

Внешний курс

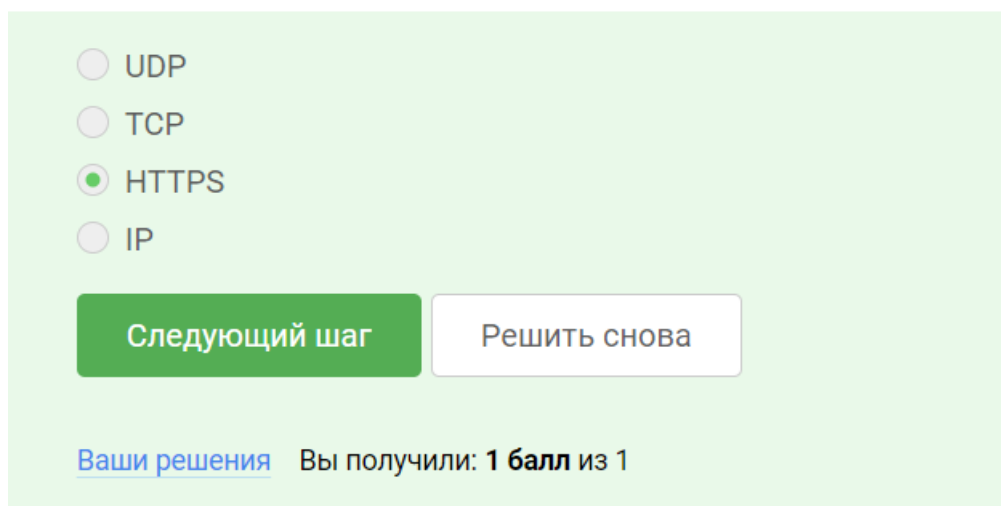
Основы Кибербезопасности

Чулкова Валерия Алексеевна

Группа: НБИбд-02-22

2.1

№1

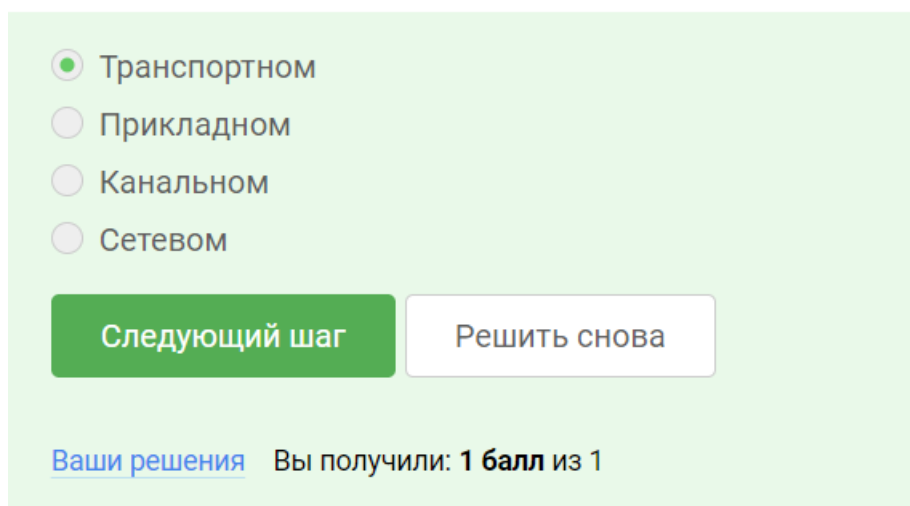


A screenshot of a quiz interface with a light green background. It features four radio button options: UDP, TCP, HTTPS (which is selected), and IP. Below the options are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score display 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.1: .

HTTP (Hypertext Transfer Protocol) — это протокол передачи гипертекстовых данных, который используется для передачи веб-страниц, файлов, медиаданных и других ресурсов через Интернет. Протокол HTTP передает данные в открытом, незашифрованном виде между клиентом (обычно веб-браузером) и сервером.

№2



A screenshot of a quiz interface with a light green background. It features four radio button options: Транспортном (Transport) (which is selected), Прикладном (Application), Канальном (Data Link), and Сетевом (Network). Below the options are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score display 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.2: .

TCP (Transmission Control Protocol) работает на транспортном уровне модели взаимодействия открытых систем (OSI). Транспортный уровень является четвертым уровнем в семиуровневой модели OSI.

Основные задачи и функции TCP на транспортном уровне:

1. Установление и поддержание соединения между двумя конечными узлами (хостами) для обмена данными.
2. Разбиение данных от вышележащих уровней (например, прикладного уровня) на

небольшие сегменты для передачи.

3. Обеспечение надежной доставки сегментов данных в правильном порядке, с проверкой целостности данных и механизмами повторной передачи в случае потери или повреждения данных.

4. Управление потоком данных, чтобы избежать перегрузки получателя.

№3

A screenshot of a quiz interface with a light green background. It lists four IP addresses, each with a checkbox to its left: 421.0.15.19, 43.12.256.7, 90.11.90.22, and 25.198.0.15. The checkboxes for 90.11.90.22 and 25.198.0.15 are checked and marked with green checkmarks. Below the list are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, it says 'Ваши решения' (Your solutions) and 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.3: .

Адрес IPv4 состоит из 32 бит, разделенных на четыре октета (по 8 бит в каждом). Каждый октет представляется десятичным числом от 0 до 255.

№4

A screenshot of a quiz interface with a light green background. It lists four functions of DNS, each with a radio button to its left: 'сопоставляет IP адреса доменным именам' (maps IP addresses to domain names), 'сегментирует данные на транспортном уровне' (segments data at the transport level), 'выбирает маршрут пакета в сети' (chooses the packet route in the network), and 'выполняет адресацию на хосте' (performs addressing on the host). The first option is selected with a green dot. Below the list are two buttons: a green 'Следующий шаг' (Next step) button and a white 'Решить снова' (Solve again) button. At the bottom, it says 'Ваши решения' (Your solutions) and 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

☒ сопоставляет IP адреса доменным именам

☐ сегментирует данные на транспортном уровне

☐ выбирает маршрут пакета в сети

☐ выполняет адресацию на хосте

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.4: .

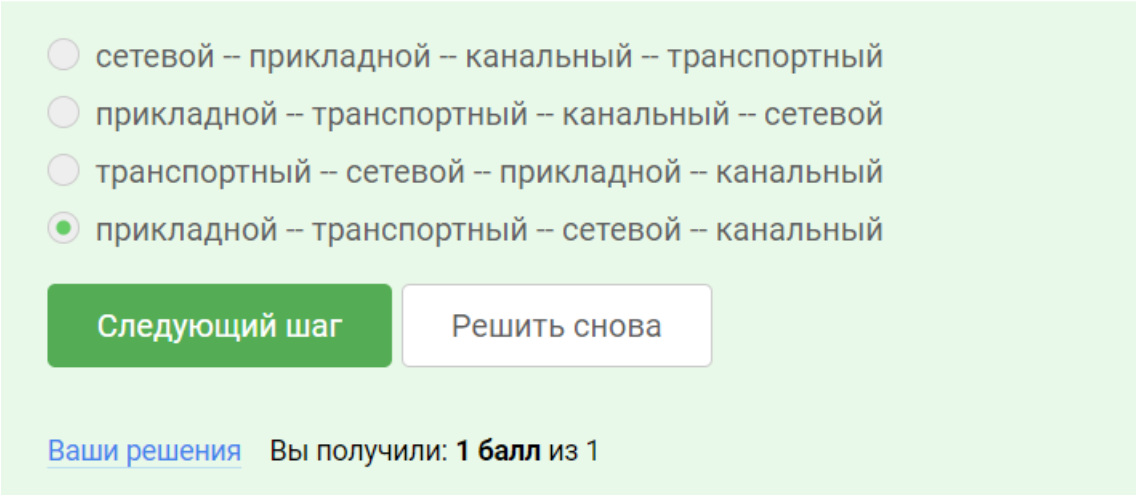
DNS-сервер (доменная система имен) сопоставляет доменные имена (на-пример, www.google.com) с их соответствующими IP-адресами (например, 172.217.13.238).

Когда пользователь вводит доменное имя в свой браузер, происходит следующий процесс:

1. Запрос к DNS-серверу: Браузер отправляет запрос к DNS-серверу, указанному в настройках сети устройства.
2. Поиск записи DNS: DNS-сервер ищет в своей базе данных запись, соответствующую введенному доменному имени. В этой записи хранится IP-адрес, связанный с этим доменным именем.
3. Возврат IP-адреса: DNS-сервер возвращает браузеру найденный IP-адрес.
4. Подключение к веб-серверу: Браузер использует возвращенный IP-адрес для установления соединения с веб-сервером, на котором размещается соответствующий веб-сайт.

Таким образом, DNS-сервер действует как переводчик между доменными именами, которые легко запоминаются пользователями, и IP-адресами, которые фактически используются веб-серверами. Без DNS-серверов пользователям пришлось бы вводить IP-адреса для доступа к веб-сайтам, что было бы намного сложнее и менее удобно.

№5



☐ сетевой – прикладной – канальный – транспортный

☐ прикладной – транспортный – канальный – сетевой

☐ транспортный – сетевой – прикладной – канальный

☒ прикладной – транспортный – сетевой – канальный

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.5: .

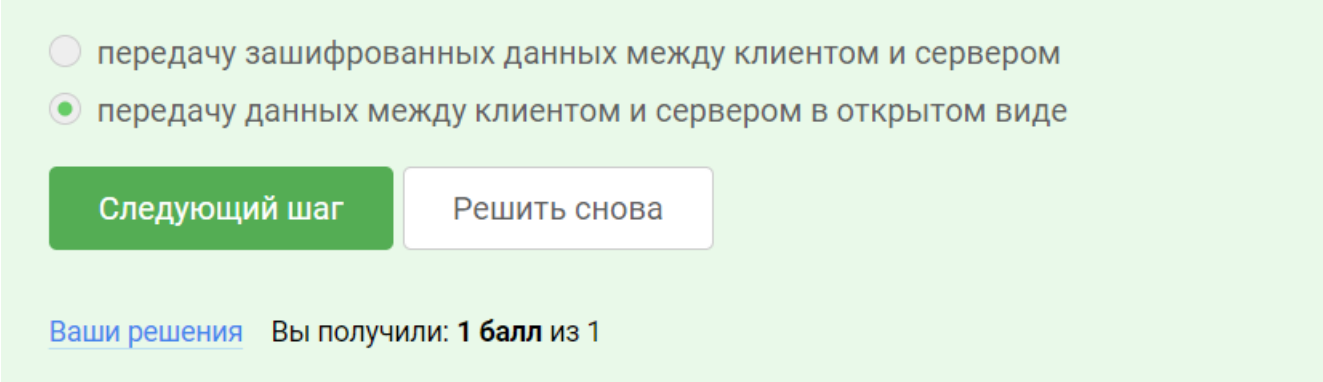
Последовательность протоколов

При отправке пакета данных устройства следуют следующей общей последовательности протоколов:

1. Прикладной уровень: Приложение создает данные.
2. Транспортный уровень: TCP или UDP инкапсулирует данные в сегменты и добавляет заголовки, такие как порты для идентификации конечных точек.
3. Сетевой уровень: IP добавляет заголовок, содержащий адрес источника и назначения.

4. Уровень сетевого доступа: Данные передаются через сетевой интерфейс, такой как сетевая карта.

№6



☐ передачу зашифрованных данных между клиентом и сервером

☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 1.6: .

