Имя: _____ Дата: _____ Баллы: _____

Прокси и VPN Рабочий лист

Сравнение прокси-серверов и виртуальных частных сетей, различий в шифровании и маршрутизации на уровне приложения и всей системы

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

- Сравните прикладные прокси с общесистемным шифрованием VPN.
- Определите возможности SOCKS5 по сравнению с обычными HTTP-прокси.
- Проанализируйте, как браузерные прокси оставляют фоновые приложения незащищёнными.
- Разберитесь, как провайдеры записывают незашифрованный трафик в прокси-туннелях.
- Выберите подходящий инструмент маршрутизации с учётом требований к скорости и безопасности.

ИНСТРУКЦИИ К РАБОЧЕМУ ЛИСТУ ПО СРАВНЕНИЮ ПРОКСИ

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: сравнению прокси и VPN. Завершите работу дополнительным заданием «Думай быстро».

ПРОКСИ И VPN (ВВЕДЕНИЕ)

Прокси и VPN выполняют разные функции цифровой конфиденциальности. Прокси-сервер работает как перенаправление на уровне приложений и скрывает ваш IP-адрес для отдельных программ без шифрования данных. VPN работает на сетевом уровне и защищает шифрованием весь системный трафик. Выбор подходящего средства зависит от ваших требований к безопасности.

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

Контрольная точка 1: Задание с выбором ответа

1 **1. На каком уровне модели OSI работает обычный HTTP-прокси?**

- A. Физический уровень
- B. Сетевой уровень
- C. Прикладной уровень
- D. Канальный уровень

2 **2. В чём главное преимущество протокола SOCKS5 перед стандартными HTTP-прокси?**

- A. Принудительно включает полное шифрование полезной нагрузки
- B. Он преобразует доменное имя в числовой IP-адрес
- C. Защищён от утечек DNS
- D. Работает непосредственно в пространстве ядра

3 **3. Почему VPN, как правило, безопаснее прокси-сервера?**

- A. Работает на более быстром удалённом оборудовании
- B. Он шифрует весь сетевой трафик в масштабах системы
- C. Не требует локальных таблиц маршрутизации
- D. Полностью устраняет сетевую задержку

4 **4. Какой тип прокси по умолчанию перенаправляет трафик без какого-либо шифрования?**

- A. Базовый HTTP-прокси
- B. Зашифрованный HTTPS-прокси
- C. Защищённый клиент WireGuard
- D. Обфусцированный VPN-сервер

5 **5. Что происходит с фоновым трафиком приложений при использовании прокси в браузере?**

- A. Шифруется автоматически
- B. Он блокируется прокси-сервером
- C. Направляется через прокси-туннель
- D. Обходит прокси и раскрывает ваш IP

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Прокси SOCKS5 шифрует всю полезную нагрузку пакетов, проходящих через сервер.

○ Верно ○ Неверно

7 Вопрос 7

7. VPN работает на сетевом уровне, защищая весь системный трафик.

○ Верно ○ Неверно

8 Вопрос 8

8. Прокси, как правило, быстрее VPN, потому что выполняют глубокое шифрование пакетов.

○ Верно ○ Неверно

9 Вопрос 9

9. Настройка прокси требует настройки перенаправления трафика внутри определённых приложений.

○ Верно ○ Неверно

10 Вопрос 10

10. Использование прокси не защищает ваш трафик данных от отслеживания локальным провайдером.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. _____ прикладного уровня перенаправляет трафик отдельных браузеров, не защищая другие приложения.

2. Надёжный _____ инкапсулирует и шифрует все пакеты данных устройства.

3. Между прикладным и транспортным уровнями работает прокси-протокол — _____ .

4. HTTP-прокси работают на уровне модели OSI под названием « _____ ».

5. Стандартные прокси-серверы не обеспечивают такую защиту полезной нагрузки, как _____ , оставляя данные уязвимыми.

6. VPN обеспечивает защиту всех сетевых адаптеров — это _____ режим.

СЛОВАРНЫЙ БАНК СЛОВ

ВИДИМОСТЬ ВПН-ТУННЕЛЬ ПОДДЕРЖКА ЮДИПИ ПРИКЛАДНОЙ СИСТЕМНЫЙ
СОКС-ПРОКСИ ХТТП-ПРОКСИ ШИФРОВАНИЕ

Напишите свои ответы здесь:

1.
2.
3.
4.
5.
6.

