/IP состоит из следующих уровней: прикладной(работа с приложением) - траспортный(передача информации внутри машины) - сетевой(передача информации по сети) - канальный(работа с информацией на физическом уровне). (рис. 2.5)

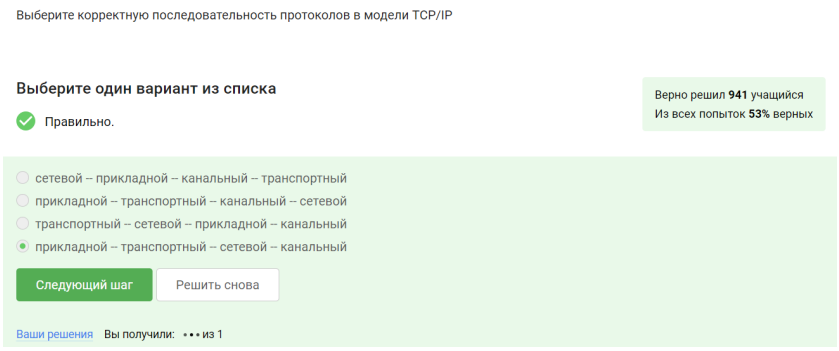

Рис. 2.5: Задание 1.1.5

6. Протокол HTTP предполагает передачу данных в открытом виде, а протокол HTTPS, который использует TLS, передает зашифрованные данныные. (рис. 2.6)

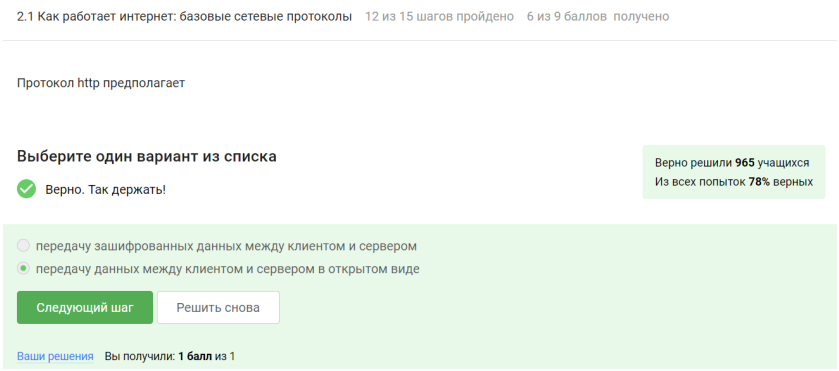

Рис. 2.6: Задание 1.1.6

7. Так как http не использует TLS при передаче данных, то этот протокол состоит из двух фаз: рукопожатие и передача данных. (рис. 2.7)

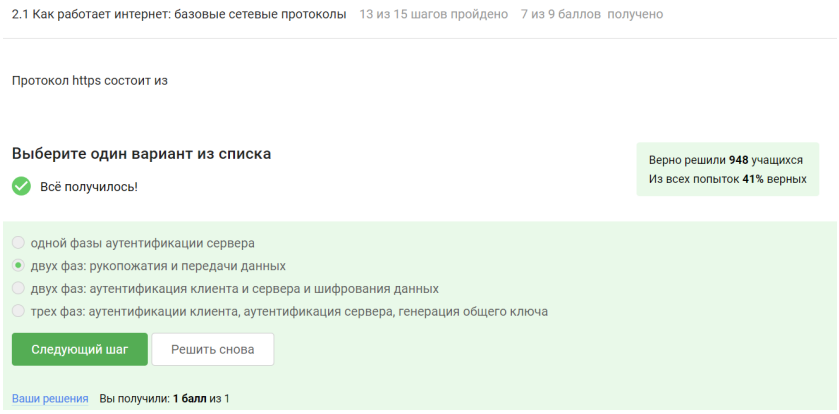

Рис. 2.7: Задание 1.1.7

8. Версию TLS клиент и сервер определяют во время ‘переговоров’. (рис. 2.8)

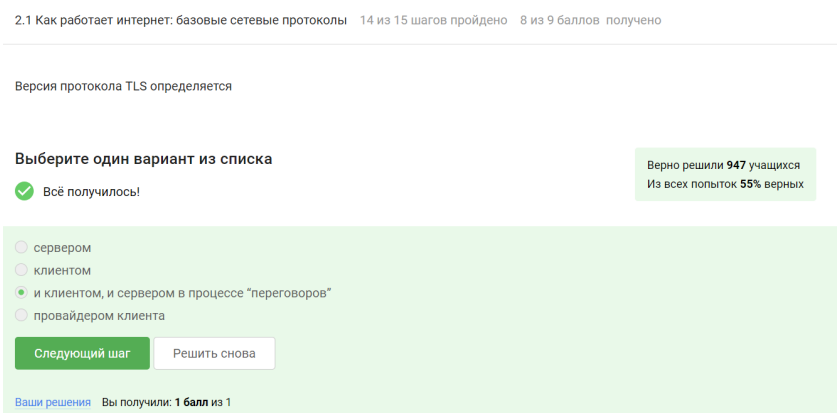

Рис. 2.8: Задание 1.1.8

9. В протоколе TLS шифрование данных предусмотрено в фазе: “Данных” (рис. 2.9)

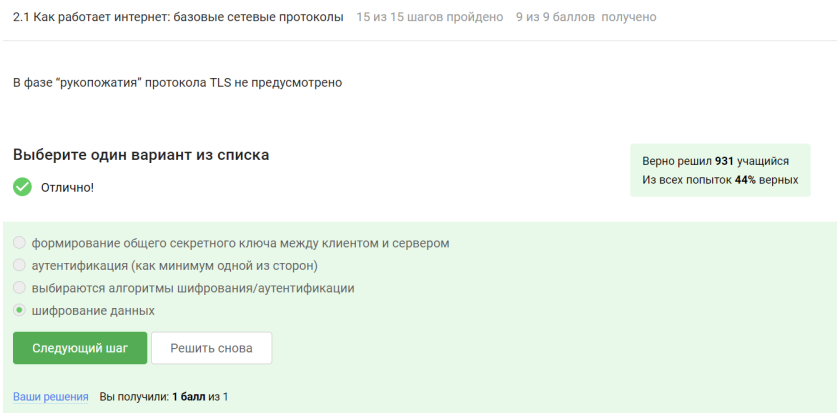

Рис. 2.9: Задание 1.1.9

2.2 Персонализация сети

1. Куки хранят id пользователя и id сессии, а также информацию о действиях пользователя на сайте. (рис. **??**)

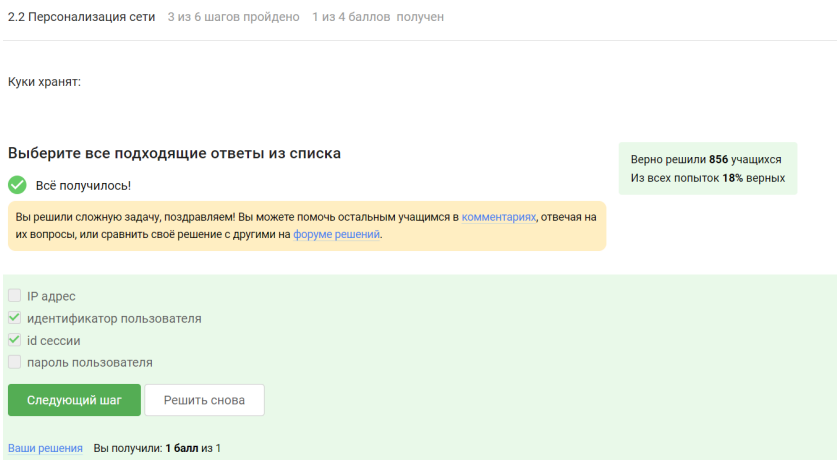

Рис. 2.10: Задание 1.2.1

2. Куки не используются для улучшения надежности соединения, они служат для того, чтобы сохранять информацию о сессии на сервере. (рис. **??**)

