

Внешний курс на Stepik

Основы кибербезопасности

Шуваев Сергей Александрович

Содержание

1 Цель работы	5
2 Раздел 2.1	6
3 Раздел 2.2	11
4 Раздел 2.3	13
5 Раздел 2.4	15
6 Раздел 3.1. защита ПК и телефона	18
7 Раздел 3.2. Пароли	20
8 Раздел 3.3. Фишинг	22
9 Раздел 3.3. Вирусы. Примеры	23
10 Раздел 3.5. Безопасность мессенджеров	24
11 Раздел 4.1 Введение в криптографию	25
12 Раздел 4.2 Цифровая подпись	27
13 Раздел 4.3 Электронные платежи	29
14 Раздел 4.4 Блокчейн	31
15 Вывод	32

Список иллюстраций

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

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 из 15 шагов пройдено 9 из 9 баллов получено

Выберите протокол прикладного уровня

Выберите один вариант из списка

Верно. Так держать!

Верно решили 895 учащихся
Из всех попыток 58% верных

UDP
 TCP
 HTTPS
 IP

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

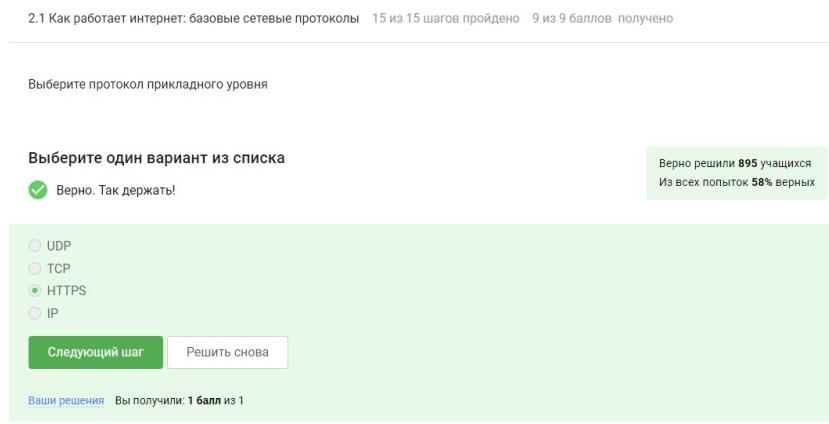


Рис. 2.1: Рис. 1

На каком уровне работает протокол TCP?: транспортном

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

Верно.

Верно решили 939 учащихся
Из всех попыток 61% верных

Транспортном
 Прикладном
 Канальном
 Сетевом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

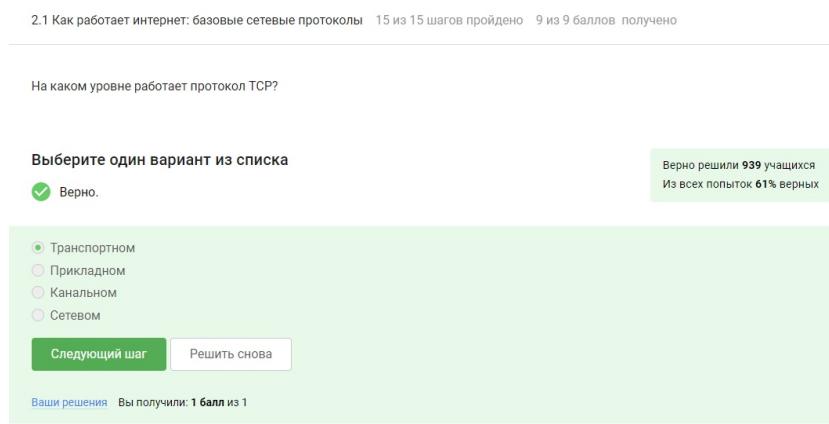


Рис. 2.2: Рис. 2

Выберите все корректные адреса IPv4: 90.11.90.22, 25.198.0.15

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

Выберите все корректные адреса IPv4

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](#).

- 421.0.15.19
- 43.12.256.7
- 90.11.90.22
- 25.198.0.15

[Следующий шаг](#)

[Решить снова](#)

Верно решил 871 учащийся
Из всех попыток 23% верных

Ваши решения Вы получили: 1 балл из 1

Рис. 2.3: Рис. 3

DNS сервер: сопоставляет IP адреса доменным именам

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

DNS сервер

Выберите один вариант из списка

Верно. Так держать!

