

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ ПО

дисциплина: Основы информационной безопасности

Студент: Исаев Булат Абубакарович

Студ. Билет: 1132227131

Группа: НПИбд-01-22

МОСКВА

2024 г.

Цель работы

Пройти спец. курс “Основы кибербезопасности” и получить сертификат.

Выполнение заданий курса

Раздел 1: “О курсе”

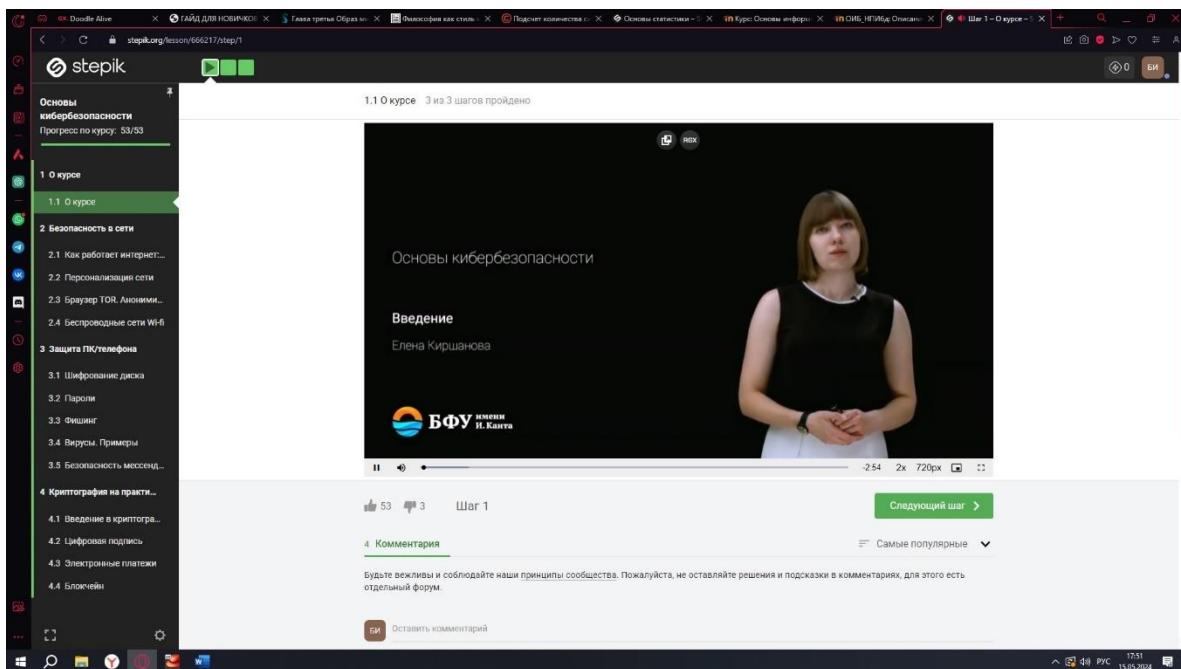


Рис. Раздел (1) – Вступление

В этом разделе нам в видео объясняют о чём будет этот курс.

Раздел 2: “Безопасность в сети”

(2.1) “Как работает интернет: базовые сетевые протоколы”

The screenshot shows a computer screen displaying a Stepik course titled "Основы кибербезопасности". The current lesson is "2 Безопасность в сети" and the specific question is "2.1 Как работает интернет: базовые сетевые протоколы". The question asks to select the application-layer protocol from a list: UDP, TCP, HTTPS, and IP. The "HTTPS" option is selected. Below the question, there is a green button labeled "Следующий шаг" and a white button labeled "Решить снова". To the right, a statistics box shows "Верно решили 895 учащихся" and "Из всех попыток 50% верных". At the bottom, there is a comment section with one comment from "Георгий Зинченко" and a timestamp "13:49 13.03.2024". The task bar at the bottom of the screen shows various icons and the date "13.03.2024".

Рис. Раздел (2.1) – Вопрос 1

Вопрос: Выберите протокол прикладного уровня

Ответ: HTTPS

UDP – транспортного уровня

TCP – транспортного уровня

HTTPS – прикладной уровня

IP – сетевого уровня

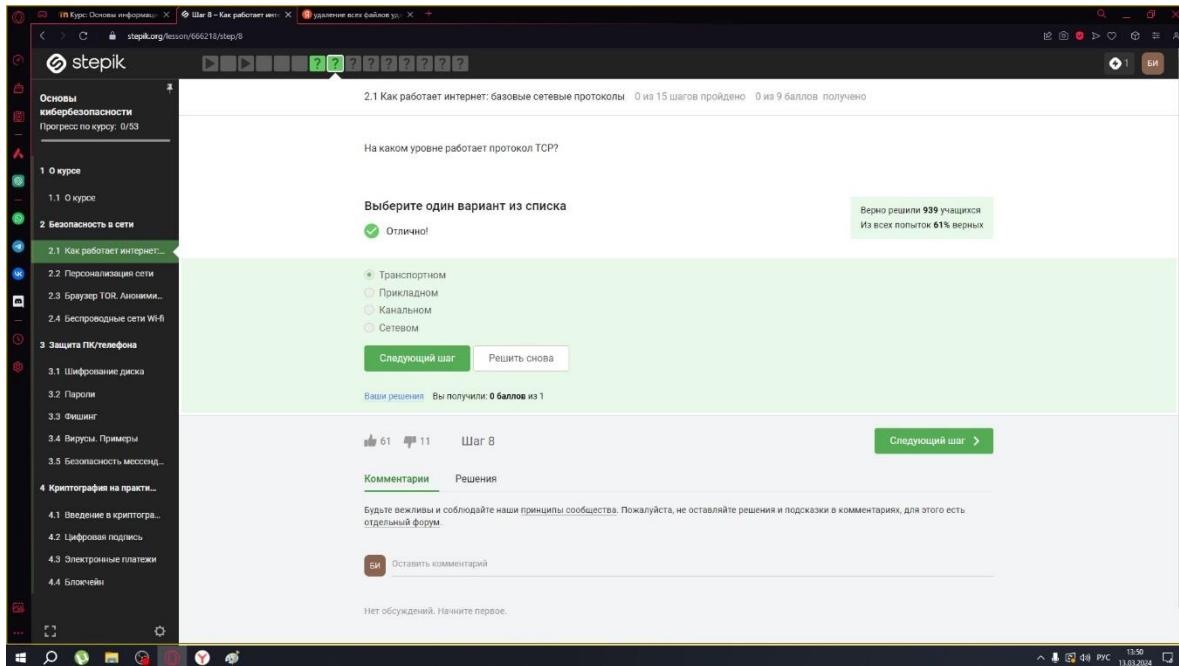


Рис. Раздел (2.1) – Вопрос 2

Вопрос: На каком уровне работает протокол TCP?

Ответ: TCP работает на транспортном уровне, который является 4-м уровнем в модели OSI

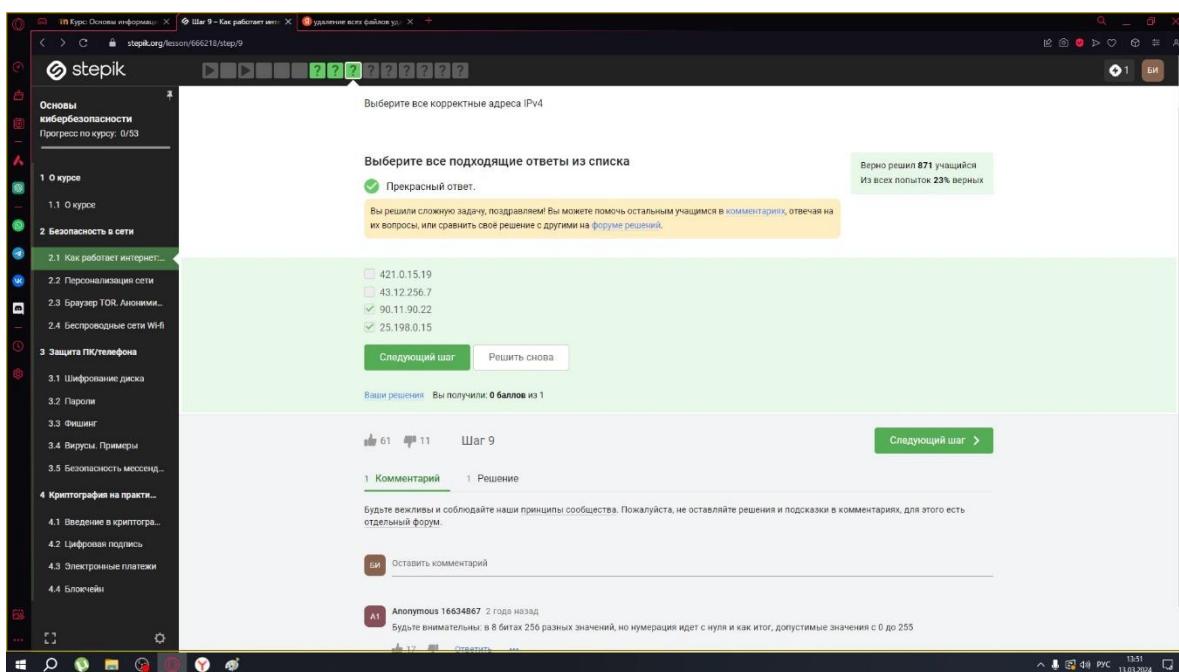


Рис. Раздел (2.1) – Вопрос 3

Вопрос: Выберите все корректные адреса IPv4

Ответ: Корректные адреса IPv4 состоят из чисел от 0 до 255

The screenshot shows a computer screen with a browser window open to a Stepik course page. The course navigation sidebar on the left lists sections such as 'Основы кибербезопасности' (Fundamentals of Cybersecurity), '2 Безопасность в сети' (Network Security), '2.1 Как работает интернет...' (How the Internet works...), and others. The main content area displays a question titled 'DNS сервер' (DNS server). The question asks to select one option from a list: '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' (selects a route for a packet in the network), and 'выполняет адресацию на хосте' (performs addressing at the host level). A green checkmark indicates that the first option is correct. Below the question are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). At the bottom of the page, there is a comment section with 61 comments and 11 likes, and a link to 'Показать обсуждения (1)' (Show discussions (1)). The status bar at the bottom of the screen shows system icons and the date/time: '13.03.2024 13:52'.

Рис. Раздел (2.1) – Вопрос 4

Вопрос: DNS сервер это

Ответ: DNS сервер - система, переводящая доменные имена в IP-адреса, позволяя пользователям легко находить веб-сайты в интернете.

The screenshot shows a computer screen displaying a Stepik course titled 'Основы кибербезопасности'. The current lesson is 'Шаг 11 – Как работает интернет' (Step 11 - How the Internet works). The question asks: 'Выберите корректную последовательность протоколов в модели TCP/IP'. The correct answer is marked as 'Прекрасный ответ' (Great answer). Below the question, there is a list of four options:

- сетевой – прикладной – канальный – транспортный
- прикладной – транспортный – канальный – сетевой
- транспортный – сетевой – прикладной – канальный
- прикладной – транспортный – сетевой – канальный

Below the list are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green bar at the bottom indicates 'Ваши решения' (Your solutions) and 'Вы получили: 0 баллов из 1' (You got: 0 points out of 1). The interface includes a sidebar with course navigation and a footer with system status icons.

