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

Как скрыть свой IP-адрес Рабочий лист

Скрытие IP-адресов, маскировка местоположения, прокси, Tor и предотвращение утечек DNS/WebRTC

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, как работают IP-адреса и как они раскрывают местоположение.
- Сравните прокси, Tor и VPN для сокрытия сетевых адресов.
- Определите методы обнаружения и предотвращения утечек DNS и WebRTC.
- Разберитесь, как сайты отслеживают пользователей по их публичному IP.
- Оцените маршрутизацию Multi-Hop и зашифрованные туннели для защиты IP.

ИНСТРУКЦИИ К РАБОЧЕМУ ЛИСТУ ПО ЗАЩИТЕ IP

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: скрытию IP-адреса и предотвращению утечек. Завершите работу дополнительным заданием «Думай быстро».

СКРЫТИЕ ВАШЕГО IP (ВВЕДЕНИЕ)

Ваш IP-адрес — это цифровой почтовый адрес, который раскрывает ваше физическое местоположение и сетевые привычки. Скрытие IP — первая линия защиты от онлайн-слежки, профилирования и геоблокировки. Понимание того, как надёжно скрыть свой адрес, помогает защитить вашу конфиденциальность в интернете.

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

Контрольная точка 1: Задание с выбором ответа

1 **1. Что публичный IP-адрес устройства раскрывает посещаемым вами сайтам?**

- A. Номер кредитной карты пользователя
- B. Ваше примерное местоположение и название вашего провайдера
- C. Полный локальный каталог файлов
- D. Настройки языка клавиатуры

2 **2. Какой метод скрывает ваш IP-адрес и шифрует весь трафик во всей системе?**

- A. Стандартный веб-прокси
- B. Очистка файлов cookie браузера
- C. Виртуальная частная сеть (VPN)
- D. Отключение встроенного межсетевого экрана

3 **3. В чём главное ограничение конфиденциальности при использовании бесплатного веб-прокси?**

- A. Не шифрует трафик данных в общедоступных сетях
- B. Требуется установка внешней операционной системы
- C. Полностью запрещён в США
- D. Требует подключения по выделенной телефонной линии

4 **4. Как сеть Tor обеспечивает пользователям высокую анонимность?**

- A. Ускоряя скорость соединения
- B. Направляя трафик через три релея, которые поддерживают волонтёры
- C. Регистрируя ваше имя в глобальной базе данных
- D. Ограничивая доступ только государственными органами

5 **5. Что такое утечка DNS?**

- A. Ошибка при отправке письма на неверный адрес
- B. Когда запросы DNS обходят туннель VPN и идут к провайдеру
- C. Аппаратный сбой блока питания локального маршрутизатора
- D. Обновление драйвера локального сетевого адаптера

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Прокси-сервер шифрует фоновый трафик ОС так же, как VPN.

○ Верно ○ Неверно

7 Вопрос 7

7. Маршрутизация Tor очень безопасна, но снижает скорость работы в сети.

○ Верно ○ Неверно

8 Вопрос 8

8. Утечки WebRTC могут раскрыть ваш настоящий IP-адрес во время активного сеанса VPN.

○ Верно ○ Неверно

9 Вопрос 9

9. Если VPN включён и утечек нет, ваш провайдер не видит, какие сайты вы посещаете.

○ Верно ○ Неверно

10 Вопрос 10

10. Скрытие IP-адреса блокирует отслеживание по цифровому отпечатку браузера.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Обход защищённого туннеля, раскрывающий ваши запросы доменных имён, называется _____ .

2. Браузерные коммуникационные API на основе технологии _____ могут случайно раскрыть ваш реальный IP-адрес.

3. _____ перенаправляет трафик браузера, но не шифрует содержимое пакетов.

4. Многослойное шифрование, которое использует _____ , обеспечивает высокий уровень анонимности.

5. Ваш публичный _____ назначается вашим оператором связи и показывает ваш регион.

6. Обход региональных блокировок медиаконтента достигается благодаря приёму, который называется _____ местоположения.

