Имя: _____ **Дата:** _____ **Баллы:** _____

Что такое VPN
Рабочий лист

Практические упражнения по сетевым протоколам, туннелированию и средствам контроля безопасности.

ОБЗОР ОБУЧЕНИЯ ПО VPN

ОБУЧАЮЩИЙСЯ
СТАТУС СТУДЕНТА
Направление «Защитник сети»

БЕЗОПАСНЫЙ
СОСТОЯНИЕ ПОДКЛЮЧЕНИЯ
Защита пакетов данных

АКТИВНО
ЗАЩИТА ОТ УТЕЧЕК
Защита от утечек DNS и IPv6

Добро пожаловать! Этот пакет заданий проведёт вас через основные принципы виртуальных частных сетей (VPN). Вы изучите то, как зашифрованные туннели защищают ваши данные, как работают сетевые протоколы и как выявлять и устранять утечки конфиденциальности.

КОНТРОЛЬНЫЕ ТОЧКИ РАБОЧЕГО ЛИСТА

- [ ] **Части 1-4: освойте понятия и протоколы VPN.**
- [ ] **Части 5-7: решите кроссворд и головоломки «поиск слов».**
- [ ] **Части 8-9: решите кейсы и задание с шифром.**
- [ ] **Часть 10: изучите страницы часто задаваемых вопросов (базовый и продвинутый уровень).**
- [ ] **Часть 11: изучите 10 интересных фактов из реальной жизни.**
- [ ] **Дополнительно: задание «Думай быстро».**

Открыть руководство VPN.com по VPN

URL: https://www.vpn.com/ru/vpn/

Ваша дорожная карта обучения: VPN

- Объясните понятие туннелирования данных и инкапсуляции.
- Определите стандартные конфигурации протоколов и методы шифрования.
- Проанализируйте роль серверов и маскировки IP-адресов в виртуальных частных сетях.
- Разберитесь, как провайдеры отслеживают просмотр сайтов и как VPN этому мешает.
- Различайте операционные границы топологии виртуальной сети.

ИНСТРУКЦИИ К РУКОВОДСТВУ «ЧТО ТАКОЕ VPN»

Ответьте на вопросы с выбором ответа и вопросы «верно/неверно», дополните предложения с пропусками, используя банк слов, сопоставьте определения и решите кроссворд и головоломку «поиск слов». Примените свои знания по теме: реальным сценариям из раздела кейсов. Завершите работу дополнительным заданием «Думай быстро».

ЧТО ТАКОЕ VPN? (ВВЕДЕНИЕ)

Виртуальная частная сеть — это не просто переключатель конфиденциальности. Это зашифрованный туннель, который направляет ваш интернет-трафик через удалённый сервер. Он скрывает ваш IP-адрес, не позволяет провайдеру вести журналы ваших действий в сети и защищает данные в общедоступных сетях. Понимание терминологии необходимо для цифровой безопасности.

ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ КАЖДУЮ КОНТРОЛЬНУЮ ТОЧКУ И ВЫБЕРИТЕ ИЛИ НАПИШИТЕ ПРАВИЛЬНЫЙ ОТВЕТ.

Контрольная точка 1: Задание с выбором ответа

1. Какова основная функция виртуальной частной сети (VPN)?

- A. Чтобы повысить скорость отрисовки в интернет-браузере
- B. Чтобы шифровать пакеты данных и скрывать ваш публичный IP
- C. Чтобы хранить базы данных cookie-файлов сайта локально
- D. Чтобы заменить физическое оборудование вашего компьютера

2. Что такое сетевое туннелирование в контексте VPN?

- A. Удаление дублирующихся сетевых файлов журналов
- B. Установка локальных файлов хранилища баз данных
- C. Обмен файлами с другими локальными компьютерами
- D. Инкапсуляция одного сетевого пакета внутри другого защищённого пакета

3. Какой стандарт шифрования широко используется для защиты VPN-трафика?

- A. Устаревшее шифрование DES
- B. Современный стандарт AES-256
- C. Кодирование base64 открытым текстом
- D. Стандартный шифр rot13

4. Какая часть вашего сетевого трафика шифруется VPN?

- A. Только задания печати по сети локального устройства
- B. Физический маршрут прокладки кабеля Ethernet
- C. Вся полезная нагрузка сетевого пакета
- D. Только история поиска в вашем веб-браузере

5. Что означает термин «шифрование» в сетевых технологиях?

