

Внешний курс

Основы информационной безопасности

Прокопьева М. Е.

Российский университет дружбы народов, Москва, Россия

Информация

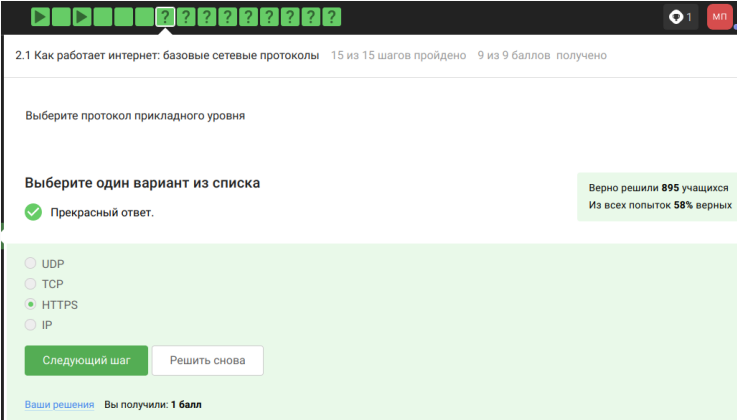
- Прокопьева Марина Евгеньевна
- студент
- Российский университет дружбы народов

Цель работы

Пройти курс на степике и узнать много нового (или нет)

Выполнение

UDP - протокол сетевого уровня TCP - протокол транспортного уровня HTTPS - протокол прикладного уровня IP - протокол сетевого уровня, поэтому ответ HTTPS



The screenshot shows a quiz interface with a progress bar at the top containing 15 green squares, the 15th of which is a question mark. The question title is "2.1 Как работает интернет: базовые сетевые протоколы". The progress indicates "15 из 15 шагов пройдено" and "9 из 9 баллов получено". The question text is "Выберите протокол прикладного уровня". Below it, a green box says "Выберите один вариант из списка". A green checkmark icon is followed by the text "Прекрасный ответ.". To the right, a green box displays statistics: "Верно решили 895 учащихся" and "Из всех попыток 58% верных". The list of options includes UDP, TCP, HTTPS (which is selected with a green dot), and IP. At the bottom, there are two buttons: "Следующий шаг" and "Решить снова". The footer shows "Ваши решения" and "Вы получили: 1 балл".

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Выберите протокол прикладного уровня

Выберите один вариант из списка

✓ Прекрасный ответ.

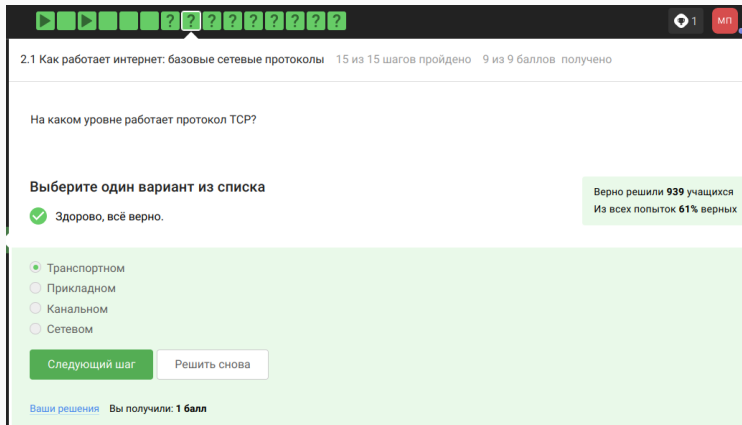
Верно решили 895 учащихся
Из всех попыток 58% верных

☐ UDP
☐ TCP
☒ HTTPS
☐ IP

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Ранее было упомянуто, что протокол TCP - transmission control protocol - работает на транспортном уровне



2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

На каком уровне работает протокол TCP?

