

# **Прохождение внешнего курса**

**Основы кибербезопасности**

**Сухальская Ксения НБИ-бд-03-22**

# Содержание

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение тестовых заданий</b>	<b>6</b>
2.1 Как работает интернет: базовые сетевые протоколы . . . . .	6
2.2 Персонализация сети . . . . .	10
2.3 Браузер TOR. Анонимизация . . . . .	12
2.4 Беспроводные сети Wi-fi . . . . .	14
2.5 Шифрование диска . . . . .	17
2.6 Пароли . . . . .	18
2.7 Фишинг . . . . .	21
2.8 Вирусы. Примеры . . . . .	22
2.9 Безопасность мессенджеров . . . . .	23
2.10 Введение в криптографию . . . . .	24
2.11 Цифровая подпись . . . . .	27
2.12 Электронные платежи . . . . .	29
2.13 Блокчейн . . . . .	31
<b>3 Выводы</b>	<b>33</b>

# List of Figures

2.1	вопрос 1	6
2.2	вопрос 2	7
2.3	вопрос 3	7
2.4	вопрос 4	7
2.5	вопрос 5	8
2.6	вопрос 6	8
2.7	вопрос 7	9
2.8	вопрос 8	9
2.9	вопрос 9	10
2.10	вопрос 1	10
2.11	вопрос 2	11
2.12	вопрос 3	11
2.13	вопрос 4	12
2.14	вопрос 1	12
2.15	вопрос 2	13
2.16	вопрос 3	13
2.17	вопрос 4	14
2.18	вопрос 1	14
2.19	вопрос 2	15
2.20	вопрос 3	15
2.21	вопрос 4	16
2.22	вопрос 5	16
2.23	вопрос 1	17
2.24	вопрос 2	17
2.25	вопрос 3	18
2.26	вопрос 1	18
2.27	вопрос 2	19
2.28	вопрос 3	19
2.29	вопрос 4	20
2.30	вопрос 5	20
2.31	вопрос 6	21
2.32	вопрос 1	21
2.33	вопрос 2	22
2.34	вопрос 1	22
2.35	вопрос 2	23
2.36	вопрос 1	23
2.37	вопрос 2	24

2.38 вопрос 1	24
2.39 вопрос 2	25
2.40 вопрос 3	25
2.41 вопрос 4	26
2.42 вопрос 5	26
2.43 вопрос 1	27
2.44 вопрос 2	27
2.45 вопрос 3	28
2.46 вопрос 4	28
2.47 вопрос 5	29
2.48 вопрос 1	29
2.49 вопрос 2	30
2.50 вопрос 3	30
2.51 вопрос 1	31
2.52 вопрос 2	31
2.53 вопрос 3	32

# **1 Цель работы**

Понять, как работает Интернет, и какие у него “слабые” места, уяснить, почему 1245YOURNAME - плохой пароль, научиться отличать шифрование от электронной подписи. Понять, как работают электронные платежи. как работает персонализация сети, Браузер TOR, анонимизация и беспроводные сети.

## 2 Выполнение тестовых заданий

### 2.1 Как работает интернет: базовые сетевые протоколы

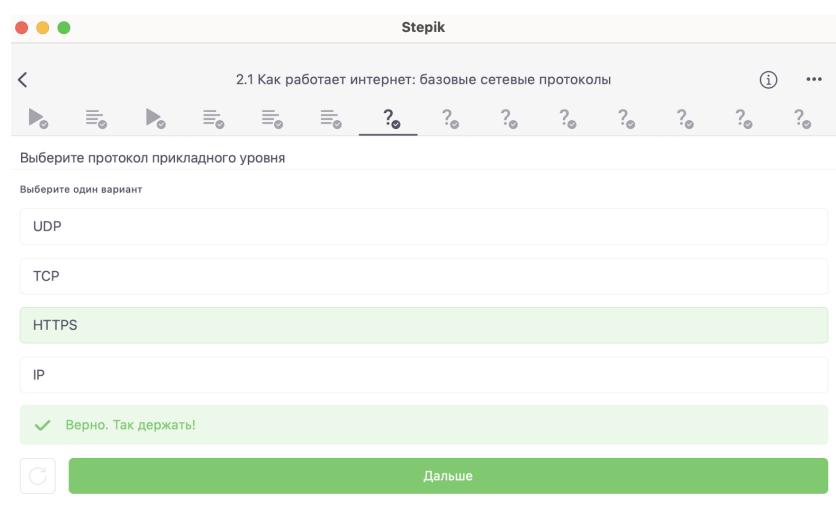


Figure 2.1: вопрос 1

Ответ: Протокол прикладного уровня - HTTPS, так как он обеспечивает безопасную передачу данных между клиентом и сервером.

На каком уровне работает протокол TCP?

Выберите один вариант

Транспортном

Прикладном

Канальном

Сетевом

Прекрасный ответ!

 Дальше



Figure 2.2: вопрос 2

Ответ: Протокол TCP работает на транспортном уровне, так как он обеспечивает надежную доставку данных между узлами в сети.

Выберите все корректные адреса IPv4

Выберите один или несколько вариантов

421.0.15.19

43.12.256.7

90.11.90.22

25.198.0.15

Отлично!

 Дальше

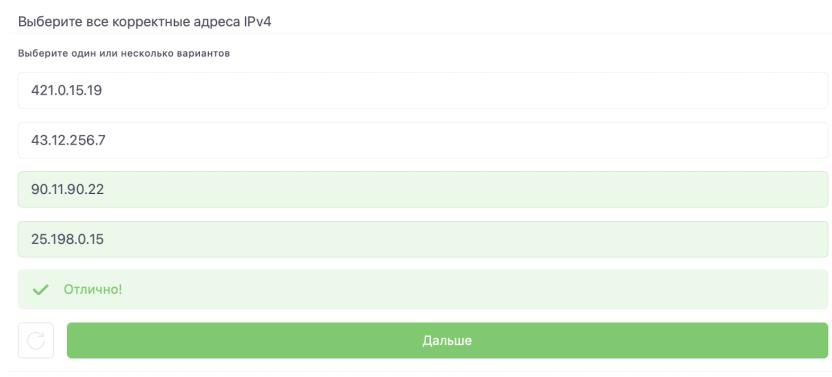


Figure 2.3: вопрос 3

Ответ: Корректные адреса IPv4: 90.11.90.22 и 25.198.0.15, так как они соответствуют формату IPv4 (четыре числа от 0 до 255, разделенные точками).

DNS сервер

Выберите один вариант

сопоставляет IP адреса доменным именам

сегментирует данные на транспортном уровне

выбирает маршрут пакета в сети

выполняет адресацию на хосте

Верно.

 Дальше

Домашка: 0/23 Успешно: 66%

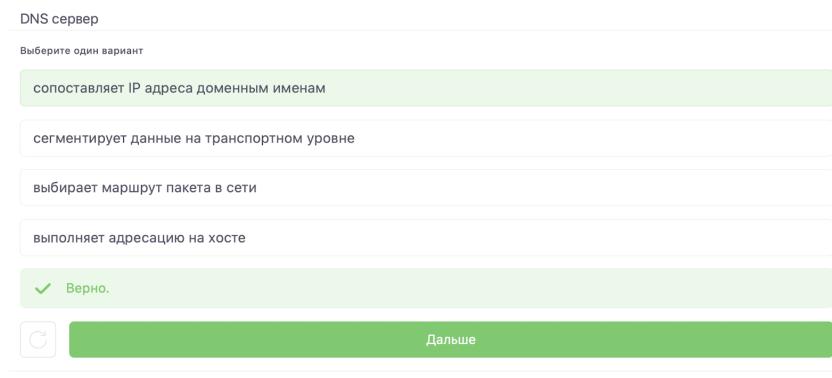


Figure 2.4: вопрос 4

Ответ: DNS сервер сопоставляет IP адреса доменным именам для обеспечения разрешения доменных имен в IP адреса.

