

Основы кибербезопасности

Прохождение курса

Астраханцева А. А.

Содержание

1	Цель работы	5
2	Выполнение	6
2.1	Безопасность в сети	6
2.1.1	Как работает интернет: базовые сетевые протоколы	6
2.1.2	Персонализация сети	14
2.1.3	Браузер TOR. Анонимизация	18
2.1.4	Беспроводные сети Wi-fi	22
2.2	Защита ПК/телефона	25
2.2.1	Шифрование диска	25
2.2.2	Пароли	28
2.2.3	Фишинг	33
2.2.4	Вирусы. Примеры	35
2.2.5	Безопасность мессенджеров	36
2.3	Криптография на практике	38
2.3.1	Введение в криптографию	38
2.3.2	Цифровая подпись	42
2.3.3	Электронные платежи	45
2.3.4	Блокчейн	48
3	Выводы	52

Список иллюстраций

2.1	Как работает интернет. Вопрос №1	7
2.2	Как работает интернет. Вопрос №2	8
2.3	Как работает интернет. Вопрос №3	9
2.4	Как работает интернет. Вопрос №4	10
2.5	Как работает интернет. Вопрос №5	11
2.6	Как работает интернет. Вопрос №6	12
2.7	Как работает интернет. Вопрос №7	12
2.8	Как работает интернет. Вопрос №8	13
2.9	Как работает интернет. Вопрос №9	14
2.10	Персонализация сети. Вопрос №1	15
2.11	Персонализация сети. Вопрос №2	16
2.12	Персонализация сети. Вопрос №3	17
2.13	Персонализация сети. Вопрос №4	18
2.14	Браузер TOR. Анонимизация. Вопрос №1	19
2.15	Браузер TOR. Анонимизация. Вопрос №2	20
2.16	Браузер TOR. Анонимизация. Вопрос №3	21
2.17	Браузер TOR. Анонимизация. Вопрос №4	21
2.18	Беспроводные сети Wi-fi. Вопрос №1	22
2.19	Беспроводные сети Wi-fi. Вопрос №2	23
2.20	Беспроводные сети Wi-fi. Вопрос №3	24
2.21	Беспроводные сети Wi-fi. Вопрос №4	24
2.22	Беспроводные сети Wi-fi. Вопрос №5	25
2.23	Шифрование диска. Вопрос №1	26
2.24	Шифрование диска. Вопрос №2	27
2.25	Шифрование диска. Вопрос №3	28
2.26	Пароли. Вопрос №1	29
2.27	Пароли. Вопрос №2	30
2.28	Пароли. Вопрос №3	31
2.29	Пароли. Вопрос №4	31
2.30	Пароли. Вопрос №5	32
2.31	Пароли. Вопрос №6	33
2.32	Фишинг. Вопрос №1	34
2.33	Фишинг. Вопрос №2	34
2.34	Вирусы. Примеры. Вопрос №1	35
2.35	Вирусы. Примеры. Вопрос №2	36
2.36	Безопасность мессенджеров. Вопрос №1	37
2.37	Безопасность мессенджеров. Вопрос №2	37

2.38 Введение в криптографию. Вопрос №1	38
2.39 Введение в криптографию. Вопрос №2	39
2.40 Введение в криптографию. Вопрос №3	40
2.41 Введение в криптографию. Вопрос №4	41
2.42 Введение в криптографию. Вопрос №5	42
2.43 Цифровая подпись. Вопрос №1	43
2.44 Цифровая подпись. Вопрос №2	43
2.45 Цифровая подпись. Вопрос №3	44
2.46 Цифровая подпись. Вопрос №4	45
2.47 Цифровая подпись. Вопрос №5	45
2.48 Электронные платежи. Вопрос №1	46
2.49 Электронные платежи. Вопрос №2	47
2.50 Электронные платежи. Вопрос №3	48
2.51 Блокчейн. Вопрос №1	49
2.52 Блокчейн. Вопрос №2	50
2.53 Блокчейн. Вопрос №3	51
2.54 Окончание курса	51

1 Цель работы

Прохождение курса “Основы кибербезопасности” и получение сертификата.

2 Выполнение

2.1 Безопасность в сети

2.1.1 Как работает интернет: базовые сетевые протоколы

Протокол прикладного уровня в данном списке — это HTTPS.

UDP, TCP и IP являются протоколами более низких уровней. UDP и TCP относятся к транспортному уровню, а IP — к сетевому уровню (рис. 2.1).

Выберите протокол прикладного уровня

Выберите один вариант из списка

✓ Всё правильно.

- ☐ UDP
- ☐ TCP
- ☒ HTTPS
- ☐ IP

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **0 баллов** из 1

Рис. 2.1: Как работает интернет. Вопрос №1

Протокол TCP работает на транспортном уровне (рис. 2.2).

На каком уровне работает протокол TCP?

Выберите один вариант из списка

☒ Хорошая работа.

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

[Следующий шаг](#) [Решить снова](#)

[Ваши решения](#) Вы получили: **0 баллов** из 1

Рис. 2.2: Как работает интернет. Вопрос №2

Корректные адреса IPv4 в данном списке: 90.11.90.22 и 25.198.0.15. Варианты 421.0.15.19 и 43.12.256.7 - некорректные, так как значения в каждом октете могут быть от 0 до 255 (рис. 2.3).

