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

Руководство по самым безопасным VPN

Технический анализ проектирования высокозащищённых VPN, серверов на энергозависимой памяти только на ОЗУ, защиты доступа по модели Zero Trust, частных зашифрованных средств защиты от утечек DNS и проверенных конфигураций WireGuard.

ОБЗОР ОБУЧЕНИЯ: РУКОВОДСТВО ПО САМЫМ БЕЗОПАСНЫМ 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 технические стандарты высокозащищённых VPN. Вы изучите серверное оборудование только на RAM, безопасность доступа по принципу нулевого доверия, частные зашифрованные DNS-резолверы и проверенные аудитом конфигурации WireGuard.

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/naibolee-bezopasnyy-vpn/

Ваша дорожная карта обучения: самый безопасный VPN

- Проанализируйте техническую архитектуру и стандарты шифрования в руководстве по самым защищённым VPN.
- Настройте параметры клиента, чтобы предотвратить утечки трафика IP, DNS и WebRTC.
- Сравните собственные туннельные протоколы со стандартными реализациями.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО САМЫМ БЕЗОПАСНЫМ 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: серверному оборудованию только на RAM и системам Zero Trust. Завершите работу дополнительным заданием «Думай быстро».

ИНФРАСТРУКТУРЫ ТОЛЬКО НА RAM И СЕТИ С НУЛЕВЫМ ДОВЕРИЕМ (ВВЕДЕНИЕ)

По-настоящему защищённый VPN опирается на модель zero trust, серверы только на RAM (чтобы изъятие дисков не раскрыло журналы), частные зашифрованные DNS-преобразователи и проверенные протоколы, такие как WireGuard. Эти меры вместе защищают ценные цифровые активы от угроз перехвата.

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

Контрольная точка 1: Задание с выбором ответа

1. Какая архитектура принципиальна для обеспечения наивысшей безопасности в современных VPN-серверах?

- A) Серверная инфраструктура только на RAM
- B) Хранилище на дисках
- C) Динамическая маршрутизация DNS
- D) Включение проброса портов

2. Какой протокол широко рекомендуется для самых безопасных и современных конфигураций VPN?

- A) WireGuard
- B) PPTP
- C) L2TP/IPSec
- D) SSTP

3. Какая модель безопасности требует непрерывной проверки каждого подключения без исключений?

- A) Архитектура Zero Trust
- B) Периметровые межсетевые экраны
- C) Динамическая маршрутизация
- D) Общие секретные ключи

4. Какова основная роль защиты от утечек DNS в VPN-клиенте?

- A) Направлять все DNS-запросы через частные зашифрованные преобразователи
- B) Обфускация IP-пакетов
- C) Локальное кэширование DNS-запросов
- D) Отключить серверы имён

5. Как многоузловая маршрутизация (Multi-Hop) повышает общую безопасность VPN-туннеля?

- A) Пропускает данные последовательно через два отдельных сервера
- B) Повышает скорость сжатия
- C) Шифрует данные слабыми шифрами
- D) Обходит межсетевые экраны

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Серверы, работающие только на RAM, хранят файлы журналов в кратковременной памяти, которая стирается при перезагрузке.

○ Верно ○ Неверно

7 Вопрос 7

7. WireGuard использует современные криптографические алгоритмы, менее подверженные узким местам скорости.

○ Верно ○ Неверно

8 Вопрос 8

8. Kill switch VPN работает, блокируя весь сетевой трафик при обрыве туннеля.

○ Верно ○ Неверно

9 Вопрос 9

9. Независимые аудиты третьих сторон не имеют значения для проверки обязательств по безопасности.

○ Верно ○ Неверно

10 Вопрос 10

10. Модели нулевого доверия считают все внутренние сетевые соединения безопасными по умолчанию.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Администраторы обеспечивают безопасность, внедряя строгую концепцию « _____ **».**

2. Маршрутизация пакетов через несколько точек входа требует защищённой конфигурации в режиме _____ **.**

3. Чтобы предотвратить утечку данных с украденных накопителей, применяют схему « _____ **».**

4. Перехват трафика интернет-провайдером предотвращается встроенной функцией: _____ **.**

5. Чтобы блокировать трафик при сбоях соединения, включите механизм — _____ **.**

6. Чтобы свести к минимуму хранение журналов в базах данных, выбирайте провайдера, прошедшего полный _____ **.**

