Отчет о прохождении курса Stepik

Дашкина Анита Тагировна

17 мая, 2025, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Теоретическое введение

Ознакомиться с основами кибер безопасности по нескольким пунктам, а именно:

1. Безопасность в сети
2. Защита ПК/Телефона
3. Криптография

Цель лабораторной работы

Ознакомиться с кибербезопасностью

Выполнение лабораторной работы

Первый раздел

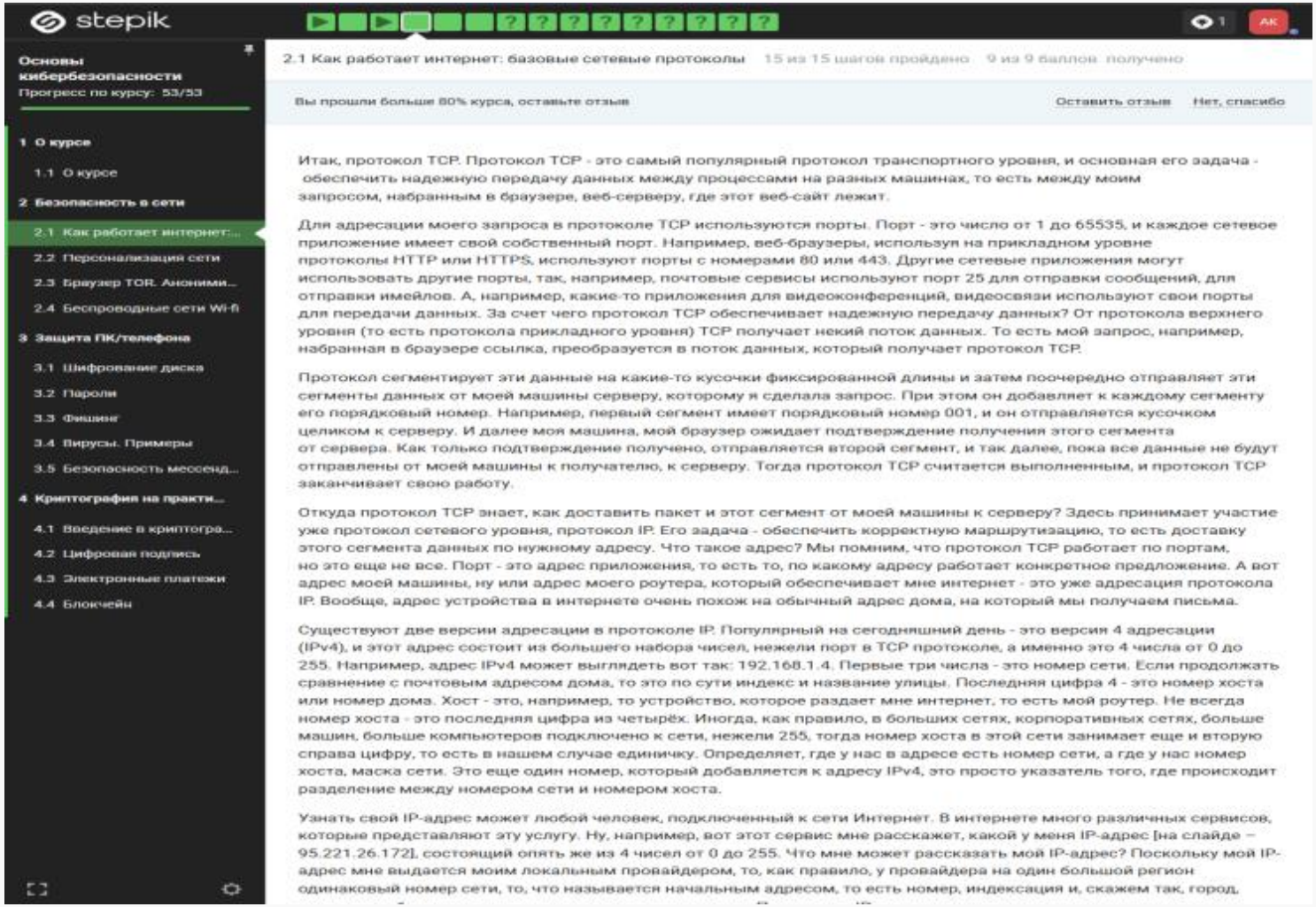

Рис. 1: Ознакомление с Интернет-безопасностью

Тесты первого раздела

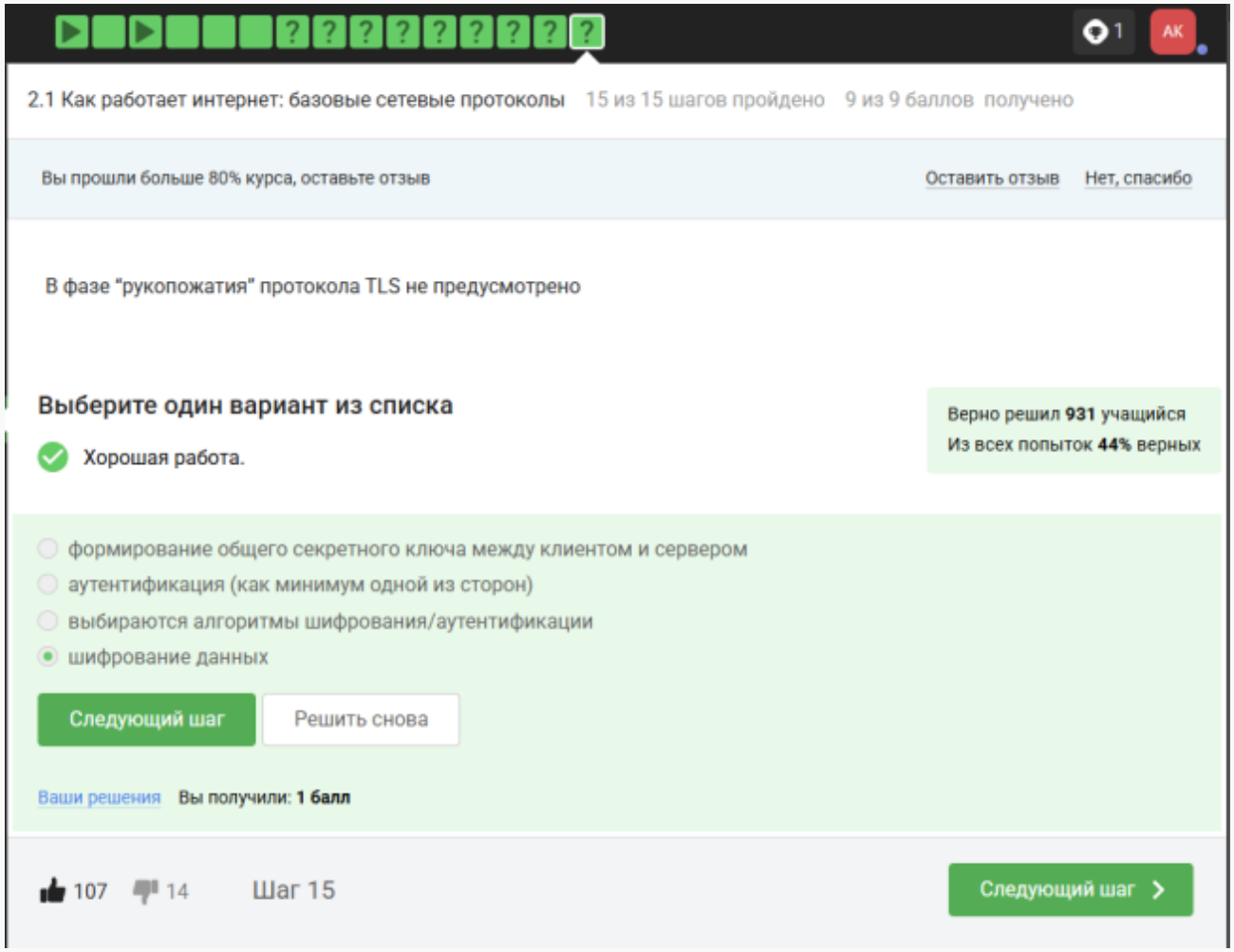

Рис. 2: Прохождение тестов

Раздел второй

3.1 Шифрование диска 5 из 5 шагов пройдено · 3 из 3 баллов получено

Вы прошли больше 80% курса, оставьте отзыв Оставить отзыв Нет, спасибо

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. Конечно, генерируете не вы сами, за вас это делает программа. Для того, чтобы этот ключ получить потом при дешифровании, вы должны запомнить пароль. Пароль - позволяет потом разблокировать этот ключ шифрования и дешифрования. Иногда вас спросят запомнить довольно длинный пароль. Вот, например, у меня на картинке пример пароля, предложенного утилитой шифрования в MacOS, и этот пароль вам нужно сохранить (где и как его хранить, мы