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 939 учащихся
Из всех попыток 61% верных

☒ Транспортном
☐ Прикладном
☐ Канальном
☐ Сетевом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 2: нет названия

В адресе типа IPv4 не может быть чисел больше 255, поэтому первые два варианта не подходят

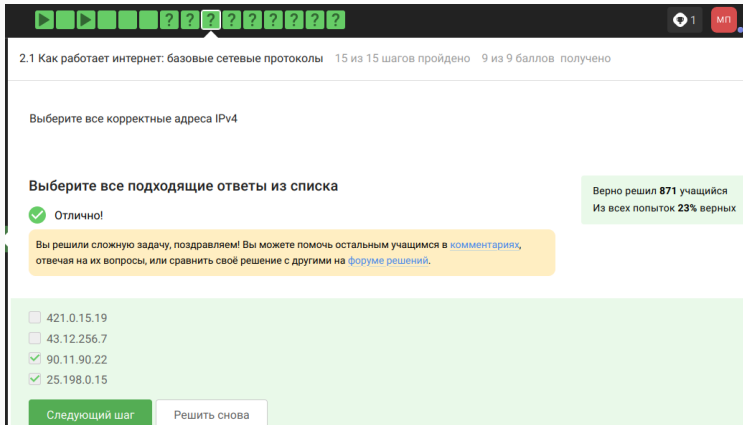
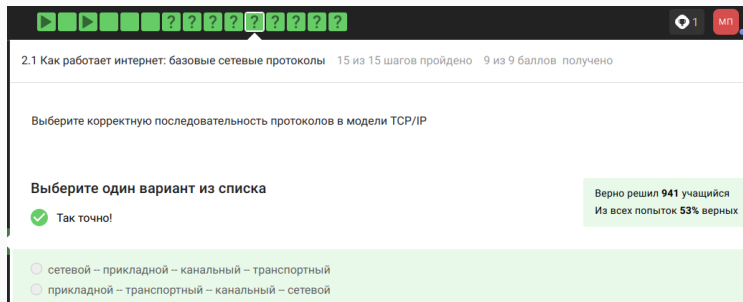


Рис. 3: нет названия

Распределение протоколов в модели TCP/IP:

- Прикладной уровень (Application Layer): HTTP, RTSP, FTP, DNS.
- Транспортный уровень (Transport Layer): TCP, UDP, SCTP, DCCP.
- Сетевой (Межсетевой) уровень (Network Layer): IP.
- Уровень сетевого доступа (Канальный) (Link Layer): Ethernet, IEEE 802.11, WLAN, SLIP, Token Ring



The screenshot shows a quiz interface with a progress bar at the top containing 15 green squares, the 15th of which is highlighted. The quiz title is "2.1 Как работает интернет: базовые сетевые протоколы" with a progress of "15 из 15 шагов пройдено" and a score of "9 из 9 баллов получено". The question asks to "Выберите корректную последовательность протоколов в модели TCP/IP". The instruction says "Выберите один вариант из списка". The correct answer, "Так точно!", is marked with a green checkmark. A statistics box on the right states "Верно решил 941 учащийся" and "Из всех попыток 53% верных". Two incorrect options are listed at the bottom:

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

протокол http передает не зашифрованные данные, а протокол https уже будет передавать зашифрованные данные

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

Протокол http предполагает

Выберите один вариант из списка

✓ Здорово, всё верно.

Верно решили 965 учащихся
Из всех попыток 78% верных

☐ передачу зашифрованных данных между клиентом и сервером

☒ передачу данных между клиентом и сервером в открытом виде

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

103 13 Шаг 12 Следующий шаг >

Рис. 6: нет названия

https передает зашифрованные данные, одна из фаз - передача данных, другая должна быть рукопожатием

[illegible]

Рис. 7: нет названия

**TLS определяется и клиентом, и сервером, чтобы было возможно подклю-
читься**

[illegible]

Рис. 8: нет названия

остальные варианты в протоколе предусмотрены

▶

▶

▶

▶

▶

?

?

?

?

?

?

?

?

?

1

МП

2.1 Как работает интернет: базовые сетевые протоколы 15 из 15 шагов пройдено 9 из 9 баллов получено

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

☒ Абсолютно точно.

☐ 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: **1 балл**

Верно решил **931** учащихся

Из всех попыток **44%** верных

Рис. 9: нет названия

Куки точно не хранят пароли и IP-адреса, а id сессии и идентификатор хранят

1

МП

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

Куки хранят:

Выберите все подходящие ответы из списка

☒ Отличное решение!