Рис. Раздел (2.1) – Вопрос 5

Вопрос: Выберите корректную последовательность протоколов в модели TCP/IP

Ответ: В модели TCP/IP, которая является набором сетевых протоколов, используемых для передачи данных в интернете, протоколы организованы в четыре уровня: прикладной – транспортный – сетевой – канальный

The screenshot shows a computer screen displaying a Stepik course titled 'Основы кибербезопасности'. The current lesson is 'Шаг 12 – Как работает интернет' (Step 12 - How the Internet works). The question asks: 'Протокол http предполагает'. The correct answer is marked as 'Верно'. Below the question, there is a list of two options:

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

Below the list are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green bar at the bottom indicates 'Ваши решения' (Your solutions) and 'Вы получили: 0 баллов из 1' (You got: 0 points out of 1). The interface includes a sidebar with course navigation and a footer with system status icons.

Рис. Раздел (2.1) – Вопрос 6

Вопрос: Протокол http предполагает

Ответ: Протокол HTTP предполагает стандартный способ передачи веб-страниц от сервера к клиенту

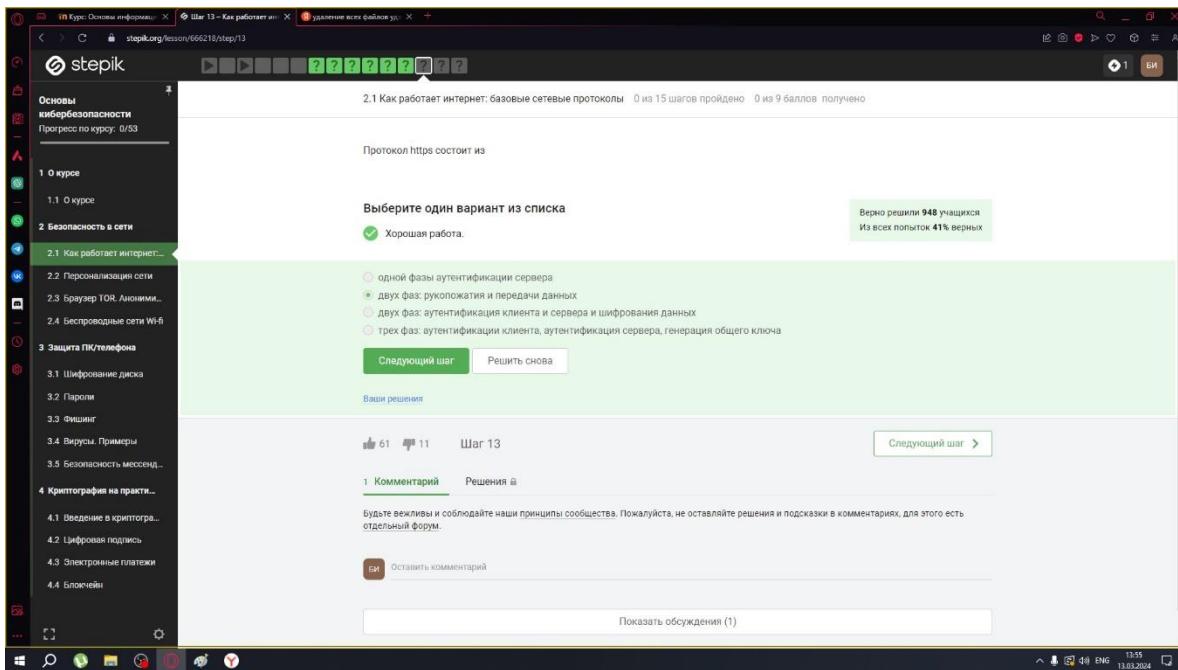


Рис. Раздел (2.1) – Вопрос 7

Вопрос: Протокол https состоит из

Ответ: Протокол HTTPS включает в себя две основные фазы в процессе установления защищенного соединения между клиентом и сервером:

1. **Фаза рукопожатия:** В этой фазе клиент и сервер обмениваются информацией, необходимой для установления безопасного соединения.
2. **Фаза передачи данных:** После успешного рукопожатия и установления защищенного канала связи начинается передача зашифрованных данных.

The screenshot shows a computer screen with a browser window open to a Stepik course page. The course is titled 'Основы кибербезопасности' (Basics of Cybersecurity) and the current step is 'Шаг 14 – Как работает интернет: базовые сетевые протоколы' (Step 14 – How the Internet Works: Basic Network Protocols). The question asks: 'Версия протокола TLS определяется' (The version of the TLS protocol is determined by). Below the question is a list of four options with radio buttons:

- сервером
- клиентом
- и клиентом, и сервером в процессе "переговоров"
- провайдером клиента

Below the list are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). To the right, a green box indicates: 'Верно решили 947 учащихся' (947 students solved correctly) and 'Из всех попыток 55% верных' (55% of all attempts were correct). At the bottom of the page, there are sections for 'Комментарии' (Comments) and 'Решения' (Solutions), along with a note: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' (Be polite and follow our community principles. Please do not leave solutions and hints in comments, for this there is a separate forum.)

Рис. Раздел (2.1) – Вопрос 8

Вопрос: Версия протокола TLS определяется

Ответ: Версия протокола TLS определяется и клиентом, и сервером в процессе “переговоров”.
Процесс переговоров - согласование обоих сторон на общие параметры безопасности, для обеспечения надежного и защищенного соединения.

The screenshot shows a computer screen with a browser window open to a Stepik course page. The course is titled 'Основы кибербезопасности' (Basics of Cybersecurity) and the current step is 'Шаг 15 – Как работает интернет: базовые сетевые протоколы' (Step 15 – How the Internet Works: Basic Network Protocols). The question asks: 'В фазе "рукопожатия" протокола TLS не предусмотрено' (In the "handshake" phase of the TLS protocol, it is not provided). Below the question is a list of five options with radio buttons:

- формирование общего секретного ключа между клиентом и сервером
- автентификация (как минимум одной из сторон)
- выбираются алгоритмы шифрования/автентификации
- шифрование данных

Below the list are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). To the right, a green box indicates: 'Верно решили 931 учащийся' (931 students solved correctly) and 'Из всех попыток 44% верных' (44% of all attempts were correct). At the bottom of the page, there are sections for 'Комментарий' (Comment) and 'Решения' (Solutions), along with a note: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' (Be polite and follow our community principles. Please do not leave solutions and hints in comments, for this there is a separate forum.)

Рис. Раздел (2.1) – Вопрос 9

Вопрос: В фазе “рукопожатия” протокола TLS не предусмотрено

Ответ: В фазе “рукопожатия” протокола TLS не предусмотрено шифрование

(2.2) “Персонализация сети”

The screenshot shows a computer screen with a browser window open to a Stepik course page. The left sidebar lists various course sections and lessons. The main content area displays a question titled "2.2 Персонализация сети". It asks to select all correct answers from a list: IP адрес, идентификатор пользователя, пароль пользователя, and id сессии. A green checkmark is next to the first three items. Below the list are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). At the bottom, there's a comment section with one comment and a link to "Решения" (Solutions). The status bar at the bottom right shows system information like battery level, signal strength, and date.

Рис. Раздел (2.2) – Вопрос 1

Вопрос: Куки хранят:

Ответ: Куки - это небольшие текстовые файлы, которые веб-сайты могут использовать для хранения информации на компьютере пользователя. IP хранится в базе данных провайдеров интернет-услуг. А пароли пользователей обычно хранятся в базах данных на серверах приложений или веб-сайтов.

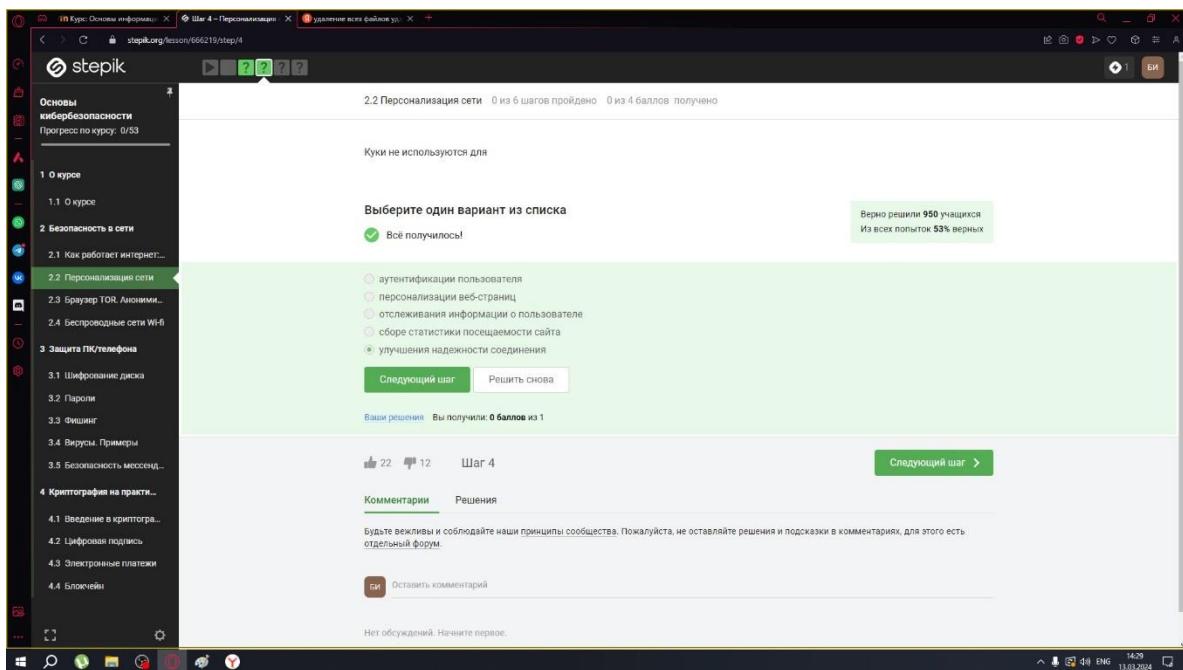


Рис. Раздел (2.2) – Вопрос 2

Вопрос: Куки не используются для

Ответ: Для улучшения надежности сетевого соединения используются различные технологии и протоколы (TCP, HTTPS)

The screenshot shows a computer screen displaying a web browser window for the Stepik platform. The URL is stepik.org/lesson/666219/step/5. The page title is "Шаг 5 – Персонализации". The main content area displays a question: "Куки генерируются" (Cookies are generated) followed by the instruction "Выберите один вариант из списка" (Select one option from the list). Two options are listed: "сервером" (by the server) with a checked radio button, and "клиентом" (by the client) with an unchecked radio button. Below the list are two buttons: "Следующий шаг" (Next step) in green and "Решить снова" (Solve again) in grey. To the right, a green box indicates "Верно решили 968 учащихся" (968 students solved correctly) and "Из всех попыток 79% верных" (79% of all attempts were correct). On the left sidebar, the course navigation is visible, including sections like "Основы кибербезопасности" and "2. Безопасность в сети". The bottom of the screen shows the Windows taskbar with various icons.

Рис. Раздел (2.2) – Вопрос 3

Вопрос: Куки генерируются

Ответ: Когда пользователь посещает веб-сайт, сервер может отправить куки в браузер пользователя для сохранения определённой информации.

The screenshot shows a computer screen displaying the Stepik learning platform. On the left, there's a sidebar with a tree view of course sections and sub-sections. The main area shows a specific step within a lesson. The title of the step is "2.2 Персонализация сети". Below it, a question asks: "Сессионные куки хранятся в браузере?". There are three options: "Да, на время пользования веб-сайтом" (selected), "Да, на некоторое время, заданное в сервером" (radio button), and "Нет" (radio button). A green feedback box at the top right says "Верно решили 959 учащихся" and "Из всех попыток 60% верных". At the bottom of the main area, there are buttons for "Следующий шаг" and "Решить снова". Below the main area, there's a section for comments and solutions, with a note about posting only principles, not answers or hints. A navigation bar at the bottom includes links for "Шаг 6", "Комментарии", and "Решения". The Windows taskbar at the bottom shows various pinned icons.

Рис. Раздел (2.2) – Вопрос 4

Вопрос: Сессионные куки хранятся в браузере?