также поговорим подробнее). Сейчас стоит запомнить, что на первом шаге мы генерируем ключ. Что мы с ним потом делаем? Потом мы с этим ключом шифруем. Программа берет этот ключ, берет наши данные, будь то весь жесткий диск или какой-то его сегмент или может быть даже загрузочный сегмент, и шифрует данные с помощью ключа. На выходе мы с вами получаем данные в зашифрованном виде. Когда мы с вами хотим получить доступ к нашим зашифрованным данным, жесткому диску или загрузочному сектору, мы дешифруем, при этом работает программа, алгоритм дешифрования. Алгоритм дешифрования берет то же самый ключ, зашифрованные данные и выдает нам дешифрованные данные: либо наши файлы в открытом виде, либо, если мы шифровали загрузочный сектор операционной системы, нам загрузят эту операционную систему.

Поговорим немного о деталях, о том, как происходит шифрование. Шифрование больших объемов данных, например, жесткого диска или сегмента жесткого диска или какой-то большой флешки, осуществляется с помощью симметричного шифрования, как правило, алгоритма AES. Это американский стандарт симметричного шифрования, он также используется для конфиденциальной передачи данных по сети. Это эффективный алгоритм, который реализован в процессорах быстро, то есть на аппаратном уровне. Благодаря тому, что это хороший алгоритм, пользователь практически не наблюдает задержек в работе, то есть данные шифруются-дешифруются быстро. Как правило, это происходит на заднем фоне, мы можем при этом работать на компьютере, будут происходить какие-то параллельные операции на шифрование и дешифрование.

На современных процессорах семейства Intel встроен TPM модуль или TPM криптопроцессор. TPM - это аббревиатура от Trusted Platform Module, и этот криптопроцессор позволяет, во-первых, эффективно шифровать, то есть на нем аппаратно реализован алгоритм шифрования AES, а во-вторых, позволяет хранить этот самый ключ, с помощью которого мы шифровали и дешифровали, на специальном сегменте блока данных, который защищен от злоумышленников.

Как я уже сказала, шифровать можно не только жесткий диск, где мы храним файлы, можно шифровать и загрузочный сектор диска. Это тот сектор, который включается сразу после того, как мы стартовали компьютер. Компьютер считывает данные в сегменте, который хранит у себя загрузочные файлы операционной системы, и мы получаем либо свой рабочий стол, либо запрос на авторизацию для доступа к нашему рабочему столу. Вот для того,