- A. Преобразование открытых данных в нечитаемый шифртекст
- B. Удаление старых записей переписки
- C. Повышение ограничений скорости вашей локальной сети
- D. Публичный обмен ключами доступа к базе данных

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. VPN шифрует ваш трафик, чтобы предотвратить перехват в локальной сети в общедоступном Wi-Fi.

○ Верно ○ Неверно

7 Вопрос 7

7. VPN физически изменяет аппаратную конфигурацию вашего роутера.

○ Верно ○ Неверно

8 Вопрос 8

8. Протоколы туннелирования помещают пакеты данных в зашифрованный транспортный уровень.

○ Верно ○ Неверно

9 Вопрос 9

9. Симметричное шифрование использует один и тот же ключ для шифрования и расшифровки трафика.

○ Верно ○ Неверно

10 Вопрос 10

10. Использование VPN делает ваше интернет-соединение физически неуязвимым для любых отключений электричества.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

Прочитайте каждое предложение ниже и вставьте пропущенный термин из банка слов.

1. Чтобы защитить ваш трафик, VPN упаковывает пакеты данных внутрь другого протокола; этот процесс называется _____ .

2. Если при просмотре потокового видео скорость загрузки низкая, причиной может быть ограниченная сетевая _____ пропускания.

3. Ограничение для пользователей из других стран у потокового сервиса, доступного только в одной стране, называется _____ .

4. Правила подключения, определяющие параметры шифрования и соединения, называются _____ VPN.

5. Ваш компьютер использует локальный _____ для мониторинга сетевого трафика и блокировки небезопасных соединений.

6. При подключении к VPN ваши данные идут через удалённый _____ , который скрывает ваш публичный IP.

СЛОВАРНЫЙ БАНК СЛОВ

БРАНДМАУЭР ГЕОБЛОКИРОВКА ПОЛОСА ПРИВАТНОСТЬ ПРОВАЙДЕР
ПРОТОКОЛ СЕРВЕР ТУННЕЛИРОВАНИЕ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление сетевых понятий

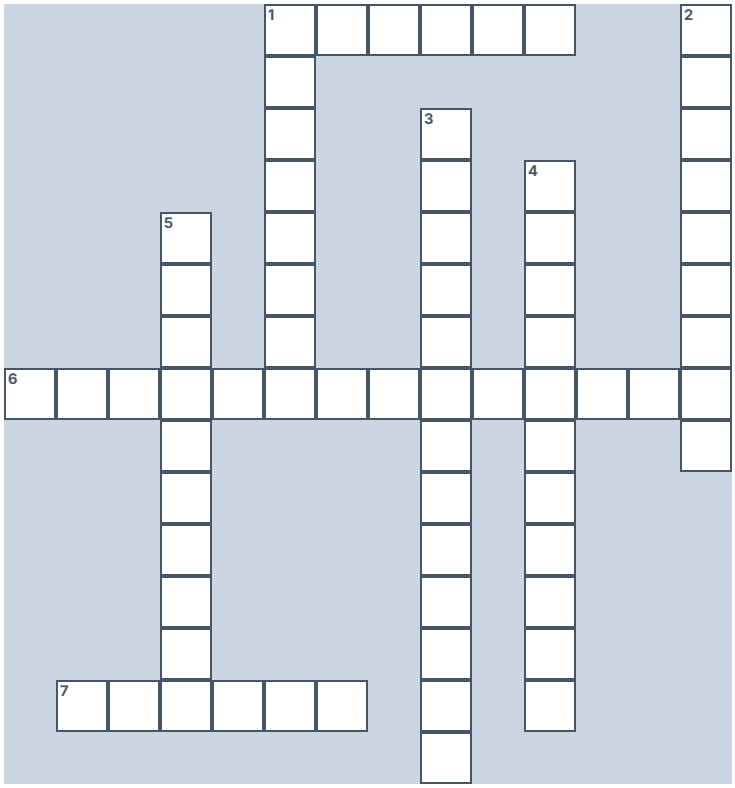
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

Сопоставьте каждый термин слева с правильным определением справа, введя соответствующую букву (A–H) в заполняемое поле.

☐	1. Туннелирование	A	Удалённый компьютер, который маршрутизирует ваш трафик и скрывает ваш IP-адрес.
☐	2. Протокол	B	Интернет-провайдер, который передаёт ваш трафик и может видеть незашифрованную активность.
☐	3. Пропускная способность	C	Ограничение, не допускающее доступ к сайтам в зависимости от физического местоположения.
☐	4. Сервер	D	Система безопасности, отслеживающая и блокирующая несанкционированный трафик.
☐	5. Геоблокировка	E	Набор правил, определяющих, как данные передаются по сети.
☐	6. Межсетевой экран	F	Состояние свободы от слежки и публичного наблюдения.
☐	7. Конфиденциальность	G	Максимальная скорость передачи данных по соединению.
☐	8. Провайдер	H	Упаковка пакетов данных в другой пакет для безопасной передачи.

