Отчет по первому этапу внешнего курса

Дисциплина: основы информационнной безопасности

Казазаев Даниил Михайлович

Содержание

# 1 Цель работы

Внешний кур состоит из трех этапов.

# 2 Этап первый

Первый этап курса состоит из 4 частей:

1. Базовые сетевые протоколы
2. Персонализация сети
3. Браузер TOR
4. Беспроводные сети Wi-fi

# 3 Выполнение первого этапа внешнего курса.

## 3.1 Базовые сетевые протоколы

HTTPS является протоколом прикладного уровня. (рис. 1)

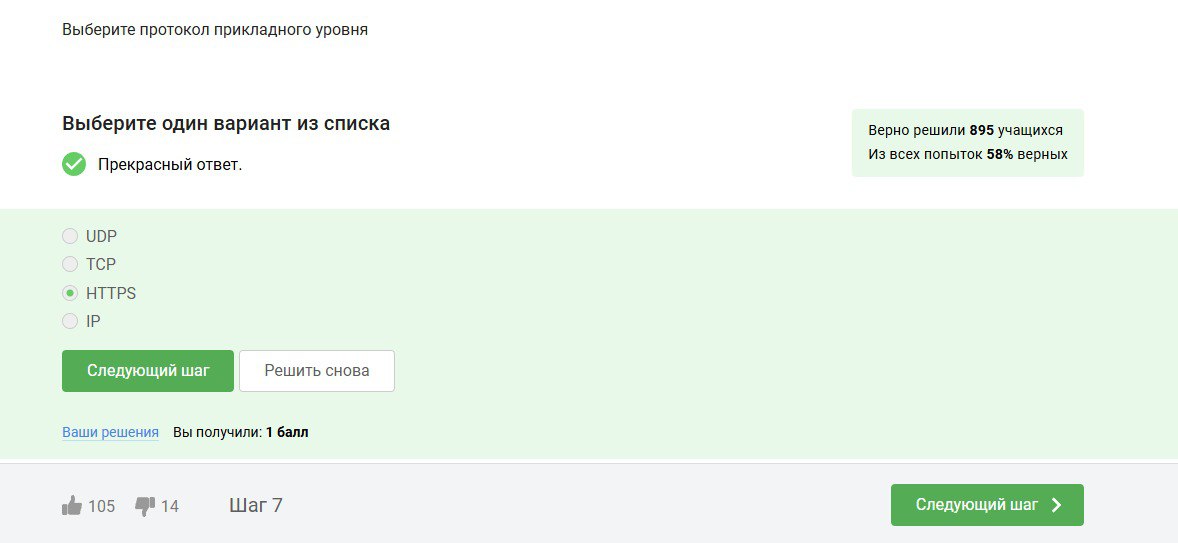


Рис. 1: Первый вопрос

Протокол TCP работает на транспортном уровне. (рис. 2)

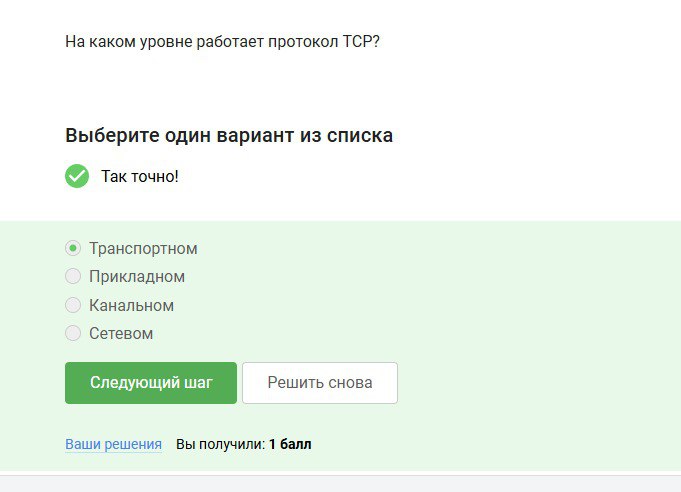


Рис. 2: Второй вопрос

Адреса формата IPv4 состоят из 4-х значений от 0 до 255. (рис. 3)