СЛОВАРНЫЙ БАНК СЛОВ

АЙПИ-АДРЕС ВЕБ-ПРОКСИ ВЕБАРТИСИ КУКИ МАСКИРОВКА СЕТЬ TOR СЛЕЖКА УТЕЧКА ДНС

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление сетевых понятий

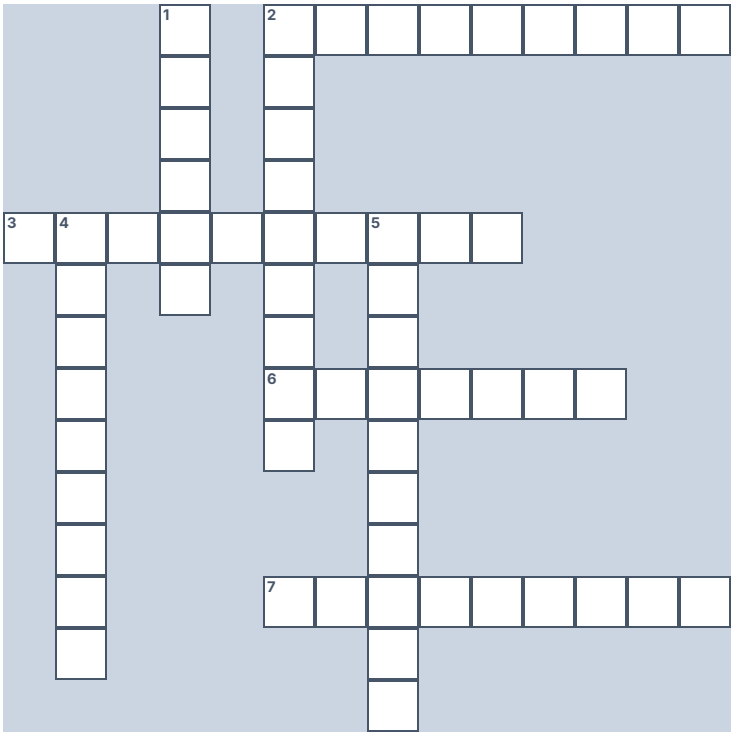
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. IP-адрес	A	Шифрует весь трафик устройства и направляет его через VPN-сервер.
☐	2. VPN-туннель	B	Направляет данные через три добровольных сервера, шифруя слои на каждом шаге.
☐	3. Сеть Tor	C	Маршрутизация подключения через сервер другой страны для обхода геоблокировок.
☐	4. Веб-прокси	D	Уникальная числовая метка, идентифицирующая интерфейс устройства в интернете.
☐	5. Утечка DNS	E	Перенаправляет трафик браузера на уровне приложения без шифрования на уровне системы.
☐	6. API WebRTC	F	Запись вашим оператором связи адресов назначения незашифрованного интернет-трафика.
☐	7. Маскировка местоположения	G	Запросы, которые разрешаются вне VPN-туннеля и раскрывают провайдеру посещённые домены.
☐	8. Отслеживание провайдером	H	Функция браузера для голоса и видео, которая может обходить туннели и раскрывать реальные IP-адреса.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

2. Функция браузера для голосовой и видеосвязи, способная обойти туннели и раскрыть реальные IP-адреса (9)

3. Маршрутизация соединения через сервер другой страны для обхода геоблокировок (10)

6. Пропускает данные через три волонтёрских сервера, шифруя слои на каждом шаге (7)

7. Запросы, обрабатываемые вне VPN-туннеля, раскрывают провайдеру посещённые домены (9)

ПО ВЕРТИКАЛИ

1. Запись вашим оператором связи адресов назначения незашифрованного интернет-трафика (6)

2. Перенаправляет трафик браузера на прикладном уровне без шифрования на уровне системы (9)

4. Уникальный числовой идентификатор сетевого интерфейса устройства в интернете (9)

5. Шифрует весь трафик устройства и направляет его через VPN-сервер (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: Функция браузера для голосовой и видеосвязи, способная обойти туннели и раскрыть реальные IP-адреса (9 букв):