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

Верно решили 856 учащихся
Из всех попыток 18% верных

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

Следующий шаг

Решить снова

Рис. 10: нет названия

куки не делают соединение более надежным

The screenshot shows a quiz interface with a dark header bar. On the left, there are six green square icons: a play button, a question mark, and four more question marks. On the right, there is a shield icon with the number '1' and a red button labeled 'МП'. Below the header, the title '2.2 Персонализация сети' is followed by progress indicators: '6 из 6 шагов пройдено' and '4 из 4 баллов получено'. The main content area has a light green background. It starts with the text 'Куки не используются для'. Below this, it says 'Выберите один вариант из списка'. There are five radio button options: 'аутентификации пользователя', 'персонализации веб-страниц', 'отслеживания информации о пользователе', 'сборе статистики посещаемости сайта', and 'улучшения надежности соединения'. The last option is selected. At the bottom, there are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). On the right side, there is a green box with the text 'Верно решили 950 учащихся' and 'Из всех попыток 53% верных'.

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

Куки не используются для

Выберите один вариант из списка

☒ Верно. Так держать!

☐ аутентификации пользователя

☐ персонализации веб-страниц

☐ отслеживания информации о пользователе

☐ сборе статистики посещаемости сайта

☒ улучшения надежности соединения

Следующий шаг Решить снова

Верно решили 950 учащихся
Из всех попыток 53% верных

Рис. 11: нет названия

This is a partial screenshot of the same quiz interface, showing the header bar with the icons and the progress bar with the text '2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено'.

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

Сессионные куки хранятся в течение сессии, то есть пока используется веб-сайт

The screenshot shows a quiz interface with a dark header bar. On the left, there are five icons: a play button, a green square, and three question marks. On the right, there is a shield icon with the number '1' and a red button labeled 'МП'. Below the header, the title '2.2 Персонализация сети' is followed by progress indicators: '6 из 6 шагов пройдено' and '4 из 4 баллов получено'. The main question is 'Сессионные куки хранятся в браузере?'. Below it, the instruction 'Выберите один вариант из списка' is shown. There are three radio button options: 'Да, на время пользования веб-сайтом' (selected), 'Нет', and 'Да, на некоторое время, заданное в сервером'. To the right of the options, a green box displays statistics: 'Верно решили 959 учащихся' and 'Из всех попыток 60% верных'. At the bottom, there are two buttons: 'Следующий шаг' and 'Решить снова'. A footer line shows 'Ваши решения' and 'Вы получили: 1 балл'.

2.2 Персонализация сети 6 из 6 шагов пройдено 4 из 4 баллов получено

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 959 учащихся
Из всех попыток 60% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 13: нет названия

Необходимо три узла - входной, промежуточный и выходной

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

☒ Отличное решение!

Верно решили 959 учащихся
Из всех попыток 77% верных

☐ 2
☒ 3
☐ 4

Следующий шаг Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 14: нет названия

IP-адрес не должен быть известен охранному и промежуточному узлам

?

?

?

?

1

МП

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

IP-адрес получателя известен

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 своё решение с другими на [форуме решений](#).

Верно решили **906** учащихся
Из всех попыток **19%** верных

☐ охранному узлу

☐ промежуточному узлу

☒ отправителю

☒ выходному узлу

Следующий шаг

Решить снова

Рис. 15: нет названия

Отправитель генерирует общий секретный ключ со узлами, через которые идет передача, то есть со всеми

??

??

1МП

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

☒ Хорошая работа.

☐ только с охранным узлом

☐ с охранным и промежуточным узлом

☒ с охранным, промежуточным и выходным узлом

☐ с промежуточным и выходным узлом

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Верно решили 959 учащихся
Из всех попыток 55% верных

Рис. 16: нет названия

Для получения пакетов не нужно использовать TOR

1

МП

2.3 Браузер TOR. Анонимизация 6 из 6 шагов пройдено 4 из 4 баллов получено

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

Выберите один вариант из списка

☒ Прекрасный ответ.

Верно решил 961 учащийся
Из всех попыток 74% верных

☐ Да

☒ Нет

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 17: нет названия

это определение Wi-Fi

1

МП

2.4 Беспроводные сети Wi-fi 8 из 8 шагов пройдено 5 из 5 баллов получено

Wi-Fi - это

Выберите один вариант из списка

Абсолютно точно.

