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

Безопасность Surfshark

Изучение функций безопасности Surfshark, включая блокировку рекламы CleanWeb, динамическую маршрутизацию MultiHop, архитектуру Nexus SDN, парк серверов только с RAM и режим Camouflage.

ОБЗОР ОБУЧЕНИЯ: БЕЗОПАСНОСТЬ SURFSHARK

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 архитектуру безопасности Surfshark. Вы изучите серверное оборудование только на RAM, динамическую ротацию IP в Nexus SDN, блокировщики рекламы CleanWeb и маршрутизацию MultiHop.

КОНТРОЛЬНЫЕ ТОЧКИ РАБОЧЕГО ЛИСТА

- [ ] **Части 1-4: освойте настройки VPN и сетевой безопасности.**
- [ ] **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 лучшим VPN

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

Ваша дорожная карта обучения: безопасность Surfshark

- Проанализируйте техническую архитектуру и правила настройки безопасности Surfshark.
- Настройте параметры клиента, чтобы предотвратить утечки трафика IP, DNS и WebRTC.
- Сравните индивидуальные цены, пробные периоды и характеристики производительности со стандартными моделями.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО БЕЗОПАСНОСТИ SURFSHARK

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: инфраструктуре только на RAM, Nexus SDN и CleanWeb. Завершите работу дополнительным заданием «Думай быстро».

ПАРК СЕРВЕРОВ ТОЛЬКО НА RAM, NEXUS SDN И АРХИТЕКТУРА CLEANWEB (ВВЕДЕНИЕ)

Surfshark защищает конфиденциальность пользователей с помощью парка серверов только на ОЗУ, программно-определяемой сети Nexus с IP Rotator, блокировки рекламы CleanWeb и динамических путей шифрования Dynamic MultiHop.

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

Контрольная точка 1: Задание с выбором ответа

1. **1. Как называется встроенный блокировщик рекламы и вредоносного ПО в Surfshark?**
   - A) AdGuard
   - B) CleanWeb
   - C) ThreatShield
   - D) NetBlocker

2. **2. Какую аппаратную архитектуру Surfshark использует на всех серверах?**
   - A) Жёсткие диски
   - B) 100% только RAM
   - C) Оптические носители
   - D) Магнитная лента

3. **3. Какая функция направляет трафик через два разных VPN-сервера?**
   - A) Обходчик
   - B) MultiHop (Double VPN)
   - C) Сеть Nexus
   - D) Статический IP

4. **4. Какая функция оффускации маскирует VPN-трафик под обычные веб-данные?**
   - A) Kill Switch
   - B) Режим маскировки
   - C) CleanWeb 2.0
   - D) Раздельное туннелирование

5. **5. Для чего нужен инструмент Surfshark Bypasser?**
   - A) Speed Booster
   - B) Раздельное туннелирование
   - C) Менеджер паролей
   - D) DNS-преобразователь

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Серверы, работающие только на RAM, стирают все рабочие данные сразу после перезагрузки сервера.

○ Верно ○ Неверно

7 Вопрос 7

7. Режим Camouflage не позволяет провайдерам обнаружить, что вы используете VPN.

○ Верно ○ Неверно

8 Вопрос 8

8. CleanWeb 2.0 работает внутри расширений браузера и блокирует всплывающие окна согласия на cookie.

○ Верно ○ Неверно

9 Вопрос 9

9. Surfshark хранит временные метки подключений и журналы использования трафика.

○ Верно ○ Неверно

10 Вопрос 10

10. Сеть Nexus периодически меняет IP-адреса пользователей без разрыва соединения.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Навязчивую рекламу, скрипты отслеживания и фишинговые ссылки блокируют фильтры « _____ **».**

2. Следов активности пользователя не остаётся: серверы работают на памяти типа « _____ **».**

3. Маршрутизация данных через два отдельных зашифрованных сервера достигается с помощью туннелей « _____ **».**

4. Чтобы скрыть использование VPN от интернет-провайдеров, пользователи включают режим « _____ **».**

5. Разрешение банковским приложениям обходить VPN-туннель настраивается в разделе « _____ **».**

6. Архитектура SDN нового поколения, объединяющая парк серверов, — это система « _____ **».**

СЛОВАРНЫЙ БАНК СЛОВ

БАЙПАСЕР КАМУФЛЯЖ КИЛЛ-СВИЧ КЛИНВЕБ МУЛЬТИХОП НЕКСУС РОТАЦИЯ ТОЛЬКО ОЗУ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о VPN и сетях

