

# Внешний курс. Блок 1

---

Неустроева И.Н.

Российский университет дружбы народов, Москва, Россия

# Информация

---

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов

- Кулябов Дмитрий Сергеевич
- д.ф.-м.н., профессор
- профессор кафедры прикладной информатики и теории вероятностей
- Российский университет дружбы народов

# Вводная часть

---

Выполнить контрольные задания первого блока “Безопасность в сети” внешнего курса “Основы кибербезопасности”.

Интернет-ресурсы

## Основная часть

---



# Как работает интернет: базовые сетевые протоколы Вопрос 2.1.1

Протокол HTTP(S) протокол прикладного уровня, ответ на вопрос 1 - HTTPS

Выберите один вариант из списка



Абсолютно точно.

Верно решили **895** учащихся  
Из всех попыток **58%** верных



UDP



TCP



HTTPS



IP

Следующий шаг

Решить снова

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



98



13

Шаг 7

Следующий шаг >

## Вопрос 2.1.2

На транспортном уровне существует два примера протокола: первый - это TCP, в честь которого названа модель.

g/lesson/666218/step/8?unit=664207

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

## Вопрос 2.1.3

Т.к адрес состоит из большого набора чисел, а именно это 4 или 6 цифр от 0 до 255. В двух вариантах встречаются цифры больше 255, что неверно

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка



Всё правильно.

Верно решил **871** учащихся  
Из всех попыток **23%** 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](#).

- ☐ 421.0.15.19
- ☐ 43.12.256.7
- ☒ 90.11.90.22
- ☒ 25.198.0.15

Следующий шаг

Решить снова

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

## Вопрос 2.1.4

Основная задача DNS это сопоставлять название ( доменное имя, с корректным IP-адресом) с тем, где лежит этот сервер, этот сайт

Выберите один вариант из списка

☒ Правильно, молодец!

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**

 98  13

Шаг 10

Следующий шаг >

## [Вопрос 2.1.5

Классификация протоколов в модели TCP/IP:

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

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка



Хорошие новости, верно!

Верно решил **941** учащийся  
Из всех попыток **53%** верных



сетевой – прикладной – канальный – транспортный

## Вопрос 2.1.6

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

Протокол http предполагает

Выберите один вариант из списка

☒ Так точно!



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**

 98  13

Шаг 12

Следующий шаг >

11/28

## Вопрос 2.1.7

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

Протокол https состоит из

Выберите один вариант из списка

☒ Хорошая работа.

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, аутентификация сервера, генерация общего ключа

Следующий шаг

Решить снова

Ваши решения Вы получили: **1 балл**

## Вопрос 2.1.8

TLS определяется клиентом и сервером, чтобы возможно было подключиться

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

☒ Верно. Так держать!

Верно решил **931** учащихся  
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**



98



13

Шаг 15

Следующий шаг >



## Вопрос 2.1.9

Фаза рукопожатия включает в себя:

- выбор параметров, протоколов
- аутентификация (как минимум, сервера)
- формируется общий секретный ключ K

Следовательно вариант с шифрованием лишний

Куки хранят:

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 решили **856** учащихся  
Из всех попыток **18%** верных

☒ id сессии

## Персонализация сети Вопрос 2.2.1

Куки хранят в себе список параметров и их значений. Этими параметрами могут быть id пользователя, id сессии, тип браузера и некоторые действия пользователей

Куки хранят:

Выберите все подходящие ответы из списка

☒ Прекрасный ответ.

Верно решили 856 учащихся  
Из всех попыток 18% 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](#).

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

Следующий шаг

Решить снова

## Вопрос 2.2.2

### Куки не делают соединение надежным

Куки не используются для

Выберите один вариант из списка



Правильно, молодец!

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**



40



13

Шаг 4

Следующий шаг >

## Вопрос 2.2.3

### Куки генерируются сервером

Куки генерируются

Выберите один вариант из списка



Всё получилось!

Верно решили **968** учащихся  
Из всех попыток **79%** верных

☐ клиентом

☒ сервером

Следующий шаг

Решить снова

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

## Вопрос 2.2.4

### Куки бывают сессионные, удаляются при закрытии окна браузера

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Абсолютно точно.