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант

сетевой -- прикладной -- канальный -- транспортный

прикладной -- транспортный -- канальный -- сетевой

транспортный -- сетевой -- прикладной -- канальный

прикладной -- транспортный -- сетевой -- канальный

✓ Здорово, всё верно.

Дальше

Figure 2.5: вопрос 5

Ответ: Корректная последовательность протоколов в модели TCP/IP: прикладной – транспортный – сетевой – канальный, так как это порядок от пользователя к физическому уровню.

2.1 Как работает интернет: базовые сетевые протоколы

Протокол http предполагает

Выберите один вариант

передачу зашифрованных данных между клиентом и сервером

передачу данных между клиентом и сервером в открытом виде

✓ Отлично!

Дальше

Figure 2.6: вопрос 6

Ответ: Протокол http предполагает передачу данных между клиентом и сервером в открытом виде.

Протокол https состоит из

Выберите один вариант

одной фазы аутентификации сервера

двух фаз: рукопожатия и передачи данных

двух фаз: аутентификация клиента и сервера и шифрования данных

трех фаз: аутентификации клиента, аутентификации сервера, генерация общего ключа

Так точно!

Figure 2.7: вопрос 7

Ответ: Протокол https состоит из двух фаз: рукопожатия и передачи данных, обеспечивая безопасную передачу данных между клиентом и сервером.

Версия протокола TLS определяется

Выберите один вариант

сервером

клиентом

и клиентом, и сервером в процессе "переговоров"

провайдером клиента

Верно. Так держать!

Figure 2.8: вопрос 8

Ответ: Версия протокола TLS определяется клиентом и сервером в процессе “переговоров”.

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант

формирование общего секретного ключа между клиентом и сервером

автентификация (как минимум одной из сторон)

выбираются алгоритмы шифрования/автентификации

шифрование данных

✓ Верно. Так держать!

Попробовать снова

Следующий урок ►

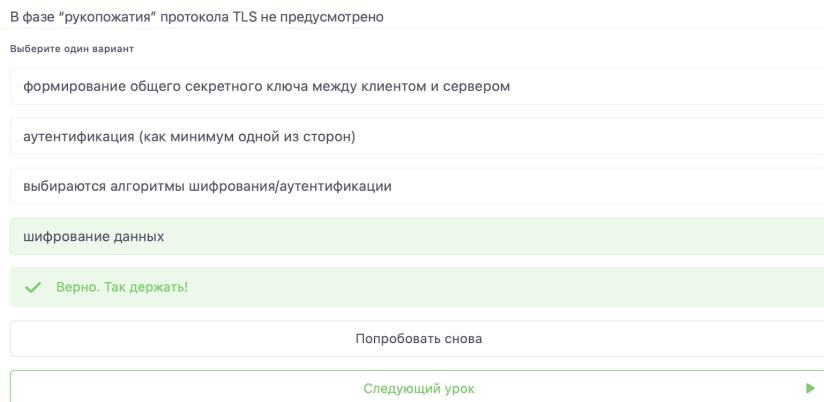


Figure 2.9: вопрос 9

Ответ: В фазе “рукопожатия” протокола TLS не предусмотрено шифрование данных, так как в этой фазе устанавливается соединение и выбираются алгоритмы шифрования/автентификации.

## 2.2 Персонализация сети

< 2.2 Персонализация сети ⓘ ...

Куки хранят:

Выберите один или несколько вариантов

идентификатор пользователя

пароль пользователя

IP адрес

id сессии

✓ Здорово, всё верно.

Дальше

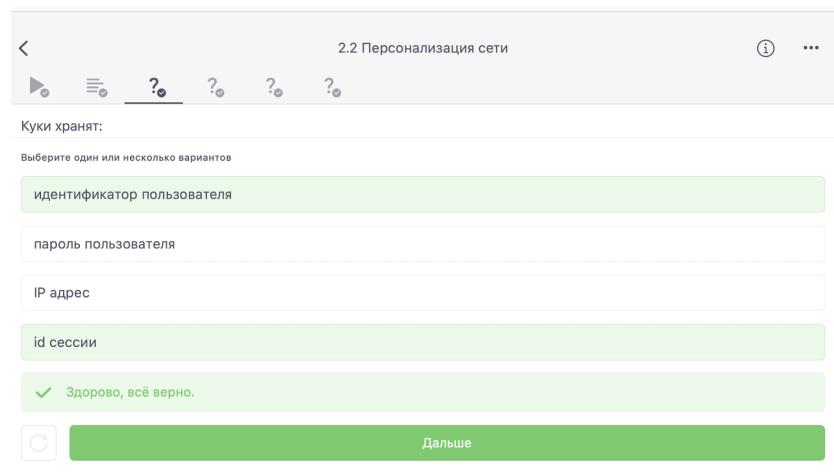


Figure 2.10: вопрос 1

Ответ: Куки хранят идентификатор пользователя, который может использоваться для идентификации пользователя на сайте, а также id сессии, который помогает отслеживать активность пользователя в рамках одной сессии на сайте.

2.2 Персонализация сети

Куки не используются для

Выберите один вариант

аутентификации пользователя

персонализации веб-страниц

отслеживания информации о пользователе

собора статистики посещаемости сайта

улучшения надежности соединения

✓ Так точно!

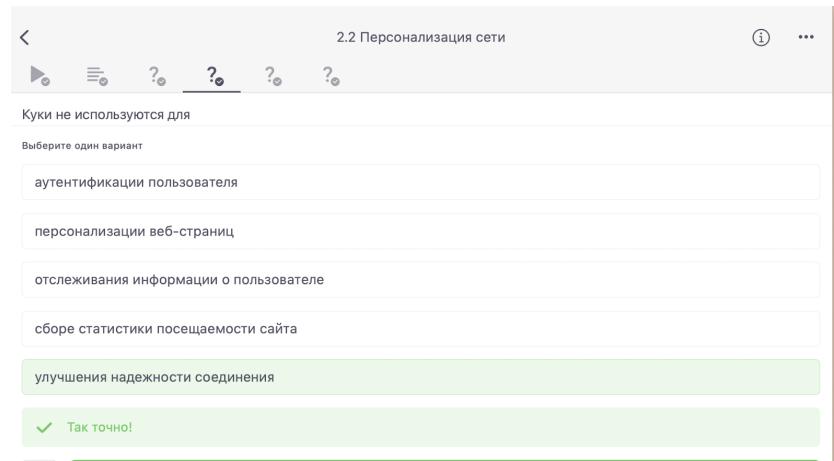


Figure 2.11: вопрос 2

Ответ: Куки не используются для улучшения надежности соединения между клиентом и сервером. Для этой цели обычно используются другие методы, такие как HTTPS протокол.

2.2 Персонализация сети

Куки генерируются

Выберите один вариант

сервером

клиентом

✓ Здорово, всё верно.