Рис. 3: Знакомство с шифрованием

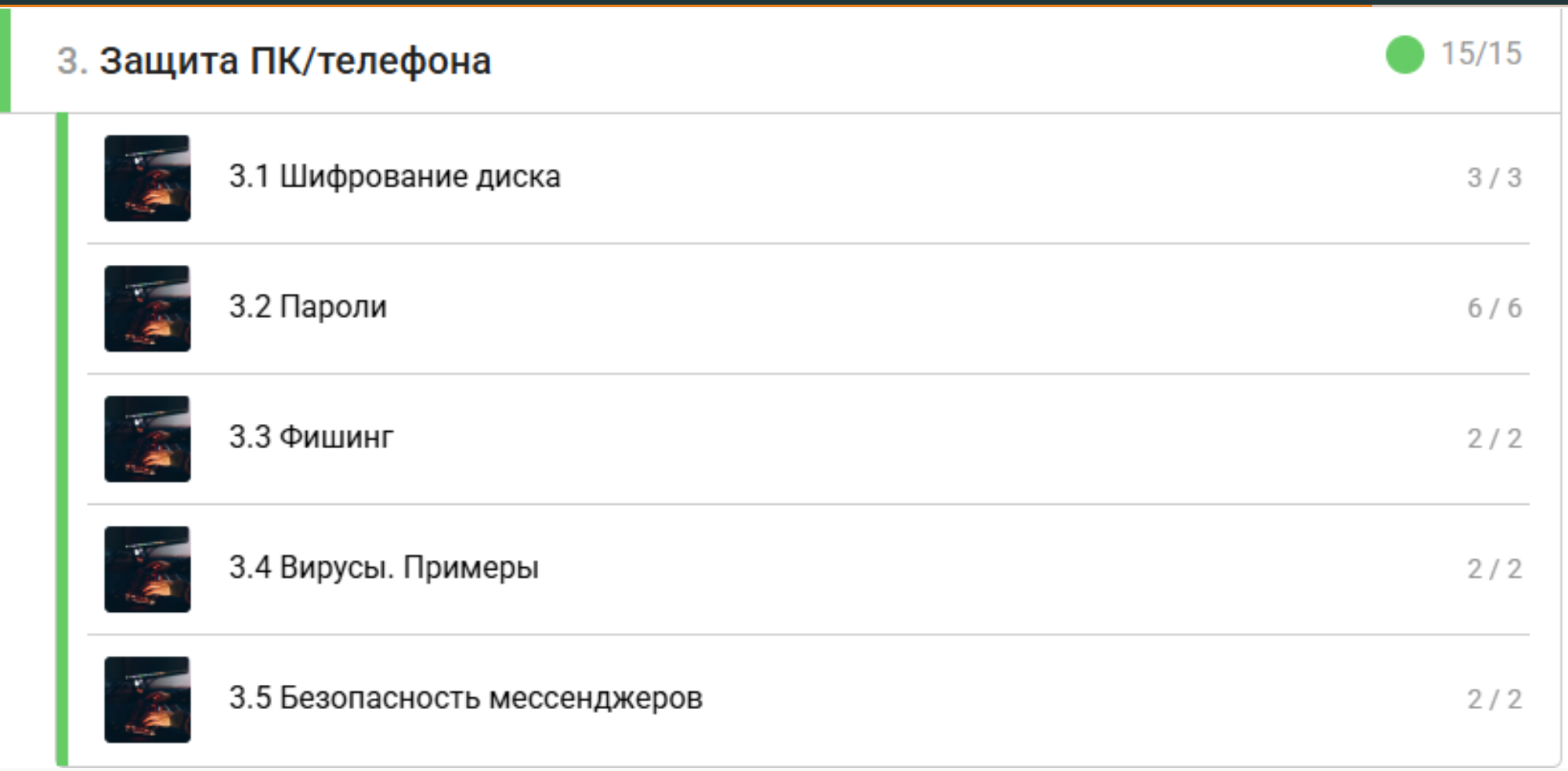

Рис. 4: Успешное прохождение всех тестов

Раздел третий

4.1 Введение в криптографию 7 из 7 шагов пройдено 5 из 5 баллов получено

Вы прошли больше 66% курса, оставьте отзыв

Оставить отзыв Нет, спасибо

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.

Вообще, если начинать категоризировать протоколы в криптографии, то мы с вами встретим два раздела: первый раздел – это симметричная криптография, второй раздел – это асимметричная криптография. Определяющее свойство симметричной криптографии состоит в том, что она включает себя протоколы, где две или более стороны имеют общие секретные ключи, поэтому она и называется симметричной. К таким протоколам относят симметричное шифрование и некоторые протоколы аутентификации. Часто симметричный протокол довольно сложно построить, сложно установить потенциальный канал связи, исключительно основываясь на симметричных протоколах, поскольку нам нужно сгенерировать общий секретный ключ, то есть либо как-то физически встретиться с другим человеком и с другим устройством, либо что-то такое сделать, чтобы мы сгенерировали общий секрет. И элегантным решением этого вопроса являются протоколы асимметричной криптографии.

В асимметричной криптографии (её еще называют криптографией с открытым ключом) у каждой из сторон есть пара ключей: открытый ключ и секретный ключ. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя. К протоколам асимметричной криптографии относят электронно-цифровую подпись и протокол генерации общего ключа – это этот протокол, который позволяет нам не общаться физически друг с другом, а установить и вычислить общий секретный ключ.

Как правило, в современных протоколах, в современных конфиденциальных коммуникациях используются вместе симметричная криптография и асимметричная криптография. Это сделано, в частности, для того, чтобы сделать конфиденциальную коммуникацию эффективной, так как симметричные примитивы обычно являются более эффективными по времени, чем асимметричные примитивы.

