Отчёт к прохождению Внешнего курса

Основы кибербезопасности

Четвергова Мария Викторовна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Слушатели курса «Основы кибербезопасности» узнают, как обеспечивается безопасность интернет-трафика, какие пароли нужно выбирать и как их хранить, познакомятся с методами защиты сообщений в мессенджерах (WhatsApp, Telegram), поймут, как работают механизмы аутентификации в электронных платежах, а также зачем нас иногда просят выбрать квадраты, где изображены светофоры.

2 Последовательность выполнения работы

Разберём каждый раздел курса.

1 часть. Безопасность в сети

###Как работает интернет: базовые сетевые протоколы

В модели TCP/IP существует несколько уровней, а именно 4. И сейчас мы рассмотрим последовательно все четыре уровня модели TCP/IP. На самом верхнем уровне, прикладном работают пользовательские программы, и задача прикладного уровня - обеспечить доступ для этих пользовательских программ к услугам Интернет. Мы с вами пользуемся достаточно большим спектром программ в интернете, и каждая программа использует свой протокол. Например, браузеры и веб-страницы используют протокол HTTP или его современную версию HTTPS.

Все эти протоколы прикладного уровня работают над транспортным уровнем, это следующий уровень в модели TCP/IP. Транспортный уровень обеспечивает передачу данных между процессами на одной машине или хосте (host). Хост - это устройство, которое подключено к интернету. Это может быть компьютер, смартфон. И транспортный уровень отвечает за корректное распределение пакетов между программами. То есть он знает, что какие-то данные пришли нам в Skype, какие-то данные пришли нам на почту, какие-то данные должны прийти в наш браузер. Кроме того, протокол транспортного уровня, ответственный за адресацию, должен понимать, для какого процесса пришёл тот или иной пакет. На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель. Этот протокол, в отличие от второго примера – UDP, обеспечивает надежную передачу

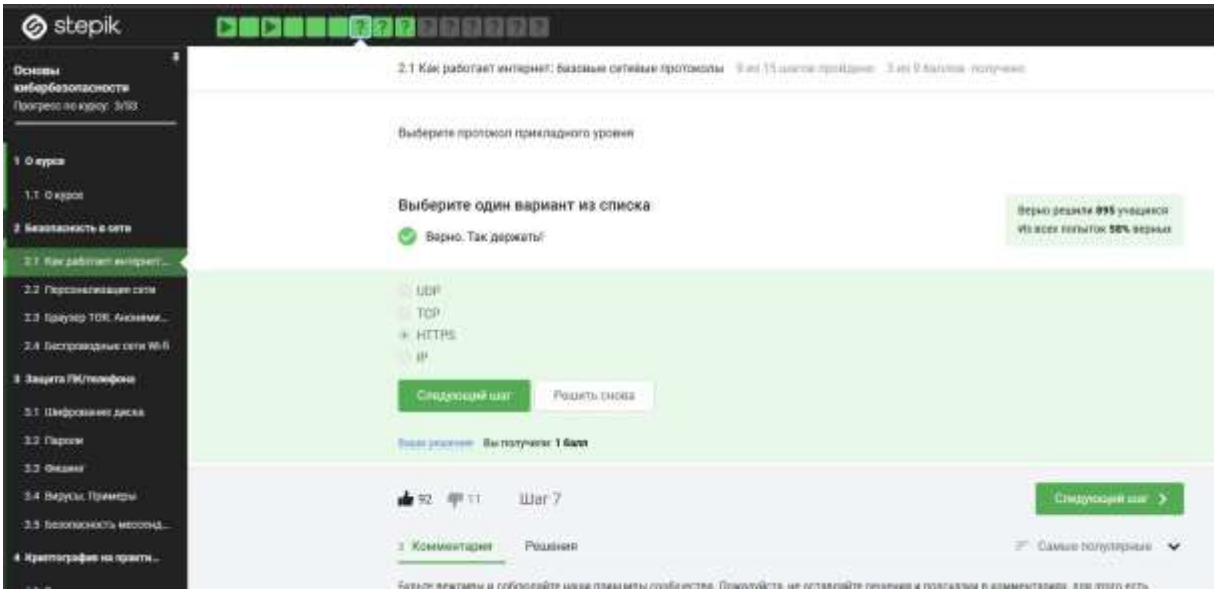
пакетов.

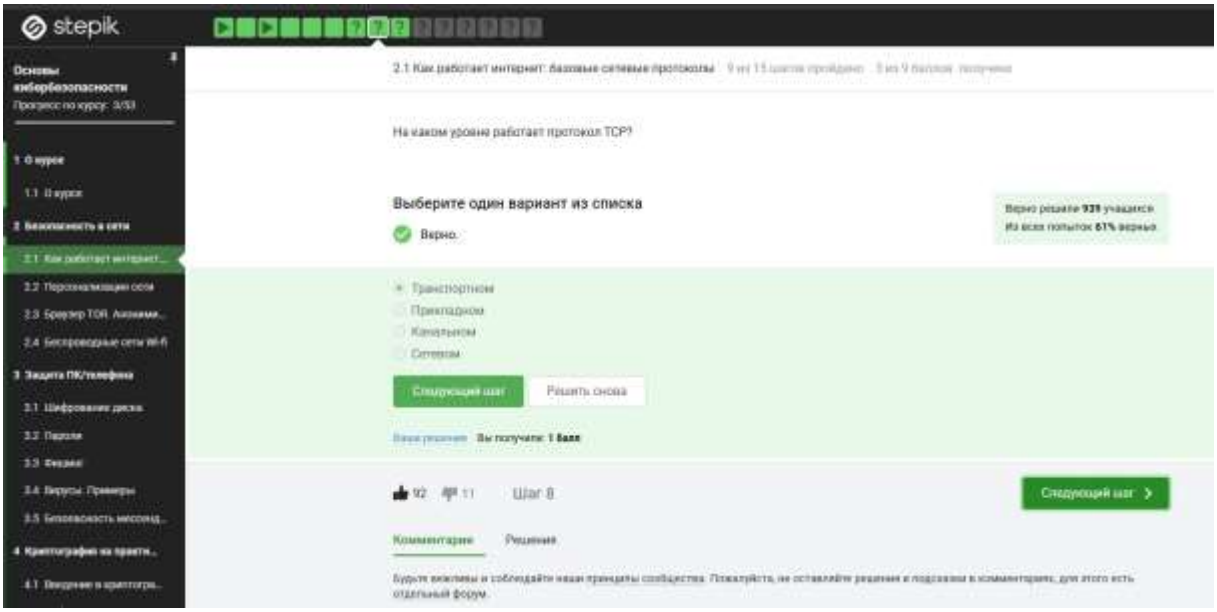
Транспортный уровень работает над следующим уровнем модели TCP, так называемым сетевым или межсетевым уровнем. В этом уровне принимает участие не только программа, не только наша машина, но уже наш роутер, то есть то устройство, к которому мы подключаемся, чтобы получить интернет. Сетевой уровень ответственен за передачу данных между различными физическими сетями; так, например, мы можем подключиться с компьютера, подключаясь через WiFi-сеть, к другому компьютеру, который, быть может, подключен через проводной интернет.

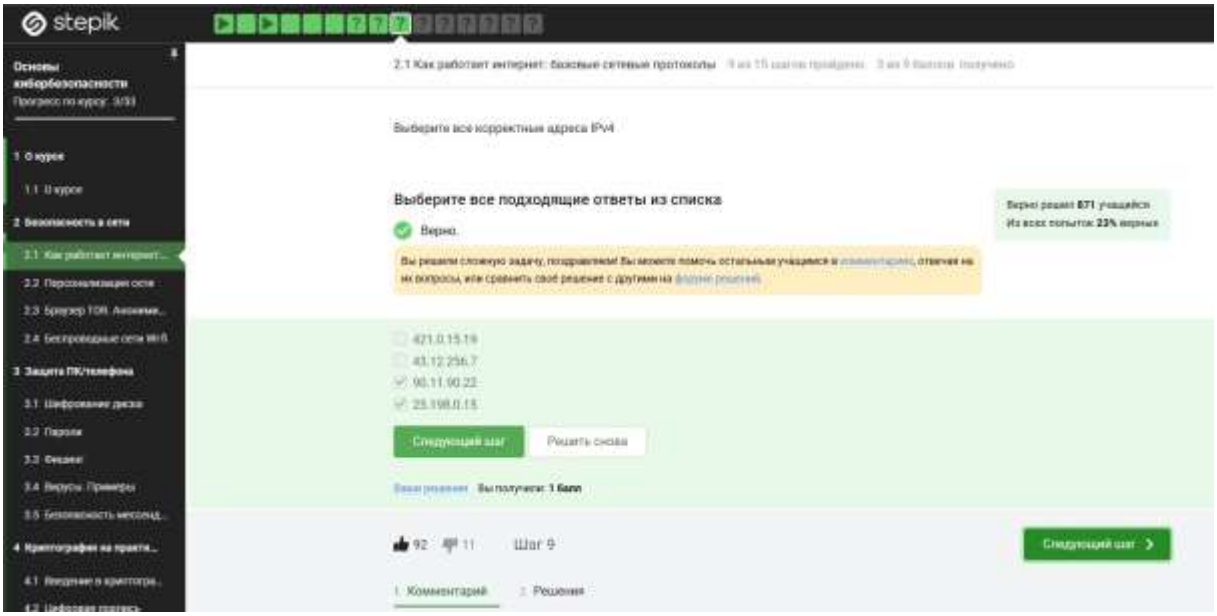
Сетевой уровень работает над так называемым канальным уровнем или самым низким уровнем модели TCP/IP. И в этой модели работает уже физика. Здесь происходит физическая передача данных. И здесь мы уже будем говорить о пропускной способности канала, об обеспечении помехоустойчивости, и основные примеры протоколов канального уровня непосредственно связаны с тем, как мы передаем данные.

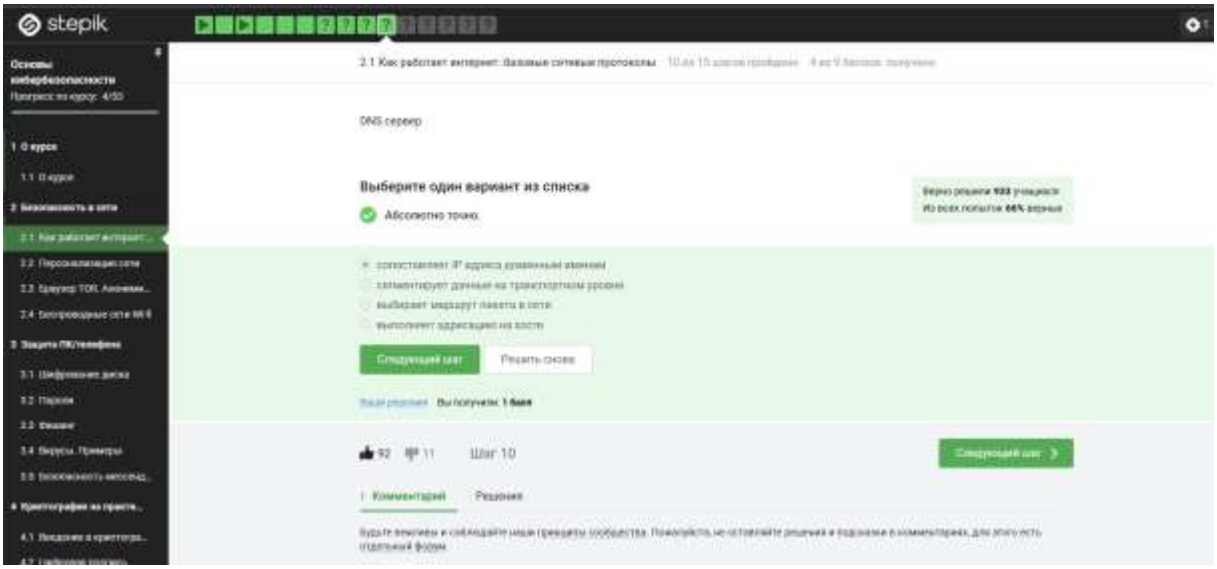
Вот эти четыре уровня модели TCP/IP и происходят между тем, как мы запросили на нашей машине открыть какую-то веб-страницу. То есть наш запрос происходит через прикладной уровень от браузера в транспортный уровень, который понимает, что это идет от браузера, в сеть, которая нам говорит, что мы хотим получить такой-то веб-сайт. И мы передаем всю эту информации в виде бит, в виде потока данных в сеть. И для того, чтобы получить назад ответ, происходит ровно тот же самый протокол, тот же самый алгоритм.

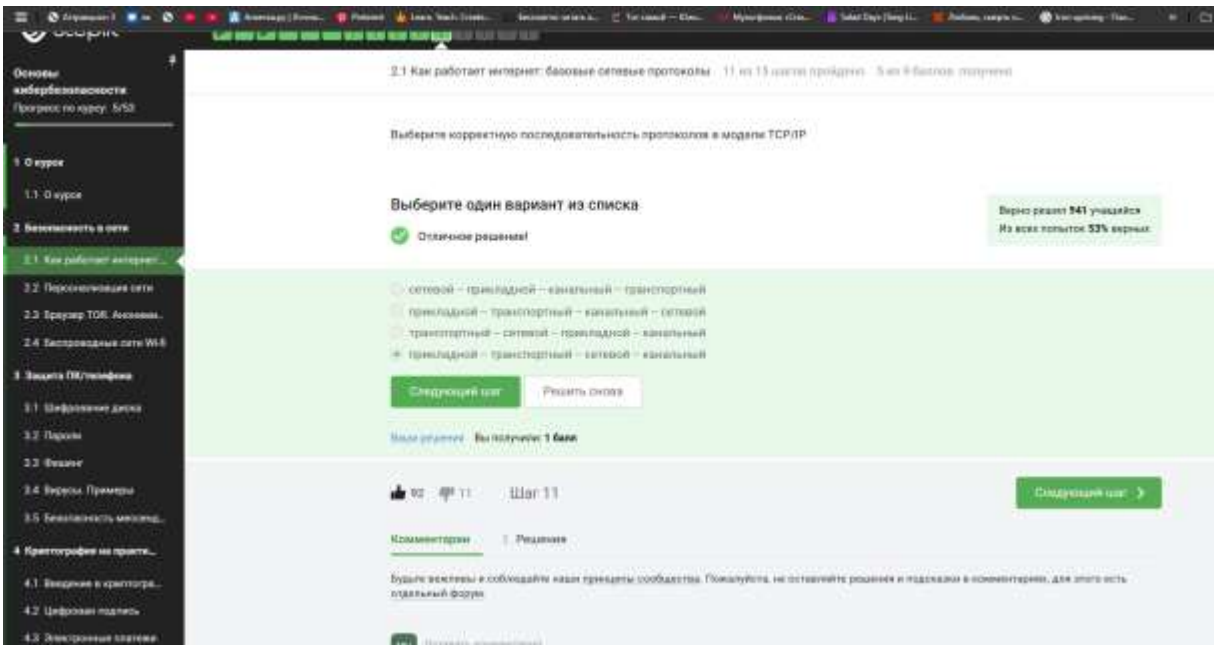
Прохождение тестовой части:

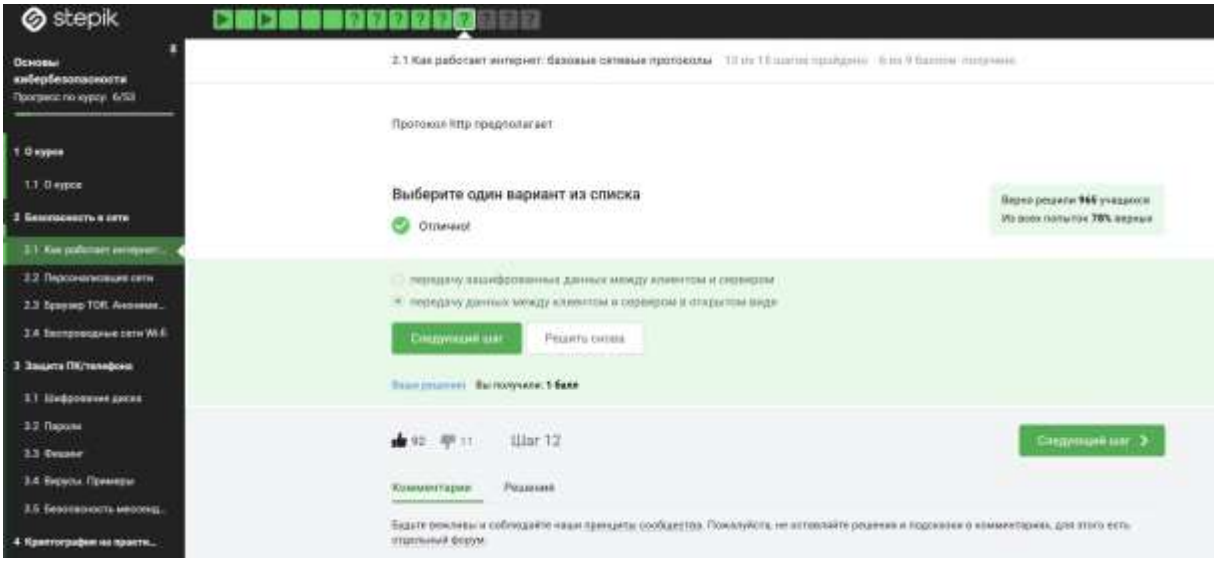

stepik
Основы кибербезопасности
2.1 Как работает интернет: базовые сетевые протоколы
Выберите протокол прикладного уровня
Выберите один вариант из списка
Верно. Так держать!
UDP
TCP
HTTPS
IP
Следующий шаг
Решить снова
Шаг 7
Следующий шаг
Комментарии
Решения