СЛОВАРНЫЙ БАНК СЛОВ

АУДИТ ЗАЩИТА ДНС КИЛЛ-СВИЧ МУЛЬТИХОП НУЛЕВОЕ ДОВЕРИЕ ПРОТОКОЛ ТОЛЬКО ОЗУ ШИФРОВАНИЕ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о VPN и сетях

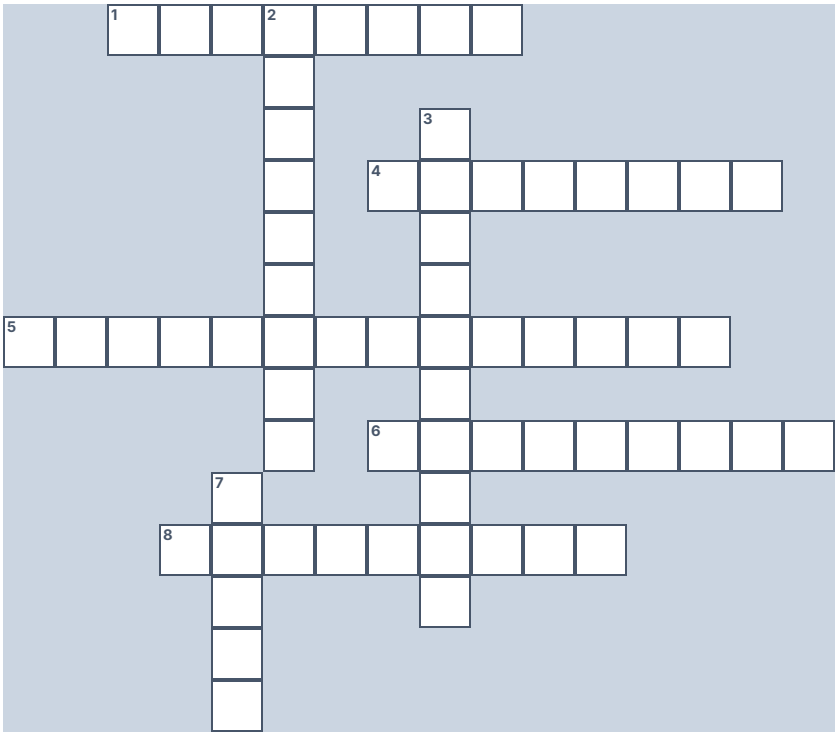
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. Нулевое доверие	A	Независимо проверенная конфигурация, подтверждающая, что журналы не хранятся.
☐	2. Multi-Hop	B	Криптографическое искажение полезной нагрузки данных для защиты при передаче.
☐	3. Сервер только на RAM	C	Модель безопасности, требующая непрерывной аутентификации всех пользователей.
☐	4. Защита DNS	D	Набор технических правил, определяющих, как данные упаковываются и отправляются.
☐	5. Kill Switch	E	Каскадная маршрутизация VPN, связывающая два серверных узла в цепочку.
☐	6. Система, прошедшая аудит	F	Серверная архитектура, использующая энергозависимую память для хранения полезных данных.
☐	7. Шифрование	G	Принудительные частные DNS-запросы для защиты поиска по серверам имён.
☐	8. Протокол	H	Отказоустойчивый механизм, блокирующий трафик при сбое VPN.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

1. Набор технических правил, определяющих, как данные упаковываются и отправляются (8)

4. Защитный механизм, блокирующий трафик при сбое VPN (8)

5. Концепция безопасности, требующая постоянной аутентификации всех пользователей (14)

6. Принудительные приватные DNS-запросы для защиты поиска по серверам имён (9)

8. Каскадная маршрутизация VPN, соединяющая в цепочку два серверных узла (9)

ПО ВЕРТИКАЛИ

2. Серверная архитектура, использующая энергозависимую память для хранения данных (9)

3. Криптографическое преобразование полезной нагрузки данных для защиты при передаче (10)

7. Независимая проверка настроек, подтверждающая, что логи не хранятся (5)

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: Набор технических правил, определяющих, как данные упаковываются и отправляются (8 букв):

4 по горизонтали: Защитный механизм, блокирующий трафик при сбое VPN (8 букв):

5 по горизонтали: Концепция безопасности, требующая постоянной аутентификации всех пользователей (14 букв):

6 по горизонтали: Принудительные приватные DNS-запросы для защиты поиска по серверам имён (9 букв):

8 по горизонтали: Каскадная маршрутизация VPN, соединяющая в цепочку два серверных узла (9 букв):

ПО ВЕРТИКАЛИ

2 по вертикали: Серверная архитектура, использующая энергозависимую память для хранения данных (9 букв):