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

✓ Правильно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным их вопросы, или сравнить своё решение с другими на [форуме решений](#).

☐ 421.0.15.19

☐ 43.12.256.7

☒ 90.11.90.22

☒ 25.198.0.15

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **0 баллов** из 1

Рис. 2.3: Как работает интернет. Вопрос №3

DNS (Domain Name System) сервер переводит понятные для человека доменные имена (например, [www.example.com](#)) в IP адреса, которые используются устройствами для взаимодействия в сети. Это позволяет пользователям легко запоминать и вводить веб-адреса, вместо использования числовых IP адресов (рис. 2.4).

DNS сервер

Выберите один вариант из списка

☒ Верно.

☒ 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: **0 баллов** из 1

Рис. 2.4: Как работает интернет. Вопрос №4

Модель TCP/IP состоит из четырех уровней. На верхнем уровне находится прикладной уровень, который взаимодействует с пользовательскими приложениями. Ниже него идет транспортный уровень, обеспечивающий передачу данных между хостами. Следующим идет сетевой уровень, отвечающий за маршрутизацию пакетов. На нижнем уровне находится канальный уровень, который управляет физической передачей данных через сеть. (рис. 2.5).

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

☒ Верно.

- ☐ сетевой -- прикладной -- канальный -- транспортный
- ☐ прикладной -- транспортный -- канальный -- сетевой
- ☐ транспортный -- сетевой -- прикладной -- канальный
- ☒ прикладной -- транспортный -- сетевой -- канальный

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 0 баллов из 1

Рис. 2.5: Как работает интернет. Вопрос №5

Протокол HTTP (HyperText Transfer Protocol) передает данные в незашифрованном виде. Это означает, что данные, передаваемые между клиентом и сервером, могут быть перехвачены и прочитаны третьими сторонами. Для безопасной передачи данных используется протокол HTTPS, который шифрует данные с помощью SSL/TLS (рис. 2.6).

Протокол http предполагает

Выберите один вариант из списка

✓ Отличное решение!

- ☐ передачу зашифрованных данных между клиентом и сервером
- ☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 0 баллов из 1

Рис. 2.6: Как работает интернет. Вопрос №6

Протокол HTTPS (HyperText Transfer Protocol Secure) включает в себя две основные фазы. Первая фаза — это “рукопожатие” (handshake), в ходе которой клиент и сервер устанавливают защищенное соединение, согласовывают параметры шифрования и аутентифицируют сервер (и, возможно, клиента). Вторая фаза — это передача данных, во время которой данные передаются в зашифрованном виде, обеспечивая их конфиденциальность и целостность (рис. 2.7).

Протокол https состоит из

Выберите один вариант из списка

✓ Правильно.

- ☐ 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: 0 баллов из 1

Рис. 2.7: Как работает интернет. Вопрос №7

Во время установления защищенного соединения по протоколу TLS, клиент и сервер договариваются о версии протокола, которую они будут использовать. Этот процесс происходит в ходе “рукопожатия” (TLS handshake), где обе стороны сообщают свои поддерживаемые версии и выбирают наивысшую общую версию, чтобы обеспечить совместимость и безопасность соединения (рис. 2.8).

Версия протокола TLS определяется

Выберите один вариант из списка

☒ Так точно!

☐ сервером

☐ клиентом

☒ и клиентом, и сервером в процессе “переговоров”

☐ провайдером клиента

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **0 баллов** из 1

Рис. 2.8: Как работает интернет. Вопрос №8

Во время “рукопожатия” (TLS handshake), клиент и сервер согласовывают параметры для установки безопасного соединения, такие как выбор версии протокола, выбор алгоритмов шифрования и аутентификации, а также происходит аутентификация (как минимум одной из сторон) и формирование общего секретного ключа. Однако фаза “рукопожатия” не включает в себя шифрование данных, так как шифрование начинается только после успешного завершения этой фазы и установления защищенного соединения (рис. 2.9).

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

✓ Правильно, молодец!

- ☐ формирование общего секретного ключа между клиентом и сервером
- ☐ аутентификация (как минимум одной из сторон)
- ☐ выбираются алгоритмы шифрования/аутентификации
- ☒ шифрование данных

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 0 баллов из 1

Рис. 2.9: Как работает интернет. Вопрос №9

2.1.2 Персонализация сети

Куки могут хранить идентификатор пользователя, что позволяет веб-сайтам отслеживать пользователя и его предпочтения, и идентификатор сеанса, который помогает серверу отслеживать состояние сеанса для конкретного пользователя.

Пароль пользователя и IP-адрес обычно не хранятся в куки из соображений безопасности. Вместо этого пароль обычно хранится в зашифрованной форме на сервере, а IP-адрес может использоваться для идентификации пользователя, но не хранится непосредственно в куках (рис. 2.10).