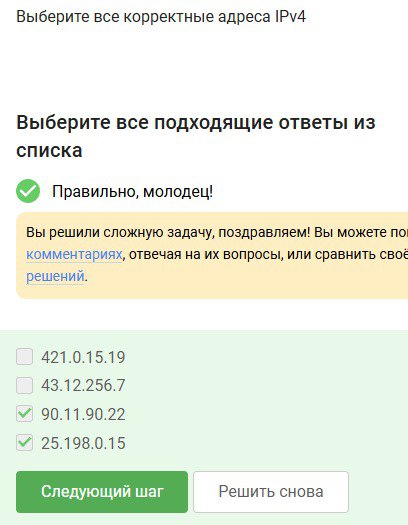


Рис. 3: Третий вопрос

DNS сервера необходимы для сопоставления IP адреса с доменным именем при маршрутизации запроса. (рис. 4)

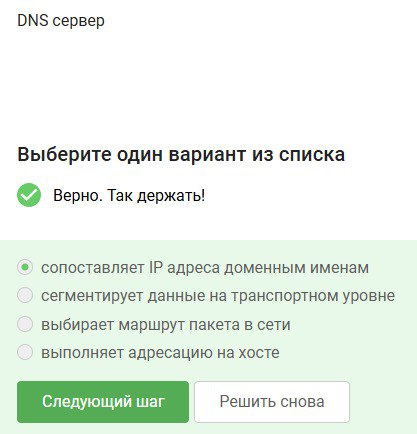


Рис. 4: Четвертый вопрос

Корректная последовательность протоколов в модели TCP/IP. (рис. 5)

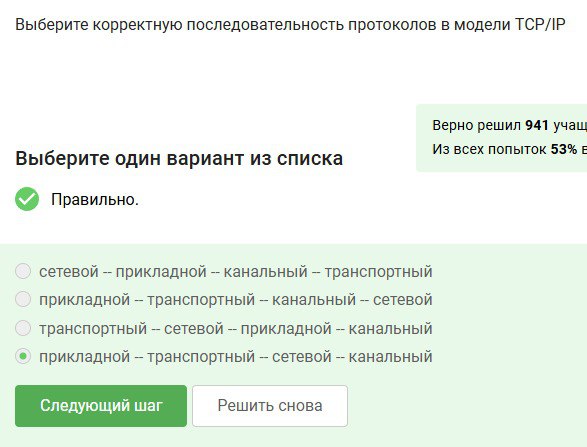


Рис. 5: Пятый вопрос

Так как http это незащищенный протокол, он предполагает передачу данных в открытом виде.(рис. 6)

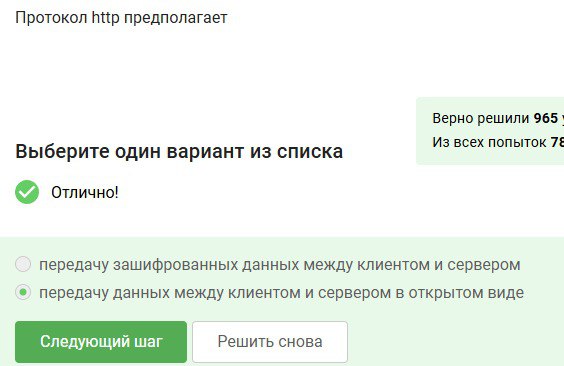


Рис. 6: Шестой вопрос

HTTPS протокол состоит из двух фаз: рукопожатия и передачи данных.(рис. 7)

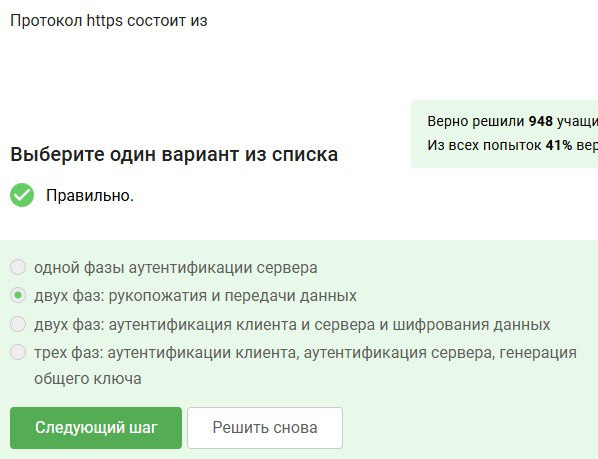


Рис. 7: Седьмой вопрос

Версия протокола TLS определяется как клиентом, так и сервером на стадии “переговоров”.(рис. 8)

