

Внешний курс на Stepik

Основы кибербезопасности

Алади Принц Чисом

Содержание

1 Цель работы	6
2 Раздел 2.1	7
3 Раздел 2.2	12
4 Раздел 2.3	14
5 Раздел 2.4	16
6 Раздел 3.1. защита ПК и телефона	19
7 Раздел 3.2. Пароли	21
8 Раздел 3.3. Фишинг	24
9 Раздел 3.3. Вирусы. Примеры	25
10 Раздел 3.5. Безопасность мессенджеров	26
11 Раздел 4.1 Введение в криптографию	28
12 Раздел 4.2 Цифровая подпись	31
13 Раздел 4.3 Электронные платежи	34
14 Раздел 4.4 Блокчейн	36
15 Вывод	38

Список иллюстраций

2.1 Рис. 1	7
2.2 Рис. 2	7
2.3 Рис. 3	8
2.4 Рис. 4	8
2.5 Рис. 5	9
2.6 Рис. 6	9
2.7 Рис. 7	10
2.8 Рис. 8	10
2.9 Рис. 9	11
3.1 Рис. 1	12
3.2 Рис. 2	12
3.3 Рис. 3	13
3.4 Рис. 4	13
4.1 Рис. 1	14
4.2 Рис. 2	14
4.3 Рис. 3	15
4.4 Рис. 4	15
5.1 Рис. 1	16
5.2 Рис. 2	16
5.3 Рис. 3	17
5.4 Рис. 4	17
5.5 Рис. 5	18
6.1 Рис. 1	19
6.2 Рис. 2	19
6.3 Рис. 3	20
7.1 Рис. 1	21
7.2 Рис. 2	21
7.3 Рис. 3	22
7.4 Рис. 5	23
7.5 Рис. 6	23
8.1 Рис. 1	24
8.2 Рис. 2	24

9.1 Рис. 1	25
9.2 Рис. 2	25
10.1 Рис. 1	26
11.1 Рис. 1	28
11.2 Рис. 3	29
11.3 Рис. 4	29
11.4 Рис. 5	30
12.1 Рис. 1	31
12.2 Рис. 3	32
12.3 Рис. 4	32
12.4 Рис. 5	33
13.1 Рис. 1	34
13.2 Рис. 2	35
13.3 Рис. 3	35
14.1 Рис. 1	36
14.2 Рис. 2	37
14.3 Рис. 3	37
15.1 Прохождение курса	38

Список таблиц

1 Цель работы

Закончить курс с сертификатом и научиться базовым приемам и методам информационной безопасности.

2 Раздел 2.1

Выберите протокол прикладного уровня: HTTPS

2.1 Как работает интернет: базовые сетевые протоколы 15 out of 15 steps passed 9 out of 9 points received

You passed more than 80%, write a review Create review No thanks

Выберите протокол прикладного уровня

Select one option from the list

Good news for you, correct!

Correct answer from 895 learners
Total 58% of tries are correct

UDP
TCP
HTTPS
IP

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 2.1: Рис. 1

На каком уровне работает протокол TCP?: транспортном

2.1 Как работает интернет: базовые сетевые протоколы 15 out of 15 steps passed 9 out of 9 points received

You passed more than 80%, write a review Create review No thanks

На каком уровне работает протокол TCP?

Select one option from the list

Great!

Correct answer from 939 learners
Total 61% of tries are correct

Транспортном
Прикладном
Канальном
Сетевом

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 2.2: Рис. 2

Выберите все корректные адреса IPv4: 90.11.90.22, 25.198.0.15

2.1 Как работает интернет: базовые сетевые протоколы 15 out of 15 steps passed 9 out of 9 points received

You passed more than 80%, write a review Create review No thanks

Выберите все корректные адреса IPv4

Select all correct options from the list

Good news for you, correct!

You've solved a complex problem, congratulations! Now you can help other learners in comments by answering their questions, or compare your solution with others on solution forum.

421.0.15.19
 43.12.256.7
 90.11.90.22
 25.198.0.15

Next step Solve again

Your submissions You got: 1 point out of 1

Correct answer from 871 learners
Total 23% of tries are correct

Рис. 2.3: Рис. 3

DNS сервер: сопоставляет IP адреса доменным именам

2.1 Как работает интернет: базовые сетевые протоколы 15 out of 15 steps passed 9 out of 9 points received

You passed more than 80%, write a review Create review No thanks

DNS сервер

Select one option from the list

Yes!

Correct answer from 933 learners
Total 66% of tries are correct

сопоставляет IP адреса доменным именам
 сегментирует данные на транспортном уровне
 выбирает маршрут пакета в сети
 выполняет адресацию на хосте

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 2.4: Рис. 4

Выберите корректную последовательность протоколов в модели TCP/IP: прикладной – транспортный – сетевой – канальный

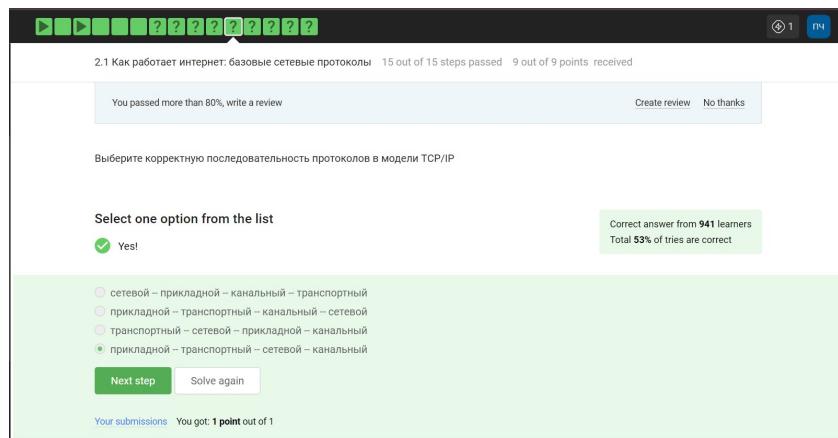


Рис. 2.5: Рис. 5

Протокол http предполагает: передачу данных между клиентом и сервером в открытом виде

