

Stepik ПО ОСНОВАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Курс Stepik - Основы кибербезопасности

Заболотная Кристина Александровна

Содержание

1	1.1 О курсе	9
2	2. Безопасность в сети	10
2.1	2.1 Как работает интернет: базовые сетевые протоколы	10
2.1.1	Протокол прикладного уровня - HTTPS.	10
2.1.2	Уровень работы протокола TCP – Транспортный.	10
2.1.3	Все корректные адреса IPv4 - 90.11.90.22, 25.198.0.15.	11
2.1.4	DNS сервер - сопоставляет IP адреса доменным именам.	12
2.1.5	Корректная последовательность протоколов в модели TCP/IP - прикладной – транспортный – сетевой – канальный.	12
2.1.6	Протокол http предполагает - передачу данных между клиентом и сервером в открытом виде.	13
2.1.7	Протокол https состоит из - двух фаз: рукопожатия и передачи данных.	14
2.1.8	Версия протокола TLS определяется - и клиентом, и сервером в процессе “переговоров”.	15
2.1.9	В фазе “рукопожатия” протокола TLS не предусмотрено - шифрование данных.	15
2.2	2.2 Персонализация сети	16
2.2.1	Куки хранят - идентификатор пользователя, id сессии.	16
2.2.2	Куки не используются для - улучшения надежности соединения.	17
2.2.3	Куки генерируются – сервером.	17
2.2.4	Сессионные куки хранятся в браузере - Да, на время пользования веб-сайтом.	18
2.3	2.3 Браузер TOR. Анонимизация.	19
2.3.1	Сколько промежуточных узлов в луковой сети TOR – 3.	19
2.3.2	IP-адрес получателя известен – отправителю и выходному узлу.	19
2.3.3	Отправитель генерирует общий секретный ключ - с охранным, промежуточным и выходном узлом.	20
2.3.4	Должен ли получатель использовать браузер Tor для успешного получения пакетов – нет.	21
2.4	2.4 Беспроводные сети Wi-fi	22
2.4.1	Wi-Fi – это - технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11.	22
2.4.2	Уровень работы протокола WiFi – канальный.	23

2.4.3	Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi – WEP.	23
2.4.4	Данные между хостом сети (компьютером или смартфоном) и роутером - передаются в зашифрованном виде после аутентификации устройств.	24
2.4.5	Для домашней сети для аутентификации обычно используется метод - WPA2 Personal.	25
3	3. Защита ПК/телефона	27
3.1	3.1 Шифрование диска	27
3.1.1	Можно ли зашифровать загрузочный сектор диска – да. . .	27
3.1.2	Шифрование диска основано на - симметричном шифровании.	27
3.1.3	С помощью каких программ можно зашифровать жесткий диск – VeraCrypt, BitLocker.	28
3.2	3.2 Пароли	29
3.2.1	Какие пароли можно отнести с стойким - UQr9@j4!S\$. . . .	29
3.2.2	Где безопасно хранить пароли - в менеджерах паролей. . .	30
3.2.3	Зачем нужна капча - для защиты от автоматизированных атак, направленных на получение несанкционированного доступа.	31
3.2.4	Для чего применяется хэширование паролей - для того, чтобы не хранить пароли на сервере в открытом виде. . . .	31
3.2.5	Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу – нет.	32
3.2.6	Какие меры защищают от утечек данных атакой перебором – разные пароли на всех сайтах, капча, сложные пароли, периодическая смена паролей.	33
3.3	3.3 Фишинг	34
3.3.1	Какие из следующих ссылок являются фишинговыми – Сбербанк онлайн, аккаунт Яндекс.	34
3.3.2	Может ли фишинговый имейл прийти от знакомого адреса – да.	34
3.4	3.4 Вирусы. Примеры	35
3.4.1	Email Спупинг – это подмена адреса отправителя в имейлах. . .	35
3.4.2	Вирус-троян - маскируется под легитимную программу. . .	36
3.5	3.5 Безопасность мессенджеров	36
3.5.1	На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal - при генерации первого сообщения стороной-отправителем.	36
3.5.2	Суть сквозного шифрования состоит в том, что - сообщения передаются по узлам связи (серверам) в зашифрованном виде.	37

4 4. Криптография на практике	38
4.1 4.1 Введение в криптографию	38
4.1.1 В асимметричных криптографических примитивах - обе стороны имеют пару ключей.	38
4.1.2 Криптографическая хэш-функция - дает на выходе фиксированное число бит независимо от объема входных данных, эффективно вычисляется, стойкая к коллизиям.	39
4.1.3 К алгоритмам цифровой подписи относятся – RSA, ECDSA, ГОСТ Р 34.10-2012.	40
4.1.4 Код аутентификации сообщения относится к - симметричным примитивам.	40
4.1.5 Обмен ключами Диффи-Хэллмана – это асимметричный примитив генерации общего секретного ключа.	41
4.2 4.2. Цифровая подпись	42
4.2.1 Протокол электронной цифровой подписи относится к - протоколам с публичным (или открытым) ключом.	42
4.2.2 Алгоритм верификации электронной цифровой подписи требует на вход - подпись, открытый ключ, сообщение.	43
4.2.3 Электронная цифровая подпись не обеспечивает – конфиденциальность.	44
4.2.4 Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС - усиленная квалифицированная.	45
4.2.5 В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи - в удостоверяющем (сертификационном) центре.	46
4.3 4.3 Электронные платежи	47
4.3.1 Выберите из списка все платежные системы – MasterCard, МИР.	47
4.3.2 Примером многофакторной аутентификации является - комбинация код в sms сообщении + отпечаток пальца, комбинация проверка пароля + код в sms сообщении.	48
4.3.3 При онлайн платежах сегодня используется - многофакторная аутентификация покупателя перед банком-эмитентом.	49
4.4 4.4 Блокчейн	50
4.4.1 Какое свойство криптографической хэш-функции используется в доказательстве работы - сложность нахождения прообраза.	50
4.4.2 Консенсус в некоторых системах блокчейн обладает свойствами – постоянства, открытость, живучесть, консенсус. .	51
4.4.3 Секретные ключи какого криптографического примитива хранят участники блокчейна - цифровая подпись.	52
4.4.4 Полученный сертификат:	53

Список иллюстраций

2.1	HTTPS	10
2.2	Транспортный	11
2.3	90.11.90.22, 25.198.0.15	11
2.4	IP	12
2.5	прикладной – транспортный – сетевой – канальный	13
2.6	передачу данных между клиентом и сервером в открытом виде	14
2.7	двух фаз: рукопожатия и передачи данных	14
2.8	шифрование данных	16
2.9	идентификатор пользователя, id сессии	16
2.10	улучшения надежности соединения	17
2.11	сервером	18
2.12	Да, на время пользования веб-сайтом	18
2.13	3	19
2.14	отправителю и выходному узлу	20
2.15	с охранным, промежуточным и выходном узлом	21
2.16	нет	22
2.17	IEEE 802.11	22
2.18	канальный	23
2.19	WEP	24
2.20	передаются в зашифрованном виде после аутентификации устройств	25
2.21	WPA2 Personal	26
3.1	да	27
3.2	симметричном шифровании	28
3.3	VeraCrypt, BitLocker	29
3.4	UQr9@j4!S\$	30
3.5	в менеджерах паролей	30
3.6	для защиты от автоматизированных атак, направленных на получение несанкционированного доступа	31
3.7	для того, чтобы не хранить пароли на сервере в открытом виде	32
3.8	нет	32
3.9	разные пароли на всех сайтах, капча, сложные пароли, периодическая смена паролей	33
3.10	Сбербанк онлайн, аккаунт Яндекс	34
3.11	да	35
3.12	это подмена адреса отправителя в имейлах	35

3.13 маскируется под легитимную программу	36
3.14 при генерации первого сообщения стороной-отправителем	37
3.15 сообщения передаются по узлам связи (серверам) в зашифрованном виде	37
4.1 обе стороны имеют пару ключей	38
4.2 дает на выходе фиксированное число бит независимо от объема входных данных, эффективно вычисляется, стойкая к коллизиям	39
4.3 RSA, ECDSA, ГОСТ Р 34.10-2012	40
4.4 симметричным примитивам	41
4.5 это асимметричный примитив генерации общего секретного ключа	42
4.6 протоколам с публичным (или открытым) ключом	43
4.7 подпись, открытый ключ, сообщение	44
4.8 конфиденциальность	45
4.9 усиленная квалифицированная	46
4.10 в удостоверяющем (сертификационном) центре	47
4.11 MasterCard, МИР	47
4.12 комбинация код в sms сообщении + отпечаток пальца, комбинация проверка пароля + код в sms сообщении	48
4.13 многофакторная аутентификация покупателя перед банком-эмитентом	49
4.14 сложность нахождения прообраза	50
4.15 постоянства, открытость, живучесть, консенсус	51
4.16 цифровая подпись	52
4.17 Сертификат	53

Список таблиц

1 1.1 О курсе

2 2. Безопасность в сети

2.1 2.1 Как работает интернет: базовые сетевые протоколы

2.1.1 Протокол прикладного уровня - HTTPS.

Протокол HTTP(S) является примером протокола прикладного уровня, по которому передаются веб-страницы. [1]

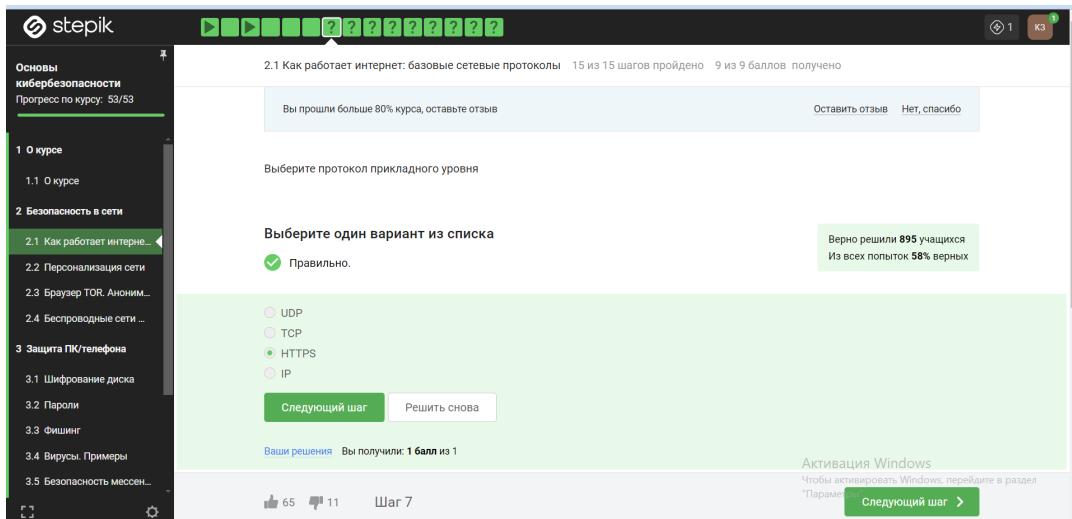


Рис. 2.1: HTTPS

2.1.2 Уровень работы протокола TCP – Транспортный.

На транспортном уровне существует два примера протокола: первый — это TCP, в честь которого названа модель. Этот протокол, в отличие от второго при-

мера – UDP, обеспечивает надежную передачу пакетов.

The screenshot shows a Stepik course interface. On the left, a sidebar lists course modules: 1 О курсе, 1.1 О курсе, 2 Безопасность в сети, 3 Защита ПК/телефона, and 4 Активация Windows. The main content area displays a step titled '2.1 Как работает интернет: базовые сетевые протоколы'. It shows progress: 15 из 15 шагов пройдено, 9 из 9 баллов получено. A message at the top says 'Вы прошли больше 80% курса, оставьте отзыв' with buttons 'Оставить отзыв' and 'Нет, спасибо'. Below this, a question asks 'На каком уровне работает протокол TCP?'. A green box indicates the correct answer was selected: 'Всё получилось!' with a checkmark. The correct answer is 'Транспортном'. The interface includes a navigation bar with arrows, a progress bar with question marks, and a sidebar with course statistics: 1 курсе, 1.0 курсе, 2 Безопасность в сети (2.1 Как работает интернет...), 3 Защита ПК/телефона (3.1 Шифрование диска), 4 Активация Windows (Чтобы активировать Windows, перейдите в раздел "Параметры"). At the bottom, there are like (65), dislike (11) buttons, and a 'Шаг 8' button.

Рис. 2.2: Транспортный

2.1.3 Все корректные адреса IPv4 - 90.11.90.22, 25.198.0.15.

Например, адрес IPv4 может выглядеть вот так: 192.168.1.4. Первые три числа — это номер сети.

This screenshot shows another Stepik course step. The sidebar and course structure are identical to the previous one. The main content area displays a step titled '2.1 Как работает интернет: базовые сетевые протоколы'. Progress: 15 из 15 шагов пройдено, 9 из 9 баллов получено. A message at the top says 'Вы прошли больше 80% курса, оставьте отзыв' with buttons 'Оставить отзыв' and 'Нет, спасибо'. Below this, a question asks 'Выберите все корректные адреса IPv4'. A green box indicates the correct answer was selected: 'Прекрасный ответ.' with a checkmark. A note below says 'Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить своё решение с другими на форуме решений.' The correct answers listed are '421.0.15.19', '43.12.256.7', '90.11.90.22', and '25.198.0.15'. The interface includes a navigation bar with arrows, a progress bar with question marks, and a sidebar with course statistics: 1 курсе, 1.0 курсе, 2 Безопасность в сети (2.1 Как работает интернет...), 3 Защита ПК/телефона (3.1 Шифрование диска), 4 Активация Windows (Чтобы активировать Windows, перейдите в раздел "Параметры"). At the bottom, there are like (65), dislike (11) buttons, and a 'Шаг 8' button.

Рис. 2.3: 90.11.90.22, 25.198.0.15

2.1.4 DNS сервер - сопоставляет IP адреса доменным именам.

Доменное имя — это как раз-таки то, что мы называем ссылкой - yandex.ru, google.com, mail.ru и так далее. И основная задача этого DNS-сервера — это со-поставить название, то есть доменное имя, с корректным IP-адресом, с тем, где лежит этот сервер, этот сайт.