Ответ: Сессионные куки хранятся в браузере на время пользования веб-сайтом

(2.3) “Браузер TOR. Анонимизация”

The screenshot shows a computer screen displaying a Stepik course titled 'Основы кибербезопасности'. The current lesson is 'Шаг 3 – Браузер TOR. Анонимизация' (Step 3 - TOR Browser. Anonymization). The question asks: 'Сколько промежуточных узлов в луковой сети TOR?' (How many intermediate nodes are there in a Tor onion network?). The correct answer is '3'. Below the question, there are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green box at the top right indicates that 959 users solved the problem correctly. The sidebar on the left lists various course modules and lessons.

Рис. Раздел (2.3) – Вопрос 1

Вопрос: Сколько промежуточных узлов в луковой сети TOR?

Ответ: В сети TOR всего 3 промежуточных узла

The screenshot shows a computer screen displaying a Stepik course titled 'Основы кибербезопасности'. The current lesson is 'Шаг 4 – Браузер TOR. Анонимизация' (Step 4 - TOR Browser. Anonymization). The question asks: 'IP-адрес получателя известен' (The recipient's IP address is known). The correct answer is 'Здорово, всё верно.' (Good, everything is correct). Below the question, there are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green box at the top right indicates that 906 users solved the problem correctly. The sidebar on the left lists various course modules and lessons.

Рис. Раздел (2.3) – Вопрос 2

Вопрос: IP-адрес получателя известен

Ответ: IP-адрес получателя известен только отправителю и выходному узлу

The screenshot shows a computer screen displaying a web browser window for a Stepik.org course. The title bar reads 'Шаг 5 – Браузер TOR. Анонимизация'. The main content area shows a question about Tor browser anonymization. The sidebar on the left lists course modules and lessons, including 'Безопасность в сети' and 'Браузер TOR. Анонимизация'. The right side shows a statistics box with '959' solved users and '55%' correct answers. Below the question are two buttons: 'Следующий шаг' and 'Решить снова'. At the bottom, there are sections for 'Комментарии' and 'Решения'.

Рис. Раздел (2.3) – Вопрос 3

Вопрос: Отправитель генерирует общий секретный ключ

Ответ: Отправитель генерирует общий секретный ключ с охранным, промежуточным и выходным ключом.

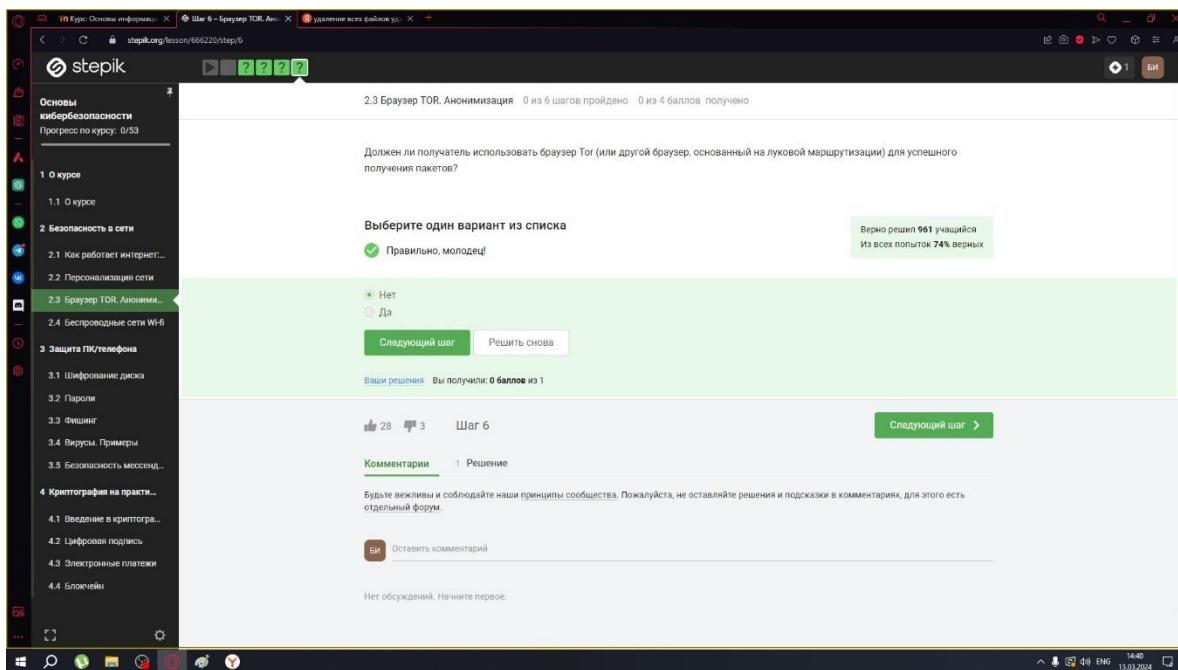


Рис. Раздел (2.3) – Вопрос 4

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

Ответ: Эти браузеры полезны для обеспечения анонимности в Интернете, а не для успешного получения пакетов.

(2.4) “Беспроводные сети Wi-fi”

The screenshot shows a computer screen displaying a course on Stepik. The left sidebar lists chapters and sub-chapters, with '2.4 Беспроводные сети Wi-Fi' currently selected. The main content area shows a question titled 'Wi-Fi - это'. Below it is a list of four options with radio buttons:

- 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 сетью Интернет

Below the list are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green box indicates that 965 users answered correctly. The bottom of the page shows a navigation bar with 'Шаг 4' and a 'Комментарии' section.

Рис. Раздел (2.4) – Вопрос 1

Вопрос: Wi-Fi это

Ответ: Wi-Fi - это беспроводная технология, которая позволяет электронным устройствам подключаться к интернету или обмениваться данными через радиоволны без физического подключения к проводной сети.

The screenshot shows a computer screen displaying a course on the Stepik platform. The course is titled "Основы кибербезопасности" (Basics of Cybersecurity) and is currently at step 5. The specific question shown is "На каком уровне работает протокол WiFi?" (At what level does the WiFi protocol work?). The user has selected the correct answer, "Канальном" (At the channel level), which is marked with a green checkmark. Below the question, there are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). A green bar at the bottom indicates "Вы получили 0 баллов из 1" (You got 0 points out of 1). The sidebar on the left lists various steps and topics, including "Беспроводные сети WiFi" (Wireless network WiFi) which is currently selected. The system status bar at the bottom right shows the date and time as 13.03.2024 14:52.

Рис. Раздел (2.4) – Вопрос 2

Вопрос: На каком уровне работает протокол WiFi?

Ответ: WiFi протокол работает на канальном уровне

This screenshot shows the same Stepik course interface as the previous one, but for step 6. The question is "Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi" (Insecure method for ensuring encryption and authentication in a Wi-Fi network). The user has selected the correct answer, "WEP", which is marked with a green checkmark. The sidebar on the left shows the user has completed 0/53 steps. The system status bar at the bottom right shows the date and time as 13.03.2024 14:52.

Рис. Раздел (2.4) – Вопрос 3

Вопрос: Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Ответ: WEP считается небезопасным для шифрования и аутентификации в Wi-Fi

The screenshot shows a computer screen displaying a course on Stepik. The sidebar on the left lists various sections: 'Основы кибербезопасности' (Fundamentals of Cybersecurity), '1 курс' (Course 1), '2 Безопасность в сети' (Network Security), '2.4 Беспроводные сети Wi-Fi' (Section 2.4: Wireless Networks Wi-Fi), '3 Защита ПК/телефона' (Section 3: PC/Phone Protection), and '4 Криптография на практике' (Section 4: Cryptography in Practice). The main content area is titled '2.4 Беспроводные сети Wi-Fi' and shows a question: 'Данные между хостом сети (компьютером или смартфоном) и роутером'. Below this is a list of four options for how data is transmitted between the host and router: 1) передаются в открытом виде (transmitted in an open format), 2) передаются в зашифрованном виде (transmitted in an encrypted format), 3) передаются в зашифрованном виде после аутентификации устройств (transmitted in an encrypted format after device authentication), and 4) передаются в открытом виде после аутентификации устройств (transmitted in an open format after device authentication). The third option is selected. A green button labeled 'Следующий шаг' (Next step) is visible. At the bottom of the page, there are sections for 'Комментарии' (Comments) and 'Решения' (Solutions), along with a link to 'Шаг 7' (Step 7). The status bar at the bottom right shows the date and time: '13.03.2024 14:53'.

Рис. Раздел (2.4) – Вопрос 4

Вопрос: Данные между хостом сети (компьютером или смартфоном) и роутером

Ответ: Данные между хостом сети (компьютером или смартфоном) и роутером

передаются в зашифрованном виде после аутентификации устройств

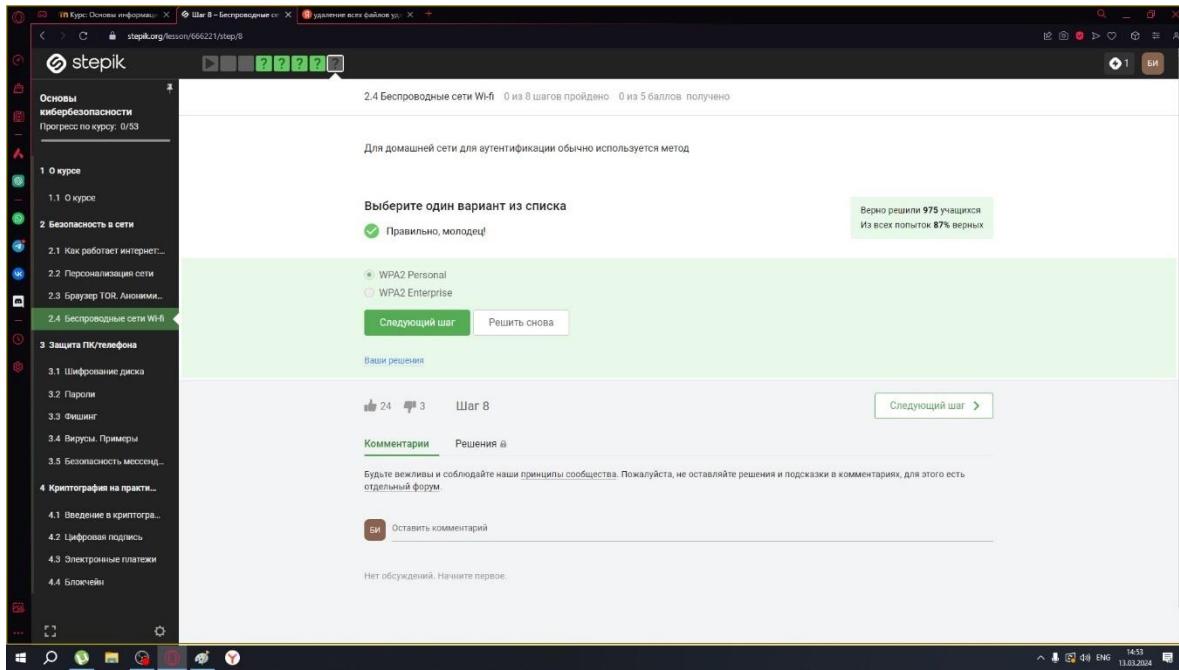


Рис. Раздел (2.4) – Вопрос 5

Вопрос: Для домашней сети для аутентификации обычно используется метод

Ответ: Для домашней сети для аутентификации обычно используется метод WPA2 Personal

Раздел 3: “Защита ПК/телефона”

(3.1) “Шифрование диска”