Дальше

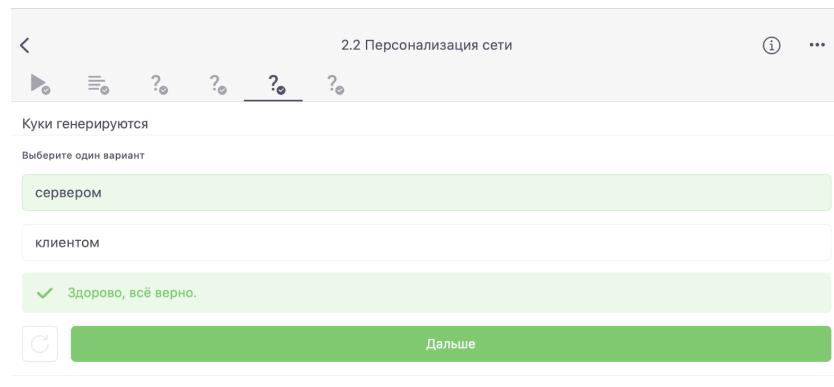


Figure 2.12: вопрос 3

Ответ: Куки генерируются сервером и отправляются на клиентскую сторону (браузер) для хранения и последующего использования при взаимодействии с сайтом.

2.2 Персонализация сети

Сессионные куки хранятся в браузере?

Выберите один вариант

Да, на время пользования веб-сайтом

Да, на некоторое время, заданное в сервером

Нет

✓ Верно. Так держать!

Попробовать снова

Следующий урок ►

Figure 2.13: вопрос 4

Ответ: Сессионные куки хранятся в браузере только на время использования веб-сайта. После закрытия браузера или завершения сессии, они обычно удаляются. Это помогает обеспечить безопасность и конфиденциальность данных пользователя.

## 2.3 Браузер TOR. Анонимизация

2.3 Браузер TOR. Анонимизация

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант

2

3

4

✓ Хорошая работа.

Дальше

Figure 2.14: вопрос 1

Ответ: В луковой сети TOR промежуточных узлов обычно 3: входной узел, промежуточный узел и выходной узел.

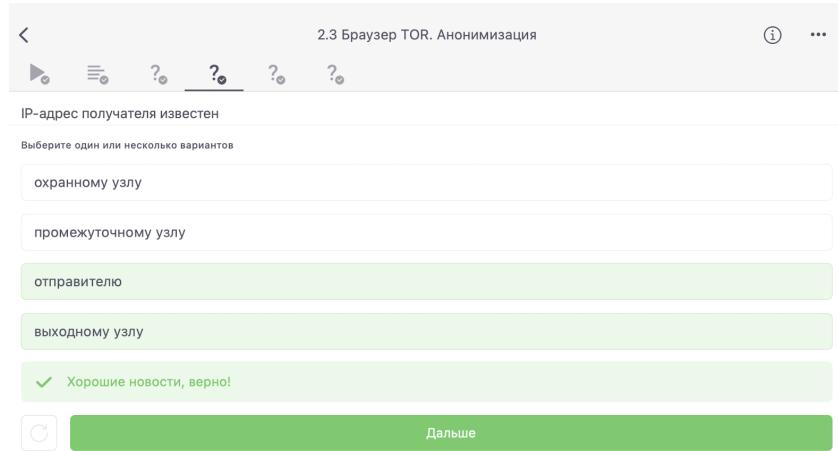


Figure 2.15: вопрос 2

Ответ: IP-адрес получателя известен отправителю, потому что отправитель сам выбирает путь для передачи данных через луковую сеть TOR. IP-адрес получателя известен также выходному узлу, потому что последний узел в цепочке расшифровывает данные и отправляет их на конечный адрес получателя.

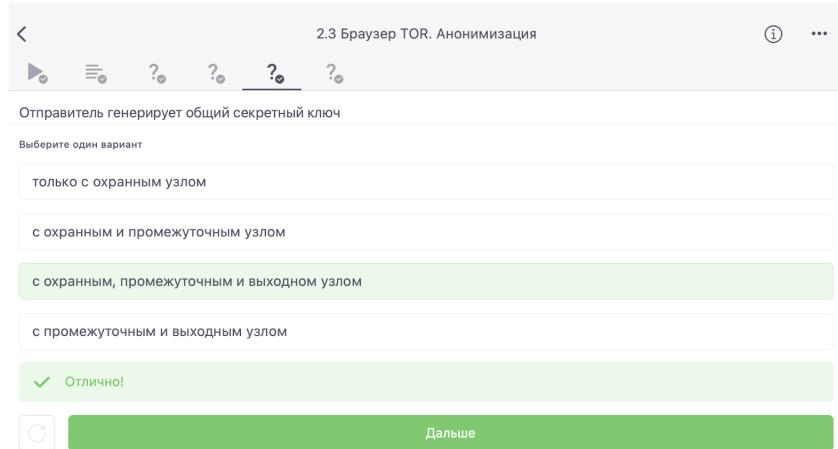


Figure 2.16: вопрос 3

Ответ: Отправитель генерирует общий секретный ключ с каждым узлом на пути через луковую сеть TOR для обеспечения конфиденциальности и целостности передаваемых данных.

< 2.3 Браузер TOR. Анонимизация ⓘ ...

Должен ли получатель использовать браузер Тор (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?

Выберите один вариант

Нет

Да

Абсолютно точно.

Попробовать снова

Следующий урок ►

Figure 2.17: вопрос 4

Ответ: Получатель не обязан использовать браузер TOR для успешного получения пакетов. Получатель может использовать обычный браузер для доступа к контенту, отправленному через луковую сеть TOR.

## 2.4 Беспроводные сети Wi-fi

< 2.4 Беспроводные сети Wi-fi ⓘ ...

Wi-Fi – это

Выберите один вариант

сокращение от "wireless fiber"

технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11

метод соединения компьютеров по проводной сети Ethernet

метод подключения смартфона с глобальной сети Интернет

Отличное решение!

Дальше

Figure 2.18: вопрос 1

Ответ: Wi-Fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11.

< 2.4 Беспроводные сети Wi-Fi ...

На каком уровне работает протокол WiFi?

Выберите один вариант

Транспортном

Прикладном

Канальном

Сетевом

✓ Хорошая работа.

Дальше

Figure 2.19: вопрос 2

Ответ: Протокол WiFi работает на канальном уровне.

< 2.4 Беспроводные сети Wi-Fi ...

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант

WPA

WEP

WPA2

WPA3

✓ Хорошая работа.

Дальше

Figure 2.20: вопрос 3

Ответ: Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi - WEP.

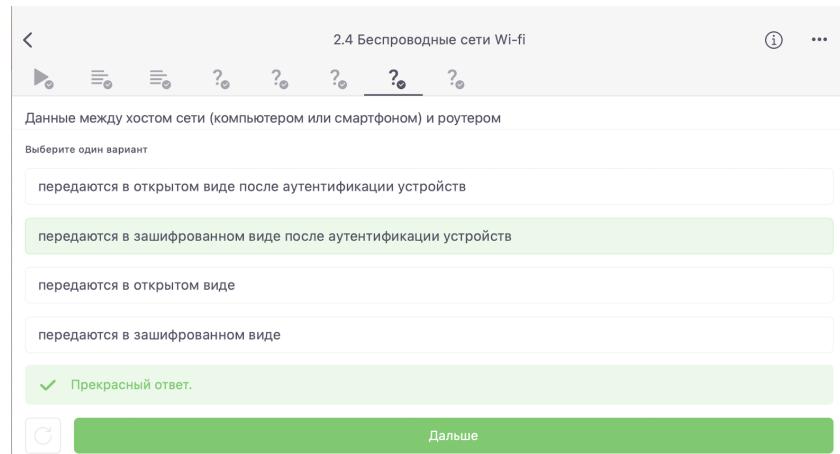


Figure 2.21: вопрос 4

Ответ: Данные между хостом сети (компьютером или смартфоном) и роутером передаются в зашифрованном виде после аутентификации устройств.