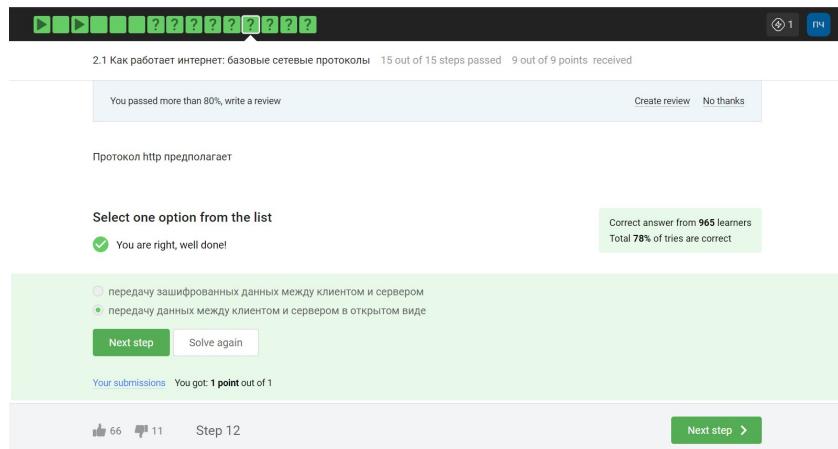


Рис. 2.6: Рис. 6

Протокол https состоит из: двух фаз: рукопожатия и передачи данных

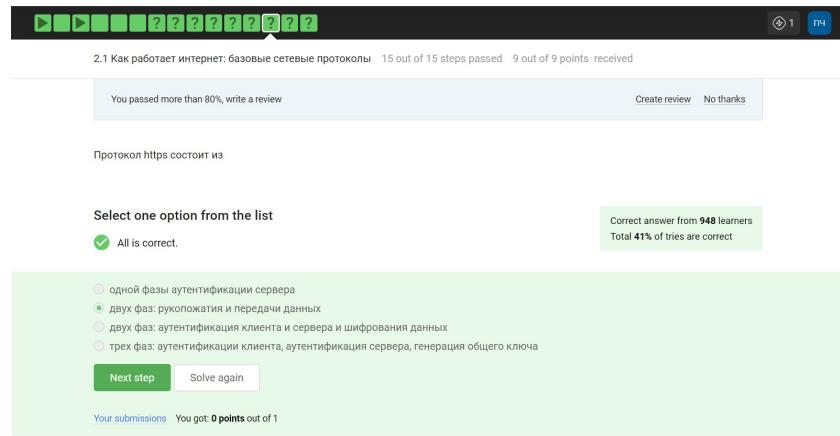


Рис. 2.7: Рис. 7

Версия протокола TLS определяется: и клиентом, и сервером в процессе “переговоров”

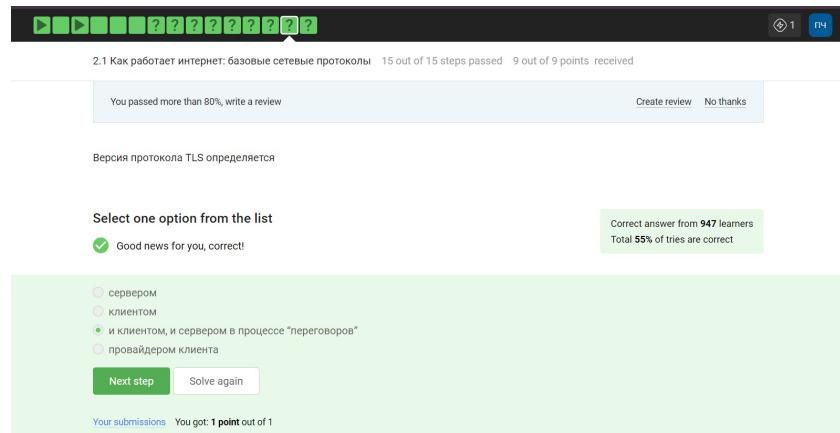


Рис. 2.8: Рис. 8

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

The screenshot shows a digital assignment interface. At the top, there is a navigation bar with icons for back, forward, and search, along with a user icon and a 'm4' button. Below the navigation bar, a progress bar indicates '15 out of 15 steps passed' and '9 out of 9 points received'. A message says 'You passed more than 80%, write a review' with options 'Create review' and 'No thanks'. A note states 'В фазе "рукопожатия" протокола TLS не предусмотрено'. The main area is titled 'Select one option from the list' and contains a question with four options: 'формирование общего секретного ключа между клиентом и сервером', 'автентификация (как минимум одной из сторон)', 'выбираются алгоритмы шифрования/автентификации', and 'шифрование данных'. The fourth option is marked with a green checkmark and the text 'Great work!'. To the right, a box shows 'Correct answer from 931 learners' and 'Total 44% of tries are correct'. At the bottom, there are 'Next step' and 'Solve again' buttons, and a note 'Your submissions You got: 1 point out of 1'.

Рис. 2.9: Рис. 9

3 Раздел 2.2

Куки хранят: id сессии, идентификатор пользователя

The screenshot shows a Moodle quiz step titled "2.2 Персонализация сети". It displays a message: "You passed more than 80%, write a review" and "Create review No thanks". Below this, a question asks: "Куки хранят:". A feedback message says: "Select all correct options from the list" and "Totally right". It also states: "You've solved a complex problem, congratulations! Now you can help other learners in comments by answering their questions, or compare your solution with others on solution forum." A list of options is shown, with "идентификатор пользователя" and "id сессии" checked. At the bottom, there are "Next step" and "Solve again" buttons, and a message: "Your submissions You got: 1 point out of 1".