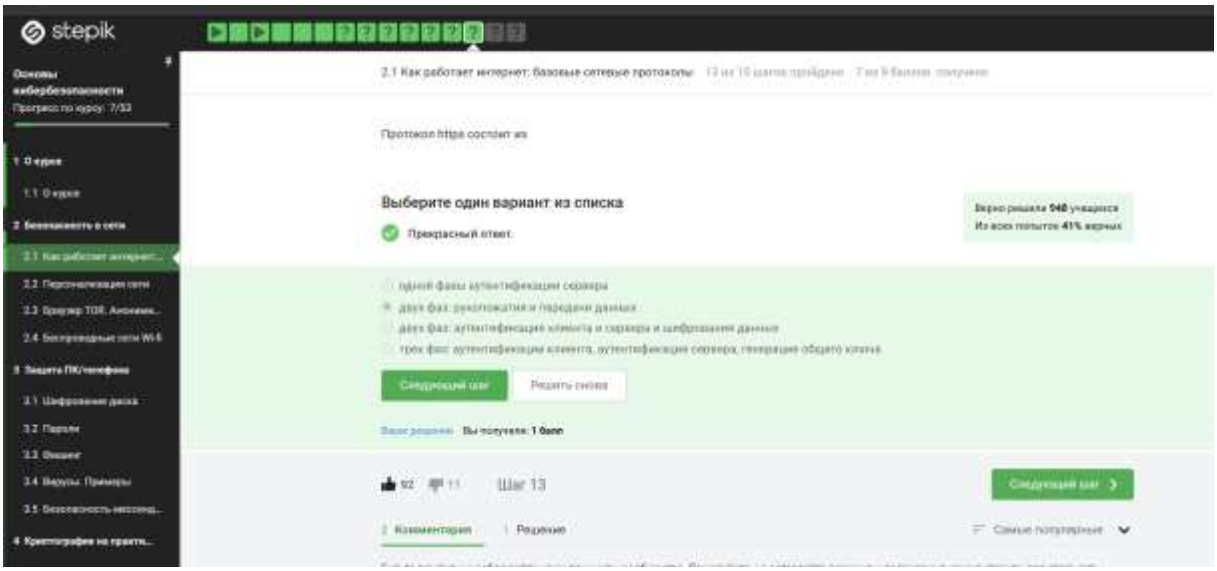

stepik
Основы кибербезопасности
2.1 Как работает интернет: базовые сетевые протоколы
На каком уровне работает протокол TCP?
Выберите один вариант из списка
Верно.
Транспортном
Прикладном
Канальном
Сетевом
Следующий шаг
Решить снова
Шаг 8
Следующий шаг
Комментарии
Решения

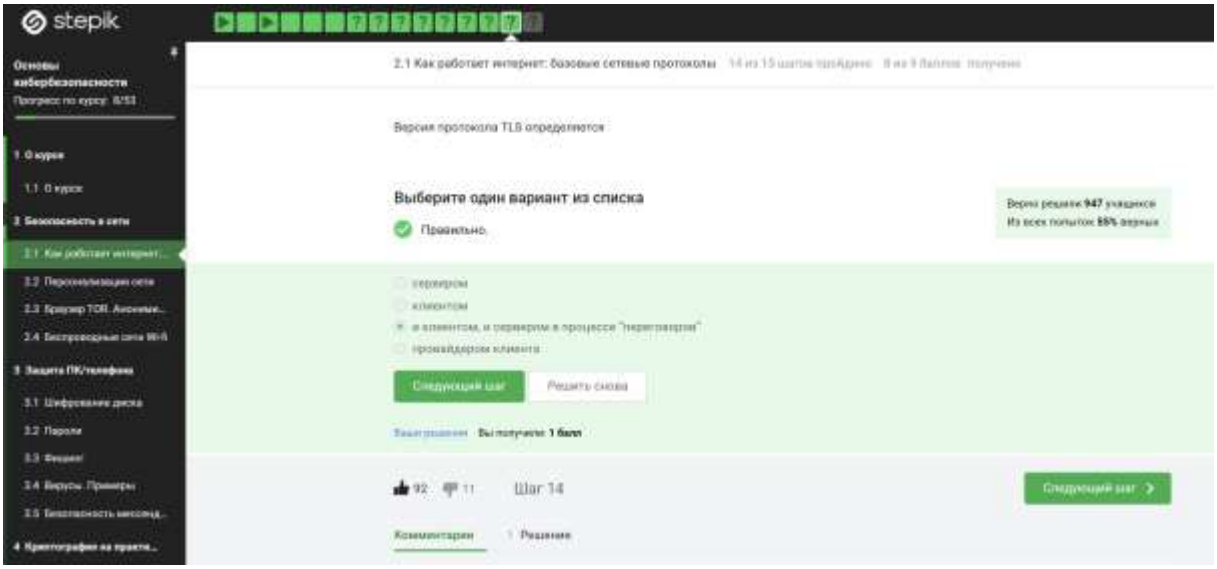

stepik
Выберите все подходящие ответы из списка
Верно.
Следующий шаг
Решать снова
Шаг 9
Комментарий
Решения

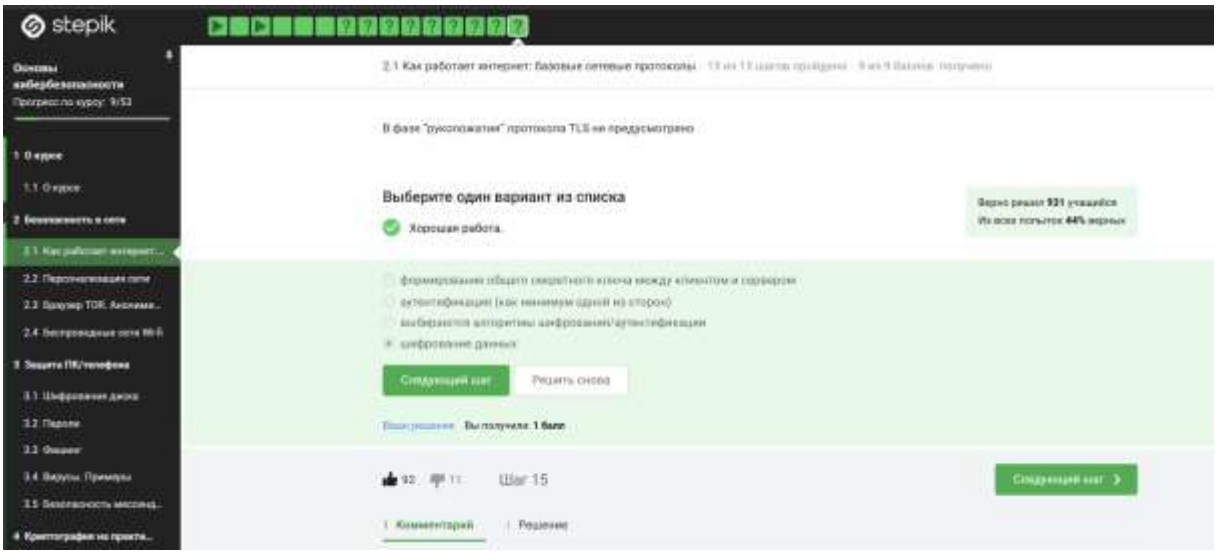

stepik
DNS сервер
Выберите один вариант из списка
Абсолютно точно.
Следующий шаг
Решать снова
Шаг 10
Комментарий
Решения


Основы кибербезопасности
Прогресс по курсу: 5/53
2.1 Как работает интернет: базовые сетевые протоколы
Выберите корректную последовательность протоколов в модели TCP/IP
Выберите один вариант из списка
Отличное решение!
Верно решил 541 учащийся
Из всех попыток 53% верных
сетевой – прикладной – канальный – транспортный
прикладной – транспортный – канальный – сетевой
транспортный – сетевой – прикладной – канальный
прикладной – транспортный – сетевой – канальный
Следующий шаг
Решить снова
Ваше решение Вы получили: 1 балл
92 11 Шаг 11
Следующий шаг
Комментарии 1 Решения
Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум


stepik
Основы кибербезопасности
Прогресс по курсу: 6/53
2.1 Как работает интернет: базовые сетевые протоколы
Протокол http предполагает
Выберите один вариант из списка
Отлично!
Верно решили 966 учащихся
Из всех попыток 78% верных
передачу зашифрованных данных между клиентом и сервером
передачу данных между клиентом и сервером в открытом виде
Следующий шаг
Решить снова
Ваше решение Вы получили: 1 балл
92 11 Шаг 12
Следующий шаг
Комментарии Решения
Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум

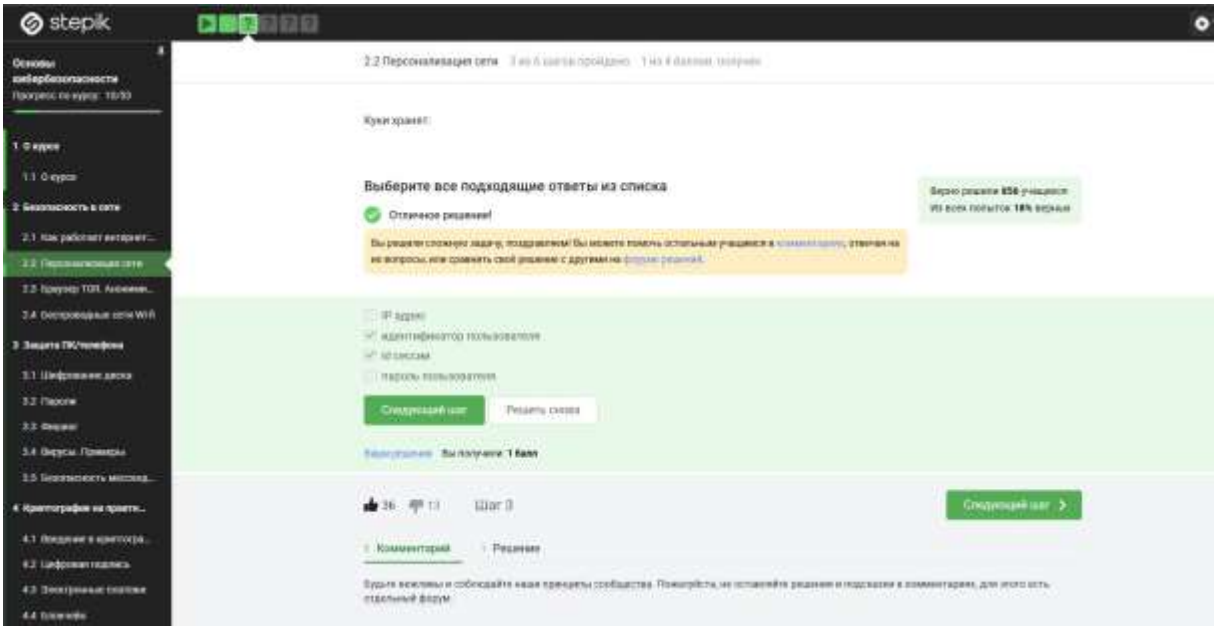

stepik
Основы кибербезопасности
Прогресс по курсу: 7/53
2.1 Как работает интернет: базовые сетевые протоколы
Протокол https состоит из
Выберите один вариант из списка
Прекрасный ответ
Верно решили 540 учащихся
Из всех попыток 41% верных
одной фазы аутентификации сервера
двух фаз: рукопожатия и передачи данных
двух фаз: аутентификации клиента и сервера и шифрования данных
трех фаз: аутентификации клиента, аутентификации сервера, генерации общего ключа
Следующий шаг
Решить снова
Ваше решение Вы получили: 1 балл
92 11 Шаг 13
Следующий шаг
Комментарии Решения
Самые популярные

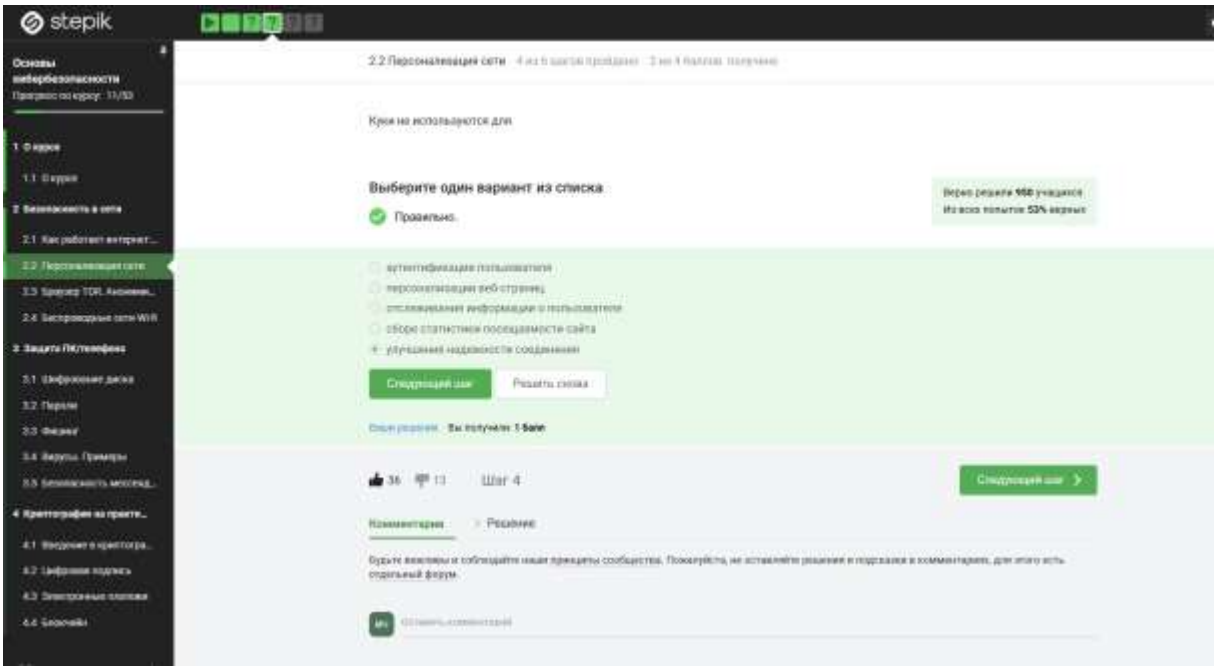


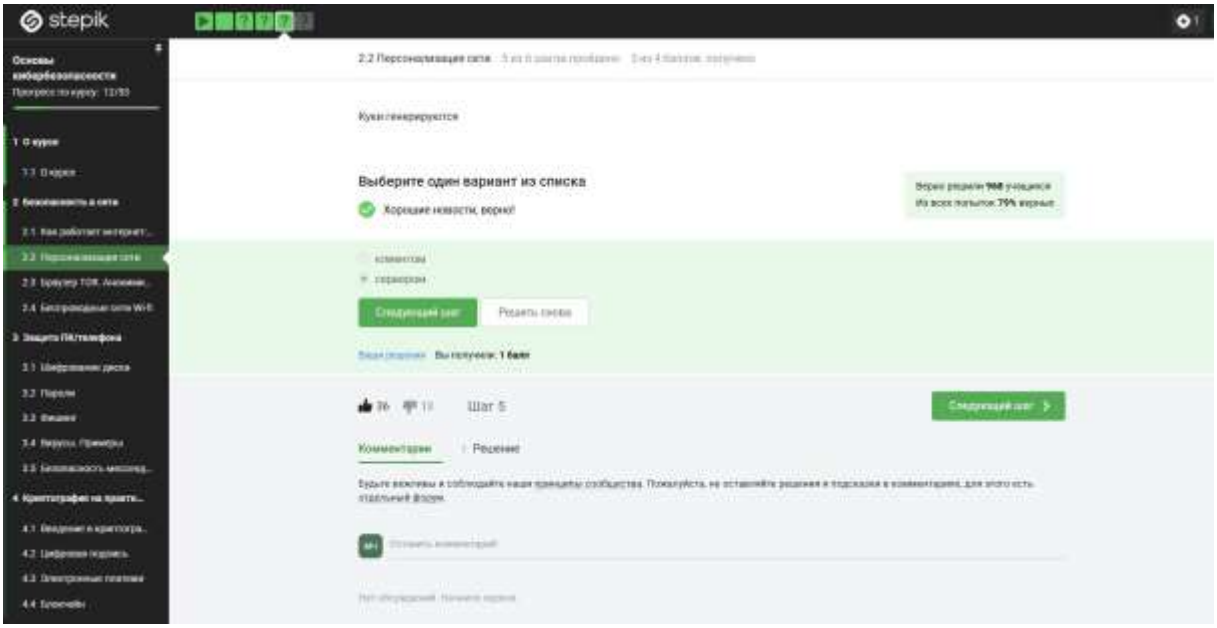


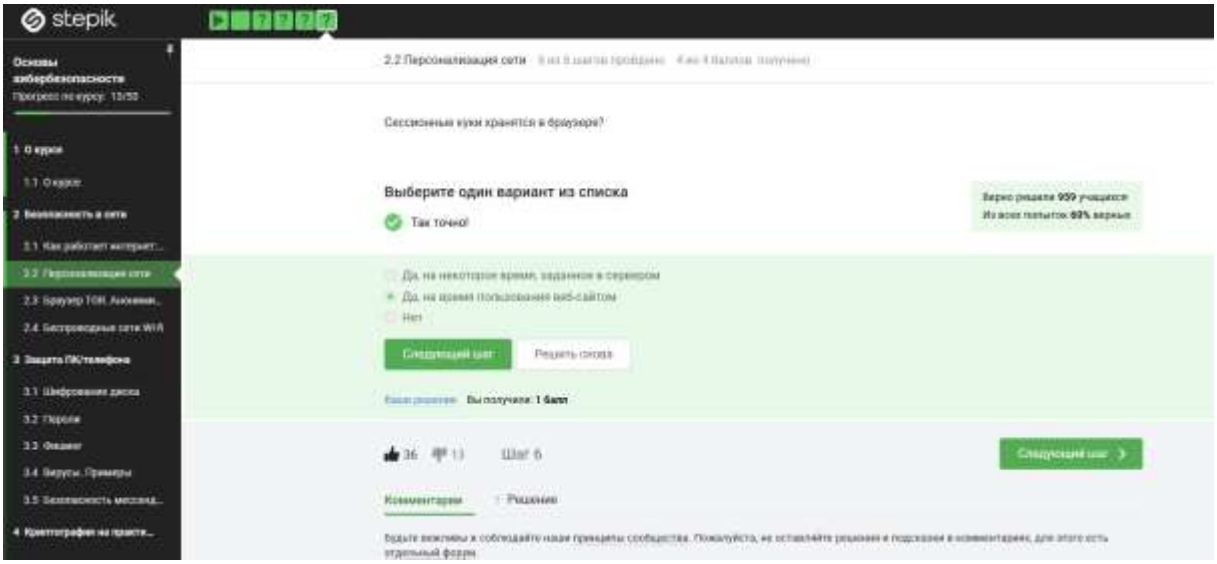
Персонализация сети

Прохождение тестовой части


stepik
Выберите все подходящие ответы из списка
Отличное решение!
Следующий шаг
Шаг 3
Комментарий
Решение