3 по вертикали: Криптографическое преобразование полезной нагрузки данных для защиты при передаче (10 букв):

7 по вертикали: Независимая проверка настроек, подтверждающая, что логи не хранятся (5 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

НУЛЕВОЕДОВЕРИЕ МУЛЬТИХОП ТОЛЬКООЗУ ЗАЩИТАДНС КИЛЛСВИЧ
АУДИТ ШИФРОВАНИЕ ПРОТОКОЛ

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. НУЛЕВОЕДОВЕРИЕ**
- **B. МУЛЬТИХОП**
- **C. ТОЛЬКООЗУ**
- **D. ЗАЩИТАДНС**
- **E. КИЛЛСВИЧ**
- **F. АУДИТ**
- **G. ШИФРОВАНИЕ**
- **H. ПРОТОКОЛ**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Защитный механизм, блокирующий трафик при сбое VPN.

_____ 2. Принудительные приватные DNS-запросы для защиты поиска по серверам имён.

_____ 3. Каскадная маршрутизация VPN, соединяющая в цепочку два серверных узла.

_____ 4. Набор технических правил, определяющих, как данные упаковываются и отправляются.

_____ 5. Криптографическое преобразование полезной нагрузки данных для защиты при передаче.

_____ 6. Серверная архитектура, использующая энергозависимую память для хранения данных.

_____ 7. Независимая проверка настроек, подтверждающая, что логи не хранятся.

_____ 8. Концепция безопасности, требующая постоянной аутентификации всех пользователей.

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. ЕОДВЕЛУОРН ИЕВЕ
2. УТЗЬОООКЛ
3. ЛИКСВЧИЛ
4. ВИОЕРНАШИ Ф
5. ХТУПИЬМОЛ
6. НИАДАЗТСЩ
7. ИТАДУ
8. ТРОЛПОКО

Дополнительное задание: Думай быстро

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

1	Замки или ключи, которыми вы пользуетесь каждый день			
2	То, что может скрыть VPN			
3	То, что делает VPN безопасным			
4	Мифы о VPN			
5	Причины использовать VPN в путешествии			
6	Безопасные места в реальном мире			
7	Слова со значением «защищённый»			
8	Обещания, которые даёт хороший VPN-провайдер			
9	Слова, связанные с конфиденциальностью			
10	Виды аудита или проверки			
11	Слова из этого рабочего листа, которые вы хотите запомнить			
12	То, что хочет украсть хакер			
13	Способы распознать поддельную сеть Wi-Fi			
14	Места, где вы пользовались бы VPN			
15	То, что может видеть ваш интернет-провайдер			

Контрольная точка 8: Кейсы по VPN и сетям

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: УКРЕПЛЕНИЕ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ



Ситуация: Банк перестраивает топологию удалённого доступа. Ему нужна архитектура Zero Trust, связывающая все клиентские устройства с защищёнными серверами.

Вопрос для обсуждения: В чём главное преимущество микросегментации сети в рамках модели Zero Trust VPN?

КЕЙС 2: ЗАЩИТА СЕРВЕРОВ «ТОЛЬКО RAM»



Ситуация: Провайдер VPN, ориентированный на безопасность, обновляет свои серверы, чтобы физическое изъятие сервера не раскрывало истории журналов пользователей.

Вопрос для обсуждения: Объясните, как конфигурации оборудования только с оперативной памятью (RAM-Only) предотвращают извлечение данных криминалистами при физическом изъятии серверов.

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

9	1	27	10	27	7	15	15	29	6		3	17	15

16	23	18	1	15	33	32	20		24	6	15	15	29	6

24	10	22	18	16	3	29	6		1	12	20	10	3	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 о виртуальных частных сетях (VPN) и туннелировании.

Q1: Что делает VPN «самым безопасным»?

Сочетание модели Zero Trust, серверов только на RAM и проверенных протоколов.

Q2: Что такое серверы только на RAM?

Серверы, работающие в энергозависимой памяти и не сохраняющие журналы на диск.

Q3: Что такое VPN с нулевым доверием?

Модель, непрерывно проверяющая каждый запрос доступа и каждое подключение.

Q4: Почему WireGuard считается безопасным?

Имеет небольшую кодовую базу, которую легко проверить, и использует современные шифры.

Q5: Как защищённые VPN предотвращают утечки DNS?

Направляя все запросы через частные зашифрованные DNS-резолверы.

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

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

Q6: Нужны ли аудиты защищённому VPN?