Есть еще один примитив, который выходит за рамки симметричной и асимметричной криптографии, поскольку он бесключевой. Ярким и, наверное, единственным примером такого криптографического примитива является криптографическая хэш-функция. Вообще, в науке есть просто хэш-функция, а есть криптографическая хэш-функция. Криптографическая хэш-функция берет на вход произвольный объем данных, то есть какие-то биты и выдает на выходе фиксированную строку, например длины n. Важно, что, как правило, функция сжимает данные: она берет большой набор данных и выдаёт потом маленькое фиксированное значение.

Важное свойство криптографической хэш-функций, то, что делает её криптографической – это стойкость к коллизиям. Что такое коллизия? Коллизия – это два разных входа в хэш-функцию, которые дают одинаковый выход. То есть это две разные строки например x и x', где x ≠ x', такие, что значения хэш-функции на них совпадают, то есть h(x) = h(x'). Это важное свойство отличает криптографическую функцию от некриптографической. Можно доказать (мы этого делать с вами не будем), что из этого свойства коллизии следует другое важное свойство, а именно то, что

Рис. 4: Знакомство с криптографией

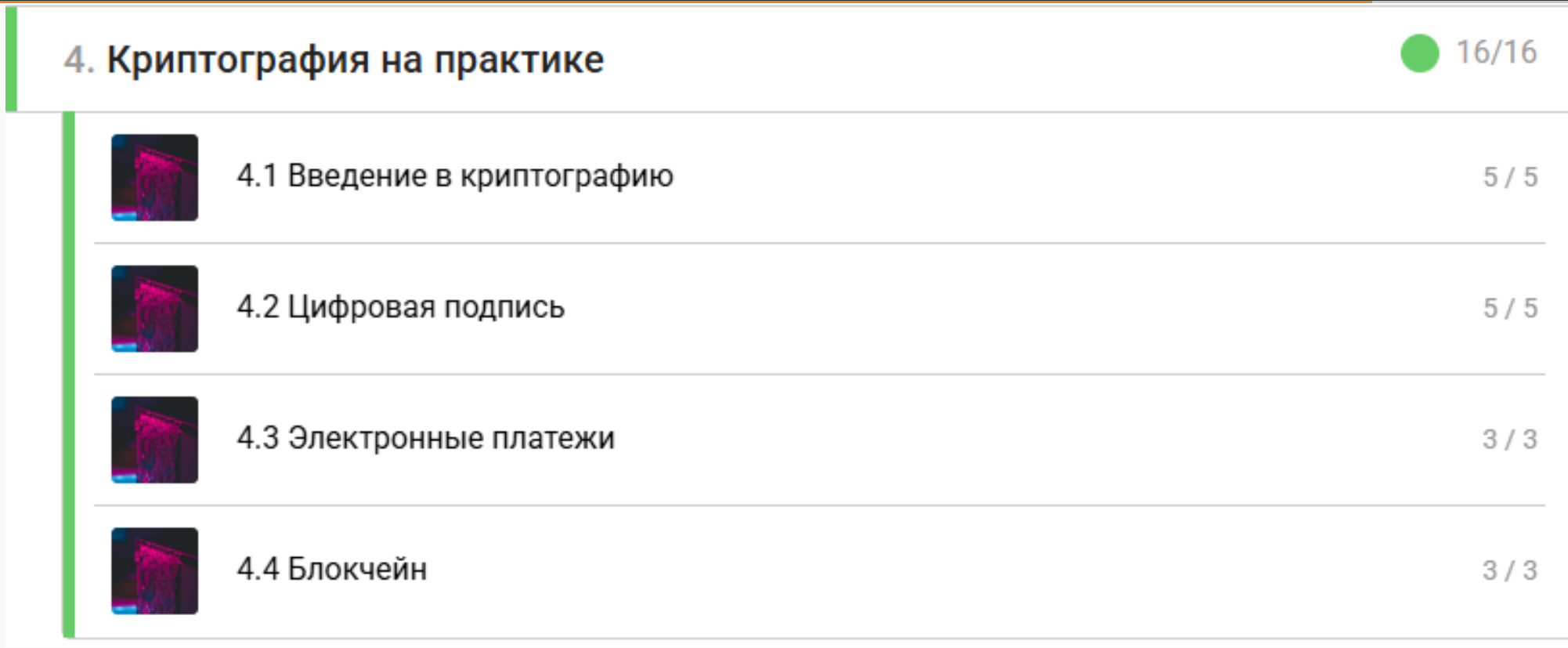

Рис. 5: Успешное прохождение всех тестов

Выводы

Результаты выполнения лабораторной работы