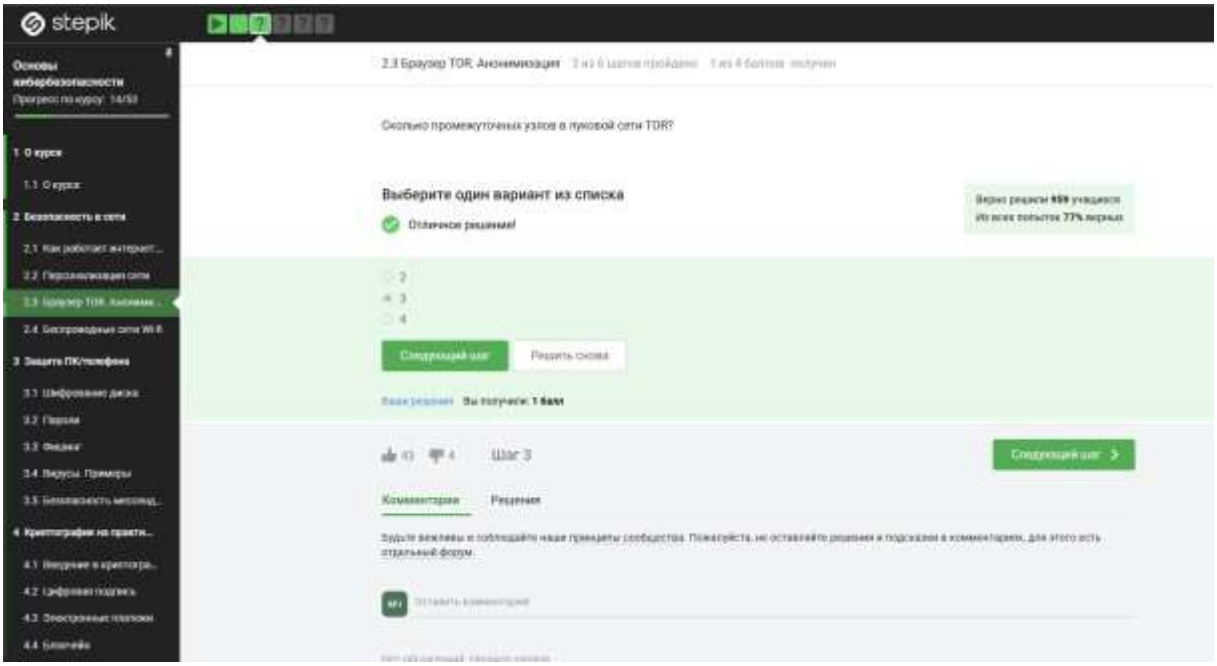

stepik
Выберите один вариант из списка
Правильно.
Следующий шаг
Шаг 4
Комментарии
Решение

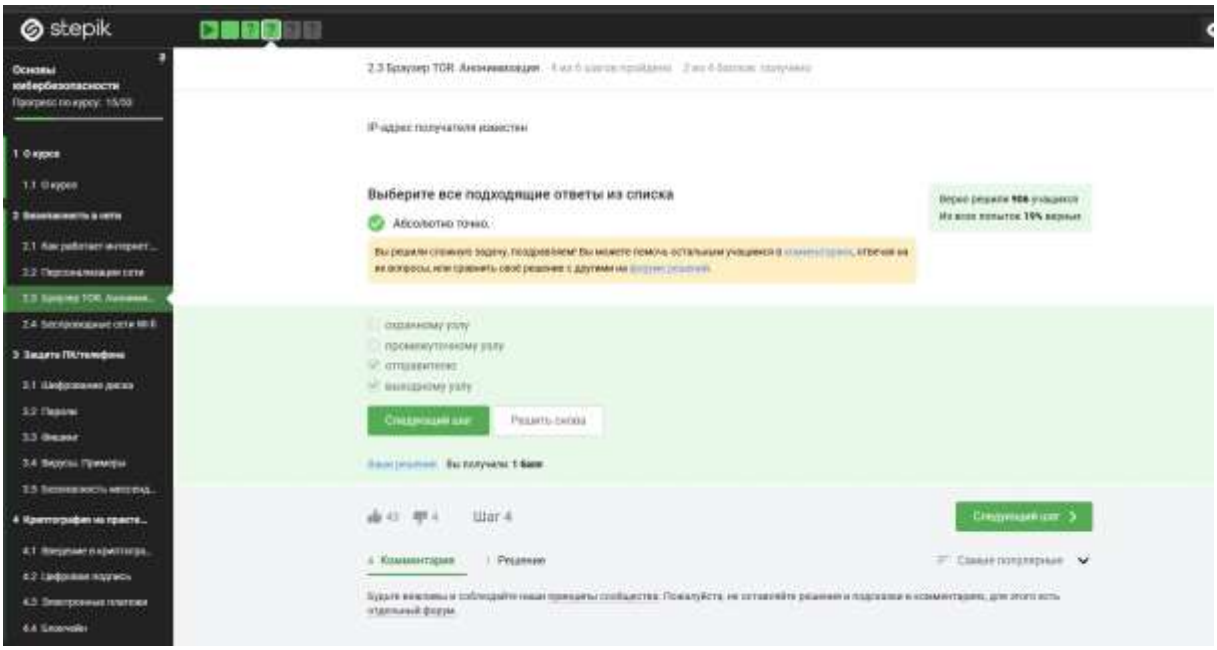


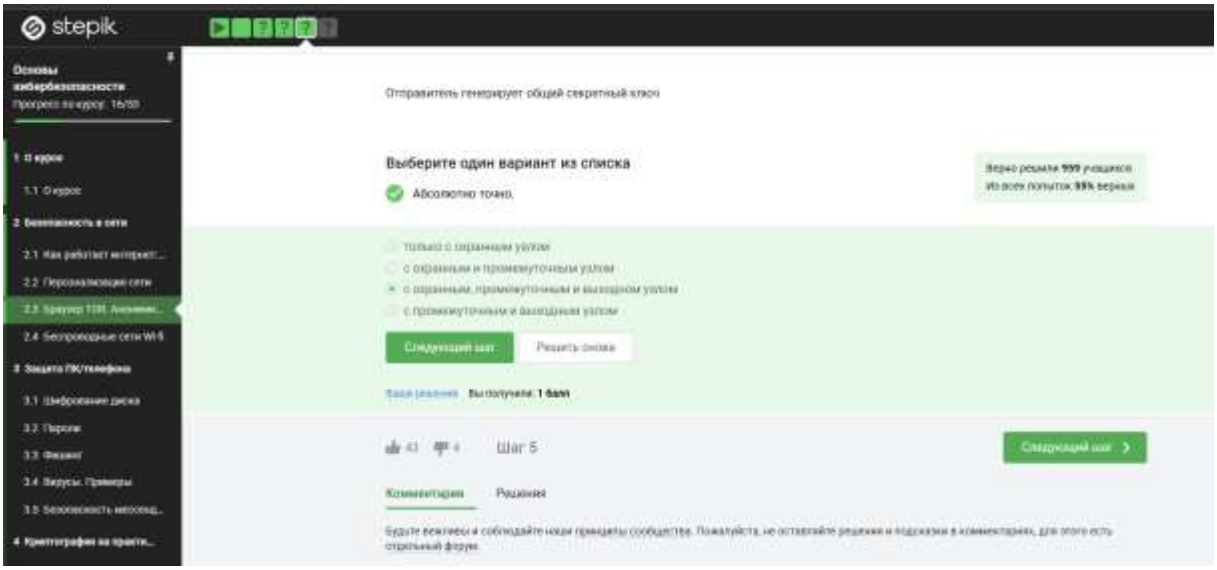


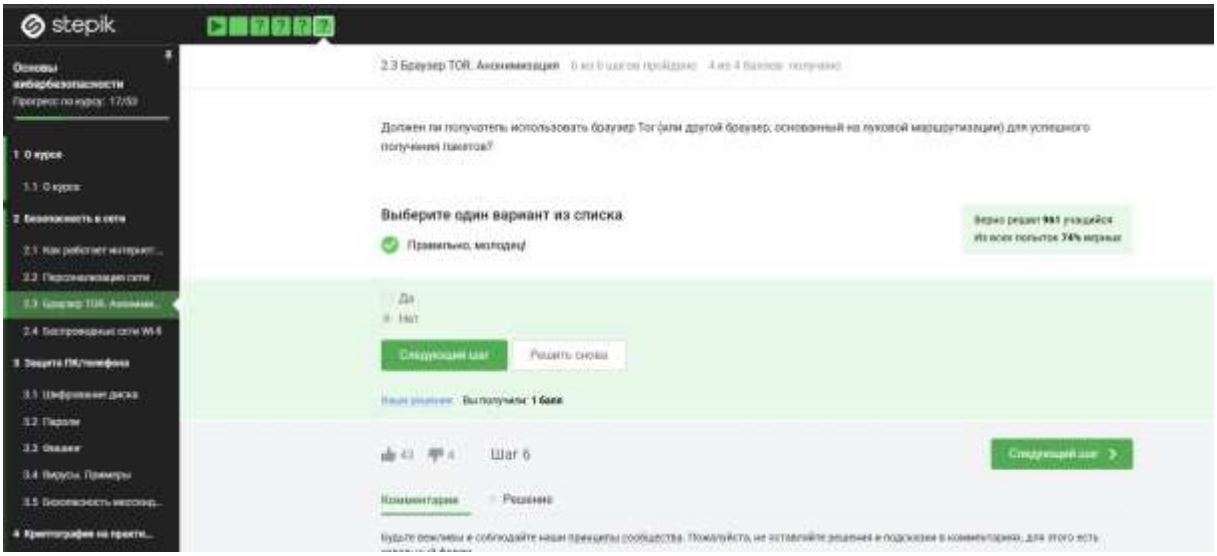
Браузер TOR. Анонимизация

Выполнение тестовой части:


stepik
Основы кибербезопасности
2.3 Браузер TOR. Анонимизация
Сколько промежуточных узлов в луковой сети TOR?
Выберите один вариант из списка
Отличное решение!
Следующий шаг
Решить снова
Вы получили: 1 балл
Шаг 3
Следующий шаг
Комментарии
Решения

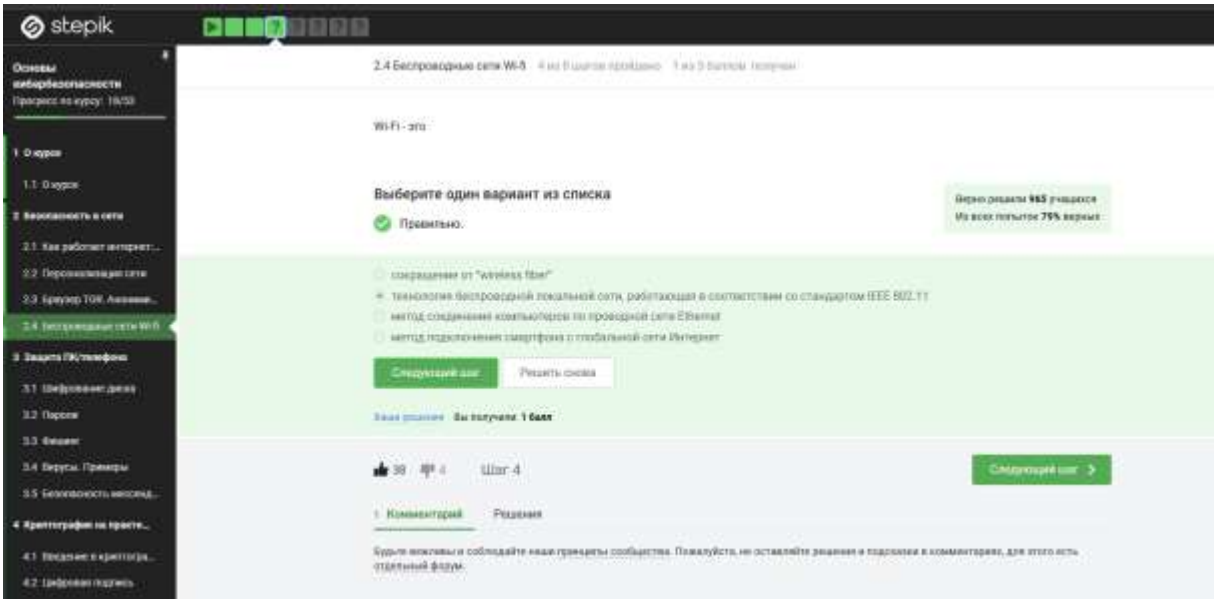

stepik
Основы кибербезопасности
2.3 Браузер TOR. Анонимизация
IP-адрес получателя известен
Выберите все подходящие ответы из списка
Абсолютно точно.
Следующий шаг
Решить снова
Вы получили: 1 балл
Шаг 4
Следующий шаг
Комментарии
Решения