3 по горизонтали: Маршрутизация соединения через сервер другой страны для обхода геоблокировок (10 букв):

6 по горизонтали: Пропускает данные через три волонтёрских сервера, шифруя слои на каждом шаге (7 букв):

7 по горизонтали: Запросы, обрабатываемые вне VPN-туннеля, раскрывают провайдеру посещённые домены (9 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Запись вашим оператором связи адресов назначения незашифрованного интернет-трафика (6 букв):

2 по вертикали: Перенаправляет трафик браузера на прикладном уровне без шифрования на уровне системы (9 букв):

4 по вертикали: Уникальный числовой идентификатор сетевого интерфейса устройства в интернете (9 букв):

5 по вертикали: Шифрует весь трафик устройства и направляет его через VPN-сервер (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.

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

СПИСОК СЛОВ СЛОВАРЯ

АЙПИАДРЕС ВПНТУННЕЛЬ СЕТЬТОР ВЕБПРОКСИ УТЕЧКАДНС ВЕБАРТИСИ МАСКИРОВКА СЛЕЖКА

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. АЙПИАДРЕС

B. ВПНТУННЕЛЬ

C. СЕТЬТОР

D. ВЕБПРОКСИ

E. УТЕЧКАДНС

F. ВЕБАРТИСИ

G. МАСКИРОВКА

H. СЛЕЖКА

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Перенаправляет трафик браузера на прикладном уровне без шифрования на уровне системы.

_____ 2. Маршрутизация соединения через сервер другой страны для обхода геоблокировок.

_____ 3. Функция браузера для голосовой и видеосвязи, способная обойти туннели и раскрыть реальные IP-адреса.

_____ 4. Уникальный числовой идентификатор сетевого интерфейса устройства в интернете.

_____ 5. Пропускает данные через три волонтёрских сервера, шифруя слои на каждом шаге.

_____ 6. Запись вашим оператором связи адресов назначения незашифрованного интернет-трафика.

_____ 7. Запросы, обрабатываемые вне VPN-туннеля, раскрывают провайдеру посещённые домены.

_____ 8. Шифрует весь трафик устройства и направляет его через VPN-сервер.

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. ДАИЙАРЕСП
2. СТРОТЬЕ
3. УАКТДСЧНЕ
4. РКИАКВОМАС
5. ЕНЬПТНУВЛН
6. СПЕКОВРИБ
7. ТВСИИАЕРБ
8. ЕАСКЖЛ

Дополнительное задание: Думай быстро

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

1	Причины использовать VPN в путешествии			
2	Известные вам браузеры			
3	То, что может скрыть VPN			
4	Слова, связанные с конфиденциальностью			
5	Слова из этого рабочего листа, которые вы хотите запомнить			
6	То, что сайт может предположить по вашему IP			
7	Цифры или символы в IP-адресе			
8	Мифы о VPN			
9	Известные вам VPN-сервисы			
10	То, что может видеть ваш интернет-провайдер			
11	Обещания, которые даёт хороший VPN-провайдер			
12	То, что может раскрыть ваш настоящий IP			
13	Причины скрыть своё местоположение			
14	Способы скрыть свой IP-адрес			
15	Устройства, которые могут использовать VPN			

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

Чтобы завершить обучение по маскировке IP, расшифруйте это секретное сообщение о сокрытии ваших цифровых следов.

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

19 12 18 16 11 20 6 19 3 16 11 1 5 18 6 19 19

17 16 14 16 27 30 32 19 12 18 29 20 16 11

19 10 19 20 6 14 29

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: Скрывает ли веб-прокси мой IP-адрес?

Да, но только для трафика, отправляемого через него, обычно это ваш браузер. Большинство веб-прокси не шифруют ваши данные, поэтому ваш провайдер или оператор сети всё равно может видеть, что вы отправляете и получаете.

Q5: Законно ли скрывать свой IP-адрес?