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

Верно решили 965 учащихся
Из всех попыток 79% верных

Рис. 18: нет названия

Для целей работы в Интернете Wi-Fi обычно располагается как канальный уровень

?

?

?

?

?

1

МП

2.4 Беспроводные сети Wi-fi 8 из 8 шагов пройдено 5 из 5 баллов получено

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

Верно. Так держать!

Верно решили 972 учащихся
Из всех попыток 58% верных

☐ Транспортном

☐ Прикладном

☒ Канальном

☐ Сетевом

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 19: нет названия

WEP (Wired Equivalent Privacy) – устаревший и небезопасный метод проверки подлинности

The screenshot shows a quiz interface with a dark header bar. On the left, there are seven colored squares: a green play button, three green squares, and three green squares with question marks. On the right, there is a white eye icon, the number '1', and a red button labeled 'МП'. Below the header, the text '2.4 Беспроводные сети Wi-Fi' is followed by '8 из 8 шагов пройдено' and '5 из 5 баллов получено'. The main content area has a title 'Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi'. Below this, it says 'Выберите один вариант из списка'. There are four radio button options: WPA, WEP (which is selected), WPA2, and WPA3. To the right of the options, a green box contains the text 'Верно решили 973 учащихся' and 'Из всех попыток 60% верных'. At the bottom, there are two buttons: 'Следующий шаг' (green) and 'Решить снова' (white). Below the buttons, it says 'Ваши решения' and 'Вы получили: 1 балл'.

2.4 Беспроводные сети Wi-Fi 8 из 8 шагов пройдено 5 из 5 баллов получено

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

☒ Так точно!

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Верно решили 973 учащихся
Из всех попыток 60% верных

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Рис. 20: нет названия

Нужно аутентифицировать устройства и позже передаются зашифрованные данные

?

?

?

?

?

1

МП

2.4 Беспроводные сети Wi-fi 8 из 8 шагов пройдено 5 из 5 баллов получено

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

✓

Всё правильно.

Верно решили 975 учащихся
Из всех попыток 53% верных

☐ передаются в зашифрованном виде

☐ передаются в открытом виде

☒ передаются в зашифрованном виде после аутентификации устройств

☐ передаются в открытом виде после аутентификации устройств

Следующий шаг

Решить снова

Ваши решения

Вы получили: 1 балл

Рис. 21: нет названия

WPA2 Personal для личного использования

1

МП

2.4 Беспроводные сети Wi-fi 8 из 8 шагов пройдено 5 из 5 баллов получено

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

Всё получилось!

Верно решили 975 учащихся
Из всех попыток 87% верных

☒ WPA2 Personal

☐ WPA2 Enterprise

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

👍 42

👎 4

Шаг 8

Следующий шаг >

Рис. 22: нет названия

Шифрование диска — технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать.

The screenshot shows a quiz interface for the topic '3.1 Шифрование диска'. At the top, there is a progress bar with five colored squares (green, green, green, yellow, yellow) and a score of '1' next to a 'МП' (minutes) icon. Below the progress bar, the title '3.1 Шифрование диска' is followed by '5 из 5 шагов пройдено' and '3 из 3 баллов получено'. The main question is 'Можно ли зашифровать загрузочный сектор диска'. Below the question, it says 'Выберите один вариант из списка'. There are two radio button options: 'Да' (selected) and 'Нет'. A green checkmark icon is next to the 'Да' option, and the text 'Правильно, молодец!' is displayed. To the right of the options, a green box contains the text 'Верно решили 949 учащихся' and 'Из всех попыток 89% верных'. Below the options, there are two buttons: 'Следующий шаг' (highlighted in green) and 'Решить снова'. At the bottom left, there is a link 'Ваши решения' and the text 'Вы получили: 1 балл'. At the bottom right, there is a green button with the text 'Следующий шаг' and a right arrow. The bottom of the interface shows a footer with a thumbs up icon, the number '44', a thumbs down icon, the number '5', the text 'Шаг 3', and a green button with the text 'Следующий шаг' and a right arrow.

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

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка

☒ Да
☐ Нет

Правильно, молодец!