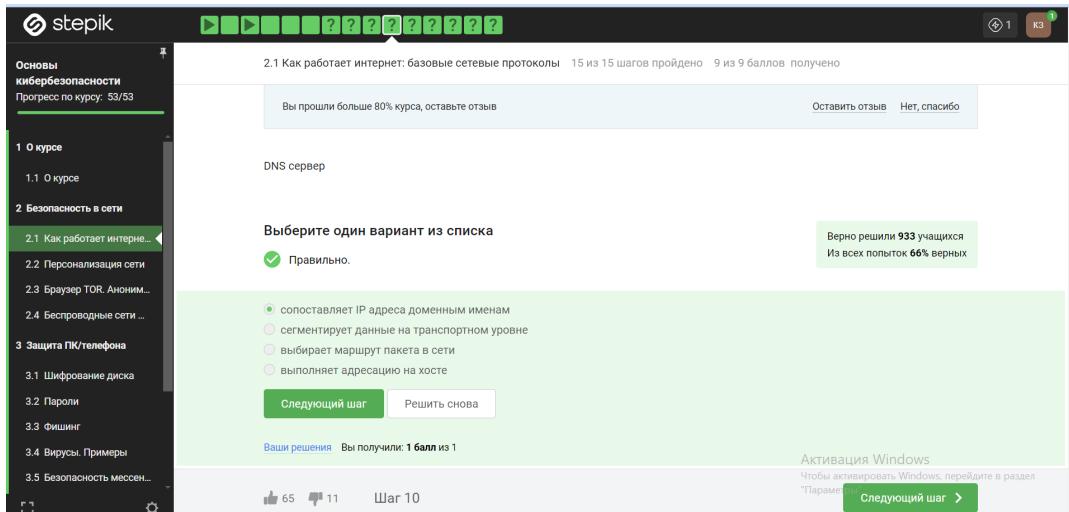


Рис. 2.4: IP

2.1.5 Корректная последовательность протоколов в модели TCP/IP - прикладной – транспортный – сетевой – канальный.

Документами, определяющими сертификацию модели, являются RFC 1122 и RFC1123. Эти стандарты описывают четыре уровня абстракции модели TCP/IP: прикладной, транспортный, межсетевой и канальный.

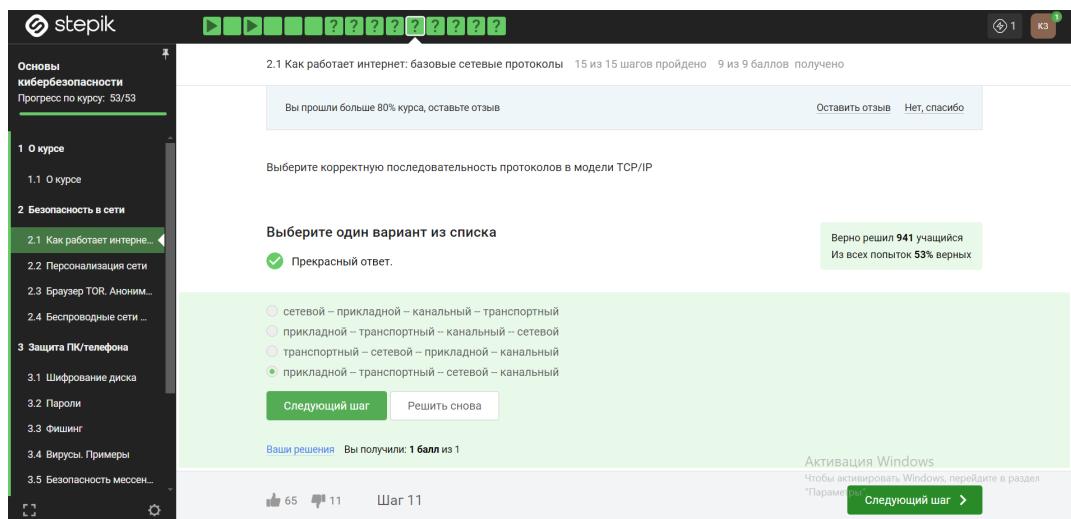


Рис. 2.5: прикладной – транспортный – сетевой – канальный

2.1.6 Протокол http предполагает - передачу данных между клиентом и сервером в открытом виде.

Принцип взаимодействия на основе протокола HTTP основан на схеме “запрос-ответ” и предполагает следующую последовательность действий: клиент формирует сообщение-запрос и передает серверу; сервер получает сообщение, анализирует и обрабатывает запрос, формирует сообщение-ответ и направляет его клиенту.

The screenshot shows a Stepik course interface. On the left, a sidebar lists chapters: 1 О курсе, 1.1 О курсе, 2 Безопасность в сети, 2.1 Как работает интернет..., 2.2 Персонализация сети, 2.3 Браузер TOR. Аноним..., 2.4 Беспроводные сети ..., 3 Защита ПК/телефона, 3.1 Шифрование диска, 3.2 Пароли, 3.3 Фишинг, 3.4 Вирусы. Примеры, 3.5 Безопасность мессен... . The main content area displays a step titled '2.1 Как работает интернет: базовые сетевые протоколы'. It shows progress: '15 из 15 шагов пройдено' and '9 из 9 баллов получено'. A message says 'Вы прошли больше 80% курса, оставьте отзыв'. Below it, a question asks 'Протокол http предполагает' with a correct answer highlighted: 'передачу данных между клиентом и сервером в открытом виде'. A green box indicates 'Верно решили 965 учащихся Из всех попыток 78% верных'. Buttons for 'Следующий шаг' and 'Решить снова' are visible. At the bottom, social sharing icons show 65 likes and 11 dislikes, and a note 'Шаг 12'. A sidebar on the right says 'Активация Windows'.

Рис. 2.6: передачу данных между клиентом и сервером в открытом виде

2.1.7 Протокол https состоит из - двух фаз: рукопожатия и передачи данных.

Клиент устанавливает TCP соединения (или другое соединение, если не используется TCP транспорт) и клиент отправляет запрос и ждёт ответа (сервер обрабатывает запрос и посыпает ответ, в котором содержится код статуса и соответствующие данные).

The screenshot shows a Stepik course interface, similar to the one above. The sidebar and main content area are identical. The question 'Протокол https состоит из' has a correct answer selected: 'двух фаз: рукопожатия и передачи данных'. A green box indicates 'Верно решили 948 учащихся Из всех попыток 41% верных'. Buttons for 'Следующий шаг' and 'Решить снова' are visible. At the bottom, social sharing icons show 65 likes and 11 dislikes, and a note 'Шаг 13'. A sidebar on the right says 'Активация Windows'.

Рис. 2.7: двух фаз: рукопожатия и передачи данных

2.1.8 Версия протокола TLS определяется - и клиентом, и сервером в процессе “переговоров”.

Протокол, используемый для данного подключения, зависит от возможностей соответствующих компонентов как на стороне клиента, так и на стороне

The screenshot shows a Stepik course interface. On the left, there's a sidebar with a navigation tree. The main area displays a question titled "2.1 Как работает интернет: базовые сетевые протоколы". The question text is: "Версия протокола TLS определяется". Below it, a note says: "Вы прошли больше 80% курса, оставьте отзыв". A button "Оставить отзыв" is visible. The question type is "Выберите один вариант из списка". The correct answer is marked with a green checkmark and labeled "Прекрасный ответ.". The options listed are: "сервером", "клиентом", "и клиентом, и сервером в процессе “переговоров”, and "провайдером клиента". A green box at the bottom right indicates: "Верно решили 947 учащихся Из всех попыток 55% верных". At the bottom of the page, there are buttons for "Следующий шаг" and "Решить снова". A note at the bottom right says: "Активация Windows Чтобы активировать Windows, перейдите в раздел “Параметры” и нажмите “Активировать”." A "Следующий шаг >" button is also present.

2.1.9 В фазе “рукопожатия” протокола TLS не предусмотрено - шифрование данных.

В ходе TLS-рукопожатия клиент и сервер вместе: указывают, какую версию TLS (TLS 1.0, 1.2, 1.3 и т. д.) они будут использовать. Решают, какие наборы шифров (см. ниже) они будут использовать. Проверяют подлинность сервера с помощью открытого ключа сервера и цифровой подписи центра сертификации SSL. Генерируют сеансовые ключи, чтобы использовать симметричное шифрование после завершения рукопожатия.

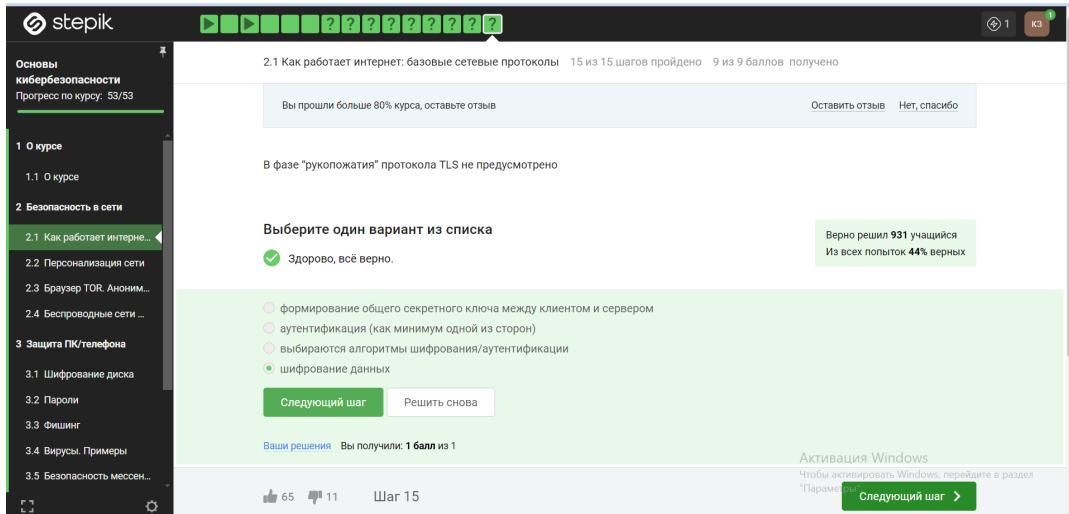


Рис. 2.8: шифрование данных

2.2 2.2 Персонализация сети

2.2.1 Куки хранят - идентификатор пользователя, id сессии.

Куки, как правило, хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, иногда описан тип браузера и время запросов, и некоторые действия пользователей.

Рис. 2.9: идентификатор пользователя, id сессии

2.2.2 Куки не используются для - улучшения надежности соединения.

Cookies используются при навигации на сайте и удаляются при закрытии окна браузера. Используются при аутентификации, сборе статистики посещаемости сайта, персонализации веб-страниц, отслеживания информации о пользователе.

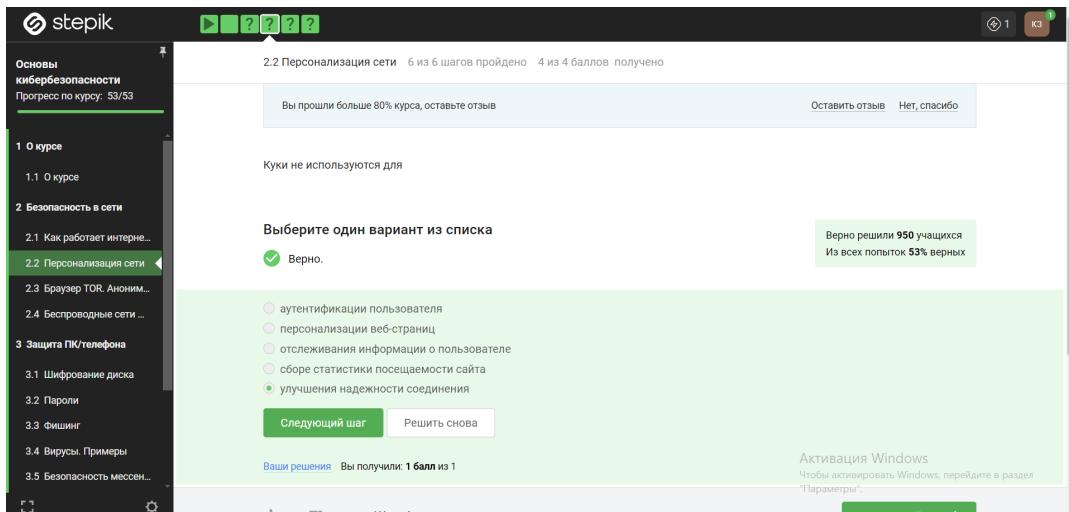


Рис. 2.10: улучшения надежности соединения

2.2.3 Куки генерируются – сервером.

Сервер кодирует настройки в cookie и отправляет cookie обратно в браузер. Таким образом, каждый раз, когда пользователь получает доступ к странице на веб-сайте, сервер может персонализировать страницу в соответствии с предпочтениями пользователя.

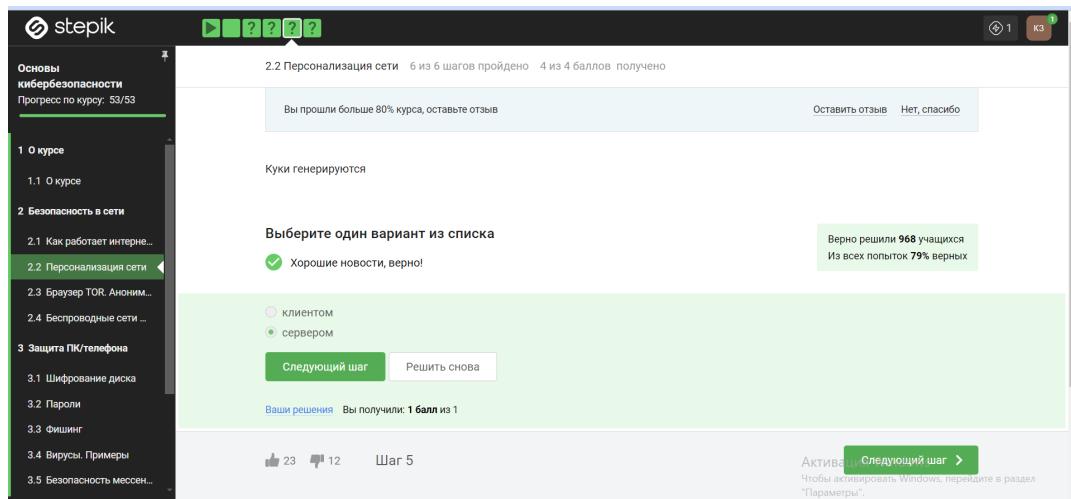


Рис. 2.11: сервером

2.2.4 Сессионные куки хранятся в браузере - Да, на время пользования веб-сайтом.

Сессионные cookies являются временными файлами, которые сохраняются в браузере пользователя только до тех пор, пока он находится на веб-сайте.