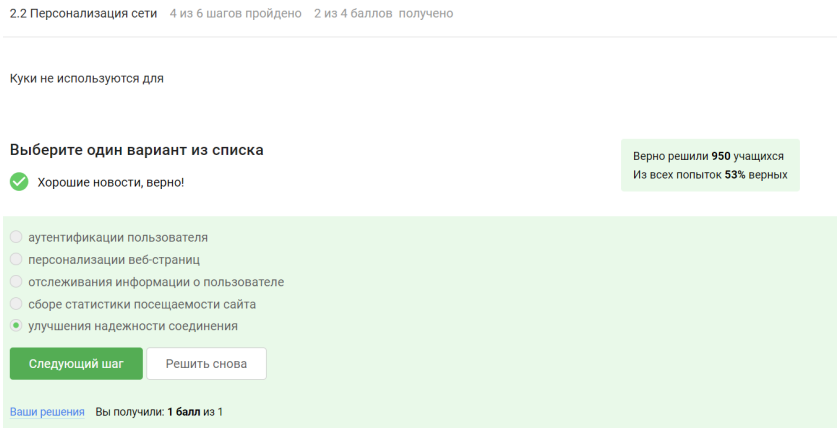

Рис. 2.11: Задание 1.2.2

3. Сервер генерирует куки и возвращает их вместе с ответом на запрос. (рис. **??**)

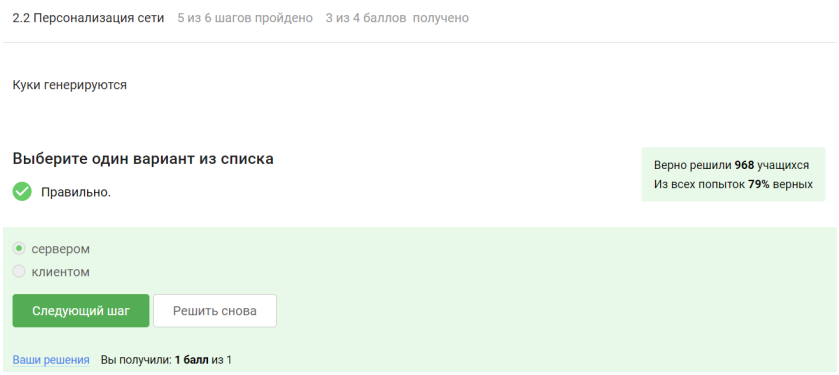

Рис. 2.12: Задание 1.2.3

4. Куки бывают сессионные и постоянные, первые хранятся на сервере и удаляются после закрытия сайта. (рис. 2.13)

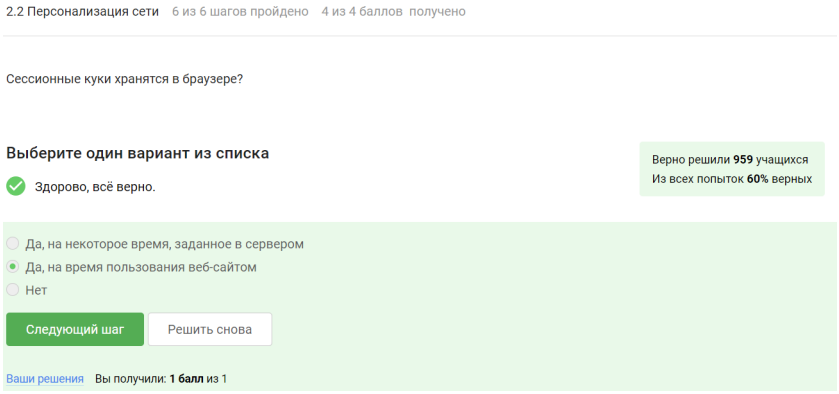

Рис. 2.13: Задание 1.2.4

2.3 Браузер TOR. Анонимизация

1. В луковой маршрутизации существует три узла: охранный, промежуточный и выходной. (рис. 2.14)

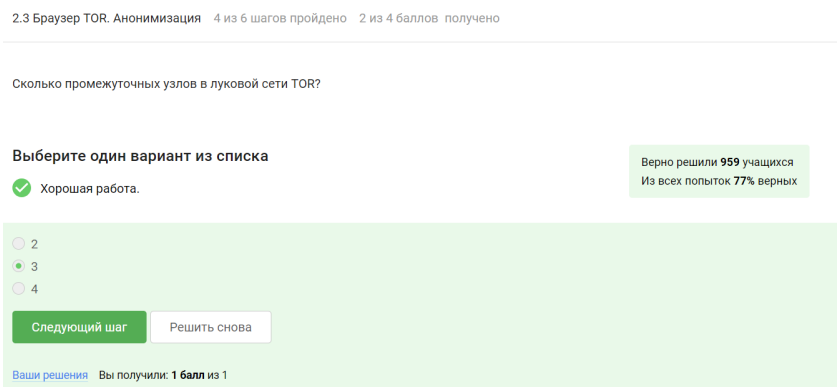

Рис. 2.14: Задание 1.3.1

2. В луковой маршрутизации IP адрес получателя известен: отправителю и выходному узлу. (рис. 2.15)

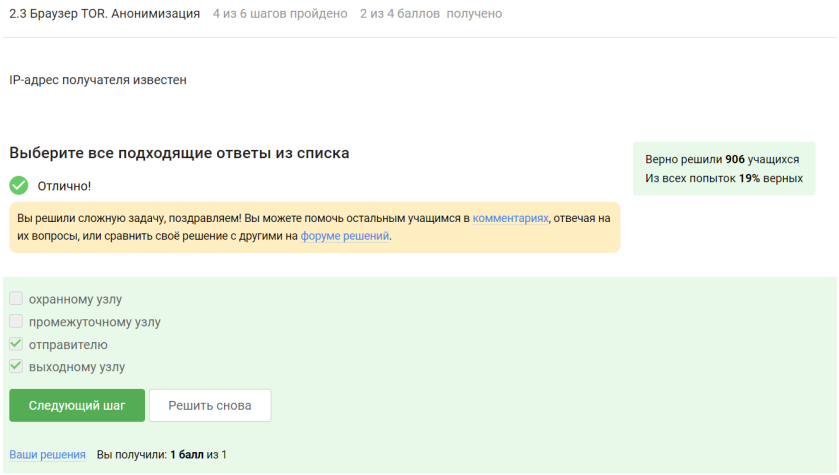

Рис. 2.15: Задание 1.3.2

3. Отправитель генерирует три общих секретных ключа: для охранного узла, для промежуточного и для выходного. (рис. 2.16)