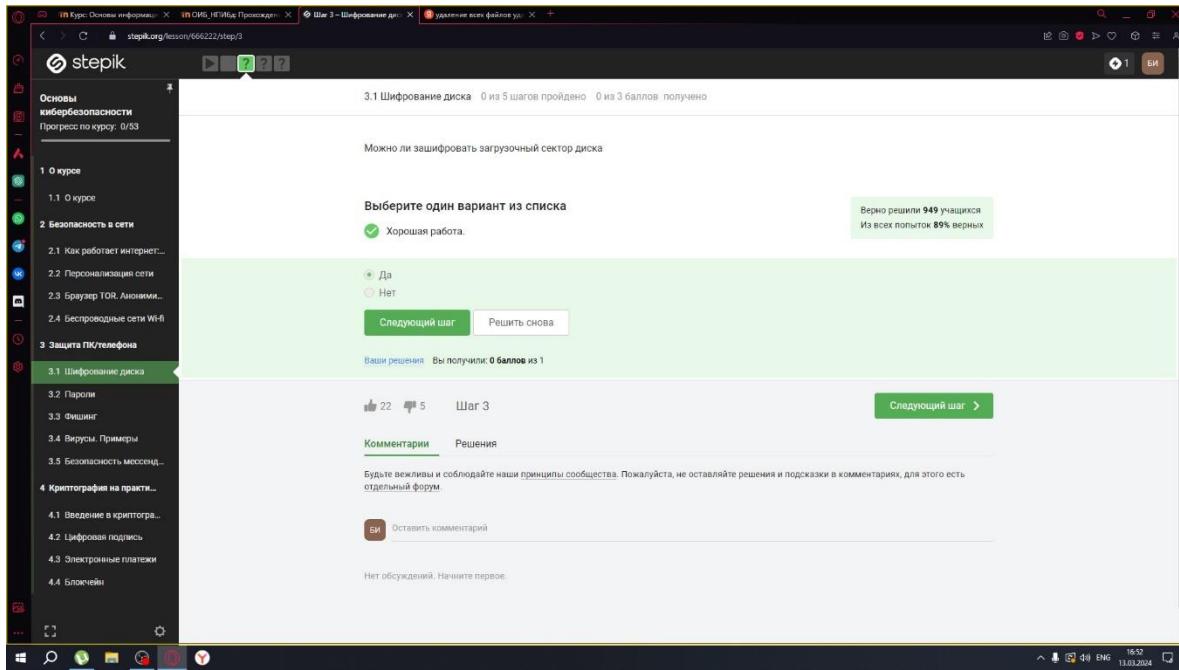


Рис. Раздел (3.1) – Вопрос 1

Вопрос: Можно ли зашифровать загрузочный сектор диска

Ответ: Да, можно зашифровать загрузочный сектор диска

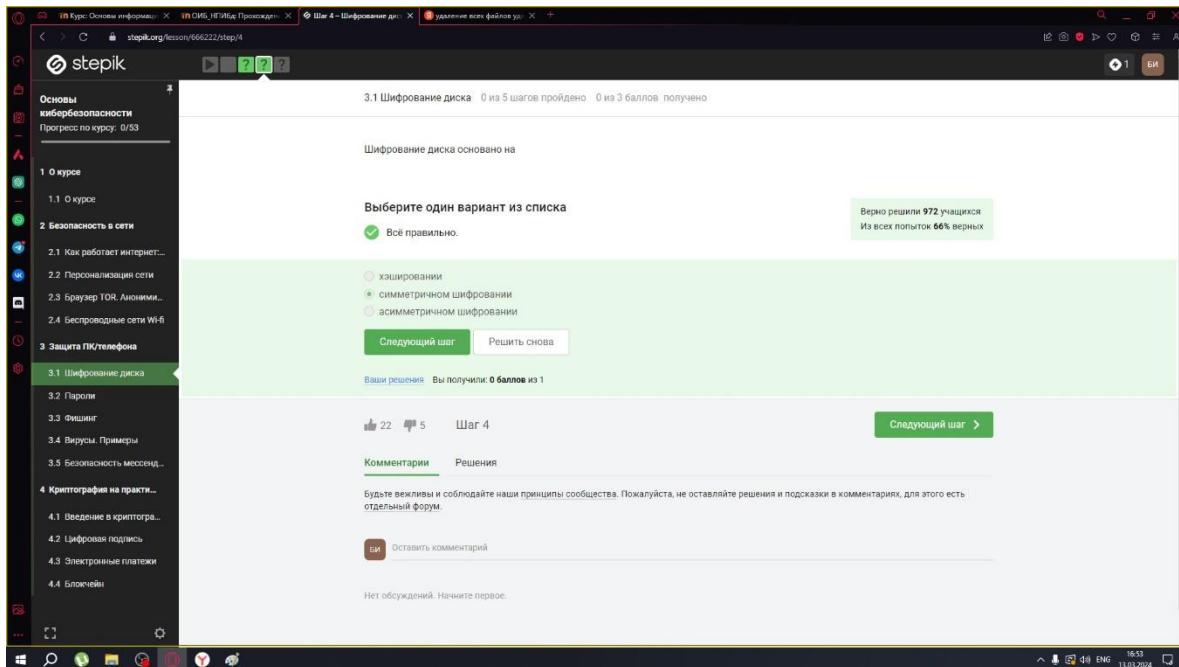


Рис. Раздел (3.1) – Вопрос 2

Вопрос: Шифрование диска основано на

Ответ: Шифрование диска основано на симметричном шифровании

The screenshot shows a computer screen with a browser window open to the Stepik platform. The user is currently on a course titled 'Основы кибербезопасности' (Basics of Cybersecurity). The specific section shown is '3.1 Шифрование диска' (Disk Encryption). The question asks: 'С помощью каких программ можно зашифровать жесткий диск?' (With which programs can you encrypt a hard drive?). Below the question, there is a list of options for users to select: BitLocker, Wireshark, VeraCrypt, and Disk Utility. The 'VeraCrypt' option is checked. At the bottom of the question area, there are two buttons: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green box at the top right indicates that 906 users solved the task correctly (28% of attempts). Below the question, there is a comment section with 22 likes and 5 comments, and a 'Шаг 5' button. At the bottom of the page, there are tabs for 'Комментарии' (Comments) and 'Решения' (Solutions), along with a link to the forum.

Рис. Раздел (3.1) – Вопрос 3

Вопрос: С помощью каких программ можно зашифровать жесткий диск?

Ответ: С помощью BitLocker и VeraCrypt можно зашифровать жесткий диск

(3.2) “Пароли”

The screenshot shows a computer screen displaying a course on Stepik. The left sidebar lists chapters and sub-chapters under 'Основы кибербезопасности'. The main content area is titled 'Шаг 4 – Пароли' and shows a question: 'Какие пароли можно отнести к стойким?'. Below the question is a list of four options with radio buttons. The third option, 'UQr9@j4!S\$', is selected. A green button at the bottom right of the list says 'Следующий шаг'. To the right of the list, a green box indicates 'Всё получилось!' and shows statistics: 'Верно решили 969 учащихся' and 'Из всех попыток 85% верных'. At the bottom of the page, there are sections for 'Комментарии' and 'Решения', and a note about respecting community guidelines.

Рис. Раздел (3.2) – Вопрос 1

Вопрос: Какие пароли можно отнести к стойким?

Ответ: UQr9@j4!S\$, потому что тут используется сложный набор символов

This screenshot shows the same course and lesson as the previous one, but the question has changed. It now asks 'Где безопасно хранить пароли?'. The list of options includes 'В менеджерах паролей', 'В заметках на рабочем столе', 'В заметках в телефоне', 'На стикере, приkleеннном к монитору', and 'В кошельке'. The first option is selected. The interface is identical to the previous screenshot, with a green 'Следующий шаг' button and statistics indicating 971 correct answers out of 740 attempts.

Рис. Раздел (3.2) – Вопрос 2

Вопрос: Где безопасно хранить пароли?

Ответ: Безопасно хранить пароли безопасно в менеджерах паролей

The screenshot shows a computer screen with a browser window open to a Stepik course page. The left sidebar lists various course modules and lessons. The main content area displays a question titled 'Зачем нужна капча?'. Below it, a list of four options is shown, with the first one selected: 'Для защиты кук пользователя'. A green button at the bottom right says 'Следующий шаг'.

Рис. Раздел (3.2) – Вопрос 3

Вопрос: Зачем нужна капча?

Ответ: Капча нужна для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

The screenshot shows a computer screen displaying a course on the Stepik platform. The left sidebar lists various course modules under 'Основы кибербезопасности'. The current module is '3.2 Пароли'. The main content area shows a question: 'Для чего применяется хэширование паролей?' with the instruction 'Выберите один вариант из списка'. The correct answer is marked with a green checkmark and the text 'Всё правильно.' Below the list of options, there are two buttons: 'Следующий шаг' and 'Решить снова'. A green box at the bottom right indicates 'Верно решили 973 учащихся' and 'Из всех попыток 61% верных'. The bottom navigation bar shows 'Шаг 7' and 'Следующий шаг >'. The task bar at the bottom of the screen shows several open windows, including 'Курс: Основы информа...', 'СМБ. НГУБа Прокси...', 'Шаг 7 - Пароли - Stepik', and 'удаление всех файлов уда...'. The system tray shows battery level, signal strength, and date/time.

Рис. Раздел (3.2) – Вопрос 4

Вопрос: Для чего применяется хэширование паролей?

Ответ: хэширование паролей применяется для того, чтобы не хранить пароли на сервере в открытом виде.

The screenshot shows a continuation of the course on the Stepik platform. The left sidebar remains the same. The current module is '3.2 Пароли'. The main content area shows a question: 'Поможет ли соль для улучшения стойкости паролей к атаке перебором, если злоумышленник получил доступ к серверу?' with the instruction 'Выберите один вариант из списка'. The correct answer is marked with a green checkmark and the text 'Правильно, молодец!'. Below the list of options, there are two buttons: 'Следующий шаг' and 'Решить снова'. A green box at the bottom right indicates 'Верно решили 967 учащихся' and 'Из всех попыток 66% верных'. The bottom navigation bar shows 'Шаг 8' and 'Следующий шаг >'. The task bar at the bottom of the screen shows several open windows, including 'Курс: Основы информа...', 'СМБ. НГУБа Прокси...', 'Шаг 8 - Пароли - Stepik', and 'удаление всех файлов уда...'. The system tray shows battery level, signal strength, and date/time.

Рис. Раздел (3.2) – Вопрос 5

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

Ответ: Нет, не поможет

The screenshot shows a computer screen displaying a course on Stepik. The left sidebar lists various chapters and lessons. The main content area shows a question titled 'Какие меры защищают от утечек данных атакой перебором?' (What measures protect against password cracking attacks?). Below the question, a message says 'Вы выбрали все подходящие ответы из списка' (You selected all correct answers from the list). A green checkmark indicates the answer 'Здорово, всё верно.' (Great, everything is correct). A note below states: 'Вы решили сложную задачу, поздравляем! Вы можете помочь остальным ученикам в комментариях, отвечая на их вопросы, или сравнить свое решение с другими на форуме решений.' (You solved a difficult task, congratulations! You can help other students in comments, answering their questions, or compare your solution with others on the forum of solutions.). A list of correct answers includes: разные пароли на всех сайтах (different passwords on all sites), периодическая смена паролей (regular password changes), сложные(=длинные) пароли (complex (=long) passwords), and капча (captcha). At the bottom, there are buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). The status bar at the bottom right shows the date and time: 13.03.2024 17:10.

Рис. Раздел (3.2) – Вопрос 6

Вопрос: Какие меры защищают от утечек данных атакой перебором?