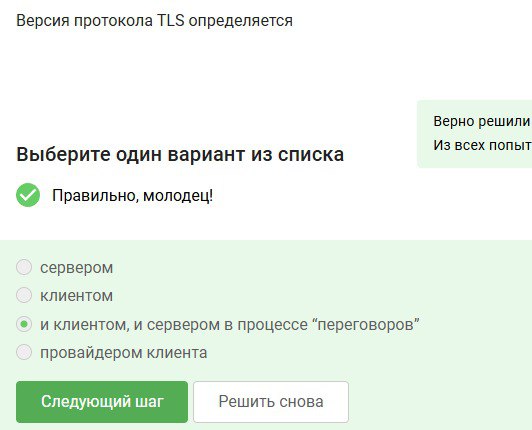


Рис. 8: Восьмой вопрос

На фазе рукопожатия протокола TLS не предусмотрено шифрование данных.(рис. 9)

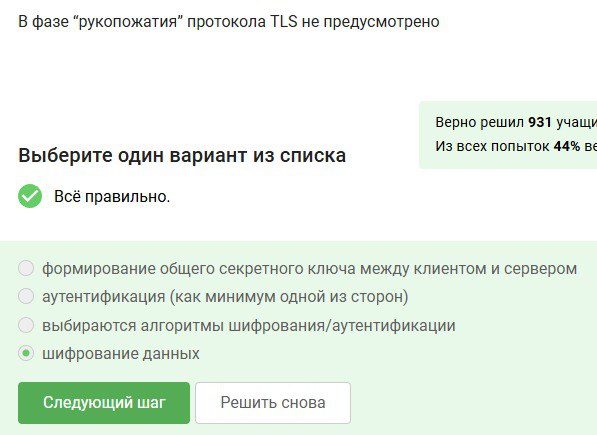


Рис. 9: Девятый вопрос

## 3.2 Персонализация сети

Куки-файлы хранят в себе информацию о идентификаторе пользователя и id сессии.(рис. 10)

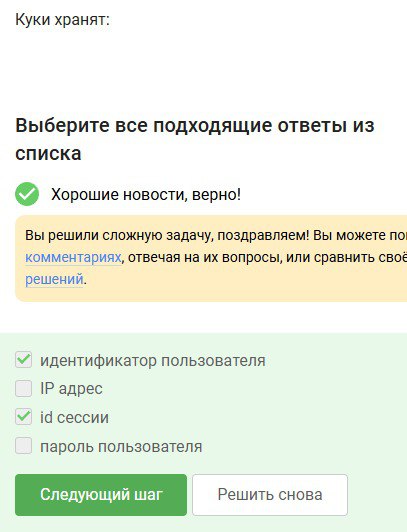


Рис. 10: Первый вопрос

Куки-файлы не используются для улучшения надежности соединения. (рис. 11)

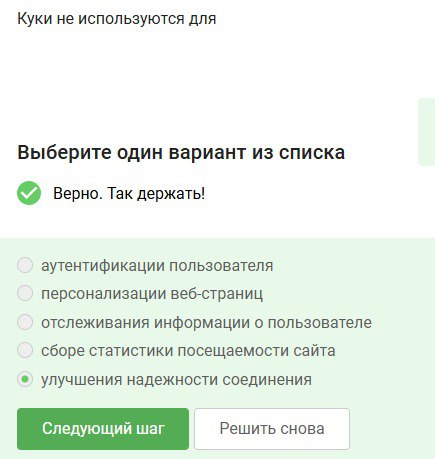


Рис. 11: Второй вопрос

Куки-файлы генерируются сервером. (рис. 12)

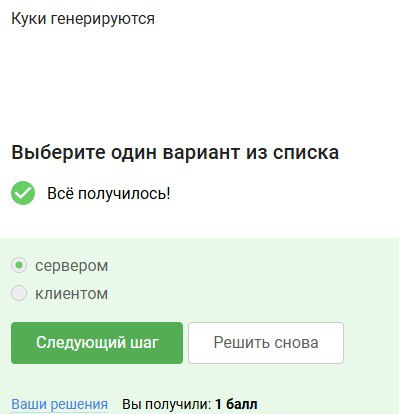


Рис. 12: Третий вопрос

Сессионные куки хранятся в браузере на время пользования им. (рис. 13)