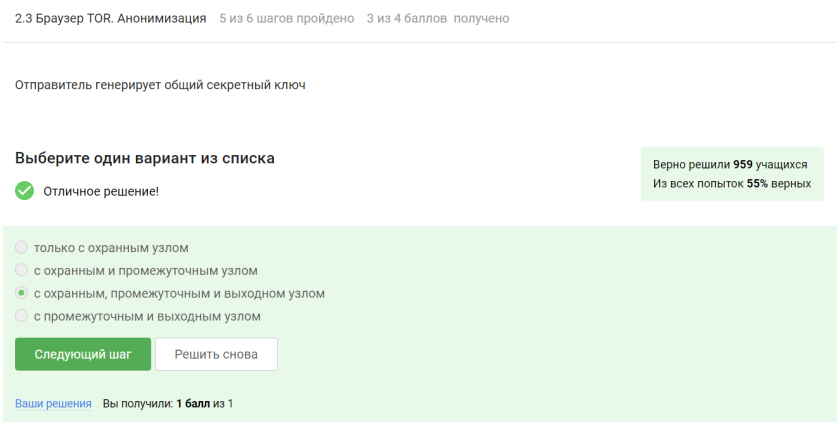

Рис. 2.16: Задание 1.3.3

4. Браузер Tor используется для анонимизации, а не для гарантии успешного получения пакетов. (рис. 2.17)

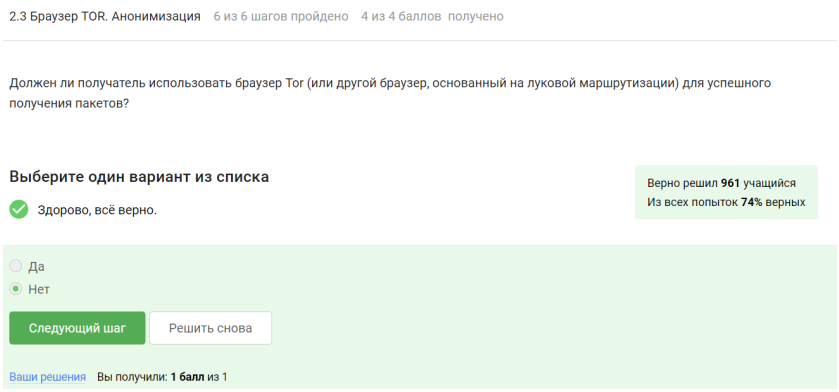

Рис. 2.17: Задание 1.3.4

2.4 Беспроводные сети Wi-fi

1. Wi-fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11. (рис. 2.18)

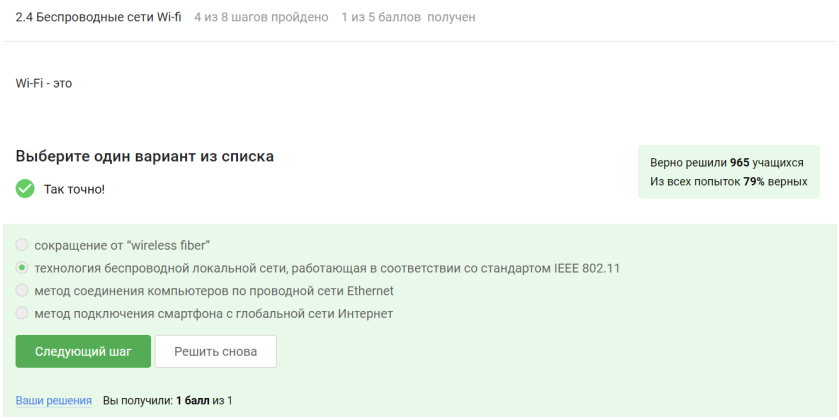

Рис. 2.18: Задание 1.4.1

2. Протокол Wi-fi работает на самом низком канальном уровне, как Ethernet. (рис. 2.19)

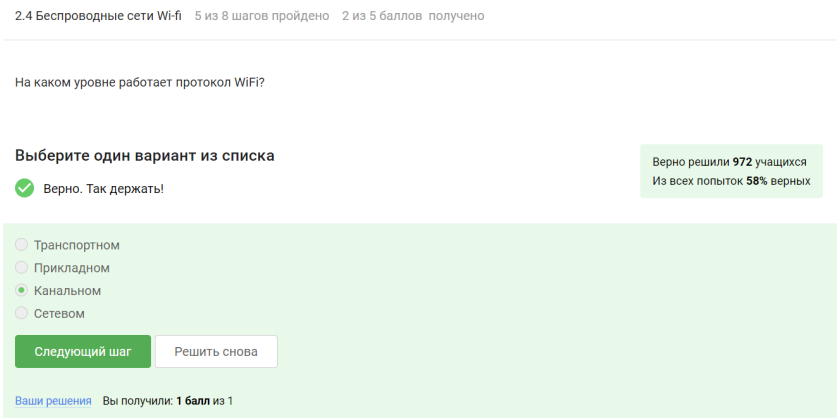

Рис. 2.19: Задание 1.4.2

3. WEP является небезопасным методом шифрования, так как имеет очень короткую длину ключа. (рис. 2.20)

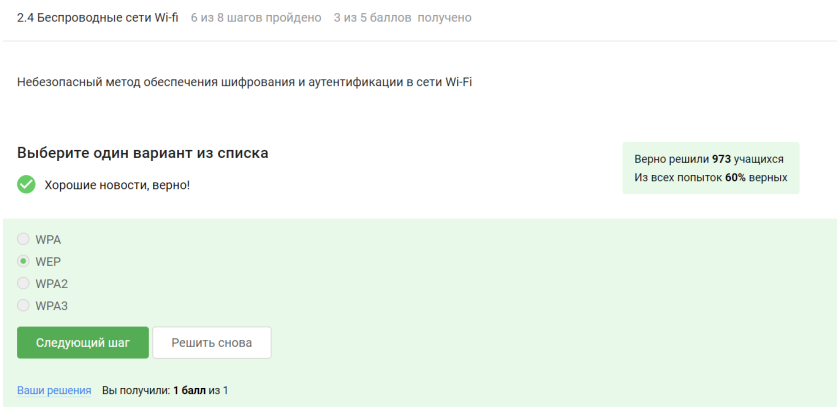

Рис. 2.20: Задание 1.4.3

4. Данные между хостом сети и роутером передаются в зашифрованном виде, после аутентификации, чтобы их нельзя было перехватить. (рис. 2.21)

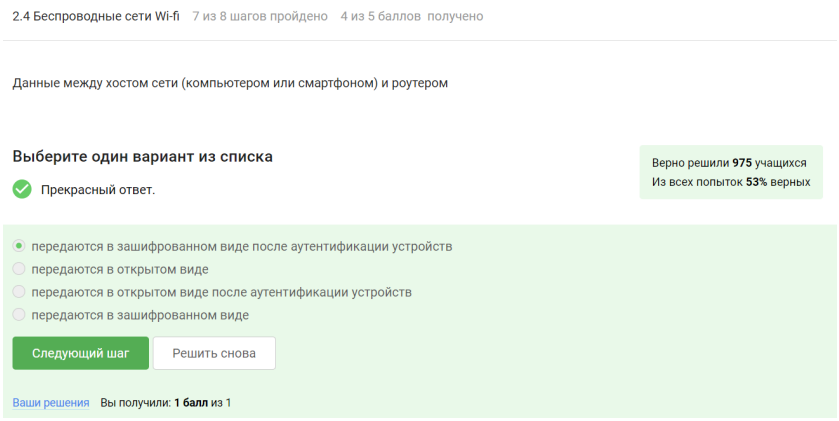

Рис. 2.21: Задание 1.4.4

5. Для домашней сети для аутентификации обычно используется метод Personal(подключение по поролю), второй метод используется для больших корпоративных сетей, он проверяет есть ли пользователь в базе данных. (рис. 2.22)