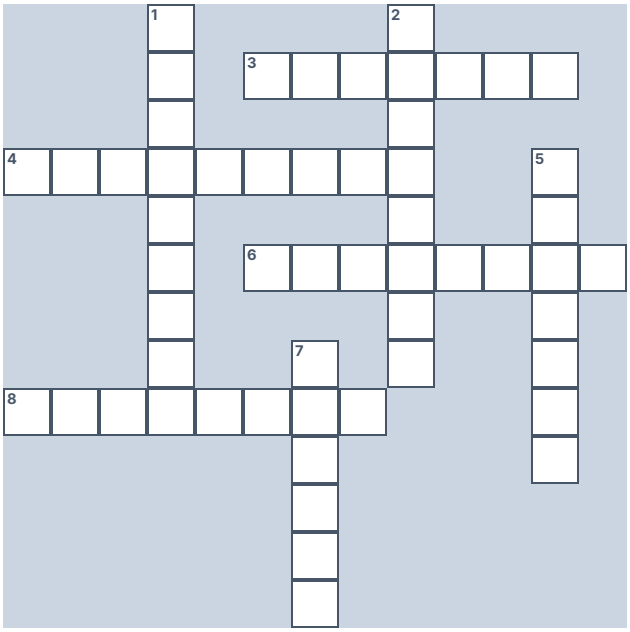
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. КЛИНВЕБ	A	Автоматическая функция безопасности, блокирующая сетевой трафик при обрыве VPN.
☐	2. ТОЛЬКО ОЗУ	B	Функция раздельного туннелирования, позволяющая выбранным приложениям обходить VPN.
☐	3. МУЛЬТИХОП	C	Продвинутый фильтр, блокирующий рекламу, вредоносное ПО и баннеры согласия на cookie.
☐	4. КАМУФЛЯЖ	D	Серверное оборудование с энергозависимой памятью, стирающее все данные при каждом цикле питания.
☐	5. ОБХОДЧИК	E	Функция, регулярно меняющая ваш внешний IP-адрес без прерывания туннелей.
☐	6. КИЛЛ-СВИЧ	F	Технология обфускации, скрывающая признаки VPN, чтобы имитировать обычный HTTPS-трафик.
☐	7. NEXUS NET	G	Функция двойного VPN, шифрующая трафик на двух разных серверных узлах.
☐	8. РОТАЦИЯ	H	Проприетарная программно-определяемая сеть, объединяющая все серверы в единую ячеистую сеть.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

3. Функция, регулярно меняющая ваш внешний IP-адрес без разрыва туннелей (7)

4. Серверное оборудование с энергозависимой памятью, стирающее все данные при каждом выключении питания (9)

6. Автоматическая защитная функция, блокирующая сетевой трафик при сбое VPN (8)

8. Функция раздельного туннелирования, позволяющая отдельным приложениям обходить VPN (8)

ПО ВЕРТИКАЛИ

1. Функция двойного VPN, шифрующая трафик через два разных серверных узла (9)

2. Технология обфускации, скрывающая признаки VPN и имитирующая обычный HTTPS-трафик (8)

5. Продвинутый фильтр, блокирующий рекламу, вредоносное ПО и баннеры согласия на cookie (7)

7. Собственная программно-определяемая сеть, объединяющая все серверы в единую ячеистую структуру (6)

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

3 по горизонтали: Функция, регулярно меняющая ваш внешний IP-адрес без разрыва туннелей (7 букв):

4 по горизонтали: Серверное оборудование с энергозависимой памятью, стирающее все данные при каждом выключении питания (9 букв):

6 по горизонтали: Автоматическая защитная функция, блокирующая сетевой трафик при сбое VPN (8 букв):

8 по горизонтали: Функция раздельного туннелирования, позволяющая отдельным приложениям обходить VPN (8 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Функция двойного VPN, шифрующая трафик через два разных серверных узла (9 букв):

2 по вертикали: Технология обфускации, скрывающая признаки VPN и имитирующая обычный HTTPS-трафик (8 букв):

5 по вертикали: Продвинутый фильтр, блокирующий рекламу, вредоносное ПО и баннеры согласия на cookie (7 букв):

7 по вертикали: Собственная программно-определяемая сеть, объединяющая все серверы в единую ячеистую структуру (6 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

КЛИНВЕБ ТОЛЬКООЗУ МУЛЬТИХОП КАМУФЛЯЖ БАЙПАСЕР КИЛЛСВИЧ НЕКСУС РОТАЦИЯ

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. КЛИНВЕБ**
- **B. ТОЛЬКООЗУ**
- **C. МУЛЬТИХОП**
- **D. КАМУФЛЯЖ**
- **E. БАЙПАСЕР**
- **F. КИЛЛСВИЧ**
- **G. НЕКСУС**
- **H. РОТАЦИЯ**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Технология обфускации, скрывающая признаки VPN и имитирующая обычный HTTPS-трафик.