Контрольная точка 5: Кроссворд

Решите кроссворд, вводя буквы в активные белые клетки. Номера соответствуют подсказкам ниже.



ПО ГОРИЗОНТАЛИ

1. Максимальная скорость передачи данных по соединению (6)

6. Упаковка пакетов данных внутрь другого пакета для безопасной передачи (14)

7. Удалённый компьютер, который маршрутизирует ваш трафик и скрывает ваш IP (6)

ПО ВЕРТИКАЛИ

1. Набор правил, определяющих, как данные передаются по сети (8)

2. Интернет-провайдер, который записывает ваш трафик, если он не зашифрован (9)

3. Ограничение, не позволяющее открыть сайт в зависимости от физического местоположения (13)

4. Состояние свободы от слежки или публичного наблюдения (11)

5. Система безопасности, которая следит за трафиком и блокирует несанкционированный (10)

Контрольная точка 5, альтернативный вариант: Доступные подсказки к кроссворду

Пользователи программ чтения с экрана и клавиатуры могут вводить ответы на кроссворд прямо в текстовые поля ниже.

ПО ГОРИЗОНТАЛИ

1 по горизонтали: Максимальная скорость передачи данных по соединению (6 букв):

6 по горизонтали: Упаковка пакетов данных внутрь другого пакета для безопасной передачи (14 букв):

7 по горизонтали: Удалённый компьютер, который маршрутизирует ваш трафик и скрывает ваш IP (6 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Набор правил, определяющих, как данные передаются по сети (8 букв):

2 по вертикали: Интернет-провайдер, который записывает ваш трафик, если он не зашифрован (9 букв):

3 по вертикали: Ограничение, не позволяющее открыть сайт в зависимости от физического местоположения (13 букв):

4 по вертикали: Состояние свободы от слежки или публичного наблюдения (11 букв):

5 по вертикали: Система безопасности, которая следит за трафиком и блокирует несанкционированный (10 букв):

Контрольная точка 6: Поиск скрытых слов

Найдите в сетке ниже 8 ключевых терминов. Слова могут идти по горизонтали, по вертикали или по диагонали.

А	Н	Ч	Ц	Ы	Х	Я	Е	Й	Ж	Ц	Г	А	О	У
К	В	Р	Э	У	А	М	Д	Н	А	Р	Б	Я	П	П
В	П	М	Ъ	С	Е	Р	В	Е	Р	Х	Щ	О	Р	А
О	Ц	Ь	М	П	П	И	Й	Р	Й	Х	Л	О	З	Н
Р	Ч	О	Х	Ь	Й	В	Щ	Ж	Э	О	Т	С	Ю	Ь
И	Ц	Й	Ш	Ь	А	У	Щ	Р	С	О	С	Ю	Т	К
К	У	Ч	Й	Т	Ъ	Ш	Т	А	К	Щ	Ш	М	А	Е
О	Т	П	Н	Б	С	Ъ	З	О	И	У	Ф	Ь	Ю	Л
Л	М	Щ	Л	Ю	Ы	Э	Л	Т	М	К	Я	К	Л	Р
Б	А	Е	Р	Е	Д	Й	А	В	О	Р	П	К	Б	Ч
О	Т	У	Н	Н	Е	Л	И	Р	О	В	А	Н	И	Е
Е	А	Л	Ж	Ы	Е	М	Я	М	Е	Н	Ф	Р	Л	А
Г	З	П	Р	И	В	А	Т	Н	О	С	Т	Ь	Т	М
С	Г	Р	В	Д	И	К	Б	Б	Т	Х	О	У	Ы	Ш
К	Ю	З	Ю	Ц	И	Э	Ы	Й	Ж	Х	Ш	С	Щ	М

СПИСОК СЛОВ СЛОВАРЯ

ТУННЕЛИРОВАНИЕ ПРОТОКОЛ ПОЛОСА СЕРВЕР ГЕОБЛОКИРОВКА
БРАНДМАУЭР ПРИВАТНОСТЬ ПРОВАЙДЕР

Контрольная точка 6, альтернативный вариант: Доступное сопоставление терминов

Сопоставьте каждый из 8 терминов из поиска слов с правильным определением, написав букву (A–H) на пустой строке.