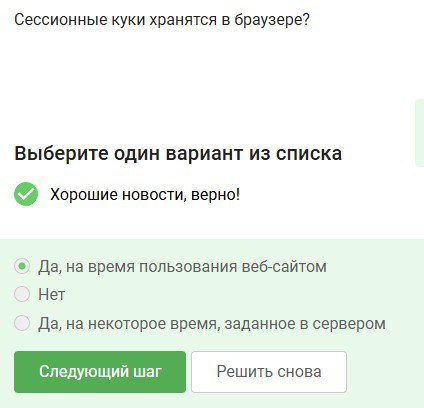


Рис. 13: Четвертый вопрос

# 4 Браузер TOR

В браузере на основе TOR три промежуточных узла: охранный, промежуточный, выходной. (рис. 14)

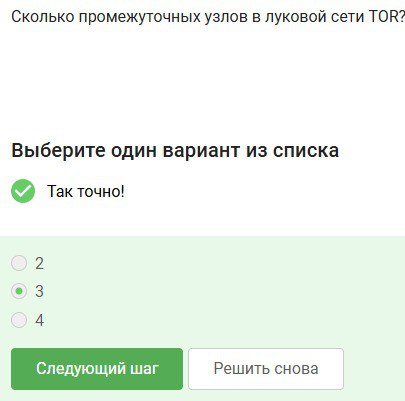


Рис. 14: Первый вопрос

IP-адрес получателя в системе TOR изместен только отправителю и выходному узлу. (рис. 15)

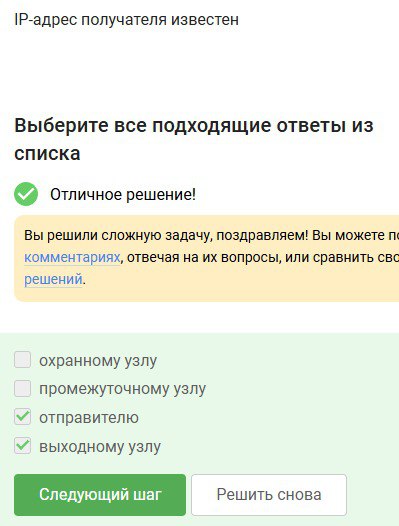


Рис. 15: Второй вопрос

При запросе через TOR отправитель гененирует общий секрутный ключ со всеми узлами. (рис. 16)

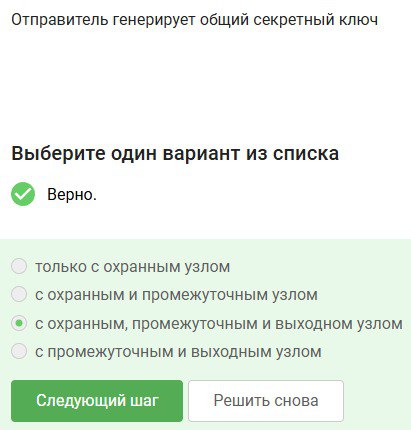


Рис. 16: Третий вопрос

Получатель может использовать любой браузер для принятия запроса из TOR. (рис. 17)

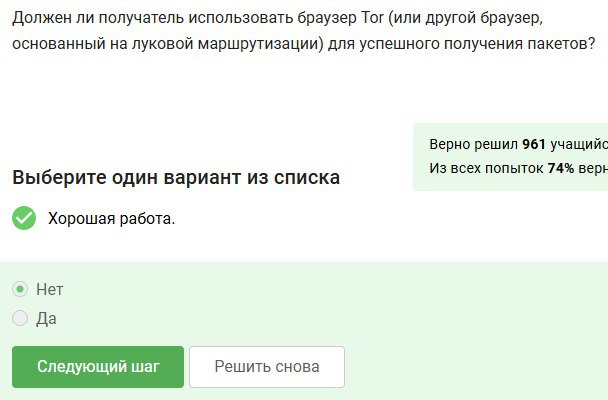


Рис. 17: Четвертый вопрос

# 5 Беспроводные сети Wi-fi

Wf-fi - это … (рис. 18)