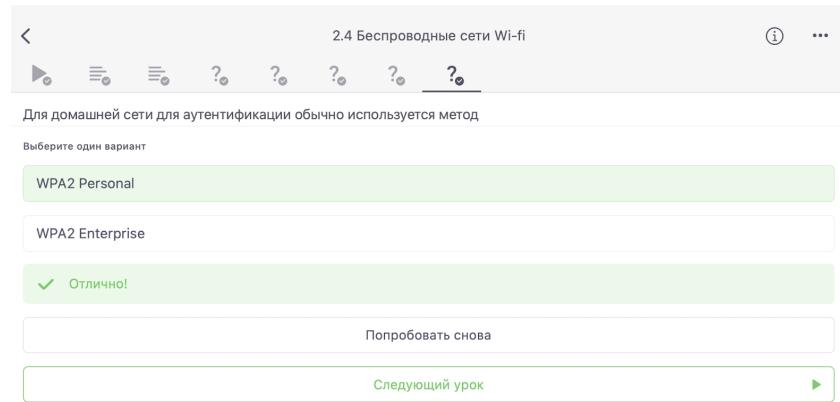


Figure 2.22: вопрос 5

Ответ: Для домашней сети для аутентификации обычно используется метод WPA2 Personal.

## 2.5 Шифрование диска

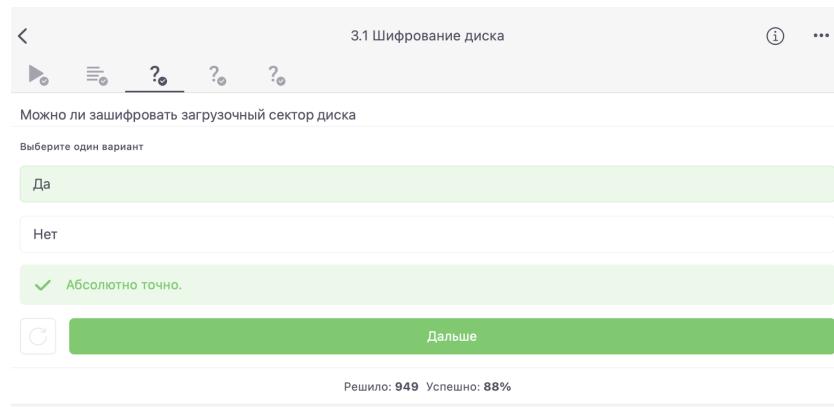


Figure 2.23: вопрос 1

Ответ: Зашифровать загрузочный сектор диска можно, выбрав вариант “Да”. Это позволит усилить безопасность системы и защитить данные при загрузке компьютера.

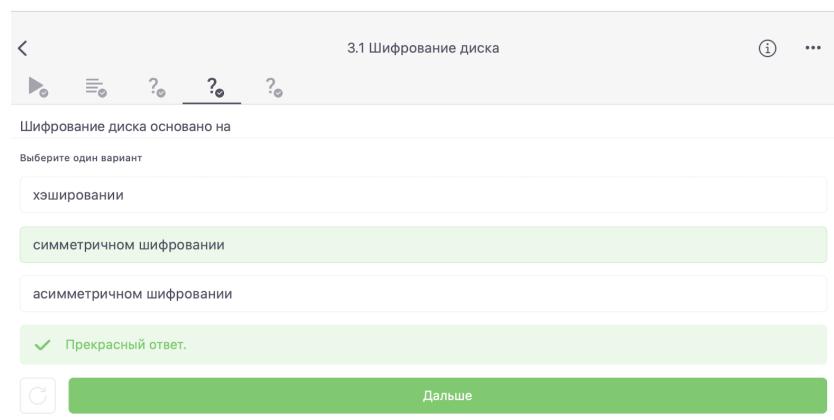


Figure 2.24: вопрос 2

Ответ: Шифрование диска основано на симметричном шифровании, где один ключ используется как для шифрования, так и для расшифровки данных.

С помощью каких программ можно зашифровать жесткий диск?

Выберите один или несколько вариантов

BitLocker

Wireshark

Disk Utility

VeraCrypt

✓ Отличное решение!

Попробовать снова

The screenshot shows a mobile application interface with a light gray background. At the top, there's a header with some text in Russian. Below it, a section asks a question in Russian and instructs the user to select one or more options. There are four options listed: 'BitLocker', 'Wireshark', 'Disk Utility', and 'VeraCrypt'. The 'BitLocker' and 'VeraCrypt' buttons are highlighted with a green background, while the others are white. Below these buttons, a green bar contains the text '✓ Отличное решение!' (Excellent answer!). At the bottom of the screen, there's a button labeled 'Попробовать снова' (Try again).

Figure 2.25: вопрос 3

Ответ: Программы, с помощью которых можно зашифровать жесткий диск, это BitLocker, VeraCrypt. Wireshark, однако, не предназначен для шифрования дисков, а используется для анализа сетевого трафика.

## 2.6 Пароли

< 3.2 Пароли ...

▶ ⏪ ⏩ ? ? ? ? ?

Какие пароли можно отнести к стойким?

Выберите один вариант

qwerty12345

ILOVECATS

UQr9@j4!S\$

IDONTLOVECATS

✓ Хорошая работа.

Дальше

The screenshot shows a mobile application interface with a light gray background. At the top, there's a header with the number '3.2' and the word 'Пароли'. Below it, a navigation bar has icons for back, forward, and search. The main question asks what passwords can be considered strong. It lists five options: 'qwerty12345', 'ILOVECATS', 'UQr9@j4!S\$', 'IDONTLOVECATS', and an empty input field. The 'UQr9@j4!S\$' input field is highlighted with a green background, and a green bar below it contains the text '✓ Хорошая работа.' (Good job.). At the bottom, there's a large green button with a white arrow pointing right and the text 'Дальше' (Next).

Figure 2.26: вопрос 1

Ответ: Пароли, которые можно отнести к стойким: -UQr9@j4!S2. Потому что в пароле есть символы, заглавные и маленькие буквы.

Где безопасно хранить пароли?

Выберите один вариант

В менеджерах паролей

В заметках на рабочем столе

В заметках в телефоне

На стикере, приkleенном к монитору

В кошельке

Прекрасный ответ.

 Дальше

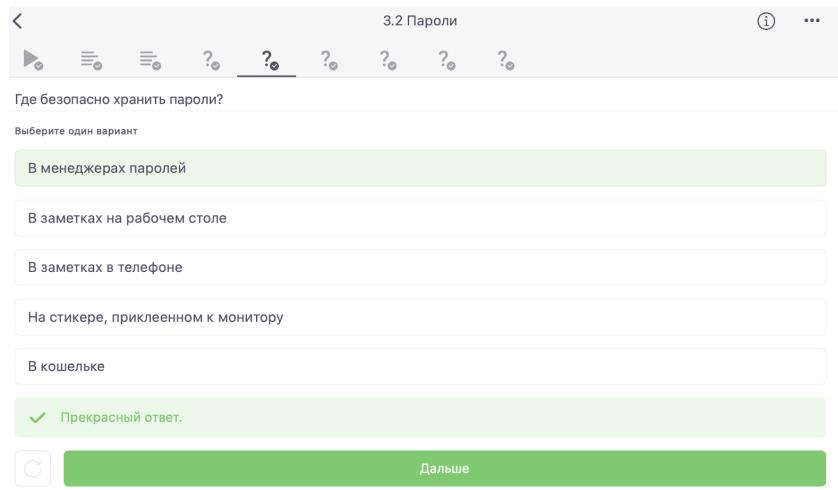


Figure 2.27: вопрос 2

Ответ: В менеджерах паролей

Зачем нужна капча?