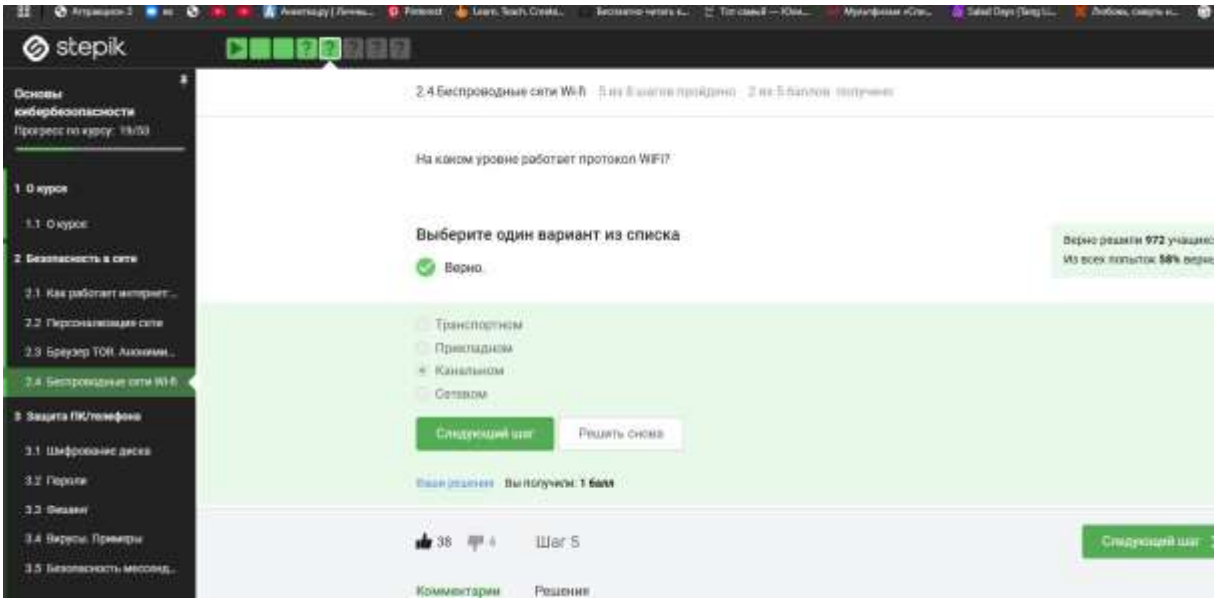


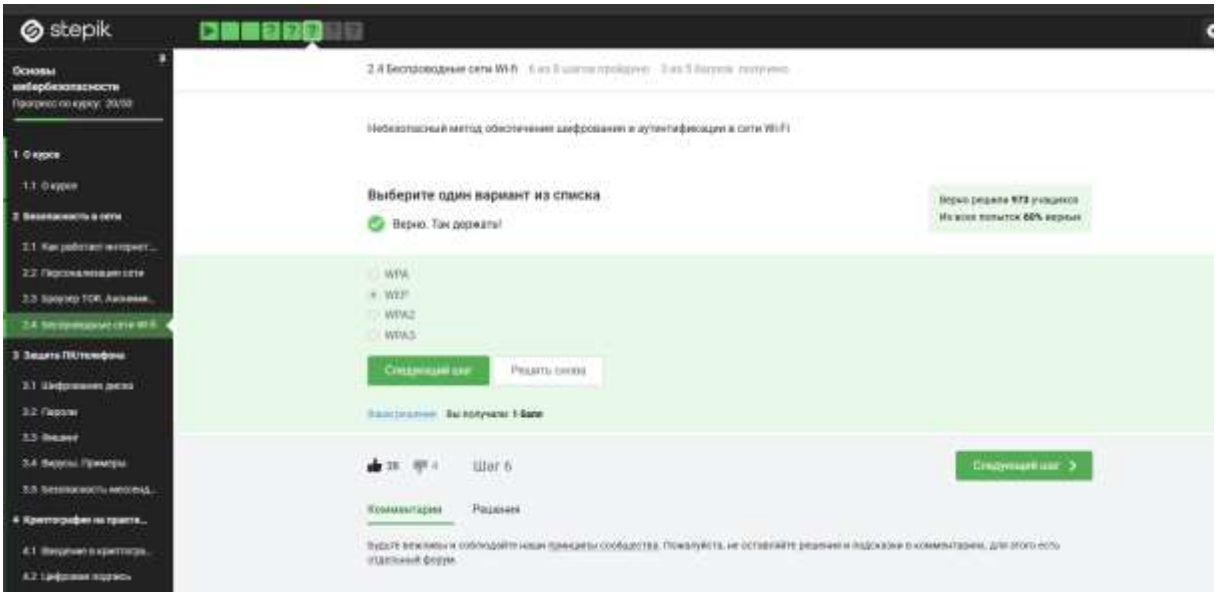


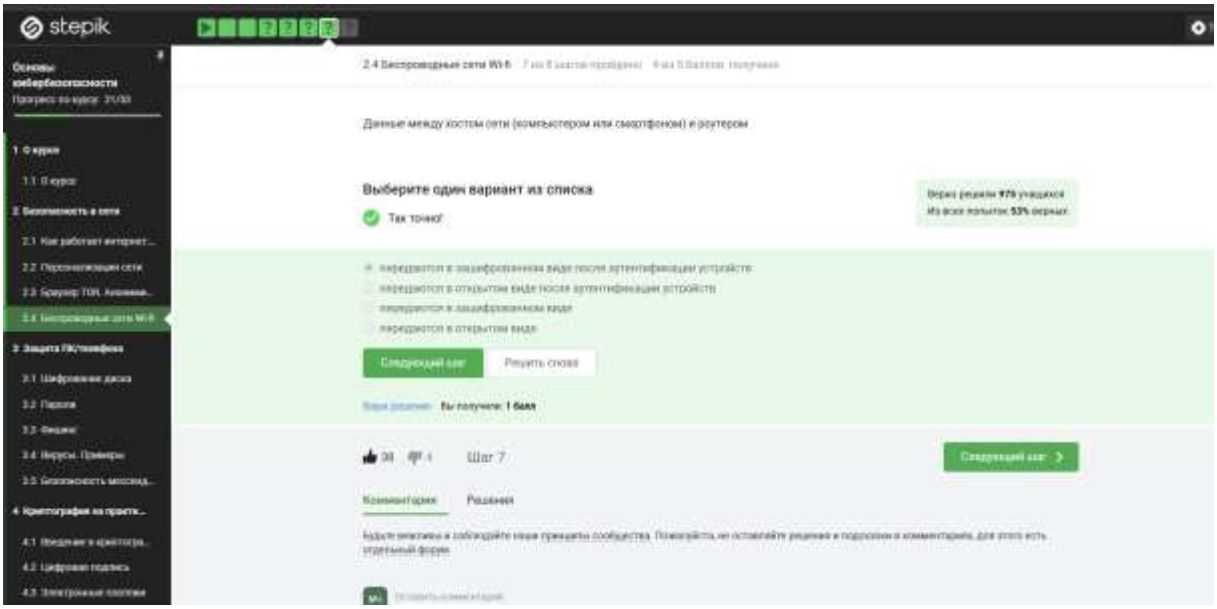
Беспроводные сети Wi-fi

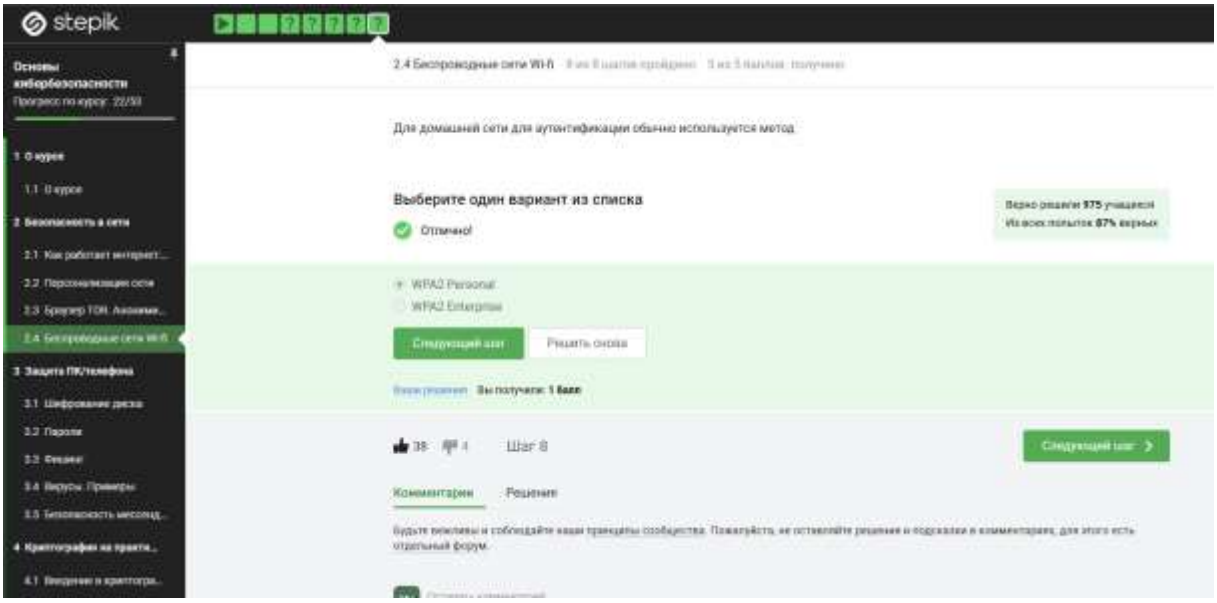
Выполнение тестовой части:


stepik
Основы кибербезопасности
2.4 Беспроводные сети Wi-fi
Выберите один вариант из списка
Правильно.
Следующий шаг
Решить снова
Шаг 4
Комментарий
Решения


stepik
Основы кибербезопасности
2.4 Беспроводные сети Wi-fi
На каком уровне работает протокол WIFI?
Выберите один вариант из списка
Верно.
Транспортном
Прикладном
Канальном
Сетевом
Следующий шаг
Решить снова
Шаг 5
Комментарии
Решения


stepik
Основы кибербезопасности
2.4 Беспроводные сети Wi-fi
Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi
Выберите один вариант из списка
Верно. Так держать!
WPA
WEP
WPA2
WPA3
Следующий шаг
Решить снова
Вы получили: 1 балл
Шаг 6
Следующий шаг
Комментарии
Решения


stepik
Основы кибербезопасности
Данные между хостом сети (компьютером или смартфоном) и роутером
Выберите один вариант из списка
Так точно!
передаются в зашифрованном виде после аутентификации устройств
передаются в открытом виде после аутентификации устройств
передаются в зашифрованном виде
передаются в открытом виде
Следующий шаг
Решить снова
Вы получили: 1 балл
Шаг 7
Следующий шаг
Комментарии
Решения



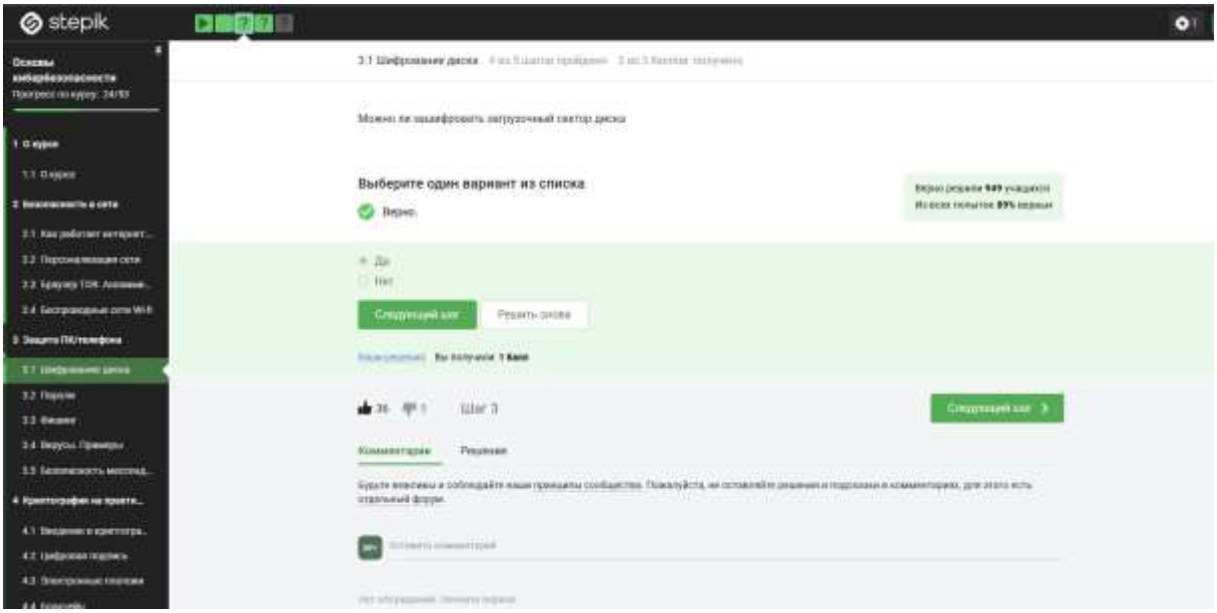
2 часть. Защита ПК/телефона

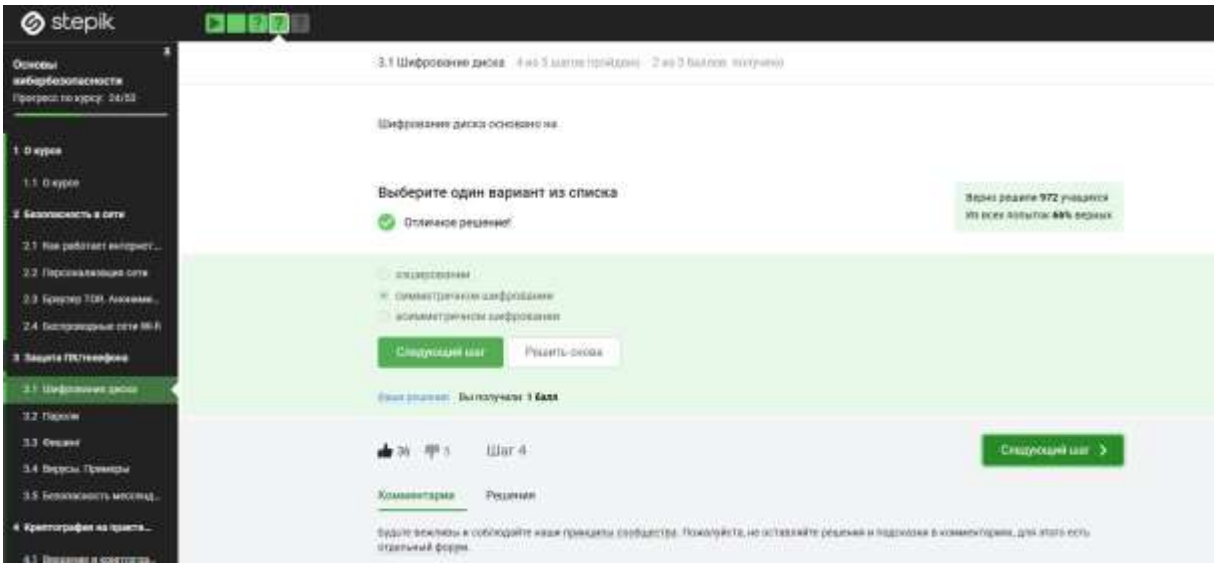
Шифрование диска

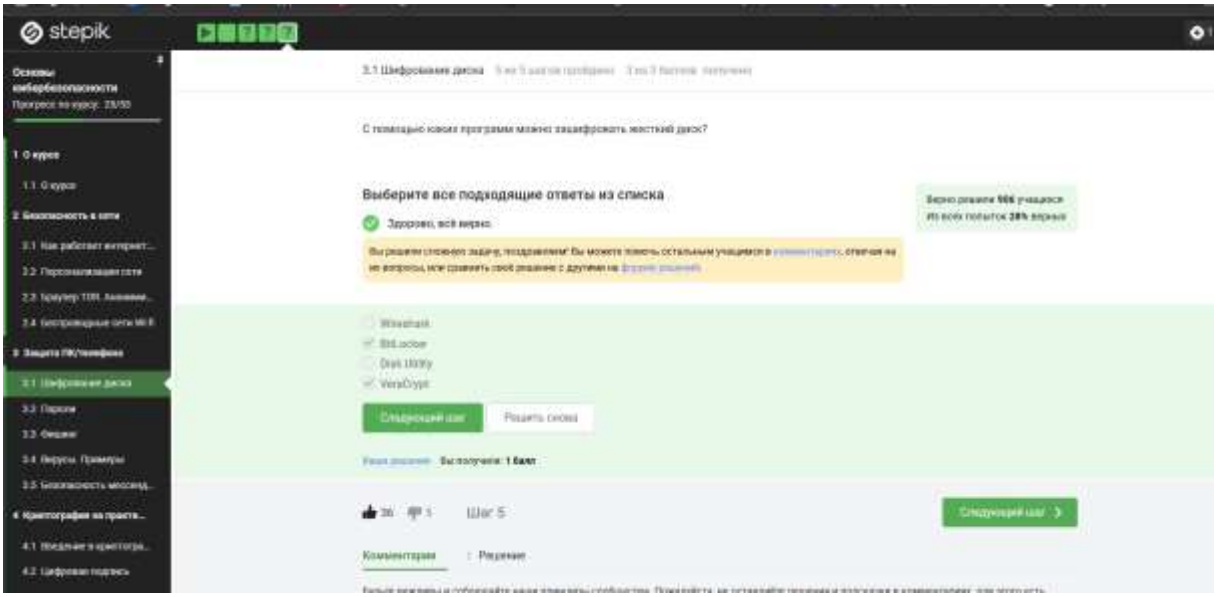
В этой лекции мы с вами поговорим о том, как шифруются носители информации и зачем это нужно. Зачем же шифровать жесткий диск, спросите вы. И ответ на этот вопрос довольно прост - шифровать жесткий диск нужно для того, чтобы избежать утечки наших персональных данных в случае утери или кражи нашего ноутбука. По статистике, это одна из основных причин утечки каких-то конфиденциальных данных типа наших паролей и каких-то документов, и шифрование жесткого диска позволяет избежать этих утечек. То есть, если злоумышленник получит физический доступ к вашему компьютеру или ноутбуку, не зная пароля, то есть не зная ключа шифрования, он не сможет получить доступ к вашим файлам. Вообще, эта политика шифрования жесткого диска часто является обязательной для таких серьезных компаний, как Яндекс, Google или в некоторых университетах. Сотрудники обязаны на своем корпоративном ноутбуке шифровать жесткий диск.

Рассмотрим, как это работает. Если не углубляться в детали, то шифрование жесткого диска происходит в три этапа. На самом первом этапе пользователь с помощью какой-то из утилит (про утилиты мы говорим позднее) генерирует ключ для шифрования.

Прохождение тестовой части:

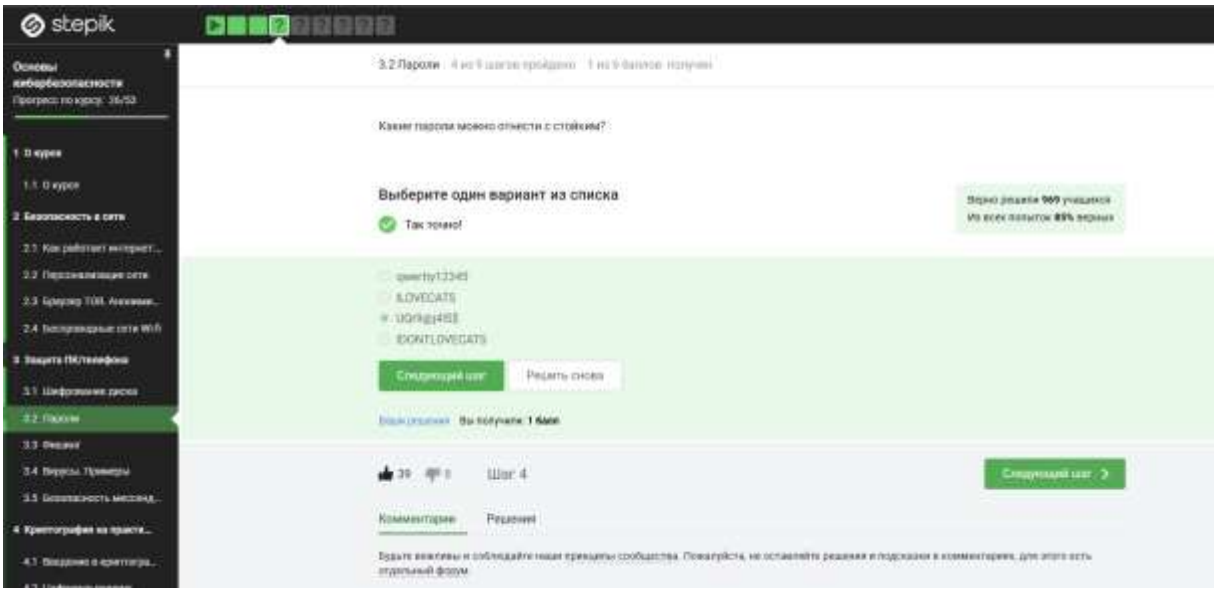


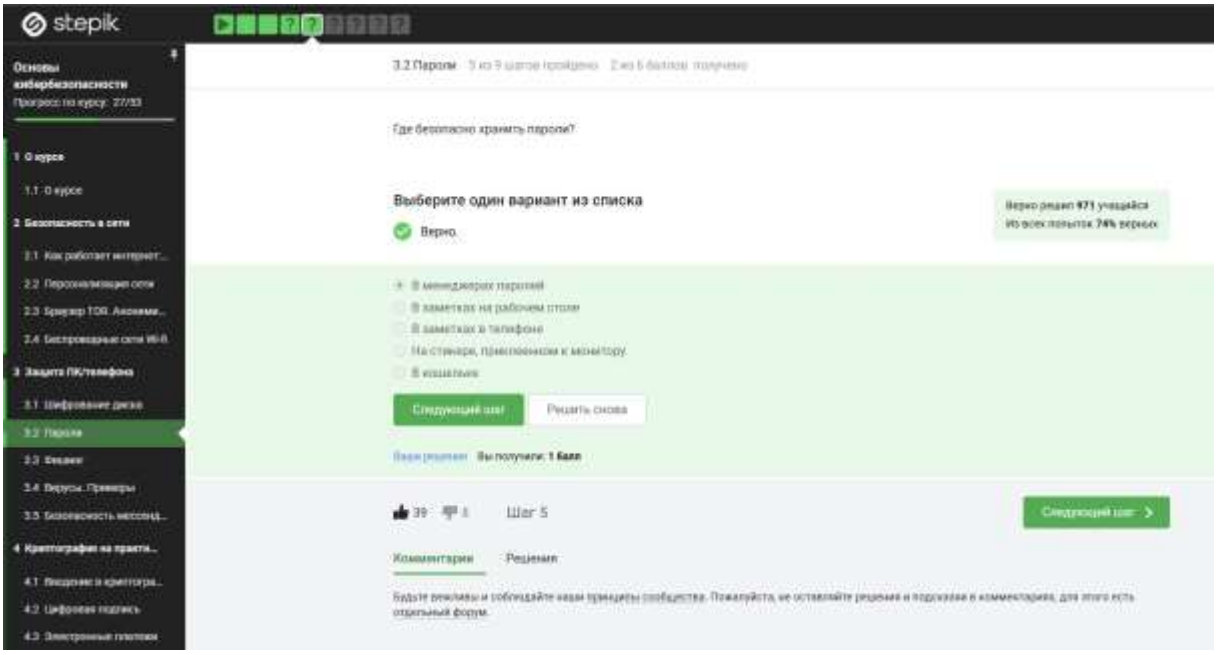


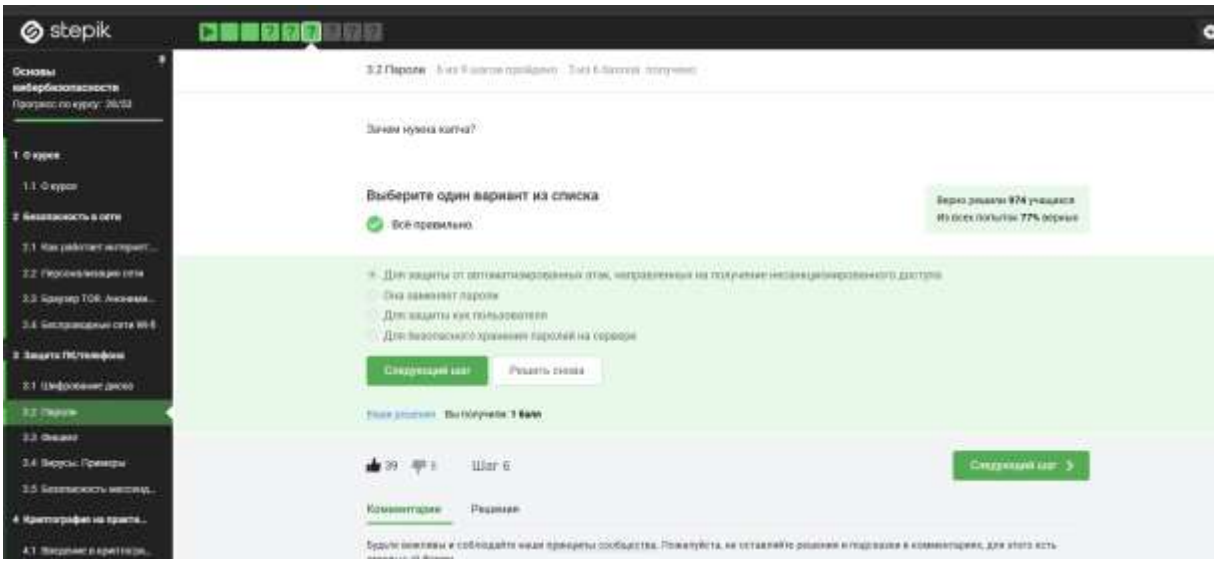


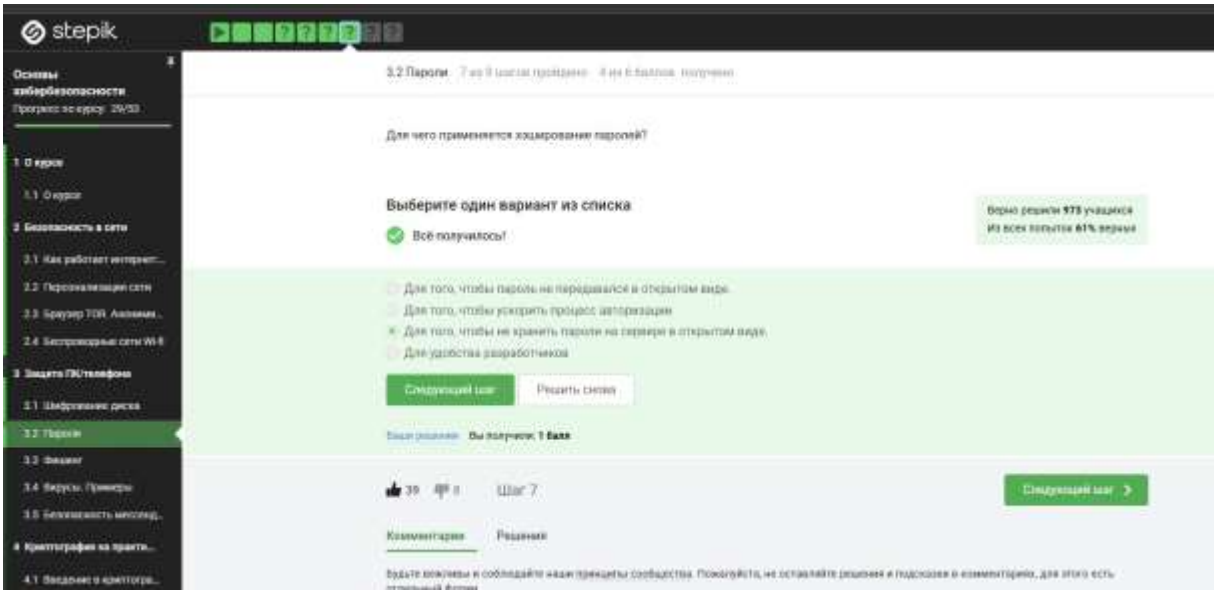
Пароли

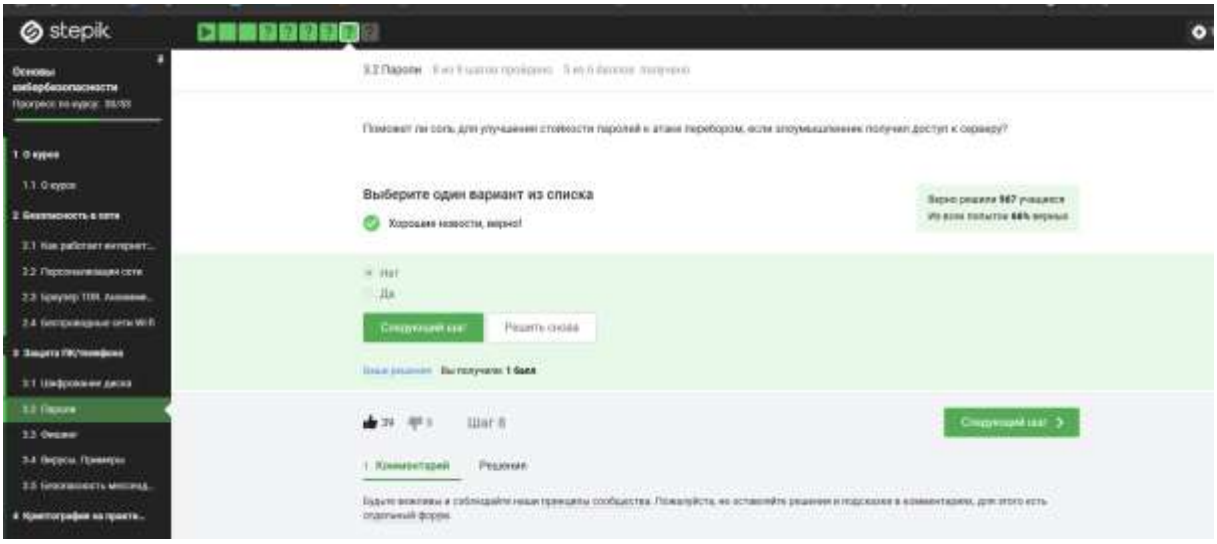
Прохождение тестовой части:

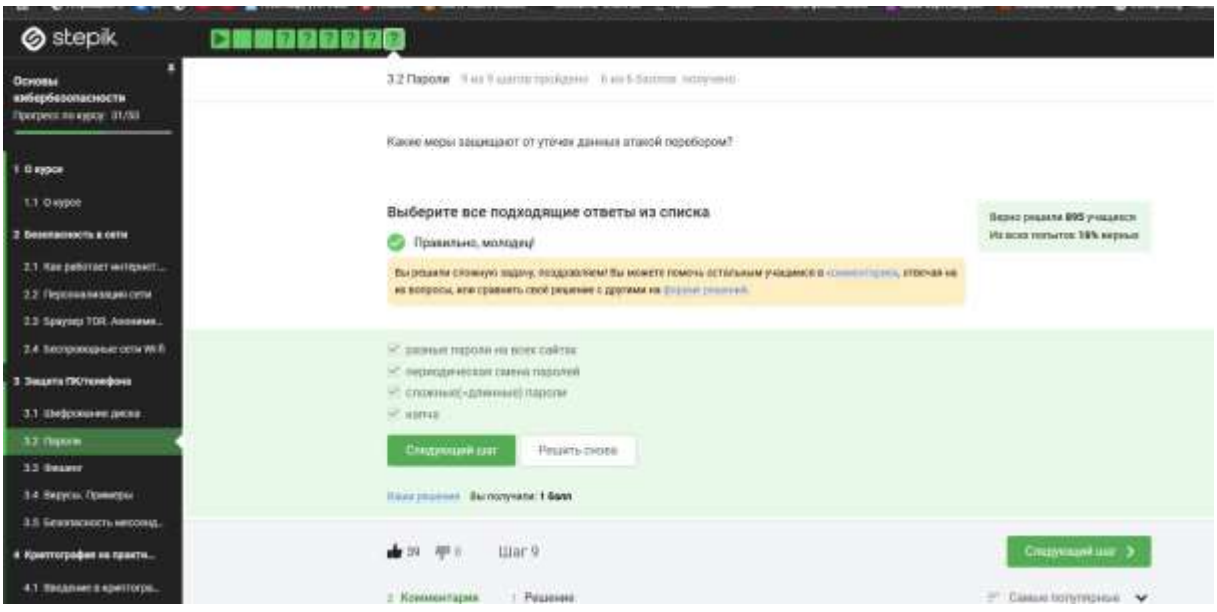



stepik
Основы кибербезопасности
Где безопасно хранить пароли?
Выберите один вариант из списка
Верно
Следующий шаг
Решать снова
Шаг 5
Комментарии
Решения


stepik
Основы кибербезопасности
Зачем нужна капча?
Выберите один вариант из списка
Всё правильно
Следующий шаг
Решать снова
Шаг 6
Комментарии
Решения

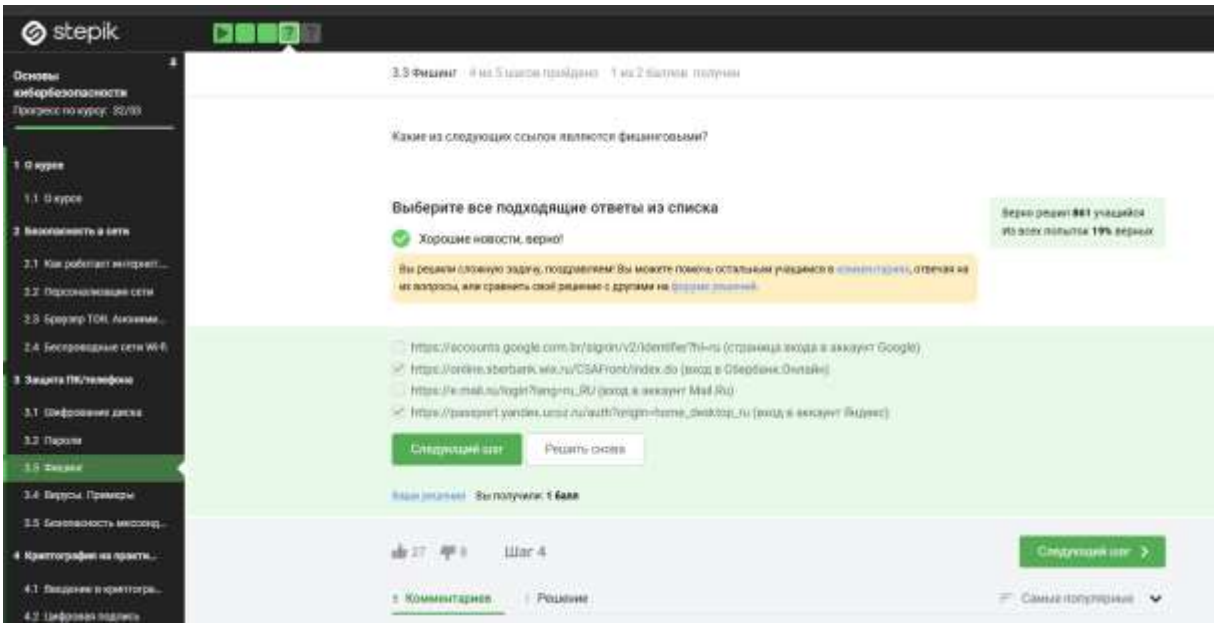

stepik
Основы кибербезопасности
3.2 Пароли
Для чего применяется хэширование паролей?
Выберите один вариант из списка
Всё получилось!
Для того, чтобы пароль не передавался в открытом виде.
Для того, чтобы ускорить процесс авторизации.
Для того, чтобы не хранить пароли на сервере в открытом виде.
Для удобства разработчиков
Следующий шаг
Решить снова
Шаг 7
Следующий шаг
Комментарии
Решения

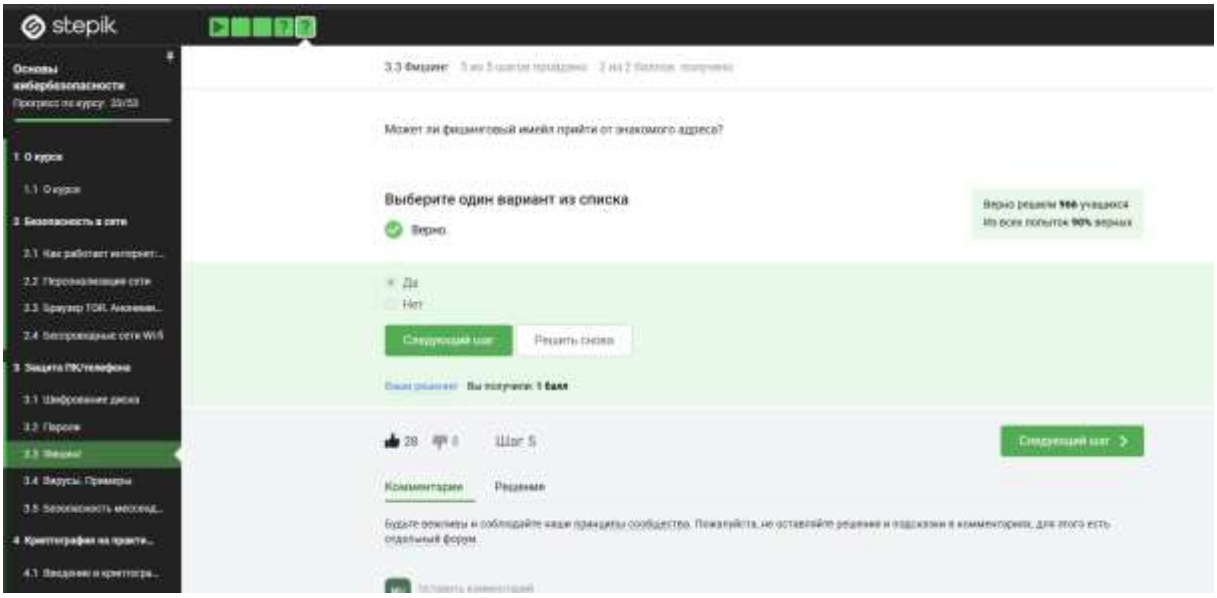

stepik
Основы кибербезопасности
3.2 Пароли
Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?
Выберите один вариант из списка
Хорошие новости, верно!
Нет
Да
Следующий шаг
Решить снова
Шаг 8
Следующий шаг
Комментарий
Решения


stepik
Основы кибербезопасности
3.2 Пароли
Какие меры защищают от утечки данных атакой перебором?
Выберите все подходящие ответы из списка
Правильно, молодец!
Следующий шаг
Решить снова
Шаг 9
Следующий шаг