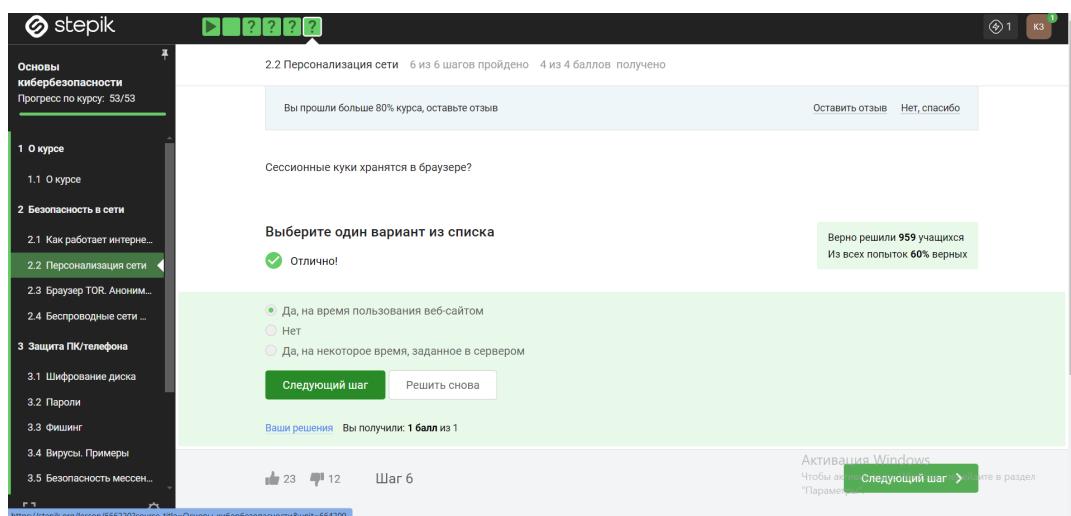


Рис. 2.12: Да, на время пользования веб-сайтом

2.3 2.3 Браузер TOR. Анонимизация.

2.3.1 Сколько промежуточных узлов в луковой сети TOR – 3.

Для каждого запроса случайно выбирается маршрут через один из трех узлов, а каждый следующий узел шифрует предыдущий.

The screenshot shows a Stepik course interface. On the left, there's a sidebar with a tree view of the course structure:

- Основы кибербезопасности
- Прогресс по курсу: 53/53
- 1 О курсе
- 1.1 О курсе
- 2 Безопасность в сети
- 2.1 Как работает интернет...
- 2.2 Персонализация сети
- 2.3 Браузер TOR. Анонимизация
- 2.4 Беспроводные сети ...
- 3 Защита ПК/телефона
- 3.1 Шифрование диска
- 3.2 Пароли
- 3.3 Фишинг
- 3.4 Вирусы. Примеры
- 3.5 Безопасность мессен...

The main content area displays a question: "Сколько промежуточных узлов в луковой сети TOR?". Below it, a list of options is shown: 2, 3 (selected), and 4. A green checkmark indicates the answer is correct. The interface also shows statistics: "Верно решили 959 учащихся" and "Из всех попыток 77% верных". At the bottom, there are buttons for "Следующий шаг" and "Решить снова".

Рис. 2.13: 3

2.3.2 IP-адрес получателя известен – отправителю и выходному узлу.

Когда отправитель отправляет данные через интернет, он указывает IP-адрес получателя в заголовке пакета данных. Этот IP-адрес известен отправителю, так как он сам его указал, и выходному узлу, который используется для маршрутизации пакетов к конечному получателю. Таким образом, IP-адрес получателя является необходимой информацией для передачи данных в сети.

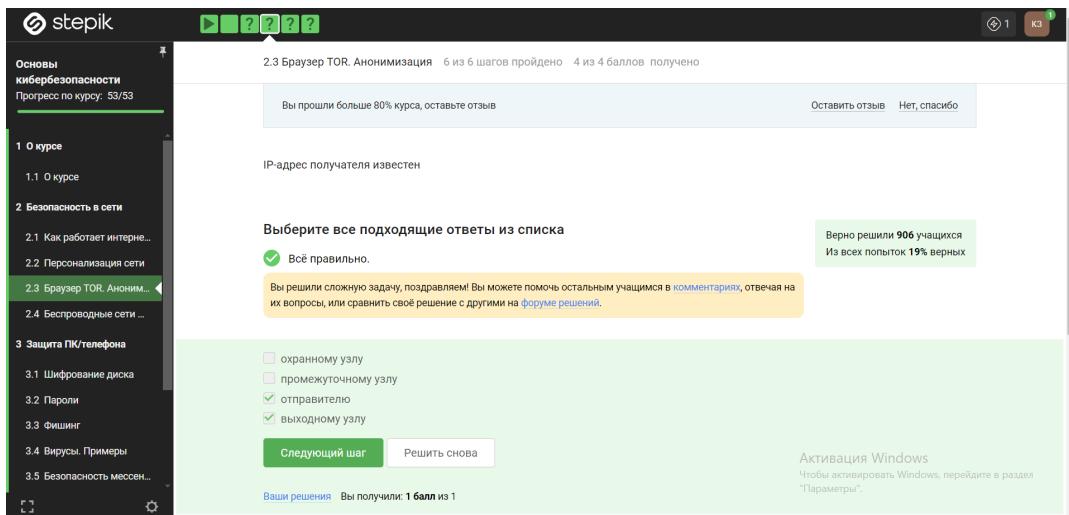


Рис. 2.14: отправителю и выходному узлу

2.3.3 Отправитель генерирует общий секретный ключ - с охранным, промежуточным и выходном узлом.

Когда отправитель генерирует общий секретный ключ для связи с другим узлом (охранной, промежуточной или выходной точкой), он использует различные криптографические методы для создания этого ключа. Общий секретный ключ позволяет обеспечить конфиденциальность и целостность передаваемых данных между узлами. После генерации общего секретного ключа отправитель и получатель могут использовать его для шифрования и расшифрования данных, а также для проверки целостности сообщений. Это позволяет им обмениваться информацией безопасным образом, чтобы трети лица не могли перехватить или изменить передаваемые данные.

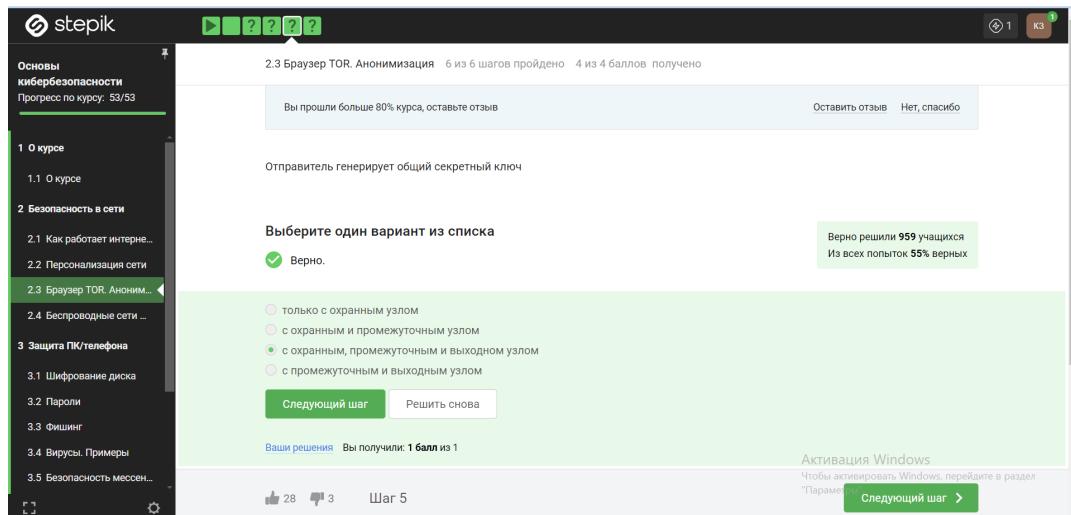


Рис. 2.15: с охранным, промежуточным и выходном узлом

2.3.4 Должен ли получатель использовать браузер Tor для успешного получения пакетов – нет.

Получатель не обязан использовать браузер Tor или другой браузер, основанный на луковой маршрутизации, для успешного получения пакетов с общим секретным ключом от отправителя. Луковая маршрутизация, такая как та, что используется в сети Tor, предназначена для обеспечения анонимности и защиты конфиденциальности пользователей в интернете путем маршрутизации их трафика через несколько узлов.

The screenshot shows a Stepik course interface for a cybersecurity basics course. The sidebar lists chapters 1 through 5. Chapter 2, 'Безопасность в сети' (Network Security), is currently selected. Chapter 2.3, 'Браузер TOR. Анонимизация' (Tor Browser. Anonymization), is the active section. A progress bar indicates 6 steps completed out of 8, with 4 points earned. The main content area displays a question: 'Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?' (Should the recipient use the Tor browser (or another browser based on onion routing) to successfully receive packages?). Below the question, a list of options is shown: 'Нет' (No) and 'Да' (Yes). The 'Нет' option is selected. Buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again) are at the bottom. A green feedback box says 'Верно решили 961 учащийся' (961 students solved correctly) and 'Из всех попыток 74% верных' (74% of attempts were correct). Below the main content, there's a sidebar for 'Активизация Windows' (Windows Activation) with a link to 'Следующий шаг'.

Рис. 2.16: нет

2.4 2.4 Беспроводные сети Wi-Fi

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

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11. IEEE – это организация, которая описывает вообще любые стандарты того, как работает интернет.

The screenshot shows a Stepik course interface for a cybersecurity basics course. The sidebar lists chapters 1 through 5. Chapter 2, 'Безопасность в сети' (Network Security), is currently selected. Chapter 2.4, 'Беспроводные сети ...' (Wireless networks ...), is the active section. A progress bar indicates 8 steps completed out of 8, with 5 points earned. The main content area displays a question: 'Wi-Fi - это' (What is WiFi?). Below the question, a list of options is shown: 'сокращение от "wireless fiber"', 'технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11', 'метод соединения компьютеров по проводной сети Ethernet', and 'метод подключения смартфона с глобальной сетью Интернет'. The second option is selected. Buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again) are at the bottom. A green feedback box says 'Верно решили 965 учащихся' (965 students solved correctly) and 'Из всех попыток 79% верных' (79% of attempts were correct). Below the main content, there's a sidebar for 'Активизация Windows' (Windows Activation) with a link to 'Следующий шаг'.

Рис. 2.17: IEEE 802.11

2.4.2 Уровень работы протокола WiFi – канальный.

WiFi работает на самом нижнем канальном уровне, на том же уровне, где работает протокол Ethernet (это протокол, обеспечивающий продвижение данных по проводу). И в этом нет ничего удивительного, поскольку по своей сути технология WiFi очень похожа на технологию Ethernet, только передает данные не по кабелю, а по радиосигналу.

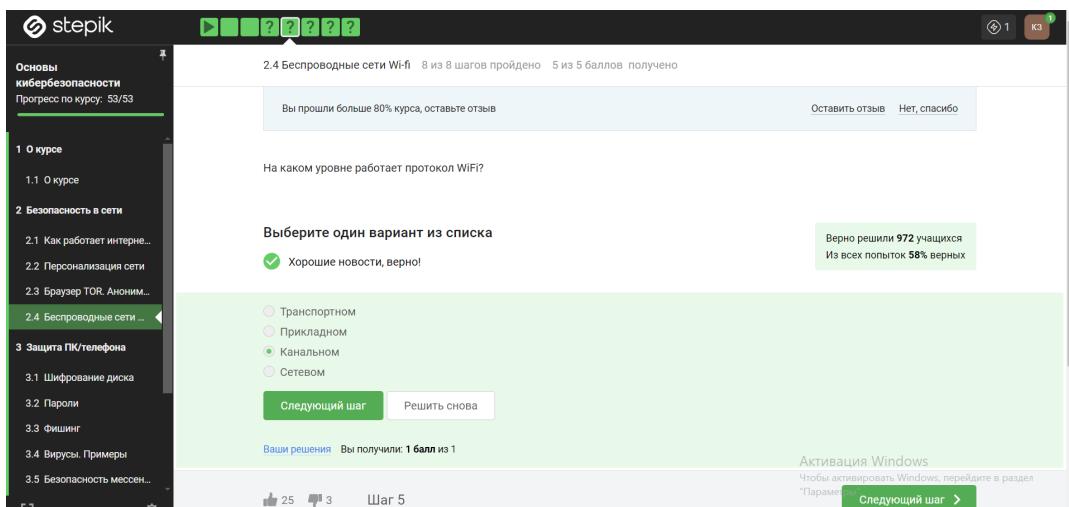


Рис. 2.18: канальный

2.4.3 Небезопасный метод обеспечения шифрования и аутентификации в сети WiFi – WEP.

Самый ранний и на сегодняшний день небезопасный метод шифрования данных WiFi называется WEP. Он устарел и уже категорически не рекомендуется к использованию. Он устарел, в частности, потому, что использовал малую длину ключа: так, например, он использовал длину ключа в 40 бит, это довольно мало на сегодняшний день, он может быть легко взломан.

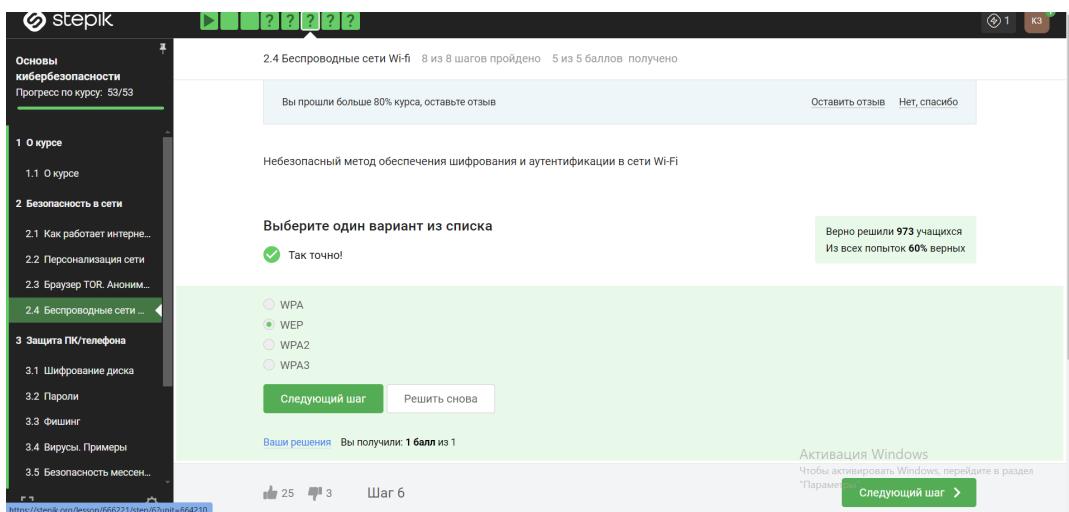


Рис. 2.19: WEP

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

Для обеспечения безопасности и конфиденциальности данных, передаваемых между хостом и роутером, обычно используются различные методы шифрования и аутентификации. Например, когда устройство подключается к защищенной беспроводной сети Wi-Fi, происходит процесс аутентификации, где устройство подтверждает свою легитимность перед роутером. После успешной аутентификации устанавливается защищенное соединение с помощью протокола шифрования, такого как WPA2 (Wi-Fi Protected Access 2), который обеспечивает шифрование данных, передаваемых между устройством и роутером.