Куки хранят:

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных вопросы, или сравнить своё решение с другими на [форуме реш](#)

- ☒ идентификатор пользователя
- ☐ IP адрес
- ☐ пароль пользователя
- ☒ id сессии

Следующий шаг

Решить снова

[Ваши решения](#)

Рис. 2.10: Персонализация сети. Вопрос №1

Куки применяются для различных целей, включая аутентификацию пользователя, персонализацию веб-страниц, отслеживание информации о пользователе и сбор статистики посещаемости сайта. Однако они не прямо связаны с улучшением надежности соединения. Улучшение надежности соединения может быть достигнуто за счет других мер безопасности, таких как использование протоколов шифрования (например, HTTPS) (рис. 2.11).

Куки не используются для

Выберите один вариант из списка

☒ Правильно.

- ☐ аутентификации пользователя
- ☐ персонализации веб-страниц
- ☐ отслеживания информации о пользователе
- ☐ сборе статистики посещаемости сайта
- ☒ улучшения надежности соединения

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **0 баллов** из 1

Рис. 2.11: Персонализация сети. Вопрос №2

Куки генерируются и отправляются сервером в ответ на запрос от клиента. Когда клиент отправляет запрос на сервер, сервер может включить в ответ заголовок Set-Cookie, чтобы установить куки на стороне клиента (рис. 2.12).

Куки генерируются

Выберите один вариант из списка

☒ Всё правильно.

☐ клиентом

☒ сервером

Следующий шаг

Решить снова

[Ваши решения](#)

Рис. 2.12: Персонализация сети. Вопрос №3

Сессионные куки хранятся в браузере только на время активной сессии пользователя на веб-сайте. Как только пользователь закрывает окно браузера или завершает сеанс, сессионные куки обычно удаляются. (рис. 2.13).

Сессионные куки хранятся в браузере?

Выберите один вариант из списка



Верно. Так держать!

☐ Нет

☒ Да, на время пользования веб-сайтом

☐ Да, на некоторое время, заданное в сервером

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: **0 баллов** из 1

Рис. 2.13: Персонализация сети. Вопрос №4

2.1.3 Браузер TOR. Анонимизация

Луковая сеть TOR использует три промежуточных узла для обеспечения анонимности пользователей. Когда пользователь отправляет запрос на веб-сайт через TOR, его запрос проходит через три промежуточных узла, прежде чем достигнет конечного назначения (рис. 2.14).

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Всё правильно.

☐ 2

☒ 3

☐ 4

Следующий шаг

Решить снова

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

Рис. 2.14: Браузер TOR. Анонимизация. Вопрос №1

В луковой сети TOR IP-адрес получателя известен отправителю, так как он должен знать, куда отправлять данные. Также IP-адрес получателя известен выходному узлу, так как это последний узел в цепочке, который фактически отправляет запрос на сервер получателя (рис. 2.15).

IP-адрес получателя известен

Выберите все подходящие ответы из

☒ Так точно!

Вы решили сложную задачу, поздравляем! Вы можете задать свои вопросы, или сравнить своё решение с другими пользователями.

- ☐ охранному узлу
- ☐ промежуточному узлу
- ☒ отправителю
- ☒ выходному узлу

Следующий шаг

Решить снова

Рис. 2.15: Браузер TOR. Анонимизация. Вопрос №2

В луковой сети TOR общий секретный ключ генерируется между отправителем и каждым узлом в цепочке (охранным, промежуточным и выходным), так как каждый из узлов “снимает” один из слоев шифра (расшифровывает) (рис. 2.16).

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

☒ Абсолютно точно.

- ☐ только с охраным узлом
- ☐ с охраным и промежуточным узлом
- ☒ с охраным, промежуточным и выходным узлом
- ☐ с промежуточным и выходным узлом

Следующий шаг

Решить снова

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

Рис. 2.16: Браузер TOR. Анонимизация. Вопрос №3

Нет, пользователь не обязан использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов. TOR используется для анонимного и безопасного доступа к ресурсам в сети (рис. 2.17).

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

Выберите один вариант из списка

☒ Так точно!

Верно решил 961 учащийся
Из всех попыток 74% верно

- ☒ Нет
- ☐ Да

Следующий шаг

Решить снова

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

Рис. 2.17: Браузер TOR. Анонимизация. Вопрос №4

2.1.4 Беспроводные сети Wi-fi

Wi-Fi является стандартом беспроводной связи, который позволяет устройствам подключаться к сети и обмениваться данными через радиоволновой сигнал. Этот стандарт определяется в IEEE 802.11 и используется для создания беспроводных локальных сетей (WLAN) (рис. 2.18).

Wi-Fi - это

Выберите один вариант из списка

☒ Верно.

- ☐ 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. 2.18: Беспроводные сети Wi-fi. Вопрос №1

Протокол WiFi определяет способы доступа к беспроводной среде и форматирование данных для передачи через радиоканал. Это происходит на канальном уровне модели OSI, который отвечает за передачу данных по физической среде. (рис. 2.19).

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

☒ Прекрасный ответ.

- ☐ Транспортном
- ☐ Прикладном
- ☒ Канальном
- ☐ Сетевом

Следующий шаг

Решить снова

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

Рис. 2.19: Беспроводные сети Wi-fi. Вопрос №2

WEP (Wired Equivalent Privacy) был одним из первых методов шифрования, использованных в беспроводных сетях Wi-Fi. Он устарел, в частности, потому, что использовал малую длину ключа: так, например, он использовал длину ключа в 40 бит, это довольно мало на сегодняшний день, он может быть легко взломан (рис. 2.20).