☐ Нет

☒ Да, на время пользования веб-сайтом

☐ Да, на некоторое время, заданное в сервером


Следующий шаг

Решить снова

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

Верно решили **959** учащихся

Из всех попыток **60%** верных

 40  13

Шаг 6

Следующий шаг >

## Браузер TOR. Анонимизация Вопрос 2.3.1

В луковой модели маршрутизации у нас тоже есть узлы. Они разделяются на охранный узел, промежуточный и выходной. В браузере Tor всегда есть три роутера, их не больше и не меньше

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**

 48  4

Шаг 3

Следующий шаг >

19/28

## Вопрос 2.3.2

IP-адрес не должен быть известен охранному и промежуточному узлам

IP-адрес получателя известен

Выберите все подходящие ответы из списка

☒ Правильно.

Верно решили **906** учащихся  
Из всех попыток **19%** 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](#).

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

Следующий шаг

Решить снова

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

## Вопрос 2.3.3

В анонимных сетях, таких как Tor, общий секретный ключ для сквозного шифрования требует участия всех трех типов узлов: охранного, промежуточного и выходного. Охранный узел сам по себе не обеспечивает генерацию ключа. Каждый узел вносит свой вклад в криптографический протокол (например, Diffie-Hellman), обеспечивая анонимность и защиту от перехвата.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

☒ Отлично!

Верно решили **959** учащихся  
Из всех попыток **55%** верных

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



## Вопрос 2.3.4

Для получения пакетов не нужно использовать TOR. TOR — это технология, которая позволяет с некоторым успехом скрыть личность человека в интернете

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** учащихся

Из всех попыток **74%** верных

☐ Нет

☐ Да

Следующий шаг

Решить снова

Ваши решения Вы получили: **1 балл**

# Беспроводные сети Wi-fi Вопрос 2.4.1

WiFi - это технология беспроводной локальной сети, она основана на стандарте IEEE 802.11

Wi-Fi - это

Выберите один вариант из списка

☒ Всё получилось!

Верно решили **965** учащихся  
Из всех попыток **79%** верных

- ☐ 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**



41



4

Шаг 4

Следующий шаг >

## Вопрос 2.4.1

### WiFi работает на самом нижнем канальном уровне

На каком уровне работает протокол WiFi?

Выберите один вариант из списка

☒ Всё получилось!

Верно решили **972** учащихся  
Из всех попыток **58%** верных

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

Следующий шаг

Решить снова

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

 41  4

Шаг 5

Следующий шаг >

## Вопрос 2.4.1

WEP - устаревший и небезопасный метод шифрования WiFi из-за короткой длины ключа (40 бит), что делает его легко взламываемым. Использовать WEP категорически не рекомендуется

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

☒ Хорошая работа.

Верно решили **973** учащихся  
Из всех попыток **60%** верных

- ☐ WPA
- ☒ WEP
- ☐ WPA2
- ☐ WPA3

Следующий шаг

Решить снова

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

## Вопрос 2.4.1

Безопасность WiFi подразумевает защиту передачи данных между устройством (телефон, компьютер) и роутером (подключенным к интернету), осуществляемую с помощью шифрования и аутентификации

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка



Отлично!

Верно решили **975** учащихся  
Из всех попыток **53%** верных

- ☐ передаются в открытом виде после аутентификации устройств
- ☐ передаются в зашифрованном виде
- ☐ передаются в открытом виде
- ☒ передаются в зашифрованном виде после аутентификации устройств

Следующий шаг

Решить снова

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

## Вопрос 2.4.1

WPA2 Personal предназначен для домашнего использования, а WPA2 Enterprise - для коммерческих организаций.

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка



Верно.

Верно решили 975 учащихся

Из всех попыток 87% верных



WPA2 Personal



WPA2 Enterprise

Следующий шаг

Решить снова

[Ваши решения](#) Вы получили: 1 балл



41



4

Шаг 8

Следующий шаг >

Комментарии

Решения

## Вывод

---

В результате выполнения блока “Безопасность в сети” я узнала, как работают сетевые пратаколы, куки-файлы, сети вайфай и для чего нужен браузер Tor.

...