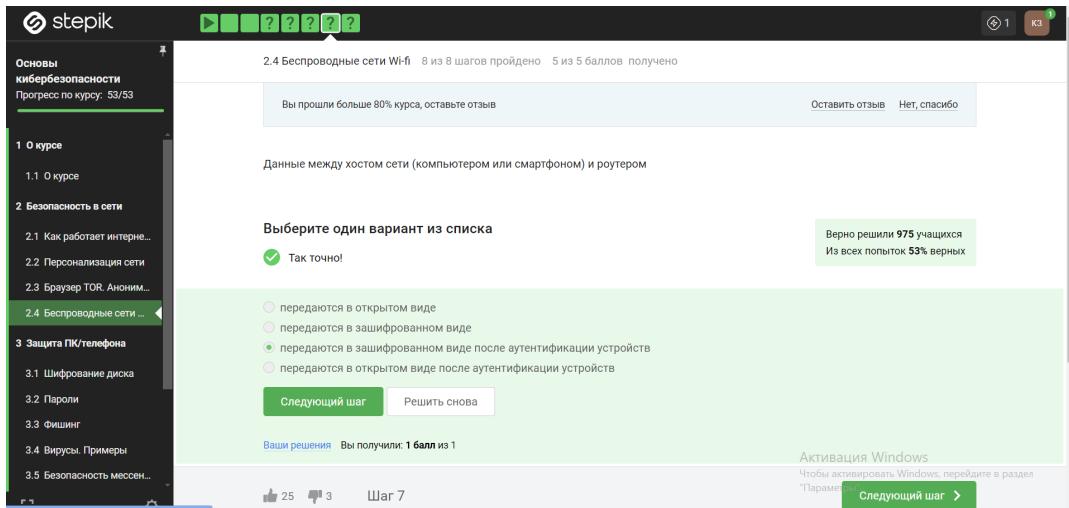


Рис. 2.20: передаются в зашифрованном виде после аутентификации устройств

2.4.5 Для домашней сети для аутентификации обычно используется метод - WPA2 Personal.

WPA2 Personal является одним из наиболее распространенных методов шифрования и аутентификации для защиты беспроводных сетей. Когда вы настраиваете свою домашнюю Wi-Fi сеть, вы обычно устанавливаете пароль (проходную фразу) для доступа к сети. Этот пароль используется для аутентификации устройств, которые пытаются подключиться к вашей сети. Когда устройство пытается подключиться к вашей защищенной сети Wi-Fi, оно должно предоставить правильный пароль для аутентификации через протокол WPA2 Personal.

The screenshot shows a Stepik course interface. On the left, a sidebar lists course modules: 1 О курсе, 1.1 О курсе, 2 Безопасность в сети, 2.1 Как работает интернет..., 2.2 Персонализация сети, 2.3 Браузер TOR. Аноним..., 2.4 Беспроводные сети ..., 3 Защита ПК/телефона, 3.1 Шифрование диска, 3.2 Пароли, 3.3 Фишинг, 3.4 Вирусы. Примеры, and 3.5 Безопасность мессен.... The main content area displays a step titled "2.4 Беспроводные сети Wi-Fi" which has been completed ("8 из 8 шагов пройдено"). A message encourages users to leave a review ("Вы прошли больше 80% курса, оставьте отзыв"). Below this, a question asks to choose one option from a list: "WPA2 Personal" (selected) and "WPA2 Enterprise". A green button labeled "Следующий шаг" is visible. To the right, a box shows statistics: "Верно решили 975 учащихся" and "Из всех попыток 87% верных". At the bottom, there are like/dislike counts (25 likes, 3 dislikes), a "Шаг 8" button, and a "Комментарии" section.

Рис. 2.21: WPA2 Personal

3 3. Защита ПК/телефона

3.1 3.1 Шифрование диска

3.1.1 Можно ли зашифровать загрузочный сектор диска – да.

Можно шифровать и загрузочный сектор диска.

The screenshot shows a user interface from the Stepik platform. On the left, there's a sidebar with a navigation tree for a course titled 'Основы кибербезопасности'. The tree includes sections like '1 О курсе', '2 Безопасность в сети', and '3 Защита ПК/телефона', with '3.1 Шифрование диска' currently selected. The main area displays a completed step: '3.1 Шифрование диска' (5 из 5 шагов пройдено) with 3 из 3 баллов получено. Below this, a question is asked: 'Можно ли зашифровать загрузочный сектор диска'. A feedback message says 'Хорошая работа.' and indicates that 949 users answered correctly. At the bottom, there are buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). The overall theme is cybersecurity, specifically disk encryption.

Рис. 3.1: да

3.1.2 Шифрование диска основано на - симметричном шифровании.

Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования, как правило, алгоритма AES.

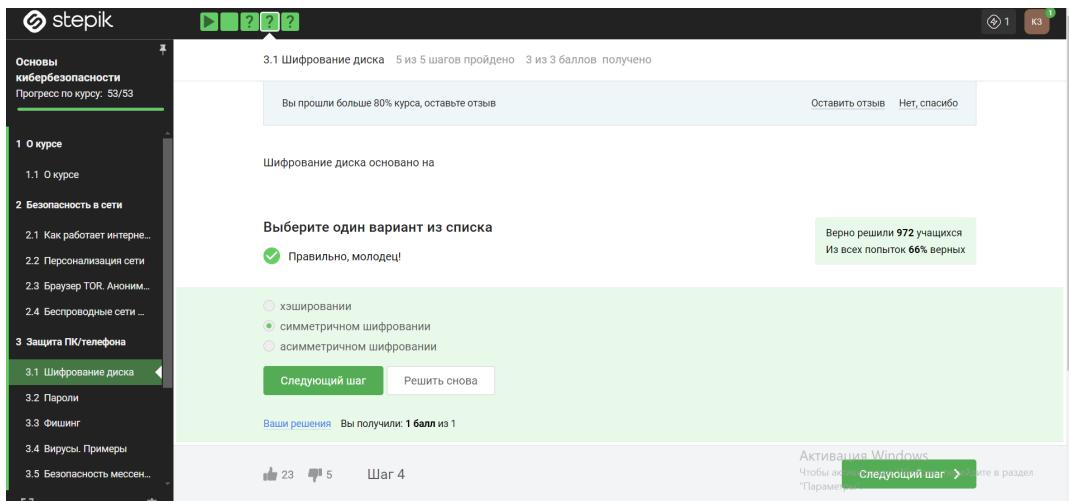


Рис. 3.2: симметричном шифровании

3.1.3 С помощью каких программ можно зашифровать жесткий диск

- VeraCrypt, BitLocker.

Во всех популярных операционных системах есть встроенные утилиты, которые позволяют шифровать жесткий диск: для Windows это Bitlocker, в Linux – LUKS, в MacOS – это FileVault. Кроме того, есть и сторонние опенсорсные (open source) программы, то есть бесплатные: это Veracrypt, PGPDisk, которые вы можете установить себе и использовать их для шифрования ваших жестких дисков, загрузочных секторов или флешек.

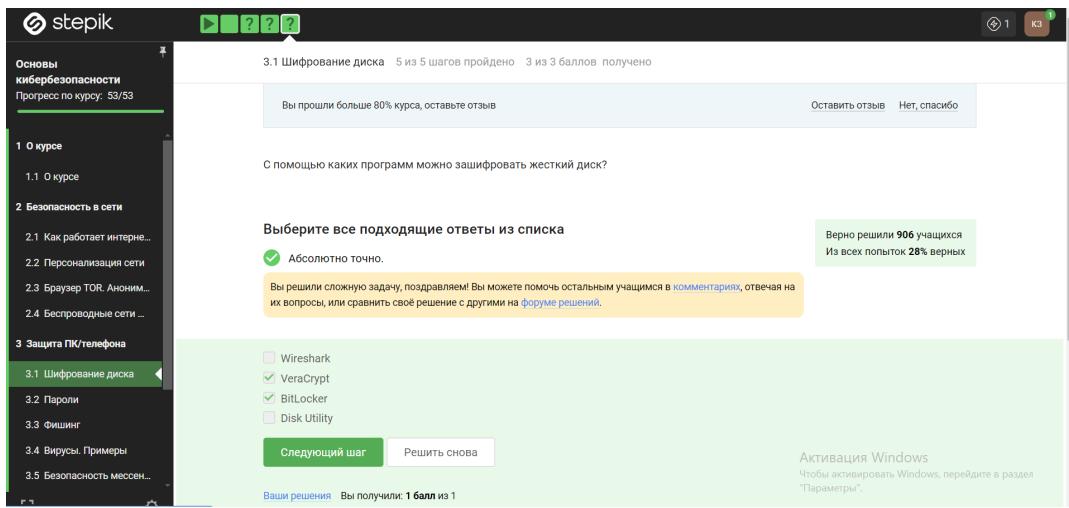


Рис. 3.3: VeraCrypt, BitLocker

3.2 3.2 Пароли

3.2.1 Какие пароли можно отнести с стойким - UQr9@j4!S\$.

Наши пароли - это банальный перебор всевозможных паролей, если мы знаем, что, например, пароль состоит из цифр и букв алфавита и каких-то еще символов, мы знаем в принципе весь алфавит, мощность этого алфавита, если мы еще, допустим, знаем длину пароля, то мы можем точно посчитать, каков размер множества всех паролей.

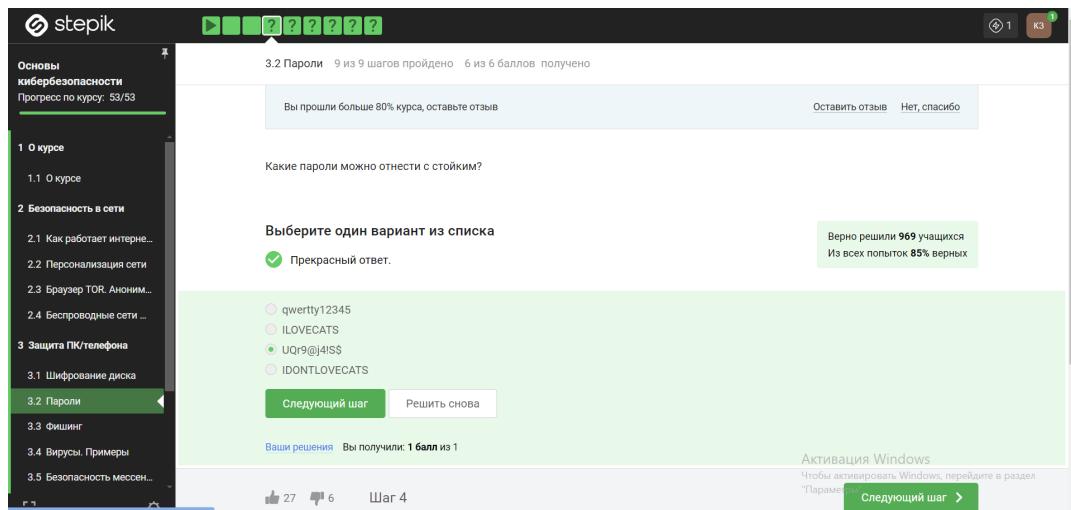


Рис. 3.4: UQR9@j4!SS

3.2.2 Где безопасно хранить пароли - в менеджерах паролей.

Нужно использовать длинные пароли с максимально большим алфавитом, хранить их стоит в менеджерах паролей, пароли нужно менять достаточно регулярно, особенно к таким критическим сервисам, как почта.

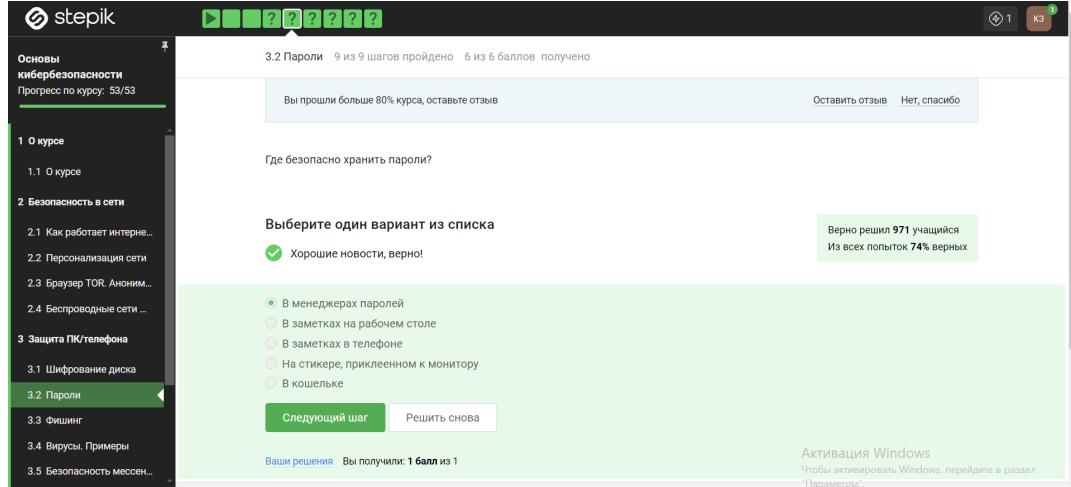


Рис. 3.5: в менеджерах паролей

3.2.3 Зачем нужна капча - для защиты от автоматизированных атак, направленных на получение несанкционированного доступа.

Капча — это аббревиатура с английского; это тест для определения, является ли пользователь, который общается с веб-сервисом, человеком или компьютером, ботом, который пытается просто-напросто перебрать все пароли. В сети часто используется такая защита, как капча.

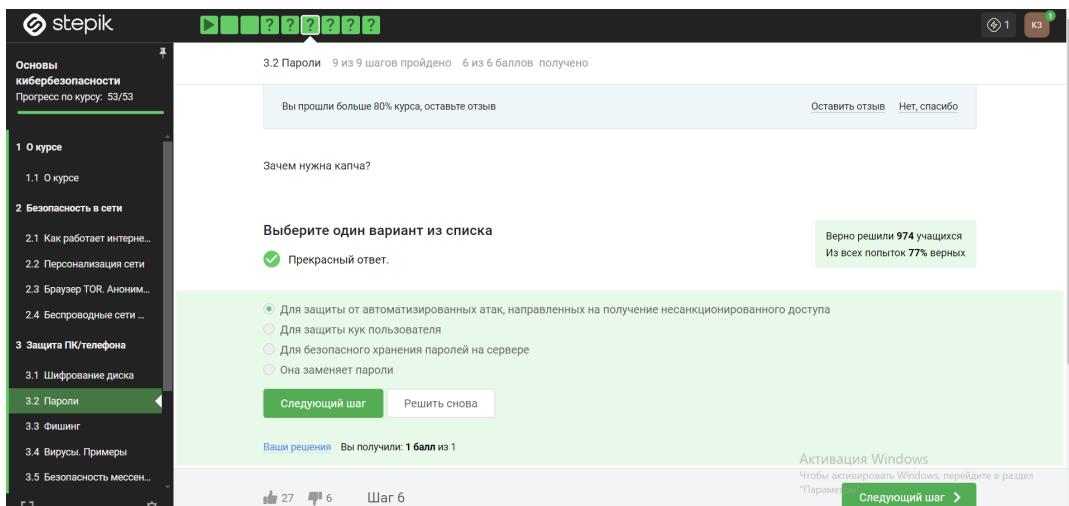


Рис. 3.6: для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

3.2.4 Для чего применяется хэширование паролей - для того, чтобы не хранить пароли на сервере в открытом виде.