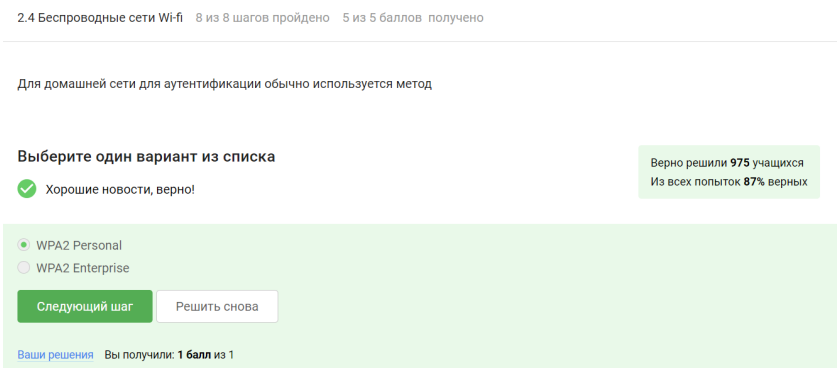

Рис. 2.22: Задание 1.4.5

3 Защита ПК/телефона

3.1 Шифрование диска

1. Можно зашифровать любой сектор диска. (рис. 3.1)

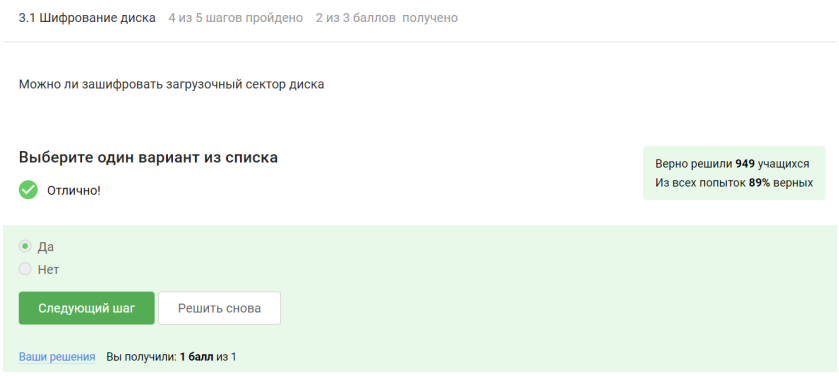

Рис. 3.1: Задание 2.1.1

2. Для шифрования диска используется симметричное шифрование, то есть один секретный ключ для шифрования и дешифрования данных. (рис. 3.2)

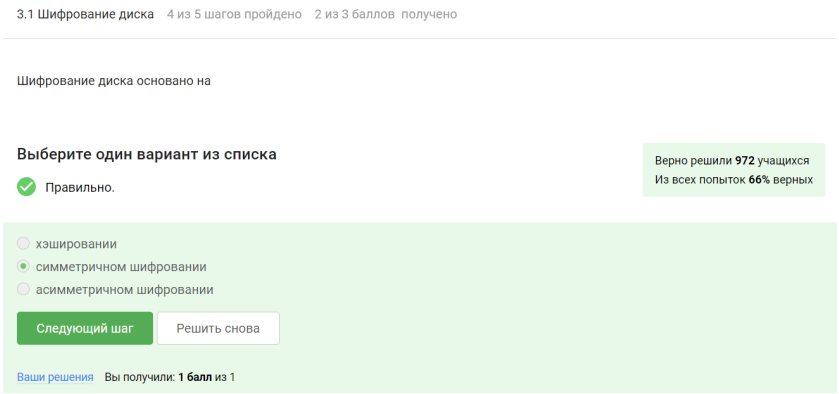

Рис. 3.2: Задание 2.1.2

3. BitLocker - для Windows, в Linux – LUKS, в MacOS – это FileVault. (рис. 3.3)

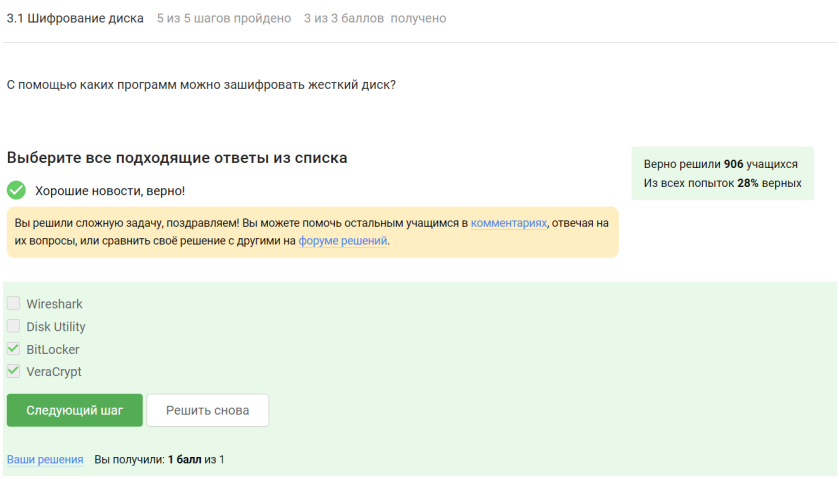

Рис. 3.3: Задание 2.1.3

3.2 Пароли

1. Стойкий пароль не должен быть коротким и должен состоять из различных символов, букв разного регистра и цифр. (рис. 3.4)

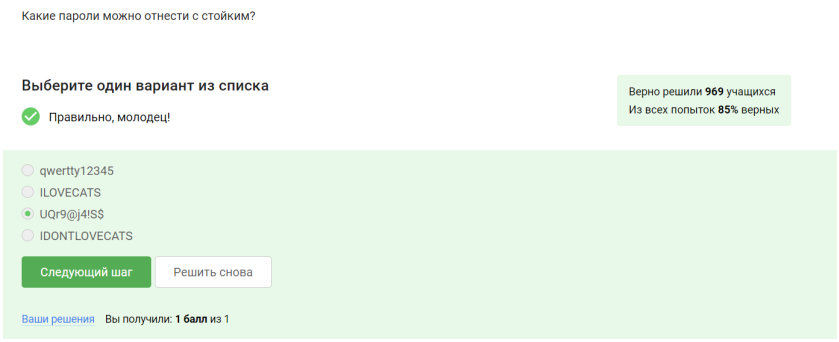

Рис. 3.4: Задание 2.2.1

2. Пароли необзодимо хранить в безопасном месте, чтобы их не смогли обнаружить случайно, например, в менеджерах для паролей. (рис. 3.5)

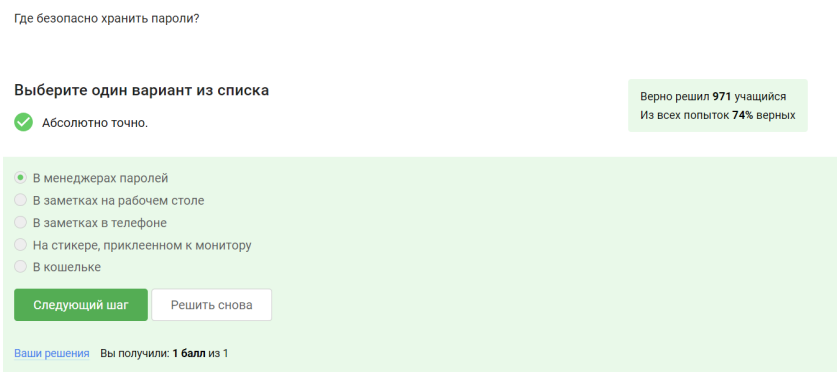

Рис. 3.5: Задание 2.2.2

3. Капча используется для предотвращения запросов к серверу со стороны ботов, что затрудняет автоматизированный перебор паролей. (рис. 3.6)