ТЕРМИНЫ СЛОВАРЯ

A. ТУННЕЛИРОВАНИЕ

B. ПРОТОКОЛ

C. ПОЛОСА

D. СЕРВЕР

E. ГЕОБЛОКИРОВКА

F. БРАНДМАУЭР

G. ПРИВАТНОСТЬ

H. ПРОВАЙДЕР

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

1. Набор правил, определяющих, как данные передаются по сети.
2. Ограничение, не позволяющее открыть сайт в зависимости от физического местоположения.
3. Система безопасности, которая следит за трафиком и блокирует несанкционированный.
4. Состояние свободы от слежки или публичного наблюдения.
5. Интернет-провайдер, который записывает ваш трафик, если он не зашифрован.
6. Упаковка пакетов данных внутрь другого пакета для безопасной передачи.
7. Удалённый компьютер, который маршрутизирует ваш трафик и скрывает ваш IP.
8. Максимальная скорость передачи данных по соединению.

Контрольная точка 7: Задание с перепутанными словами

Расставьте буквы ниже в правильном порядке, чтобы получить ключевые понятия и термины VPN. Запишите ответы в заполняемые поля.

1. **АЛРВИНУОНТИЕЕН** _____
2. **АПЛСОО** _____
3. **ЕГИОРКАОКЛОВБ** _____
4. **НТЬТИАСОПРВ** _____
5. **ОКРЛТПОО** _____
6. **ЕВСРРЕ** _____
7. **РНБАМУЭРДА** _____
8. **РАЕПВРЙДО** _____

Дополнительное задание: Думай быстро

ПО 3 ОТВЕТА В КАЖДОЙ КАТЕГОРИИ. ПОБЕЖДАЕТ ТОТ, КТО ПЕРВЫМ ЗАПОЛНИТ СПИСОК.

1	То, что может раскрыть IP-адрес			
2	Мифы о VPN			
3	То, что передаётся по интернету			
4	Обещания, которые даёт хороший VPN-провайдер			
5	Секреты, которые вы зашифровали бы			
6	От чего VPN не может вас защитить			
7	Способы распознать поддельную сеть Wi-Fi			
8	Слова, связанные с конфиденциальностью			
9	Устройства, которые могут использовать VPN			
10	То, что происходит при нажатии «Подключить»			
11	Места, где вы пользовались бы VPN			
12	Причины использовать VPN в путешествии			
13	Предметы из реальной жизни, похожие на туннель			
14	Слова из этого рабочего листа, которые вы хотите запомнить			
15	Слова, чтобы объяснить VPN ребёнку			

Контрольная точка 8: Кейсы по VPN

Примените изученные понятия к реальным ситуациям ниже.

САРА (СТУДЕНТКА В КАФЕ)

👩‍💻 “Привет! Я сижу в Coffee & Bytes. Здесь есть незащищённая общедоступная сеть «Free_Wi-Fi_No_Password». Я хочу войти в школьную почту и загрузить задание, но боюсь хакеров. Какие риски у использования этой сети без VPN и как VPN защищает мои данные?”

АЛЕКС (СТУДЕНТ-ПУТЕШЕСТВЕННИК)

👩‍💻 “Ой! Я в поездке за границей по проекту и пытаюсь посмотреть биологический документальный фильм, размещённый на сервере в моей стране. Но сайт пишет «Это видео недоступно в вашем текущем местоположении». Почему меня блокируют и как VPN поможет посмотреть его?”

Контрольная точка 9: Расшифруйте шифр

VPN шифрует ваш трафик, чтобы защитить его. Используйте ключ «буква–число» ниже, чтобы расшифровать сообщение по кибербезопасности, вписав соответствующие буквы в пустые места.

КЛЮЧ ШИФРОВАНИЯ «БУКВА В ЧИСЛО»

А=1 Б=2 В=3 Г=4 Д=5 Е=6 Ё=7 Ж=8 З=9 И=10 Й=11
К=12 Л=13 М=14 Н=15 О=16 П=17 Р=18 С=19 Т=20 У=21 Ф=22
Х=23 Ц=24 Ч=25 Ш=26 Щ=27 Ъ=28 Ы=29 Ь=30 Э=31 Ю=32 Я=33

9	1	27	10	20	10	20	6		17	18	10	3	1	20	15	16	19	20	30

19		9	1	27	10	27	7	15	15	29	14		20	21	15	15	6	13	6	14

Расшифрованное сообщение:

СОВЕТ: КАЖДОЕ ЧИСЛО ОБОЗНАЧАЕТ ПОЗИЦИЮ ЭТОЙ БУКВЫ В АЛФАВИТЕ (НАПРИМЕР, 1 = А, 2 = Б, 33 = Я).