Рис. 3.1: Рис. 1

Куки не используются для: улучшения надежности соединения

The screenshot shows a Moodle quiz step titled "2.2 Персонализация сети". It displays a message: "You passed more than 80%, write a review" and "Create review No thanks". Below this, a question asks: "Куки не используются для". A feedback message says: "Select one option from the list" and "Good news for you, correct!". It also states: "You've solved a complex problem, congratulations! Now you can help other learners in comments by answering their questions, or compare your solution with others on solution forum." A list of options is shown, with "улучшения надежности соединения" checked. At the bottom, there are "Next step" and "Solve again" buttons, and a message: "Your submissions You got: 1 point out of 1".

Рис. 3.2: Рис. 2

Куки генерируются: сервером

2.2 Персонализация сети 6 out of 6 steps passed 4 out of 4 points received

You passed more than 80%, write a review Create review No thanks

Куки генерируются

Select one option from the list

You are right, well done!

Correct answer from 968 learners
Total 79% of tries are correct

клиентом
 сервером

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 3.3: Рис. 3

Сессионные куки хранятся в браузере? Да, на время пользования веб-сайтом

2.2 Персонализация сети 6 out of 6 steps passed 4 out of 4 points received

You passed more than 80%, write a review Create review No thanks

Сессионные куки хранятся в браузере?

Select one option from the list

You're right!

Correct answer from 959 learners
Total 60% of tries are correct

Нет
 Да, на время пользования веб-сайтом
 Да, на некоторое время, заданное в сервером

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 3.4: Рис. 4

4 Раздел 2.3

Сколько промежуточных узлов в луковой сети TOR? 3

2.3 Браузер TOR. Анонимизация 6 out of 6 steps passed 4 out of 4 points received

You passed more than 80%, write a review Create review No thanks

Сколько промежуточных узлов в луковой сети TOR?

Select one option from the list

Well done!

Correct answer from 959 learners
Total 77% of tries are correct

2
 3
 4

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 4.1: Рис. 1

IP-адрес получателя известен: отправителю, выходному узлу

2.3 Браузер TOR. Анонимизация 6 out of 6 steps passed 4 out of 4 points received

You passed more than 80%, write a review Create review No thanks

IP-адрес получателя известен

Select all correct options from the list

Totally right.

You've solved a complex problem, congratulations! Now you can help other learners in comments by answering their questions, or compare your solution with others on solution forum.

Correct answer from 906 learners
Total 19% of tries are correct

охранному узлу
 промежуточному узлу
 отправителю
 выходному узлу

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 4.2: Рис. 2

Отправитель генерирует общий секретный ключ: с охранным, промежуточным и выходном узлом

The screenshot shows a Moodle quiz interface. At the top, there are navigation icons (back, forward, search, etc.) and a progress bar indicating 6 out of 6 steps passed and 4 out of 4 points received. Below the progress bar, there are buttons for 'Create review' and 'No thanks'. The main content area contains the question: 'Отправитель генерирует общий секретный ключ' (The sender generates a shared secret key). A note below the question says 'Select one option from the list'. The correct answer is marked with a green checkmark and the text 'Good news for you, correct!'. The correct answer is 'с охранным, промежуточным и выходным узлом' (with a guard, intermediate, and exit node). There are four other options listed without checkmarks: 'только с охранным узлом' (only with a guard node), 'с охранным и промежуточным узлом' (with a guard and intermediate node), 'с промежуточным и выходным узлом' (with an intermediate and exit node), and 'с выходным узлом' (with an exit node). At the bottom of the step, there are 'Next step' and 'Solve again' buttons, and a note stating 'Your submissions You got: 1 point out of 1'.

Рис. 4.3: Рис. 3

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

The screenshot shows a Moodle quiz interface. At the top, there are navigation icons (back, forward, search, etc.) and a progress bar indicating 6 out of 6 steps passed and 4 out of 4 points received. Below the progress bar, there are buttons for 'Create review' and 'No thanks'. The main content area contains the question: 'Должен ли получатель использовать браузер Tor (или другой браузер, основанный на луковой маршрутизации) для успешного получения пакетов?' (Should the recipient use a Tor browser (or another browser based on onion routing) for successful packet delivery?). A note below the question says 'Select one option from the list'. The correct answer is marked with a green checkmark and the text 'Great!'. The correct answer is 'Нет' (No). There are two other options listed without checkmarks: 'Да' (Yes) and 'Не знаю' (I don't know). At the bottom of the step, there are 'Next step' and 'Solve again' buttons, and a note stating 'Your submissions You got: 1 point out of 1'.

Рис. 4.4: Рис. 4

5 Раздел 2.4

Wi-Fi - это технология беспроводной локальной сети, работающая в соответствии со стандартом IEEE 802.11

2.4 Беспроводные сети Wi-Fi 8 out of 8 steps passed 5 out of 5 points received

You passed more than 80%, write a review Create review No thanks

Wi-Fi - это

Select one option from the list

Great work!

Correct answer from 965 learners
Total 79% of tries are correct

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

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 5.1: Рис. 1

На каком уровне работает протокол WiFi? Канальным

2.4 Беспроводные сети Wi-Fi 8 out of 8 steps passed 5 out of 5 points received

You passed more than 80%, write a review Create review No thanks

На каком уровне работает протокол WiFi?

Select one option from the list

All is correct.