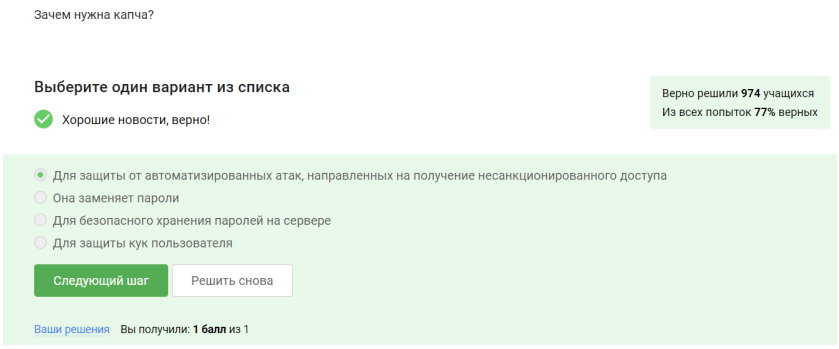

Рис. 3.6: Задание 2.2.3

4. Хэширование паролей используется серверами, чтобы не хранить пароль в открытом виде, а вместо него хранить результат применения хэш-функции к паролю. (рис. 3.7)

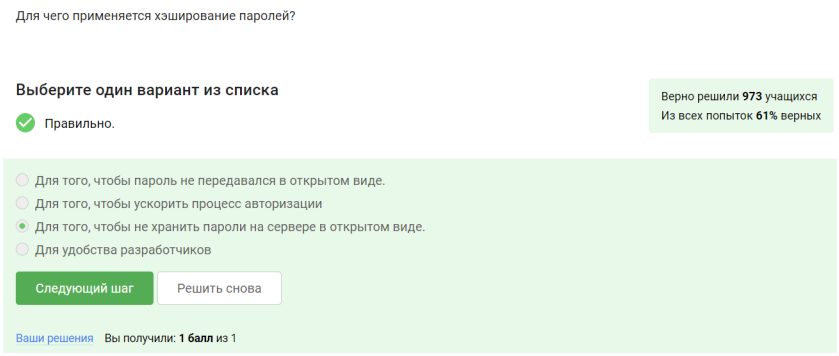

Рис. 3.7: Задание 2.2.4

5. Ответ нет, так как соль используется для того, чтобы не хранить результат хэширования часто используемого пароля, так как если злоумышленник получит доступ к серверу, где хранятся хэш-пароли, он сразу поймет прообраз хэширования. (рис. 3.8)

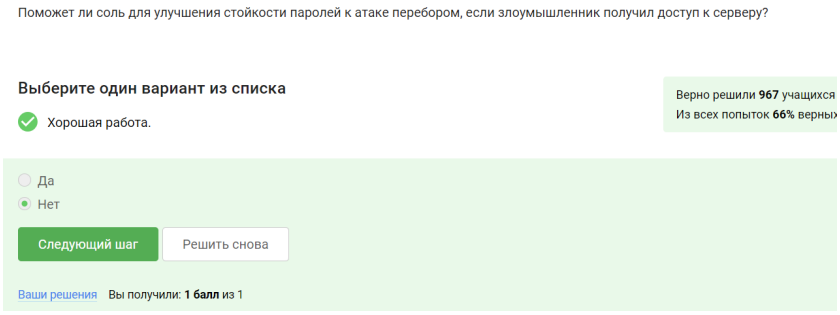

Рис. 3.8: Задание 2.2.5

6. От атак перебором помогают следующие действия: капча, длинные и сложные пароли, различные пароли, переодическая смена паролей. (рис. 3.9)

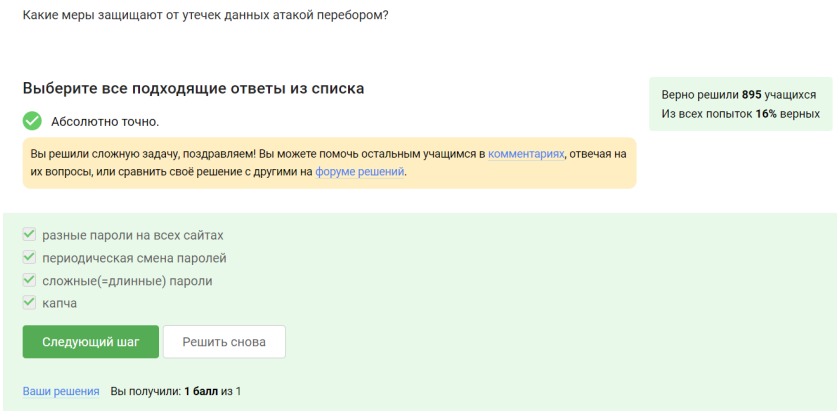

Рис. 3.9: Задание 2.2.6

3.3 Фишинг

1. В данном задании рассматривается такой тип фишинговых атак, как адресный фишинг, когда мы вроде бы переходим на известную нам страницу, но она является поддельной. (рис. 3.10)

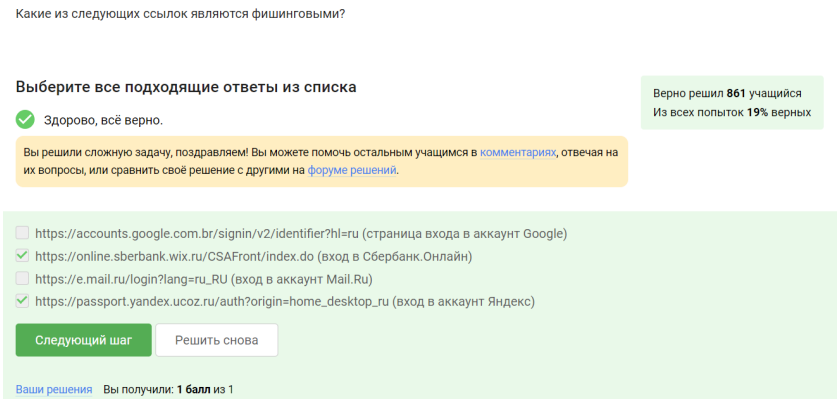

Рис. 3.10: Задание 2.3.1

2. Да такое возможно, это называет спуфинг, это происходит, потому что SMTP не включает в себя проверку адреса отправителя. (рис. 3.11)

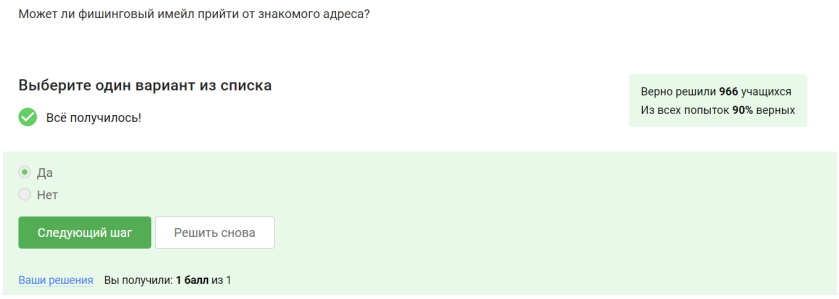

Рис. 3.11: Задание 2.3.2

3.4 Вирусы. Примеры

1. Email спуфинг - это подмена адреса отправителя в емайлах. (рис. 3.12)

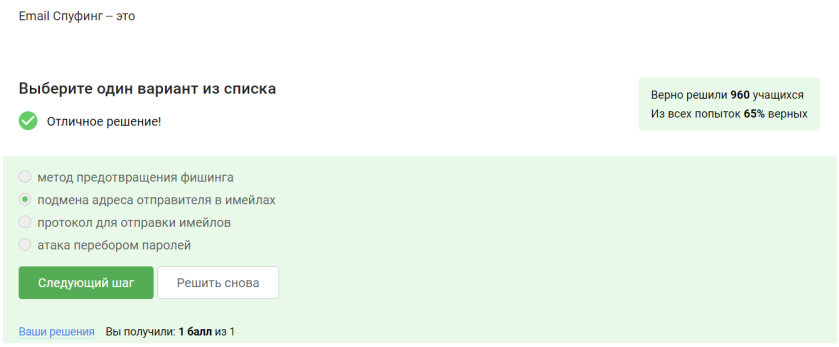

Рис. 3.12: Задание 2.4.1

2. Троян - это вирус, который маскируется под легитимное ПО. (рис. 3.13)