Выберите один вариант

Для защиты кук пользователя

Она заменяет пароли

Для безопасного хранения паролей на сервере

Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

Правильно, молодец!

 Дальше

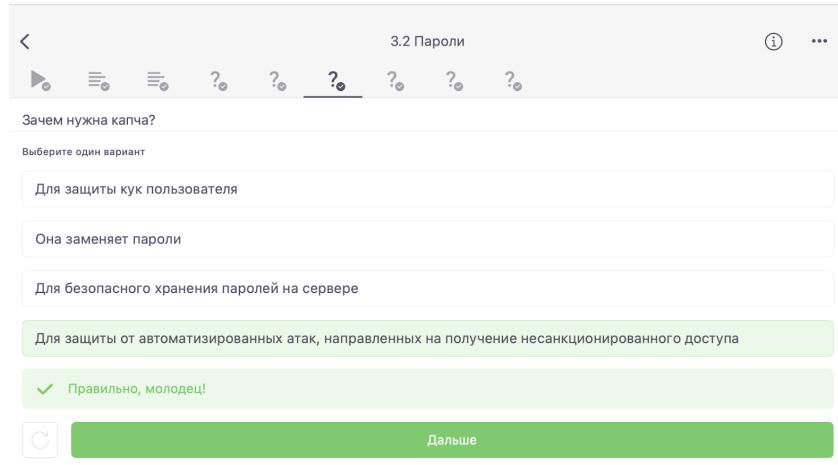


Figure 2.28: вопрос 3

Ответ: Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

< 3.2 Пароли ⓘ ...

Для чего применяется хэширование паролей?

Выберите один вариант

Для того, чтобы пароль не передавался в открытом виде.

Для того, чтобы ускорить процесс авторизации

Для того, чтобы не хранить пароли на сервере в открытом виде.

Для удобства разработчиков

✓ Верно.

◀ Дальше

Figure 2.29: вопрос 4

Ответ: Для того, чтобы пароль не передавался в открытом виде. Для того, чтобы не хранить пароли на сервере в открытом виде.

< 3.2 Пароли ⓘ ...

Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?

Выберите один вариант

Нет

Да

✓ Верно. Так держать!

◀ Дальше

Figure 2.30: вопрос 5

Ответ: Нет, если злоумышленник получил доступ к серверу соль не поможет.

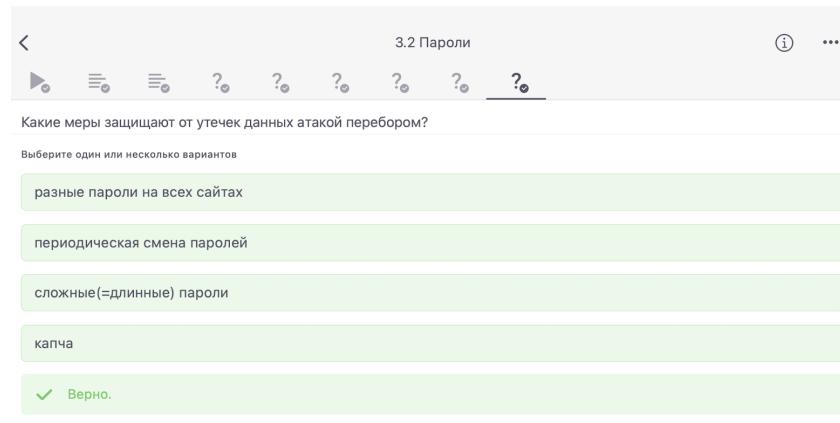


Figure 2.31: вопрос 6

Ответ: Разные пароли на всех сайтах, периодическая смена паролей, сложные (=длинные) пароли, капча.

## 2.7 Фишинг

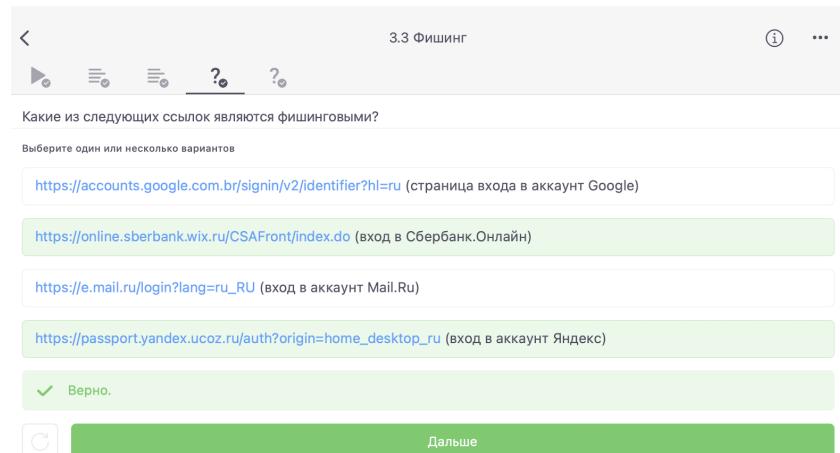


Figure 2.32: вопрос 1

Ответ: Не все предложенные ссылки являются фишинговыми, потому что название может и быть похожа на оригинал, но дальше идут не понятные символы. Чаще всего этим пользуются мошенники.

The screenshot shows a mobile application interface. At the top, there is a navigation bar with icons for back, forward, and help, followed by the title "3.3 Фишинг". On the right side of the title are three dots. Below the title is a question: "Может ли фишинговый имейл прийти от знакомого адреса?". A note below the question says "Выберите один вариант". There are two options: "Да" (selected) and "Нет". A green feedback box at the bottom left says "✓ Отличное решение!". Below the feedback box is a button labeled "Попробовать снова". At the bottom right is a button labeled "Следующий урок" with a right-pointing arrow.

Figure 2.33: вопрос 2

Ответ: Да, фишинговый имейл может прийти от знакомого адреса. Мошенники могут подделывать адрес отправителя, чтобы выглядеть более доверительно и убедительно. Поэтому всегда нужно быть осторожным.

## 2.8 Вирусы. Примеры

The screenshot shows a mobile application interface. At the top, there is a navigation bar with icons for back, forward, and help, followed by the title "3.4 Вирусы. Примеры". On the right side of the title are three dots. Below the title is a note: "Email Спупинг -- это". A note below the note says "Выберите один вариант". There are four options: "протокол для отправки имейлов", "атака перебором паролей", "подмена адреса отправителя в имейлах" (selected), and "метод предотвращения фишинга". A green feedback box at the bottom left says "✓ Всё правильно.". Below the feedback box is a button labeled "Дальше" with a circular arrow icon.

Figure 2.34: вопрос 1

Ответ: Email Спупинг – это подмена адреса отправителя в имейлах. Протокол для отправки писем SMTP не включает проверку адреса.

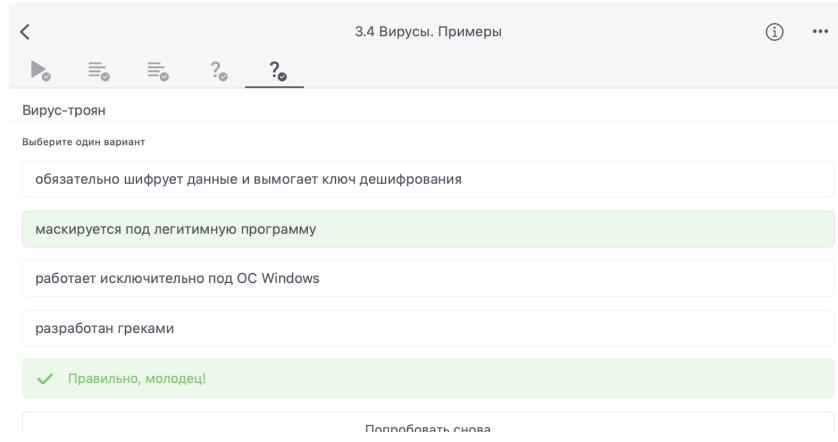


Figure 2.35: вопрос 2

Ответ: Троян - это вирус, который проникает в систему под видом какого-то легитимного программного обеспечения.