_____ 2. Автоматическая защитная функция, блокирующая сетевой трафик при сбое VPN.

_____ 3. Продвинутый фильтр, блокирующий рекламу, вредоносное ПО и баннеры согласия на cookie.

_____ 4. Функция раздельного туннелирования, позволяющая отдельным приложениям обходить VPN.

_____ 5. Серверное оборудование с энергозависимой памятью, стирающее все данные при каждом выключении питания.

_____ 6. Функция, регулярно меняющая ваш внешний IP-адрес без разрыва туннелей.

_____ 7. Функция двойного VPN, шифрующая трафик через два разных серверных узла.

_____ 8. Собственная программно-определяемая сеть, объединяющая все серверы в единую ячеистую структуру.

Контрольная точка 7: Задание с перепутанными словами

Расставьте буквы ниже в правильном порядке, чтобы получить ключевые понятия и термины виртуальных частных сетей (VPN). Запишите ответы в предусмотренные поля.

1. НЕКВБИЛ
2. ПМОЬУИХТЛ
3. ПАБАСРЕЙ
4. ССКУНЕ
5. ОКОУОЬТЗЛ
6. ЯЖУЛКФАМ
7. КЧСВИИЛЛ
8. ОАЯРИЦТ

Дополнительное задание: Думай быстро

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

1	Функции безопасности в Surfshark			
2	Признаки того, что VPN-соединение медленное			
3	Известные вам VPN-протоколы			
4	То, что защищает шифрование			
5	Угрозы в общедоступных сетях Wi-Fi			
6	Страны, известные строгими законами о конфиденциальности			
7	Способы создать надёжный пароль			
8	Устройства, на которые вы установили бы Surfshark			
9	Вопросы для службы поддержки Surfshark			
10	Настройки, которые включают для дополнительной безопасности			
11	То, что Surfshark может скрыть от вашей сети			
12	Виды утечек VPN			
13	Данные, которые VPN никогда не должен хранить			
14	Слова, описывающие хорошее VPN-приложение			
15	То, что может проверить аудит			

Контрольная точка 8: Кейсы по VPN и сетям

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ОБХОД ФИЛЬТРОВ В КАМПУСЕ И НА РАБОТЕ



Ситуация: Студент обнаруживает, что Wi-Fi в университетском кампусе блокирует все стандартные порты OpenVPN и WireGuard.

Вопрос для обсуждения: Какая функция Surfshark позволяет студенту подключиться так, чтобы его не обнаружили сетевые администраторы?

КЕЙС 2: ЖУРНАЛИСТСКОЕ РАССЛЕДОВАНИЕ ВЫСОКОГО РИСКА



Ситуация: Журналисту-расследователю нужна дополнительная защита от слежки при изучении конфиденциальных корпоративных записей.

Вопрос для обсуждения: Чем Dynamic MultiHop обеспечивает более высокую конфиденциальность по сравнению с маршрутизацией через один сервер?

Контрольная точка 9: Расшифруйте шифр

Сетевой инженер защищает каналы маршрутизации и клиентские туннели. Используйте ключ «буква–число» ниже, чтобы расшифровать сообщение, 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

15	6	12	19	21	19		19		18	16	20	1	24	10	6	11

1	11	17	10		21	19	10	13	10	3	1	6	20

17	18	10	3	1	20	15	16	19	20	30

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 о виртуальных частных сетях (VPN) и туннелировании.

Q1: Что такое Surfshark CleanWeb?

CleanWeb — это встроенная функция безопасности, блокирующая рекламу, трекеры, вредоносное ПО и фишинговые сайты.

Q2: Что такое серверы только на RAM?

Серверы, работающие только на RAM, используют энергозависимую память, поэтому данные в памяти стираются при каждой перезагрузке серверов.

Q3: Что такое Surfshark MultiHop?