Верно решили 949 учащихся
Из всех попыток 89% верных

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

44 5 Шаг 3 Следующий шаг

Рис. 23: нет названия

Шифрование диска основано на симметричном шифровании

?

?

?

1

МП

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

Шифрование диска основано на

Выберите один вариант из списка

☒ Всё правильно.

Верно решили 972 учащихся
Из всех попыток 66% верных

☐ хэшировании

☒ симметричном шифровании

☐ асимметричном шифровании

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 24: нет названия

Отмечены программы, с помощью которых можно зашифровать жетский диск

???

1МП

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

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

☒ Всё получилось!

Верно решили 906 учащихся
Из всех попыток 28% верных

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

☒ BitLocker

☒ VeraCrypt

☐ Disk Utility

☐ Wireshark

Следующий шаг

Решить снова

Рис. 25: нет названия

Стойкий пароль - тот, который тяжелее подобрать, он должен быть со спец. символами и длинный

The image shows a web-based quiz interface for password strength. At the top, there is a progress bar with 10 colored squares (green, yellow, red) and a question mark icon. Below this, the text "3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено" indicates the current progress. The main question is "Какие пароли можно отнести с стойким?". Below the question, there is a prompt "Выберите один вариант из списка". A green checkmark icon and the text "Всё получилось!" indicate a correct answer. A list of four password options is shown: "qwerty12345", "ILOVECATS", "UQr9@j4!S\$", and "IDONTLOVECATS". The option "UQr9@j4!S\$" is selected. Below the list, there are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). In the bottom right corner, there is a green box with the text "Верно решили 969 учащихся Из всех попыток 85% верных". At the bottom left, there is a link "Ваши решения" and the text "Вы получили: 1 балл".

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Всё получилось!

☐ qwerty12345

☐ ILOVECATS

☒ UQr9@j4!S\$

☐ IDONTLOVECATS

Следующий шаг

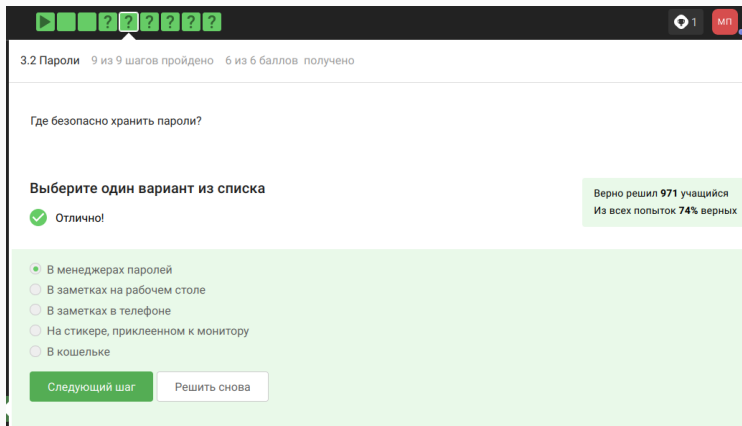
Решить снова

Верно решили 969 учащихся
Из всех попыток 85% верных

Ваши решения Вы получили: 1 балл

Рис. 26: нет названия

Все варианты, кроме менеджера паролей, совершенно не надежные



The screenshot shows a quiz interface with a dark header bar. On the left, there's a progress indicator with colored squares and question marks. On the right, there's a user profile icon with the number '1' and a red button labeled 'МП'. Below the header, the text '3.2 Пароли' is followed by '9 из 9 шагов пройдено' and '6 из 6 баллов получено'. The main question is 'Где безопасно хранить пароли?'. Below it, the instruction 'Выберите один вариант из списка' is shown. A green checkmark icon is next to the text 'Отлично!'. To the right, a green box contains the text 'Верно решил 971 учащихся' and 'Из всех попыток 74% верных'. The list of options includes: 'В менеджерах паролей' (selected), 'В заметках на рабочем столе', 'В заметках в телефоне', 'На стикере, приклеенном к монитору', and 'В кошельке'. At the bottom, there are two buttons: 'Следующий шаг' and 'Решить снова'.

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Где безопасно хранить пароли?

Выберите один вариант из списка

Отлично!

