

Презентация к внешнему курсу

Презентация

Филиппева К.Д.

17 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Филиппева Ксения Дмитриевна
- Студент
- Российский университет дружбы народов
- 1132230795@pfur.ru

Цель работы

Целью работы является выполнение контрольных заданий первого модуля курса “Основы кибербезопасности” по теме “Безопасность в сети”.

Устройство интернета и сетевые протоколы

HTTPS – это протокол прикладного уровня, который требуется в первом вопросе.

Выберите протокол прикладного уровня

Выберите один вариант из списка



Всё правильно.

- UDP
- TCP
- HTTPS
- IP

Следующий шаг

Видеть ответ

TCP дал название модели.

На каком уровне работает протокол TCP?

Выберите один вариант из списка



Всё получилось!

- Транспортном
- Прикладном
- Канальном
- Сетевом

Следующий шаг

Решить снова

Рис. 2: Вопрос 2.1

IP-адрес должен состоять из 4 или 6 чисел в диапазоне от 0 до 255.

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 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: Вопрос 2.1

DNS-сервер связывает доменное имя с IP-адресом.

DNS сервер

Выберите один вариант из списка

 Правильно, молодец!

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

[Следующий шаг](#) [Решить снова](#)

Рис. 4: Вопрос 2.1

Протоколы по уровням TCP/IP.

Выберите корректную последовательность протоколов в модели TCP/IP

Выберите один вариант из списка



Абсолютно точно.

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

Следующий шаг

Решить снова

Рис. 5: Вопрос 2.1

HTTP не шифрует данные, в отличие от HTTPS.

Протокол http предполагает

Выберите один вариант из списка



Правильно, молодец!

- передачу зашифрованных данных между клиентом и сервером
- передачу данных между клиентом и сервером в открытом виде

[Следующий шаг](#)

[Решить снова](#)

Рис. 6: Вопрос 2.1

TLS настраивается клиентом и сервером.

Протокол https состоит из

Выберите один вариант из списка

 Верно. Так держать!

- 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](#)

Рис. 7: Вопрос 2.1

Установление соединения по TLS требует согласования.

Версия протокола TLS определяется

Выберите один вариант из списка



Хорошая работа.



сервером



клиентом



и клиентом, и сервером в процессе "переговоров"



провайдером клиента

Следующий шаг

Решить снова

Рис. 8: Вопрос 2.1

Фаза TLS-рукопожатия включает выбор алгоритма, проверку, создание ключа.

В фазе "рукопожатия" протокола TLS не предусмотрено

Выберите один вариант из списка

 Так 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](#)

Рис. 9: Вопрос 2.1

Идентификация через куки

Куки-файлы содержат параметры сессии.

Куки хранят:

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](#).

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

Следующий шаг

Решить снова

Рис. 10: Вопрос 2.2

Куки не обеспечивают безопасную передачу данных.

Куки не используются для

Выберите один вариант из списка



Так точно!

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

Следующий шаг

Решить снова

Рис. 11: Вопрос 2.2

Сервер формирует куки и передаёт их клиенту.

Куки генерируются

Выберите один вариант из списка



Верно. Так держать!



клиентом



сервером

Следующий шаг

Решить снова

Рис. 12: Вопрос 2.2

Сессионные куки удаляются при закрытии браузера.

Сессионные куки хранятся в браузере?

Выберите один вариант из списка



Всё правильно.

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

Следующий шаг

Решить снова

Рис. 13: Вопрос 2.2

Анонимность в сети через TOR

Маршрутизация в Tor включает три узла: охранный, промежуточный, выходной.

Сколько промежуточных узлов в луковой сети TOR?

Выберите один вариант из списка



Хорошие новости, верно!

2

3

4

Следующий шаг

Решить снова

IP скрыт от охранного и промежуточного узлов.

IP-адрес получателя известен

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](#).

- охранному узлу
- промежуточному узлу
- отправителю
- выходному узлу

Следующий шаг

Решить снова

Рис. 15: Вопрос 2.3

Tor использует три узла для формирования общего ключа шифрования.

Отправитель генерирует общий секретный ключ

Выберите один вариант из списка

Абсолютно точно.

только с охранным узлом
 с охранным и промежуточным узлом
 с охранным, промежуточным и выходном узлом
 с промежуточным и выходным узлом

[Следующий шаг](#) [Решить снова](#)

Рис. 16: Вопрос 2.3

Tor используется для маскировки личности.

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

Выберите один вариант из списка

Правильно, молодец!