В результате выполнения работы этот курс научил, как защищаться от цифровых угроз в современном мире. Я узнал, что такое кибербезопасность и почему она важна для каждого. Раздел криптографии объяснит, как работают шифрование и цифровые подписи, чтобы ваши сообщения и данные оставались конфиденциальными. В части защиты сетей расскажут, как безопасно пользоваться Wi-Fi, распознавать фишинг и защищаться от хакерских атак с помощью VPN и фаерволов. Веб-безопасность научит избегать опасных сайтов и защищать свои аккаунты от взлома. Раздел защиты ПК и телефонов даст практические советы: ставить антивирусы, вовремя обновлять программы и не качать подозрительные файлы. Вы поймете, как социальная инженерия манипулирует людьми (например, через фальшивые звонки "из банка"), и научитесь не попадаться на уловки мошенников. Если что-то пошло не так, раздел реагирования на инциденты подскажет, как действовать при утечке данных или заражении вирусом. Курс также затрагивает законы о персональных данных и этические вопросы — чтобы вы не только защищали себя, но и не нарушали чужие права. Главный вывод: безопасность начинается с простых шагов — сложных паролей, критического мышления и базовых цифровых привычек.

Результаты выполнения лабораторной работы

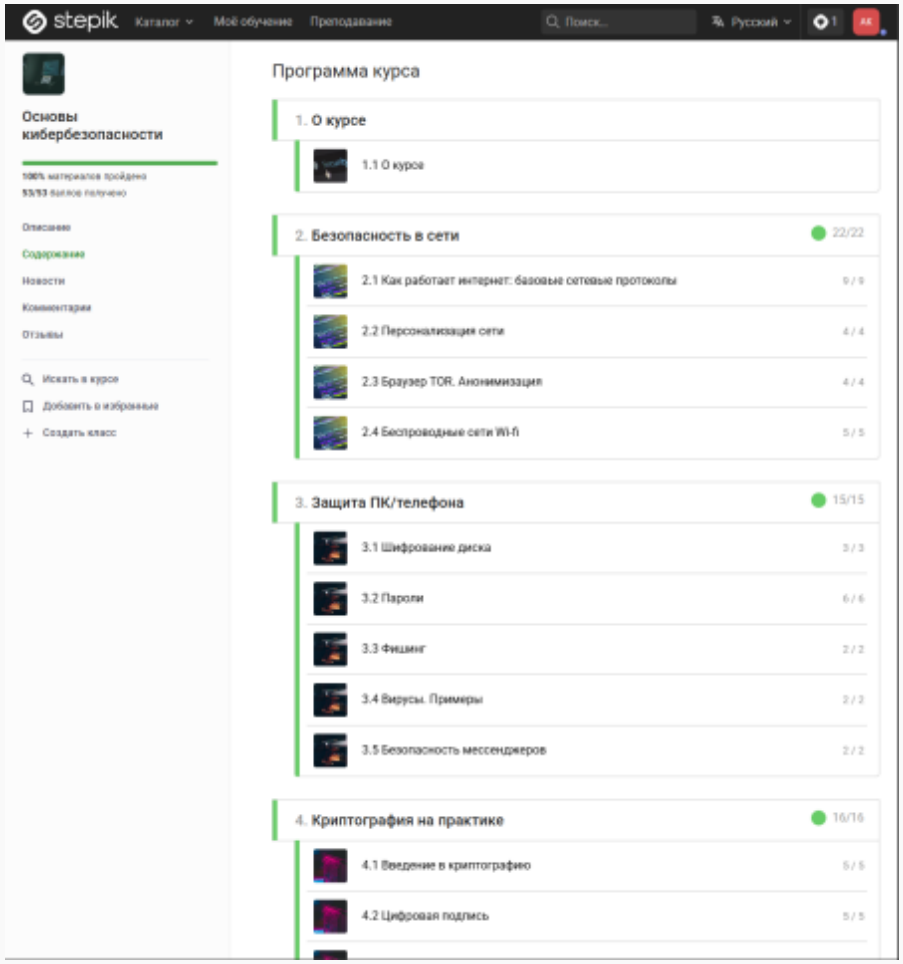

Рис. 5: Сертификатов не дают вот доказательство прохождения