Во многих странах да, но в некоторых ограничивают или запрещают VPN и другие средства, скрывающие IP-адрес. Скрытие IP никогда не делает незаконное действие законным, поэтому перед использованием проверьте местные законы.

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

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

Q6: Скрывает ли Tor мой IP-адрес?

Да. Tor направляет ваш трафик через три добровольных ретранслятора (входной, промежуточный и выходной), поэтому сайты видят адрес выходного ретранслятора, и ни один ретранслятор не знает одновременно, кто вы и куда идёте. [1]

Q7: Что раскрывает мой IP-адрес?

Ваш публичный IP-адрес обычно раскрывает вашего провайдера и примерное местоположение, например страну или город. Сайты также могут использовать его, чтобы связывать ваши посещения и применять геоблокировку.

Q8: Как проверить, что адрес скрыт?

Подключитесь к VPN, затем зайдите на сайт проверки IP и запустите тесты на утечки DNS и WebRTC. Показанные IP и DNS-серверы должны принадлежать VPN, а не вашему провайдеру. Если отображается ваш реальный IP, включите защиту от утечек.

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: Почему сайты всё ещё могут отслеживать меня после скрытия IP-адреса?

Скрытие IP-адреса не останавливает снятие цифрового отпечатка браузера. Трекеры могут объединить такие детали, как разрешение экрана, установленные шрифты и настройки браузера, в идентификатор, а вас могут идентифицировать также файлы cookie или вход в учётные записи, поэтому используйте и браузер, ориентированный на конфиденциальность. [3]

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: Может ли трафик IPv6 раскрыть мой настоящий IP-адрес?

Да, если ваш VPN туннелирует только IPv4. Тогда устройство может отправлять IPv6-трафик вне туннеля, раскрывая адрес, назначенный провайдером. Используйте VPN, который туннелирует или блокирует IPv6, и проверьте это тестом на утечку IPv6.

Q5: Как обфускация обходит блокировки VPN?

Обфускация (или «скрытый VPN») маскирует пакеты VPN-трафика под обычный HTTPS-трафик (порт 443). Это помогает 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: Раскрывает ли раздельное туннелирование мой настоящий IP-адрес?

Да, для приложений, которые вы исключили. Трафик вне туннеля использует ваш настоящий IP-адрес, а RFC 8828 отмечает, что WebRTC может раскрыть адрес провайдера даже при VPN с раздельным туннелированием, если браузер этого не ограничивает. [2]

Q7: Что такое общий IP-адрес и как он помогает конфиденциальности?

При общем IP-адресе множество пользователей VPN одновременно выходят в сеть с одним и тем же адресом. Из-за этого сайту намного сложнее связать конкретное посещение с вами, чем при выделенном IP-адресе, которым пользуетесь только вы.

Q8: Может ли мой провайдер видеть, что я использую VPN для скрытия IP-адреса?

Обычно да. Ваш провайдер видит, что вы подключаетесь к IP-адресу VPN-сервера, когда вы подключаетесь и сколько данных отправляете, но не видит посещаемые вами сайты и содержимое внутри зашифрованного туннеля.

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: Что лучше для скрытия IP-адреса: прокси или VPN?

Обычно лучше VPN. Он скрывает ваш IP-адрес для каждого приложения на устройстве и шифрует трафик, тогда как веб-прокси, как правило, охватывает только браузер и часто не добавляет шифрования.

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), ранний VPN-протокол от группы под руководством Microsoft в 1990-х годах, сегодня считается небезопасным, поэтому современные VPN используют WireGuard или OpenVPN.

2. СНЯТИЕ ЦИФРОВОГО ОТПЕЧАТКА

Скрытие IP-адреса не останавливает снятие цифрового отпечатка браузера, который может идентифицировать вас по таким деталям, как разрешение экрана и установленные шрифты. [3]

3. РЕВОЛЮЦИЯ WIREGUARD

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

4. РАСКРЫТИЕ АДРЕСА ЧЕРЕЗ WEBRTC

RFC 8828 предупреждает, что WebRTC может обнаружить как публичный адрес VPN, так и адрес провайдера, через который работает VPN, если браузер этого не ограничивает. [2]

5. ПРОИСХОЖДЕНИЕ АЛЬЯНСА 5 EYES

Разведывательное партнёрство «Пять глаз» в составе США, Великобритании, Канады, Австралии и Новой Зеландии выросло из сотрудничества союзников в области радиотехнической разведки времён Второй мировой войны.

6. ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ

Продвинутые межсетевые экраны применяют глубокую инспекцию пакетов (DPI), чтобы анализировать метаданные сетевых пакетов и блокировать типичные признаки VPN-подключений.

7. ПОВТОРНОЕ ИСПОЛЬЗОВАНИЕ ЦЕПОЧКИ TOR

Tor использует одну и ту же цепочку примерно десять минут, а затем строит новую, что затрудняет связывание вашей активности в браузере. [1]

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, выходной) для максимальной конфиденциальности. [1]

10. ПРОКСИ И VPN-ТУННЕЛИ

Веб-прокси меняет IP-адрес, который сайт видит для трафика вашего браузера, но, в отличие от VPN, обычно не шифрует этот трафик и не охватывает другие приложения на вашем устройстве. [5]

Технические ссылки и источники

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

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] Tor Project. (n.d.). Overview.

https://support.torproject.org/about-tor/how-tor-works/overview/

[2] IETF. (2021). RFC 8828: WebRTC IP Address Handling Requirements.

https://www.rfc-editor.org/rfc/rfc8828

[3] Electronic Frontier Foundation. (n.d.). Cover Your Tracks: Learn.

https://coveryourtracks.eff.org/learn

[4] Electronic Frontier Foundation. (2026). Choosing the VPN That's Right for You.

https://ssd.eff.org/module/choosing-vpn-thats-right-you

[5] Federal Trade Commission. (2018). FTC Provides Tips for Using VPN Apps.

https://www.ftc.gov/news-events/news/press-releases/2018/02/ftc-provides-tips-using-vpn-apps

Ответы: скрытие IP-адресов, маскировка местоположения, прокси, Tor и предотвращение утечек DNS/WebRTC

1 Вопрос 1

Правильный ответ: B

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что публичный IP-адрес устройства раскрывает посещаемым вами сайтам? → Ваше примерное местоположение и название вашего провайдера

2 Шифрование системы VPN ЗАДЕРЖКА

Правильный ответ: C

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В отличие от прокси, перенаправляющих только трафик браузера, VPN создаёт зашифрованный туннель для всей системы, защищая фоновые приложения, игры и запросы ОС. Источник: Tor Project Relays, W3C WebRTC API.

3 Отсутствие шифрования в прокси БЕЗОПАСНОСТЬ WI-FI

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Веб-прокси лишь пересылают трафик браузера и не шифруют содержимое пакетов, поэтому оператор вашей сети или провайдер всё равно может отследить ваш трафик. Источник: IETF Proxy Vulnerabilities.

4 Вопрос 4

Правильный ответ: B

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Как сеть Tor обеспечивает пользователям высокую анонимность? → Направляя трафик через три релея, которые поддерживают волонтёры

5 Утечки через DNS-туннель КОНФИДЕНЦИАЛЬНОСТЬ

Правильный ответ: B

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Утечка DNS происходит, когда запросы на преобразование доменных имён обходят VPN-туннель и уходят напрямую к преобразователям (резолверам) вашего провайдера, раскрывая записи о посещённых доменах. Источник: DNSSEC Tunnel Testing, EFF Tracking Evasion.

Ответы: контрольная точка 2 – верно или неверно

6 **Подробности об ограничениях прокси** МАСКИРОВКА IP **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Прокси работают на уровне приложений и не имеют общесистемной интеграции с сетевым драйвером, как VPN-туннель. Источник: IETF Proxy Vulnerabilities.

7 **Вопрос 7** **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Передача трафика через три волонтёрских релея с многоуровневым шифрованием добавляет задержку, поэтому Tor обычно медленнее прямого соединения.