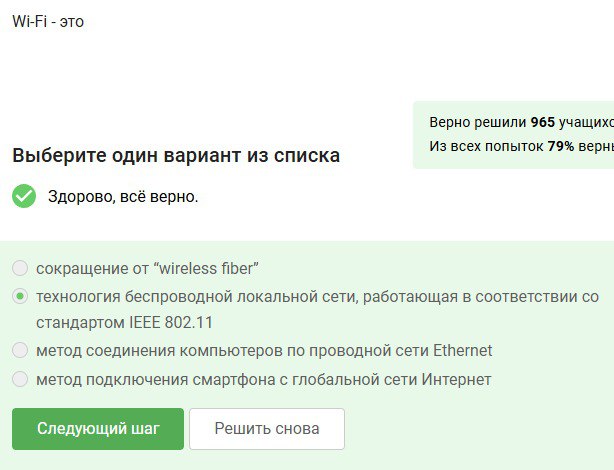


Рис. 18: Первый вопрос

Протоколы Wf-fi работают на канальном уровне. (рис. 19)

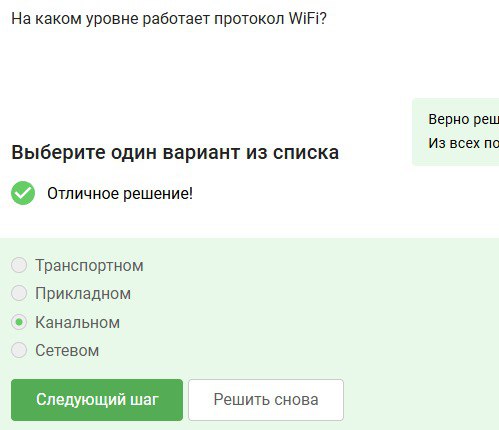


Рис. 19: Второй вопрос

Самой небезопасный метод шифрования и аунтификации Wf-fi это WEP, так как он старый и в нем используется малое кольчество бит для шифрования. (рис. 20)

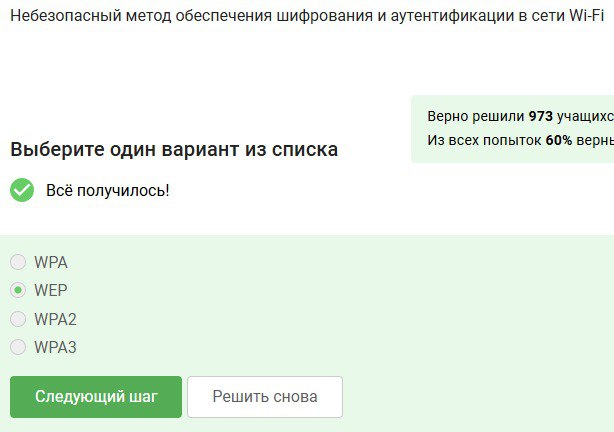


Рис. 20: Третий вопрос

Данные шифруются после аунтификации польователя. (рис. 21)

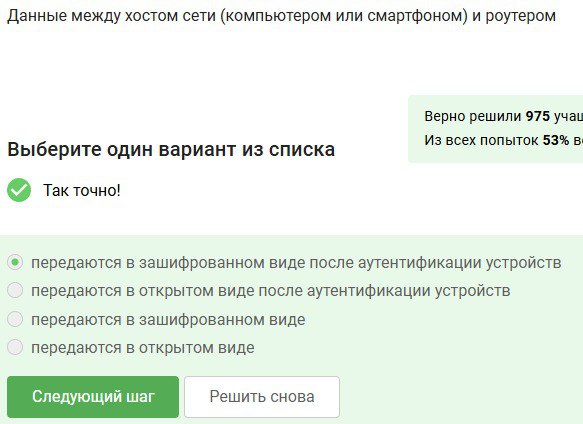


Рис. 21: Четвертый вопрос

Для домашних сетей используется аунтификатор Wi-fi Personal. (рис. 22)

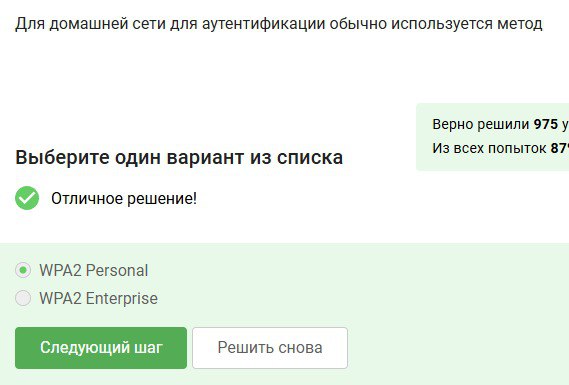


Рис. 22: Пятый вопрос

# 6 Вывод

Выполнен первый этап внешнего курса