Выберите один вариант из списка

✓ Здорово, всё верно.

A screenshot of a quiz interface. At the top, it says 'Выберите один вариант из списка' (Choose one option from the list). Below this, there is a green checkmark icon followed by the text 'Здорово, всё верно.' (Great, everything is correct). The main area contains a list of four radio button options: WPA, WEP, WPA2, and WPA3. The 'WEP' option is selected, indicated by a green dot. Below the list 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 the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Следующий шаг

Решить снова

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

Рис. 2.20: Беспроводные сети Wi-fi. Вопрос №3

После успешной аутентификации устройств в сети Wi-Fi, данные, передаваемые между этими устройствами и роутером, могут передаваться в открытом виде. Тем не менее, если используется шифрование (например, WPA2 или WPA3), то данные передаются в зашифрованном виде после успешной аутентификации. (рис. 2.21).

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓ Отлично!

A screenshot of a quiz interface. At the top, it says 'Выберите один вариант из списка' (Choose one option from the list). Below this, there is a green checkmark icon followed by the text 'Отлично!' (Great!). The main area contains a list of four radio button options: 'передаются в зашифрованном виде после аутентификации устройств' (transmitted in encrypted form after device authentication), 'передаются в открытом виде после аутентификации устройств' (transmitted in open form after device authentication), 'передаются в открытом виде' (transmitted in open form), and 'передаются в зашифрованном виде' (transmitted in encrypted form). The first option is selected, indicated by a green dot. Below the list 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 the text 'Вы получили: 1 балл из 1' (You received: 1 point out of 1).

☒ передаются в зашифрованном виде после аутентификации устройств

☐ передаются в открытом виде после аутентификации устройств

☐ передаются в открытом виде

☐ передаются в зашифрованном виде

Следующий шаг

Решить снова

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

Рис. 2.21: Беспроводные сети Wi-fi. Вопрос №4

WPA Personal — это тип аутентификации по паролю, который часто применяется в домашних сетях или небольших корпоративных сетях. В случае использования этого метода, каждый пользователь подключается к сети, используя общий предварительно установленный пароль. В отличие от этого, WPA Enterprise — это более сложный метод аутентификации, при котором существует централизованная база данных всех пользователей. При подключении к сети WiFi, пользователь проверяется в этой базе данных, что обычно хранится на специальных серверах. Этот метод обеспечивает более высокий уровень безопасности, но, как правило, он не требуется для небольших домашних сетей (рис. 2.22).

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

✓ Абсолютно точно.

☒ WPA2 Personal

☐ WPA2 Enterprise

Следующий шаг

Решить снова

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

Рис. 2.22: Беспроводные сети Wi-fi. Вопрос №5

2.2 Защита ПК/телефона

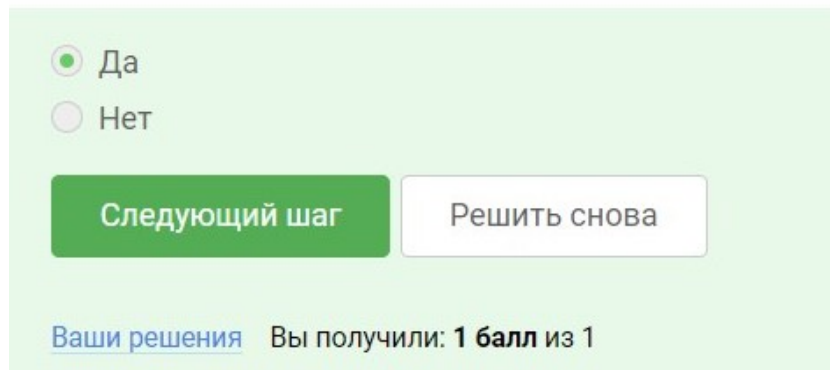
2.2.1 Шифрование диска

Загрузочный сектор диска содержит информацию, необходимую для загрузки операционной системы при запуске компьютера. Этот сектор также может быть зашифрован, чтобы обеспечить дополнительный уровень безопасности и защиты данных на диске от несанкционированного доступа. (рис. 2.23).

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Прекрасный ответ.



☒ Да

☐ Нет

Следующий шаг

Решить снова

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

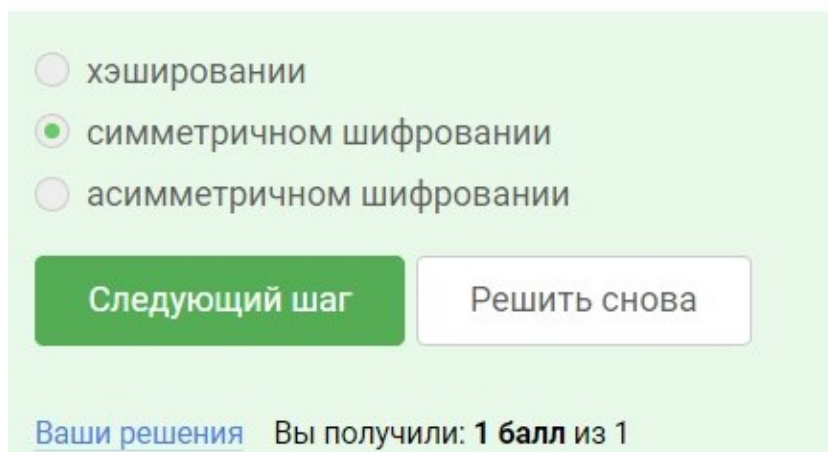
Рис. 2.23: Шифрование диска. Вопрос №1

В симметричном шифровании используется один и тот же ключ для шифрования и дешифрования данных. При шифровании диска такой ключ используется для зашифрования данных, а затем для их дешифрования при необходимости доступа к данным на диске (рис. 2.24).