Хэширование паролей - это процесс преобразования введенного пользователем пароля в некоторую строку фиксированной длины (хэш), которая затем сохраняется на сервере. Главная цель хэширования паролей - это обеспечение безопасности хранения пользовательских паролей.

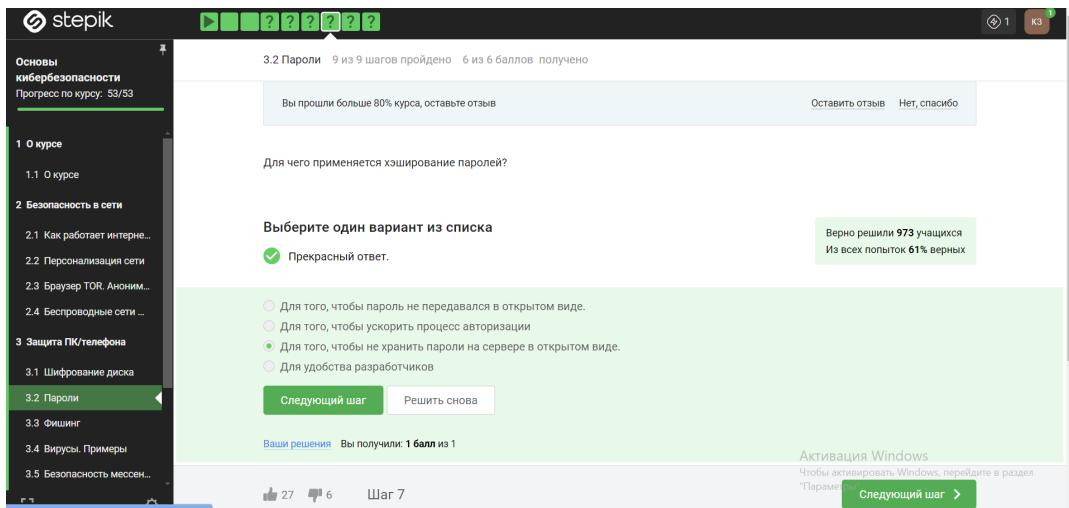


Рис. 3.7: для того, чтобы не хранить пароли на сервере в открытом виде

3.2.5 Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу – нет.

Соль используется для того, чтобы увеличить стойкость пароля для пользователей, которые сами не догадались о стойкости своих паролей.

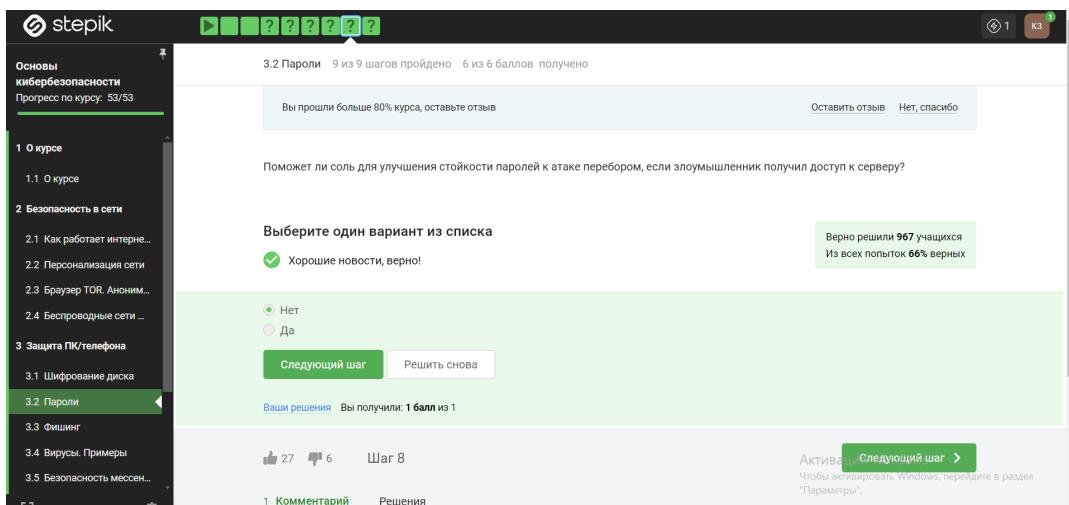


Рис. 3.8: нет

3.2.6 Какие меры защищают от утечек данных атакой перебором – разные пароли на всех сайтах, капча, сложные пароли, периодическая смена паролей.

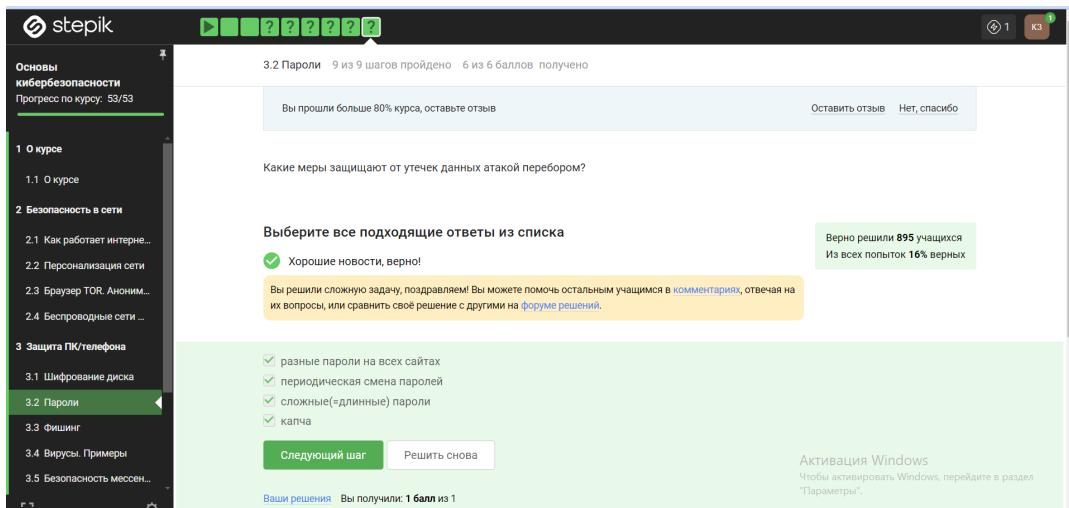
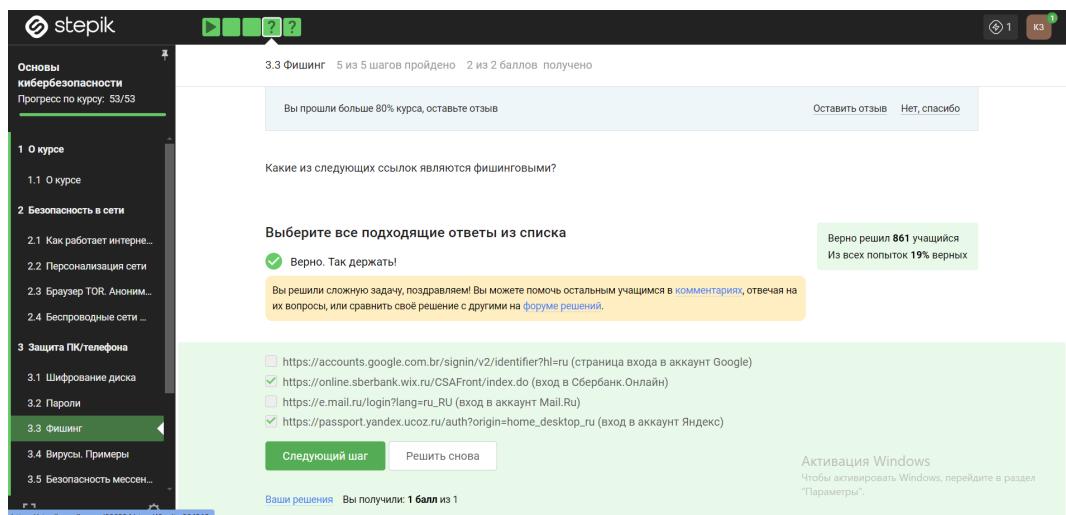


Рис. 3.9: разные пароли на всех сайтах, капча, сложные пароли, периодическая смена паролей

3.3 3.3 Фишинг

3.3.1 Какие из следующих ссылок являются фишинговыми – Сбербанк онлайн, аккаунт Яндекс.



The screenshot shows a Stepik course interface. On the left, a sidebar lists course modules: 1 О курсе, 2 Безопасность в сети, 3 Защита ПК/телефона, and 3.3 Фишинг (which is highlighted). The main content area displays a question titled "Какие из следующих ссылок являются фишинговыми?". Below the question, a box says "Выберите все подходящие ответы из списка". It contains four options, with the second one checked: "✓ Верно. Так держать!". A yellow box below the list says "Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), отвечая на их вопросы, или сравнить свое решение с другими на [форуме решений](#)". At the bottom, a green box shows statistics: "Верно решил 861 учащийся Из всех попыток 19% верных". Below the list, there are two buttons: "Следующий шаг" and "Решить снова".

Рис. 3.10: Сбербанк онлайн, аккаунт Яндекс

3.3.2 Может ли фишинговый имейл прийти от знакомого адреса – да.

Спуфинг – это глобальный термин атак, есть IP spoofing - это подмена IP-адреса, есть email spoofing - подмена адреса отправителя. Суть состоит в том, что мы получаем фишинговое письмо от якобы знакомого нам человека, а на самом деле отправлено оно было не им.

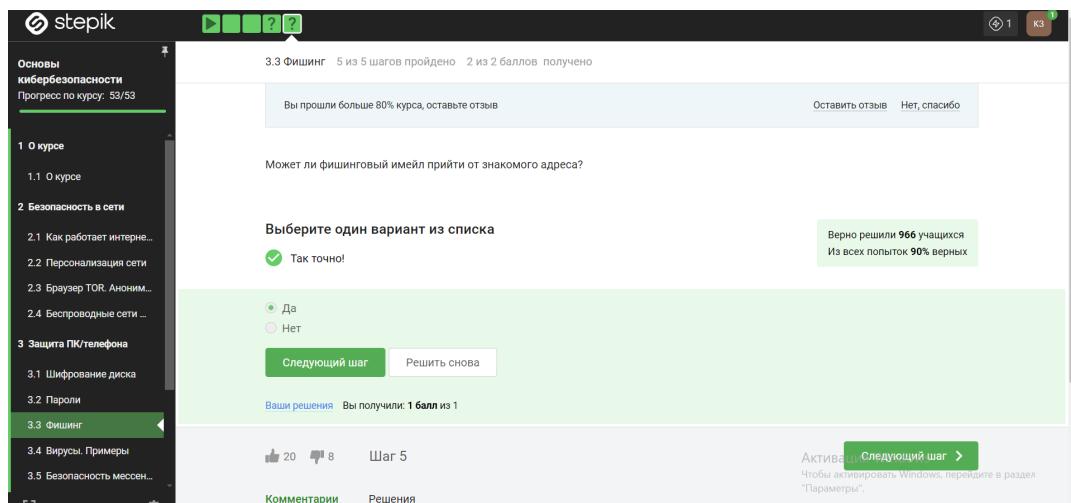


Рис. 3.11: да

3.4 Вирусы. Примеры

3.4.1 Email Спупинг – это подмена адреса отправителя в имейлах.

Спупинг – это глобальный термин атак, есть IP spoofing – это подмена IP-адреса, есть email spoofing – подмена адреса отправителя.

Рис. 3.12: это подмена адреса отправителя в имейлах

3.4.2 Вирус-тロян - маскируется под легитимную программу.

Троян - это вирус, который проникает в систему под видом какого-то легитимного программного обеспечения, это аллюзия к троянскому коню. Этот вирус также распространялся по почте с вполне себе невинным письмом с темой “Re: Details” (re от слова reply) или подобным ему. Само письмо содержало примечательный текст “See the attached file for details” («Просмотри вложение для подробной информации»).

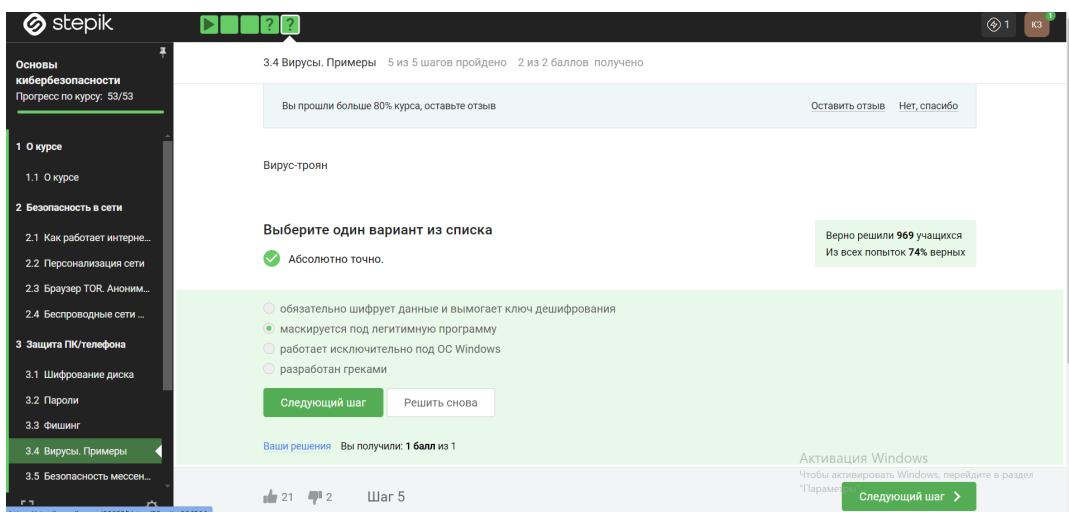


Рис. 3.13: маскируется под легитимную программу

3.5 3.5 Безопасность мессенджеров

3.5.1 На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal - при генерации первого сообщения стороной-отправителем.

Протокол мессенджера Signal использует протокол двойного ratchet для шифрования сообщений, который обеспечивает прямое и обратное шифрование сообщений между отправителем и получателем. Ключи шифрования формируются на различных этапах в процессе обмена сообщениями.