Ответ: Всё перечисленное на слайде является отличной защитой

(3.3) “Фишинг”

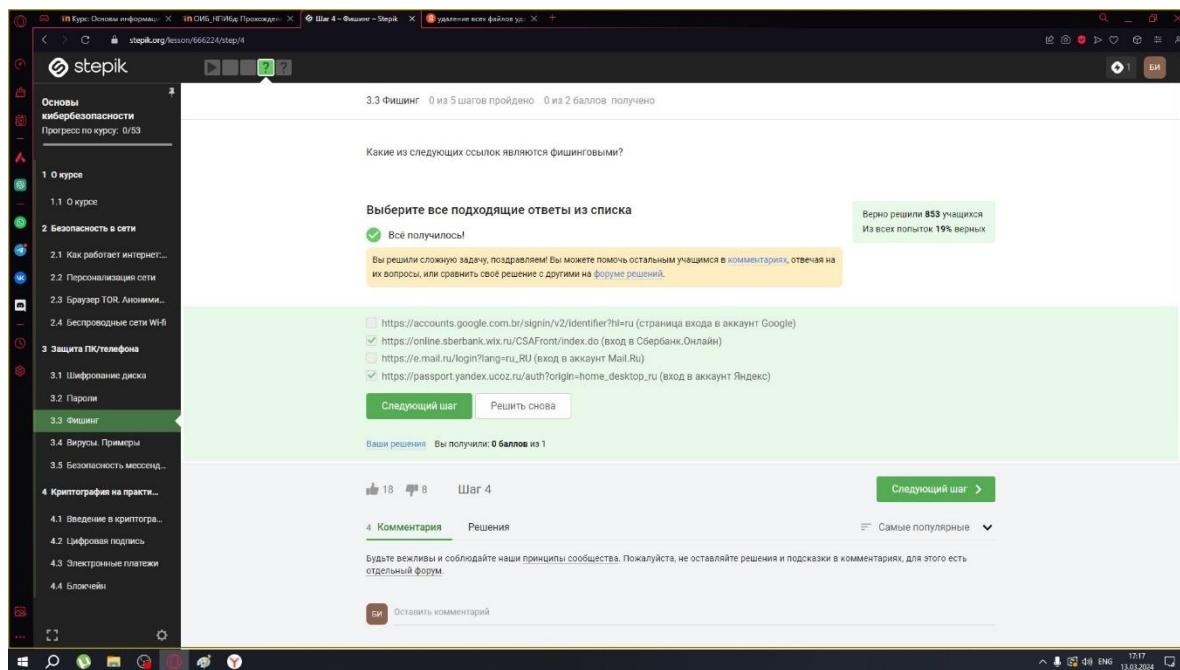


Рис. Раздел (3.3) – Вопрос 1

Вопрос: Какие из следующих ссылок являются фишинговыми?

Ответ: Фишинговая ссылка — это мошенническая ссылка, которая выглядит достоверно, но на самом деле используется для кражи личных данных пользователя. Тут подходят сайты Сбербанка (.wix лишня) и Яндекса (.usoz лишня)

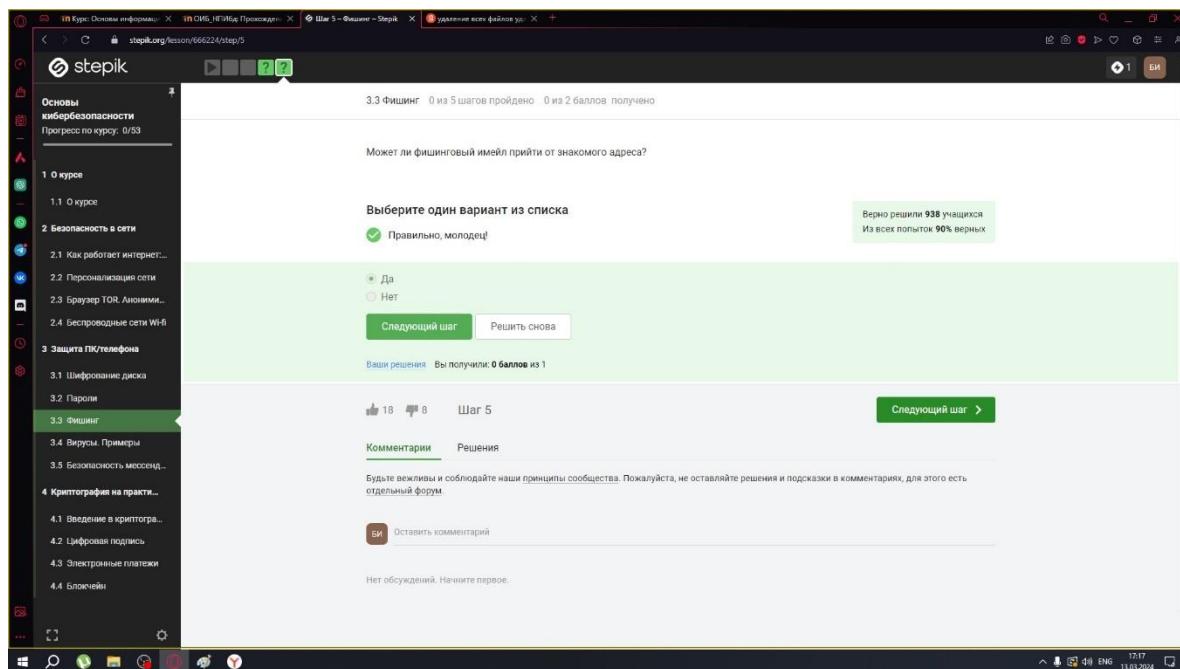
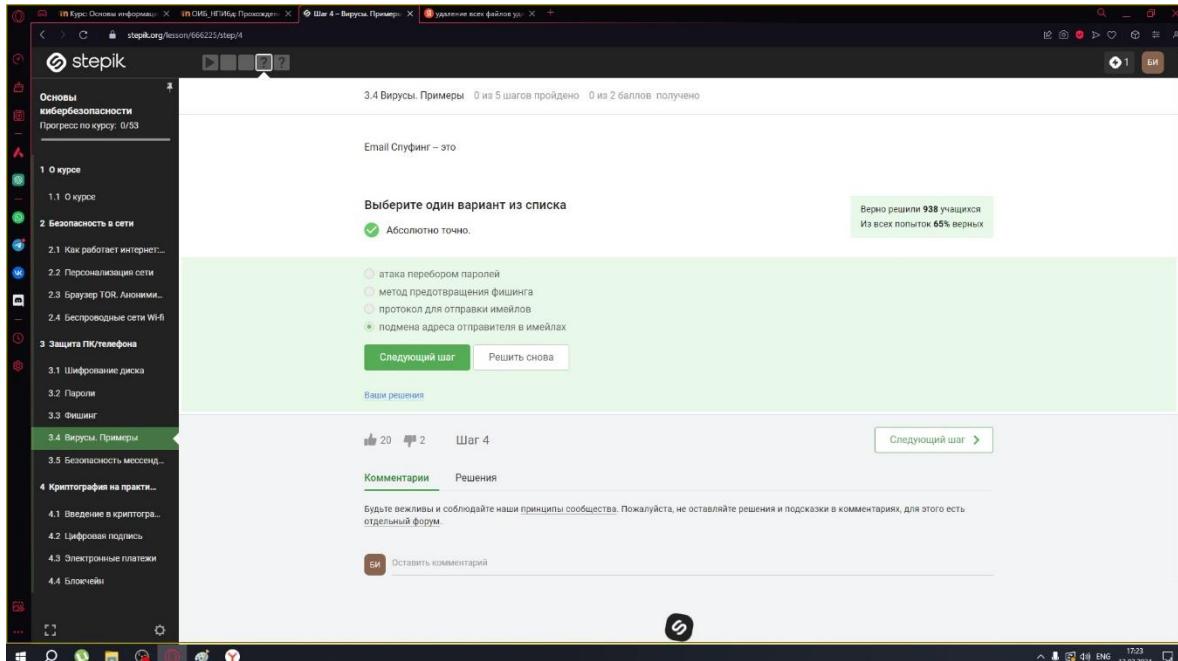


Рис. Раздел (3.3) – Вопрос 2

Вопрос: Может ли фишинговый имейл прийти от знакомого адреса?

Ответ: Может, потому что они маскируются под известные пользователям сайты и почты

(3.4) “Вирусы. Примеры”



3.4 Вирусы. Примеры 0 из 5 шагов пройдено 0 из 2 баллов получено

Email Спупинг – это

Выберите один вариант из списка

Абсолютно точно.

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

Следующий шаг Решить снова

Ваше решение

Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.

Комментарии Решения

Оставить комментарий

Рис. Раздел (3.4) – Вопрос 1

Вопрос: Email Спупинг - это

Ответ: Email Спупинг - это подмена адреса отправителя в имейлах

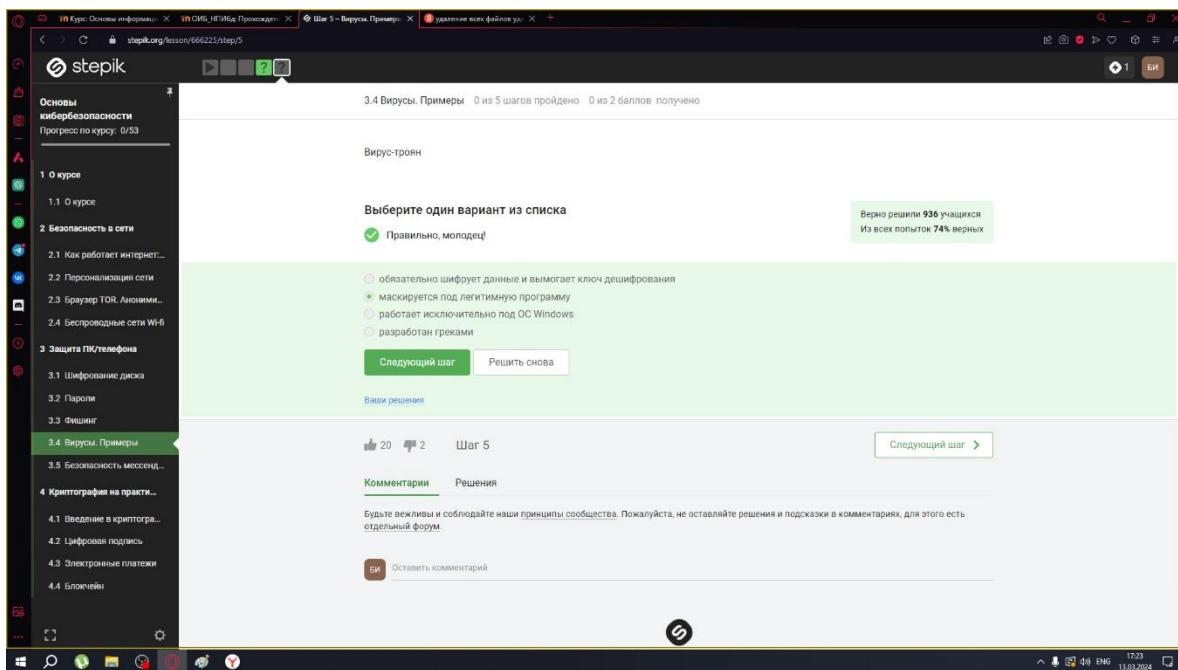


Рис. Раздел (3.4) – Вопрос 2

Вопрос: Вирус-троян

Ответ: Он маскируется под легитимную программу или игры, чтобы взломать компьютер или украдь данные

(3.5) “Безопасность мессенджеров”