Шифрование диска основано на

Выберите один вариант из списка

✓ Отлично!



☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

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

Рис. 2.24: Шифрование диска. Вопрос №2

Зашифровать жесткий диск с помощью следующих программ: BitLocker и VeraCrypt. Обе эти программы предоставляют возможность шифрования данных на жестком диске для обеспечения их безопасности и защиты от несанкционированного доступа.

Wireshark используется для анализа сетевого трафика, а Disk Utility (или Дисковая утилита) преимущественно для работы с дисками на операционных системах Mac OS (рис. 2.25).

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

✓ Отлично!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учих вопросы, или сравнить своё решение с другими на [форуме решений](#).

- ☒ BitLocker
- ☐ Wireshark
- ☒ VeraCrypt
- ☐ Disk Utility

Следующий шаг

Решить снова

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

Рис. 2.25: Шифрование диска. Вопрос №3

2.2.2 Пароли

Стойкими можно считать пароли, которые включают в себя сложную комбинацию символов, такие как буквы в верхнем и нижнем регистрах, цифры и специальные символы, и имеют достаточную длину для предотвращения атак методом перебора (рис. 2.26).

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQr9@j4!S\$
- ☐ IDONTLOVECATS

Следующий шаг

Решить снова

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

Рис. 2.26: Пароли. Вопрос №1

Менеджеры паролей представляют собой защищенное приложение, которое помогает хранить и организовывать пароли, обеспечивая их безопасность с помощью мощного шифрования и других мер безопасности. При использовании менеджера паролей пользователю необходимо помнить только один основной пароль для доступа к приложению, а все остальные пароли хранятся в безопасном хранилище (рис. 2.27).

Где безопасно хранить пароли?

Выберите один вариант из списка

☒ Верно.

- ☒ 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. 2.27: Пароли. Вопрос №2

Капча представляет собой тест, который обычно решают люди легко, но который сложно или невозможно выполнить для компьютерных программ или роботов. Она используется для различия между человеком и автоматизированными программами (ботами), что помогает защитить веб-ресурсы от спама, несанкционированного доступа и других видов вредоносной деятельности (рис. 2.28).

Зачем нужна капча?

Выберите один вариант из списка

Верно
Из 5

✓ Верно.

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.28: Пароли. Вопрос №3

Хэширование паролей преобразует пароль в непонятную для человека строку (хэш), которая не может быть преобразована обратно в исходный пароль. Это обеспечивает безопасное хранение паролей на сервере, так как даже если злоумышленник получит доступ к базе данных хэшей паролей, ему будет крайне сложно или невозможно восстановить исходные пароли (рис. 2.29).

Для чего применяется хэширование паролей?

Выберите один вариант из списка

✓ Отличное решение!

- ☐ 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. 2.29: Пароли. Вопрос №4

Использование соли (случайной дополнительной строки, добавляемой к па-

ролю перед хэшированием) не поможет улучшить стойкость паролей к атаке перебором, если злоумышленник получил доступ к серверу.

Соль предназначена для усложнения процесса подбора паролей. Однако, если злоумышленник получил доступ к серверу и базе данных паролей, то соль также будет доступна ему, что делает ее бесполезной для защиты паролей в этом случае. (рис. 2.30).

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

Выберите один вариант из списка

☒ Правильно, молодец!

Верно решили 967 уча
Из всех попыток 66% е

☒ Нет
☐ Да

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.30: Пароли. Вопрос №5

Все приведенные методы защищают от утечек данных атакой перебором (рис. 2.31).

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных вопросы, или сравнить своё решение с другими на [форуме решений](#)

- ☒ разные пароли на всех сайтах
- ☒ периодическая смена паролей
- ☒ сложные(=длинные) пароли
- ☒ капча

Следующий шаг

Решить снова

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

Рис. 2.31: Пароли. Вопрос №6

2.2.3 Фишинг

Выбранные ссылки могут пытаться подделать легитимные веб-сайты банков и интернет-провайдеров, чтобы получить доступ к учетным данным пользователей. Необходимо обратить внимание, что настоящие страницы входа в банковские или почтовые аккаунты обычно имеют домены, которые принадлежат этим организациям, а не сторонним сервисам, как в приведенных примерах. (рис. 2.32).

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

☒ Отличное решение!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#), ответить на их вопросы, или сравнить своё решение с другими на [форуме решений](#).

- ☐ <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. 2.32: Фишинг. Вопрос №1

Фишинговое письмо может прийти от знакомого адреса. Злоумышленники могут подделывать адрес отправителя, делая его похожим на адрес знакомого или даже настоящего контакта, чтобы убедить получателя открыть вредоносный вложение или перейти по ссылке на поддельный веб-сайт (рис. 2.33).

