

Презентация по выполнению стороннего курса

Информационная безопасность

Арбатова В. П.

12 мая 2025

Российский университет дружбы народов, Москва, Россия

Выполнение заданий

HTTPS - протокол прикладного уровня, выбираю его

Выберите протокол прикладного уровня

Выберите один вариант из списка



Всё правильно.

☐ UDP

☐ TCP

☒ HTTPS

☐ IP

Следующий шаг


Решить снова

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

TCP работает на транспортном уровне

На каком уровне работает протокол TCP?

Выберите один вариант из списка

 **Правильно, молодец!**

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

Следующий шаг


Решить снова

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

Выбираю все корректные номера

Выберите все корректные адреса IPv4

Выберите все подходящие ответы из списка

 **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](#).

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

Следующий шаг Решить снова

Рис. 3: 3

DNS сервер сопоставляет IP адреса доменным именам

DNS сервер

Выберите один вариант из списка



Правильно.

- ☒ 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**

Эта модель работает по такой последовательности, которую я выбрала

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ 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**

Этот протокол передает данные в открытом виде

Протокол http предполагает

Выберите один вариант из списка



Верно.

- ☐ 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**

Так как данные в открытом виде, шифрование не нужно, задачи этого протокола не включают аутентификацию

Протокол https состоит из

Выберите один вариант из списка

☒ Отлично!

- ☐ 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**

Рис. 7: 7

Это происходит с обеих сторон

Версия протокола TLS определяется

Выберите один вариант из списка



Здорово, всё верно.

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

Следующий шаг

Решить снова

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

Этот протокол в фазе рукопожатия не предусматривает шифрование данных

В фазе “рукопожатия” протокола TLS не предусмотрено

Выберите один вариант из списка

☒ Хорошая работа.

- ☐ 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**

Выбираю, что хранят куки

Куки хранят:

Выберите все подходящие ответы из списка

☒ Верно.

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](#).

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

[Следующий шаг](#) [Решить снова](#)

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

Куки никак не связаны с улучшением надежности соединения

Куки не используются для

Выберите один вариант из списка

☒ Хорошая работа.

- ☐ 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**

Клиент не занимается генерацией куки, это делает сервер

Куки генерируются

Выберите один вариант из списка



Правильно, молодец!

☐ клиентом

☒ сервером

Следующий шаг

Решить снова

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

Сессионные куки хранятся в браузере?

Выберите один вариант из списка

☒ Верно. Так держать!

☐ Нет

☐ Да, на некоторое время, заданное в сервером

☒ Да, на время пользования веб-сайтом

Следующий шаг

Решить снова

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

В этой луковой сети 3 промежуточных узла

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка



Абсолютно точно.



2



3



4

Следующий шаг

Решить снова

[Ваши решения](#)

Вы получили: **1 балл**

IP-адрес получателя известен отправителю и выходному узлу

IP-адрес получателя известен

Выберите все подходящие ответы из списка

☒ Здорово, всё верно.

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

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

Следующий шаг

Решить снова

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

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка



Всё получилось!

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

Следующий шаг

Решить снова

Для этого подходит любой браузер, поэтому нет

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

Выберите один вариант из списка

☒ Отличное решение!

☐ Да

☐ Нет

[Следующий шаг](#) [Решить снова](#)

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

Верно решил **961** учащийся
Из всех попыток **74%** верных

Рис. 17: 17

Это определение Wi-Fi

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**

Рис. 18: 18

Это тоже факт

На каком уровне работает протокол WiFi?

Выберите один вариант из списка



Так точно!

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

Следующий шаг

Решить снова

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

Выбираю небезопасный метод

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка

☒ Абсолютно точно.

☐ WPA

☒ WEP

☐ WPA2

☐ WPA3

Следующий шаг

Решить снова

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

Это делается для безопасности

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка



Абсолютно точно.

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

Следующий шаг

Решить снова

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

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка

☒ Правильно.

☐ WPA2 Personal

☐ WPA2 Enterprise

Следующий шаг

Решить снова

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

Это правда

Можно ли зашифровать загрузочный сектор диска

Выберите один вариант из списка



Хорошие новости, верно!



Да



Нет

Следующий шаг

Решить снова

[Ваши решения](#)

Вы получили: **1 балл**

Шифрование диска основано на симметричном шифровании

Шифрование диска основано на

Выберите один вариант из списка



Всё правильно.

- ☐ хэшировании
- ☒ симметричном шифровании
- ☐ асимметричном шифровании

Следующий шаг


Решить снова

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

Выбираю программы для зашифровки жесткого диска

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

 Всё правильно.

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

- ☒ BitLocker
- ☐ Wireshark
- ☐ Disk Utility
- ☒ VeraCrypt

Следующий шаг

Решить снова

Этот пароль можно отнести к стойким, так как он содержит и строчные, и заглавные буквы, цифры, специальные знаки

Какие пароли можно отнести к стойким?

Выберите один вариант из списка



Всё правильно.

- ☐ qwerty12345
- ☐ ILOVECATS
- ☒ UQr9@j4!S\$
- ☐ IDONTLOVECATS

Следующий шаг

Решить снова

Менеджер паролей специально предназначен для безопасного хранения паролей

Где безопасно хранить пароли?

Выберите один вариант из списка



Верно. Так держать!

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

Следующий шаг

Решить снова

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

Выбираю предназначение капчи

Зачем нужна капча?

Выберите один вариант из списка

☒ Отлично!