Контрольная точка 10: Базовые вопросы о VPN (Часть A)

Просмотрите самые частые вопросы и ответы потенциальных клиентов об использовании виртуальных частных сетей.

Q1: Что такое VPN и как он работает?

Виртуальная частная сеть (VPN) шифрует ваше интернет-соединение и направляет трафик через защищённый удалённый сервер. Это скрывает ваш публичный IP-адрес и ограничивает то, что наблюдатели в локальной сети и ваш провайдер могут узнать о трафике, проходящем через VPN-туннель.

Q2: Зачем мне использовать VPN?

VPN защищает вашу цифровую конфиденциальность, обеспечивает безопасность подключения в общедоступных сетях Wi-Fi (например, в кафе или аэропортах), может снижать замедление по типу активности, если провайдер не может определить тип зашифрованного трафика, обходит геоограничения для доступа к мировому контенту и помогает защитить ресурсы удалённой работы.

Q3: Делает ли VPN меня полностью анонимным в интернете?

Нет. Хотя VPN скрывает ваш IP-адрес и шифрует трафик, вас всё равно можно отследить через cookie браузера, активные аккаунты (например, Google или Facebook), цифровой отпечаток браузера или если ваш VPN-провайдер ведёт журналы ваших данных.

Q4: Замедлит ли VPN скорость моего интернета?

Да, незначительно. Процесс шифрования и физическое расстояние до VPN-сервера добавляют задержку и накладные расходы. Влияние зависит от провайдера, протокола, удалённости сервера, устройства и условий сети.

Q5: Законно ли использовать VPN?

Использование VPN легально во многих странах, но в некоторых юрисдикциях услуги VPN ограничивают, регулируют или блокируют. Перед использованием проверьте действующие местные законы. Подробнее см. в руководствах по законности на VPN.com.

Контрольная точка 10: Базовые вопросы о VPN (Часть B)

Просмотрите самые частые вопросы и ответы потенциальных клиентов об использовании виртуальных частных сетей.

Q6: Можно ли пользоваться бесплатным VPN?

Бесплатные VPN могут опираться на рекламу, ограниченные функции, аналитику использования, лимиты данных или другие модели монетизации. Перед использованием пользователям следует изучить политику конфиденциальности провайдера, его владельцев, аудиты и бизнес-модель.

Q7: Что такое политика «no-logs» (без журналов)?

Политика отсутствия журналов описывает, какие данные об активности и подключениях провайдер, по его заявлению, не хранит. Точный объём различается, поэтому читателям стоит изучить политику и результаты независимых аудитов.

Q8: Как выбрать лучший VPN?

Ищите проверенные аудитом политики отсутствия журналов, надёжные протоколы (WireGuard, OpenVPN), безопасные расположения серверов, высокую скорость, серверы только на ОЗУ, функцию kill switch и юрисдикцию вне альянсов обмена разведданными (например, 5/9/14 глаз).

Q9: Можно ли использовать VPN на телефоне и смарт-телевизоре?

Да. Современные VPN-провайдеры предлагают отдельные приложения для iOS, Android, macOS, Windows, Linux и смарт-телевизоров, а также настройки для роутеров, защищающие все устройства в вашей домашней сети.

Q10: Что такое Kill Switch?

Kill Switch — это функция безопасности, которая автоматически отключает ваше устройство от интернета при обрыве VPN-соединения. Это предотвращает утечку ваших незашифрованных данных или реального IP-адреса.

Контрольная точка 10: Продвинутые вопросы о VPN (Часть C)

Изучите технические и структурные аспекты виртуальных частных сетей и защищённых протоколов туннелирования.

Q1: В чём разница между WireGuard, OpenVPN и IKEv2?

WireGuard — современный лёгкий протокол (всего около 4000 строк кода), обеспечивающий высокую скорость и быстрое подключение. OpenVPN — очень безопасный, проверенный временем протокол с открытым исходным кодом. IKEv2 отлично подходит для мобильных устройств благодаря способности быстро переподключаться при смене сети. [4]

Q2: Что такое двойной VPN или маршрутизация Multi-Hop?

Multi-Hop направляет ваш трафик последовательно через два или более VPN-сервера. Это добавляет второй уровень шифрования и помогает скрыть ваш настоящий IP-адрес от второго узла, если один из серверов будет скомпрометирован.