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка

☒ Верно.

- ☒ Да
- ☐ Нет

Следующий шаг

Решить снова

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

Рис. 2.33: Фишинг. Вопрос №2

2.2.4 Вирусы. Примеры

Спуфинг - это метод, который используется для изменения адреса отправителя электронной почты, делая его похожим на адрес, с которого обычно приходят легитимные сообщения. Это может использоваться злоумышленниками для фишинговых атак или распространения вредоносных программ (рис. 2.34).

Email Спуфинг -- это

Выберите один вариант из списка



Верно. Так держать!

- ☐ атака перебором паролей
- ☐ метод предотвращения фишинга
- ☒ подмена адреса отправителя в имейлах
- ☐ протокол для отправки имейлов

Следующий шаг

Решить снова

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

Рис. 2.34: Вирусы. Примеры. Вопрос №1

Вирус-троян получил свое название от легенды о древнегреческом троянском коне, который скрывал в себе вооруженных воинов. Такой вирус маскируется под полезное или легитимное программное обеспечение, чтобы обмануть пользователя и получить доступ к системе или данным (рис. 2.35).

Выберите один вариант из списка

✓ Правильно.

- ☐ 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: ••• из 1

Рис. 2.35: Вирусы. Примеры. Вопрос №2

2.2.5 Безопасность мессенджеров

Ключ шифрования в протоколе мессенджеров Signal формируется при генерации первого сообщения стороной-отправителем. Это обеспечивает конфиденциальность и безопасность обмена сообщениями с момента начала общения между отправителем и получателем (рис. 2.36).

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

✓ Всё получилось!

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

Следующий шаг

Решить снова

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

Рис. 2.36: Безопасность мессенджеров. Вопрос №1

Суть сквозного шифрования заключается в том, что сообщения передаются по узлам связи (серверам) в зашифрованном виде. Это означает, что данные шифруются на устройстве отправителя и дешифруются только на устройстве получателя, при этом промежуточные серверы (узлы связи) не имеют доступа к содержанию сообщений (рис. 2.37).

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Всё получилось!

- ☒ 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. 2.37: Безопасность мессенджеров. Вопрос №2

2.3 Криптография на практике

2.3.1 Введение в криптографию

В асимметричных криптографических примитивах обе стороны имеют пару ключей. Это пара ключей состоит из открытого и секретного ключей. Открытый ключ публикуется в открытом доступе, а закрытый или секретный ключ сторона хранит у себя (рис. 2.38).

В асимметричных криптографических примитивах

Выберите один вариант из списка

☒ Верно.

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 2.38: Введение в криптографию. Вопрос №1

Криптографическая хэш-функция является стойкой к коллизиям, эффективно вычисляется и дает на выходе фиксированное число бит независимо от объема входных данных. Криптографическая хэш-функция не обеспечивает конфиденциальность данных, она используется для генерации хэш-кодов (рис. 2.39).

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [комментариях](#) к их вопросам, или сравнить своё решение с другими на [форуме решений](#).

- ☐ обеспечивает конфиденциальность захэшированных данных
- ☒ стойкая к коллизиям
- ☒ эффективно вычисляется
- ☒ дает на выходе фиксированное число бит независимо от объема входных данных

Следующий шаг

Решить снова

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

Рис. 2.39: Введение в криптографию. Вопрос №2

К алгоритмам цифровой подписи относятся RSA, ECDSA и ГОСТ Р 34.10-2012. AES и SHA2 относятся к алгоритмам шифрования, но не к алгоритмам цифровой подписи (рис. 2.40).

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Отлично!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных
их вопросы, или сравнить своё решение с другими на [форуме решений](#)

- ☐ AES
- ☐ SHA2
- ☒ RSA
- ☒ ECDSA
- ☒ ГОСТ Р 34.10-2012

Следующий шаг

Решить снова

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

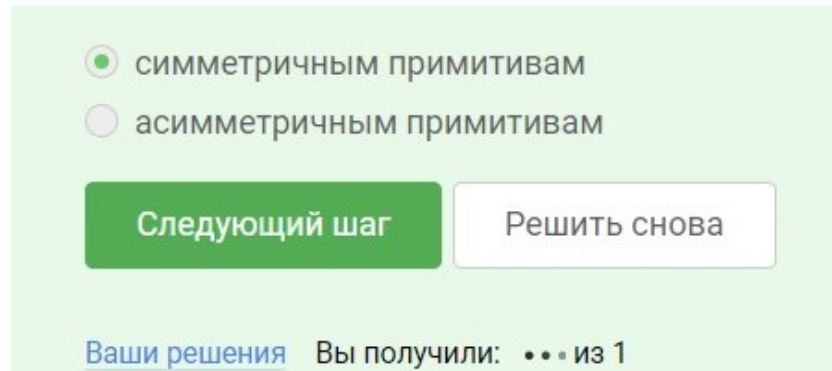
Рис. 2.40: Введение в криптографию. Вопрос №3

Код аутентификации - это симметричный примитив, который берет на вход какой-то ключ (это должен быть другой ключ, не тот, с которого мы шифровали) и сообщение и выдает код аутентификации сообщения. Корректно об этом примитиве думать, как о симметричной версии подписи. Как правило, код аутентификации сообщения строится с помощью хэш-функции или симметричного шифрования. Код аутентификации обеспечивает целостность данных (рис. 2.41).