☐ Она заменяет пароли

☒ Для защиты от автоматизированных атак, направленных на получение несанкционированного доступа

☐ Для защиты кук пользователя

☐ Для безопасного хранения паролей на сервере

[Ваше решение](#) Вы получили: **1 балл**

[Следующий шаг](#) [Решить снова](#)

Верно решено.
Из всех возможных вариантов

Рис. 28: 6

Хэширование нужно, чтобы не хранить пароли на сервере в открытом виде

Для чего применяется хэширование паролей?

Выберите один вариант из списка



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

Это правда

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

Выберите один вариант из списка

☒ Правильно, молодец!

☐ Да

☐ Нет

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

Верно решили **967** учащихся
Из всех попыток **66%** верно

Следующий шаг


Решить снова

Рис. 30: 8

Выбираю все, так как все представленные меры защищают от утечек данных атакой перебором

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка

 Так точно!

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


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

Следующий шаг

Решить снова

Какие из следующих ссылок являются фишинговыми?

Выберите все подходящие ответы из списка

 **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](#).

- ☐ <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

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

Может. Человека могли взломать, он мог ошибиться

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка



Правильно.

☒ Да

☐ Нет

Следующий шаг

Решить снова

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

Email Спуфинг -- это

Выберите один вариант из списка



Здорово, всё верно.

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

Следующий шаг

Решить снова

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

Это определение

Вирус-троян

Выберите один вариант из списка



Верно. Так держать!

- ☐ 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**

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка



Прекрасный ответ.

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

Следующий шаг

Решить снова

Рис. 36: 14

Выбираю суть сквозного шифрования

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка



Отличное решение!

- ☒ 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

Рис. 37: 15

Это факт

В асимметричных криптографических примитивах

Выберите один вариант из списка



Всё правильно.

- ☐ одна сторона имеет только секретный ключ, а другая -- пару из открытого и секретного ключей
- ☐ обе стороны имеют общий секретный ключ
- ☐ одна сторона публикует свой секретный ключ, другая - держит его в секрете
- ☒ обе стороны имеют пару ключей

Следующий шаг

Решить снова

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

Рис. 38: 1

Из всего эта хэш-функция только не обеспечивает конфиденциальность захешированных данных

Криптографическая хэш-функция

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

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](#).

- ☒ дает на выходе фиксированное число бит независимо от объема входных данных
- ☒ стойкая к коллизиям
- ☒ эффективно вычисляется
- ☐ обеспечивает конфиденциальность захешированных данных

[Следующий шаг](#) [Решить снова](#)

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

Первые 2 не относятся

К алгоритмам цифровой подписи относятся

Выберите все подходящие ответы из списка

☒ Верно. Так держать!

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

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

Следующий шаг

Решить снова

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

Код аутентификации сообщения относится к

Выберите один вариант из списка



Здорово, всё верно.



асимметричным примитивам



симметричным примитивам

Следующий шаг

Решить снова

Это определение

Обмен ключам Диффи-Хэллмана - это

Выберите один вариант из списка



Так точно!

- ☐ 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: **1 балл**

Это факт

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Здорово, всё верно.



протоколам с симметричным ключом



протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова

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

Это было сказано в видео

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

☒ Отличное решение!

- ☐ подпись, секретный ключ
- ☐ подпись, открытый ключ
- ☐ подпись, секретный ключ, сообщение
- ☒ подпись, открытый ключ, сообщение

Следующий шаг

Решить снова

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

Правда, ключ открытый, например

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка



Отлично!

- ☒ конфиденциальность
- ☐ неотказ от авторства
- ☐ аутентификацию
- ☐ целостность

Следующий шаг

Решить снова

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

Это требование

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

Выберите один вариант из списка

☒ Хорошая работа.

☐ простая

☐ усиленная неквалифицированная

☐ усиленная квалифицированная

[Ваше решение](#) Вы получили: **1 балл**

Верно р
Из всех

Следующий шаг Решить снова

Рис. 46: 9

Это специализированный центр

В какой организации вы можете получить квалифицированный сертификат ключа проверки электронной подписи?

Выберите один вариант из списка

☒ Правильно, молодец!

☐ в любой организации, имеющей соответствующую лицензию ФСБ

☐ в минкомсвязи РФ

☒ в удостоверяющем (сертификационном) центре

☐ в любой организации по месту работы

[Следующий шаг](#) [Решить снова](#)

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

Верно решил **971** уч.
Из всех попыток **61**

Рис. 47: 10

Все остальное - криптовалюта, методы снятия или пополнения денег со счёта и так далее

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка

✓ Здорово, всё верно.

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](#).

- ☐ BitCoin
- ☒ MasterCard
- ☐ SecurePay
- ☐ POS-терминал
- ☐ банкомат
- ☒ МИР

Следующий шаг

Решить снова

Все остальное не является

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка

☒ Хорошие новости, верно!

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

- ☐ 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

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

Для защиты используется то, что я выбрала

При онлайн платежах сегодня используется

Выберите один вариант из списка

☒ Здорово, всё верно.

- ☐ 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: 13

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка



Хорошие новости, верно!

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

Следующий шаг

Решить снова

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

Рис. 51: 14

Всё выбранные свойства нам подходят

Консенсус в некоторых системах блокчейн обладает свойствами

Выберите все подходящие ответы из списка

☒ Так точно!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным участвуя в конкурсе, или сравнить своё решение с другими на [форуме решений](#)

☒ постоянства

☒ консенсус

☒ открытость

☒ живучесть

Следующий шаг

Решить снова

Ваши решения Вы получили: **1 балл**

Цифровая подпись, которой и был посвящен этот раздел

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

☒ Правильно.

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

[Следующий шаг](#) [Решить снова](#)

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

Рис. 53: 16