Correct answer from 972 learners
Total 58% of tries are correct

Транспортном
 Примедном
 Канальным
 Сетевом

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 5.2: Рис. 2

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi WEP

The screenshot shows a Moodle quiz interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by a user icon and the text '⊕ 1' and 'пн'. Below the navigation bar, the title '2.4 Беспроводные сети Wi-Fi' is displayed, along with '8 out of 8 steps passed' and '5 out of 5 points received'. A message says 'You passed more than 80%, write a review' with 'Create review' and 'No thanks' buttons. To the right, a box indicates 'Correct answer from 973 learners' and 'Total 60% of tries are correct'. The main content area contains the question 'Select one option from the list' and a list of four options: 'WPA', 'WEP' (which is selected), 'WPA2', and 'WPA3'. Below the list are 'Next step' and 'Solve again' buttons. At the bottom, it says 'Your submissions You got: 1 point out of 1'.

Рис. 5.3: Рис. 3

Данные между хостом сети (компьютером или смартфоном) и роутером: передаются в зашифрованном виде после аутентификации устройств

The screenshot shows a Moodle quiz interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by a user icon and the text '⊕ 1' and 'пн'. Below the navigation bar, the title '2.4 Беспроводные сети Wi-Fi' is displayed, along with '8 out of 8 steps passed' and '5 out of 5 points received'. A message says 'You passed more than 80%, write a review' with 'Create review' and 'No thanks' buttons. To the right, a box indicates 'Correct answer from 975 learners' and 'Total 53% of tries are correct'. The main content area contains the question 'Select one option from the list' and a list of four options: 'передаются в зашифрованном виде', 'передаются в открытом виде после аутентификации устройств', 'передаются в открытом виде', and 'передаются в зашифрованном виде после аутентификации устройств' (the last one is selected). Below the list are 'Next step' and 'Solve again' buttons. At the bottom, it says 'Your submissions You got: 1 point out of 1'.

Рис. 5.4: Рис. 4

Для домашней сети для аутентификации обычно используется метод: WPA2 Personal

The screenshot shows a Moodle assignment interface. At the top, there is a navigation bar with icons for back, forward, search, and user profile. Below it, the title '2.4 Беспроводные сети Wi-Fi' is displayed, along with '8 out of 8 steps passed' and '5 out of 5 points received'. A progress bar below the title shows 8 green squares followed by 2 question marks. On the right side of the header, there are buttons for 'Create review' and 'No thanks'.

The main content area contains a question: 'Для домашней сети для аутентификации обычно используется метод'. Below the question, a green box contains the instruction 'Select one option from the list' and a note 'Correct answer from 975 learners. Total 87% of tries are correct'. A green checkmark icon next to the text 'Absolutely right.' indicates the correct answer. There are two radio button options: 'WPA2 Personal' (selected) and 'WPA2 Enterprise'. At the bottom of the box are 'Next step' and 'Solve again' buttons. A status bar at the bottom left says 'Your submissions' and 'You got: 1 point out of 1'.

Рис. 5.5: Рис. 5

6 Раздел 3.1. защита ПК и телефона

Можно ли зашифровать загрузочный сектор диска: да

3.1 Шифрование диска 5 out of 5 steps passed 3 out of 3 points received

You passed more than 80%, write a review Create review No thanks

Можно ли зашифровать загрузочный сектор диска

Select one option from the list

Absolutely right.

Да
 Нет

Correct answer from 949 learners
Total 89% of tries are correct

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 6.1: Рис. 1

Шифрование диска основано на: симметричном шифровании

3.1 Шифрование диска 5 out of 5 steps passed 3 out of 3 points received

You passed more than 80%, write a review Create review No thanks

Шифрование диска основано на

Select one option from the list

You are right, well done!

хэшированием
 симметричном шифровании
 асимметричном шифровании

Correct answer from 972 learners
Total 66% of tries are correct

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 6.2: Рис. 2

С помощью каких программ можно зашифровать жесткий диск?:BitLocker,
VeraCrypt

The screenshot shows a Moodle-based learning environment. At the top, there is a navigation bar with icons for back, forward, and search, along with a user icon and a '1' in a box. Below the navigation bar, the title '3.1 Шифрование диска' is displayed, along with '5 out of 5 steps passed' and '3 out of 3 points received'. A message below the title says 'You passed more than 80%, write a review' with options to 'Create review' or 'No thanks'. A green box at the bottom left says 'Your submissions' and 'You got: 1 point out of 1'. The main content area contains a question: 'С помощью каких программ можно зашифровать жесткий диск?'. Below the question, a list of options is shown: 'VeraCrypt' (selected), 'Disk Utility' (not selected), 'Wireshark' (not selected), and 'BitLocker' (selected). A green button labeled 'Next step' is visible, along with a 'Solve again' button. A small box in the top right corner indicates 'Correct answer from 906 learners' and 'Total 28% of tries are correct'.

Рис. 6.3: Рис. 3

7 Раздел 3.2. Пароли

Какие пароли можно отнести с стойким? UQr9@j4!S\$

The screenshot shows a digital quiz interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by a progress bar showing 9 out of 9 steps passed and 6 out of 6 points received. Below the progress bar is a message: "You passed more than 80%, write a review" with "Create review" and "No thanks" buttons. The main content area asks: "Какие пароли можно отнести с стойким?". A list of options is provided: "qwerty12345", "ILOVECATS", "UQr9@j4!S\$", and "IDONTLOVECATS". The correct answer, "UQr9@j4!S\$", is marked with a green checkmark and labeled "Well done!". There are "Next step" and "Solve again" buttons at the bottom. A submission summary at the bottom indicates "Your submissions You got: 1 point out of 1".