## 2.9 Безопасность мессенджеров

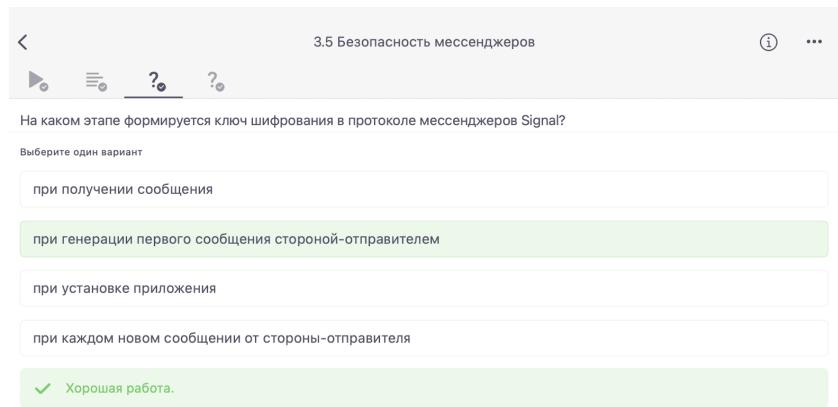


Figure 2.36: вопрос 1

Ответ: Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителем. Signal использует протокол двойного ключа, где каждый пользователь имеет свой уникальный ключ шифрования.

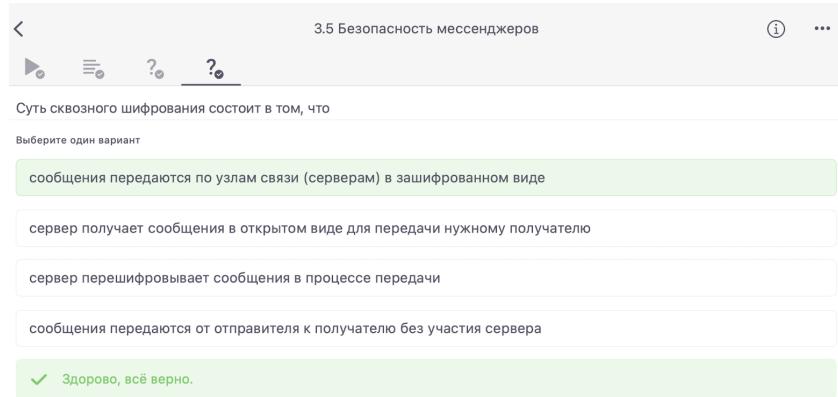


Figure 2.37: вопрос 2

Ответ: Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в защищенном виде. Это означает, что сервер не имеет доступа к содержимому сообщений, так как они зашифрованы на устройствах отправителя и расшифровываются только на устройстве получателя.

## 2.10 Введение в криптографию

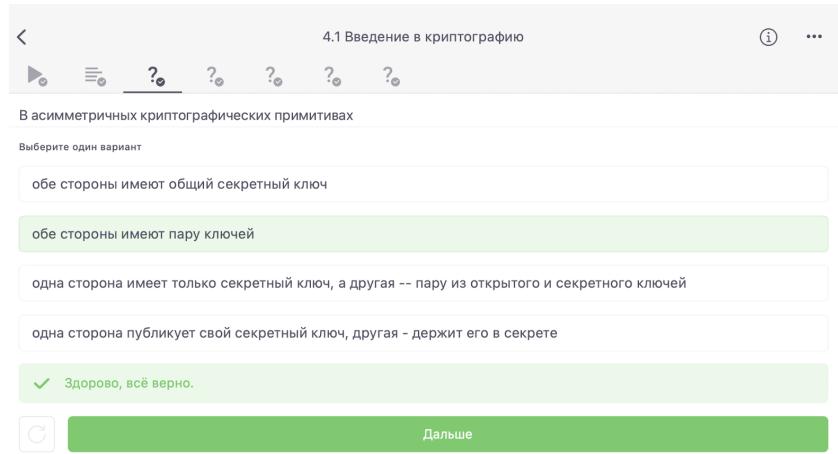


Figure 2.38: вопрос 1

Ответ: В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ.

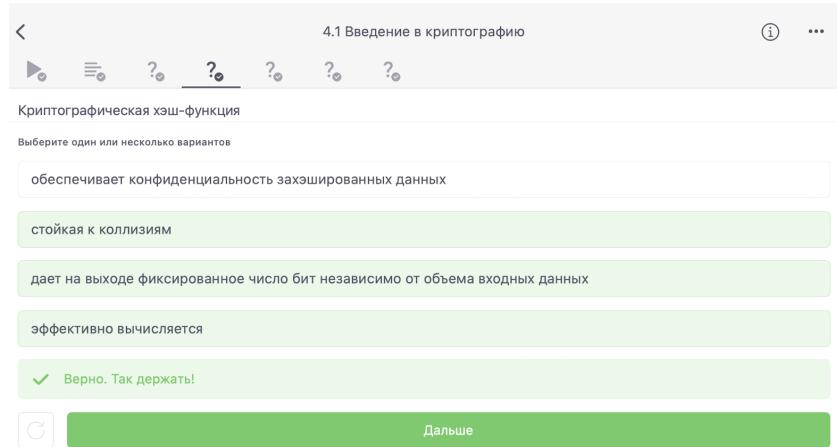


Figure 2.39: вопрос 2

Ответ: Криптографическая хэш-функция стойкая к коллизиям. Это важное свойство отличает криптографическую функцию от некриптографической. Криптографическую хэш-функцию сложно обратить. Также применение хэш-функции – это доказательство работы. По-другому это называется протоколом proof of work, который используется, например, в таком блокчейне, как биткойн.