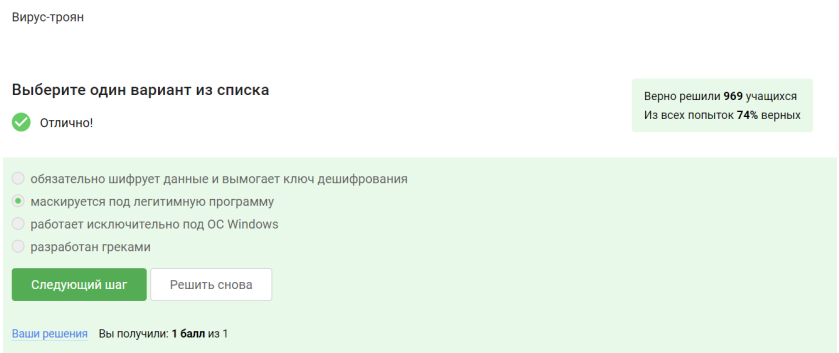

Рис. 3.13: Задание 2.4.2

3.5 Безопасность мессенджеров

1. В протоколе мессенджеров Signal ключ формируется при генерации первого сообщения строной-отправителем. (рис. 3.14)

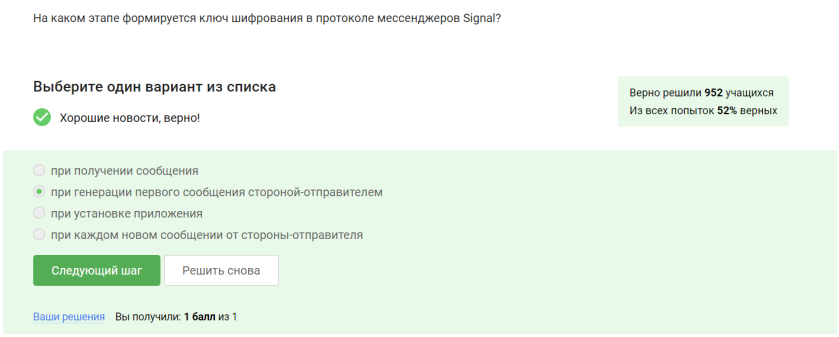

Рис. 3.14: Задание 2.5.1

2. Суть сквозного шифрования состоит в том, что отправитель передает на сервер уже зашифрованное сообщение, сервер отправляет шифрованные данные получателю, а тот их дешифрует, таким образом сервер значет только куда надо передать сообщение. (рис. 3.15)

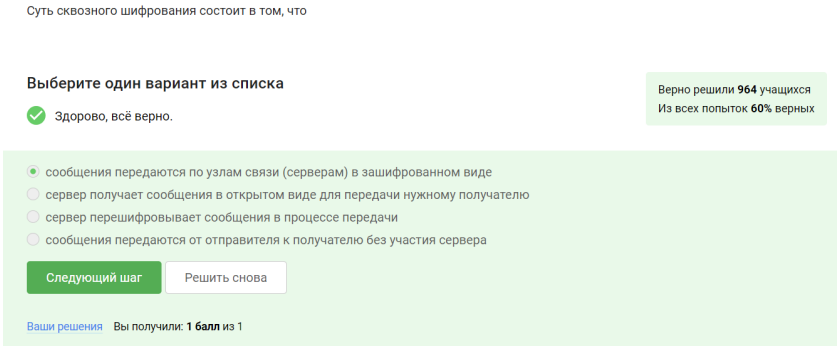

Рис. 3.15: Задание 2.5.2

4 Криптография на практике

4.1 Введение в криптографию

1. В асимметричных криптографических примитивах обе стороны имеют пару ключей - публичный и секретный. (рис. 4.1)

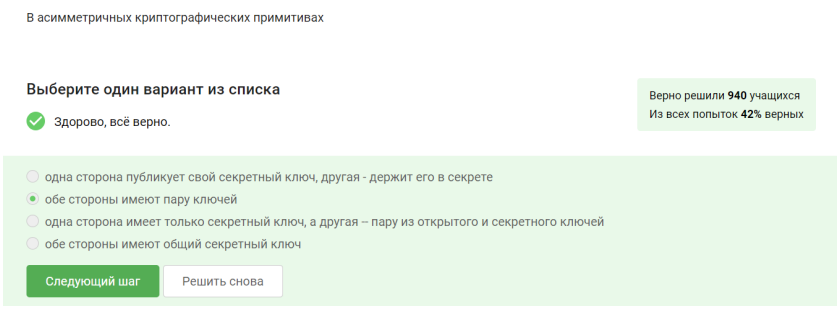

Рис. 4.1: Задание 3.1.1

2. Криптографическая хэш-функция обладает следующими свойствами: возвращает последовательность бит фиксированной длинны, устойчива к коллизиям и эффективно вычисляется. (рис. 4.2)

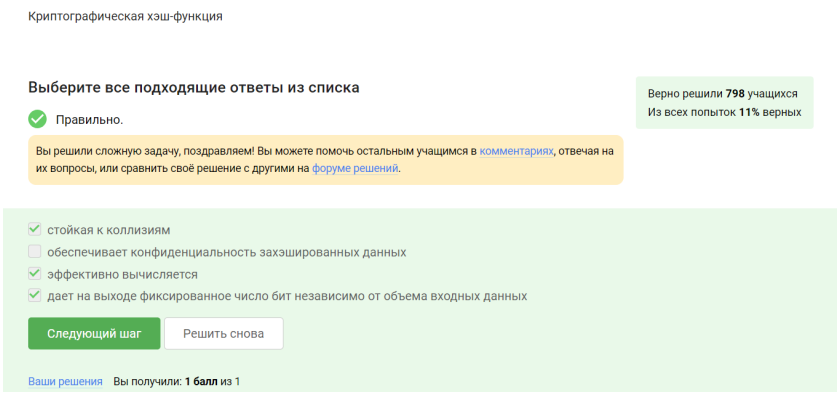

Рис. 4.2: Задание 3.1.2

3. К алгоритмам цифровой подписи относятся: RSA, американский стандарт ECDSA, российский стандарт ГОСТ Р 34.10-2012. (рис. 4.3)

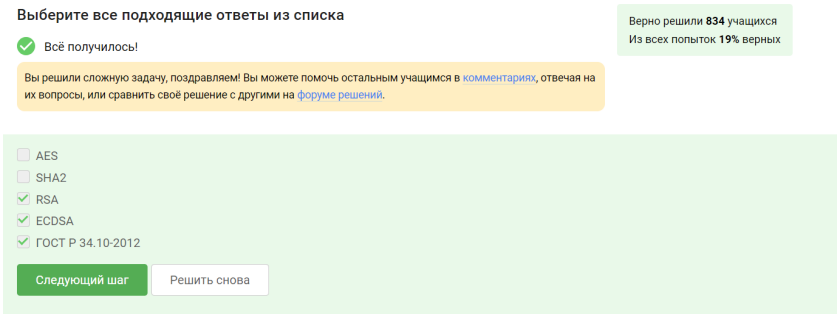

Рис. 4.3: Задание 3.1.3

4. Код аутентификации сообщения относится к симметричным примитивам. (рис. 4.4)