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

Да
 Нет

[Следующий шаг](#) [Решить снова](#)

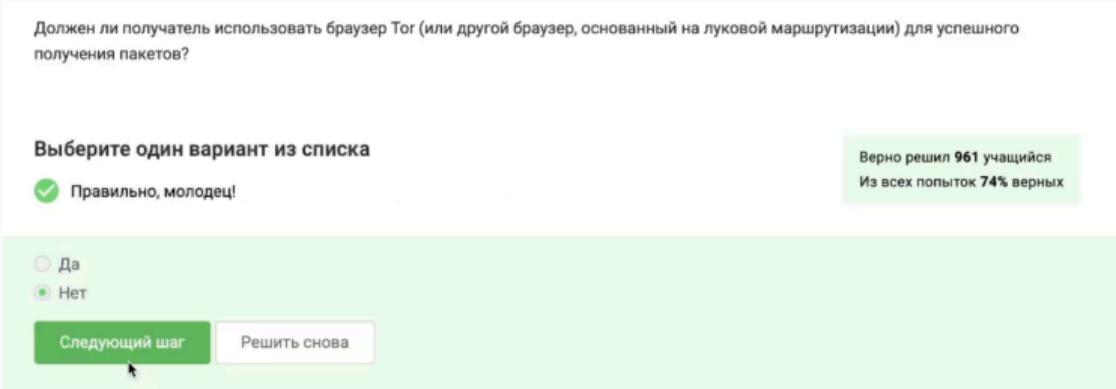


Рис. 17: Вопрос 2.3

Wi-Fi и его защита

Wi-Fi – это технология по стандарту IEEE 802.11.

Wi-Fi - это

Выберите один вариант из списка

Так точно!

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

Рис. 18: Вопрос 2.4

Он функционирует на канальном уровне.

На каком уровне работает протокол WiFi?

Выберите один вариант из списка



Верно.

- Транспортном
- Прикладном
- Канальном
- Сетевом

Следующий шаг

Решить снова

WEP устарел и уязвим.

Небезопасный метод обеспечения шифрования и аутентификации в сети Wi-Fi

Выберите один вариант из списка



Так точно!

- WPA
- WEP
- WPA2
- WPA3

Следующий шаг

Решить снова

Рис. 20: Вопрос 2.4

Шифрование Wi-Fi защищает соединение.

Данные между хостом сети (компьютером или смартфоном) и роутером

Выберите один вариант из списка

Здорово, всё верно.

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

Следующий шаг

Решить снова

Рис. 21: Вопрос 2.4

WPA2 Personal — для дома, Enterprise — для компаний.

Для домашней сети для аутентификации обычно используется метод

Выберите один вариант из списка



Хорошие новости, верно!



WPA2 Personal



WPA2 Enterprise

Следующий шаг

Решить снова

Рис. 22: Вопрос 2.4

Шифрование диска

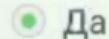
Рекомендуется защищать основной раздел и загрузочную область.

Можно ли зашифровать загрузочный сектор диска

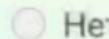
Выберите один вариант из списка



Всё получилось!



Да



Нет

Следующий шаг

Решить снова



Используется симметричное шифрование.

Шифрование диска основано на

Выберите один вариант из списка



Отличное решение!

- хэшировании
- симметричном шифровании
- асимметричном шифровании

Следующий шаг

Решить снова

Рис. 24: Вопрос 3.1

Есть встроенные средства и альтернативы с открытым кодом.

С помощью каких программ можно зашифровать жесткий диск?

Выберите все подходящие ответы из списка

Всё получилось!

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](#).

- Wireshark
- BitLocker
- Disk Utility
- VeraCrypt

[Следующий шаг](#)

[Решить снова](#)

Рис. 25: Вопрос 3.1

Безопасные пароли

Надёжный пароль содержит буквы, цифры, символы.

Какие пароли можно отнести к стойким?

Выберите один вариант из списка



Абсолютно точно.

- qwertty12345
- ILOVECATS
- UQr9@j4!S\$
- IDONTLOVECATS

Пароли хранятся в менеджерах, не в мессенджерах.

Где безопасно хранить пароли?

Выберите один вариант из списка



Хорошая работа.

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

Следующий шаг

Решить снова

CAPTCHA отличает человека от робота.

Зачем нужна капча?

Выберите один вариант из списка

Здорово, всё верно.

Вер

Из

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

Следующий шаг

Решить снова

Рис. 28: Вопрос 3.2

Пароли хранятся в виде хэшей.

Для чего применяется хэширование паролей?

Выберите один вариант из списка



Правильно, молодец!

- 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

Рис. 29: Вопрос 3.2

Соль усиливает защиту пароля.

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

Выберите один вариант из списка

Верно.

Верно решили **967** учащихся

Из всех попыток **66%** верны

- Да
 Нет

Следующий шаг

Решить снова

Рис. 30: Вопрос 3.2

Рекомендуется использовать длинные и сложные пароли.

Какие меры защищают от утечек данных атакой перебором?

Выберите все подходящие ответы из списка



Абсолютно точно.

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [коммейтингах](#), 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

Фишинг

Фишинговые сайты маскируются под настоящие.

Какие из следующих ссылок являются фишинговыми?

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](#).

- <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: Вопрос 3.3

Фишинг может прийти с адреса знакомого.

Может ли фишинговый имейл прийти от знакомого адреса?

Выберите один вариант из списка



Верно.