MultiHop (Double VPN) направляет и шифрует ваше интернет-соединение через два разных расположения серверов.

Q4: Как работает режим Camouflage Mode?

Режим Camouflage обфусцирует трафик VPN, чтобы ваш провайдер не мог определить, что вы используете VPN.

Q5: Что такое функция Bypasser?

Bypasser — инструмент раздельного туннелирования Surfshark, позволяющий отдельным приложениям или сайтам обходить VPN.

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

Просмотрите самые частые вопросы и ответы о виртуальных частных сетях (VPN) и туннелировании.

Q6: Есть ли в Surfshark Kill Switch?

Да, Kill Switch отключает вас от интернета, если VPN неожиданно разрывается.

Q7: Какой стандарт шифрования использует Surfshark?

Surfshark использует AES-256-GCM и ChaCha20, а также AEGIS-256X2 в своём новом протоколе Dausos.

Q8: Проходила ли политика отсутствия журналов Surfshark аудит?

Да, компания Deloitte подтвердила политику отсутствия журналов Surfshark в 2023 году и повторно в 2025 году.

Q9: Что такое Surfshark Nexus?

Nexus — это продвинутая архитектура SDN, объединяющая все серверы в единую сеть для более плавной маршрутизации.

Q10: Что такое функция IP Rotator?

IP Rotator автоматически меняет ваш IP-адрес каждые несколько минут, не разрывая сеанс VPN.

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

Изучите продвинутые технические аспекты протоколов VPN-туннелирования, интеграции мобильных клиентов и корпоративного развёртывания.

Q1: Чем Dynamic MultiHop отличается от традиционного Double VPN?

Dynamic MultiHop позволяет настроить любую комбинацию входных и выходных серверов по всему миру.

Q2: Работает ли CleanWeb 2.0 в расширениях для браузеров?

Да, CleanWeb 2.0 блокирует видеорекламу, всплывающие окна согласия на cookie и баннеры оповещений в Chrome и Firefox.

Q3: Что такое Alternative ID в пакете безопасности?

Alternative ID создаёт уникальные личные псевдонимы, адреса электронной почты и маски телефонных номеров.

Q4: Как Surfshark предотвращает утечки DNS?

Surfshark направляет все запросы доменных имён через собственные частные DNS-серверы на каждом узле.

Q5: Поддерживает ли Surfshark шифрование ChaCha20 на мобильных устройствах?

Да, WireGuard на Android и iOS использует ChaCha20-Poly1305 для высокой эффективности на мобильных устройствах.

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

Изучите продвинутые технические аспекты протоколов VPN-туннелирования, интеграции мобильных клиентов и корпоративного развёртывания.

Q6: Что такое режим NoBorders в Surfshark?

NoBorders автоматически обнаруживает сети с ограничениями и предоставляет специальные серверы.

Q7: Кто проводил аудиты безопасности браузерных расширений Surfshark?

Независимая фирма по кибербезопасности Cure53 завершила аудиты браузерных расширений и серверных систем.

Q8: Как Surfshark защищает от утечек IPv6?

Surfshark безопасно маршрутизирует трафик IPv6 или надёжно ограничивает его, чтобы не допустить утечки незашифрованных данных.

Q9: В какой юрисдикции находится Surfshark?

Surfshark работает по законодательству Нидерландов, соблюдая строгие европейские стандарты конфиденциальности GDPR.

Q10: Поддерживает ли Surfshark двухфакторную аутентификацию (2FA)?

Да, а Surfshark One добавляет защиту 2FA, чтобы только вы могли менять настройки функций.

Часть 11: 10 реальных фактов и выводов о VPN

Ознакомьтесь с реальными фактами о скорости шифрования VPN, аудитах протоколов, мобильном подключении и корпоративной удалённой работе.

1. АНАЛИЗ VPN

1. Surfshark заявляет, что вся её сеть из 4,500+ серверов работает на бездисковом оборудовании с энергозависимой памятью, только на ОЗУ.

2. АНАЛИЗ VPN

2. Компания «большой четвёрки» Deloitte подтвердила политику Surfshark по отсутствию журналов в 2023 году и повторно в ноябре 2025 года.

3. АНАЛИЗ VPN

3. Собственная архитектура Nexus объединяет все мировые серверы в динамическую программно-определяемую сеть.