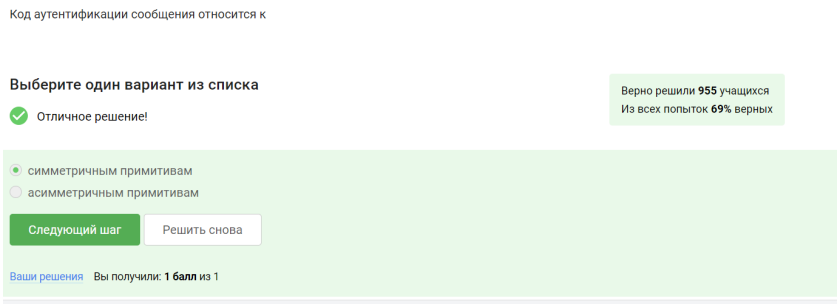

Рис. 4.4: Задание 3.1.4

5. Обмен ключам Диффи-Хэллмана - это ассиметричный примитив, который используется для генерации общего секретного ключа. (рис. 4.5)

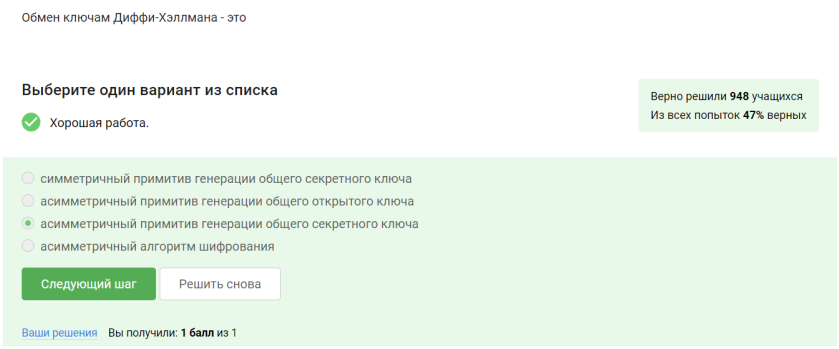

Рис. 4.5: Задание 3.1.5

4.2 Цифровая подпись

1. Протокол электронной цифровой подписи относится к ассиметричным протоколам, то есть с публичным и секретным ключами. (рис. 4.6)

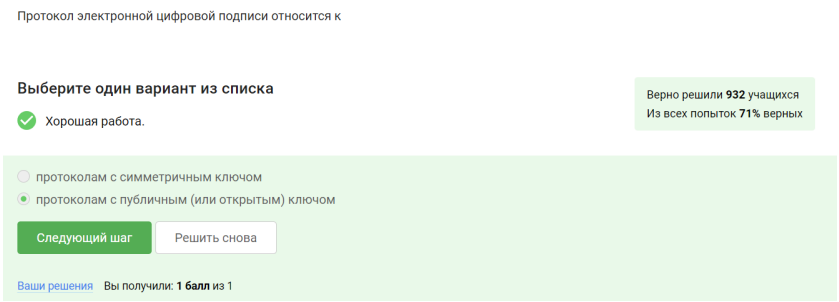

Рис. 4.6: Задание 3.2.1

2. Алгоритм верификации электронной цифровой подписи требует на вход три вещи - это подпись, сообщение и открытый ключ. (рис. 4.7)

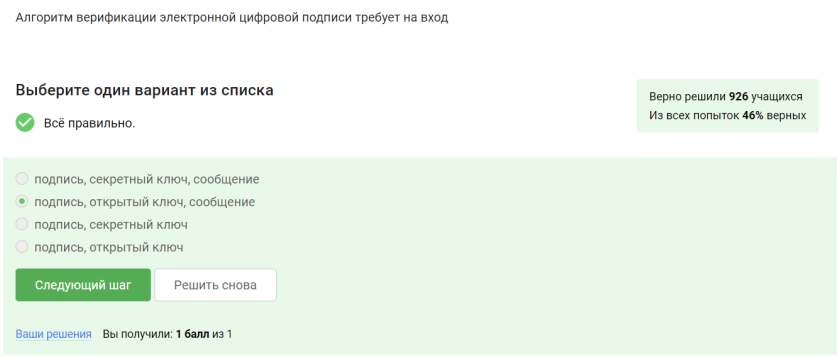

Рис. 4.7: Задание 3.2.2

3. Электронная цифровая подпись не обеспечивает конфиденциальности - она используется для аутентификации, проверки на целостность и неотказ от авторства. (рис. 4.8)

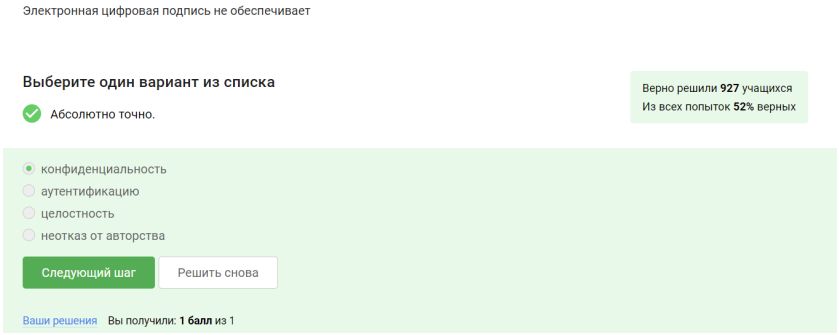

Рис. 4.8: Задание 3.2.3

4. Для отправки налоговой отчетности в ФНС необходимо использовать усиленную квалифицированную подпись. (рис. 4.9)

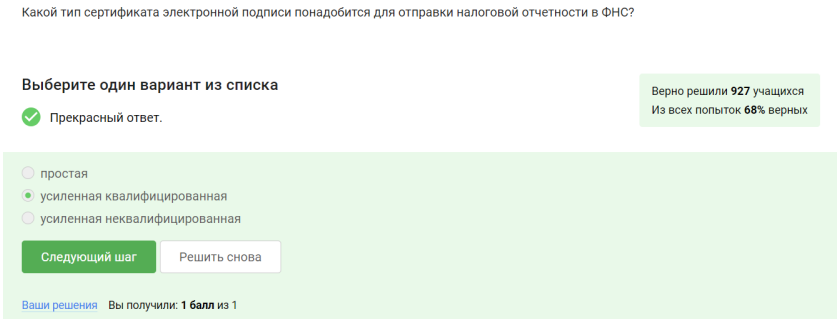

Рис. 4.9: Задание 3.2.4

5. Квалифицированный сертификат можно получить в сертификационном центре. (рис. 4.10)

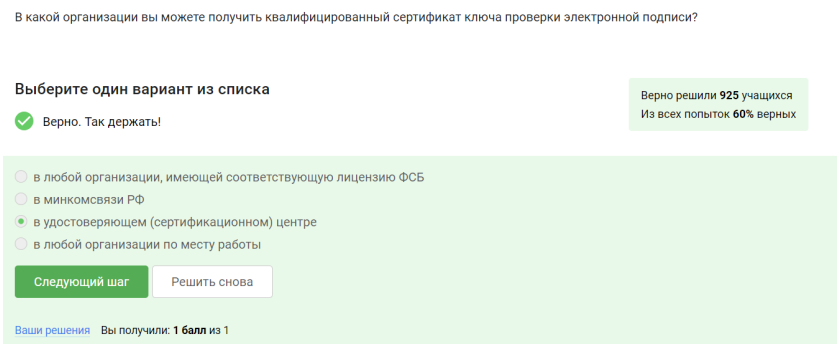

Рис. 4.10: Задание 3.2.5

4.3 Электронные платежи

1. Выбираем платежные системы MasterCard и МИР. (рис. 4.11)