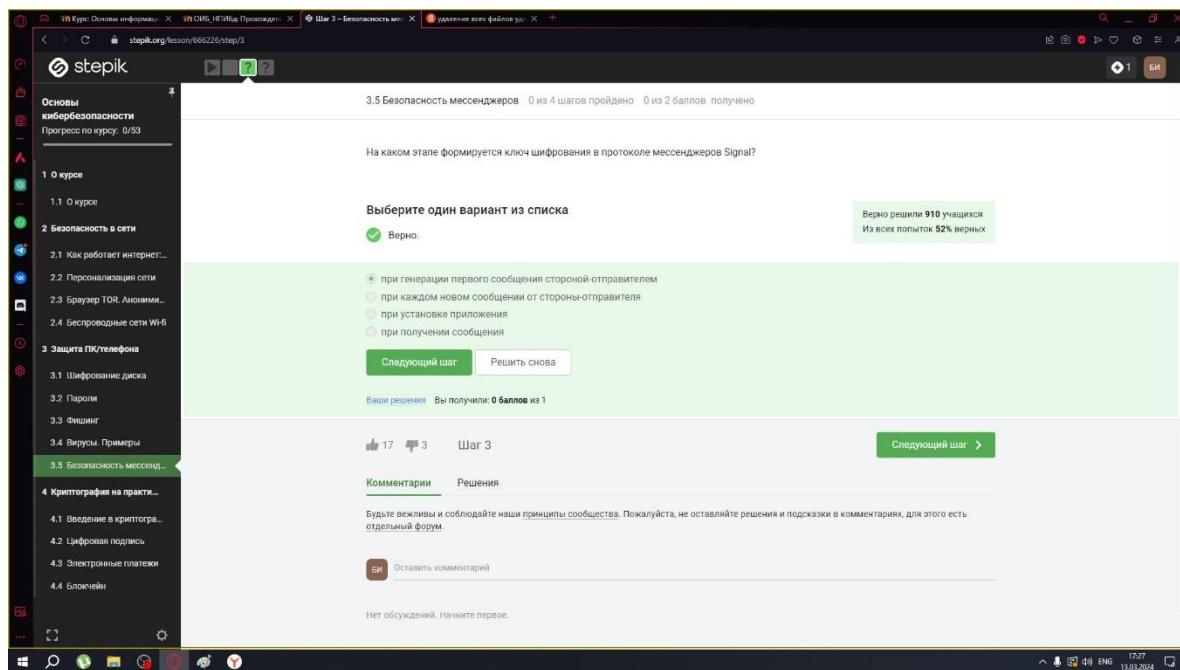


Рис. Раздел (3.5) – Вопрос 1

Вопрос: На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Ответ: Ключ шифрования в протоколе мессенджеров Signal формируется **при генерации первого сообщения стороной-отправителем**

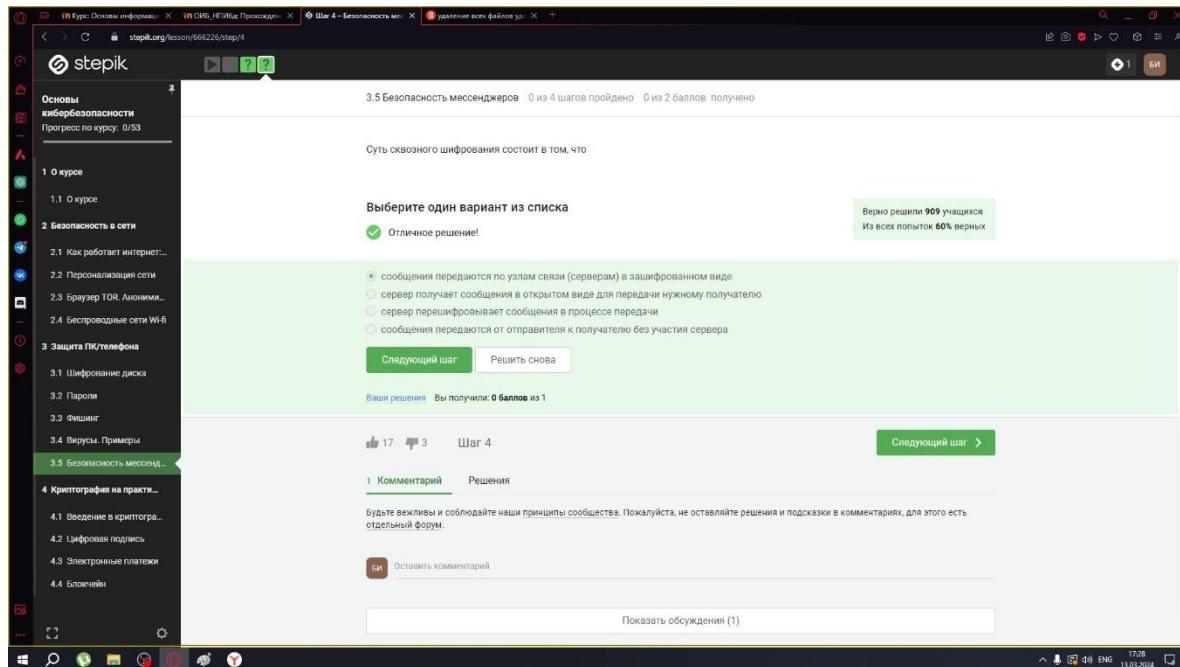


Рис. Раздел (3.5) – Вопрос 2

Вопрос: Суть сквозного шифрования состоит в том, что

Ответ: Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи (серверам) в зашифрованном виде

Раздел 4: “Криптография на практике”

(4.1) “Введение в криптографию”

The screenshot shows a computer desktop with a browser window open to the Stepik platform. The user is viewing a lesson titled '4.1 Введение в криптографию'. The sidebar on the left lists various sections of the course, including 'Основы кибербезопасности', '1 курсе', '2 Безопасность в сети', '3 Защита ПК/телефона', and '4 Криптография на практике'. The current section, '4.1 Введение в криптографию', is highlighted with a green background. The main content area displays a question about asymmetric cryptographic primitives. The question asks to choose one option from a list of four. The correct answer, 'обе стороны имеют пару ключей' (both sides have a pair of keys), is marked with a green checkmark. Below the question, there are buttons for 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). To the right, a statistics box shows 'Верно решили 876 участников' (876 participants solved correctly) and 'Из всех попыток 42% верных' (42% of all attempts were correct). At the bottom of the content area, there are tabs for 'Комментарии' (Comments) and 'Решения' (Solutions), along with a note: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' (Be polite and follow our community principles. Please do not leave solutions and hints in comments, there is a separate forum for that.) There are also buttons for 'Оставить комментарий' (Leave a comment) and 'Нет обсуждений. Начните первое.' (No discussions. Start the first one.). The browser's address bar shows the URL 'stepik.org/lesson/666227/step/3'. The system tray at the bottom indicates the date as 13.03.2024 and the time as 18:06.

Рис. Раздел (4.1) – Вопрос 1

Вопрос: В асимметричных криптографических примитивах

Ответ: Обе стороны имеют пару ключей

4.1 Введение в криптографию 0 из 7 шагов пройдено 0 из 5 баллов получено

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

Так точно!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить свое решение с другими на форуме решений.

эффективно вычисляется

стойкая к коллизиям

дает на выходе фиксированное число бит независимо от объема входных данных

обеспечивает конфиденциальность зашифрованных данных

Следующий шаг Решить снова

Ваши решения Вы получили: 0 баллов из 1

Шаг 4

Комментарии Решения

Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.

Оставить комментарий

Рис. Раздел (4.1) – Вопрос 2

Вопрос: Криптографическая хэш-функция

Ответ: Всё верно, кроме пункта “обеспечивает конфиденциальность захэшированных данных”

4.1 Введение в криптографию 0 из 7 шагов пройдено 0 из 5 баллов получено

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

Хорошие новости, верно!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить свое решение с другими на форуме решений.

AES

SHA2

RSA

ECDSA

ГОСТ Р 34.10-2012

Следующий шаг Решить снова

Ваши решения Вы получили: 0 баллов из 1

Шаг 5

1 Комментарий Решения

Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.

Оставить комментарий

Рис. Раздел (4.1) – Вопрос 3

Вопрос: К алгоритмам цифровой подписи относятся

Ответ: RSA, ECDSA и ГОСТ Р 34.10-2012. SHA2 – это семейство криптографических хеш-функций, а AES – это алгоритм симметричного шифрования.

The screenshot shows a computer screen with a dark-themed interface. At the top, there are several tabs: 'Курс: Основы информатики', 'СИБ. НГУБа. Проходит...', 'Шаг 6 – Введение в крипто...', and 'удаление всех файлов уда...'. Below the tabs, the main content area has a title '4.1 Введение в криптографию' with a progress bar indicating '0 из 7 шагов пройдено' and '0 из 5 баллов получено'. A question is displayed: 'Код аутентификации сообщения относится к'. Below the question, a note says 'Выберите один вариант из списка' and 'Абсолютно точно.' A radio button next to the text 'симметричным примитивам' is selected. There are two buttons at the bottom: 'Следующий шаг' and 'Решить снова'. To the right, a green box shows statistics: 'Верно решили 840 учащихся' and 'Из всех попыток 69% верных'. Below this, another section starts with 'Шаг 6' and 'Комментарии' and 'Решения'. A note at the bottom of this section reads: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' A button 'Оставить комментарий' is visible. The bottom of the screen shows the Windows taskbar with icons for search, file explorer, and other applications, along with system status indicators like battery level and date/time.

Рис. Раздел (4.1) – Вопрос 4

Вопрос: Код аутентификации сообщения относится к

Ответ: Код аутентификации сообщения относится к симметричным примитивам

The screenshot shows a computer screen displaying a Stepik course interface. On the left, a sidebar lists course sections: 1. О курсе, 2. Безопасность в сети, 3. Защита ПК/телефона, and 4. Криптография на практике. The fourth section is currently selected. A sub-menu under '4. Криптография на практике' includes '4.1 Введение в криптографию', which is also selected. The main content area displays a step titled '4.1 Введение в криптографию'. The question asks: 'Обмен ключами Диффи-Хэллмана - это'. Below the question, a list of options is shown: 'симметричный примитив генерации общего секретного ключа', 'асимметричный примитив генерации общего открытого ключа', 'асимметричный примитив генерации общего секретного ключа' (with a green checkmark), and 'асимметричный алгоритм шифрования'. A message at the top right says 'Верно решили 833 учащихся Из всех попыток 46% верных'. At the bottom of the content area, there are buttons for 'Следующий шаг' and 'Решить снова'. The status bar at the bottom shows 'Шаг 7' and '17 из 6'. The taskbar at the very bottom includes icons for search, file explorer, and other applications.