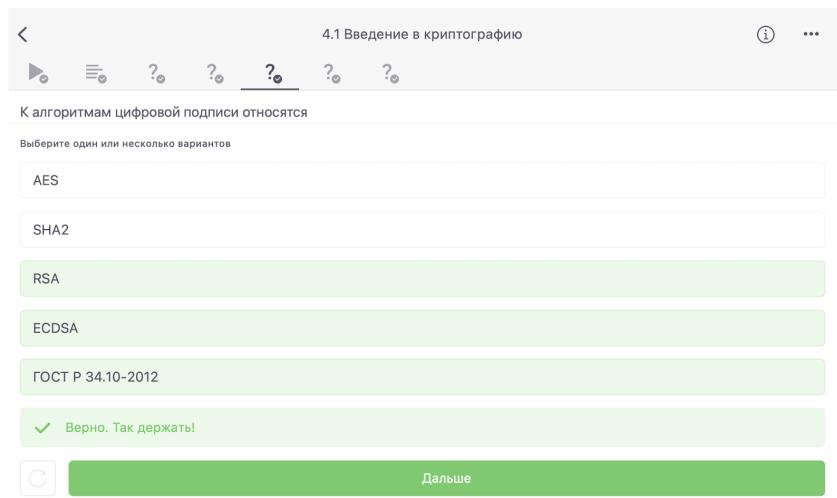


Figure 2.40: вопрос 3

Ответ: К алгоритмам цифровой подписи относятся: RSA ECDSA ГОСТ Р 34.10-2012

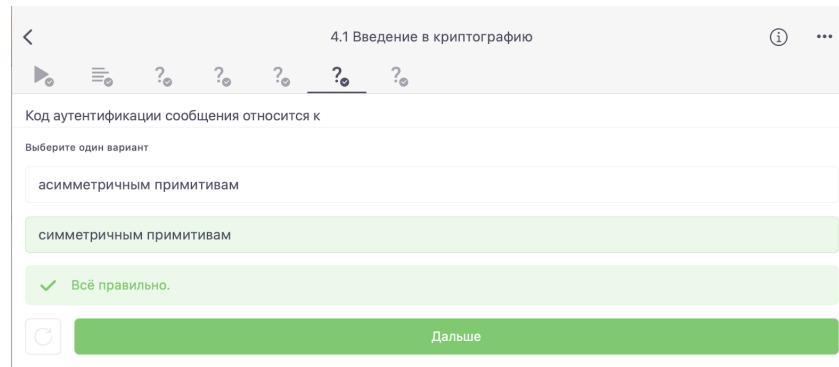


Figure 2.41: вопрос 4

Ответ: Симметричная криптография включает протоколы, где две или более стороны имеют общие секретные ключи, поэтому она и называется симметричной. К таким протоколам относят симметричное шифрование.

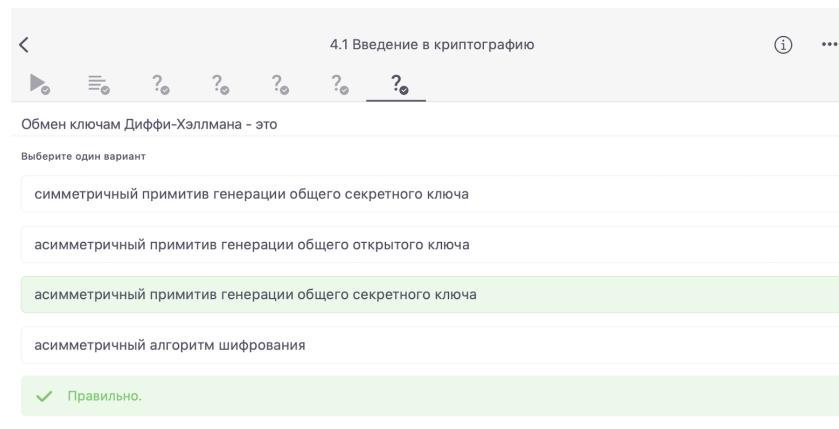


Figure 2.42: вопрос 5

Ответ: Асимметричный примитив генерации общего секретного ключа.

## 2.11 Цифровая подпись

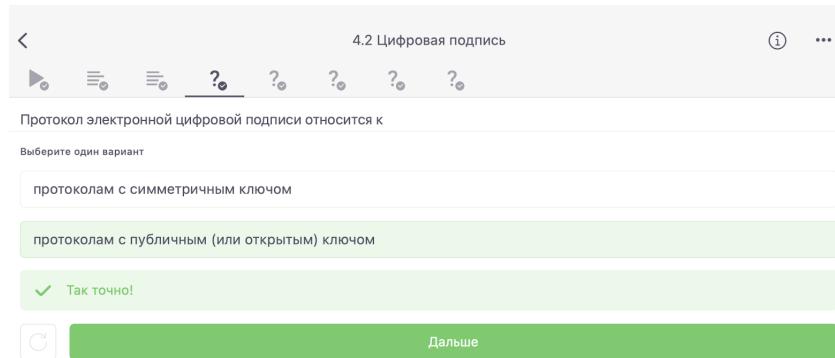


Figure 2.43: вопрос 1

Ответ: Цифровая подпись имеет прямую связь с асимметричной криптографии.

У каждой из сторон есть пара ключей: открытый ключ и секретный ключ.

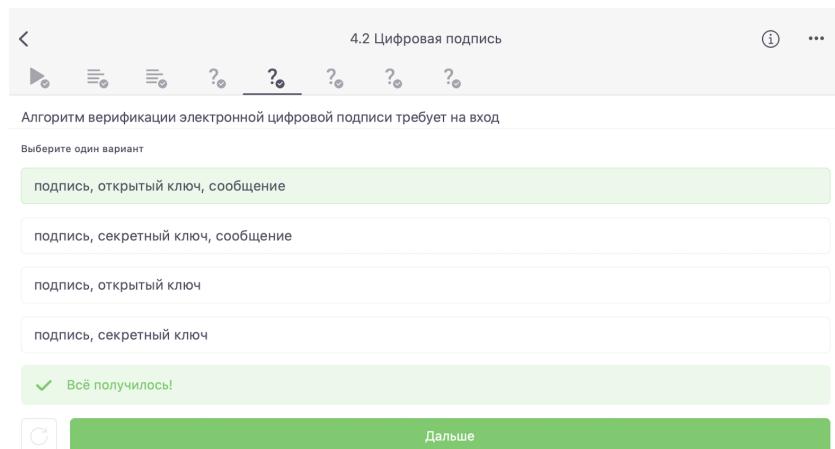


Figure 2.44: вопрос 2

Ответ: Первый алгоритм – генерирует ключи. Второй алгоритм – это генерация подписи, которая берет на вход сообщение и секретный ключ и выдает нам подпись. И третий – это верификация подписи, которая берёт на вход подпись, сообщение и открытый ключ и выдает нам либо тот факт, что подпись верна, либо тот факт, что подпись неверна.

The screenshot shows a digital quiz interface. At the top, there are navigation icons (back, forward, search, etc.) and the title "4.2 Цифровая подпись". Below the title is a question: "Электронная цифровая подпись не обеспечивает". A note below says "Выберите один вариант". There are four options in boxes: "неотказ от авторства" (not checked), "конфиденциальность" (checked, highlighted in green), "автентификацию" (not checked), and "целостность" (not checked). At the bottom, a green bar indicates the correct answer: "✓ Так точно!".

Figure 2.45: вопрос 3

Ответ: Цифровая подпись: обеспечивает целостность сообщения, аутентификацию сообщения, то есть мы можем установить принадлежность подписи владельцу. А также неотказ от авторства, то есть как только подпись подписана, подписавший её человек не может отказаться от того факта.

The screenshot shows a digital quiz interface. At the top, there are navigation icons (back, forward, search, etc.) and the title "4.2 Цифровая подпись". Below the title is a question: "Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?". A note below says "Выберите один вариант". There are three options in boxes: "усиленная квалифицированная" (checked, highlighted in green), "простая" (not checked), and "усиленная неквалифицированная" (not checked). At the bottom, a green bar indicates the correct answer: "✓ Прекрасный ответ.".

Figure 2.46: вопрос 4

Ответ: Усиленная квалифицированная, потому что первые два типа не имеет юридической силы или она довольно ограничена.

4.2 Цифровая подпись

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант

в любой организации, имеющей соответствующую лицензию ФСБ

в минкомсвязи РФ

в удостоверяющем (сертификационном) центре

в любой организации по месту работы

✓ Всё получилось!

Figure 2.47: вопрос 5

Ответ: Чтобы получить такую подпись, вам нужно пойти со своим паспортом и с другими данными в сертификационный центр, который должен быть аккредитован конкретным министерством.

## 2.12 Электронные платежи

4.3 Электронные платежи

Выберите из списка все платежные системы.

Выберите один или несколько вариантов

BitCoin

MasterCard

SecurePay

POS-терминал

банкомат

МИР

✓ Всё правильно.

Figure 2.48: вопрос 1

Ответ: MasterCard и Visa являются платежными системами, потому что они представляют инфраструктуру для обработки платежей между банками, торговыми

точками и потребителями, обеспечивая безопасность, эффективность и удобство в проведении финансовых транзакций.