Q3: Что такое утечка WebRTC и как VPN её предотвращает?

WebRTC — это браузерный протокол, который может раскрыть ваши настоящие локальный и публичный IP-адреса, даже если VPN активен. Премиальные VPN блокируют или подменяют запросы WebRTC в своих приложениях для компьютеров и смартфонов и в расширениях для браузеров.

Q4: Что такое серверы, работающие только в оперативной памяти, и почему они важны?

Обычные серверы записывают данные на жёсткие диски, которые могут быть изъяты или скомпрометированы. Серверы только на RAM (без дисков) работают целиком в энергозависимой памяти (RAM). При перезагрузке или выключении сервера данные в памяти стираются.

Q5: Как обфускация обходит блокировки VPN?

Обфускация (или «скрытый VPN») маскирует VPN-трафик так, что он выглядит как обычный HTTPS-трафик (порт 443). Это может помочь обойти глубокую проверку пакетов (DPI), которую используют правительства или школьные и офисные сети для блокировки VPN.

Контрольная точка 10: Продвинутые вопросы о VPN (Часть D)

Изучите технические и структурные аспекты виртуальных частных сетей и защищённых протоколов туннелирования.

Q6: Что такое раздельное туннелирование и когда его следует использовать?

Раздельное туннелирование позволяет выбрать, какие приложения передают трафик через зашифрованный туннель VPN, а какие подключаются к интернету напрямую. Используйте его, чтобы направлять банковские приложения через VPN, а локальные игры подключать напрямую и избегать задержки, добавляемой VPN.

Q7: Как работает прямая секретность (Perfect Forward Secrecy)?

PFS гарантирует, что для каждого сеанса создаётся уникальный временный ключ шифрования. Даже если закрытый ключ будет скомпрометирован в будущем, его нельзя использовать для расшифровки прошлых или будущих сеансов, поскольку в них применялись независимые ключи.

Q8: Что такое альянсы 5/9/14 Eyes и почему это важно?

Юрисдикция может влиять на правовой процесс, с которым может столкнуться провайдер, но практический риск для конфиденциальности зависит также от того, какие данные провайдер хранит, его технической архитектуры, владельцев, отчётов о прозрачности и истории аудитов.

Q9: Что такое защита от утечек DNS?

Защита от утечек DNS заставляет ваше устройство отправлять запросы на поиск сайтов (DNS-запросы) через частные зашифрованные DNS-серверы VPN, а не через серверы вашего провайдера. Это не позволяет провайдеру отслеживать, какие сайты вы посещаете.

Q10: Может ли VPN обойти ограничение скорости интернета провайдером?

Иногда. VPN может помочь, если провайдер выборочно замедляет определённые виды активности, но он не устранит перегрузку, лимиты трафика, ограничения скорости на уровне аккаунта или плохое качество сети.

Часть 11: 10 интересных фактов о VPN и выводов из реальной практики

Ознакомьтесь с этими очень ценными реальными фактами и сведениями об истории, рынке и технологиях VPN.

1. ПЕРВЫЙ VPN-ПРОТОКОЛ

PPTP (Point-to-Point Tunneling Protocol) был разработан группой производителей, включая Microsoft, и опубликован как RFC 2637 в июле 1999 года для поддержки VPN удалённого доступа. [6]

2. РЫНОЧНАЯ ОЦЕНКА

Мировой рынок VPN быстро растёт на фоне увеличения потребности в удалённой работе и требований корпоративной безопасности.

3. РЕВОЛЮЦИЯ WIREGUARD

У WireGuard очень компактная кодовая база, рассчитанная на эффективность, поэтому её проще проверять на уязвимости безопасности, чем традиционные протоколы. [4]

4. СТРОГИЕ СТАНДАРТЫ АУДИТА

Ведущие VPN-провайдеры нанимают внешних аудиторов (например, Cure53 или PwC) для независимых проверок кода и подтверждения того, что они не ведут журналов активности пользователей.

5. ПРОИСХОЖДЕНИЕ АЛЬЯНСА 5 EYES

Альянс «Пять глаз» вырос из соглашения UKUSA 1946 года о радиотехнической разведке между США и Великобританией, к которому позже присоединились Канада, Австралия и Новая Зеландия.

6. ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ

Глубокая инспекция пакетов (DPI) изучает содержимое пакетов и характер трафика, а не только заголовки, и некоторые брандмауэры используют её для обнаружения и блокировки распространённых VPN-протоколов.