Верно решили 933 учащихся
Из всех попыток 66% верных

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

[Следующий шаг](#)

[Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

Рис. 2.4: Рис. 4

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

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

Хорошая работа.

Верно решил 941 учащийся
Из всех попыток 53% верных

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Рис. 2.5: Рис. 5

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

Протокол http предполагает

Выберите один вариант из списка

Верно. Так держать!

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 из 1

Следующий шаг >

Рис. 2.6: Рис. 6

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

Протокол https состоит из

Выберите один вариант из списка

✓ Всё получилось!

Верно решили 948 учащихся
Из всех попыток 41% верных

- одной фазы аутентификации сервера
- двух фаз: рукопожатия и передачи данных
- двух фаз: аутентификация клиента и сервера и шифрования данных
- трех фаз: аутентификации клиента, аутентификации сервера, генерация общего ключа

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 59

Ненавижу 11

Шаг 13

Следующий шаг >

Рис. 2.7: Рис. 7

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

Версия протокола TLS определяется

Выберите один вариант из списка

✓ Правильно, молодец!

Верно решили 947 учащихся
Из всех попыток 55% верных

- сервером
- клиентом
- и клиентом, и сервером в процессе “переговоров”
- провайдером клиента

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 59

Ненавижу 11

Шаг 14

Следующий шаг >

Рис. 2.8: Рис. 8

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

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

Хорошая работа.

Верно решил 931 учащийся
Из всех попыток 44% верных

- 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 из 1

 59  11 Шаг 15

[Следующий шаг >](#)

Рис. 2.9: Рис. 9

3 Раздел 2.2

Куки хранят: id сессии, идентификатор пользователя

Куки хранят:

Выберите все подходящие ответы из списка

Хорошая работа.

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](#).

пароль пользователя
 IP адрес
 id сессии
 идентификатор пользователя

Следующий шаг **Решить снова**

Ваши решения Вы получили: 1 балл из 1

Верно решили 856 учащихся
Из всех попыток 18% верных



Рис. 3.1: Рис. 1

Куки не используются для: улучшения надежности соединения

Куки не используются для

Выберите один вариант из списка

Хорошие новости, верно!

Верно решили 950 учащихся
Из всех попыток 53% верных

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

Следующий шаг **Решить снова**

Ваши решения Вы получили: 1 балл из 1

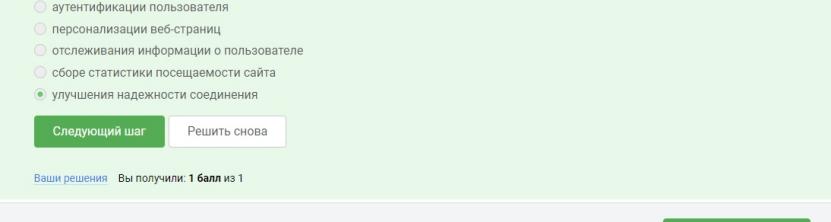


Рис. 3.2: Рис. 2

Куки генерируются: сервером

Куки генерируются

Выберите один вариант из списка

Хорошие новости, верно!

Верно решили 968 учащихся
Из всех попыток 79% верных

сервером
 клиентом

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

👍 22 🗞 11 Шаг 5 Следующий шаг >

Рис. 3.3: Рис. 3

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

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

Так точно!

Верно решили 959 учащихся
Из всех попыток 60% верных

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

👍 22 🗞 11 Шаг 6 Следующий шаг >

Рис. 3.4: Рис. 4

4 Раздел 2.3

Сколько промежуточных узлов в луковой сети TOR? 3

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка

Хорошая работа.

2
 3
 4

Следующий шаг Решить снова

Верно решили 959 учащихся
Из всех попыток 77% верных

Ваши решения Вы получили: 1 балл из 1

28 3 Шаг 3 Следующий шаг >

Рис. 4.1: Рис. 1

IP-адрес получателя известен: отправителю, выходному узлу

IP-адрес получателя известен

Выберите все подходящие ответы из списка

Абсолютно 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](#).

охранному узлу
 промежуточному узлу
 отправителю
 выходному узлу

Следующий шаг Решить снова

Верно решили 906 учащихся
Из всех попыток 19% верных

Ваши решения Вы получили: 1 балл из 1

28 3 Шаг 4 Следующий шаг >

Рис. 4.2: Рис. 2

Отправитель генерирует общий секретный ключ: с охранным, промежуточ-

НЫМ И ВЫХОДНОМ УЗЛОМ

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

Хорошие новости, верно!