Верно решил 971 учащихся
Из всех попыток 74% верных

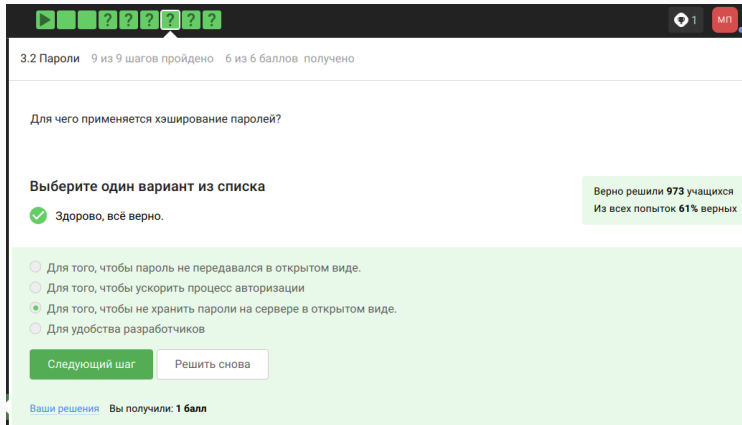
- ☒ В менеджерах паролей
- ☐ В заметках на рабочем столе
- ☐ В заметках в телефоне
- ☐ На стикере, приклеенном к монитору
- ☐ В кошельке

Следующий шаг Решить снова

Рис. 27: нет названия

Капча нужна для проверки на то, что за экраном “не робот”

Опасно хранить пароли в открытом виде, поэтому хранят их хэши



The screenshot shows a quiz interface with a dark header bar. On the left, there are eight colored squares: a green play button, three green squares, and three green squares with question marks. On the right, there is a white eye icon with the number '1' and a red square with the letters 'МП'. Below the header, the text '3.2 Пароли' is followed by '9 из 9 шагов пройдено' and '6 из 6 баллов получено'. The main question is 'Для чего применяется хэширование паролей?'. Below it, the instruction 'Выберите один вариант из списка' is shown. There are four radio button options: 'Здорово, всё верно.' (which is selected with a green checkmark), 'Для того, чтобы пароль не передавался в открытом виде.', 'Для того, чтобы ускорить процесс авторизации', and 'Для того, чтобы не хранить пароли на сервере в открытом виде.'. At the bottom, there are two buttons: 'Следующий шаг' (highlighted in green) and 'Решить снова'. On the right side, a green box displays statistics: 'Верно решили 973 учащихся' and 'Из всех попыток 61% верных'. At the bottom left, it says 'Ваши решения' and 'Вы получили: 1 балл'.

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Для чего применяется хэширование паролей?

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ 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

Верно решили 973 учащихся
Из всех попыток 61% верных

Ваши решения Вы получили: 1 балл

Рис. 29: нет названия

Все приведенные меры защищают от утечек данных

?

?

?

?

?

?

1МП

3.2 Пароли 9 из 9 шагов пройдено 6 из 6 баллов получено

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Всё правильно.

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

Верно решили 895 учащихся

Из всех попыток 16% верных

☒ разные пароли на всех сайтах

☒ периодическая смена паролей

☒ сложные(=длинные) пароли

☒ капча

Следующий шаг

Решить снова

Рис. 31: нет названия

Фишинговые ссылки очень похожи на ссылки известных сервисов, но с некоторыми отличиями

?

?

1

МП

3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

Прекрасный ответ.

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

Верно решил 861 учащийся
Из всех попыток 19% верных

☐ <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

Рис. 32: нет названия

Ответ дан в соответствии с определением

?

?

1

МП

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

Email Спуфинг – это

Выберите один вариант из списка

☒ Здорово, всё верно.

☐ 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**

Верно решили **960** учащихся
Из всех попыток **65%** верных

Рис. 34: нет названия

Троян маскируется под обычную программу

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

Вирус-троян

Выберите один вариант из списка

✓ Отлично!

Верно решили **969** учащихся
Из всех попыток **74%** верных

- ☐ 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: **1 балл**

Рис. 35: нет названия

При установке первого сообщения отправителем формируется ключ шифрования

Суть сквозного шифрования состоит в том, что сообщения передаются по узлам связи в зашифрованном виде

▶

■

?