Рис. 7.1: Рис. 1

Где безопасно хранить пароли? В менеджерах паролей

The screenshot shows a digital quiz interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by a progress bar showing 9 out of 9 steps passed and 6 out of 6 points received. Below the progress bar is a message: "You passed more than 80%, write a review" with "Create review" and "No thanks" buttons. The main content area asks: "Где безопасно хранить пароли?". A list of options is provided: "В менеджерах паролей" (selected), "В заметках на рабочем столе", "В заметках в телефоне", "На стикере, приклеенном к монитору", and "В кошелеке". The correct answer, "В менеджерах паролей", is marked with a green checkmark and labeled "Great work!". There are "Next step" and "Solve again" buttons at the bottom. A submission summary at the bottom indicates "Your submissions You got: 0 points out of 1".

Рис. 7.2: Рис. 2

Зачем нужна капча? Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

The screenshot shows a Moodle quiz step titled "3.2 Пароли". The progress bar indicates 9 out of 9 steps passed and 6 out of 6 points received. The question asks "Зачем нужна капча?". Below the question, a list of options is shown, with the correct answer selected: "Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа". A green box at the bottom right shows that 974 learners answered correctly, with a total of 77% of tries being correct. Buttons for "Next step" and "Solve again" are visible.

Рис. 7.3: Рис. 3

Для чего применяется хэширование паролей? Для того, чтобы не хранить паро-

The screenshot shows a Moodle quiz step titled "3.2 Пароли". The progress bar indicates 9 out of 9 steps passed and 6 out of 6 points received. The question asks "Для чего применяется хэширование паролей?". Below the question, a list of options is shown, with the correct answer selected: "Для того, чтобы не хранить пароли на сервере в открытом виде.". A green box at the bottom right shows that 973 learners answered correctly, with a total of 61% of tries being correct. Buttons for "Next step" and "Solve again" are visible.

ли на сервере в открытом виде.

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

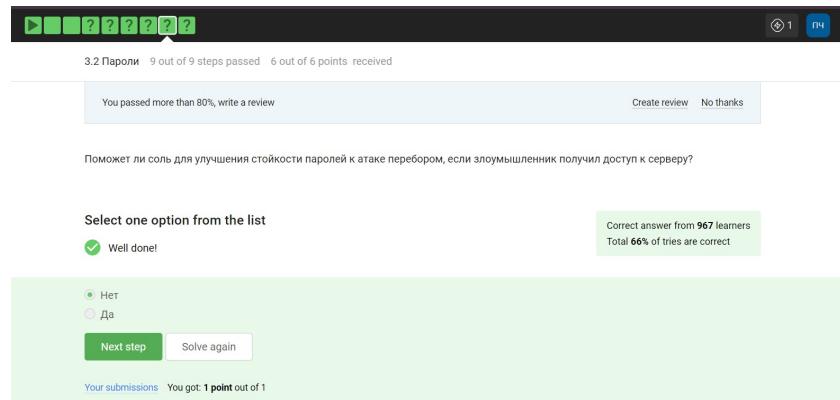


Рис. 7.4: Рис. 5

Какие меры защищают от утечек данных атакой перебором?

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

Рис. 7.5: Рис. 6

8 Раздел 3.3. Фишинг

Какие из следующих ссылок являются фишинговыми? - <https://online.sberbank.wix.ru/CSAFront> (вход в Сбербанк.Онлайн) - https://passport.yandex.ucoz.ru/auth?origin=home_desktop_ru (вход в аккаунт Яндекс)

The screenshot shows a digital assessment interface. At the top, there are navigation icons and a progress bar indicating "3.3 Фишинг" with "5 out of 5 steps passed" and "2 out of 2 points received". Below the progress bar, a message says "You passed more than 80%, write a review" with "Create review" and "No thanks" buttons. The main question asks: "Какие из следующих ссылок являются фишинговыми?". Below the question, a list of four URLs is provided, each with a checkbox:

- <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)

At the bottom of the list are "Next step" and "Solve again" buttons.

Рис. 8.1: Рис. 1

Может ли фишинговый имейл прийти от знакомого адреса? да

The screenshot shows a digital assessment interface. At the top, there are navigation icons and a progress bar indicating "3.3 Фишинг" with "5 out of 5 steps passed" and "2 out of 2 points received". Below the progress bar, a message says "You passed more than 80%, write a review" with "Create review" and "No thanks" buttons. The main question asks: "Может ли фишинговый имейл прийти от знакомого адреса?". Below the question, a list of two options is provided, each with a radio button:

- Да
- Нет

At the bottom of the list are "Next step" and "Solve again" buttons. A note at the bottom states "Your submissions You got: 1 point out of 1".

Рис. 8.2: Рис. 2

9 Раздел 3.3. Вирусы. Примеры

Email Спупинг – это подмена адреса отправителя в имейлах

3.4 Вирусы. Примеры 5 out of 5 steps passed 2 out of 2 points received

You passed more than 80%, write a review Create review No thanks

Email Спупинг – это

Select one option from the list

✓ Good job.

Correct answer from 960 learners
Total 65% of tries are correct

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

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 9.1: Рис. 1

Вирус-троян маскируется под легитимную программу

3.4 Вирусы. Примеры 5 out of 5 steps passed 2 out of 2 points received

You passed more than 80%, write a review Create review No thanks

Вирус-троян

Select one option from the list

✓ Correct.

Correct answer from 969 learners
Total 74% of tries are correct

обязательно шифрует данные и вымогает ключ дешифрования
 маскируется под легитимную программу
 работает исключительно под ОС Windows
 разработан греками

Next step Solve again

Your submissions You got: 1 point out of 1

Рис. 9.2: Рис. 2

10 Раздел 3.5. Безопасность мессенджеров

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

- при генерации первого сообщения стороной-отправителем

The screenshot shows a digital assignment interface. At the top, there are icons for back, forward, and help, followed by a progress bar showing 1 step completed out of 4, and a point value of 2 out of 2. Below the header, a message says 'You passed more than 80%, write a review' with options to 'Create review' or 'No thanks'. A question is displayed: 'На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?'. Below the question, a list of four options is shown, with the second one being correct: 'при генерации первого сообщения стороной-отправителем'. A green checkmark indicates 'Good job.' A note states 'Correct answer from 952 learners' and 'Total 52% of tries are correct'. At the bottom, there are buttons for 'Next step' and 'Solve again', and a message 'Your submissions You got: 1 point out of 1'.