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошая работа.



☒ симметричным примитивам

☐ асимметричным примитивам

Следующий шаг

Решить снова

Ваши решения Вы получили: ... из 1

Рис. 2.41: Введение в криптографию. Вопрос №4

Самым популярным примером протокола обмена ключами является протокол Диффи-Хэллмана, как раз он, либо его модификации используются в современных мессенджерах и в протоколе TLS для того, чтобы мы смогли сгенерировать **общий секретный ключ** и дальше шифровать наши данные с помощью симметричного алгоритма, то есть с помощью ключа sk_{AB} . Если реализовать генерацию общего ключа так, как она описана у Диффи-Хэллмана, мы получим довольно слабый протокол, нестойкий к активным злоумышленникам. Сделать этот протокол стойким к активным злоумышленникам помогает цифровая подпись (рис. 2.42).

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

☒ Верно. Так держать!

- ☐ симметричный примитив генерации общего секретного ключа
- ☐ асимметричный примитив генерации общего открытого ключа
- ☒ асимметричный примитив генерации общего секретного ключа
- ☐ асимметричный алгоритм шифрования

Следующий шаг

Решить снова

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

Рис. 2.42: Введение в криптографию. Вопрос №5

2.3.2 Цифровая подпись

Протокол электронной цифровой подписи относится к протоколам с публичным (или открытым) ключом. Эти протоколы используют пару ключей - публичный (или открытый) и приватный (секретный) - для создания и проверки цифровых подписей (рис. 2.43).

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

☒ Хорошая работа.

- ☐ протоколам с симметричным ключом
☒ протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

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

Рис. 2.43: Цифровая подпись. Вопрос №1

Алгоритм верификации электронной цифровой подписи требует на вход подпись, открытый ключ, сообщение. Это позволяет алгоритму проверить подлинность сообщения с использованием открытого ключа, соответствующего закрытому ключу, с помощью которого была создана цифровая подпись (рис. 2.44).

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Верно. Так держать!

- ☒ подпись, открытый ключ, сообщение
☐ подпись, секретный ключ
☐ подпись, секретный ключ, сообщение
☐ подпись, открытый ключ

Следующий шаг

Решить снова

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

Рис. 2.44: Цифровая подпись. Вопрос №2

Электронная цифровая подпись не обеспечивает конфиденциальность. Электронная цифровая подпись обеспечивает аутентификацию, целостность и неотказ от авторства, но не скрывает содержимое сообщения от посторонних лиц (рис. 2.45).

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

✓ Всё получилось!

- ☒ конфиденциальность
- ☐ целостность
- ☐ аутентификацию
- ☐ отказ от авторства

Следующий шаг

Решить снова

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

Рис. 2.45: Цифровая подпись. Вопрос №3

Усиленная неквалифицированная подпись может быть подтверждена сертификатом, который может быть выпущен самостоятельно, то есть кроме того, что пользователь выпускает свою пару секретных ключей, он еще и может сам их сертифицировать. Такая подпись может быть использована в коммерческом документообороте в небольших негосударственных структурах. А вот что касается усиленной квалифицированной подписи, эта подпись уже имеет юридическую силу, она, как правило, равнозначна рукописной (рис. 2.46).

Какой тип сертификата электронной подписи понадобится для отправки налоговой отчетности в ФНС?

Выберите один вариант из списка

✓ Правильно, молодец!

- ☒ усиленная квалифицированная
- ☐ простая
- ☐ усиленная неквалифицированная

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.46: Цифровая подпись. Вопрос №4

Получить квалифицированный сертификат ключа проверки электронной подписи можно в удостоверяющем (сертификационном) центре. Эти центры имеют соответствующие полномочия и аккредитации для выдачи квалифицированных сертификатов, которые имеют юридическую силу (рис. 2.47).

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

Выберите один вариант из списка

✓ Верно.

Верно решили 9
Из всех попыток

- ☐ в любой организации, имеющей соответствующую лицензию ФСБ
- ☐ в минкомсвязи РФ
- ☒ в удостоверяющем (сертификационном) центре
- ☐ в любой организации по месту работы

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1


Рис. 2.47: Цифровая подпись. Вопрос №5

2.3.3 Электронные платежи

Платежные системы: MasterCard - одна из крупнейших мировых платежных систем. МИР - российская национальная платежная система. Платежные системы обычно обеспечивают возможность осуществления электронных и физических транзакций между покупателем и продавцом, включая торговлю онлайн, в магазинах и через банкоматы (рис. 2.48).

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

 Отлично!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных вопросы, или сравнить своё решение с другими на [форуме реше](#)

☐ BitCoin

☒ MasterCard

☐ SecurePay

☐ POS-терминал

☐ банкомат

☒ МИР

Следующий шаг

Решить снова

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

Рис. 2.48: Электронные платежи. Вопрос №1

Данные примеры демонстрируют использование нескольких факторов (что-то, что пользователь знает и что-то, что пользователь имеет или может получить) для повышения безопасности процесса аутентификации (рис. 2.49).