Да



Нет

Следующий шаг

Решить снова

Рис. 33: Вопрос 3.3

Вредоносные программы

Спуфинг — подделка адреса отправителя.

Email Спуфинг -- это

Выберите один вариант из списка



Отличное решение!

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

Трояны маскируются под обычное ПО.

Вирус-троян

Выберите один вариант из списка

 Так точно!

- обязательно шифрует данные и вымогает ключ дешифрования
- маскируется под легитимную программу
- работает исключительно под ОС Windows
- разработан греками

Следующий шаг

Решить снова

Рис. 35: Вопрос 3.4

Шифрование в мессенджерах

При первом сообщении создаётся ключ.

На каком этапе формируется ключ шифрования в протоколе мессенджеров Signal?

Выберите один вариант из списка



Правильно.

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

Следующий шаг

Решить снова

Рис. 36: Вопрос 3.5

Сквозное шифрование скрывает переписку от сервера.

Суть сквозного шифрования состоит в том, что

Выберите один вариант из списка



Абсолютно точно.

- 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: Вопрос 3.5

Основы криптографии

Асимметричное шифрование: публичный и приватный ключи.

В асимметричных криптографических примитивах

Выберите один вариант из списка



Прекрасный ответ.

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

Следующий шаг

Решить снова

Рис. 38: Вопрос 4.1

Хэш-функции преобразуют данные в строку фиксированной длины.

Криптографическая хэш-функция

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](#).

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

Следующий шаг

Решить снова

Рис. 39: Вопрос 4.1

MAC использует общий ключ.

Код аутентификации сообщения относится к

Выберите один вариант из списка



Верно. Так держать!

- симметричным примитивам
- асимметричным примитивам

Следующий шаг

Решить снова

Диффи-Хеллман — для обмена ключами.

Обмен ключами Диффи-Хэллмана - это

Выберите один вариант из списка



Отличное решение!

- 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

Электронная подпись

ЭЦП использует криптографию с открытым ключом.

Протокол электронной цифровой подписи относится к

Выберите один вариант из списка



Хорошая работа.



протоколам с симметричным ключом



протоколам с публичным (или открытым) ключом

Следующий шаг

Решить снова



Верификация включает обновление, подпись, открытый ключ.

Алгоритм верификации электронной цифровой подписи требует на вход

Выберите один вариант из списка

 Хорошая работа.

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

[Следующий шаг](#)

[Решить снова](#)

Рис. 44: Вопрос 4.2

Подпись обеспечивает целостность, личность и неотказуемость.

Электронная цифровая подпись не обеспечивает

Выберите один вариант из списка



Отличное решение!

- конфиденциальность
- аутентификацию
- неотказ от авторства
- целостность

Следующий шаг

Решить снова

УКЭП приравнивается к обычной подписи.

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

Выберите один вариант из списка

 Хорошие новости, верно!

- простая
- усиленная квалифицированная
- усиленная неквалифицированная

Следующий шаг

Решить снова

Рис. 46: Вопрос 4.2

Сертификат заверяется подписью УЦ.

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

Выберите один вариант из списка

 Отличное решение!

Верно реши
Из всех поп

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

Следующий шаг

Решить снова

Рис. 47: Вопрос 4.2

Платёжные системы

Популярные системы: Visa, MasterCard, МИР.

Выберите из списка все платежные системы.

Выберите все подходящие ответы из списка



Абсолютно точно.

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

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

Факторы идентификации: знание, устройство, биометрия, местоположение.

Примером многофакторной аутентификации является

Выберите все подходящие ответы из списка



Правильно, молодец!

Вы решили сложную задачу, поздравляем! Вы можете помочь остальным учащимся в [коих](#) вопросах, или сравнить своё 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

Онлайн-платежи используют MFA.

При онлайн платежах сегодня используется

Выберите один вариант из списка



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

Рис. 50: Вопрос 4.3

Proof-of-Work — валидация через вычисления.

Какое свойство криптографической хэш-функции используется в доказательстве работы?

Выберите один вариант из списка



Отличное решение!

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

Следующий шаг

Решить снова

Рис. 51: Вопрос 4.4

Свойства блокчейна: неизменяемость, согласованность, доступность, открытость.

Консенсус в некоторых системах блокчейн обладает свойствами

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](#).

- живучесть
- постоянства
- консенсус
- открытость

[Следующий шаг](#)

[Решить снова](#)

Рис. 52: Вопрос 4.4

Участники подписывают транзакции закрытым ключом.

Секретные ключи какого криптографического примитива хранят участники блокчейна?

Выберите один вариант из списка

Абсолютно точно.

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

[Следующий шаг](#)

[Решить снова](#)

Рис. 53: Вопрос 4.4

Общий результат

Финальный результат



X

Поздравляем!

Вы завершили курс «Основы кибербезопасности».

Вы набрали **53 балла из 53**, изучив 100% материалов курса.

Сертификат в нём не выдаётся, но вы можете поделиться своим результатом в соцсетях.



<https://stepik.org/course/111512>

☆ Оставить отзыв

Найти новый курс