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 из 1

Лайк 28 Пинг 3 Шаг 5 [Следующий шаг >](#)

Рис. 4.3: Рис. 3

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

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

Выберите один вариант из списка

Верно.

Нет
 Да

[Следующий шаг](#) [Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

Лайк 28 Пинг 3 Шаг 6 [Следующий шаг >](#)

Комментарии 1 Решение

Рис. 4.4: Рис. 4

5 Раздел 2.4

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

The screenshot shows a question from an online quiz. The question is: "Wi-Fi - это". Below it is a list of options:

- 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

Below the list are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). To the right, a green box displays statistics: "Верно решили 965 учащихся" (965 students answered correctly) and "Из всех попыток 79% верных" (79% of attempts were correct). At the bottom, it says "Ваши решения Вы получили: 1 балл из 1".

Below the main question area, there is a navigation bar with icons for likes (24), dislikes (3), and the step number "Шаг 4". To the right of the navigation bar is another "Следующий шаг" button.

Рис. 5.1: Рис. 1

На каком уровне работает протокол WiFi? Канальном

The screenshot shows a question from an online quiz. The question is: "На каком уровне работает протокол WiFi?". Below it is a list of options:

- Транспортном
- Прикладном
- Канальном
- Сетевом

Below the list are two buttons: "Следующий шаг" (Next step) and "Решить снова" (Solve again). To the right, a green box displays statistics: "Верно решили 972 учащихся" (972 students answered correctly) and "Из всех попыток 58% верных" (58% of attempts were correct). At the bottom, it says "Ваши решения Вы получили: 1 балл из 1".

Below the main question area, there is a navigation bar with icons for likes (24), dislikes (3), and the step number "Шаг 5". To the right of the navigation bar is another "Следующий шаг" button.

Рис. 5.2: Рис. 2

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

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

Всё правильно.

Верно решили 973 учащихся
Из всех попыток 60% верных

WPA
 WEP
 WPA2
 WPA3

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 24 Дизлайк 3 Шаг 6 Следующий шаг >

Рис. 5.3: Рис. 3

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

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

Здорово, всё верно.

Верно решили 975 учащихся
Из всех попыток 53% верных

передаются в зашифрованном виде после аутентификации устройств
 передаются в зашифрованном виде
 передаются в открытом виде
 передаются в открытом виде после аутентификации устройств

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 24 Дизлайк 3 Шаг 7 Следующий шаг >

Рис. 5.4: Рис. 4

Для домашней сети для аутентификации обычно используется метод: WPA2 Personal

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

WPA2 Personal
 WPA2 Enterprise

Правильно, молодец!

Верно решили 975 учащихся
Из всех попыток 87% верных

[Следующий шаг](#) [Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

24 3 Шаг 8 [Следующий шаг >](#)

Рис. 5.5: Рис. 5

6 Раздел 3.1. защита ПК и телефона

Можно ли зашифровать загрузочный сектор диска: да



Рис. 6.1: Рис. 1

Шифрование диска основано на: симметричном шифровании



Рис. 6.2: Рис. 2

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

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

Отлично!

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](#).

Верно решили 906 учащихся
Из всех попыток 28% верных

Wireshark

Disk Utility

BitLocker

VeraCrypt

[Следующий шаг](#)

[Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

Рис. 6.3: Рис. 3

7 Раздел 3.2. Пароли

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

Какие пароли можно отнести с стойким?

Выберите один вариант из списка

✓ Так точно!

- qwerty12345
- ILOVECATS
- UQr9@j4!SS\$
- IDONTLOVECATS

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

23 6 Шаг 4

Где безопасно хранить пароли?

Выберите один вариант из списка

✓ Здорово, всё верно.

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

23 6 Шаг 5

Комментарии Решения

Где безопасно хранить пароли? В менеджерах паролей

Зачем нужна капча? Для защиты от автоматизированных атак, направленных

Зачем нужна капча?

Выберите один вариант из списка

✓ Здорово, всё верно.

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

23 6 Шаг 6

на получение несанкционированного доступа

Следующий

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

Для чего применяется хэширование паролей?

Выберите один вариант из списка

Здорово, всё верно.

Верно решили 954 учащихся
Из всех попыток 61% верных

- Для того, чтобы пароль не передавался в открытом виде.
- Для того, чтобы ускорить процесс авторизации
- Для того, чтобы хранить пароли на сервере в открытом виде.
- Для удобства разработчиков

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 23 Плюс 6 Шаг 7

Следующий шаг >

роли на сервере в открытом виде.