?

1

МП

3.5 Безопасность мессенджеров 4 из 4 шагов пройдено 2 из 2 баллов получено

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка

✓ Отлично!

Верно решили 964 учащихся
Из всех попыток 60% верных

☒ 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

Рис. 37: нет названия

Для ответа на вопрос используется определение асимметричного шифрования с двумя ключами

?

?

?

?

?

1

МП

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

В асимметричных криптографических примитивах

Выберите один вариант из списка

Правильно.

Верно решили 940 учащихся
Из всех попыток 42% верных

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

☒ обе стороны имеют пару ключей

☐ обе стороны имеют общий секретный ключ

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Рис. 38: нет названия

Отмечены алгоритмы цифровой подписи

The screenshot shows a quiz interface with a dark header bar. On the left, there are six colored squares: a green play button, a green square, and four squares with question marks (green, green, yellow, green). On the right, there is a shield icon with the number '1' and a red button labeled 'МП'. Below the header, the text '4.1 Введение в криптографию' is followed by '7 из 7 шагов пройдено' and '5 из 5 баллов получено'. The main content area has a light green background. It contains the text 'К алгоритмам цифровой подписи относятся' and a prompt 'Выберите все подходящие ответы из списка'. A green checkmark icon is followed by the text 'Правильно, молодец!'. Below this, a yellow box contains a congratulatory message and links to 'комментариях' and 'форуме решений'. On the right, a green box shows statistics: 'Верно решили 834 учащихся' and 'Из всех попыток 19% верных'. At the bottom, a list of algorithms is shown with checkboxes: AES (unchecked), SHA2 (unchecked), RSA (checked), ECDSA (checked), and ГОСТ Р 34.10-2012 (checked).

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

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

✓ Правильно, молодец!

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

Верно решили 834 учащихся
Из всех попыток 19% верных

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

Рис. 40: нет названия

В информационной безопасности аутентификация

сообщения или аутентификация источника данных-это свойство, которое гарантирует, что сообщение не было изменено во время передачи (целостность данных) и что принимающая сторона может проверить источник сообщения

The screenshot shows a quiz interface for a lesson titled "4.1 Введение в криптографию". The progress bar indicates "7 из 7 шагов пройдено" and "5 из 5 баллов получено". The question asks: "Код аутентификации сообщения относится к". Below the question, it says "Выберите один вариант из списка". There are two radio button options: "симметричным примитивам" (selected) and "асимметричным примитивам". At the bottom, there are two buttons: "Следующий шаг" and "Решить снова". On the right side, there is a green box with statistics: "Верно решили 955 учащихся" and "Из всех попыток 69% верных". At the bottom left, it says "Ваши решения" and "Вы получили: 1 балл".

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

Код аутентификации сообщения относится к

Выберите один вариант из списка

✓ Хорошие новости, верно!

☒ симметричным примитивам
☐ асимметричным примитивам

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл

Верно решили 955 учащихся
Из всех попыток 69% верных

Определение обмена ключами Диффи-Хэллмана.

?

?

?

?

?

1

МП

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

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка

Хорошая работа.

Верно решили 948 учащихся
Из всех попыток 47% верных

☐ 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: ...

Рис. 42: нет названия

По определению цифровой подписи протокол ЭЦП относится к протоколам с^{39/48}
публичным ключом

На первом этапе получатель сообщения строит собственный вариант хэш-функции подписанного документа. На втором этапе происходит расшифровка хэш-функции, содержащейся в сообщении с помощью открытого ключа отправителя. На третьем этапе производится сравнение двух хэш-функций. Их совпадение гарантирует одновременно подлинность содержимого документа и его авторства

?

?

?

?

?

1

МП

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Правильно, молодец!

Верно решили 962 учащихся
Из всех попыток 46% верных

☐ подпись, открытый ключ

☐ подпись, секретный ключ

☒ подпись, открытый ключ, сообщение

☐ подпись, секретный ключ, сообщение

Следующий шаг

Решить снова

Электронная подпись обеспечивает все указанное, кроме конфиденциальности

?

?

?

?

?

1

МП

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка

Верно.