Фишинг

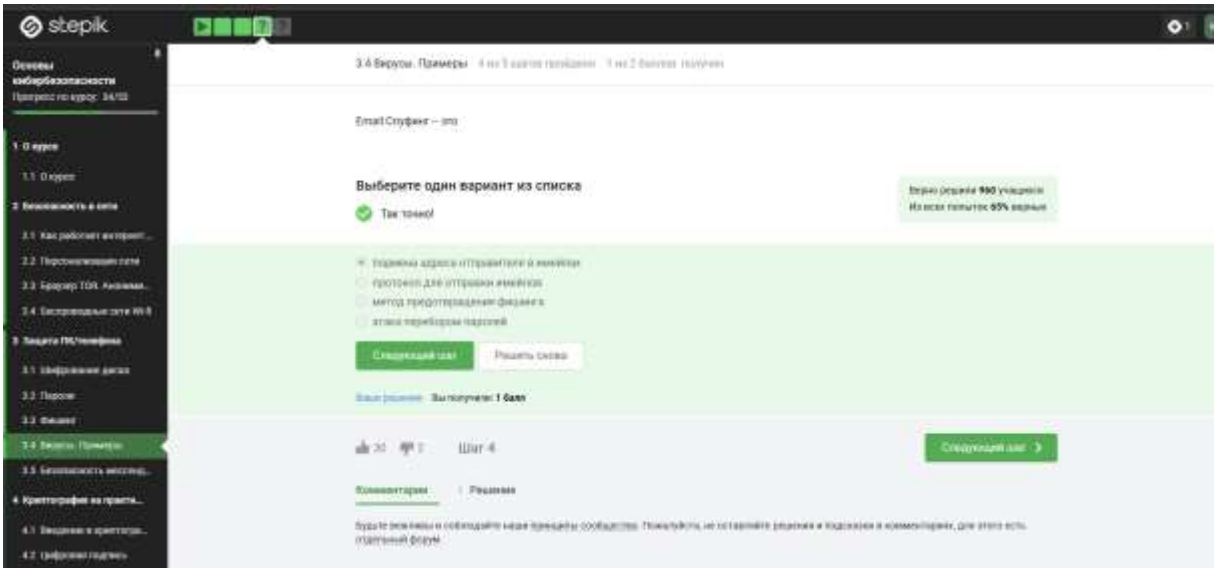
Прохождение тестовой части:

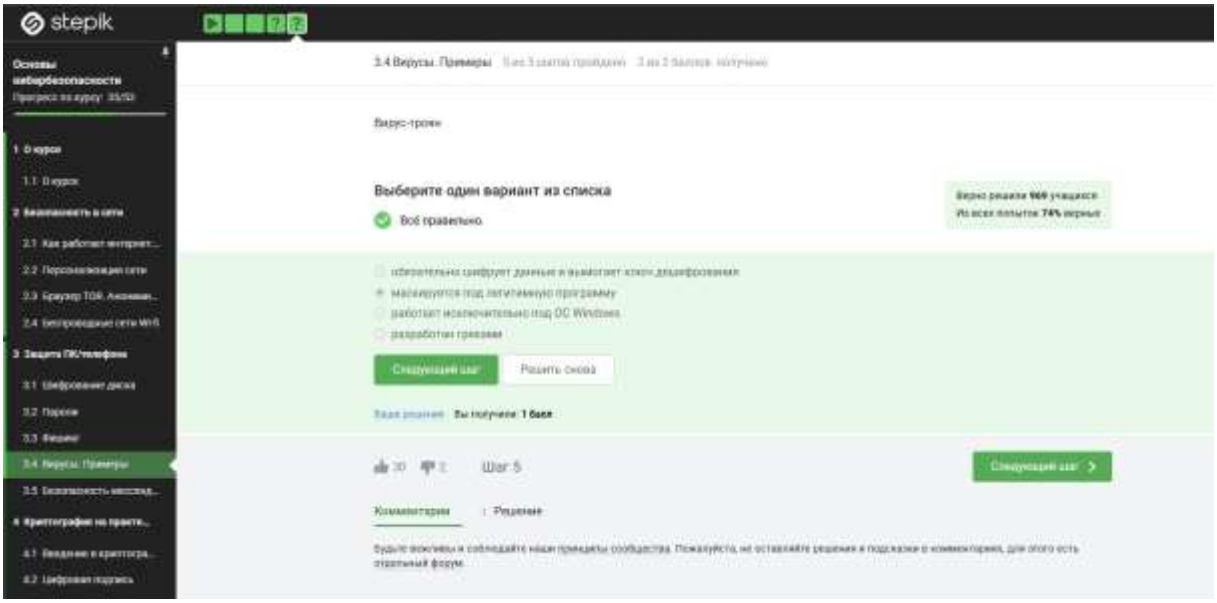




Вирусы. Примеры

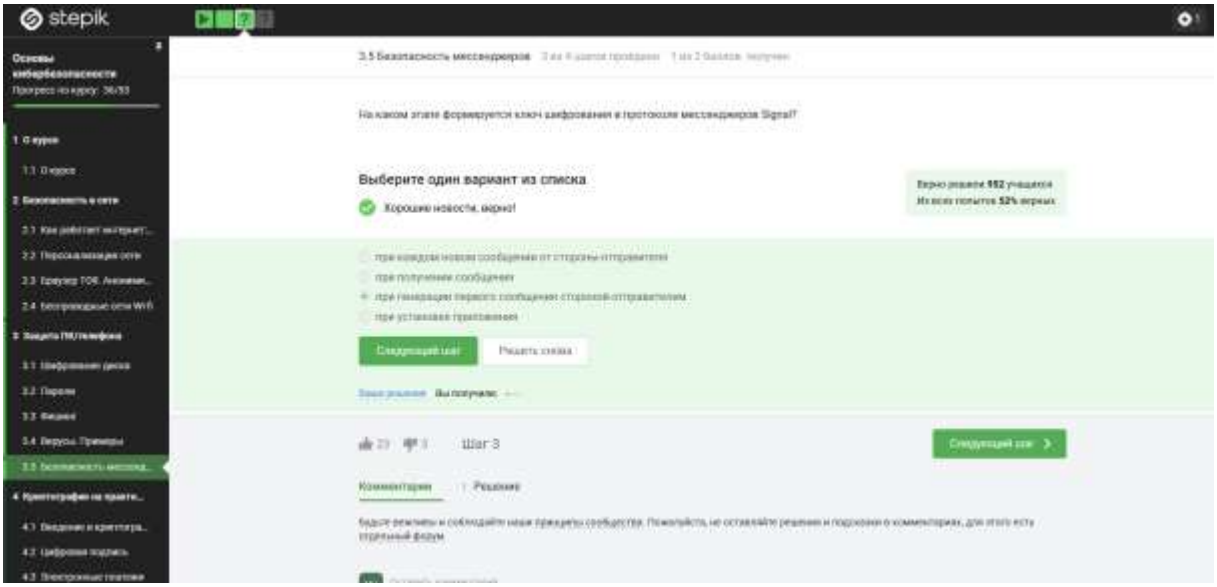
Прохождение тестовой части:

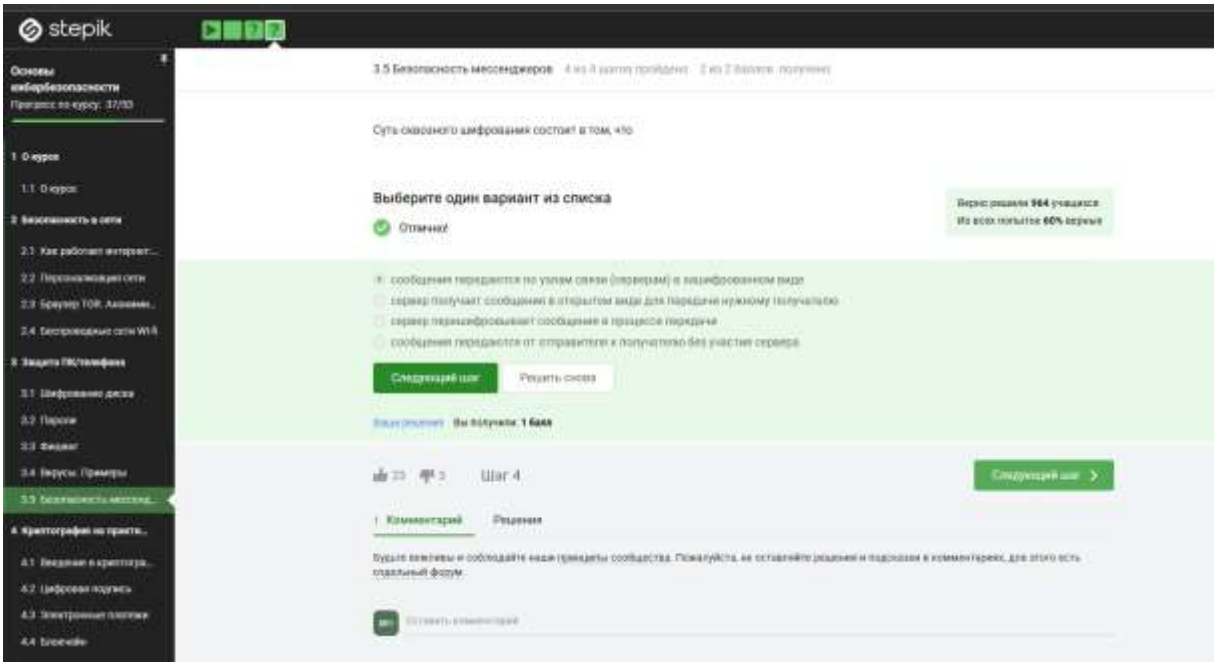




Безопасность мессенджеров

Прохождение тестовой части:





3 часть. Криптография на практике

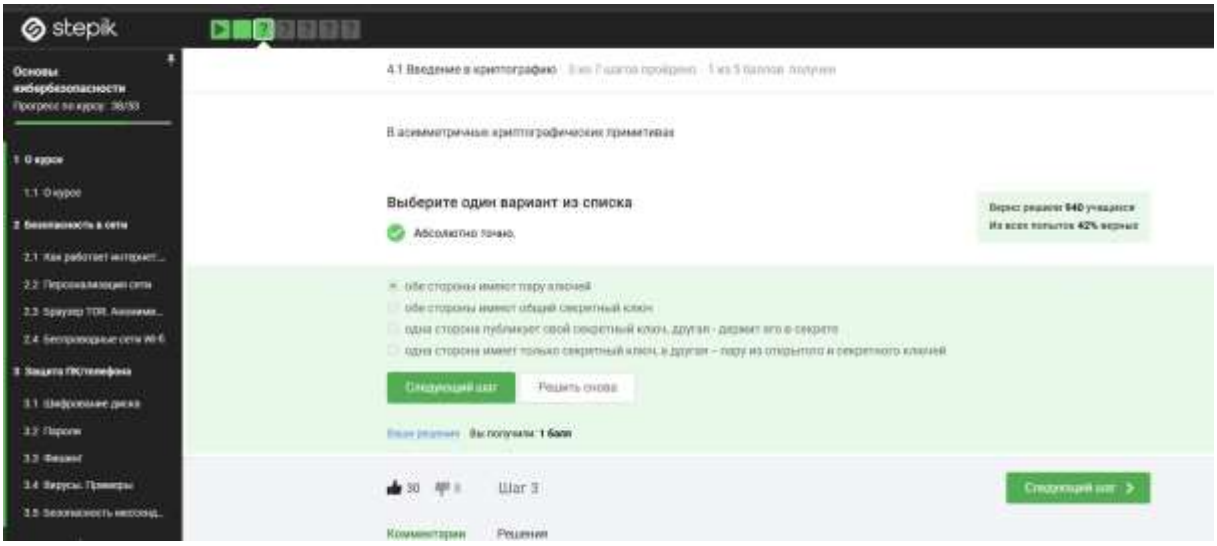
Введение в криптографию

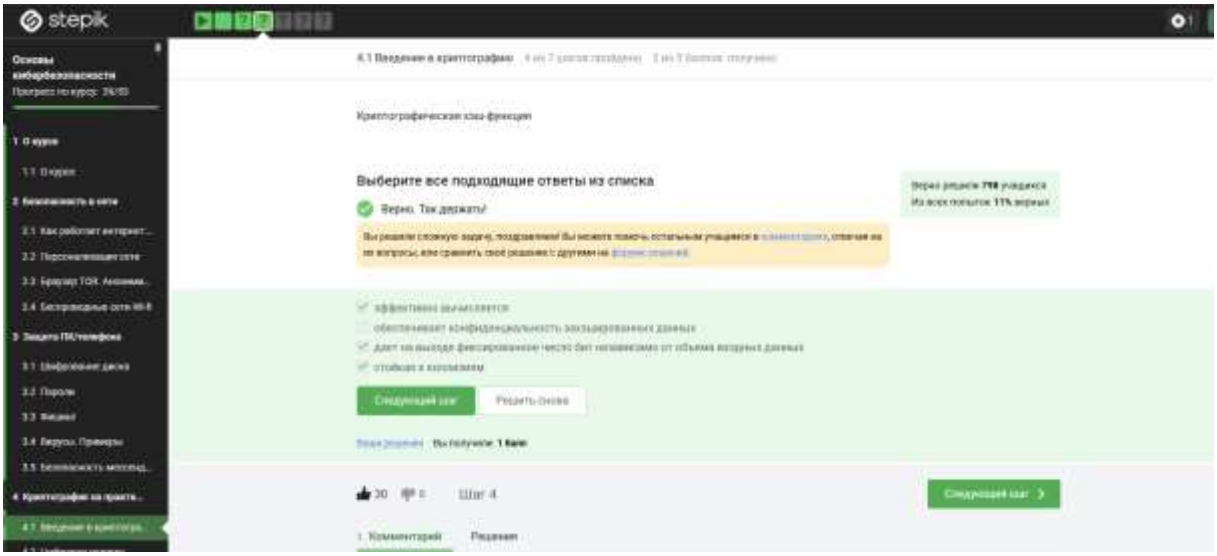
Довольно часто люди, даже те, которые работают в IT-секторе, путают основные криптографические понятия. Они иногда не отличают цифровую подпись от шифрования, от аутентификации, от хэш-функции. Моя сегодняшняя цель – это научить вас отличать основные криптографические протоколы, их еще называют примитивами, а именно – симметричное

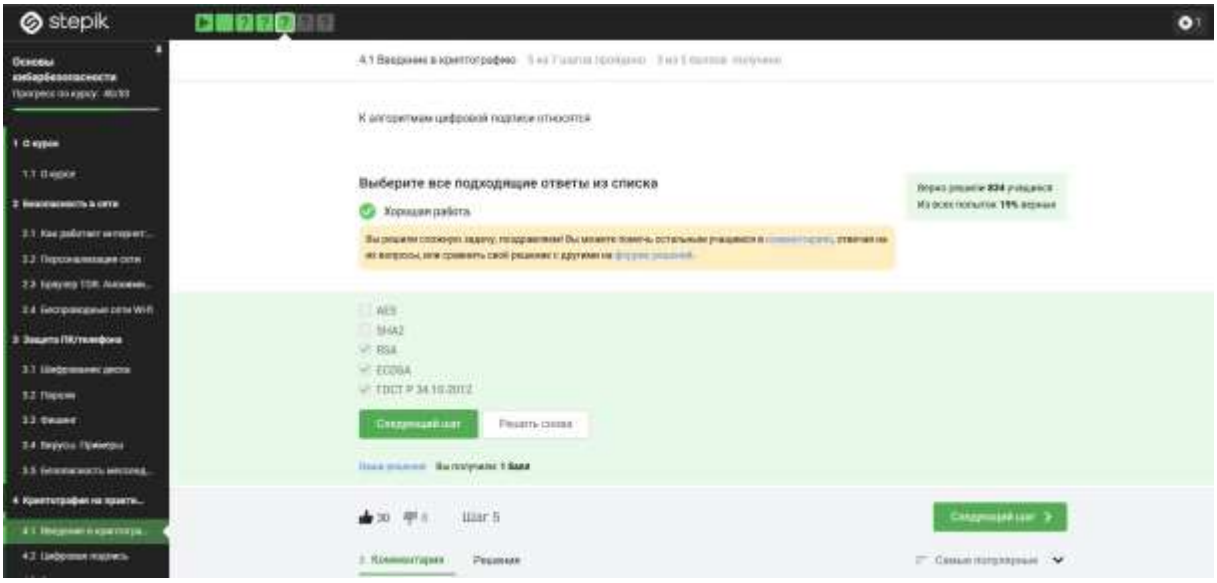
шифрование, аутентификацию, цифровую подпись и хэширование.

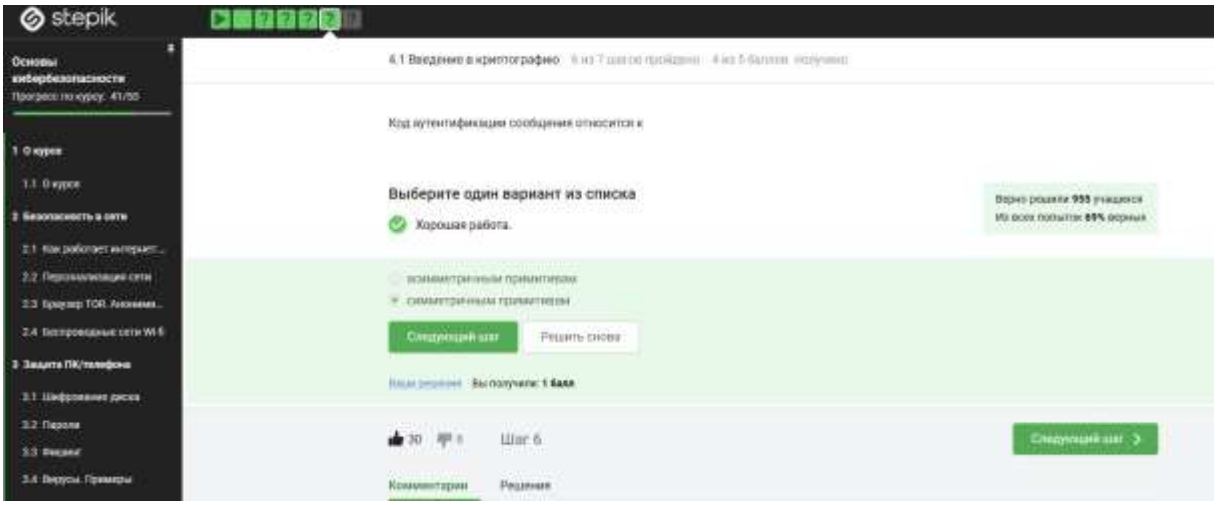
Для того, чтобы мы с вами говорили на одном языке и чтобы вы не плавали в этих понятиях, имеет смысл структурировать их и определить, зачем они нужны и какую функцию они несут. Эти разные протоколы – подпись, симметричное шифрование, аутентификация – играют разную роль, и поэтому они также по-разному строятся. Как они строятся, мы рассказывать в этом курсе не будем, это довольно сложные математические объекты, и аппарат, который нужно знать, чтобы понимать, как она устроена, очень сложный. Но зачем эти примитивы сделаны и какую цель они преследуют, мы сегодня с вами разберём.