Контрольная точка 4: Сопоставление сетевых понятий

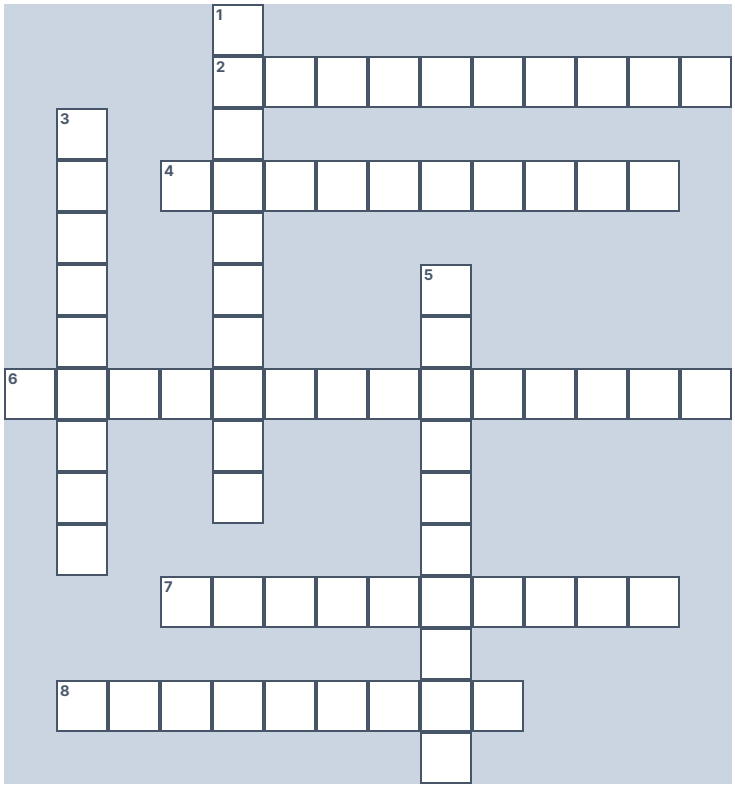
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. HTTP-прокси	A	Маршрутизация на уровне операционной системы, шифрующая трафик всех приложений.
☐	2. Прокси SOCKS5	B	Прикладной уровень, на котором работают стандартные протоколы веб-прокси.
☐	3. VPN-туннель	C	Способность SOCKS5 передавать UDP, а не только TCP, в отличие от обычных HTTP-прокси.
☐	4. Общесистемный	D	Клиентское расширение, скрывающее трафик только внутри песочницы браузера.
☐	5. Уровень 7 модели OSI	E	Шифрование и инкапсуляция, охватывающие весь фоновый трафик устройства.
☐	6. Поддержка UDP	F	Состояние трафика, при котором незашифрованные данные прокси остаются видимыми для провайдеров.
☐	7. Прокси в браузере	G	Прокси уровня приложений, перенаправляющий трафик отдельных веб-браузеров.
☐	8. Видимость для провайдера	H	Прокси-протокол между прикладным и транспортным уровнями, без шифрования.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

2. Уровень приложений, на котором работают стандартные веб-прокси-протоколы (10)

4. Прокси прикладного уровня, перенаправляющий трафик отдельных веб-браузеров (10)

6. Способность SOCKS5 ретранслировать UDP наряду с TCP, в отличие от обычных HTTP-прокси (14)

7. Прокси-протокол между прикладным и транспортным уровнями без шифрования (10)

8. Маршрутизация на уровне операционной системы, шифрующая трафик всех приложений (9)

ПО ВЕРТИКАЛИ

1. Шифрование и инкапсуляция, охватывающие весь фоновый трафик устройства (10)

3. Состояние трафика, при котором нешифрованные данные прокси остаются видимыми для провайдеров (9)

5. Клиентское расширение, скрывающее только трафик внутри песочницы браузера (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

2 по горизонтали: Уровень приложений, на котором работают стандартные веб-прокси-протоколы (10 букв):

4 по горизонтали: Прокси прикладного уровня, перенаправляющий трафик отдельных веб-браузеров (10 букв):

6 по горизонтали: Способность SOCKS5 ретранслировать UDP наряду с TCP, в отличие от обычных HTTP-прокси (14 букв):

7 по горизонтали: Прокси-протокол между прикладным и транспортным уровнями без шифрования (10 букв):

8 по горизонтали: Маршрутизация на уровне операционной системы, шифрующая трафик всех приложений (9 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Шифрование и инкапсуляция, охватывающие весь фоновый трафик устройства (10 букв):

3 по вертикали: Состояние трафика, при котором нешифрованные данные прокси остаются видимыми для провайдеров (9 букв):

5 по вертикали: Клиентское расширение, скрывающее только трафик внутри песочницы браузера (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.