Поможет ли соль для улучшения стойкости паролей к атаке перебором, если

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

Выберите один вариант из списка

Отлично!

Верно решили 954 учащихся

Из всех попыток 61% верных

- Да
- Нет

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 23 Плюс 6 Шаг 8

Следующий шаг >

злоумышленник получил доступ к серверу? Нет

Какие меры защищают от утечек данных атакой перебором?

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

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

Хорошие новости, верно!

Верно решили 874 учащихся

Из всех попыток 16% 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](#).

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

Следующий шаг

Решить снова

Ваши решения Вы получили: 1 балл из 1

Лайк 23 Плюс 6 Шаг 9

Следующий шаг >

- капча

8 Раздел 3.3. Фишинг

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

The screenshot shows a mobile application interface for a quiz. At the top, it says "3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено". Below this is a question: "Какие из следующих ссылок являются фишинговыми?". A green button below the question says "Выберите все подходящие ответы из списка". A green checkmark next to the text "Правильно." indicates the answer is correct. A green box on the right says "Верно решили 836 учащихся из всех попыток 19% верных". Below the question, there is a yellow box containing the following text: "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](#)". A list of five URLs is provided for selection:

- <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, there are two buttons: "Следующий шаг" and "Решить снова". Below these buttons, a message says "Ваши решения Вы получили: 1 балл из 1".

Рис. 8.1: Рис. 1

The screenshot shows a mobile application interface for a quiz. At the top, it says "3.3 Фишинг 5 из 5 шагов пройдено 2 из 2 баллов получено". Below this is a question: "Может ли фишинговый имейл прийти от знакомого адреса?". A green button below the question says "Выберите один вариант из списка". A green checkmark next to the text "Абсолютно точно." indicates the answer is correct. A green box on the right says "Да" and "Нет". Below the question, there is a yellow box containing the following text: "Может ли фишинговый имейл прийти от знакомого адреса? Да". A list of two options is provided for selection:

- Да
- Нет

Below the list, there are two buttons: "Следующий шаг" and "Решить снова". Below these buttons, a message says "Ваши решения Вы получили: 1 балл из 1". At the very bottom, there are two tabs: "Комментарии" and "Решения".

Может ли фишинговый имейл прийти от знакомого адреса? да

9 Раздел 3.3. Вирусы. Примеры

Email Спупинг – это подмена адреса отправителя в имейлах

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

Email Спупинг – это

Выберите один вариант из списка

Верно. Так держать!

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

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

19 2 Шаг 4

Вирус-трокян маскируется под легитимную программу

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

Вирус-трокян

Выберите один вариант из списка

Отлично!

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 из 1

10 Раздел 3.5. Безопасность мессенджеров

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

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

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка

Хорошие новости, верно!

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

[Следующий шаг](#) [Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

17 3 Шаг 3

- при генерации первого сообщения стороной-отправителем

Суть сквозного шифрования состоит в том, что

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

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

Так точно!

Верно решили 889 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 пересифривает сообщения в процессе передачи
 сообщения передаются от отправителя к получателю без участия сервера

[Следующий шаг](#) [Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

17 3 Шаг 4 [Следующий шаг >](#)

11 Раздел 4.1 Введение в криптографию

В асимметричных криптографических примитивах - обе стороны имеют пару

ключей

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

числяется

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



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

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

Верно решили 716 учащихся

Из всех попыток 18% верных

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](#).

[Следующий шаг](#)

[Решить снова](#)

Ваше решение Вы получили 1 балл из 1

16 6 Шаг 5

[Следующий шаг >](#)

Код аутентификации сообщения относится к - симметричным примитивам



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!

Верно решили 820 учащихся

Из всех попыток 69% верных

- симметричным примитивам
- асимметричным примитивам

[Следующий шаг](#)

[Решить снова](#)

Ваше решение Вы получили 1 балл из 1

16 6 Шаг 6

[Следующий шаг >](#)

Комментарии Решений

Обмен ключами Диффи-Хэллмана - это -асимметричный примитив генерации



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

Обмен ключами Диффи-Хэллмана - это

Выберите один вариант из списка

- Отлично!

Верно решили 813 учащихся

Из всех попыток 46% 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](#)

Ваше решение Вы получили 1 балл из 1

16 6 Шаг 7

[Следующий шаг >](#)

общего секретного ключа

12 Раздел 4.2 Цифровая подпись

Протокол электронной цифровой подписи относится к - протоколам с публич-

ным (или открытым) ключом

Алгоритм верификации электронной цифровой подписи требует на вход -

подпись, открытый ключ, сообщение

Электронная цифровая подпись не обеспечивает -конфиденциальность

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
✓ Верно.