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

✓ Хорошая работа.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальных их вопросы, или сравнить своё решение с другими на [форуме решений](#)

- ☐ комбинация проверки пароля + Капча
- ☒ комбинация проверка пароля + код в sms сообщении
- ☒ комбинация код в sms сообщении + отпечаток пальца
- ☐ комбинация PIN код + пароль

Следующий шаг

Решить снова

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

Рис. 2.49: Электронные платежи. Вопрос №2

При онлайн платежах сегодня используется многофакторная аутентификация покупателя перед банком-эмитентом. Это означает, что для подтверждения платежа требуется предоставление нескольких видов аутентификационных данных или факторов безопасности, таких как пароль, одноразовый код, отпечаток пальца или другие подтверждения, чтобы обеспечить дополнительный уровень безопасности и защиты от мошенничества (рис. 2.50).

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☒ 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. 2.50: Электронные платежи. Вопрос №3

2.3.4 Блокчейн

Свойство криптографической хэш-функции, которое используется в доказательстве работы, это сложность нахождения прообраза. Доказательство работы включает в себя выполнение некоторой вычислительной работы, результат которой должен удовлетворять определенным критериям, например, начинать с определенного количества нулей в хэш-значении. Это требование обеспечивает, что выполнение работы требует значительных вычислительных ресурсов (рис. 2.51).

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

☒ Верно. Так держать!

- ☐ фиксированная длина выходных данных
- ☒ сложность нахождения прообраза
- ☐ обеспечение целостности
- ☐ эффективность вычисления

Следующий шаг

Решить снова

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

Рис. 2.51: Блокчейн. Вопрос №1

Консенсус в терминах криптовалют представляет собой общепризнанное соглашение, закодированное в общедоступной структуре данных, известной как “бухгалтерская книга”. Этот “ledger” хранит историю всех транзакций, учитывая, кто передал какие средства кому и когда. Эта структура данных должна соответствовать четырем основным принципам. Во-первых, это постоянство, что означает, что добавленные данные не должны быть удалены. Во-вторых, это единое мнение, или сам консенсус, когда все участники видят и соглашаются с одинаковыми данными, за исключением недавних изменений. В-третьих, это живучесть, что позволяет добавлять новые транзакции по мере необходимости. И, наконец, открытость, так как любой может стать участником этой структуры данных блокчейна, по крайней мере, в случае с Bitcoin (рис. 2.52).

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Верно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным уч
их вопросы, или сравнить своё решение с другими на [форуме решений](#).

- ☒ открытость
- ☒ живучесть
- ☒ постоянства
- ☒ консенсус

Следующий шаг

Решить снова

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

Рис. 2.52: Блокчейн. Вопрос №2

Секретные ключи, которые хранят участники блокчейна, относятся к криптографическому примитиву “цифровая подпись”. Эти ключи используются для создания и верификации цифровых подписей, которые подтверждают подлинность и авторство транзакций в блокчейне (рис. 2.53).

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Всё получилось!

- ☐ обмен ключами
- ☐ шифрование
- ☒ цифровая подпись
- ☐ хэш-функция

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.53: Блокчейн. Вопрос №3

На этом курс заканчивается. После прохождения сертификат не выдается, а лишь появляется уведомление об успешном прохождении (рис. 2.54).

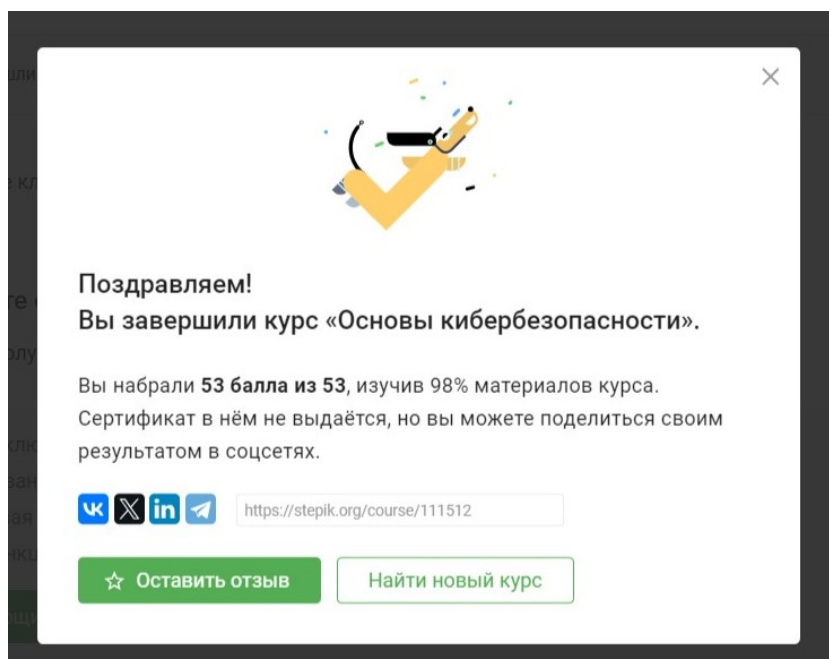


Рис. 2.54: Окончание курса

3 Выводы

В ходе прохождения курса “Основы кибербезопасности” я узнала новую полезную информацию о безопасности в сети и криптографии.