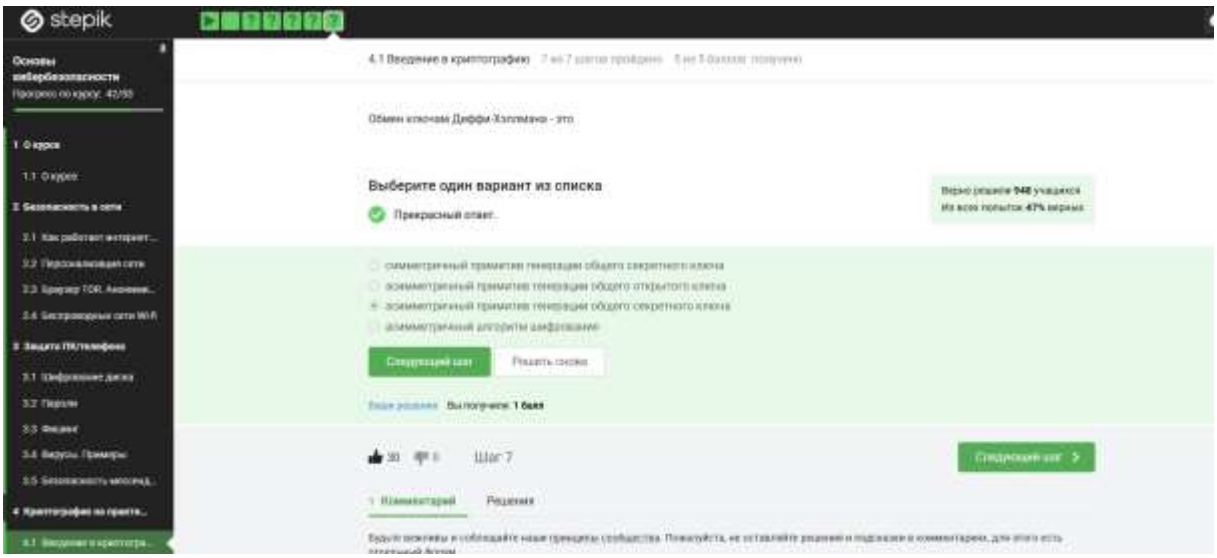
Выполнение тестовой части:





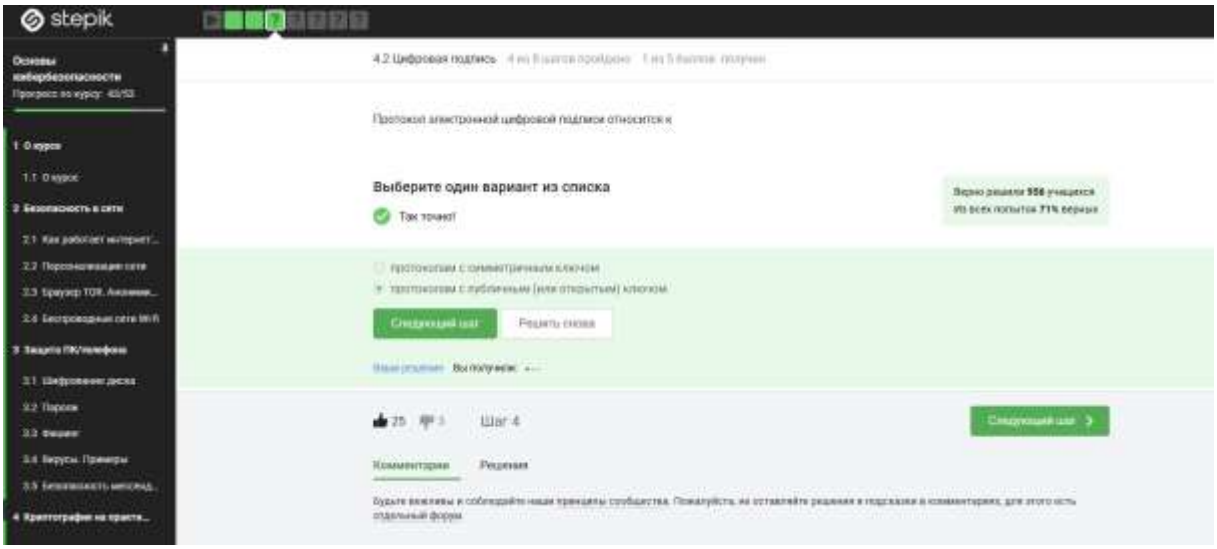

stepik
4.1 Введение в криптографию
К алгоритмам цифровой подписи относятся
Выберите все подходящие ответы из списка
Хорошая работа
AES
SHA2
RSA
ECDSA
ГОСТ Р 34.10-2012
Следующий шаг
Решить снова
Шаг 5
Следующий шаг
Комментарии
Решения

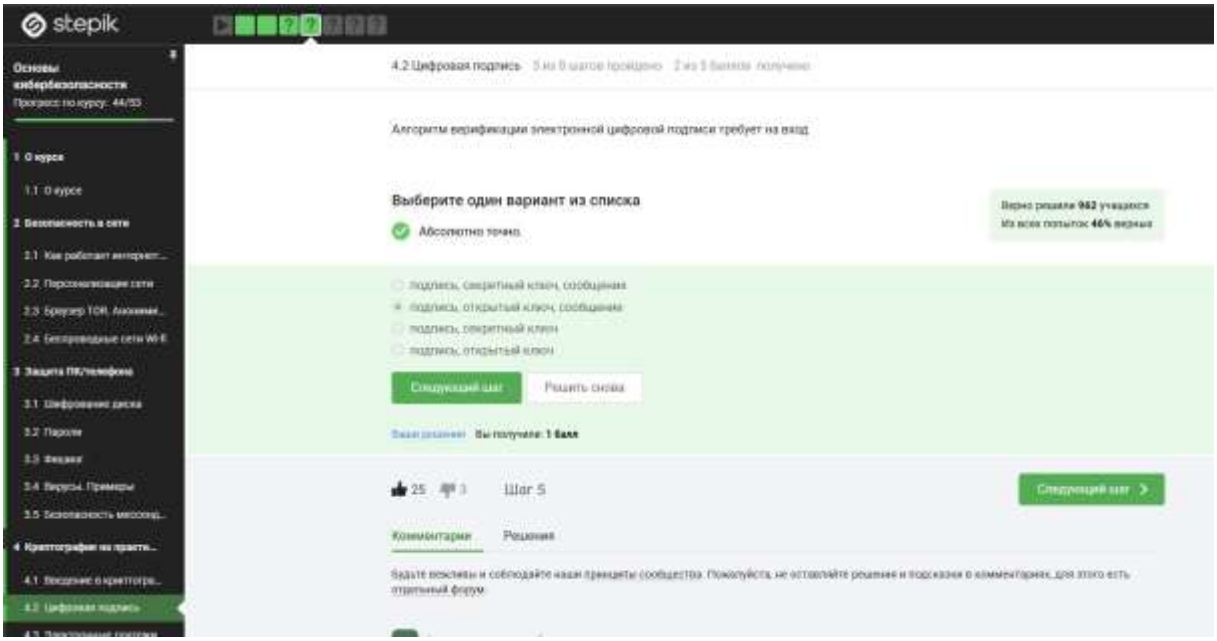

stepik
4.1 Введение в криптографию
Код аутентификации сообщения относится к
Выберите один вариант из списка
Хорошая работа.
Следующий шаг
Решить снова
Шаг 6
Следующий шаг
Комментарии
Решения

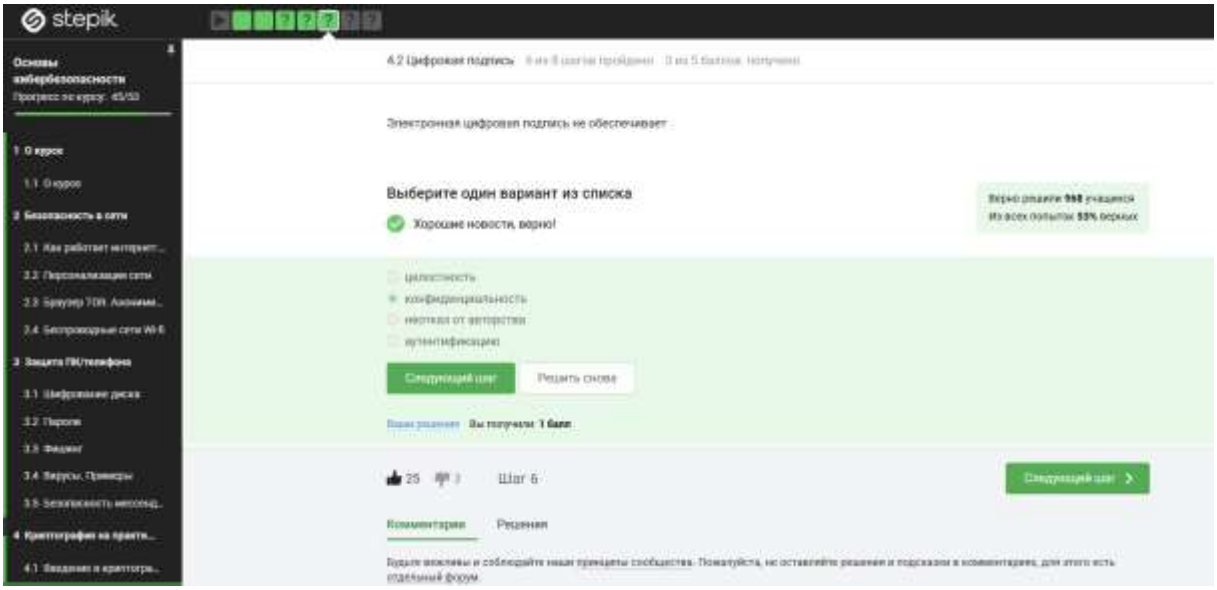

stepik
4.1 Введение в криптографию
Обмен ключами Диффи-Хэллмана - это
Выберите один вариант из списка
Прекрасный ответ.
Следующий шаг
Решить снова
Шаг 7
Следующий шаг
Комментарий
Решения

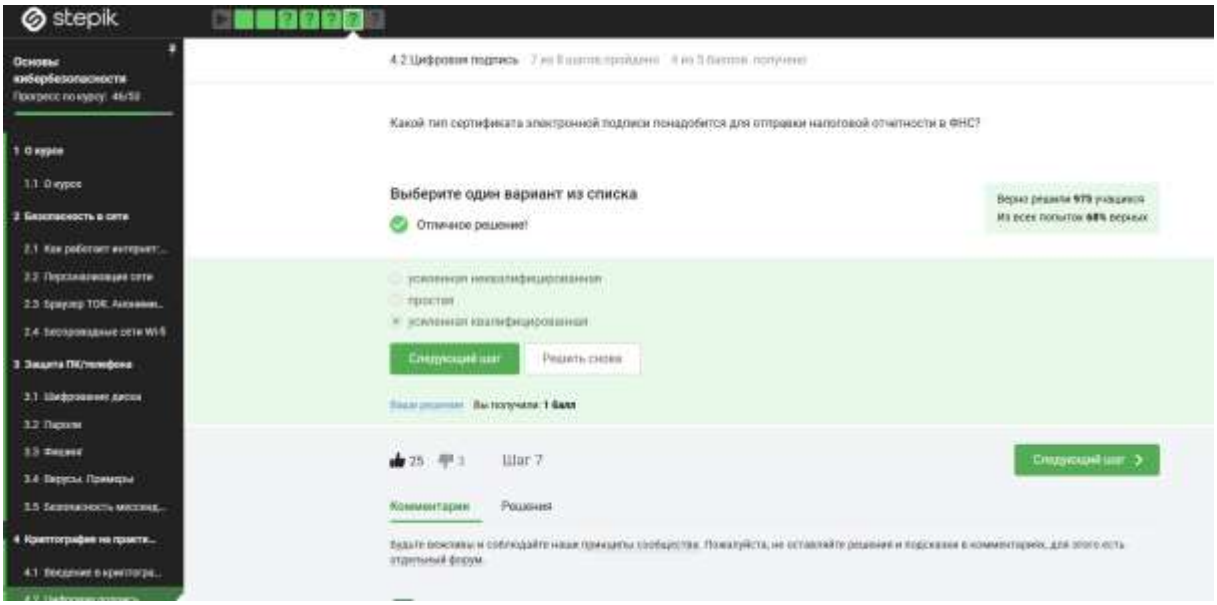
Цифровая подпись

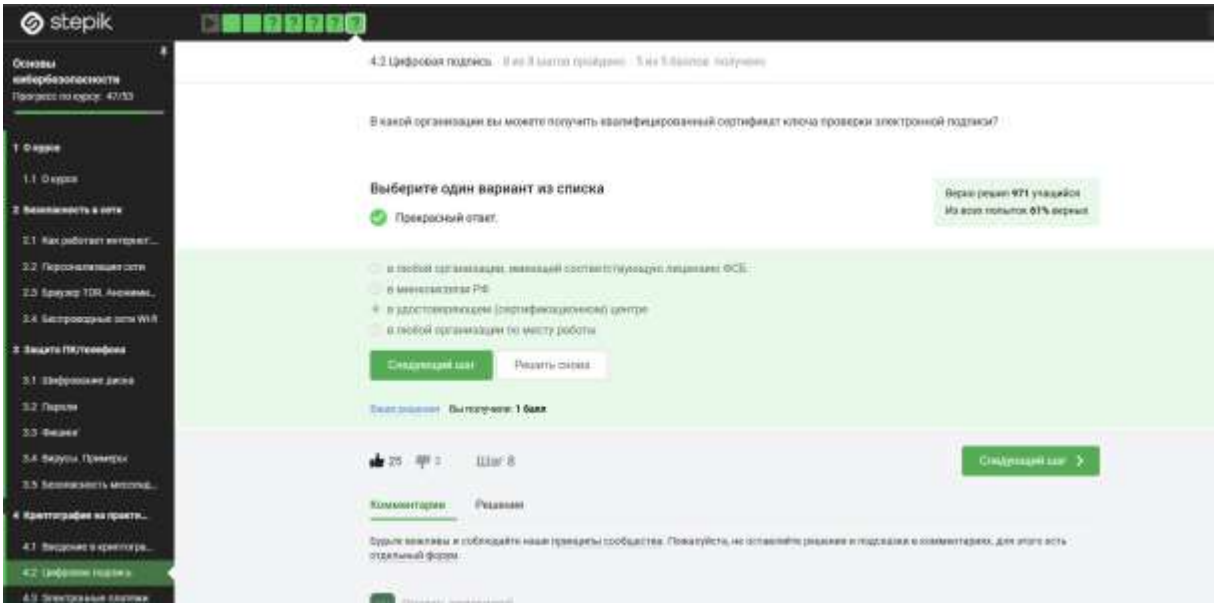
Прохождение тестовой части:





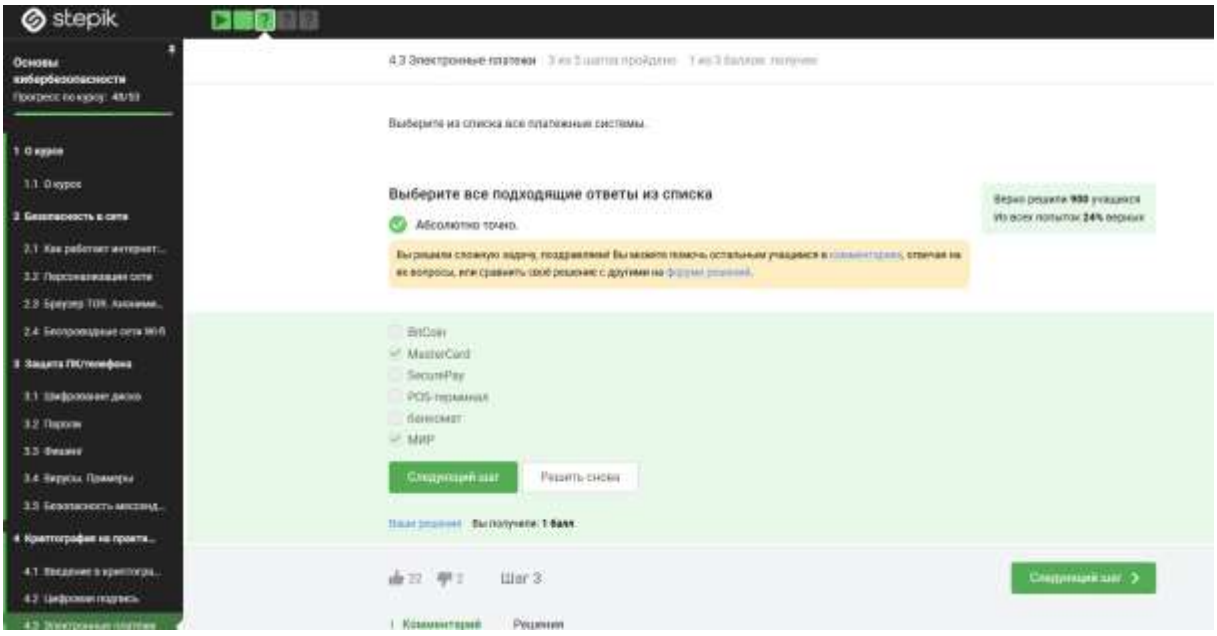

stepik
Основы кибербезопасности
4.2 Цифровая подпись
Электронная цифровая подпись не обеспечивает
Выберите один вариант из списка
Хорошие новости, верно!
целостность
конфиденциальность
авторство
аутентификацию
Следующий шаг
Решить снова
Шаг 6
Следующий шаг
Комментарии
Решения