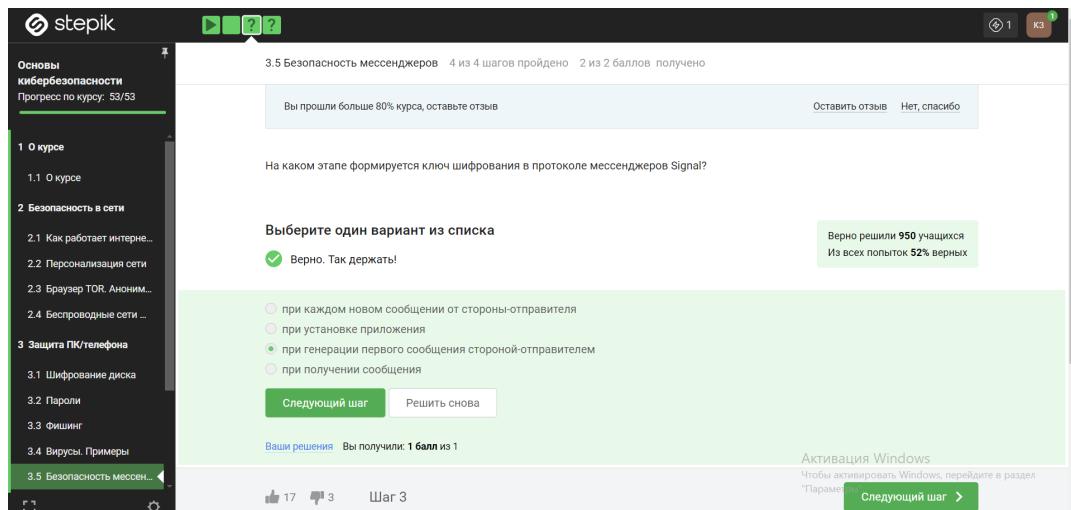


Рис. 3.14: при генерации первого сообщения стороной-отправителем

3.5.2 Суть сквозного шифрования состоит в том, что - сообщения передаются по узлам связи (серверам) в зашифрованном виде.

Сквозное шифрование - это парадигма большого числа безопасных коммуникаций; сквозное шифрование - по-английски E2E или End-to-End encryption.

Рис. 3.15: сообщения передаются по узлам связи (серверам) в зашифрованном виде

4 4. Криптография на практике

4.1 4.1 Введение в криптографию

4.1.1 В асимметричных криптографических примитивах - обе стороны имеют пару ключей.

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

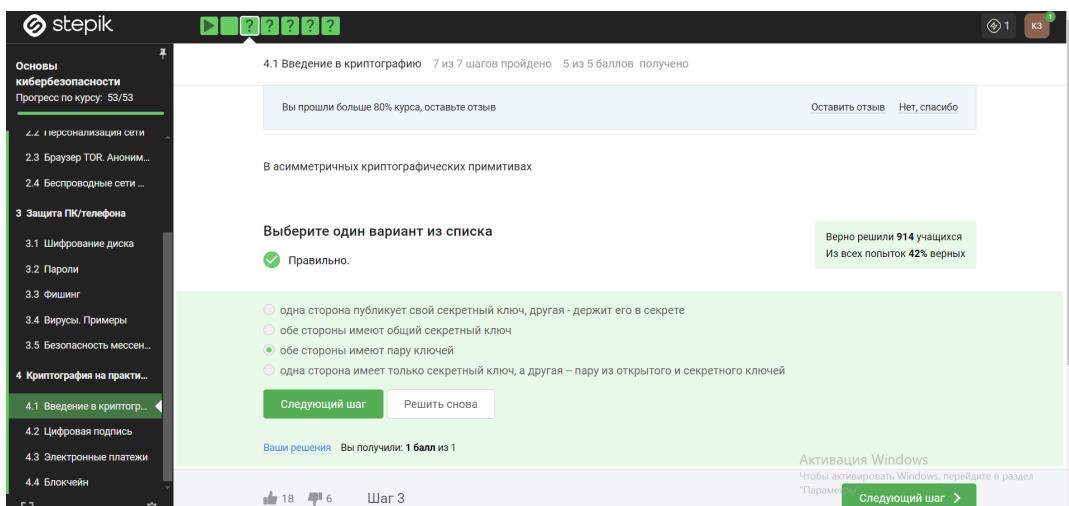


Рис. 4.1: обе стороны имеют пару ключей

4.1.2 Криптографическая хэш-функция - дает на выходе фиксированное число бит независимо от объема входных данных, эффективно вычисляется, стойкая к коллизиям.

Криптографическая хэш-функция - это функция, которая принимает входные данные любого размера и преобразует их в фиксированный набор битов, называемый хэшем. Она обладает свойствами такими как эффективность в вычислениях, необратимость (невозможность восстановления исходных данных из хэша), устойчивость к коллизиям (когда два разных входных значения дают одинаковый хэш) и многими другими. Криптографические хэш-функции широко используются в криптографических системах для обеспечения безопасности данных, а также в цифровой подписи, проверке целостности данных и хранения паролей.

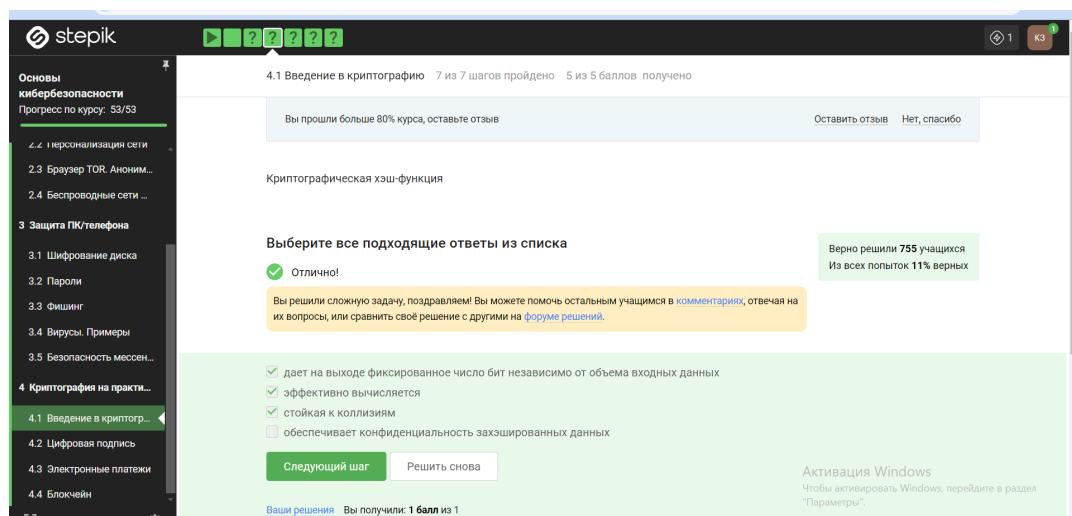


Рис. 4.2: дает на выходе фиксированное число бит независимо от объема входных данных, эффективно вычисляется, стойкая к коллизиям

4.1.3 К алгоритмам цифровой подписи относятся – RSA, ECDSA, ГОСТ

P 34.10-2012.

К примерам цифровой подписи относятся интернет-сертификаты, подпись RSA, американский стандарт ECDSA и отечественный стандарт ГОСТ стандарт Р 34.20.2012.

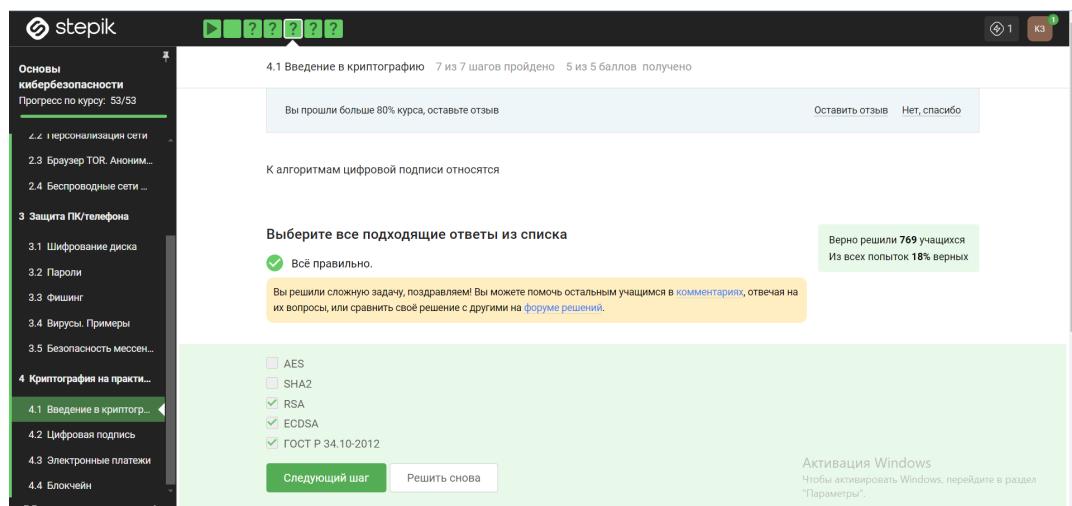


Рис. 4.3: RSA, ECDSA, ГОСТ Р 34.10-2012

4.1.4 Код аутентификации сообщения относится к - симметричным примитивам.

Как правило, код аутентификации сообщения строится с помощью хэш-функции или симметричного шифрования.

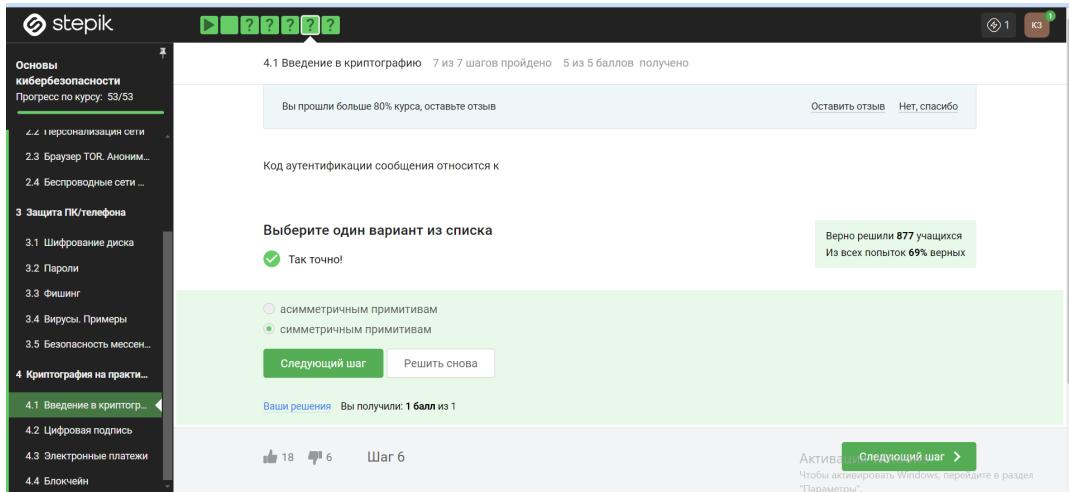


Рис. 4.4: симметричным примитивам

4.1.5 Обмен ключами Диффи-Хэллмана – это асимметричный примитив генерации общего секретного ключа.

Самым популярным примером протокола обмена ключами является протокол Диффи-Хэллмана, как раз он, либо его модификации используются в современных мессенджерах и в протоколе TLS для того, чтобы мы смогли сгенерировать общий секретный ключ и дальше шифровать наши данные с помощью симметричного алгоритма, то есть с помощью ключа skAB. Если реализовать генерацию общего ключа так, как она описана у Диффи-Хэллмана, мы получим довольно слабый протокол, нестойкий к активным злоумышленникам. Сделать этот протокол стойким к активным злоумышленникам помогает цифровая подпись.

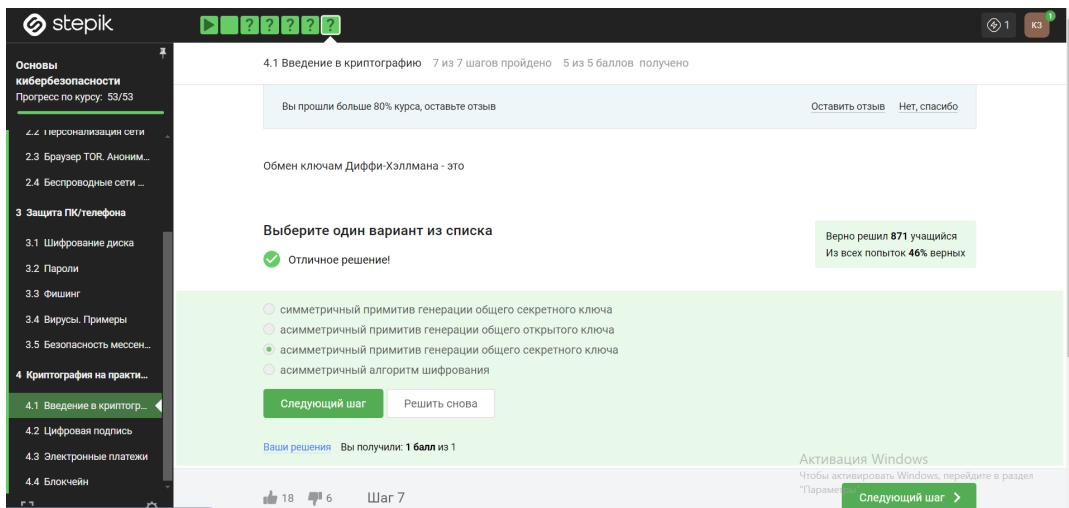


Рис. 4.5: это асимметричный примитив генерации общего секретного ключа

4.2 4.2. Цифровая подпись

4.2.1 Протокол электронной цифровой подписи относится к - протоколам с публичным (или открытым) ключом.

Протокол электронной цифровой подписи (ЭЦП) относится к протоколам с публичным ключом, также известным как открытым ключом, потому что он использует два ключа - приватный и публичный. Публичный ключ используется для проверки подписи, в то время как приватный ключ используется для создания подписи. При использовании ЭЦП отправитель использует свой приватный ключ для создания уникальной цифровой подписи, которая затем отправляется вместе с документом. Получатель может затем использовать публичный ключ отправителя для проверки подлинности подписи и целостности документа. Таким образом, протокол ЭЦП обеспечивает возможность проверки подлинности документов и их авторства в сети с публичным доступом к ключам.