7. КОРПОРАТИВНОЕ ИСПОЛЬЗОВАНИЕ

Значительная доля сотрудников предприятий по всему миру использует защищённые VPN для входа во внутренние базы данных, что делает это ключевым стандартом безопасности.

8. ДЕЦЕНТРАЛИЗОВАННЫЕ VPN

Децентрализованные VPN (dVPN) распределяют трафик по сети узлов, которыми управляют сами участники, что снижает зависимость от единого централизованного провайдера.

9. АНОНИМНОСТЬ: TOR И VPN

VPN направляет трафик через одного провайдера, а Tor (The Onion Router) пропускает трафик через три добровольных ретранслятора (входной, промежуточный и выходной), так что ни один из них не знает обоих концов соединения.

10. СТОИМОСТЬ УТЕЧЕК ДАННЫХ

Использование модели безопасного доступа с нулевым доверием вместе с VPN помогает организациям защищать интеллектуальную собственность и смягчать финансовые последствия утечек данных.

Технические ссылки и источники

Цитируемые публикации, криптографические спецификации и официальные стандарты документов, использованные в этом рабочем листе.

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[2] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[3] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[4] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

Ответы: рабочий лист «Что такое VPN»

1 **Основная функция** ПРОТОКОЛЫ — **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Главная задача VPN — создать зашифрованный туннель, защищающий полезную нагрузку пакетов и скрывающий публичный IP-адрес пользователя. Источник: IETF Tunnel RFC.

2 **Сетевое туннелирование** ЗАДЕРЖКА — **Правильный ответ: D**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Протоколы туннелирования инкапсулируют исходные пакеты данных во внешние пакеты-носители, чтобы безопасно проходить через общедоступные сети. Источник: IETF Tunnel RFC.

3 **Вопрос 3** — **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой стандарт шифрования широко используется для защиты VPN-трафика? → Современный стандарт AES-256

4 **Зашифрованные компоненты** УПРАВЛЕНИЕ МАРШРУТИЗАЦИЕЙ — **Правильный ответ: C**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN шифрует всю полезную нагрузку IP-пакетов, сохраняя содержимое передачи конфиденциальным. Источник: IETF Tunnel RFC.

5 **Вопрос 5** — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Шифрование использует алгоритм и ключ, чтобы превратить открытый текст в нечитаемый шифртекст.

Ответы: контрольная точка 2 – верно или неверно

6 **Блокировка перехвата** МАСКИРОВКА IP — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Зашифрованные туннели делают полезную нагрузку пакетов нечитаемой для тех, кто перехватывает данные в локальных сетях Wi-Fi. Источник: Deloitte Advisory.

7 **Изменения оборудования** СКОРОСТИ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN — это программные сетевые туннели, которые физически не меняют оборудование вашего шлюзового маршрутизатора. Источник: Cure53 Audit.

8 **Туннелирование пакетов** РИСК ПЕРЕХВАТА — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Туннелирование работает за счёт упаковки исходных сетевых пакетов в транспортные заголовки на время передачи. Источник: IETF Tunnel RFC.

9 **Симметричные ключи** БРАНДМАУЭРЫ — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Симметричная криптография использует общий ключ как для шифрования, так и для расшифровки сетевых потоков. Источник: WireGuard Project.

10 **Иммунитет к нагрузке** БЕЗ ЖУРНАЛОВ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN шифрует только сигналы активного соединения; он не может предотвратить сбои сервиса, вызванные локальными отключениями электричества. Источник: EDRi Retention Guidelines.

Ключи к словарю и критерии оценивания

Критерии оценивания для преподавателя: ставьте 1 балл за каждое верное сопоставление (всего 8 баллов) и за каждый контекстный термин (всего 6 баллов).

КОНТРОЛЬНАЯ ТОЧКА 4: ОТВЕТЫ – СОПОСТАВЛЕНИЕ ПОНЯТИЙ

H 1. Туннелирование	E 2. Протокол	G 3. Пропускная способность	A 4. Сервер
C 5. Геоблокировка	D 6. Межсетевой экран	F 7. Конфиденциальность	B 8. Провайдер

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ТУННЕЛИРОВАНИЕ	2 ПОЛОСА	3 ГЕОБЛОКИРОВКА	4 ПРОТОКОЛ
5 БРАНДМАУЭР	6 СЕРВЕР		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 B – ПРОТОКОЛ	2 E – ГЕОБЛОКИРОВКА	3 F – БРАНДМАУЭР	4 G – ПРИВАТНОСТЬ
5 H – ПРОВАЙДЕР	6 A – ТУННЕЛИРОВАНИЕ	7 D – СЕРВЕР	8 C – ПОЛОСА