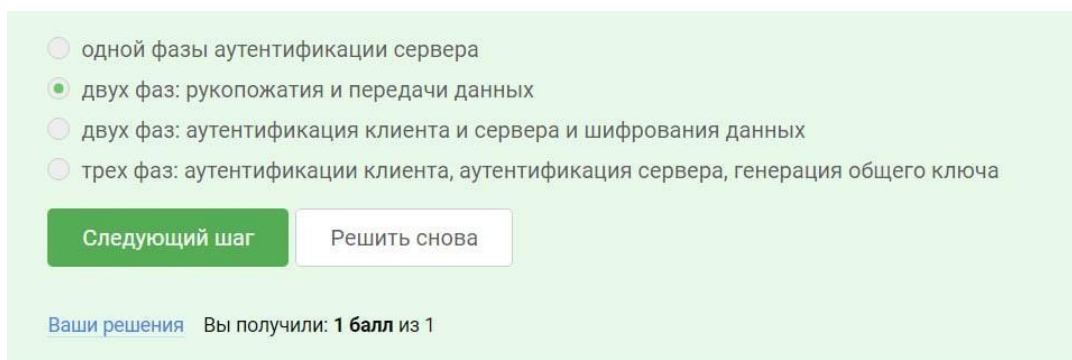
Протокол HTTP (Hypertext Transfer Protocol) является популярным протоколом передачи данных в сети Интернет, но он имеет ряд недостатков, связанных с безопасностью передачи данных.

Основная причина, по которой данные передаются в открытом виде в HTTP, заключается в том, что этот протокол был изначально разработан для обмена гипертекстовыми документами, а не для передачи конфиденциальной информации.

Вот несколько основных причин, почему HTTP передает данные в открытом виде:

1. Простота реализации: протокол HTTP был разработан для быстрой и простой передачи веб-страниц, поэтому его разработчики не фокусировались на безопасности передачи данных.
2. Отсутствие шифрования: HTTP не включает в себя механизмы шифрования данных, поэтому информация передается в открытом виде, без защиты от перехвата или модификации.
3. Обратная совместимость: для обеспечения обратной совместимости с более ранними версиями веб-браузеров и серверов, HTTP продолжает использоваться без шифрования.
4. Производительность: шифрование данных требует дополнительных вычислительных ресурсов, что может снизить производительность системы.

Для решения этой проблемы безопасности был разработан протокол HTTPS (HTTP Secure), который использует SSL/TLS-шифрование для защиты передаваемой информации. HTTPS обеспечивает конфиденциальность, целостность и аутентификацию данных, делая их менее уязвимыми для перехвата или модификации.



☐ одной фазы аутентификации сервера
☒ двух фаз: рукопожатия и передачи данных
☐ двух фаз: аутентификация клиента и сервера и шифрования данных
☐ трех фаз: аутентификации клиента, аутентификация сервера, генерация общего ключа

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 1.7: .

Протокол HTTPS (HTTP Secure) состоит из двух основных фаз: фаза рукопожатия (handshake) и фаза передачи данных.

1. Фаза рукопожатия (Handshake):

- Клиент (например, веб-браузер) инициирует соединение с сервером, отправляя запрос на установление защищенного HTTPS-соединения.
- Сервер отвечает, отправляя свой SSL/TLS сертификат, который содержит информацию о сервере, включая его открытый криптографический ключ.
- Клиент проверяет подлинность сертификата сервера, используя предварительно установленные корневые сертификаты доверенных центров сертификации.
- Клиент генерирует случайный ключ сеанса (session key) и шифрует его с помощью открытого ключа сервера, полученного из сертификата. Затем клиент отправляет зашифрованный ключ сеанса серверу.
- Сервер расшифровывает ключ сеанса с помощью своего закрытого ключа и подтверждает успешное установление соединения.

2. Фаза передачи данных:

- После завершения фазы рукопожатия, клиент и сервер используют ключ сеанса для шифрования и дешифрования всех последующих данных, передаваемых между ними.
- Этот ключ сеанса используется для симметричного шифрования, что обеспечивает высокую скорость шифрования/дешифрования в сравнении с асимметричной криптографией, использованной в фазе рукопожатия.
- Шифрование данных на этой стадии гарантирует их конфиденциальность, целостность и аутентичность в процессе передачи между клиентом и сервером.

Таким образом, фаза рукопожатия устанавливает защищенное SSL/TLS-соединение, а фаза передачи данных использует этот канал для безопасной передачи информации между клиентом и сервером.

The image shows a quiz interface with a light green background. At the top, there are four radio button options: "сервером", "клиентом", "и клиентом, и сервером в процессе “переговоров”", and "провайдером клиента". The third option is selected, indicated by a green dot. Below the options are two buttons: a green "Следующий шаг" button and a white "Решить снова" button. At the bottom, there is a link "Ваши решения" and a score display "Вы получили: 1 балл из 1".

Рис. 1.8: .

Вы правы, версия протокола TLS в HTTPS-соединении определяется в результате “переговоров” между клиентом и сервером.

Процесс определения версии TLS происходит следующим образом:

1. Клиент инициирует соединение и предлагает список версий TLS, которые он поддерживает (например, TLS 1.2, TLS 1.3).
2. Сервер анализирует список версий, предложенных клиентом, и выбирает наиболее подходящую версию TLS, которую он также поддерживает.
3. Сервер отправляет выбранную версию TLS в ответ клиенту, сообщая, какую версию он будет использовать для дальнейшего соединения.
4. Клиент подтверждает использование выбранной версии TLS, и дальнейший обмен данными происходит с использованием этой версии протокола.

Этот процесс “переговоров” позволяет клиенту и серверу согласовать единую версию TLS, которая будет применяться для защищенной передачи данных. Он важен, так как разные версии TLS могут иметь различные алгоритмы шифрования, возможности и уровни безопасности.

Таким образом, окончательная версия TLS определяется в результате совместного решения клиента и сервера, основанного на поддерживаемых ими версиях протокола. Это обеспечивает совместимость и безопасность HTTPS-соединения.

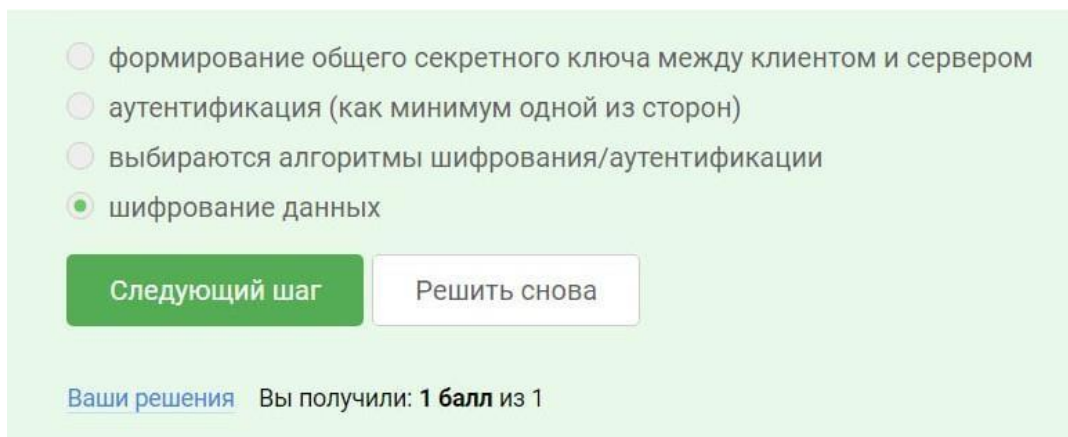


Рис. 1.9: .

Вы правы, в фазе “рукопожатия” (handshake) протокола TLS данные не шифруются. Это связано с особенностями этой начальной фазы установления защищенного соединения.

Во время фазы “рукопожатия” происходит следующее:

1. Клиент отправляет серверу сообщение “Client Hello”, в котором указывает поддерживаемые им версии TLS, алгоритмы шифрования и хеширования.
2. Сервер отвечает сообщением “Server Hello”, в котором выбирает версию TLS и алгоритмы, которые будут использоваться.
3. Сервер также отправляет свой цифровой сертификат, который содержит открытый ключ сервера.
4. Клиент проверяет сертификат сервера и, если он валидный, генерирует секретный ключ сеанса (pre-master secret).
5. Клиент шифрует pre-master secret открытым ключом сервера, полученным из сертификата, и отправляет его серверу.
6. Сервер расшифровывает pre-master secret своим закрытым ключом.

На этом этапе клиент и сервер вычисляют общий секретный ключ сеанса, который будет использоваться для шифрования данных в дальнейшем.

Важно отметить, что до момента генерации общего секретного ключа сеанса данные, передаваемые между клиентом и сервером, не шифруются. Это необходимо для того, чтобы успешно провести процедуру “рукопожатия” и согласовать ключ.

Только после завершения фазы “рукопожатия” соединение переходит к шифрованию данных с применением согласованных алгоритмов и ключа сеанса.

The image shows a web form with a light green background. It contains four checkboxes with labels in Russian: 'id сессии' (checked), 'пароль пользователя' (unchecked), 'идентификатор пользователя' (checked), and 'IP адрес' (unchecked). Below the checkboxes are two buttons: a green one labeled 'Следующий шаг' and a white one with a grey border labeled 'Решить снова'. At the bottom, there is a link 'Ваши решения' and a score 'Вы получили: 1 балл из 1'.

Рис. 1.10: .

Вы правы, куки (cookies) могут хранить различную информацию, в том числе идентификатор сессии и идентификатор пользователя. Рассмотрим подробнее, какую роль они играют:

1. Идентификатор сессии (session ID):

- Когда пользователь входит в систему, сервер генерирует уникальный идентификатор сессии.
- Этот идентификатор сохраняется в куке на клиентской стороне.
- При каждом последующем запросе от пользователя браузер отправляет этот идентификатор сессии на сервер.
- Сервер использует этот идентификатор, чтобы связать текущий запрос с сессией пользователя и, таким образом, поддерживать состояние между запросами.
- Это позволяет серверу помнить, что данный пользователь уже авторизован и имеет определенные права доступа.

2. Идентификатор пользователя (user ID):

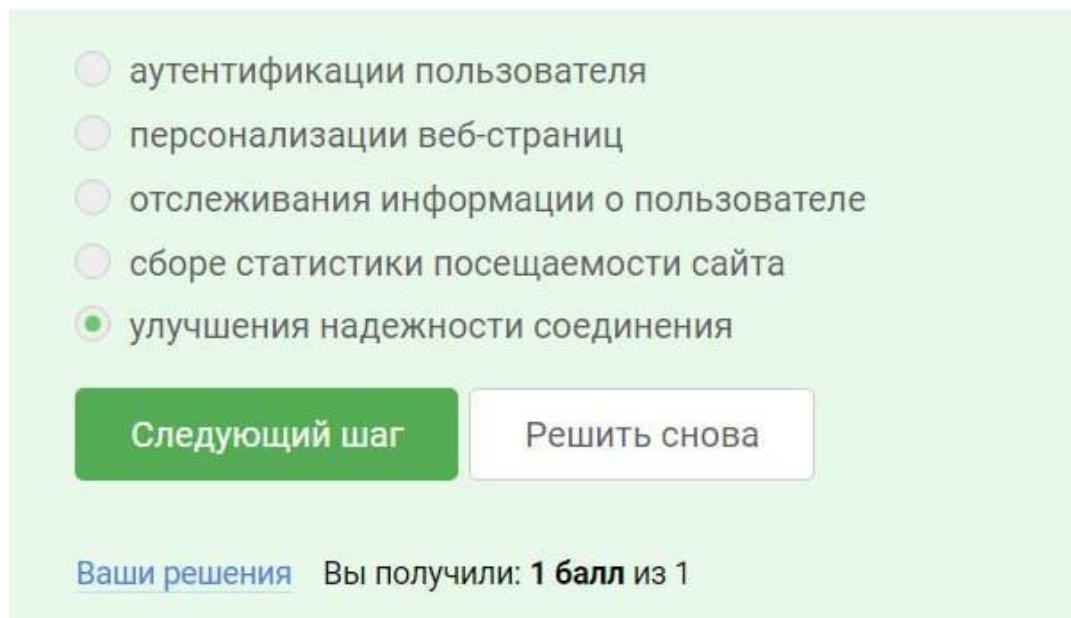
- Когда пользователь авторизуется в системе, сервер может сохранять его уникальный идентификатор (user ID) в куке.
- Это позволяет серверу определять, кто именно выполняет текущий запрос, даже если сессия была утеряна или истекла.
- Сохранение user ID в куке обеспечивает возможность персонализации контента и настроек для конкретного пользователя.