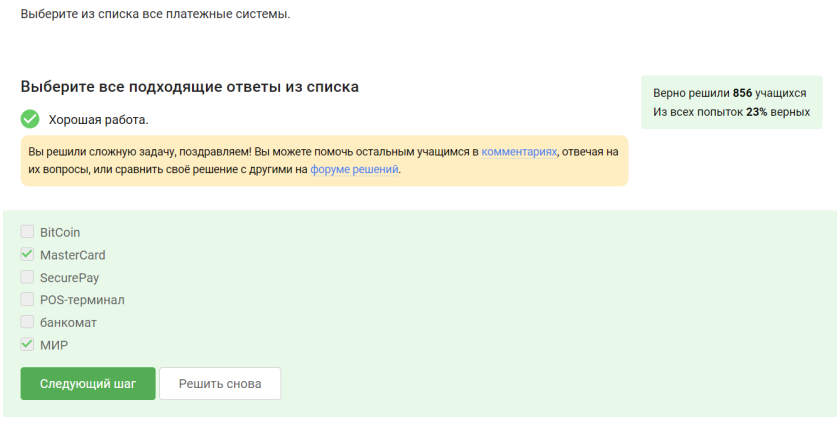

Рис. 4.11: Задание 3.3.1

2. Примером многофакторной аутентификации является те, что я выбрал. (рис. 4.12)

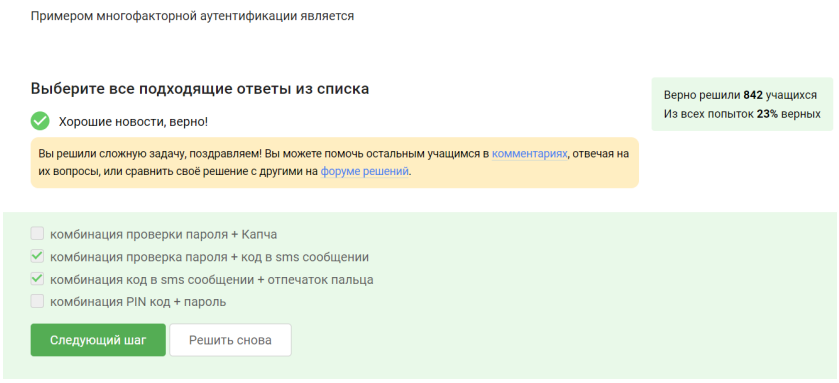

Рис. 4.12: Задание 3.3.2

3. При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом. (рис. 4.13)

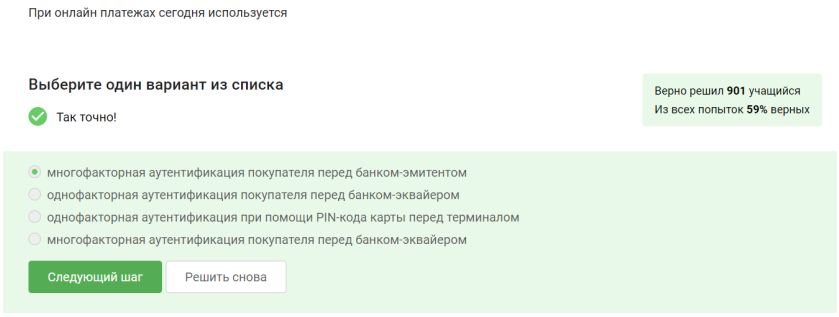

Рис. 4.13: Задание 3.3.3

4.4 Блокчейн

1. В доказательстве работы используется сложность вычисления прообраза хэш-функции, так как единственным эффективным способом атаки на хэш-функцию является перебор. (рис. 4.14)

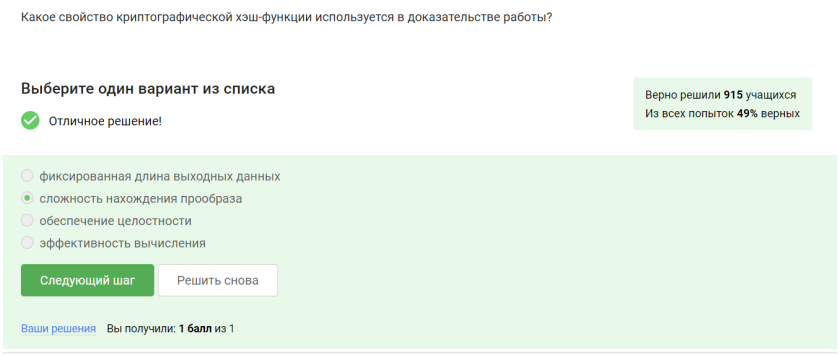

Рис. 4.14: Задание 3.4.1

2. Консенсус в некоторых системах блокчейн обладает свойствами - живучесть, консенсус, постоянства, открытость. (рис. 4.15)

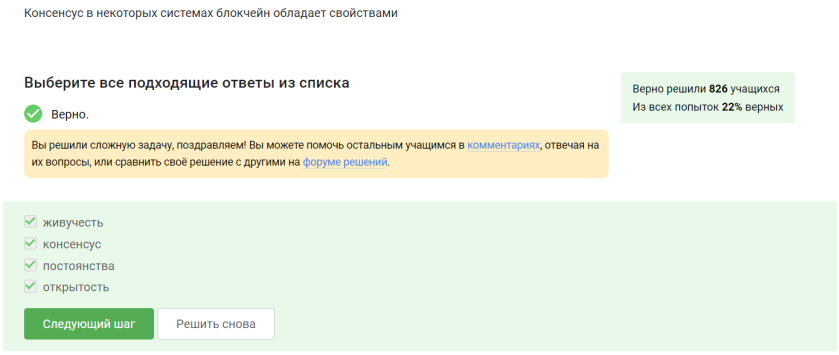

Рис. 4.15: Задание 3.4.2

3. Участники блокчейна хранят секретные ключи электронной подписи, которые используют для подписи транзакций. (рис. 4.16)

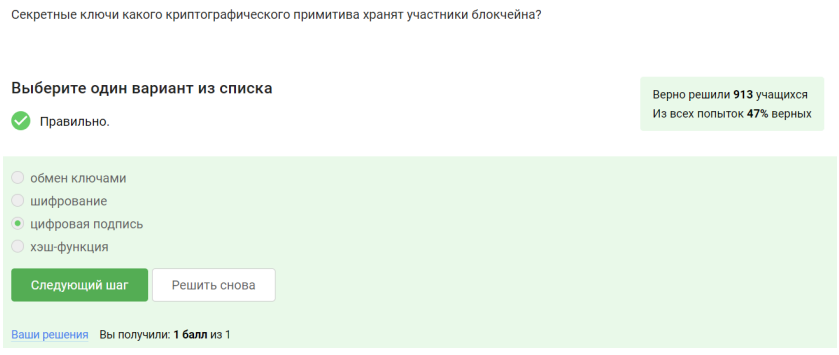

Рис. 4.16: Задание 3.4.3

5 Выводы

Были изучены основы кибербезопасности.