целостность

аутентификацию

неотказ от авторства

☒ конфиденциальность

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл

Верно решили 968 учащихся
Из всех попыток 53% верных

Рис. 45: нет названия

Для отправки налоговой отчетности в ФНС используется усиленная квалифицированная электронная подпись

?

?

?

?

?

1

МП

4.2 Цифровая подпись 8 из 8 шагов пройдено 5 из 5 баллов получено

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

Выберите один вариант из списка

Правильно, молодец!

Верно решили 975 учащихся
Из всех попыток 68% верных

☐ усиленная неквалифицированная

☒ усиленная квалифицированная

☐ простая

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл

Рис. 46: нет названия

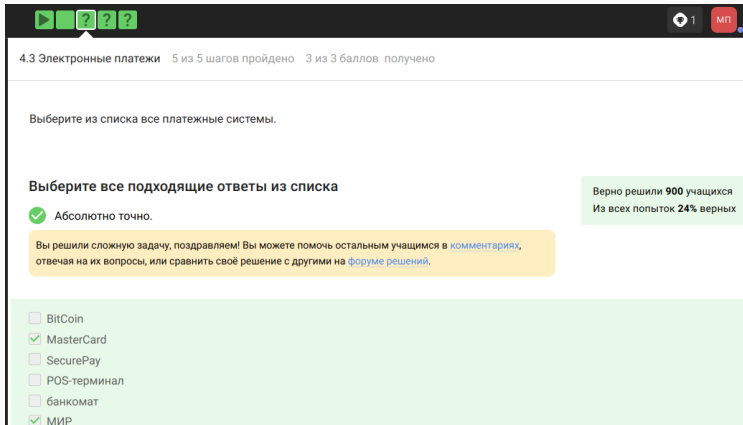
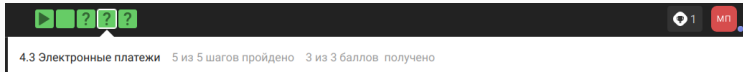


Рис. 48: нет названия



При онлайн платежах используется многофакторная аутентификация

1

МП

4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено

При онлайн платежах сегодня используется

Выберите один вариант из списка

Правильно.

Верно решили 957 учащихся
Из всех попыток 59% верных

☒ 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

Рис. 50: нет названия

Proof-of-Work, или PoW, (доказательство выполнения работы) — это алгоритм достижения консенсуса в блокчейне

?

?

?

1

МП

4.4 Блокчейн 6 из 6 шагов пройдено 3 из 3 баллов получено

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка

✓

Хорошая работа.

фиксированная длина выходных данных

●

сложность нахождения прообраза

обеспечение целостности

эффективность вычисления

Следующий шаг

Решить снова

Ваши решения

Вы получили: 1 балл

Верно решили 932 учащихся

Из всех попыток 49% верных

Рис. 51: нет названия

Консенсус блокчейна — это процедура, в ходе которой участники сети достигают согласия о текущем состоянии данных в сети

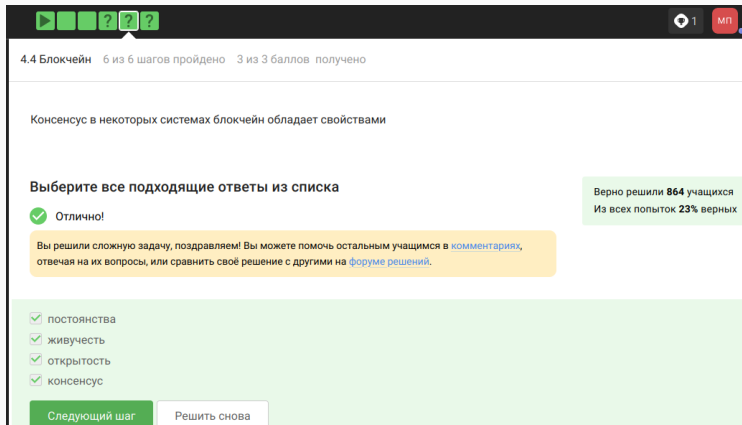


Рис. 52: нет названия



Основы кибербезопасности

100% материалов пройдено

53/53 баллов получено

Описание

Содержание

Новости

Комментарии

Отзывы

Выводы

Прошла курс на степике