Использование куков для хранения идентификаторов сессии и пользователя является распространенной практикой в веб-приложениях. Это позволяет поддерживать состояние между запросами и обеспечивать персонализированный опыт для каждого пользователя.

Важно отметить, что куки могут содержать и другую информацию, например предпочтения пользователя, корзину покупок и т.д. Однако идентификатор сессии

и идентификатор пользователя являются наиболее распространенными данными, хранящимися в куках.

№2



A screenshot of a quiz interface with a light green background. It contains five radio button options: 'аутентификации пользователя', 'персонализации веб-страниц', 'отслеживания информации о пользователе', 'сборе статистики посещаемости сайта', and 'улучшения надежности соединения'. The last option is selected. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

☐ аутентификации пользователя

☐ персонализации веб-страниц

☐ отслеживания информации о пользователе

☐ сборе статистики посещаемости сайта

☒ улучшения надежности соединения

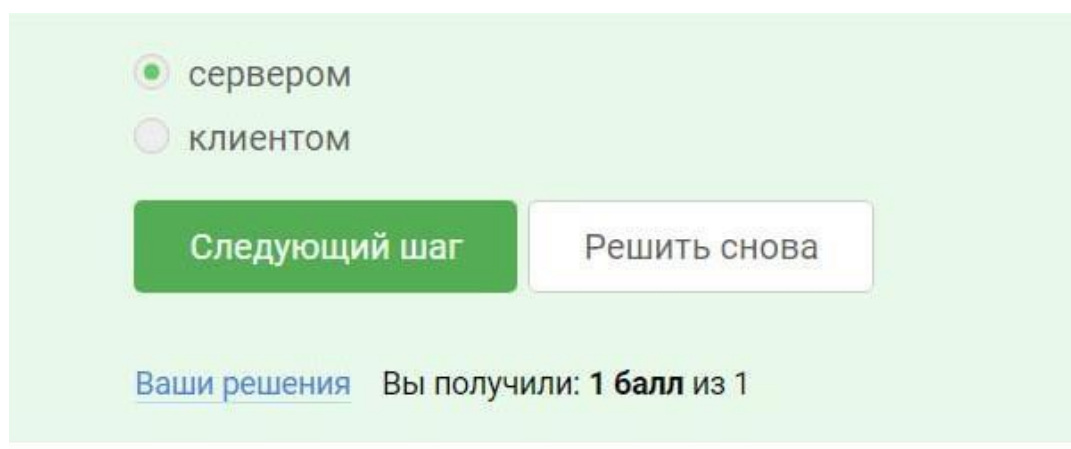
Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.11: .

Потому что куки не связаны напрямую с надежностью соединения.

№3



A screenshot of a quiz interface with a light green background. It contains two radio button options: 'сервером' (selected) and 'клиентом'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

☒ сервером

☐ клиентом

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.12: .

Куки генерируются сервером, потому что:

Защищенная среда: Сервер — это более безопасная среда, чем браузер пользователя, что снижает риск атак и злонамеренной деятельности.

Централизованный контроль: Сервер имеет централизованный контроль над созданием и управлением куки, что гарантирует согласованность и соблюдение политик. Эффективность: Сервер может генерировать куки более эффективно, чем браузер, особенно в случае больших и сложных куки. Безопасность: Сервер

может применять механизмы безопасности, такие как шифрование и аутентификация, для защиты данных куки. Управление сессиями: Сервер использует куки для управления сеансами пользователей и отслеживает их деятельность на сайте. Персонализация: Сервер может использовать куки для хранения и управления пользовательскими предпочтениями, такими как тема, язык и настройки контента. Анализ и отслеживание: Куки помогают серверу отслеживать активность пользователей на сайте и собирать аналитические данные.

№4



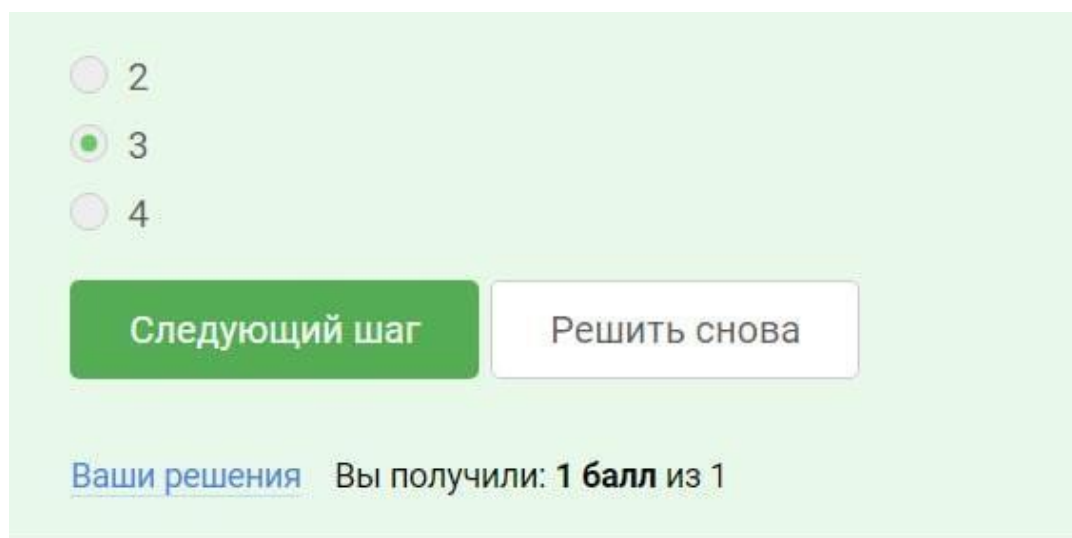
A screenshot of a quiz interface with a light green background. It contains three radio button options: 'Да, на время пользования веб-сайтом' (selected), 'Да, на некоторое время, заданное в сервером', and 'Нет'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

Рис. 1.13: .

Сессионные куки хранятся в браузере на время пользования веб-сайтом. Они удаляются, когда пользователь закрывает браузер. Сессионные куки используются для временного хранения данных, связанных с текущим сеансом пользователя.

2.3

№1

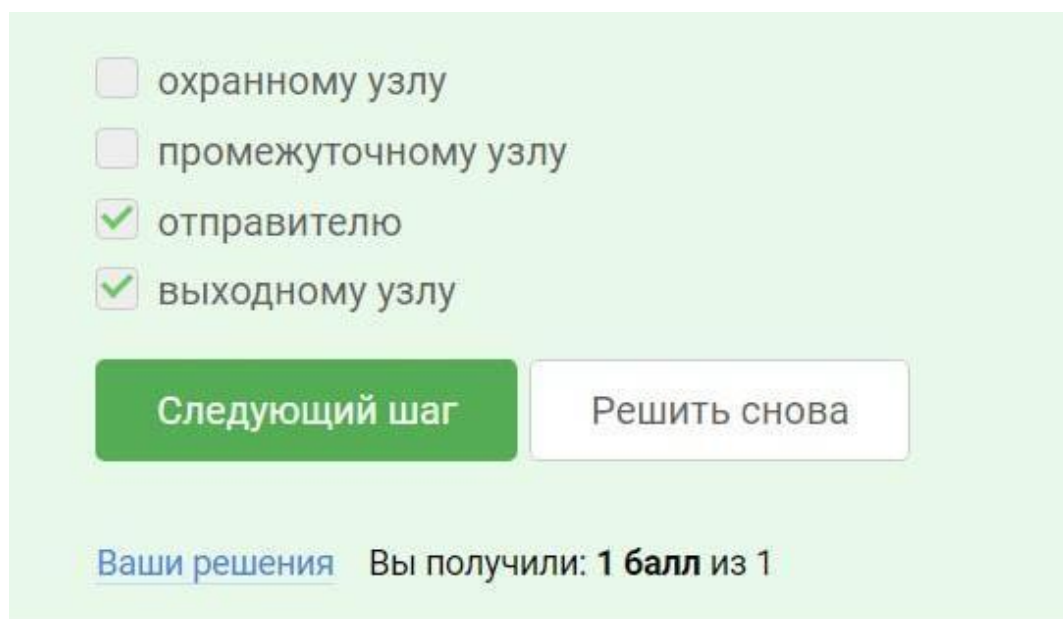


A screenshot of a quiz interface with a light green background. It contains three radio button options: '2', '3' (selected), and '4'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

Рис. 1.14: .

В луковой сети TOR передаваемые данные шифруются трижды и последовательно передаются через три промежуточных узла, прежде чем достигнут конечного получателя.

№2



A screenshot of a quiz interface with a light green background. It contains four radio button options: 'охранному узлу' (unchecked), 'промежуточному узлу' (unchecked), 'отправителю' (checked with a green checkmark), and 'выходному узлу' (checked with a green checkmark). Below the options are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, it says 'Ваши решения' followed by 'Вы получили: 1 балл из 1'.

☐ охранному узлу

☐ промежуточному узлу

☒ отправителю

☒ выходному узлу

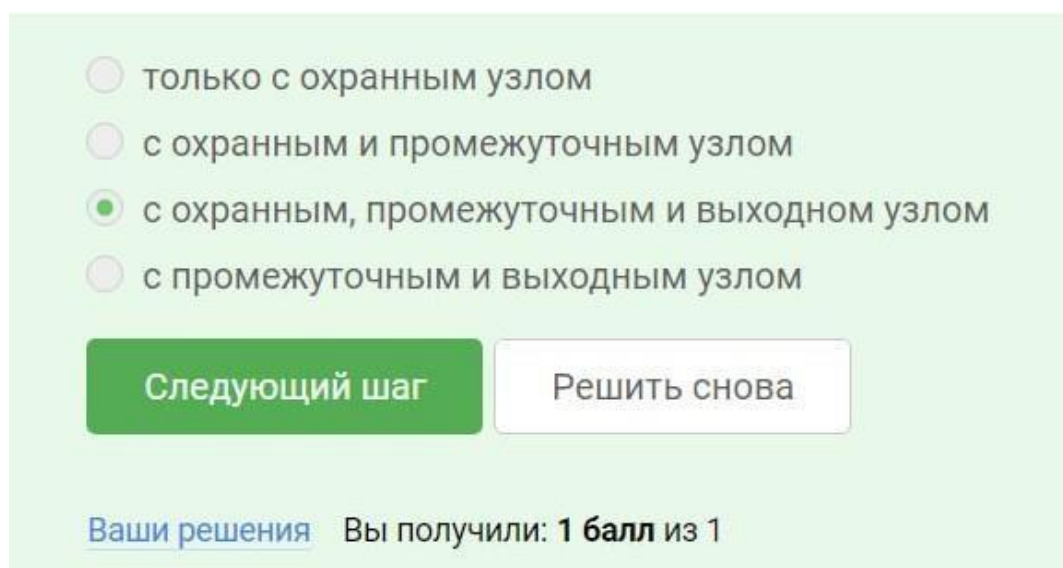
Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.15: .

Отправителю: IP-адрес получателя известен отправителю, так как он включен в заголовок пакета, отправляемого получателю. Выходному узлу: IP-адрес получателя известен выходному узлу, так как выходной узел передает пакет от отправителя к получателю.

№3



A screenshot of a quiz interface with a light green background. It contains four radio button options: 'только с охранным узлом' (unchecked), 'с охранным и промежуточным узлом' (unchecked), 'с охранным, промежуточным и выходным узлом' (checked with a green dot), and 'с промежуточным и выходным узлом' (unchecked). Below the options are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, it says 'Ваши решения' followed by 'Вы получили: 1 балл из 1'.

☐ только с охранным узлом

☐ с охранным и промежуточным узлом

☒ с охранным, промежуточным и выходным узлом

☐ с промежуточным и выходным узлом

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.16: .

Генерация общего секретного ключа отправляющей стороной

Отправитель генерирует общий секретный ключ, который будет использоваться для защищенного обмена сообщениями с охранным, промежуточным и выходным узлами в сети Tor. Этот ключ включает в себя:

С охранным узлом:

Краткосрочный идентификатор (Ephemeral Identity, EI): Уникальный одноразовый ключ, используемый для аутентификации с охранным узлом.