4. АНАЛИЗ VPN

4. Rotating IP меняет ваш IP-адрес примерно каждые пять минут без разрыва VPN-подключения.

5. АНАЛИЗ VPN

5. CleanWeb 2.0 блокирует навязчивые всплывающие окна согласия на cookie и видеорекламу прямо в браузерах.

6. АНАЛИЗ VPN

6. Dynamic MultiHop позволяет создавать пользовательские двухсерверные пути шифрования в 100 странах.

7. VPN: ВАЖНО ЗНАТЬ

7. Camouflage Mode удаляет сигнатуры заголовков VPN, и трафик становится неотличим от обычного HTTPS.

8. VPN: ВАЖНО ЗНАТЬ

8. Alternative ID создаёт одноразовые псевдонимы и маски электронной почты, защищающие пользователей от утечек баз данных.

9. VPN: ВАЖНО ЗНАТЬ

9. Surfshark использует симметричное шифрование AES-256-GCM наряду с ChaCha20 в протоколах WireGuard.

10. АНАЛИЗ VPN

10. Режим NoBorders включается автоматически в сетях с ограничениями, обеспечивая устойчивый доступ через туннель.

Технические ссылки и источники

Учебное пособие и интерактивные головоломки составлены на основе мировых технических стандартов, спецификаций и нормативных рамок.

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Встроенный блокировщик контента** ЗАЩИТА ОТ РЕКЛАМЫ И ВРЕДОНОСНОГО ПО **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

CleanWeb — это встроенный фильтр безопасности Surfshark, который на уровне сети блокирует рекламу, домены трекеров, фишинговые сайты и вредоносные скрипты URL. Источник: CleanWeb Security Specs.

2 **100% инфраструктура только на ОЗУ** АРХИТЕКТУРА RAM **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Surfshark использует серверы только на ОЗУ, поэтому данные, находящиеся в памяти сервера, стираются при его выключении или перезагрузке. Источник: Cure53 Infrastructure Audit.

3 **Двойное туннелирование MultiHop** VPN MULTIHOP **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

MultiHop (Double VPN) шифрует трафик через два разных серверных узла в разных странах, чтобы предотвратить атаки корреляции трафика. Источник: руководство по Surfshark MultiHop.

4 **Режим Camouflage: обфускация** ОБФУСКАЦИЯ **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Режим Camouflage изменяет заголовки пакетов OpenVPN, маскируя трафик VPN под обычный трафик HTTPS и обходя блокировки строгих межсетевых экранов. Источник: Surfshark Stealth Whitepaper.

5 **Раздельное туннелирование Bypasser** РАЗДЕЛЬНОЕ ТУННЕЛИРОВАНИЕ **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Bypasser — инструмент раздельного туннелирования Surfshark, позволяющий пользователям выбирать отдельные приложения или сайты, трафик которых идёт напрямую через обычное подключение к провайдеру. Источник: Surfshark Client Features.

Ответы: контрольная точка 2 – верно или неверно

6 **Стирание данных энергозависимой памяти** БЕЗОПАСНОСТЬ СЕРВЕРА **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Серверы, работающие только на RAM, не хранят данных на постоянных жёстких дисках; перезагрузка оборудования сразу очищает всю рабочую память. Источник: RAM Server Architecture.

7 **Режим Camouflage: сокрытие от провайдера** СОКРЫТИЕ ТРАФИКА **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Режим Camouflage удаляет сигнатуры протокола OpenVPN, не позволяя провайдерам обнаружить, что пользователь подключён к туннелю VPN. Источник: Deep Packet Inspection Guide.

8 **Расширения браузера CleanWeb 2.0** РАСШИРЕНИЕ БРАУЗЕРА **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

CleanWeb 2.0 работает внутри расширений браузера и в реальном времени блокирует всплывающие окна согласия на cookie, видеорекламу и вредоносные скрипты перенаправления. Источник: CleanWeb 2.0 Release Notes.

9 **Нулевое хранение журналов подключений** ПОЛИТИКА БЕЗ ЖУРНАЛОВ **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Surfshark придерживается строгой политики отсутствия журналов, прошедшей независимый аудит: IP-адреса, временные метки подключений и журналы трафика не записываются. Источник: Deloitte No-Logs Audit.

10 **Динамическая ротация IP Nexus** СЕТЬ NEXUS **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Программно-определяемая сеть Surfshark Nexus динамически меняет IP-адреса пользователей каждые несколько минут, не разрывая активное VPN-соединение. Источник: Surfshark Nexus Architecture.