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

СПИСОК СЛОВ СЛОВАРЯ

ХТТППРОКСИ СОКСПРОКСИ ВПНТУННЕЛЬ СИСТЕМНЫЙ ПРИКЛАДНОЙ
ПОДДЕРЖКАЮДИПИ БРАУЗЕРНЫЙ ВИДИМОСТЬ

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. ХТТППРОКСИ

B. СОКСПРОКСИ

C. ВПНТУННЕЛЬ

D. СИСТЕМНЫЙ

E. ПРИКЛАДНОЙ

F. ПОДДЕРЖКАЮДИПИ

G. БРАУЗЕРНЫЙ

H. ВИДИМОСТЬ

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Уровень приложений, на котором работают стандартные веб-прокси-протоколы.

_____ 2. Способность SOCKS5 ретранслировать UDP наряду с TCP, в отличие от обычных HTTP-прокси.

_____ 3. Прокси прикладного уровня, перенаправляющий трафик отдельных веб-браузеров.

_____ 4. Клиентское расширение, скрывающее только трафик внутри песочницы браузера.

_____ 5. Шифрование и инкапсуляция, охватывающие весь фоновый трафик устройства.

_____ 6. Маршрутизация на уровне операционной системы, шифрующая трафик всех приложений.

_____ 7. Состояние трафика, при котором нешифрованные данные прокси остаются видимыми для провайдеров.

_____ 8. Прокси-протокол между прикладным и транспортным уровнями без шифрования.

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. СОРПТХКИПТ
2. ЛТВПУЬНЕНН
3. ПАОДРЛЙКНИ
4. ЕЫЗЙУНРБРА
5. КРИОСОПССК
6. ЫТИНМСЕЙС
7. ДПЮПАОДИРИКДЖЕ
8. ЬМТВИИОСД

Дополнительное задание: Думай быстро

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

1	Отличия прокси от VPN			
2	То, что остаётся незашифрованным без VPN			
3	Способы распознать поддельную сеть Wi-Fi			
4	То, что делает посредник в повседневной жизни			
5	Ситуации, в которых достаточно прокси			
6	Устройства, которые могут использовать VPN			
7	Известные вам типы прокси			
8	То, что может скрыть VPN			
9	Мифы о VPN			
10	Обещания, которые даёт хороший VPN-провайдер			
11	От чего VPN не может вас защитить			
12	Слова из этого рабочего листа, которые вы хотите запомнить			
13	Причины использовать VPN в путешествии			
14	Ситуации, в которых нужен VPN			
15	Места, где вы пользовались бы VPN			

Контрольная точка 8: Кейсы по VPN

Примените изученные понятия к реальным ситуациям ниже.

САРА (СТУДЕНТКА В КАФЕ)

👩‍💻 “Привет! Я в Coffee & Bytes, подключена к открытой сети «Free_Wi-Fi_No_Password». Мне нужно войти в школьную почту, а друг говорит, что бесплатного браузерного прокси достаточно для безопасности. Защитит ли прокси мой вход и файлы, или мне нужен VPN?”

АЛЕКС (СТУДЕНТ-ПУТЕШЕСТВЕННИК)

👩‍💻 “Я за границей, а биологический документальный фильм, размещённый в моей стране, показывает сообщение «Это видео недоступно в вашем текущем местоположении». Одноклассник пользуется прокси, а у меня VPN. Почему меня блокируют и какой инструмент сработает лучше?”

Контрольная точка 9: Расшифруйте шифр

Чтобы завершить обучение по сравнению прокси, расшифруйте это секретное сообщение о защищённом туннелировании.

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

17	6	18	6	15	1	17	18	1	3	13	33	11	20	6

20	18	1	22	10	12		25	6	18	6	9		17	18	16	12	19	10

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: Что такое прокси-сервер?

Прокси-сервер — это посредник, пересылающий запросы между вашим приложением и целевым сервером. Сайт видит IP-адрес прокси вместо вашего, но перенаправляется только трафик приложений, настроенных на его использование, а базовый прокси этот трафик не шифрует.

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: Прокси — это VPN?

Нет. Прокси передаёт трафик отдельных приложений, как правило, без шифрования. VPN создаёт зашифрованный туннель на сетевом уровне, который несёт весь трафик устройства, включая фоновые приложения.