Долговременный ключ (Long-Term Key, LTK): Ключ для долгосрочной аутентификации сохранен на охранном узле.

С промежуточным узлом:

Скрытый сервис (Onion Service): Скрытый адрес, используемый для отправки сообщений промежуточному узлу.

С выходным узлом:

Общий секретный ключ (Shared Secret Key, SSHK): Ключ, совместно используемый отправителем и выходным узлом, сгенерированный во время процедуры установления соединения.

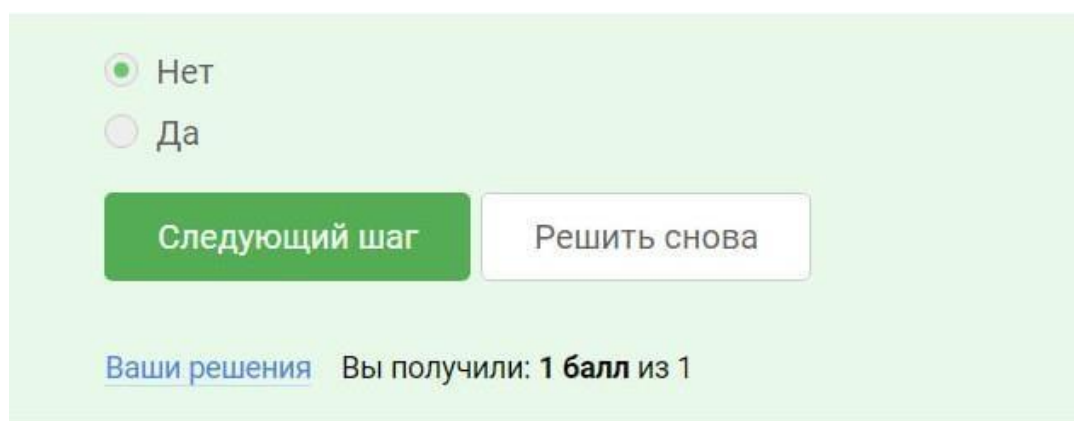
Процесс генерации

Отправитель выполняет следующие шаги для генерации общего секретного ключа:

1. Генерирует EI и LTK.
2. Отправляет EI на охранный узел.
3. Получает LTK от охранного узла.
4. Создает скрытый сервис и предоставляет его промежуточному узлу.
5. Устанавливает прямое соединение с выходным узлом и генерирует SSHK.

Этот процесс гарантирует, что только отправитель и соответствующие узлы могут расшифровать сообщения, передаваемые через сеть Tor.

№4



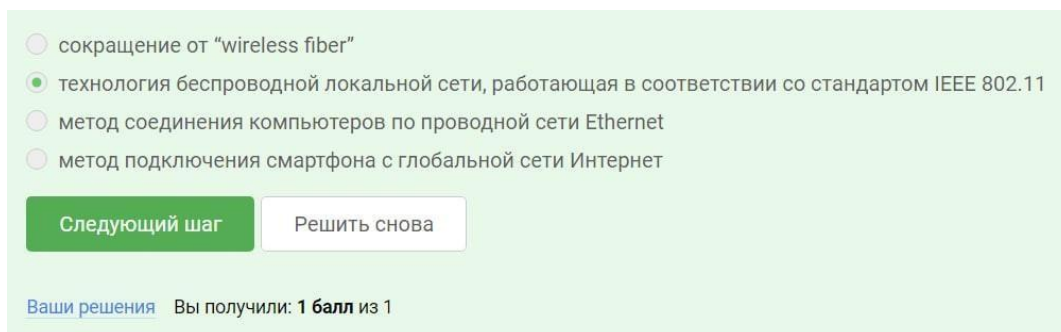
The image shows a confirmation dialog box with a light green background. At the top, there are two radio buttons: the first is selected and labeled 'Нет' (No), and the second is unselected and labeled 'Да' (Yes). Below the buttons are two rectangular buttons: a green one labeled 'Следующий шаг' (Next step) and a white one with a grey border labeled 'Решить снова' (Solve again). At the bottom, there is a blue link-like text 'Ваши решения' (Your solutions) followed by the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.17: .

Получатель не обязан использовать браузер Tor для успешного получения пакетов. Браузер Tor основан на луковой маршрутизации, которая шифрует и анонимизирует трафик, но эта функция не требуется для получения пакетов. Для получения пакетов получателю нужен только обычный веб-браузер.

2.4

№1



☐ 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

[Следующий шаг](#) [Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

Рис. 1.18: .

Wi-Fi (Wireless Fidelity) — это беспроводная технология локальной сети, которая позволяет устройствам подключаться к интернету и друг к другу без использования проводов. Она работает в соответствии со стандартом IEEE 802.11, который определяет технические характеристики и протоколы связи для беспроводных сетей.

Стандарт IEEE 802.11 включает несколько различных вариантов, каждый из которых имеет свои возможности и характеристики. Наиболее распространенными вариантами являются:

802.11a: работает в диапазоне 5 ГГц, обеспечивая высокую скорость передачи данных, но с меньшей дальностью действия. 802.11b: работает в диапазоне 2,4 ГГц, обеспечивая более низкую скорость передачи данных, но с большей дальностью действия. 802.11g: Работает в диапазоне 2,4 ГГц, обеспечивая среднюю скорость передачи данных между 802.11a и 802.11b. 802.11n: Работает как в диапазоне 2,4 ГГц, так и в диапазоне 5 ГГц, обеспечивая более высокую скорость передачи данных и расширенный радиус действия. 802.11ac: работает только в диапазоне 5 ГГц, обеспечивая еще более высокую скорость передачи данных и меньшую задержку.

Ключевые характеристики Wi-Fi

Беспроводное соединение: позволяет устройствам подключаться к сети без проводов, обеспечивая свободу перемещения. Диапазон: Дальность действия Wi-Fi-сигнала зависит от стандарта 802.11 и препятствий в среде. Скорость передачи данных: Скорость передачи данных варьируется в зависимости от стандарта 802.11, частотного диапазона и других факторов. Безопасность: Wi-Fi-сети можно защитить с помощью различных методов, таких как пароли, шифрование и брандмауэры. Удобство использования: Wi-Fi-сети просты в настройке и использовании, что позволяет легко подключать устройства к интернету и обмениваться данными.

№2

A screenshot of a quiz interface. It features four radio button options: 'Транспортном', 'Прикладном', 'Канальном', and 'Сетевом'. The 'Канальном' option is selected, indicated by a green dot. Below the options are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, there is a feedback line: 'Ваши решения' followed by 'Вы получили: 1 балл из 1'.

Рис. 1.19: .

Потому что протокол WiFi работает на Канальном уровне модели OSI, которая отвечает за физическую передачу данных и управление доступом к общей среде передачи.

№3

A screenshot of a quiz interface. It features four radio button options: 'WPA', 'WEP', 'WPA2', and 'WPA3'. The 'WEP' option is selected, indicated by a green dot. Below the options are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, there is a feedback line: 'Ваши решения' followed by 'Вы получили: 1 балл из 1'.

Рис. 1.20: .

WEP (Wired Equivalent Privacy), эквивалент проводного шифрования, является небезопасным методом обеспечения шифрования и аутентификации в сети Wi-Fi из-за следующих причин:

Слабые ключи шифрования: WEP использует 128-битные (или 64-битные) ключи шифрования, которые легко взломать с помощью атак грубой силы или атак повторного воспроизведения. Уязвимость IV: WEP использует инициализирующий вектор (IV) для шифрования каждого пакета, что позволяет злоумышленникам восстанавливать IV и расшифровывать сообщения. Атака повторного воспроизведения: Злоумышленники могут повторно перехватывать и проигрывать пакеты, зашифрованные WEP, что позволяет им обходить защиту шифрования. Атака воровского узла: Злоумышленники могут присоединиться к

сети Wi-Fi и внедрять воровской узел, который перехватывает и модифицирует трафик, проходящий через сеть. Устаревшая технология: WEP была разработана в 1999 году и устарела более современными и безопасными протоколами, такими как WPA2 и WPA3.

№4

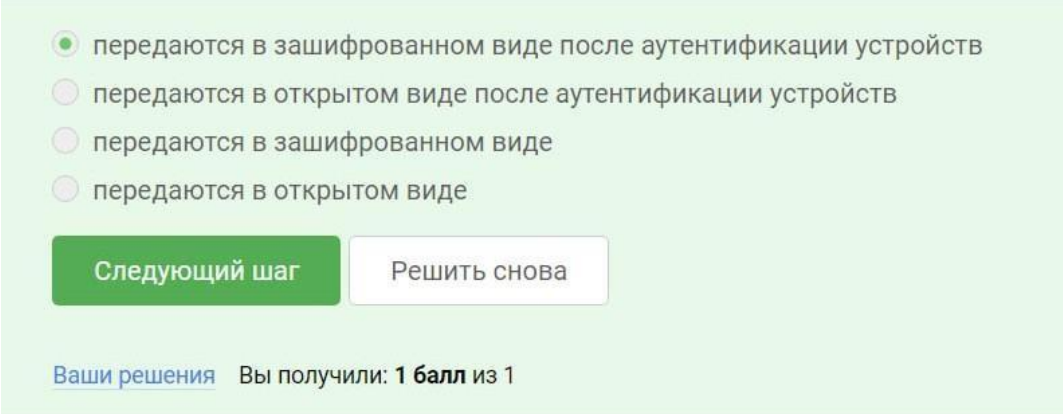


Рис. 1.21: .

После аутентификации устройств для подключения к сети данные между хостом (компьютером или смартфоном) и роутером передаются в зашифрованном виде для обеспечения безопасности и конфиденциальности.

Этот процесс обычно включает следующие шаги:

1. Аутентификация:

- Устройство клиента (хост) передает свои учетные данные (например, имя пользователя и пароль) роутеру для проверки полномочий.
- Роутер проверяет учетные данные и разрешает или отклоняет доступ в соответствии с настроенными правилами.

2. Настройка шифрования:

- После успешной аутентификации устанавливается защищенное соединение между хостом и роутером.
- Выбирается протокол шифрования, например WPA2 или WPA3, и генерируется уникальный ключ шифрования.

3. Шифрование данных:

- Перед передачей все данные между хостом и роутером шифруются с использованием согласованного ключа шифрования.
- Это гарантирует, что данные остаются конфиденциальными и защищенными от перехвата или взлома.

4. Расшифровка данных:

- Когда данные достигают пункта назначения (хоста или роутера), они расшифровываются с использованием того же ключа шифрования.

- После расшифровки данные становятся доступными и читаемыми для авторизованного устройства.

Шифрование данных между хостом и роутером выполняет следующие функции:

Конфиденциальность: защищает данные от несанкционированного доступа и прослушивания. Целостность данных: обеспечивает, что данные не были изменены или повреждены во время передачи. Аутентичность: подтверждает подлинность источника данных и предотвращает спуфинг или подделку.

№5

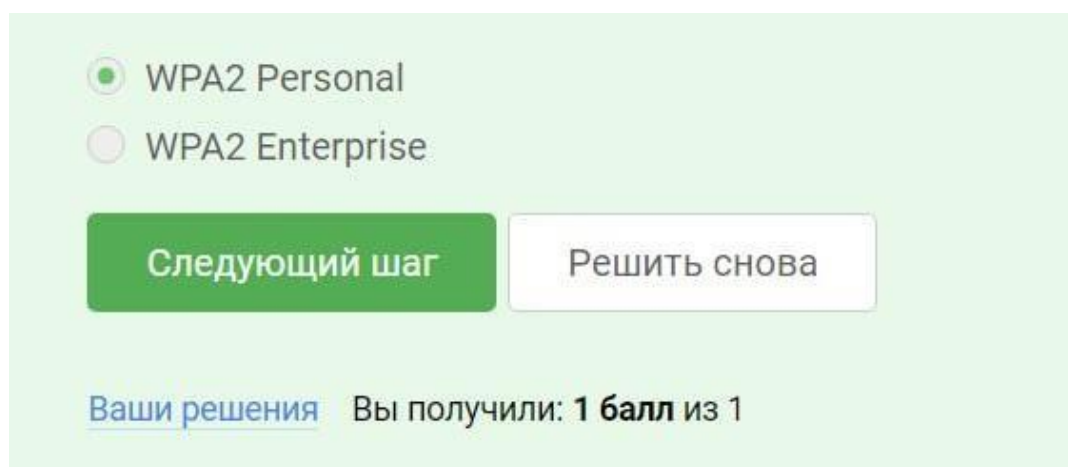


Рис. 1.22: .