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

C 1. КЛИНВЕБ	D 2. ТОЛЬКО ОЗУ	G 3. МУЛЬТИХОП	F 4. КАМУФЛЯЖ
B 5. ОБХОДЧИК	A 6. КИЛЛ-СВИЧ	H 7. NEXUS NET	E 8. РОТАЦИЯ

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 КЛИНВЕБ	2 ТОЛЬКО ОЗУ	3 МУЛЬТИХОП	4 КАМУФЛЯЖ
5 БАЙПАСЕР	6 НЕКСУС		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 D – КАМУФЛЯЖ	2 F – КИЛЛСВИЧ	3 A – КЛИНВЕБ	4 E – БАЙПАСЕР
5 B – ТОЛЬКООЗУ	6 H – РОТАЦИЯ	7 C – МУЛЬТИХОП	8 G – НЕКСУС

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить КЛИНВЕБ, ТОЛЬКО ОЗУ и МУЛЬТИХОП 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

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

3 по горизонтали: РОТАЦИЯ Функция, регулярно меняющая ваш внешний IP-адрес без разрыва туннелей (7 букв)

4 по горизонтали: ТОЛЬКООЗУ Серверное оборудование с энергозависимой памятью, стирающее все данные при каждом выключении питания (9 букв)

6 по горизонтали: КИЛЛСВИЧ Автоматическая защитная функция, блокирующая сетевой трафик при сбое VPN (8 букв)

8 по горизонтали: БАЙПАСЕР Функция раздельного туннелирования, позволяющая отдельным приложениям обходить VPN (8 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: МУЛЬТИХОП Функция двойного VPN, шифрующая трафик через два разных серверных узла (9 букв)

2 по вертикали: КАМУФЛЯЖ Технология обфускации, скрывающая признаки VPN и имитирующая обычный HTTPS-трафик (8 букв)

5 по вертикали: КЛИНВЕБ Продвинутый фильтр, блокирующий рекламу, вредоносное ПО и баннеры согласия на cookie (7 букв)

7 по вертикали: НЕКСУС Собственная программно-определяемая сеть, объединяющая все серверы в единую ячеистую структуру (6 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. НЕКВБИЛ — **КЛИНВЕБ**
2. ПМОЬУИХТЛ — **МУЛЬТИХОП**
3. ПАБАСРЕЙ — **БАЙПАСЕР**
4. ССКУНЕ — **НЕКСУС**
5. ОКОУОЬТЗЛ — **ТОЛЬКООЗУ**
6. ЯЖУЛКФАМ — **КАМУФЛЯЖ**
7. КЧСВИИЛЛ — **КИЛЛСВИЧ**
8. ОАЯРИЦТ — **РОТАЦИЯ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"НЕКСУС С РОТАЦИЕЙ АЙПИ УСИЛИВАЕТ ПРИВАТНОСТЬ"

Ответы к кейсам

A КЕЙС 1: ОБХОД ФИЛЬТРОВ В КАМПУСЕ И НА РАБОТЕ

Решение для преподавателя

КРИТЕРИИ ОЦЕНИВАНИЯ И РЕКОМЕНДАЦИИ ПО РЕШЕНИЮ

- Анализ ситуации: студент обнаруживает, что Wi-Fi университетского кампуса блокирует все стандартные порты OpenVPN и WireGuard.
- Ключевой вопрос: какая функция Surfshark позволяет студенту подключаться незаметно для сетевых администраторов?
- Рекомендуемая стратегия и решение: включите Camouflage Mode (OpenVPN), который скрывает метаданные VPN, чтобы межсетевые экраны видели обычный просмотр сайтов по HTTPS.

B КЕЙС 2: ЖУРНАЛИСТСКОЕ РАССЛЕДОВАНИЕ ВЫСОКОГО РИСКА

Решение для преподавателя

КРИТЕРИИ ОЦЕНИВАНИЯ И РЕКОМЕНДАЦИИ ПО РЕШЕНИЮ

- Анализ ситуации: журналисту-расследователю нужна дополнительная защита от слежки при изучении конфиденциальных корпоративных документов.
- Ключевой вопрос: чем Dynamic MultiHop обеспечивает более высокую конфиденциальность по сравнению с маршрутизацией через один сервер?
- Рекомендуемая стратегия и решение: динамический MultiHop направляет трафик через входной и выходной серверы в двух странах, поэтому ни один отдельный сервер не может раскрыть пользователя.