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 прокси?

Можно, но бесплатные прокси часто содержат неизвестные операторы. Поскольку базовый прокси не шифрует трафик, его оператор может видеть и даже изменять незашифрованные страницы. Прежде чем пользоваться, проверьте, кто управляет сервисом.

Q7: Ведёт ли прокси журналы?

Может. Прокси обрабатывает каждый пересылаемый запрос, поэтому его оператор может записывать ваш IP-адрес, посещаемые сайты и время. Проверьте, кто им управляет и что говорит его политика конфиденциальности.

Q8: Когда достаточно прокси?

Прокси может быть достаточным для задач с низким риском, например для смены видимого местоположения одного браузера. Для банковских операций, общедоступного Wi-Fi или защиты каждого приложения на устройстве VPN — более безопасный выбор, потому что он шифрует весь трафик.

Q9: Может ли прокси защитить все приложения на моём телефоне?

Нет. Его используют только приложения, учитывающие настройку прокси; остальные подключаются напрямую. VPN-приложение же направляет все приложения телефона через свой зашифрованный туннель.

Q10: Что такое прокси SOCKS5?

SOCKS5, определённый в RFC 1928, — это прокси-протокол, расположенный между прикладным и транспортным уровнями. Он может передавать соединения TCP и дейтаграммы UDP и поддерживает аутентификацию, но встроенного шифрования в нём нет. [1]

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

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

Q1: На каких сетевых уровнях работают прокси и VPN?

HTTP-прокси работает на прикладном уровне (уровень 7) и понимает веб-запросы. SOCKS5 находится между прикладным и транспортным уровнями. VPN-протоколы, такие как IPsec или WireGuard, работают на сетевом уровне, поэтому могут передавать весь IP-трафик устройства.

Q2: Остаётся ли сайт HTTPS зашифрованным через прокси?

Да. Когда вы открываете сайт HTTPS через прокси, шифрование TLS работает сквозным образом между вашим браузером и сайтом, поэтому прокси видит домен, но не содержимое страниц. Обычные страницы HTTP остаются читаемыми.

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 прозрачный прокси и кто его использует?

Прозрачный прокси перехватывает трафик без какой-либо настройки на устройстве пользователя. Школы, компании и провайдеры используют их для кеширования или фильтрации контента. Пользователи часто не знают о его наличии, и он не даёт им никакой конфиденциальности.

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: Почему прокси может казаться быстрее VPN-подключения?

Базовый прокси не шифрует трафик и обрабатывает данные только одного приложения, поэтому нагрузка на процессор меньше. VPN шифрует каждый пакет с устройства. С современными протоколами разница часто невелика, а прокси обеспечивает намного меньшую защиту.

Q8: Могут ли сайты определить, что я использую прокси или VPN?

Часто да. Многие сайты сверяют IP-адреса со списками известных прокси-и VPN-серверов, а HTTP-прокси могут добавлять заголовки, такие как Via или X-Forwarded-For. Стриминговые сервисы обычно блокируют и то, и другое.

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 прокси остановить ограничение скорости провайдером?

Редко. Обычный прокси не шифрует трафик, поэтому провайдер всё равно видит, какого рода это активность. VPN скрывает типы трафика, но ни один из инструментов не решает проблемы перегрузки или лимитов данных.

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. СТАНДАРТ SOCKS

Протокол SOCKS версии 5 был опубликован IETF как RFC 1928 в марте 1996 года и до сих пор остаётся эталонной спецификацией для прокси SOCKS5, которые используют браузеры и приложения. [1]

2. ПРОМЕЖУТОЧНЫЙ СЛОЙ

RFC 1928 описывает SOCKS как прослойку между прикладным и транспортным уровнями, поэтому он не может пересылать трафик сетевого уровня, например ICMP. [1]

3. UDP-РЕТРАНСЛЯТОР

В SOCKS5 добавлена команда UDP ASSOCIATE, позволяющая прокси передавать дейтаграммы UDP, а также соединения TCP; обычные HTTP-прокси этого не умеют. [1]

4. ПОРТ SOCKS ПО УМОЛЧАНИЮ

Клиенты SOCKS5 по умолчанию подключаются к прокси-серверу по TCP-порту 1080, как определено в RFC 1928; многие прокси-сервисы позволяют выбирать другие порты. [1]

5. HTTP-ПОСРЕДНИКИ

Стандарт HTTP (RFC 9110) определяет прокси как агент пересылки сообщений, выбираемый клиентом, который передаёт запросы дальше к исходному серверу.

6. ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ

Глубокая инспекция пакетов (DPI) изучает содержимое пакетов и характер трафика; незашифрованный прокси-трафик ей полностью виден, а VPN-трафик раскрывает гораздо меньше.

7. VPN СЕТЕВОГО УРОВНЯ

IPsec, описанный в NIST SP 800-77, защищает трафик на сетевом уровне, поэтому IP-пакеты любого приложения можно защитить без настройки для каждого приложения. [2]

8. ОХВАТ ТОЛЬКО БРАУЗЕРА

Прокси, заданный в одном браузере, влияет только на этот браузер; почтовые клиенты, игры и системные обновления продолжают использовать обычное подключение устройства.

9. TOR И ПРОКСИ

Tor пропускает трафик через три добровольных ретранслятора (входной, средний и выходной) и обычно доступен через локальный прокси SOCKS, добавляя уровни, которых не может дать один прокси.

10. КОМПРОМИСС ПО СКОРОСТИ

Прокси могут казаться быстрее, потому что пропускают шифрование, но современные VPN-протоколы, например WireGuard, добавляют мало издержек и при этом защищают весь трафик устройства.

Технические ссылки и источники

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

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

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

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

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

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

Ответы: сравнение прокси-серверов и виртуальных частных сетей, различия в шифровании и маршрутизация на уровне приложения и всей системы

1 **Уровень OSI для прокси** ПРОТОКОЛЫ **Правильный ответ: C**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Стандартные прокси HTTP/HTTPS работают на прикладном уровне (уровень 7) и перенаправляют трафик отдельных браузеров. У них нет общесистемной сетевой маршрутизации. Источник: Tor Project Foundation.

2 **Вопрос 2** **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

SOCKS5 передаёт трафик TCP и UDP между прикладным и транспортным уровнями, но по умолчанию не шифрует, тогда как HTTP-прокси обрабатывают веб-запросы.

3 **Шифрование системы VPN** БЕЗОПАСНОСТЬ WI-FI **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN инкапсулирует и шифрует весь трафик операционной системы, тогда как прокси перенаправляет трафик только определённых настроенных приложений. Источник: Deloitte Advisory.

4 **Отсутствие шифрования в прокси** УПРАВЛЕНИЕ МАРШРУТИЗАЦИЕЙ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

HTTP-прокси пересылают трафик браузера на прикладном уровне, не шифруя содержимое пакетов, поэтому оператор вашей сети или провайдер всё равно могут отследить ваш контентный трафик. Источник: IETF Proxy Vulnerabilities.

5 **Уязвимость обхода** КОНФИДЕНЦИАЛЬНОСТЬ **Правильный ответ: D**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Прокси браузера применяют правила только к самому веб-браузеру. Фоновые приложения, обновления операционной системы и почтовые клиенты обходят прокси, раскрывая ваш настоящий IP-адрес. Источник: W3C Consortium.

Ответы: контрольная точка 2 – верно или неверно

6 **Вопрос 6** **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

SOCKS5 передаёт трафик между прикладным и транспортным уровнями, но по умолчанию не выполняет шифрование, поэтому содержимое пакетов остаётся читаемым при передаче.

7 **Туннели сетевого уровня** СКОРОСТИ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Работая на сетевом уровне, VPN маршрутизирует и шифрует исходящий трафик с вашего устройства, помогая защитить трафик во всей системе. Источник: Deloitte Advisory.

8 **Ограничение шифрования в прокси** РИСК ПЕРЕХВАТА **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Прокси иногда бывают быстрее, но только потому, что НЕ выполняют шифрование. Отсутствие шифрования делает данные уязвимыми для просмотра. Источник: IETF Proxy Vulnerabilities.

9 **Перенаправление на уровне приложений** БРАНДМАУЭРЫ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В отличие от VPN на уровне всей системы, прокси-серверы нужно настраивать вручную в параметрах браузера или в полях прокси отдельных приложений. Источник: W3C Consortium.