WPA2 Personal используется в качестве метода аутентификации для домашних сетей по нескольким причинам:

Безопасность: WPA2 Personal обеспечивает более высокий уровень безопасности по сравнению с предыдущими методами аутентификации, такими как WEP, за счет использования протокола Advanced Encryption Standard (AES). AES известен своей криптографической стойкостью и защищает передаваемые данные от несанкционированного доступа.

Легкость использования: WPA2 Personal прост в настройке и не требует использования сертификатов или сервера аутентификации, как в случае WPA2 Enterprise. Это делает его идеальным выбором для домашних пользователей, которые не обладают техническими знаниями.

Распространенность: WPA2 Personal широко поддерживается клиентами беспроводной связи и маршрутизаторами. Это гарантирует совместимость с большинством устройств, позволяя пользователям легко подключаться к домашним сетям.

Защита от перехвата: WPA2 Personal использует динамический ключ, который меняется при каждом подключении. Это предотвращает перехват злоумышленниками ключей шифрования и доступ к конфиденциальным данным, передаваемым по сети.

Компромисс между безопасностью и удобством: WPA2 Personal предлагает хороший компромисс между безопасностью и удобством использования. Он обеспечивает достаточный уровень безопасности для домашних сетей, не жертвуя при этом удобством использования.

В отличие от WPA2 Enterprise, который используется в корпоративных средах, WPA2 Personal предназначен для упрощения аутентификации в домашних сетях. Он не требует сложной настройки и позволяет пользователям подключаться к сети с использованием предварительно согласованного пароля.

3.1

№1

☒ Да
☐ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.23: .

Да, можно зашифровать загрузочный сектор диска. Причины:

Предотвращение несанкционированной загрузки: Шифрование загрузочного сектора делает невозможным загрузку операционной системы без ключа шифрования. Это защищает компьютер от несанкционированного доступа и атак использованием вредоносных программ. Защита важных данных: Загрузочный сектор содержит важные данные, такие как таблица разделов и информация о загрузке. Шифрование этих данных защищает их от модификации или уничтожения. Соблюдение нормативных требований: Некоторые отрасли и организации требуют шифрования загрузочных секторов для соответствия нормативным требованиям. Защита от атак с помощью вредоносных программ: Шифрование загрузочного сектора затрудняет для вредоносных программ установку модификацию системных файлов.

№2

☐ хэшировании
☒ симметричном шифровании
☐ асимметричном шифровании

Следующий шаг Решить снова

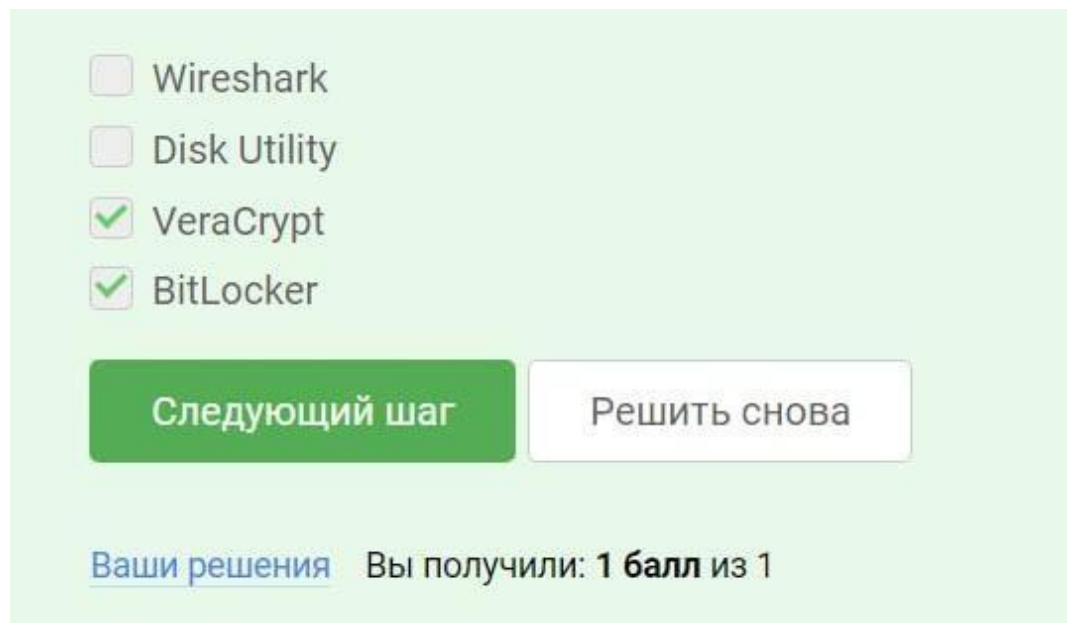
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.24: .

Шифрование диска основано на симметричном шифровании.

Симметричное шифрование, также известное как шифрование с секретным ключом, использует один и тот же криптографический ключ для шифрования и расшифровки данных. Этот ключ должен быть известен как отправителю, так и получателю и храниться в секрете.

№3



☐ Wireshark

☐ Disk Utility

☒ VeraCrypt

☒ BitLocker

Следующий шаг **Решить снова**

Ваши решения Вы получили: **1 балл** из 1

Рис. 1.25: .

Обе приведенные программы, VeraCrypt и BitLocker, могут быть использованы для шифрования жестких дисков. Вот их краткое сравнение:

VeraCrypt

Бесплатная и с открытым исходным кодом доступно для Windows, macOS, Linux и Android поддерживает несколько алгоритмов шифрования, включая AES, Serpent и Twofish создает шифрованные тома, которые можно монтировать как обычные диски имеет расширенные функции безопасности, такие как скрытые тома и связанные тома

BitLocker

Встроен в Windows Доступен только для Windows поддерживает алгоритм шифрования AES шифрует весь жесткий диск или отдельные разделы имеет функции самовосстановления и защиты от атак грубой силы

Почему обе программы полезны:

VeraCrypt является отличным выбором для тех, кто ищет бесплатное и многоплатформенное решение для шифрования дисков. Он предлагает широкий набор функций и алгоритмов, чтобы удовлетворить различные потребности в безопасности.

BitLocker лучше подходит для пользователей Windows, ищущих удобный и встроенный способ зашифровать свой жесткий диск. Он прост в использовании и предоставляет базовый уровень безопасности.

В конечном счете выбор лучшей программы зависит от конкретных требований и предпочтений пользователя.

3.2

№1

Рис. 1.26: .

Из приведенных вариантов стойким можно считать пароль "UQr9@j4!S\$".

Стойкий пароль должен обладать следующими характеристиками:

1. Достаточная длина (обычно рекомендуется не менее 8-12 символов).
2. Использование букв в разных регистрах (строчные и прописные).
3. Включение цифр.
4. Включение специальных символов (!@#%&*).
5. Отсутствие распространенных слов или фраз.

№2

A screenshot of a quiz interface with a light green background. It contains five radio button options for storing passwords. The first option, 'В менеджерах паролей', is selected. Below the options are two buttons: a green 'Следующий шаг' and a white 'Решить снова'. At the bottom, it shows 'Ваши решения' and 'Вы получили: 1 балл из 1'.

- ☒ В менеджерах паролей
- ☐ В заметках на рабочем столе
- ☐ В заметках в телефоне
- ☐ На стикере, приклеенном к монитору
- ☐ В кошельке

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.27: .

Наиболее безопасным способом хранения паролей является использование менеджеров паролей.

Менеджеры паролей (password managers) — это специальные программы или онлайн-сервисы, предназначенные для хранения логинов, паролей и другой конфиденциальной информации в зашифрованном виде. Основные преимущества использования менеджеров паролей:

1. Шифрование данных: менеджеры паролей хранят все данные в зашифрованном виде, что обеспечивает защиту даже в случае кражи или утечки данных.
2. Генерация сложных паролей: они способны генерировать длинные, случайные и сложные пароли для каждого аккаунта, что значительно повышает безопасность.
3. Централизованное хранение: все пароли хранятся в одном защищенном месте, что исключает необходимость запоминать или записывать их в незащищенных местах.
4. Мультиплатформенность: многие менеджеры синхронизируют данные между различными устройствами, обеспечивая доступ к паролям из любого места.

№3

A screenshot of a quiz interface with a light green background. It contains four radio button options about the benefits of password managers. The first option, 'Для защиты от автоматизированных атак...', is selected. Below the options are two buttons: a green 'Следующий шаг' and a white 'Решить снова'. At the bottom, it shows 'Ваши решения' and 'Вы получили: 1 балл из 1'.

- ☒ Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа
- ☐ Для безопасного хранения паролей на сервере
- ☐ Она заменяет пароли
- ☐ Для защиты кук пользователя

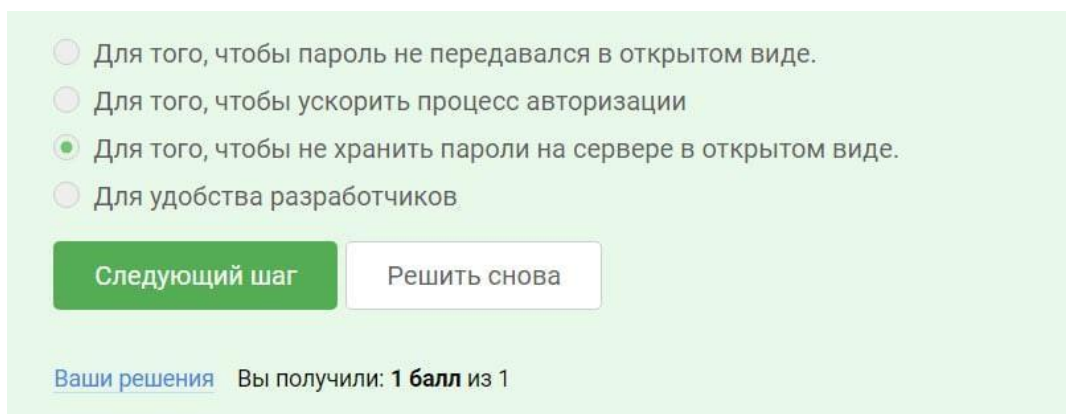
Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.28: .

Капча (CAPTCHA - Completely Automated Public Turing test to tell Computers and Humans Apart) необходима для защиты от автоматизированных атак, направленных на получение несанкционированного доступа.

№4



A screenshot of a CAPTCHA interface with a light green background. It contains four radio button options for a multiple-choice question. The third option is selected. Below the options are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

- ☐ 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

Следующий шаг Решить снова

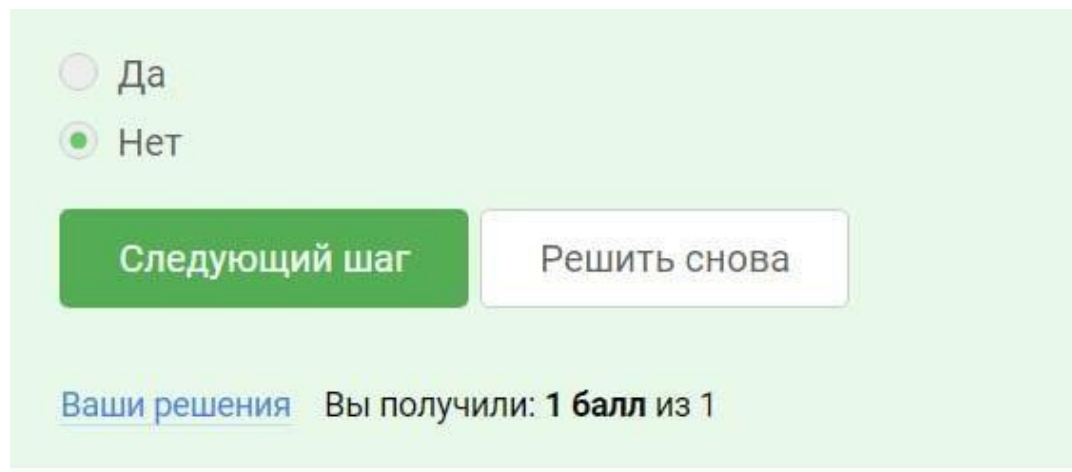
[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.29: .