Рис. 10.1: Рис. 1

Суть сквозного шифрования состоит в том, что

- сообщения передаются по узлам связи (серверам) в зашифрованном виде

The screenshot shows a Moodle quiz step titled "3.5 Безопасность мессенджеров". It displays a question about end-to-end encryption and a list of four options. The correct option is selected. The interface includes navigation icons, a progress bar, and a feedback message indicating a correct submission.

You passed more than 80%, write a review

Create review No thanks

Суть сквозного шифрования состоит в том, что

Select one option from the list

Correct

Correct answer from 964 learners
Total 60% of tries are correct

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

Next step Solve again

Your submissions You got: 1 point out of 1

11 Раздел 4.1 Введение в криптографию

В асимметричных криптографических примитивах - обе стороны имеют пару ключей

4.1 Введение в криптографию 7 out of 7 steps passed 5 out of 5 points received

You passed more than 80%, write a review Create review No thanks

В асимметричных криптографических примитивах

Select one option from the list

Correct answer from 940 learners
Total 42% of tries are correct

Yes!

обе стороны имеют общий секретный ключ

одна сторона публикует свой секретный ключ, другая - держит его в секрете

обе стороны имеют пару ключей

одна сторона имеет только секретный ключ, а другая - пару из открытого и секретного ключей

Next step Solve again

Your submissions: You got: 1 point out of 1

Рис. 11.1: Рис. 1

Криптографическая хэш-функция - стойкая к коллизиям - дает на выходе фиксированное число бит независимо от объема входных данных - эффективно вычисляется

К алгоритмам цифровой подписи относятся - RSA - ECDSA - ГОСТ Р 34.10-2012.

The screenshot shows a completed challenge titled "4.1 Введение в криптографию". The user has passed more than 80% and can write a review or skip it. The challenge content asks: "К алгоритмам цифровой подписи относятся". Below is a list of options: AES, SHA2, RSA, ECDSA, and ГОСТ Р 34.10-2012. RSA and ECDSA are checked. A green box says "Great work!". A message box says: "You've solved a complex problem, congratulations! Now you can help other learners in [comments](#) by answering their questions, or compare your solution with others on [solution forum](#)." A green box at the bottom right says "Correct answer from 820 learners Total 19% of tries are correct". Buttons at the bottom are "Next step" and "Solve again".

Рис. 11.2: Рис. 3

Код аутентификации сообщения относится к - симметричным примитивам

The screenshot shows a completed challenge titled "4.1 Введение в криптографию". The user has passed more than 80% and can write a review or skip it. The challenge content asks: "Код аутентификации сообщения относится к". Below is a list of options: асимметричным примитивам and симметричным примитивам. The second option is selected. A green box says "Absolutely right.". A green box at the bottom right says "Correct answer from 934 learners Total 69% of tries are correct". Buttons at the bottom are "Next step" and "Solve again". A message at the bottom says: "Your submissions You got: 1 point out of 1".

Рис. 11.3: Рис. 4

Обмен ключами Диффи-Хэллмана - это -асимметричный примитив генерации общего секретного ключа

The screenshot shows a digital learning platform interface. At the top, there is a progress bar with seven steps, where the first six are green and the last one is grey. Below the progress bar, the text "4.1 Введение в криптографию" is displayed, along with "7 out of 7 steps passed" and "5 out of 5 points received". On the right side of the header, there are icons for a user profile, a search bar, and a help button.

In the main content area, a message says "You passed more than 80%, write a review" with options "Create review" and "No thanks". Below this, a note states "Обмен ключами Диффи-Хеллмана - это".

A question is presented: "Select one option from the list". The correct answer is marked with a green checkmark and the text "Good news for you, correct!". The question asks about the Diffie-Hellman key exchange mechanism. The correct option is highlighted with a green dot:

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

At the bottom of the question area, there are two buttons: "Next step" and "Solve again". A note at the very bottom says "Your submissions You got: 1 point out of 1".

Рис. 11.4: Рис. 5

12 Раздел 4.2 Цифровая подпись

Протокол электронной цифровой подписи относится к - протоколам с публичным (или открытым) ключом

The screenshot shows a digital assessment interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by the title '4.2 Цифровая подпись'. Below the title, it says '8 out of 8 steps passed' and '5 out of 5 points received'. A message box indicates 'You passed more than 80%, write a review' with 'Create review' and 'No thanks' buttons. The main content area contains the question: 'Протокол электронной цифровой подписи относится к'. Below the question, a list of options is shown with the correct answer selected: '• протоколам с публичным (или открытым) ключом'. There are 'Next step' and 'Solve again' buttons. A feedback box states 'Correct answer from 896 learners' and 'Total 70% of tries are correct'. At the bottom, it shows 'Your submissions You got: 1 point out of 1' and a progress bar indicating Step 4 of 8.

Рис. 12.1: Рис. 1

Алгоритм верификации электронной цифровой подписи требует на вход - под-

The screenshot shows a digital assessment interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by the title '4.2 Цифровая подпись'. Below the title, it says '8 out of 8 steps passed' and '5 out of 5 points received'. A message box indicates 'You passed more than 80%, write a review' with 'Create review' and 'No thanks' buttons. The main content area contains the question: 'Алгоритм верификации электронной цифровой подписи требует на вход'. Below the question, a list of options is shown with the correct answer selected: '• подпись, открытый ключ, сообщение'. There are 'Next step' and 'Solve again' buttons. A feedback box states 'Correct answer from 890 learners' and 'Total 45% of tries are correct'. At the bottom, it shows 'Your submissions You got: 1 point out of 1' and a progress bar indicating Step 4 of 8.