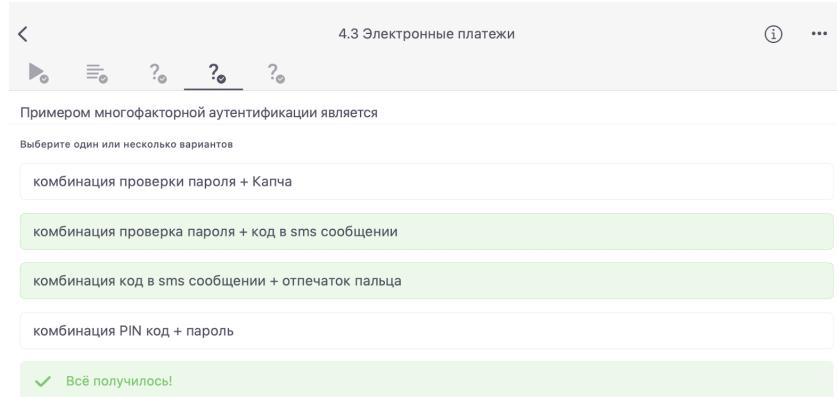


Figure 2.49: вопрос 2

Ответ: Комбинация проверки пароля + код в SMS сообщений: Это пример увеличивает безопасность доступа. Комбинация код в SMS сообщений + отпечаток пальца: Это также пример многофакторной аутентификации, что делает процесс аутентификации более надежным.

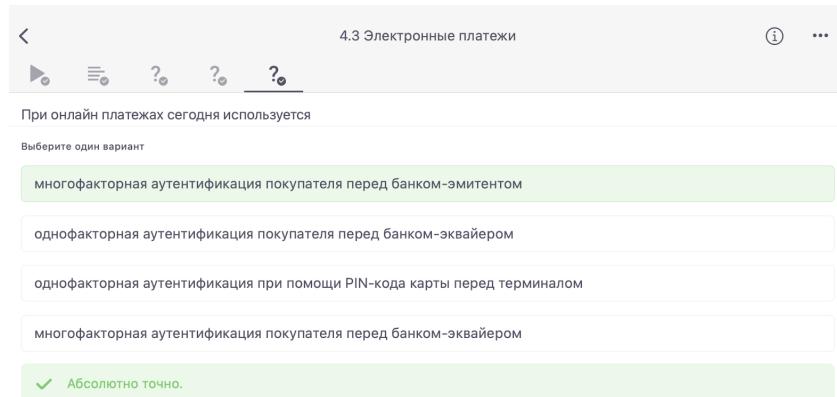


Figure 2.50: вопрос 3

Ответ: . Аутентификация это криптографический протокол, в котором есть две стороны: первая – это доказуемая (в этом случае покупатель) и проверяющая (в этом случае это банк), которые доказывают, что некое утверждение верно.

## 2.13 Блокчейн

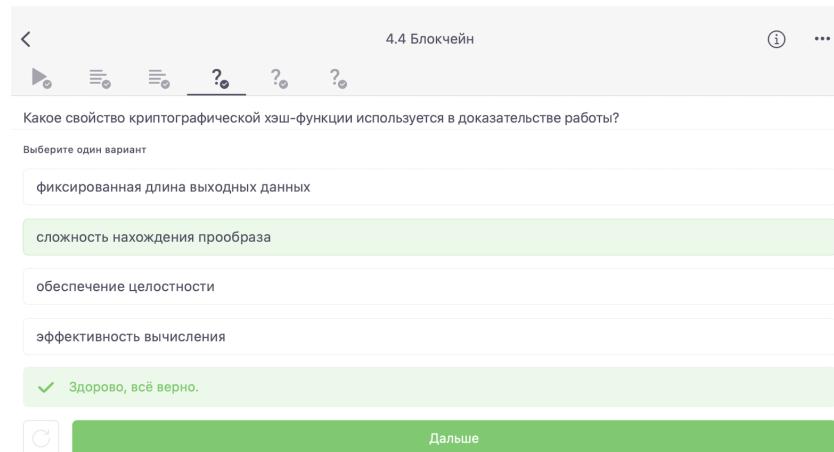


Figure 2.51: вопрос 1

Ответ: Свойство криптографической хэш-функции, используемое в доказательстве работы - сложность нахождения прообраза. Это означает, что для данного хэш-значения сложно найти исходное сообщение, что делает доказательство работы более надежным.

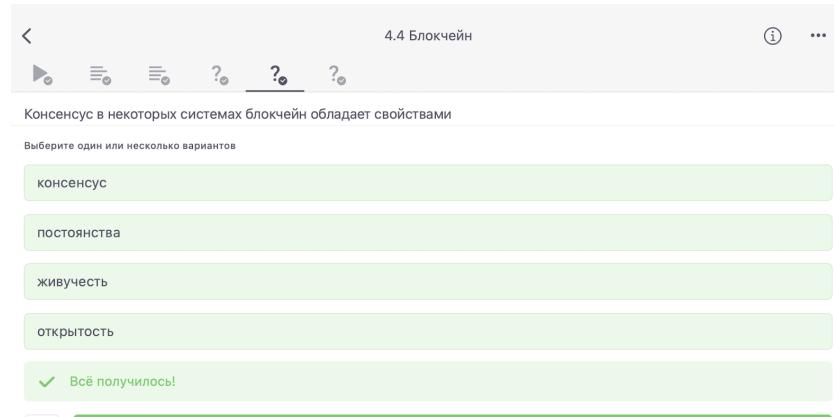


Figure 2.52: вопрос 2

Ответ: Консенсус в некоторых системах блокчейн обладает свойствами постоянства, консенсуса и живучести и открытости. Эти свойства позволяют системе блокчейн функционировать надежно, сохраняя целостность данных, достигая согласия участников и обеспечивая устойчивость к атакам.

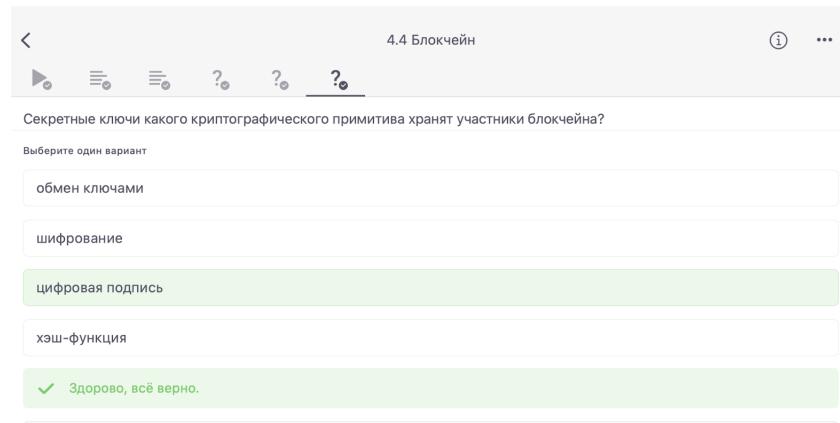


Figure 2.53: вопрос 3

Ответ: Участники блокчейна хранят секретные ключи для цифровой подписи. Цифровая подпись используется для подтверждения авторства и целостности данных в блокчейне, а хранение секретных ключей является важным для обеспечения безопасности этого процесса.

## **3 Выводы**

Мы узнали, как работает персонализация сети, Браузер TOR, анонимизация и беспроводные сети Wi-fi . Мы научились шифровать диск и находить правильные пароли. Узнали, как можно обезопасить свои мессенджеры и для чего нужна цифровая подпись. Разобрались, откуда появился блокчейн и как он работает.