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

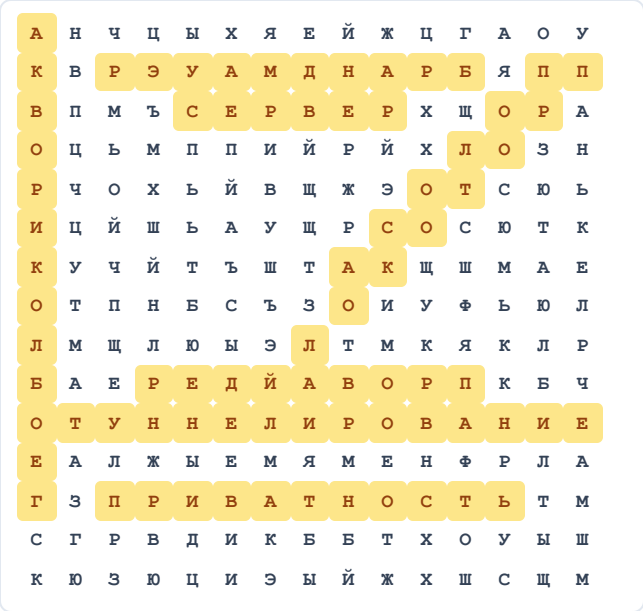
Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить Туннелирование, Протокол и Пропускная способность и привести пример для каждого термина.

Кейсы:
Попросите учащихся обосновывать свои рекомендации фактами из рабочего листа, а не мнениями.

Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ



РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

1 по горизонтали: ПОЛОСА Максимальная скорость передачи данных по соединению (6 букв)

6 по горизонтали: ТУННЕЛИРОВАНИЕ Упаковка пакетов данных внутрь другого пакета для безопасной передачи (14 букв)

7 по горизонтали: СЕРВЕР Удалённый компьютер, который маршрутизирует ваш трафик и скрывает ваш IP (6 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ПРОТОКОЛ Набор правил, определяющих, как данные передаются по сети (8 букв)

2 по вертикали: ПРОВАЙДЕР Интернет-провайдер, который записывает ваш трафик, если он не зашифрован (9 букв)

3 по вертикали: ГЕОБЛОКИРОВКА Ограничение, не позволяющее открыть сайт в зависимости от физического местоположения (13 букв)

4 по вертикали: ПРИВАТНОСТЬ Состояние свободы от слежки или публичного наблюдения (11 букв)

5 по вертикали: БРАНДМАУЭР Система безопасности, которая следит за трафиком и блокирует несанкционированный (10 букв)

Ключ к словам-перевёртышам и шифру

Ключ для проверки заданий на расшифровку слов и «Секретного шифра».

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. АЛРВИНУОНТИЕЕН — **ТУННЕЛИРОВАНИЕ**
2. АПЛСОО — **ПОЛОСА**
3. ЕГИОРКАОКЛОВБ — **ГЕОБЛОКИРОВКА**
4. НТЬТИАСОПРВ — **ПРИВАТНОСТЬ**
5. ОКРЛТПОО — **ПРОТОКОЛ**
6. ЕВСРРЕ — **СЕРВЕР**
7. РНБАМУЭРДА — **БРАНДМАУЭР**
8. РАЕПВРЙДО — **ПРОВАЙДЕР**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЗАЩИТИТЕ ПРИВАТНОСТЬ С ЗАЩИЩЁННЫМ ТУННЕЛЕМ"

Ответы к кейсам

A Ситуация A: безопасность общедоступной сети

ПЕРЕХВАТ И ШИФРОВАНИЕ | Дилемма Сары

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Риски: перехват пакетов, перехват данных и атаки «человек посередине». Кто-то в той же сети кафе мог бы перехватить её данные для входа или файл с домашним заданием.
- Защита VPN: шифрует полезную нагрузку сетевых пакетов, делая перехваченный трафик туннеля нечитаемым для пассивных наблюдателей в локальной сети при правильной настройке VPN.

B Ситуация B: доступ к заблокированным ресурсам

ГЕОБЛОКИРОВКА И IP | Дилемма Алекса

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Почему заблокировано: стриминговый хост использует геоблокировку, которая сопоставляет локальный IP-адрес путешественника с его физической страной и блокирует его по территориальным лицензиям.
- Чем помогает VPN: скрывает его реальное местоположение, направляя трафик через сервер в его родной стране. Сайт видит IP-адрес родной страны, и доступ разрешается.