пись, открытый ключ, сообщение

Электронная цифровая подпись не обеспечивает -конфиденциальность

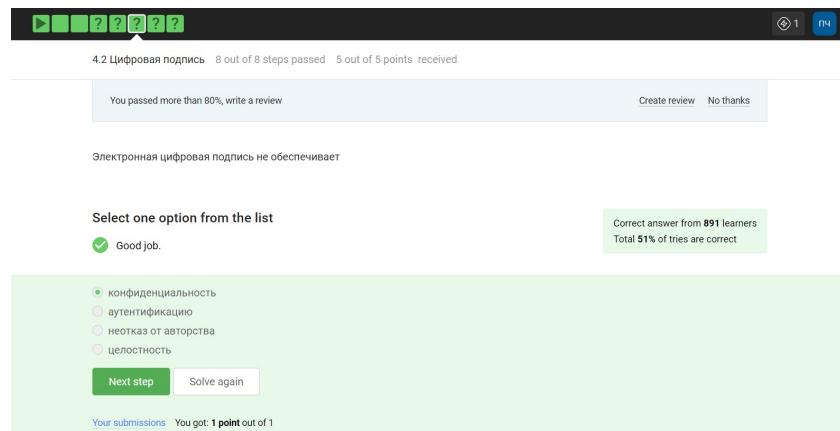


Рис. 12.2: Рис. 3

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

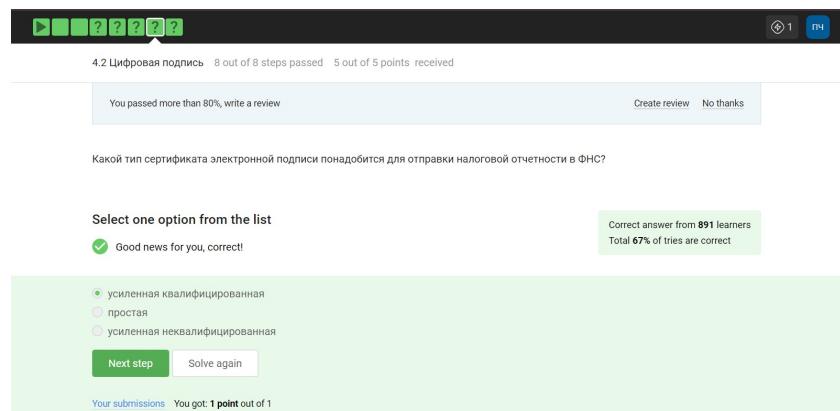


Рис. 12.3: Рис. 4

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи? -в удостоверяющем (сертификационном) центре

The screenshot shows a step in a course titled "4.2 Цифровая подпись". It displays a progress bar with 8 steps completed (green) and 1 step pending (yellow). The status bar indicates "8 out of 8 steps passed" and "5 out of 5 points received". A message says "You passed more than 80%, write a review" with options "Create review" and "No thanks". Below the message is a question: "В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?". A green box contains the instruction "Select one option from the list" and a "Well done!" message. A green button labeled "Next step" is visible. The correct answer is highlighted with a green dot and the text "в удостоверяющем (сертификационном) центре". A note at the bottom right says "Correct answer from 889 learners" and "Total 60% of tries are correct".

Рис. 12.4: Рис. 5

13 Раздел 4.3 Электронные платежи

Выберите из списка все платежные системы. - MasterCard - МИР

The screenshot shows a Moodle assignment interface. At the top, there are navigation icons (moodle, user, search, etc.) and a progress bar indicating 5 out of 5 steps passed and 3 out of 3 points received. Below the title '4.3 Электронные платежи' is a message: 'You passed more than 80%, write a review' with options 'Create review' and 'No thanks'. A note below says 'Выберите из списка все платежные системы.' A feedback box states 'Select all correct options from the list' and 'Great!' with a green checkmark. It also mentions 'You've solved a complex problem, congratulations! Now you can help other learners in comments by answering their questions, or compare your solution with others on solution forum.' A green box at the bottom lists the correct options: BitCoin (unchecked), MasterCard (checked), SecurePay (unchecked), POS-терминал (unchecked), банкомат (unchecked), and МИР (checked). Buttons for 'Next step' and 'Solve again' are visible.

Рис. 13.1: Рис. 1

Примером многофакторной аутентификации является - комбинация проверка пароля + код в sms сообщении - комбинация код в sms сообщении + отпечаток пальца

The screenshot shows a digital learning platform interface. At the top, there is a navigation bar with icons for back, forward, and search, followed by a user icon and a 'my' button. Below the navigation bar, the title '4.3 Электронные платежи' is displayed, along with '5 out of 5 steps passed' and '3 out of 3 points received'. A message box says 'You passed more than 80%, write a review' with 'Create review' and 'No thanks' buttons. To the right, there is a green box indicating 'Correct answer from 806 learners' and 'Total 23% of tries are correct'. The main content area has a light green background. It asks 'Select all correct options from the list' and provides a list of four items, three of which are checked: 'комбинация проверки пароля + Капча', 'комбинация проверка пароли + код в sms сообщении', and 'комбинация код у sms сообщении + отпечаток пальца'. The fourth item, 'комбинация PIN код + пароль', is unchecked. Below the list are 'Next step' and 'Solve again' buttons. A yellow box at the bottom says 'You've solved a complex problem, congratulations! Now you can help other learners in comments by answering their questions, or compare your solution with others on solution forum.'