Рис. Раздел (4.1) – Вопрос 5

Вопрос: Обмен ключам Диффи-Хэллмана - это

Ответ: Обмен ключам Диффи-Хэллмана – это асимметричный примитив генерации общего секретного ключа

(4.2) “Цифровая подпись”

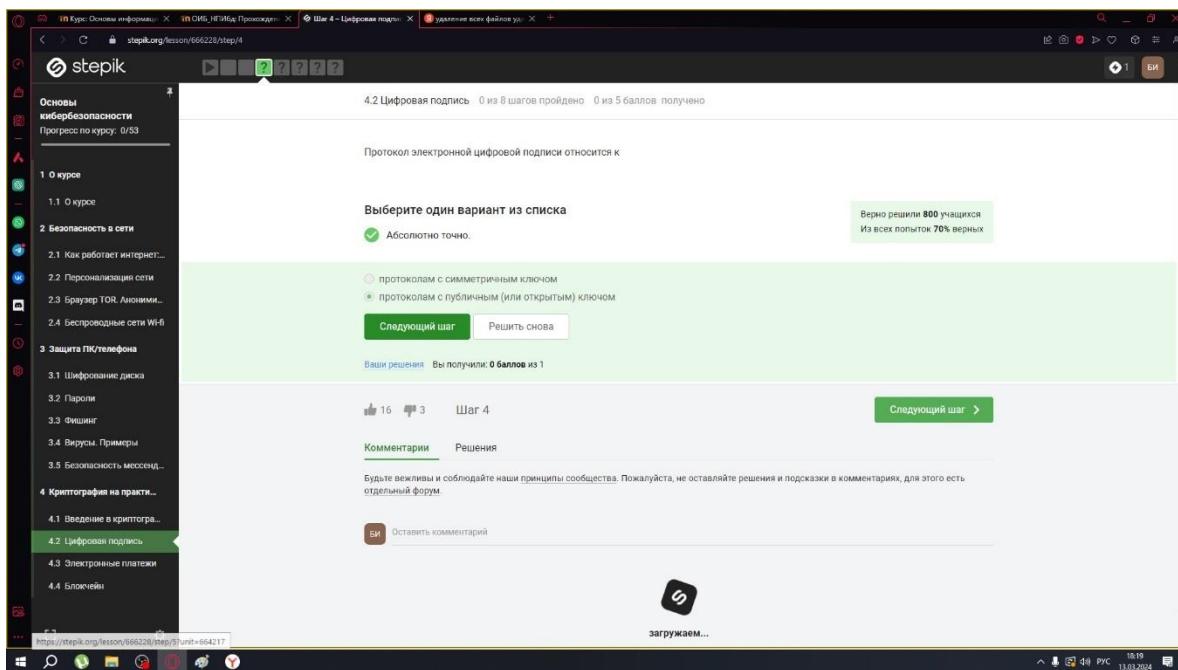


Рис. Раздел (4.2) – Вопрос 1

Вопрос: Протокол электронной цифровой подписи относится к

Ответ: Он относится к протоколам с публичным (или открытым) ключом

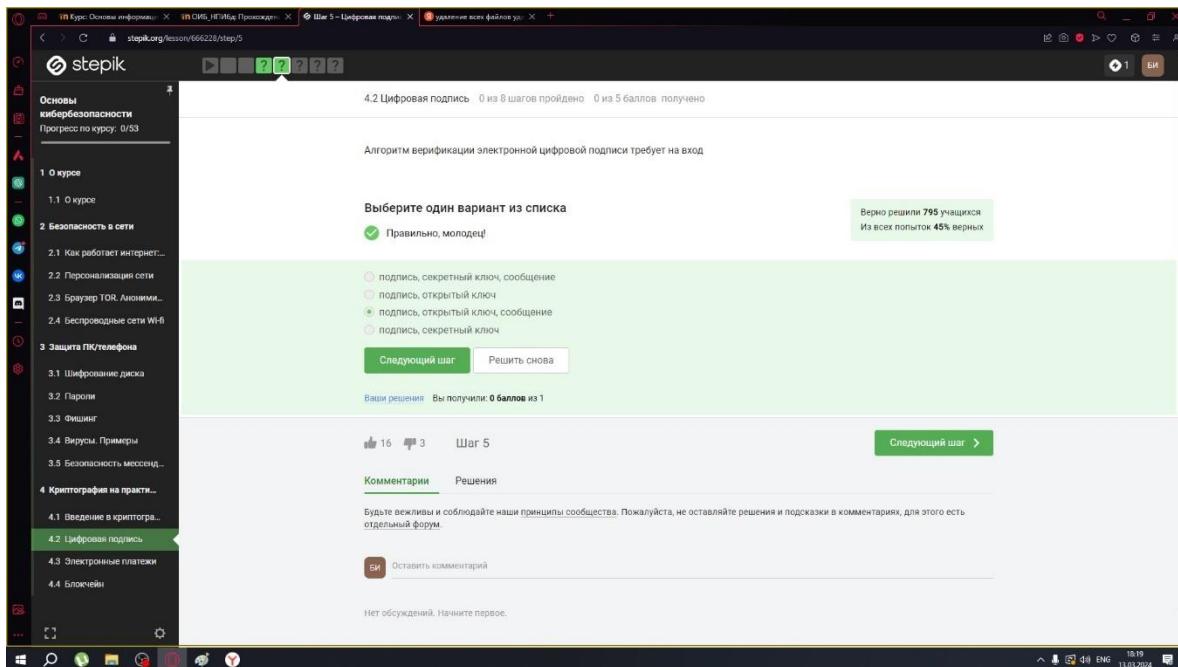


Рис. Раздел (4.2) – Вопрос 2

Вопрос: Алгоритм верификации электронной цифровой подписи требует на вход

Ответ: Этот алгоритм вход требует подпись, открытый ключ, сообщение

The screenshot shows a computer screen displaying a course on Stepik. The left sidebar lists chapters and lessons, with '4.2 Цифровая подпись' currently selected. The main content area shows a question titled '4.2 Цифровая подпись'. The question text reads: 'Электронная цифровая подпись не обеспечивает'. Below this is a list of four options with radio buttons:

- неотказ от авторства
- целостность
- автентификация
- конфиденциальность

The fourth option is selected. There are two buttons at the bottom: 'Следующий шаг' (Next step) and 'Решить снова' (Solve again). A green box on the right indicates: 'Верно решили 796 учащихся' and 'Из всех попыток 51% верных'. At the bottom of the page, there are tabs for 'Комментарии' and 'Решения', and a note: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' A button labeled 'Оставить комментарий' is visible.

Рис. Раздел (4.2) – Вопрос 3

Вопрос: Электронная цифровая подпись не обеспечивает

Ответ: Электронная цифровая подпись не может обеспечить конфиденциальность

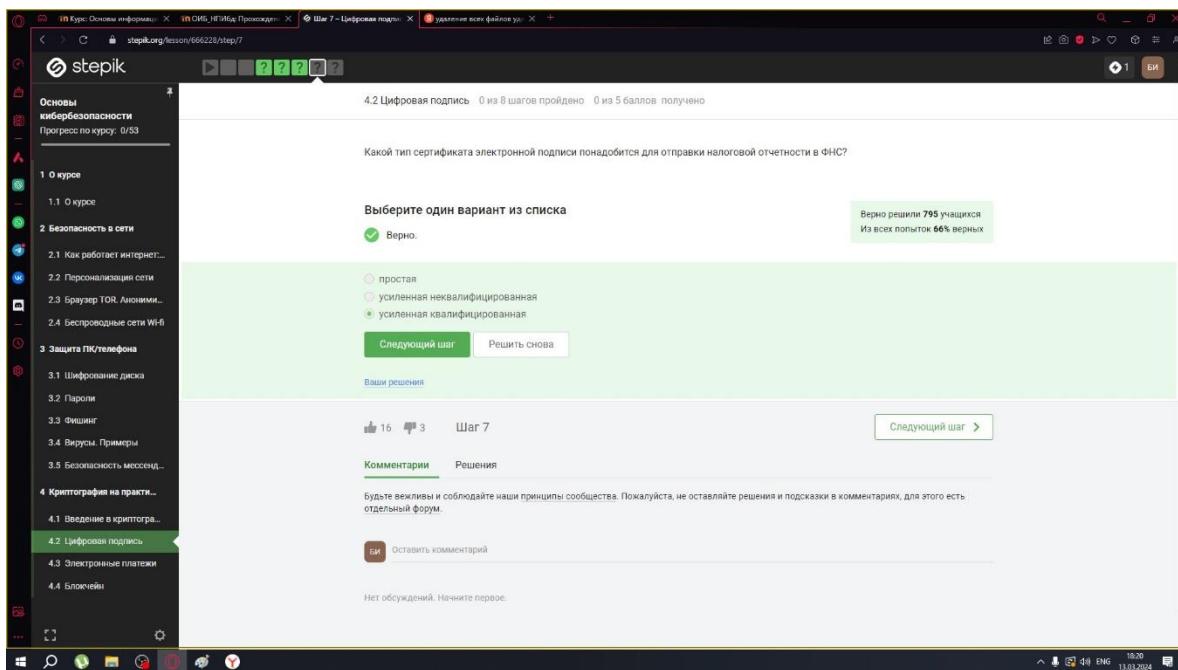


Рис. Раздел (4.2) – Вопрос 4

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

Ответ: ФНС требует сертификат электронной подписи с усиленной квалификацией

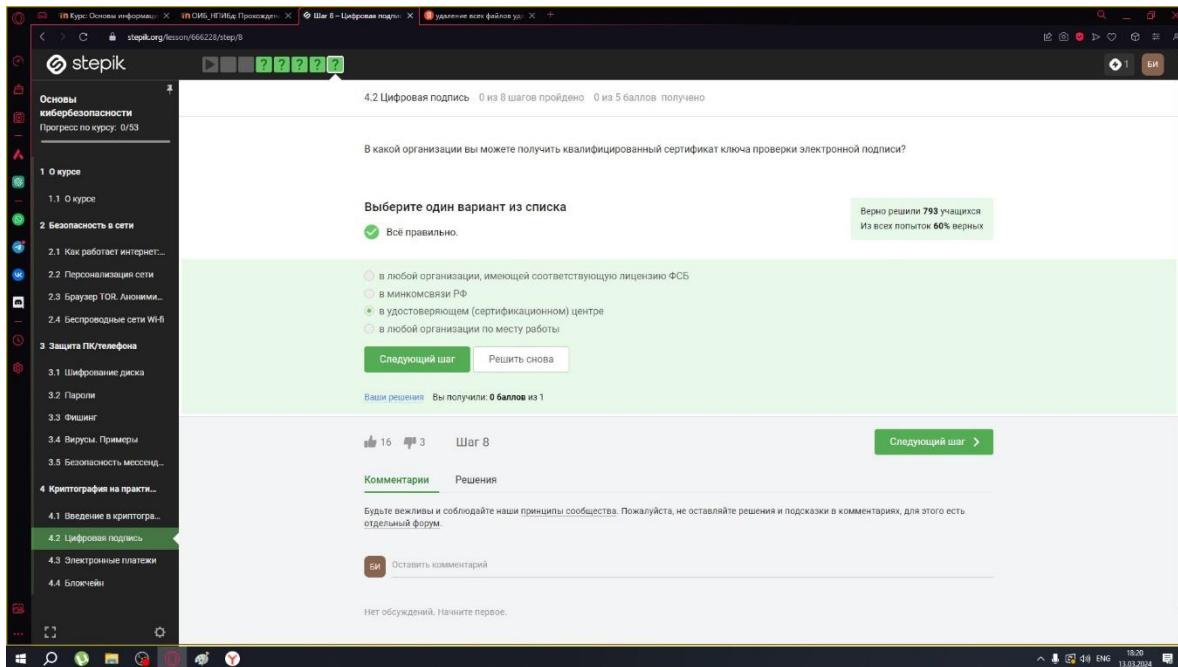


Рис. Раздел (4.2) – Вопрос 5

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

Ответ: Сертификаты ключа проверки электронной подписи выдаются в сертификационном центре

(4.3) “Электронные платежи”

The screenshot shows a computer screen displaying a Stepik course titled "Основы кибербезопасности". The current step is "Шаг 3 – Электронные платежи". The question asks to select all correct payment systems from a list. The correct answers are MasterCard and МИР. A green box highlights the correct answer "Правильно, молодец!". Below the question, there is a message: "Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в комментариях, отвечая на их вопросы, или сравнить свой ответ с другими на форуме решений." At the bottom, there are buttons for "Следующий шаг" and "Решить снова". On the right, it says "Верно решили 733 учащихся Из всех попыток 23% верных". The sidebar on the left lists other steps and topics.

Рис. Раздел (4.3) – Вопрос 1

Вопрос: Выберите из списка все платежные системы.