Хэширование паролей является одной из важнейших мер безопасности при работе с паролями пользователей. Это процесс преобразования пароля в уникальную строку фиксированной длины с помощью криптографической хэш-функции.

Основная цель хэширования паролей - избежать хранения паролей в открытом (незашифрованном) виде на сервере или в базе данных. Вместо этого хранится хэш-значение пароля. При аутентификации пользователя его введенный пароль также преобразуется в хэш, и это значение сравнивается с хранящимся хэш-значением.

№5



A screenshot of a CAPTCHA interface with a light green background. It contains two radio button options for a multiple-choice question. The second option is selected. Below the options are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, there is a link 'Ваши решения' (Your solutions) and a score 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

- ☐ Да
- ☒ Нет

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.30: .

Если злоумышленник получил доступ к серверу, у него будет прямой доступ к базе данных паролей, и он сможет извлечь пароли в виде хешей. Добавление соли к паролям не изменит значения хешей, поэтому злоумышленник все равно сможет совершить атаку перебором с теми же хешами.

№6

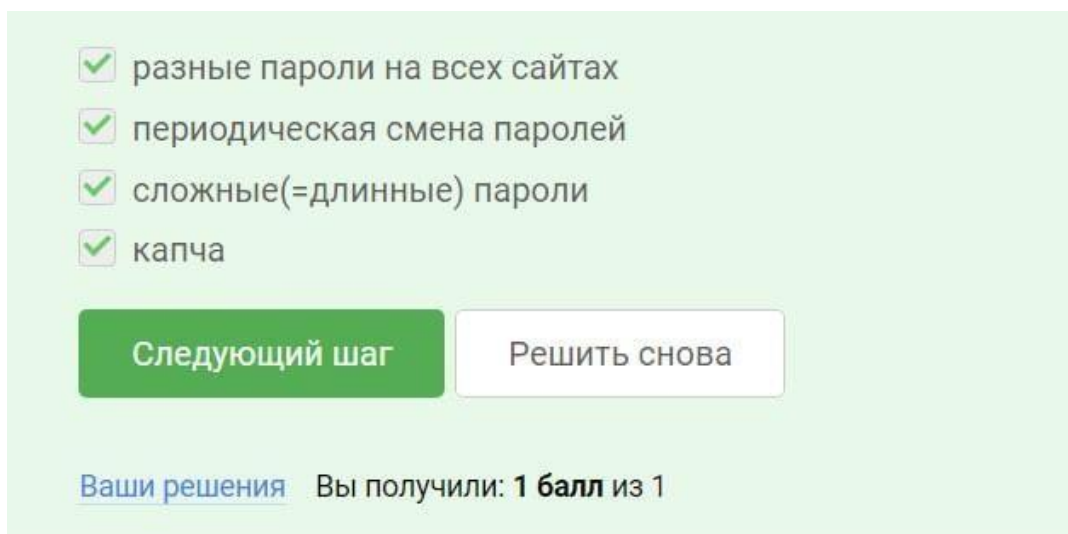


Рис. 1.31: .

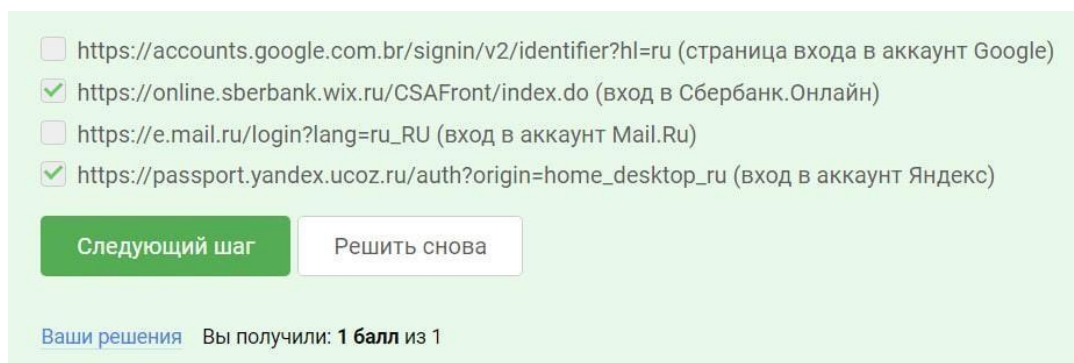
Для защиты от утечек данных атакой перебором необходимо применять следующие меры:

1. Использовать сложные (длинные) пароли. Чем длиннее и сложнее пароль, тем труднее его подобрать методом перебора. Рекомендуется использовать пароли длиной не менее 12 символов с комбинацией букв, цифр и специальных символов.
2. Использовать разные пароли на всех сайтах. Повторное использование одного и того же пароля на нескольких ресурсах значительно увеличивает риски в случае его компрометации на одном из сайтов.
3. Периодически менять пароли. Своевременная смена паролей снижает риск успешной атаки перебором, так как злоумышленникам придется постоянно обновлять свои словари.
4. Применять капчу (CAPTCHA) или другие меры защиты от автоматизированных атак на этапе ввода пароля. Это затрудняет использование скриптов для перебора паролей и вынуждает злоумышленников прибегать к более трудоемким методам.
5. Использовать хеширование паролей с солью. Хранение хешей паролей вместо паролей в открытом виде, а также применение уникальных солей для каждого пароля существенно затрудняет атаку перебором.
6. Ограничивать количество попыток ввода пароля и блокировать учетную запись после определенного числа неудачных попыток. Это предотвращает бесконечный перебор паролей для конкретной учетной записи.
7. Использовать двухфакторную или многофакторную аутентификацию. Даже если злоумышленник подберет пароль, ему потребуется дополнительный фактор (например, одноразовый код) для доступа.

Комбинация этих мер значительно повышает стойкость системы аутентификации к атакам перебором и риску утечки данных пользователей.

3.3

№1



☐ <https://accounts.google.com.br/signin/v2/identifier?hl=ru> (страница входа в аккаунт Google)

☒ <https://online.sberbank.wix.ru/CSAFront/index.do> (вход в Сбербанк.Онлайн)

☐ https://e.mail.ru/login?lang=ru_RU (вход в аккаунт Mail.Ru)

☒ https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс)

Следующий шаг **Решить снова**

[Ваши решения](#) Вы получили: **1 балл** из 1

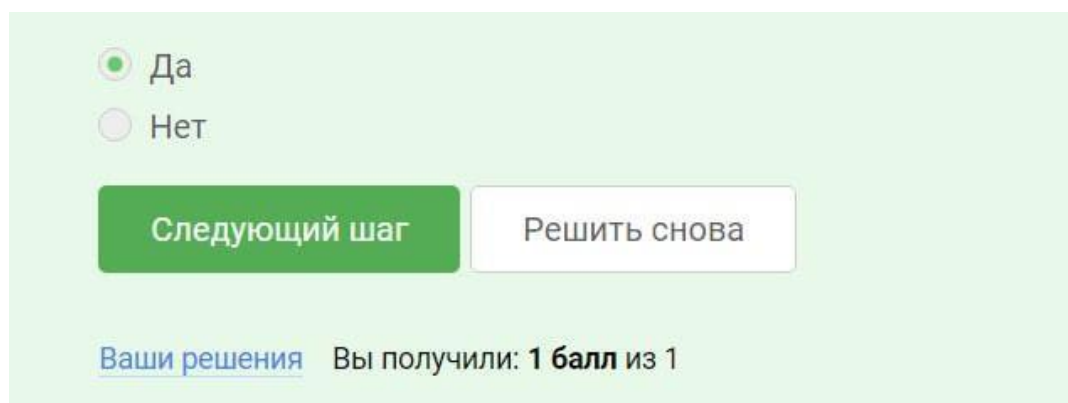
Рис. 1.32: .

Фишинговыми являются следующие ссылки:

[httpsNO LINKSonline.sberbank.wix.ru/CSAFront/index.do](https://online.sberbank.wix.ru/CSAFront/index.do) [httpsNO LINKSpassport.yandex.uco](https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru) Признаки фишинга:

Доменное имя не соответствует официальному имени компании: Официальное доменное имя Сбербанка: sberbank.ru Официальное доменное имя Яндекса: yandex.ru Адрес электронной почты отправителя не связан с компанией. Наличие грамматических ошибок или опечаток в тексте ссылки.

№2



☒ Да

☐ Нет

Следующий шаг **Решить снова**

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.33: .

Да, фишинговый имейл может прийти от знакомого адреса.

Это происходит по нескольким причинам:

1. Взлом учетной записи

Если учетная запись электронной почты вашего знакомого была взломана злоумышленниками, они могут использовать эту учетную запись для рассылки фишинговых писем от имени владельца.

2. Подмена отправителя (Email Spoofing)

Злоумышленники могут подделать заголовки электронного письма, чтобы оно выглядело

как отправленное от определенного адреса. Это возможно из-за недостатков в протоколах электронной почты и отсутствия надлежащей аутентификации отправителя на некоторых серверах.

3. Вредоносное ПО

Если компьютер знакомого заражен вредоносным программным обеспечением (вирусом, троянцем и т.д.), злоумышленники могут получить доступ к его учетным данным и использовать его учетную запись для рассылки фишинговых писем.

4. Техника "Ближний круг"

Фишеры часто используют социальную инженерию, делая вид, что сообщение исходит от кого-то близкого жертве (друг, коллега, родственник), чтобы повысить доверие и вероятность того, что жертва откроет вложение или перейдет по вредоносной ссылке.

3.4

№1

The image shows a quiz interface on a light green background. It contains four radio button options: 'протокол для отправки имейлов', 'подмена адреса отправителя в имейлах' (which is selected), 'атака перебором паролей', and 'метод предотвращения фишинга'. Below these are two buttons: a green 'Следующий шаг' button and a white 'Решить снова' button. At the bottom, it says 'Ваши решения' followed by 'Вы получили: 1 балл из 1'.

Рис. 1.34: .

Правильный ответ: Email Спуфинг (Email Spoofing) — это подмена адреса отправителя в имейлах.

Email Spoofing позволяет злоумышленникам отправлять электронные письма от имени других людей или организаций, подделывая адрес отправителя в заголовках сообщения. Это может использоваться для фишинговых атак, распространения спама, а также в качестве части более сложных схем мошенничества.

№2

A screenshot of a quiz interface with a light green background. It contains four radio button options: 'обязательно шифрует данные и требует ключ дешифрования', 'маскируется под легитимную программу' (selected), 'работает исключительно под ОС Windows', and 'разработан греками'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

- ☐ обязательно шифрует данные и требует ключ дешифрования
- ☒ маскируется под легитимную программу
- ☐ работает исключительно под ОС Windows
- ☐ разработан греками

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.35: .

Трояны — это вид вредоносного программного обеспечения, которое маскируется под безвредные или полезные программы, чтобы обмануть пользователя и получить доступ к его компьютерной системе. Основная особенность троянов - их способность прикидываться чем-то другим, например, игрой, программой для редактирования фото или даже антивирусом.

3.5

№1

A screenshot of a quiz interface with a light green background. It contains four radio button options: 'при получении сообщения', 'при генерации первого сообщения стороной-отправителем' (selected), 'при установке приложения', and 'при каждом новом сообщении от стороны-отправителя'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link, followed by 'Вы получили: 1 балл из 1'.

- ☐ при получении сообщения
- ☒ при генерации первого сообщения стороной-отправителем
- ☐ при установке приложения
- ☐ при каждом новом сообщении от стороны-отправителя

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.36: .