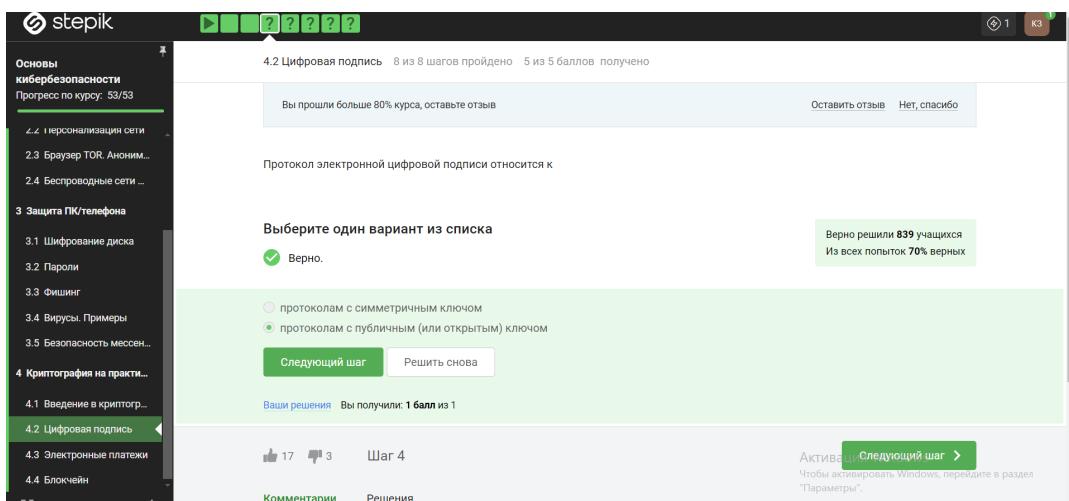


Рис. 4.6: протоколам с публичным (или открытым) ключом

4.2.2 Алгоритм верификации электронной цифровой подписи

требует на вход - подпись, открытый ключ, сообщение.

Если говорить более формально о том, что такое электронно-цифровая подпись, то это криптографический примитив, который состоит из трех эффективных алгоритмов. Эффективный алгоритм означает, что мы можем быстро его запустить на не сильно мощной машине. Первый алгоритм занимается генерацией ключей, он генерирует публичный ключ и секретный ключ. Публичный ключ мы держим в открытом доступе, секретный ключ – у себя, никому не показываем. Секретный ключ еще называется подписывающим ключом, а открытый – проверяющим или ключом верификации. 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.

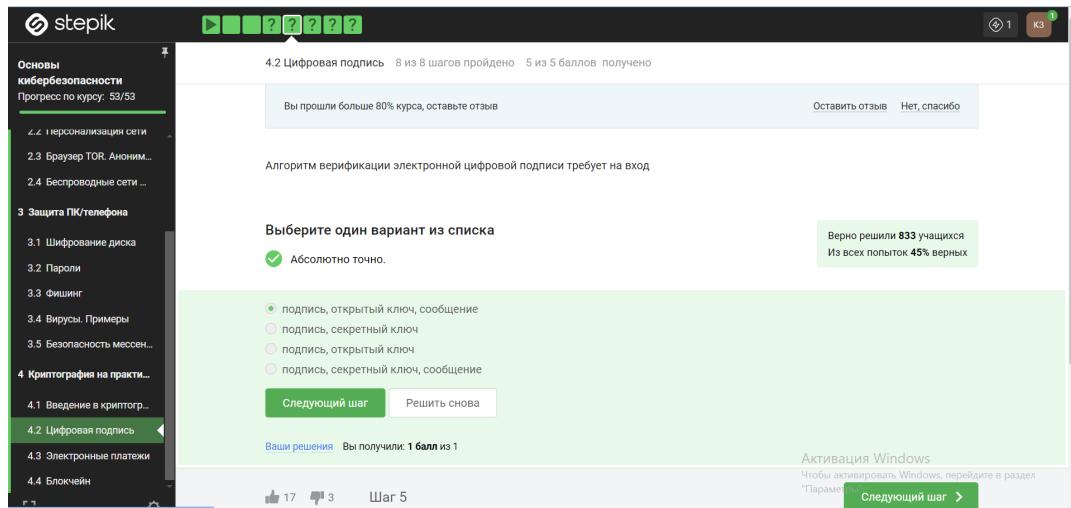


Рис. 4.7: подпись, открытый ключ, сообщение

4.2.3 Электронная цифровая подпись не обеспечивает – конфиденциальность.

Электронная цифровая подпись (ЭЦП) не обеспечивает конфиденциальность данных. Её основная цель – подтверждение подлинности и целостности данных, то есть их авторства и неприкосновенности. ЭЦП позволяет убедиться, что документ или сообщение были созданы конкретным отправителем и не были изменены после подписания. Для обеспечения конфиденциальности данных, таких как защита от несанкционированного доступа или прослушивания, обычно используются другие методы, такие как алгоритмы шифрования. Эти методы позволяют шифровать данные таким образом, что только авторизованные пользователи могут расшифровать их.

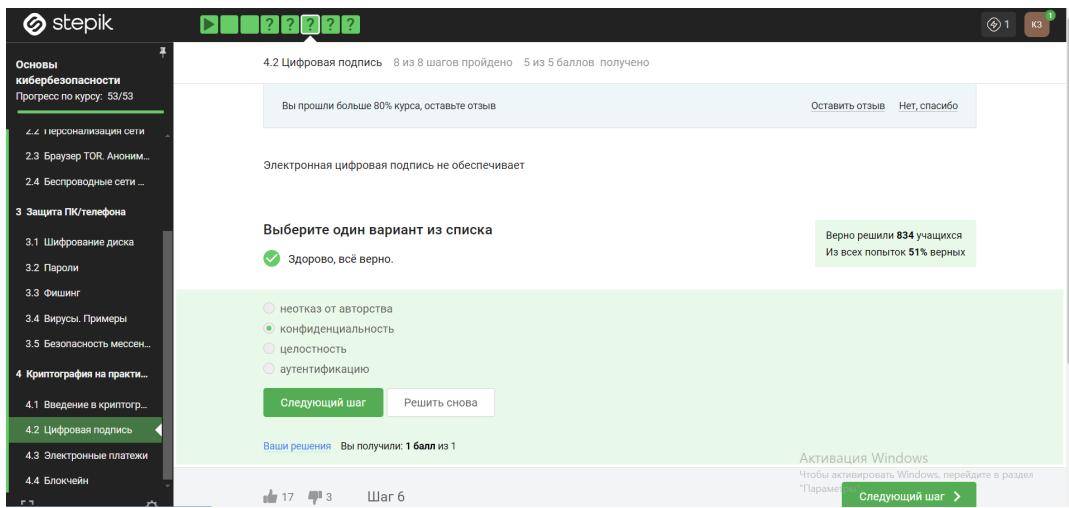


Рис. 4.8: конфиденциальность

4.2.4 Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС - усиленная квалифицированная.

Усиленная квалифицированная электронная подпись (УКЭП) – это специальный тип сертификата электронной подписи, который обладает увеличенным уровнем достоверности и законной силой. Этот тип ЭП используется для подписания важных и юридически значимых документов, таких как налоговая отчетность, передаваемая в Федеральную налоговую службу (ФНС). Чтобы получить усиленную квалифицированную электронную подпись, необходимо обратиться к аккредитованному удостоверяющему центру (УЦ), который проведет проверку личности подписчика и выдаст соответствующий сертификат. Такие сертификаты имеют особые требования к процедурам проверки личности и могут быть использованы для юридически значимых документов.

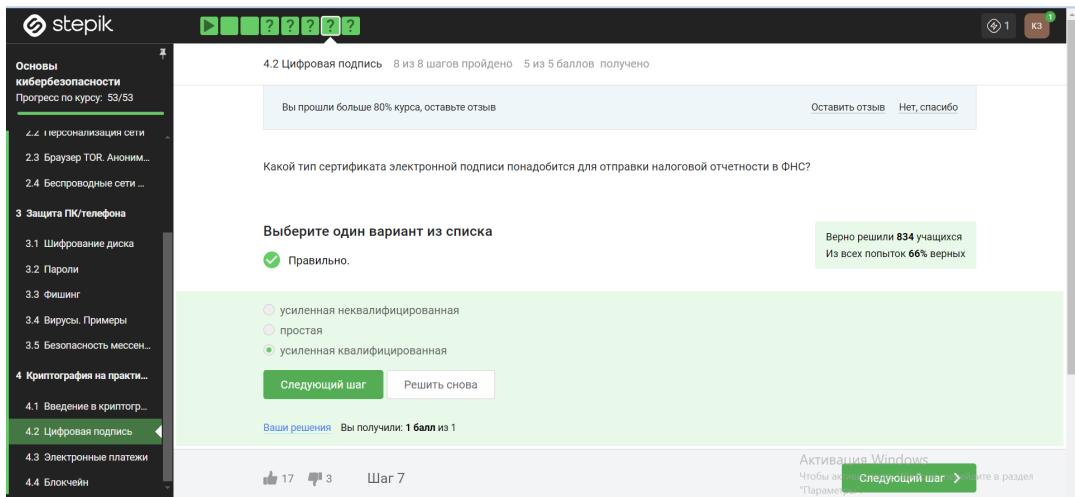


Рис. 4.9: усиленная квалифицированная

4.2.5 В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи - в удостоверяющем (сертификационном) центре.

Квалифицированный сертификат ключа проверки электронной подписи (КЭП) можно получить в удостоверяющем центре (УЦ), который является специализированной организацией, уполномоченной на выдачу сертификатов ключей электронных подписей. УЦ проводит процедуры проверки подлинности идентификационных данных заявителя, выпускает и распространяет сертификаты ключей электронных подписей, управляет их отзывом при необходимости, а также обеспечивает безопасность и надежность процесса выдачи и использования сертификатов. Получение квалифицированного сертификата ключа проверки электронной подписи на УЦ включает в себя предъявление документов, подтверждающих личность, прохождение процедур авторизации и подтверждения личности, и подписание необходимых соглашений. УЦ должен быть аккредитован уполномоченным государственным органом и соответствовать установленным законодательством требованиям по выдаче квалифицированных сертификатов ключей электронных подписей.

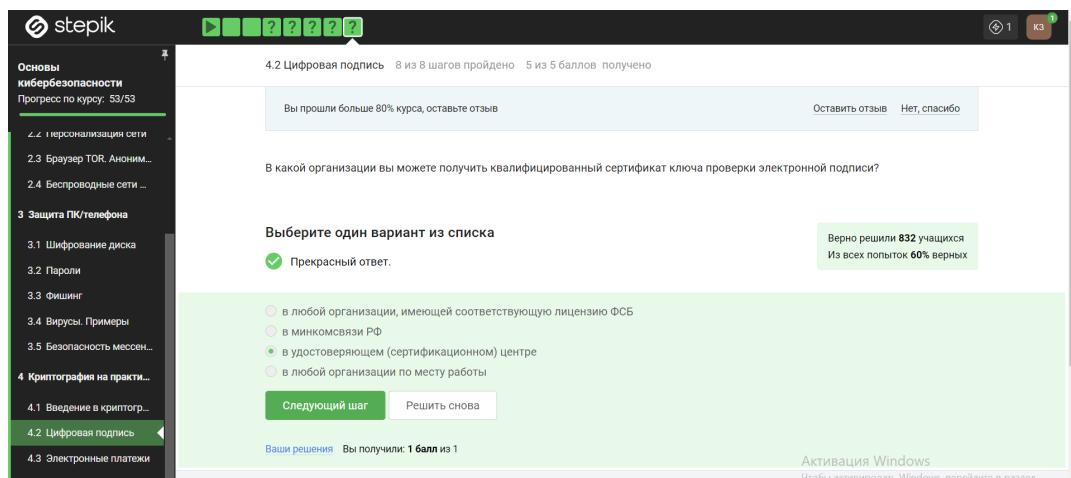


Рис. 4.10: в удостоверяющем (сертификационном) центре

4.3 Электронные платежи

4.3.1 Выберите из списка все платежные системы – MasterCard, МИР.

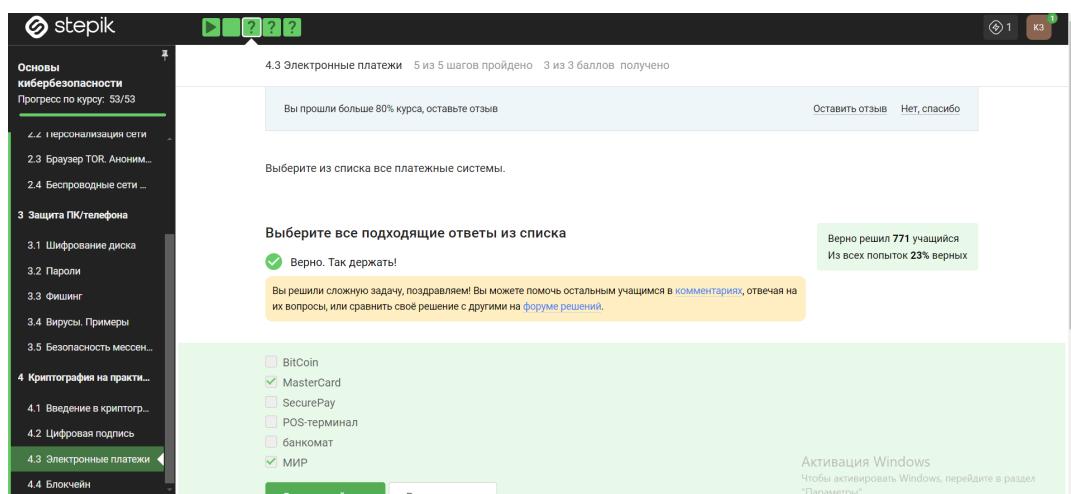


Рис. 4.11: MasterCard, МИР

4.3.2 Примером многофакторной аутентификации является - комбинация код в sms сообщении + отпечаток пальца, комбинация проверка пароля + код в sms сообщении.

Многофакторная аутентификация - это процесс подтверждения личности пользователя с использованием двух или более различных методов аутентификации. Примеры, которые вы привели, отлично иллюстрируют это: 1. Комбинация кода из SMS-сообщения и отпечатка пальца: В этом случае пользователю необходимо предоставить два разных типа подтверждения - что-то, что он знает (код из SMS) и что-то, что он имеет (отпечаток пальца). Это повышает безопасность, так как злоумышленнику будет сложнее обойти оба уровня защиты. 2. Проверка пароля и кода из SMS-сообщения: Здесь также сочетаются два различных метода - что-то, что пользователь знает (пароль) и что-то, что он получает на внешнем устройстве (код из SMS). Это создает двойную проверку личности и уменьшает риск несанкционированного доступа.