Ответ: МИР и MasterCard являются платежными системами

The screenshot shows a computer screen displaying a Stepik course page. The left sidebar lists course modules: Основы кибербезопасности, 1. О курсе, 2. Безопасность в сети, 3. Защита ПК/телефона, 4. Криптография на практике, and 4.4 Блокчейн. The current module is 4.4 Блокчейн. The main content area displays a question titled 'Шаг 4 – Электронные платежи' with the sub-instruction 'удаление всех файлов удаляется'. The question asks to select all correct answers from a list: 'Хорошая работа.' (checkbox checked), 'комбинация проверки пароля + Капча' (checkbox unchecked), 'комбинация проверка пароля + код в sms сообщении' (checkbox checked), 'комбинация код в sms сообщении + отпечаток пальца' (checkbox checked), and 'комбинация PIN код + пароль' (checkbox unchecked). A green button 'Следующий шаг' is at the bottom left, and a grey button 'Решить снова' is at the bottom right. A progress bar shows 14 steps completed, 1 step pending, and a total of 15 steps. The right side of the screen shows a statistics box: 'Верно решили 713 учащихся' and 'Из всех попыток 22% верных'. Below the statistics is a forum section with tabs 'Комментарии' and 'Решения'. A note says: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' A brown button 'Оставить комментарий' is visible. The bottom status bar shows system icons and the date/time: 18:29 13.03.2024.

Рис. Раздел (4.3) – Вопрос 2

Вопрос: Примером многофакторной аутентификации является

Ответ: К многофакторной аутентификации относятся: проверка пароля, код в sms сообщении и отпечаток пальца

This screenshot shows the same Stepik course interface as the previous one, but for a different question in Step 5. The sidebar and course structure are identical. The main content area displays a question titled 'Шаг 5 – Электронные платежи' with the sub-instruction '0 из 5 шагов пройдено 0 из 3 баллов получено'. The question asks to select one correct answer from a list: 'Правильно.' (radio button checked), 'многофакторная аутентификация покупателя перед банком-эмитентом' (radio button checked), 'однофакторная аутентификация покупателя перед банком-эквайером' (radio button unchecked), 'однофакторная аутентификация при помощи PIN-кода карты перед терминалом' (radio button unchecked), and 'многофакторная аутентификация покупателя перед банком-эквайером' (radio button unchecked). A green button 'Следующий шаг' is at the bottom left, and a grey button 'Решить снова' is at the bottom right. A progress bar shows 14 steps completed, 1 step pending, and a total of 15 steps. The right side of the screen shows a statistics box: 'Верно решили 769 учащихся' and 'Из всех попыток 58% верных'. Below the statistics is a forum section with tabs 'Комментарии' and 'Решения'. A note says: 'Будьте вежливы и соблюдайте наши принципы сообщества. Пожалуйста, не оставляйте решения и подсказки в комментариях, для этого есть отдельный форум.' A brown button 'Оставить комментарий' is visible. The bottom status bar shows system icons and the date/time: 18:30 13.03.2024.

Рис. Раздел (4.3) – Вопрос 3

Вопрос: При онлайн платежах сегодня используется

Ответ: Онлайн платежи используют многофакторную аутентификацию покупателя перед банком-эмитентом

(4.4) “Блокчейн”

The screenshot shows a computer screen with a browser window open to the Stepik platform. The URL in the address bar is stepik.org/lesson/666230/step/4. The page title is "Шаг 4 – Блокчейн - Stepik". The main content area displays a question: "Какое свойство криптографической хэш-функции используется в доказательстве работы?". Below the question, there is a list of four options with radio buttons:

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

Below the list are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). A green box at the top right indicates: "Верно решили 784 учащихся. Из всех попыток 47% верных". At the bottom of the page, there are sections for "Комментарии" (Comments) and "Решения" (Solutions), along with a button "Оставить комментарий" (Leave a comment).

Рис. Раздел (4.4) – Вопрос 1

Вопрос: Какое свойство криптографической хэш-функции используется в доказательстве работы?

Ответ: Используется сложность нахождения прообраза

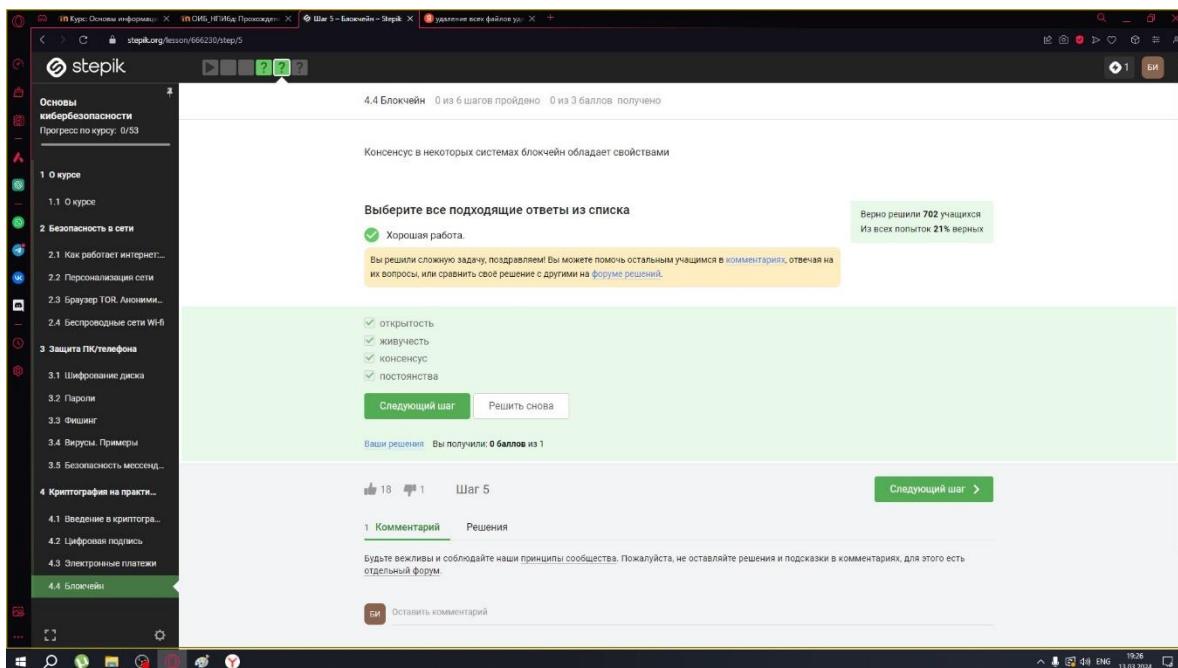


Рис. Раздел (4.4) – Вопрос 2

Вопрос: Консенсус в некоторых системах блокчейн обладает свойствами

Ответ: Обладает всеми перечисленными свойствами

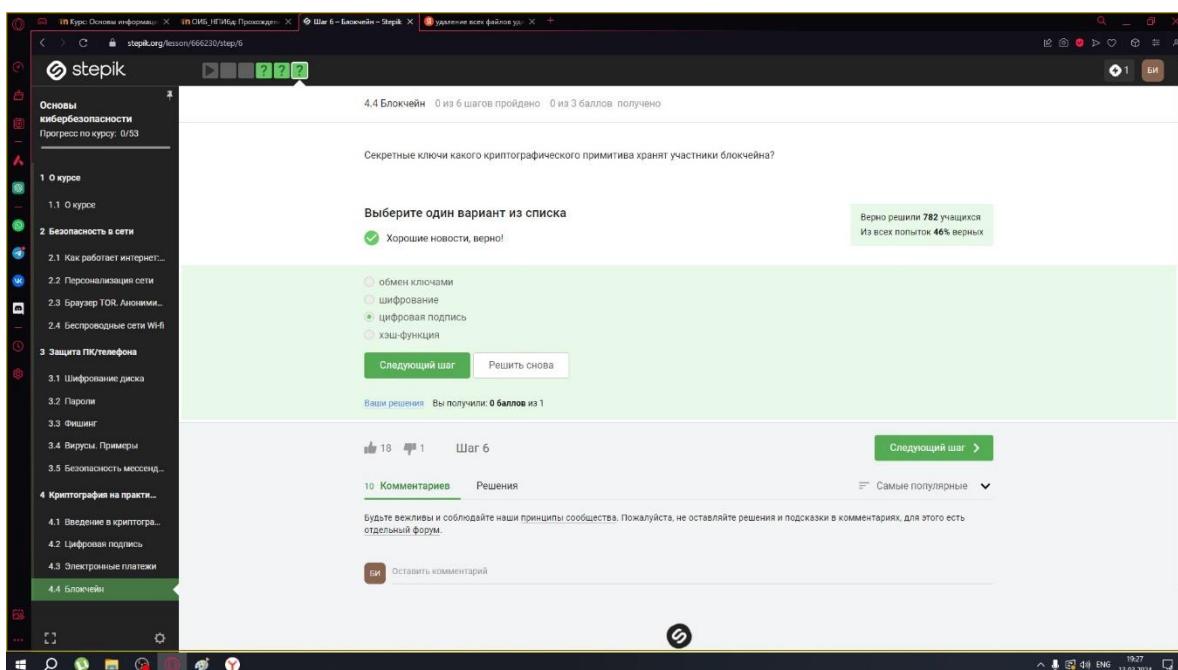


Рис. Раздел (4.4) – Вопрос 3

Вопрос: Секретные ключи какого криптографического примитива хранят участники блокчейна?

Ответ: Участники блокчейна хранят секретные ключи, которые используются для цифровой подписи

Раздел 5: “Сертификат”

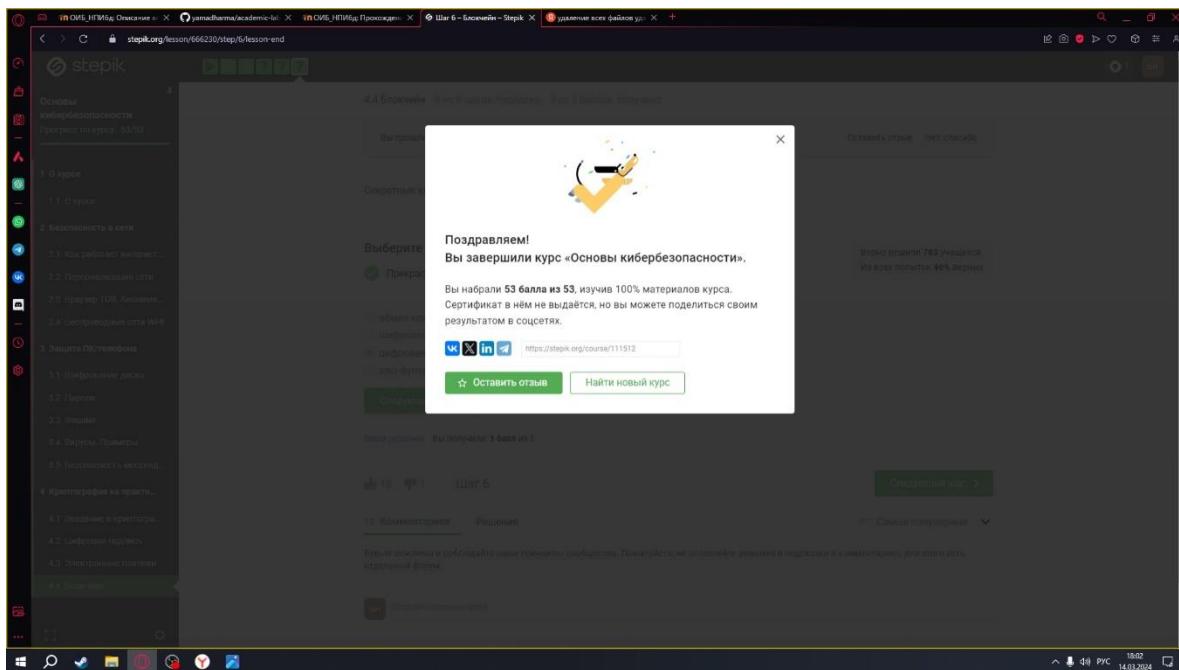


Рис. Раздел (5) - Сертификат

Вывод

В ходе прохождения внешних курсов были получены навыки о “Безопасности в сети”, “Зашите ПК/телефона” и “Криптографии”.