Верно решили 773 учащихся
Из всех попыток 44% верных

подпись, открытый ключ
подпись, секретный ключ, сообщение
подпись, секретный ключ
подпись, открытый ключ, сообщение

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

16 3 Шаг 5 Следующий шаг >

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.

Верно решили 774 учащихся
Из всех попыток 51% верных

автентификацию
конфиденциальность
целостность
неотказ от авторства

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

16 3 Шаг 6 Следующий шаг >

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
✓ Хорошая работа.

Верно решили 773 учащихся
Из всех попыток 66% верных

простая
усиленная неквалифицированная
усиленная квалифицированная

Следующий шаг Решить снова

Ваши решения Вы получили: 1 балл из 1

16 3 Шаг 7 Следующий шаг >

Какой тип сертификата электронной подписи понадобится для отправки на-



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

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной

Выберите один вариант из списка

Здорово, всё верно.

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

[Следующий шаг](#) [Решить снова](#)

Ваше решение Вы получили: 1 балл из 1

16 3 Шаг 8

логовой отчетности в ФНС? -усиленная квалифицированная

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



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

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка

Отличное решение!

Верно решили 778 учащихся

Из всех попыток 70% верных

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

[Следующий шаг](#) [Решить снова](#)

Ваши решения Вы получили: 1 балл из 1

[Следующий шаг >](#)

Комментарии Решения

ном) центре

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

13 Раздел 4.3 Электронные платежи

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

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

Так точно!

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

BitCoin
 MasterCard
 SecurePay
 POS-терминал
 банкомат
 МИР

[Следующий шаг](#) [Решить снова](#)

Ваше решение: Вы получили 1 балл из 1

Выберите из списка все платежные системы. - MasterCard - МИР

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

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

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

Правильно, молодец!

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

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

[Следующий шаг](#) [Решить снова](#)

Ваше решение: Вы получили 1 балл из 1

Следующий шаг >

Пальца

13 1 Шаг 4

При онлайн платежах сегодня используется - многофакторная аутентификация

ция покупателя перед банком-эмитентом

The screenshot shows a user interface for an online quiz. At the top, there is a navigation bar with a logo and the text "4.3 Электронные платежи 5 из 5 шагов пройдено 3 из 3 баллов получено". Below this, a message says "При онлайн платежах сегодня используется". A question asks "Выберите один вариант из списка" (Select one option from the list). The correct answer is marked with a green checkmark and the text "Верно. Так держать!". A statistics box indicates "Верно решили 747 участника" (747 participants answered correctly) and "Из всех попыток 58% верных" (58% of all attempts were correct). The list of options includes:

- 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

At the bottom, there are buttons for "Следующий шаг" (Next step) and "Решить снова" (Solve again), along with a progress bar showing "Шаг 5" (Step 5) and "Вы получили: 1 балл из 1" (You received: 1 point out of 1).

14 Раздел 4.4 Блокчейн

Какое свойство криптографической хэш-функции используется в доказательстве работы?

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

✓ Правильно.

Верно решили 761 учащийся
Из всех попыток 47% верных

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

[Следующий шаг](#) [Решить снова](#)

Ваше решение Вы получили: 1 балл из 1

стве работы? - сложность нахождения прообраза

Консенсус в некоторых системах блокчейн обладает свойствами - открытость -

4.4 Блокчейн

6 из 6 шагов пройдено 3 из 3 баллов получено

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

✓ Всё получилось!

Верно решили 682 учащихся
Из всех попыток 22% верных

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

- открытость
- консенсус
- постоянства
- живучесть

[Следующий шаг](#) [Решить снова](#)

Ваше решение Вы получили: 1 балл из 1

консенсус - постоянства - живучесть

Секретные ключи какого криптографического примитива хранят участники

4.4 Блокчейн

6 из 6 шагов пройдено 3 из 3 баллов получено

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

✓ Так точно!

Верно решили 760 учащихся
Из всех попыток 46% верных

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

[Следующий шаг](#) [Решить снова](#)

Ваше решение Вы получили: 1 балл из 1

18 1 Шаг 6

[Следующий шаг](#) >

блокчейна? - цифровая подпись

15 Вывод

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

методам информационной безопасности