Рис. 13.2: Рис. 2

При онлайн платежах сегодня используется - многофакторная аутентификация покупателя перед банком-эмитентом

The screenshot shows a digital learning platform interface, similar to Figure 2. At the top, there is a navigation bar with icons for back, forward, and search, followed by a user icon and a 'my' button. Below the navigation bar, the title '4.3 Электронные платежи' is displayed, along with '5 out of 5 steps passed' and '3 out of 3 points received'. A message box says 'You passed more than 80%, write a review' with 'Create review' and 'No thanks' buttons. To the right, there is a green box indicating 'Correct answer from 865 learners' and 'Total 59% of tries are correct'. The main content area has a light green background. It asks 'Select one option from the list' and provides a list of four items, with the first item checked: 'многофакторная аутентификация покупателя перед банком-эмитентом'. The other three items are unchecked: 'однофакторная аутентификация покупателя перед банком-эквайером', 'однофакторная аутентификация при помощи PIN-кода карты перед терминалом', and 'многофакторная аутентификация покупателя перед банком-эквайером'. Below the list are 'Next step' and 'Solve again' buttons. A yellow box at the bottom says 'Your submissions You got: 1 point out of 1'.

Рис. 13.3: Рис. 3

14 Раздел 4.4 Блокчейн

Какое свойство криптографической хэш-функции используется в доказательстве работы? - сложность нахождения прообраза

The screenshot shows a digital assignment interface. At the top, there is a navigation bar with icons for back, forward, search, and user profile. Below it, a progress bar indicates '6 out of 6 steps passed' and '3 out of 3 points received'. A message says 'You passed more than 80%, write a review' with options to 'Create review' or 'No thanks'. The main question is: 'Какое свойство криптографической хэш-функции используется в доказательстве работы?' Below the question, a list of options is shown:

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

At the bottom of the list, there are two buttons: 'Next step' and 'Solve again'. A note at the bottom states: 'Your submissions You got: 1 point out of 1'. To the right of the list, a box shows statistics: 'Correct answer from 880 learners' and 'Total 48% of tries are correct'.

Рис. 14.1: Рис. 1

Консенсус в некоторых системах блокчейн обладает свойствами - открытость - консенсус - постоянства - живучесть

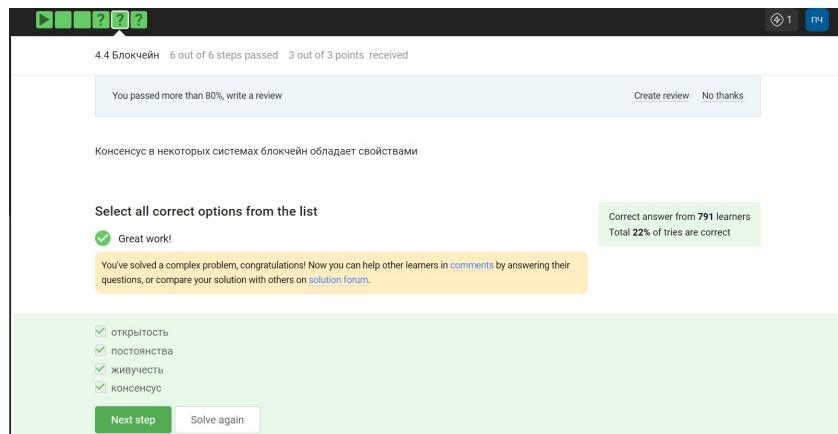


Рис. 14.2: Рис. 2

Секретные ключи какого криптографического примитива хранят участники блокчейна? - цифровая подпись

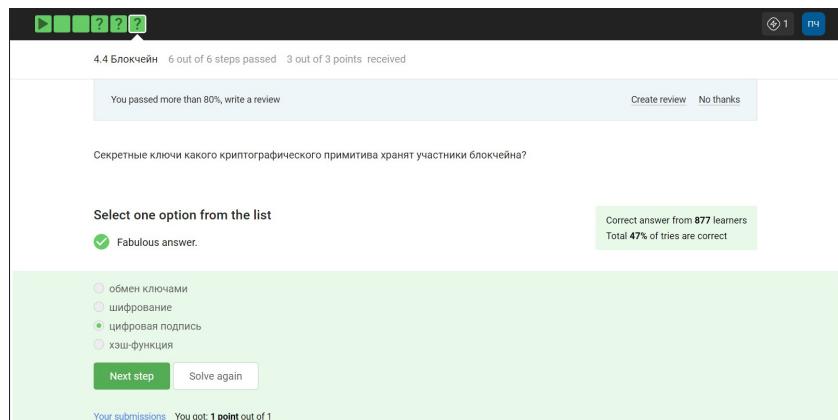


Рис. 14.3: Рис. 3

15 Вывод

Курс пройден, сертификат не выдаётся на этом курсе. Я научился основным методам информационной безопасности

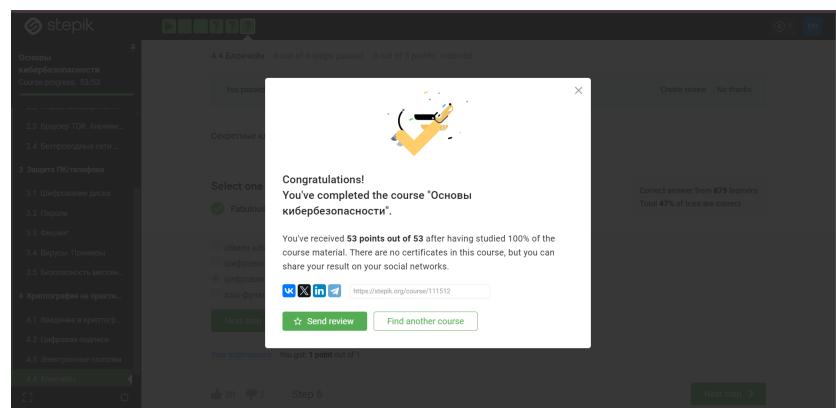


Рис. 15.1: Прохождение курса