8 **Вопрос 8** **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WebRTC может раскрыть локальные адреса и, при некоторых настройках VPN, публичный IP, присвоенный провайдером, под туннелем (RFC 8828).

9 **Вопрос 9** **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Без утечек DNS или WebRTC провайдер видит только зашифрованный трафик к VPN-серверу, а не сайты, которые вы посещаете.

10 **Ограничения фингерпринтинга** БЕЗ ЖУРНАЛОВ **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Фингерпринтинг нацелен на метрики конфигурации устройства (разрешение экрана, шрифты, плагины), которые остаются видимыми, даже когда IP скрыт. Источник: EFF Tracking Evasion.

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

D 1. IP-адрес	A 2. VPN-туннель	B 3. Сеть Tor	E 4. Веб-прокси
G 5. Утечка DNS	H 6. API WebRTC	C 7. Маскировка местоположения	F 8. Отслеживание провайдером

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 УТЕЧКА ДНС	2 ВЕБАРТИСИ	3 ВЕБ-ПРОКСИ	4 СЕТЬ ТОР
5 АЙПИ-АДРЕС	6 МАСКИРОВКА		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 D – ВЕБПРОКСИ	2 G – МАСКИРОВКА	3 F – ВЕБАРТИСИ	4 A – АЙПИАДРЕС
5 C – СЕТЬТОР	6 H – СЛЕЖКА	7 E – УТЕЧКАДНС	8 B – ВПНТУННЕЛЬ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить IP-адрес, VPN-туннель и Сеть Tor 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

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

РЕШЕНИЕ КРОССВОРДА

		С		В	Е	Б	А	Р	Т	И	С	И
		Л		Е								
		Е		Б								
		Ж		П								
М	А	С	К	И	Р	О	В	К	А			
	Й		А		О		П					
	П				К		Н					
	И				С	Е	Т	Ь	Т	О	Р	
	А				И		У					
	Д						Н					
	Р						Н					
	Е				У	Т	Е	Ч	К	А	Д	Н	С
	С						Л					
							Ь					

РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

2 по горизонтали: ВЕБАРТИСИ Функция браузера для голосовой и видеосвязи, способная обойти туннели и раскрыть реальные IP-адреса (9 букв)

3 по горизонтали: МАСКИРОВКА Маршрутизация соединения через сервер другой страны для обхода геоблокировок (10 букв)

6 по горизонтали: СЕТЬТОР Пропускает данные через три волонтёрских сервера, шифруя слои на каждом шаге (7 букв)

7 по горизонтали: УТЕЧКАДНС Запросы, обрабатываемые вне VPN-туннеля, раскрывают провайдеру посещённые домены (9 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: СЛЕЖКА Запись вашим оператором связи адресов назначения незашифрованного интернет-трафика (6 букв)

2 по вертикали: ВЕБПРОКСИ Перенаправляет трафик браузера на прикладном уровне без шифрования на уровне системы (9 букв)

4 по вертикали: АЙПИАДРЕС Уникальный числовой идентификатор сетевого интерфейса устройства в интернете (9 букв)

5 по вертикали: ВПНТУННЕЛЬ Шифрует весь трафик устройства и направляет его через VPN-сервер (10 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ДАИЙАРЕСП — **АЙПИАДРЕС**
2. СТРОТЬЕ — **СЕТЬТОР**
3. УАКТДСЧНЕ — **УТЕЧКАДНС**
4. РКИАКВОМАС — **МАСКИРОВКА**
5. ЕНЬПТНУВЛН — **ВПНТУННЕЛЬ**
6. СПЕКОВРИБ — **ВЕБПРОКСИ**
7. ТВСИИАЕРБ — **ВЕБАРТИСИ**
8. ЕАСКЖЛ — **СЛЕЖКА**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"СКРОЙТЕ СВОЙ АДРЕС С ПОМОЩЬЮ СКРЫТОЙ СИСТЕМЫ"

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.