В протоколе мессенджера Signal ключ шифрования (также называемый сеансовым ключом) формируется при инициализации каждого нового сеанса отправки сообщений между двумя участниками.

№2

☒ сообщения передаются по узлам связи (серверам) в зашифрованном виде
☐ сервер получает сообщения в открытом виде для передачи нужному получателю
☐ сервер перешифровывает сообщения в процессе передачи
☐ сообщения передаются от отправителя к получателю без участия сервера

Следующий шаг Решить снова

Ваши решения Вы получили: **1 балл** из 1

Рис. 1.37: .

Суть сквозного (конца в конец, end-to-end) шифрования заключается в том, что сообщения шифруются на устройстве отправителя перед их передачей и расшифровываются только на устройстве получателя. Промежуточные узлы связи, такие как серверы или провайдеры, не могут расшифровать эти сообщения, так как не имеют доступа к ключам шифрования.

4.1

№1

☒ обе стороны имеют пару ключей
☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
☐ одна сторона имеет только секретный ключ, а другая – пару из открытого и секретного ключей
☐ обе стороны имеют общий секретный ключ

Следующий шаг Решить снова

Ваши решения Вы получили: **1 балл** из 1

Рис. 1.38: .

В асимметричных криптографических примитивах обе стороны действительно имеют пару ключей по следующим причинам:

Разделение открытого и закрытого ключей: Асимметричная криптография основана на разделении открытого и закрытого ключей. Открытый ключ известен всем, а закрытый ключ хранится в секрете владельцем.

Шифрование и расшифровка: Открытый ключ используется для шифрования сообщений, которые может расшифровать только владелец соответствующего закрытого ключа. Это обеспечивает безопасность передачи сообщений через незащищенный канал.

Цифровые подписи: Закрытый ключ используется для создания цифровых подписей, которые подтверждают подлинность и целостность сообщений. Открытый ключ может использоваться для проверки этих подписей.

Удобство: Использование пары ключей удобно, поскольку устраняет необходимость обмена секретными ключами между сторонами.

Защита от компрометации: если один из ключей пары будет скомпрометирован, другой ключ остается безопасным, обеспечивая дополнительный уровень защиты.

№2

☒ эффективно вычисляется

☒ стойкая к коллизиям

☒ дает на выходе фиксированное число бит независимо от объема входных данных

☐ обеспечивает конфиденциальность захешированных данных

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.39: .

Криптографическая хэш-функция — это одностороннее преобразование данных произвольной длины в строку фиксированной длины (дайджест или хэш). Ключевыми свойствами хеш-функций являются:

1) Дает на выходе фиксированное число бит независимо от объема входных данных. Например, SHA-256 всегда выдает 256-битный хэш, независимо от размера файла или текста на входе.

2) Эффективно вычисляется.

Хэш-функции работают быстро и просто в вычислении.

3) Стойкая к коллизиям.

Практически невозможно подобрать два различных входных сообщения, хэши которых совпадут. Это свойство обеспечивает целостность данных.

№3

☐ AES

☐ SHA2

☒ RSA

☒ ECDSA

☒ ГОСТ Р 34.10-2012

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.40: .

Потому что RSA, ECDSA и ГОСТ Р 34.10-2012 являются алгоритмами цифровой подписи.

Алгоритм цифровой подписи — это криптографический алгоритм, используемый для создания электронной подписи, которая обеспечивает целостность и подлинность цифровых данных.

RSA (Алгоритм Ривеста — Шамира — Адельмана) — один из первых и наиболее широко используемых алгоритмов цифровой подписи. ECDSA (Алгоритм цифровой подписи с эллиптическими кривыми) — более современный и эффективный алгоритм цифровой подписи, основанный на криптографии эллиптических кривых. ГОСТ Р 34.10-2012 — российский стандарт алгоритма цифровой подписи, основанный на ГОСТ 28147-89.

№4

Рис. 1.41: .

MAC представляет собой небольшую последовательность бит, которая формируется от исходного сообщения и секретного ключа при помощи заданного алгоритма. MAC позволяет гарантировать целостность сообщения и аутентифицировать его источник для сторон, владеющих общим секретным ключом.

Симметричный характер MAC обусловлен тем, что для его вычисления и проверки требуется общий секретный ключ, известный как отправителю, так и получателю данных. Это отличает MAC от цифровых подписей, использующих асимметричную криптографию.

№5

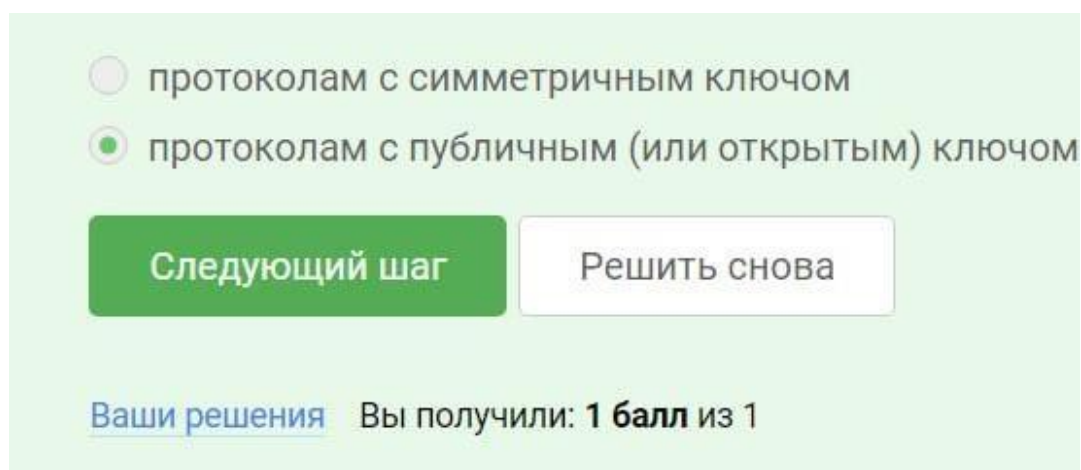
Рис. 1.42: .

Этот протокол позволяет двум сторонам безопасно установить общий секретный ключ по открытому каналу связи. При этом не требуется предварительного обмена каким-либо секретным ключом.

Работа протокола основана на вычислительной сложности задачи дискретного логарифмирования в конечном поле. Каждая сторона генерирует свою пару открытого и секретного ключей, обменивается открытыми ключами, и на основе полученных данных вычисляет общий секретный ключ.

4.2

№1



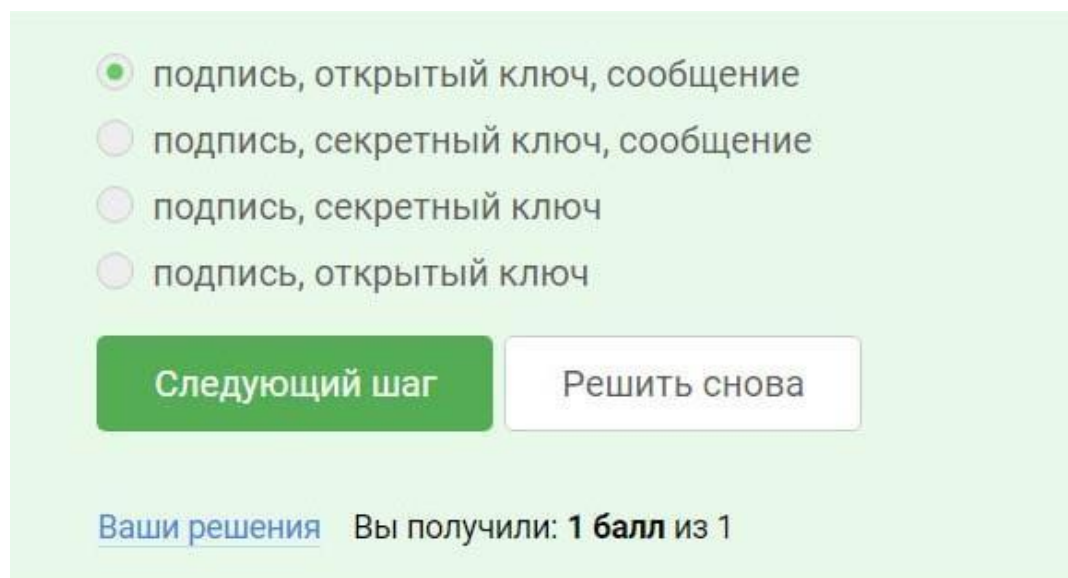
The screenshot shows a quiz interface with a light green background. At the top, there are two radio button options: the first is 'протоколам с симметричным ключом' (protocols with a symmetric key) and the second is 'протоколам с публичным (или открытым) ключом' (protocols with a public (or open) key). The second option is selected, indicated by a green dot. Below the options are two buttons: a green button labeled 'Следующий шаг' (Next step) and a white button with a green border labeled 'Решить снова' (Solve again). At the bottom, there is a blue link 'Ваши решения' (Your solutions) followed by the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.43: .

Протокол электронной цифровой подписи относится к протоколам с публичным (или открытым) ключом, потому что он использует асимметричную криптографию, в которой для подписи документа используется один (частный) ключ, а для проверки подписи — другой (публичный) ключ.

В отличие от протоколов с симметричным ключом, где один и тот же ключ используется для шифрования и расшифровки, в протоколах с открытым ключом частный ключ хранится в секрете, а публичный ключ может быть общедоступным. Это позволяет подписывать документы таким образом, что их могут проверить другие стороны без необходимости обмениваться секретными ключами.

№2



The screenshot shows a quiz interface with a light green background. At the top, there are four radio button options: the first is 'подпись, открытый ключ, сообщение' (signature, public key, message) and is selected with a green dot; the second is 'подпись, секретный ключ, сообщение' (signature, secret key, message); the third is 'подпись, секретный ключ' (signature, secret key); and the fourth is 'подпись, открытый ключ' (signature, public key). Below the options are two buttons: a green button labeled 'Следующий шаг' (Next step) and a white button with a green border labeled 'Решить снова' (Solve again). At the bottom, there is a blue link 'Ваши решения' (Your solutions) followed by the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.44: .

Для проверки электронной цифровой подписи (ЭЦП) требуется на вход подпись, открытый ключ и сообщение по следующим причинам:

Подпись: Подпись необходима для проверки ее достоверности и подтверждения подлинности подписавшего.

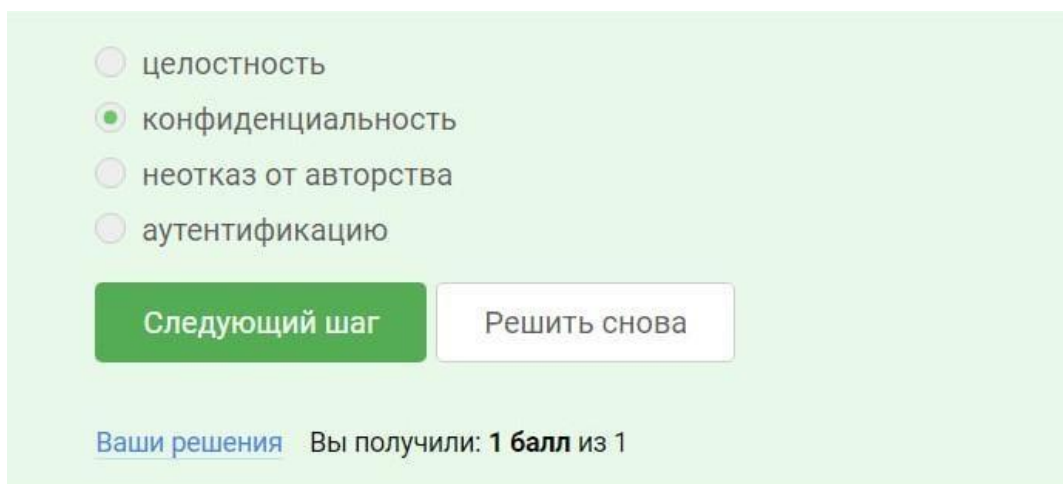
Открытый ключ: Открытый ключ используется для дешифрования подписи и извлечения хеша сообщения. Он обеспечивает возможность проверки того, что именно владелец закрытого ключа, соответствующего открытому ключу, подписал сообщение.