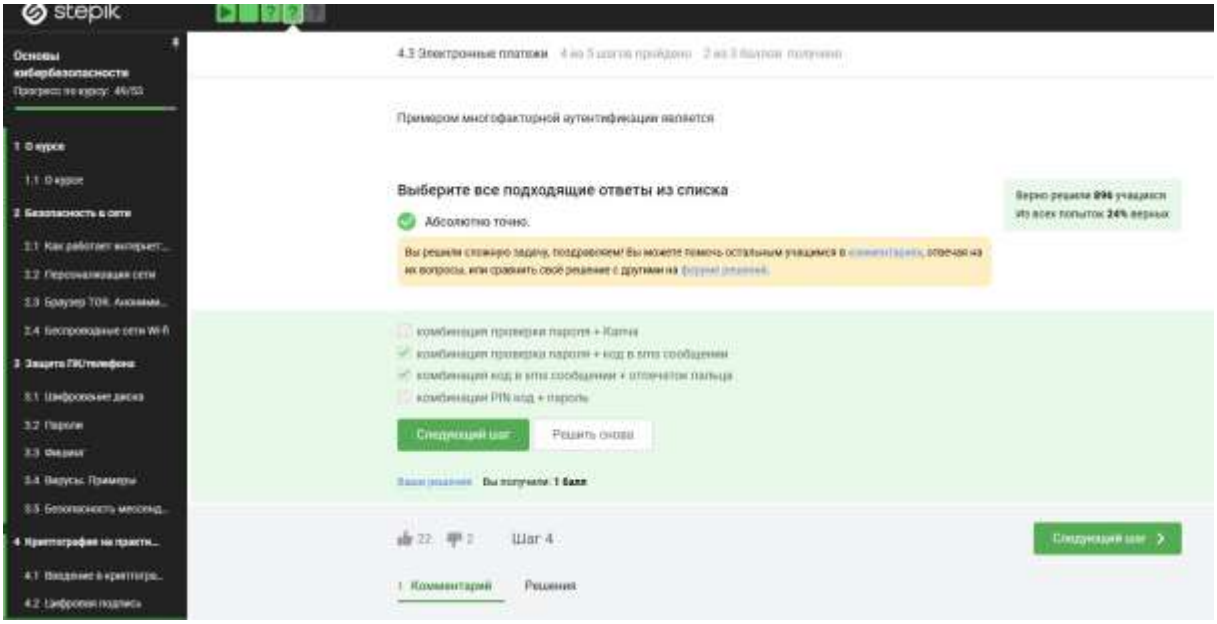

stepik
Основы кибербезопасности
4.2 Цифровая подпись
Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?
Выберите один вариант из списка
Отличное решение!
усиленная квалифицированная
Следующий шаг
Решить снова
Шаг 7
Следующий шаг
Комментарии
Решения

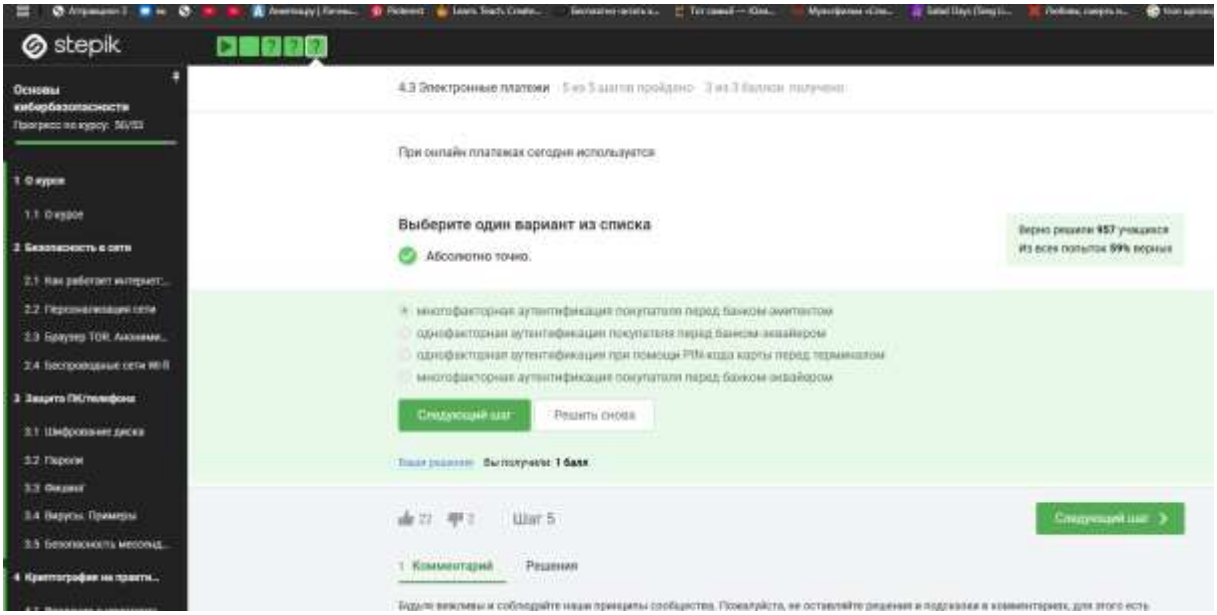


Электронные платежи

Прохождение тестовой части:

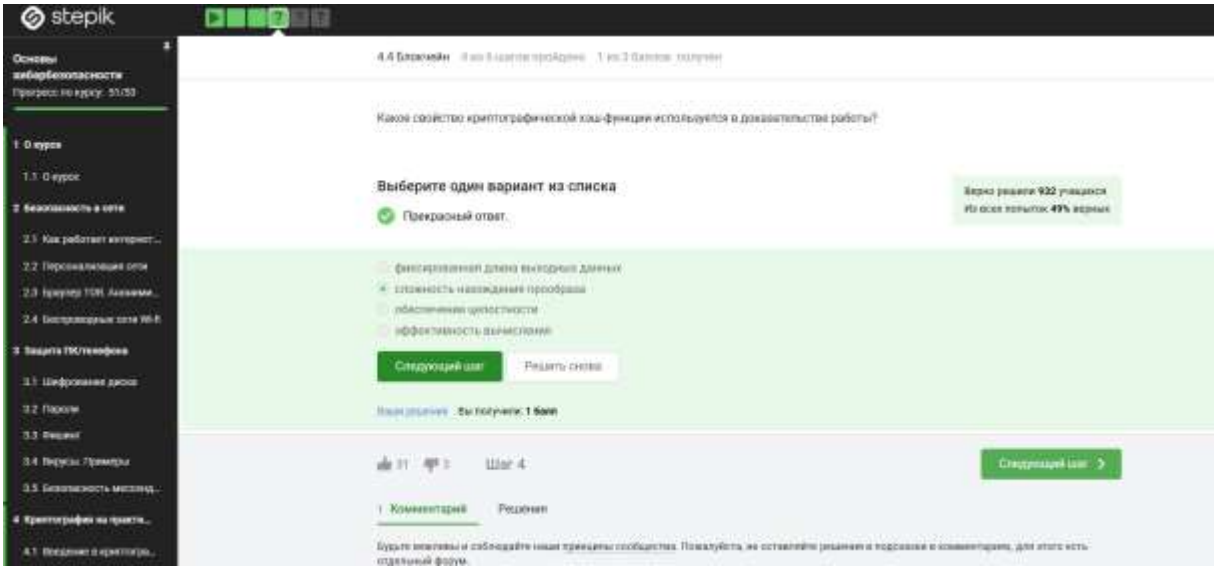


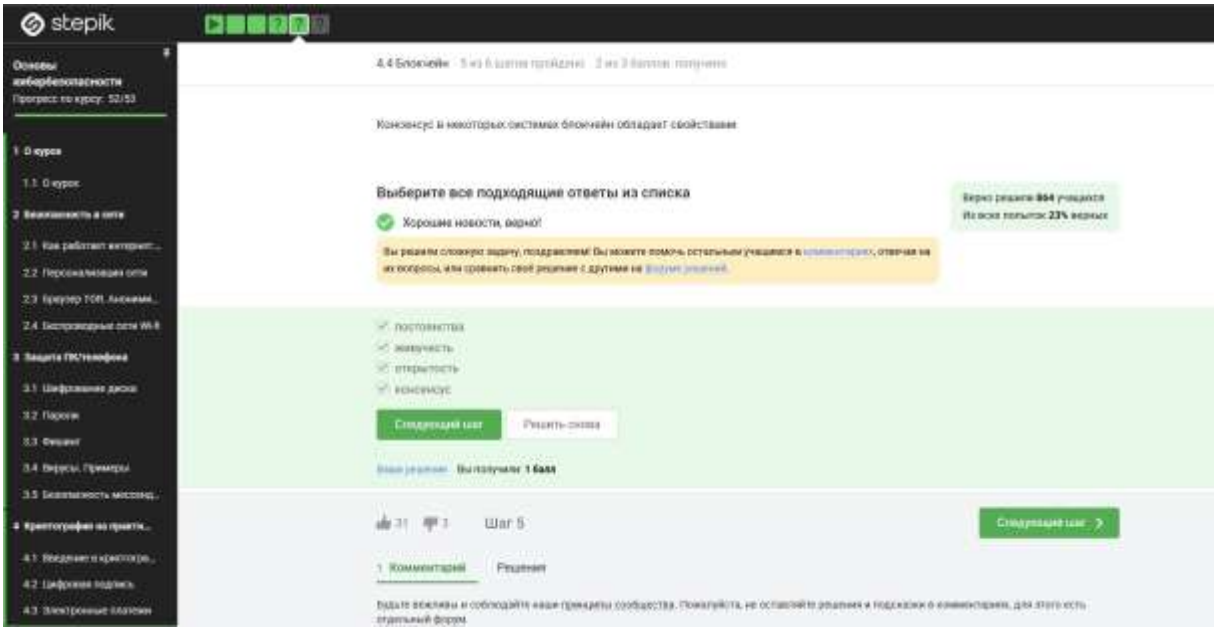


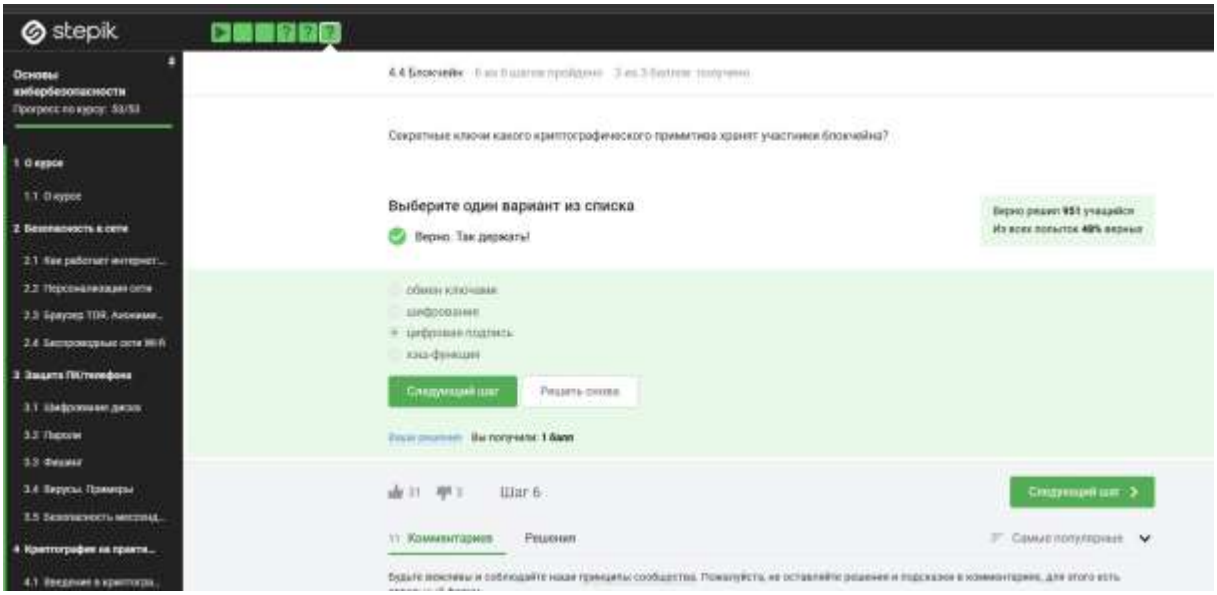


Блокчейн

Прохождение тестовой части:


stepik
Основы кибербезопасности
Прогресс по курсу: 51/53
4.4 Блокчейн
Какое свойство криптографической хэш-функции используется в доказательстве работы?
Выберите один вариант из списка
Прекрасный ответ.
Верно решили 922 учащихся
Из всех попыток 49% верных
фиксированная длина выходных данных
сложность нахождения прообраза
обеспечение целостности
эффективность вычисления
Следующий шаг
Решить снова
Ваше решение: Вы получили: 1 балл
Шаг 4
Следующий шаг
Комментарий
Решения
Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.


stepik
Основы кибербезопасности
Прогресс по курсу: 52/53
4.4 Блокчейн
Консенсус в некоторых системах блокчейн обладает свойствами
Выберите все подходящие ответы из списка
Хорошие новости, верно!
Верно решили 804 учащихся
Из всех попыток 23% верных
постоянства
живучесть
открытость
консенсус
Следующий шаг
Решить снова
Ваше решение: Вы получили: 1 балл
Шаг 5
Следующий шаг
Комментарий
Решения
Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.



4. Выводы.

Прохождение курса позволило достичь поставленных учебных целей и существенно углубить понимание ключевых аспектов информационной безопасности и технологий интернета.

Понимание работы Интернета и выявление слабых мест. Изучены принципы функционирования глобальной сети, её структуры и архитектуры. Освоено понятие сетевых протоколов и осознаны потенциальные угрозы безопасности данных при передаче через Интернет. Особое внимание уделялось вопросам конфиденциальности и защиты персональных данных пользователей.

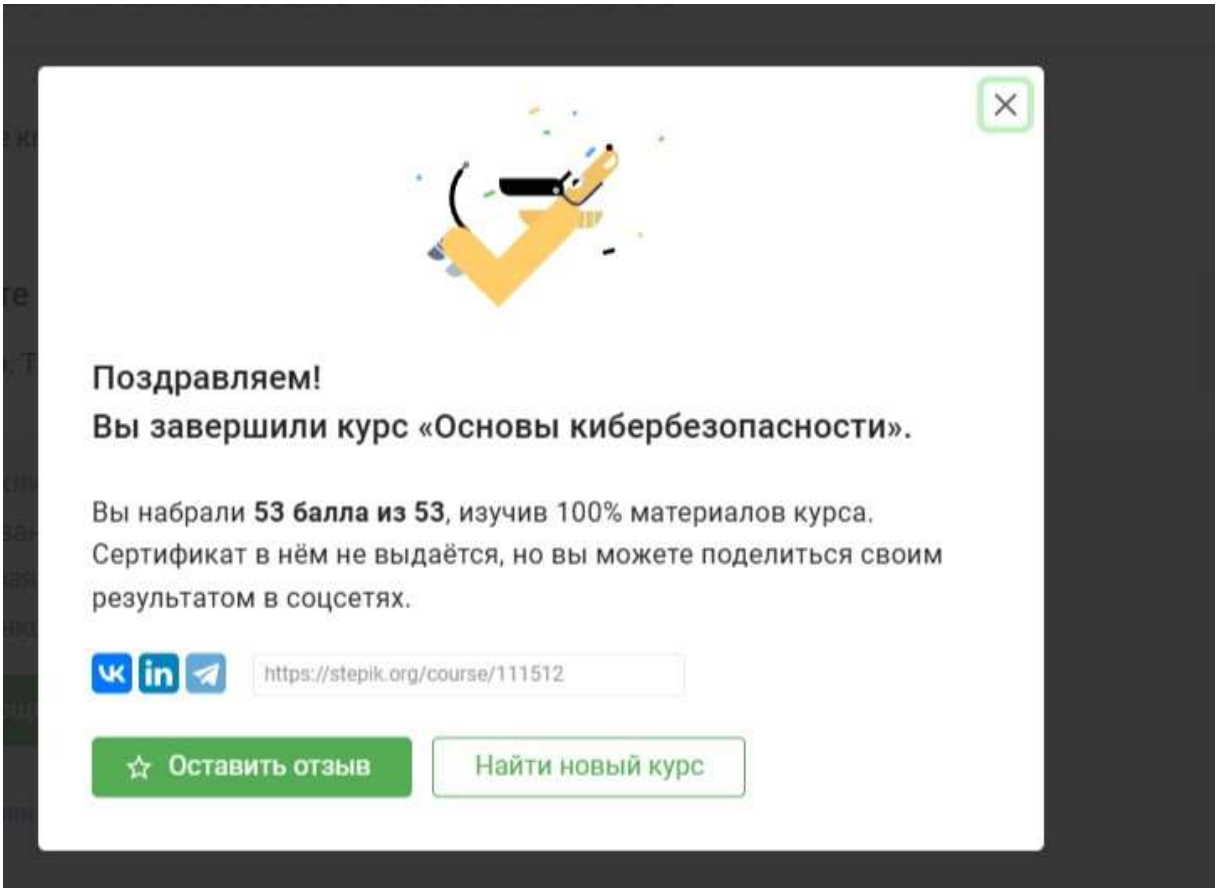
Осознание опасности простых паролей. Проанализированы риски использования очевидных комбинаций символов в качестве пароля. Рассмотрены механизмы взлома паролей методом подбора и продемонстрирована необходимость использования сложных, уникальных и надёжных паролей для предотвращения несанкционированного доступа к аккаунтам.

Различие между шифрованием и электронной подписью. Разобраны концепции криптографии, изучены различия между методами шифрования и электронными цифровыми подписями. Получены практические навыки определения защищённых коммуникаций и верификации цифровых

документов посредством ЭЦП.

Знание принципов электронных платежей. Изучение механизмов совершения онлайн-платежей, методов аутентификации и авторизации клиентов, используемых финансовых стандартов и правил обработки транзакций. Овладение основными инструментами анализа рисков мошенничества и обеспечением безопасной среды оплаты товаров и услуг.

Сертификат не выдаётся. Скрин о прохождении курса:



:::

{#refs} :::