10 **Риск отслеживания провайдером** БЕЗ ЖУРНАЛОВ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Поскольку обычные прокси HTTP/SOCKS5 не шифруют полезные данные, ваш местный провайдер сохраняет полную видимость ваших действий в сети. 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

G 1. HTTP-прокси	H 2. Прокси SOCKS5	E 3. VPN-туннель	A 4. Общесистемный
B 5. Уровень 7 модели OSI	C 6. Поддержка UDP	D 7. Прокси в браузере	F 8. Видимость для провайдера

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ХТТП-ПРОКСИ	2 ВПН-ТУННЕЛЬ	3 СОКС-ПРОКСИ	4 ПРИКЛАДНОЙ
5 ШИФРОВАНИЕ	6 СИСТЕМНЫЙ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 E – ПРИКЛАДНОЙ	2 F – ПОДДЕРЖКАЮДИПИ	3 A – ХТТППРОКСИ	4 G – БРАУЗЕРНЫЙ
5 C – ВПНТУННЕЛЬ	6 D – СИСТЕМНЫЙ	7 H – ВИДИМОСТЬ	8 B – СОКСПРОКСИ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить HTTP-прокси, Прокси SOCKS5 и VPN-туннель и привести пример для каждого термина.

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

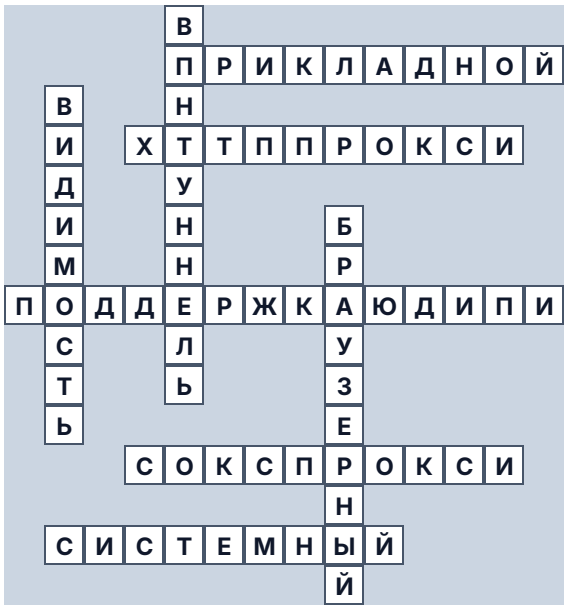
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

2 по горизонтали: ПРИКЛАДНОЙ Уровень приложений, на котором работают стандартные веб-прокси-протоколы (10 букв)

4 по горизонтали: ХТТППРОКСИ Прокси прикладного уровня, перенаправляющий трафик отдельных веб-браузеров (10 букв)

6 по горизонтали: ПОДДЕРЖКАЮДИПИ Способность SOCKS5 ретранслировать UDP наряду с TCP, в отличие от обычных HTTP-прокси (14 букв)

7 по горизонтали: СОКСПРОКСИ Прокси-протокол между прикладным и транспортным уровнями без шифрования (10 букв)

8 по горизонтали: СИСТЕМНЫЙ Маршрутизация на уровне операционной системы, шифрующая трафик всех приложений (9 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ВПНТУННЕЛЬ Шифрование и инкапсуляция, охватывающие весь фоновый трафик устройства (10 букв)

3 по вертикали: ВИДИМОСТЬ Состояние трафика, при котором нешифрованные данные прокси остаются видимыми для провайдеров (9 букв)

5 по вертикали: БРАУЗЕРНЫЙ Клиентское расширение, скрывающее только трафик внутри песочницы браузера (10 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. СОРПТХКИПТ — **ХТТППРОКСИ**
2. ЛТВПУЬНЕННН — **ВПНТУННЕЛЬ**
3. ПАОДРЛЙКНИ — **ПРИКЛАДНОЙ**
4. ЕЫЗЙУНРБРА — **БРАУЗЕРНЫЙ**
5. КРИОСОПССК — **СОКСПРОКСИ**
6. ЫТИНМСЕЙС — **СИСТЕМНЫЙ**
7. ДПЮПАОДИРИКДЖЕ — **ПОДДЕРЖКАЮДИПИ**
8. ЬМТВИИОСД — **ВИДИМОСТЬ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ПЕРЕНАПРАВЛЯЙТЕ ТРАФИК ЧЕРЕЗ ПРОКСИ"

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.
- Прокси и VPN: обычный прокси в браузере не шифрует её трафик. VPN шифрует всё на устройстве, из-за чего перехваченные пакеты становятся нечитаемыми для местных перехватчиков.

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.
- Что лучше: оба дают ему IP-адрес родной страны, но прокси охватывает только настроенное приложение, а VPN шифрует ещё и весь трафик его устройства.