Сообщение: Сообщение необходимо для вычисления его хеш-функции. Хеш-функция используется для проверки целостности сообщения и подтверждения того, что не было никаких изменений после подписания.

Алгоритм верификации ЭЦП работает следующим образом:

1. Вычисляется хеш-функция сообщения.
2. Хеш используется для дешифрования подписи с использованием открытого ключа.
3. Результат дешифрования сравнивается с вычисленным хешем сообщения.
4. Если два хеша совпадают, значит, подпись является действительной и сообщение не было изменено.

№3



☐ целостность

☒ конфиденциальность

☐ неотказ от авторства

☐ аутентификацию

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.45: .

Электронная цифровая подпись (ЭЦП) не обеспечивает конфиденциальность, поскольку она не шифрует содержимое сообщения. ЭЦП предназначена для проверки подлинности и целостности сообщения, а не для его защиты от несанкционированного доступа. Шифрование является отдельным механизмом, который необходимо использовать для обеспечения конфиденциальности. Вот почему:

ЭЦП используется для аутентификации отправителя. Она подтверждает, что сообщение было отправлено определенным лицом или организацией. Она не скрывает содержимое сообщения. ЭЦП защищает от изменений. Она гарантирует, что сообщение не было изменено после его подписи. Однако она не защищает его

от чтения другими лицами. Шифрование необходимо для конфиденциальности. Шифрование преобразует сообщение в нечитаемый формат, доступный только тем, кто обладает ключом или паролем.

Таким образом, ЭЦП и шифрование служат разным целям, и оба механизма необходимы для обеспечения как подлинности, так и конфиденциальности сообщений.

№4

The screenshot shows a quiz interface with three radio button options: "простая" (unselected), "усиленная квалифицированная" (selected), and "усиленная неквалифицированная" (unselected). Below the options are two buttons: "Следующий шаг" (Next step) in green and "Решить снова" (Solve again) in white. At the bottom, it says "Ваши решения" (Your solutions) and "Вы получили: 1 балл из 1" (You received: 1 point out of 1).

Рис. 1.46: .

Усиленная квалифицированная электронная подпись (КЭП) необходима для отправки налоговой отчетности в ФНС, потому что:

Согласно статье 6 Федерального закона № 63-ФЗ “Об электронной подписи”, при представлении налоговой отчетности в электронной форме используются усиленные квалифицированные электронные подписи руководителя или уполномоченного лица. КЭП соответствует самым высоким требованиям безопасности и подтверждена аккредитованным удостоверяющим центром. Она позволяет однозначно идентифицировать отправителя налоговой отчетности и обеспечивает юридическую значимость передаваемых сведений.

№5

The screenshot shows a quiz interface with four radio button options: "в любой организации, имеющей соответствующую лицензию ФСБ" (unselected), "в минкомсвязи РФ" (unselected), "в удостоверяющем (сертификационном) центре" (selected), and "в любой организации по месту работы" (unselected). Below the options are two buttons: "Следующий шаг" (Next step) in green and "Решить снова" (Solve again) in white. At the bottom, it says "Ваши решения" (Your solutions) and "Вы получили: 1 балл из 1" (You received: 1 point out of 1).

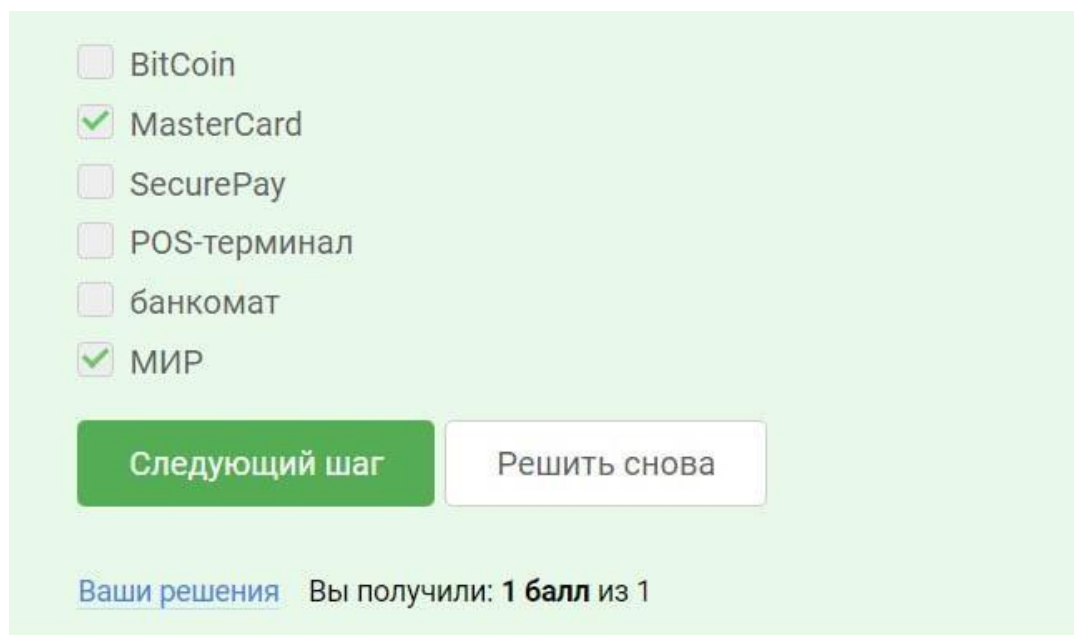
Рис. 1.47: .

Удостоверяющий (сертификационный) центр — это организация, которая выдает квалифицированные сертификаты ключа проверки электронной подписи. Эти сертификаты подтверждают, что электронная подпись принадлежит

определенному лицу или организации и что она прошла проверку на соответствие установленным стандартам.

4.3

№1



A screenshot of a web interface for selecting payment methods. It features a list of options with checkboxes: BitCoin, MasterCard (checked), SecurePay, POS-терминал, банкомат, and МИР (checked). Below the list are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, it says 'Ваши решения' (Your solutions) and 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.48: .

Потому что они являются платежными системами

№2



A screenshot of a web interface for selecting security methods. It features a list of options with checkboxes: комбинация проверки пароля + Капча, комбинация проверка пароля + код в sms сообщении (checked), комбинация код в sms сообщении + отпечаток пальца (checked), and комбинация PIN код + пароль. Below the list are two buttons: 'Следующий шаг' (Next step) in green and 'Решить снова' (Solve again) in white. At the bottom, it says 'Ваши решения' (Your solutions) and 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

Рис. 1.49: .

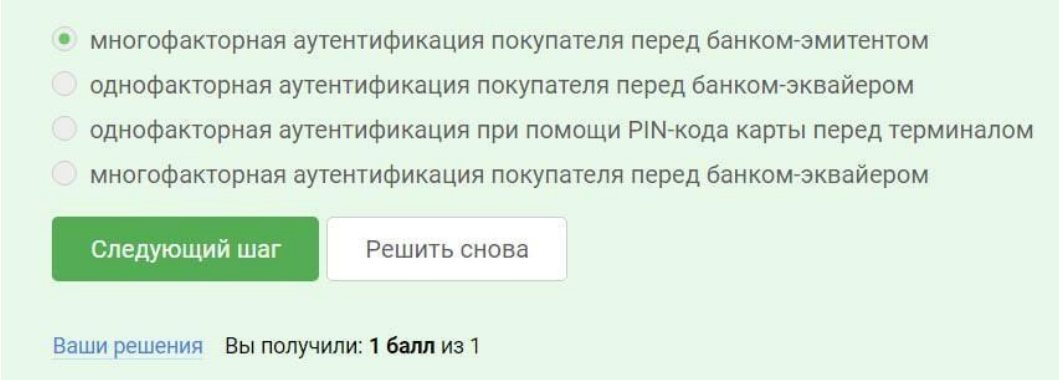
Комбинация проверки пароля + код в sms сообщении является примером двухфакторной аутентификации, так как она использует два разных фактора: что-то, что вы знаете (пароль) и что-то, что у вас есть (телефон с SIM-картой, номер которой привязан к аккаунту).

Комбинация код в sms сообщении + отпечаток пальца также является примером двухфакторной аутентификации, поскольку она использует два разных фактора:

что-то, что у вас есть (телефон с SIM-картой) и что-то, что является уникальным для вас (отпечаток пальца).

Многофакторная аутентификация предполагает использование трех или более различных факторов аутентификации, поэтому ни один из приведенных примеров не является примером многофакторной аутентификации.

№3



☒ многофакторная аутентификация покупателя перед банком-эмитентом

☐ однофакторная аутентификация покупателя перед банком-эквайером

☐ однофакторная аутентификация при помощи PIN-кода карты перед терминалом

☐ многофакторная аутентификация покупателя перед банком-эквайером

Следующий шаг Решить снова

Ваши решения Вы получили: **1 балл** из 1

Рис. 1.50: .

Многофакторная аутентификация используется при онлайн-платежах перед банком-эмитентом по нескольким причинам:

1. **Повышенная безопасность:** Многофакторная аутентификация добавляет дополнительный уровень защиты, требуя от пользователей предоставлять более одного способа подтверждения своей личности. Это затрудняет злоумышленникам доступ к учетным записям и совершение несанкционированных транзакций.
2. **Соблюдение нормативных требований:** Во многих странах действуют нормативные требования, которые предписывают банкам использовать многофакторную аутентификацию для защиты транзакций онлайн-банкинга. Это помогает банкам соответствовать этим требованиям и снижает риск мошенничества и штрафов.
3. **Защита от мошенничества:** Многофакторная аутентификация помогает предотвращать мошенничество, требуя от злоумышленников не только логин и пароль, но и другие факторы, такие как код подтверждения, отправленный по SMS или электронной почте, или биометрические данные.
4. **Повышение доверия клиентов:** когда клиенты знают, что их онлайн- транзакции защищены многофакторной аутентификацией, они чувствуют себя более уверенно, совершая покупки в Интернете. Это повышает доверие клиентов и лояльность к банкам и поставщикам услуг.
5. **Снижение потерь от мошенничества:** Многофакторная аутентификация значительно снижает количество успешных мошеннических атак, что приводит к снижению потерь от мошенничества для банков и продавцов.

№1

A screenshot of a quiz interface with a light green background. It contains four radio button options: 'фиксированная длина выходных данных', 'сложность нахождения прообраза' (which is selected), 'обеспечение целостности', and 'эффективность вычисления'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link and 'Вы получили: 1 балл из 1'.

Рис. 1.51: .

Свойство криптографической хэш-функции, которое используется в доказательстве работы, — это сложность нахождения прообраза.

№2

A screenshot of a quiz interface with a light green background. It contains four checked checkbox options: 'открытость', 'постоянства', 'консенсус', and 'живучесть'. Below the options are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). At the bottom, it says 'Ваши решения' with a link and 'Вы получили: 1 балл из 1'.

Рис. 1.52: .

Открытость: Любой может просмотреть и проверить блокчейн, чтобы убедиться в его достоверности. Постоянство: после того, как данные записаны в блокчейн, их невозможно изменить или удалить, обеспечивая постоянство записанных транзакций. Консенсус: Все участники сети должны согласиться с текущим состоянием блокчейна, прежде чем новые блоки могут быть добавлены. Живучесть: Блокчейны обычно распределены по множеству узлов, что делает их устойчивыми к сбоям отдельных узлов.

№3

☐ обмен ключами

☐ шифрование

☒ цифровая подпись

☐ хэш-функция

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **1 балл** из 1

Рис. 1.53: .

Хэш-функция является одним из фундаментальных криптографических примитивов, который широко применяется в современных системах защиты информации.



Поздравляем!

Вы завершили курс «Основы кибербезопасности».

Вы набрали **53 балла из 53**, изучив 100% материалов курса.

Сертификат в нём не выдаётся, но вы можете поделиться своим результатом в соцсетях.



<https://stepik.org/course/111512>

☆ [Оставить отзыв](#)

[Найти новый курс](#)