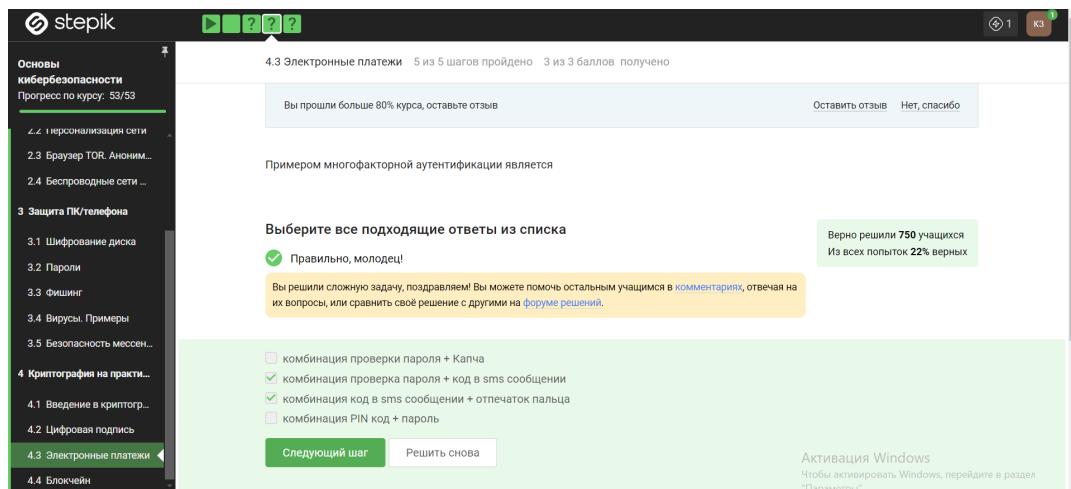


Рис. 4.12: комбинация код в sms сообщении + отпечаток пальца, комбинация проверка пароля + код в sms сообщении

4.3.3 При онлайн платежах сегодня используется - многофакторная аутентификация покупателя перед банком-эмитентом.

В сфере онлайн платежей сегодня все более широко внедряется многофакторная аутентификация покупателя перед банком-эмитентом. Это означает, что при совершении онлайн транзакций покупателю требуется предоставить несколько различных методов аутентификации для подтверждения своей личности перед банком, который выпускает его платежную карту. Например, при совершении онлайн платежа покупателю может потребоваться ввести свой пароль или PIN-код (что-то, что он знает), а затем получить одноразовый код подтверждения на свой мобильный телефон (что-то, что он имеет). Такая комбинация факторов делает процесс аутентификации более надежным и защищает от мошенничества, поскольку злоумышленнику будет гораздо сложнее обойти оба уровня защиты. Многофакторная аутентификация позволяет банкам повысить безопасность онлайн платежей, защитить клиентов от несанкционированных транзакций и уменьшить риски финансовых мошенничеств.

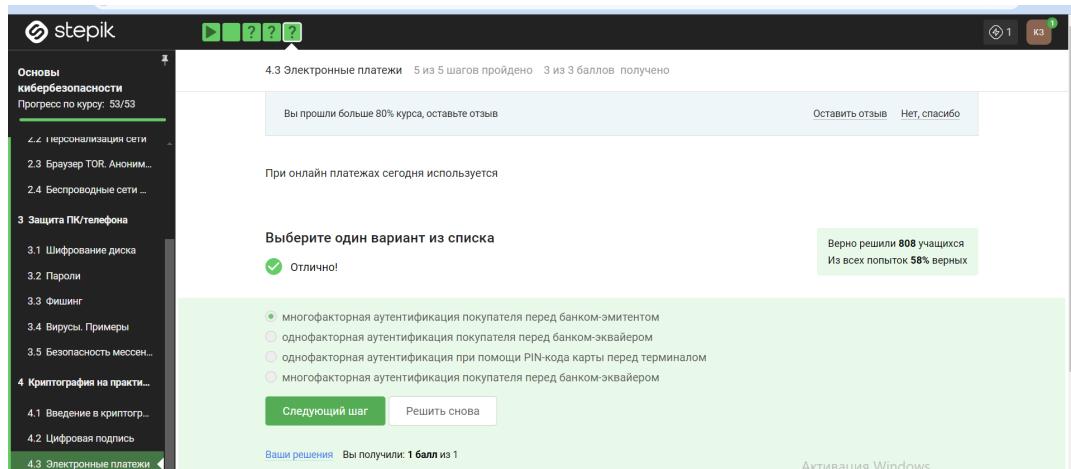


Рис. 4.13: многофакторная аутентификация покупателя перед банком-эмитентом

4.4 4.4 Блокчейн

4.4.1 Какое свойство криптографической хэш-функции используется в доказательстве работы - сложность нахождения прообраза.

Криптографическая хэш-функция обладает свойством сложности нахождения прообраза, что означает, что для заданного значения хэш-суммы сложно найти исходное сообщение, которое бы привело к данной хэш-сумме. Это свойство является важным для обеспечения безопасности данных и целостности информации. При использовании криптографической хэш-функции, например, при хэшировании паролей или цифровой подписи, важно, чтобы невозможно было найти исходное сообщение, зная только его хэш-сумму. То есть, даже при наличии хэш-суммы злоумышленнику будет крайне сложно или практически невозможно восстановить исходное сообщение. Это свойство обеспечивает уровень безопасности, так как даже при доступе к хэш-сумме злоумышленнику будет трудно восстановить исходное сообщение без знания алгоритма хэширования и без изначальных данных. Таким образом, сложность нахождения прообраза является важным криптографическим свойством, обеспечивающим надежность и безопасность при работе с хэш-функциями.

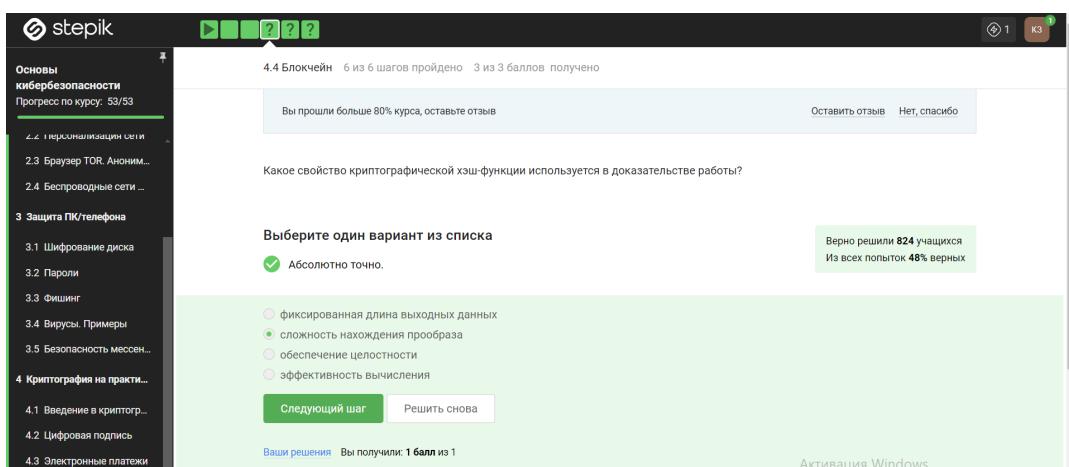


Рис. 4.14: сложность нахождения прообраза

4.4.2 Консенсус в некоторых системах блокчейн обладает свойствами – постоянства, открытость, живучесть, консенсус.

В основе любого блокчейна, в частности биткоина, лежит консенсус – соглашение, в терминах криптовалют консенсус - это некая публичная структура данных или ledger (переводится с английского как «бухгалтерская книга»), где просто содержится история всех переводов, хранится список того, кто что кому заплатил, в какое время. Почему консенсус? Потому что эта публичная структура, и бухгалтерский учет должен обеспечивать четыре основных свойства. Первое – это постоянство, то есть когда-либо добавленные данные не должны быть удалены из этой структуры. Второе – это сам консенсус, то есть все участники видят одни и те же данные и соглашаются с одним и теми же данными, исключением могут быть последние пары блоков, то есть последние изменения в этом блокчейне, в этой публичной структуре данных. Третье – это живучесть, это означает, что мы можем добавлять новые транзакции, когда хотим, мы можем осуществлять платежи, когда хотим. И последнее четвертое свойство – это открытость, то есть любой человек может быть участником блокчейна. Это справедливо не для всех блокчейнов, для биткоина это справедливо.

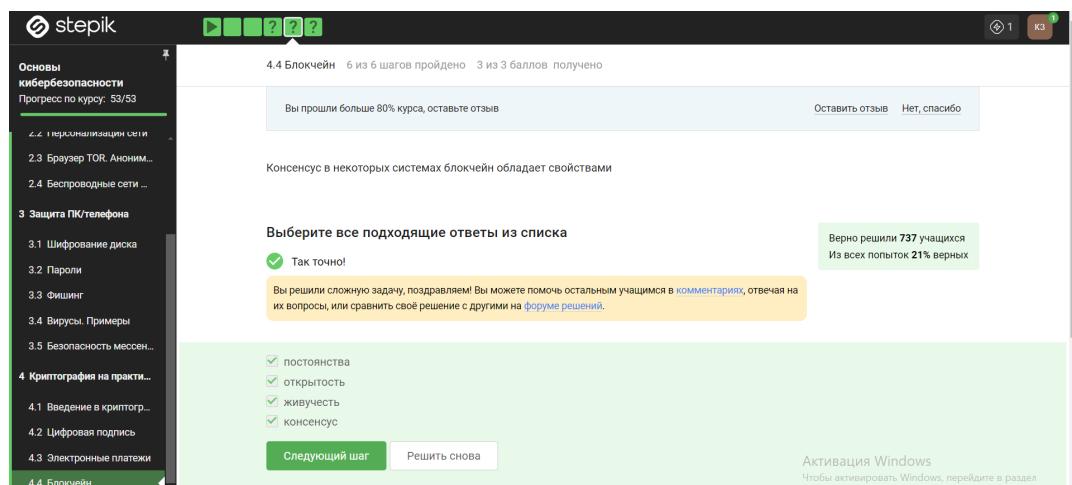


Рис. 4.15: постоянства, открытость, живучесть, консенсус

4.4.3 Секретные ключи какого криптографического примитива хранят участники блокчейна - цифровая подпись.

Участники блокчейна хранят секретные ключи для цифровой подписи. Цифровая подпись – это криптографический примитив, который позволяет участнику блокчейна подтверждать свою личность и подписывать транзакции с использованием своего секретного ключа. При создании цифровой подписи участник использует свой закрытый ключ для шифрования информации о транзакции, и другие участники могут проверить подлинность подписи, используя открытый ключ этого участника. Таким образом, секретный ключ для цифровой подписи является важным элементом для обеспечения безопасности и целостности данных в блокчейне. Хранение секретных ключей в блокчейне обеспечивает аутентификацию участников, защиту от подделки и обеспечивает безопасность транзакций. Поэтому секретные ключи для цифровой подписи являются важным криптографическим компонентом в системе блокчейн.

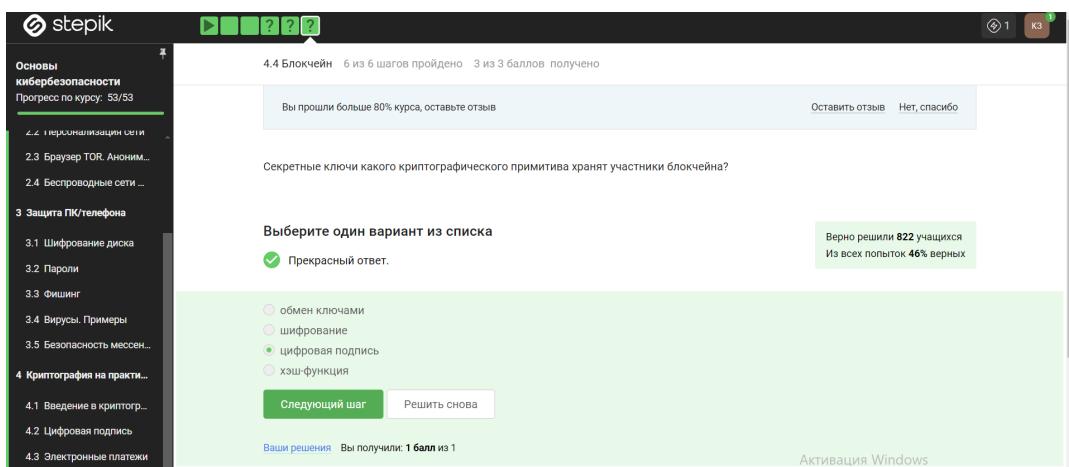


Рис. 4.16: цифровая подпись

4.4.4 Полученный сертификат:

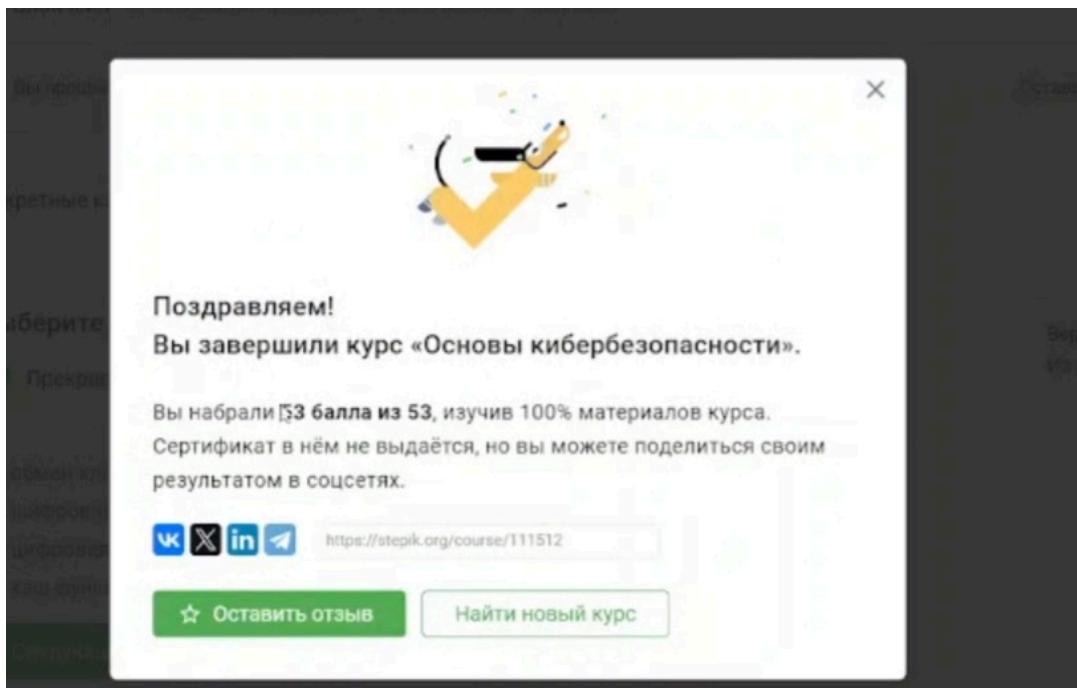


Рис. 4.17: Сертификат

Список литературы

1. Таненбаум Э., Бос Х. Современные операционные системы. 4-е изд. СПб.: Питер, 2015. 1120 с.