Да, независимые аудиты подтверждают заявления об отсутствии журналов и безопасность кода.

Q7: Какую роль играет kill switch?

Немедленно останавливает сетевой трафик, если VPN-подключение обрывается.

Q8: Какое шифрование используется в защищённых VPN?

AES-256 и ChaCha20 — отраслевые стандарты шифрования.

Q9: Безопасна ли маршрутизация Multi-Hop?

Да, он объединяет два или более серверов в цепочку, чтобы затруднить анализ трафика.

Q10: Чем помогает офшорная юрисдикция?

Может ограничить круг применимых законов, но не даёт абсолютного иммунитета.

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

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

Q1: Как серверы только на RAM снижают риски изъятия данных?

Поскольку они работают на RAM, отключение питания стирает данные, хранящиеся в памяти.

Q2: Как Zero Trust заменяет стандартную периметровую защиту?

Считает каждый клиент враждебным и требует постоянной аутентификации.

Q3: Почему кодовую базу WireGuard проще проверять?

Его код для Linux занимает менее 4,000 строк, что намного меньше типичных VPN-стеков. [4]

Q4: Как DNSSEC защищает DNS-запросы?

Подписывает записи DNS, чтобы резолверы могли обнаружить поддельные или изменённые ответы.

Q5: Как Multi-Hop усложняет корреляцию трафика?

Разделяя входящие и исходящие IP-адреса между разными хостинг-провайдерами.

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

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

Q6: Почему юрисдикции «Пяти глаз» рискованны для VPN?

Государства-участники обмениваются разведданными и могут использовать судебные предписания для получения данных пользователей.

Q7: Как kill switch реализуется на уровне ядра?

Использует правила системного брандмауэра (например, iptables или WFP) для блокировки исходящего трафика.

Q8: Что такое прямая секретность при VPN-рукопожатии?

Генерирует уникальные сеансовые ключи, чтобы прошлые сеансы нельзя было расшифровать.

Q9: Как защищённые VPN снижают риск утечек WebRTC?

Блокируя запросы WebRTC или направляя их через туннель.

Q10: Как независимые аудиты обеспечивают соблюдение требований конфиденциальности?

Аудиторы проводят тестирование на проникновение и проверяют конфигурации серверов.

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

Серверы, работающие только на RAM, загружают операционную систему в память при запуске, поэтому после перезагрузки на диске ничего не остаётся.

2. АНАЛИЗ VPN

WireGuard использует среду Noise с Curve25519, ChaCha20, Poly1305, BLAKE2s и HKDF. [3]

3. АНАЛИЗ VPN

Нулевое доверие предоставляет доступ к каждому ресурсу отдельно и не предполагает неявного доверия на основе расположения в сети (NIST SP 800-207). [1]

4. АНАЛИЗ VPN

В разведывательный альянс «Пять глаз» входят США, Великобритания, Канада, Австралия и Новая Зеландия.

5. АНАЛИЗ VPN

Утечки WebRTC происходят, когда браузеры раскрывают настоящий публичный IP-адрес клиента через запросы STUN.

6. АНАЛИЗ VPN

Совершенная прямая секретность (PFS) гарантирует, что компрометация долговременного ключа не раскроет прошлые ключи сеансов. [3]

7. VPN: ВАЖНО ЗНАТЬ

Cure53, берлинская компания по безопасности, опубликовала аудиты нескольких VPN-провайдеров.

8. VPN: ВАЖНО ЗНАТЬ

Утечки DNS возникают, когда DNS-запросы обходят VPN-туннель и попадают на серверы имён локального провайдера.

9. VPN: ВАЖНО ЗНАТЬ

Энергозависимым микросхемам RAM для хранения данных нужно постоянное электропитание, и при выключении их содержимое теряется.

10. АНАЛИЗ VPN

Корпоративные системы Zero Trust проводят проверки состояния устройства, прежде чем разрешить подключение к защищённым ресурсам. [1]

Технические ссылки и источники

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

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/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] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

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

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Сервер только на RAM** ТОЛЬКО RAM **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Серверы, работающие только на RAM, не хранят журналы на диске, а при перезагрузке данные стираются. Источник: Most Secure VPN.

2 **Вопрос 2** **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard сочетает небольшую, доступную для аудита кодовую базу с современными шифрами.

3 **Модель нулевого доверия** НУЛЕВОЕ ДОВЕРИЕ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Модели нулевого доверия постоянно проверяют соответствие устройства требованиям перед предоставлением доступа. Источник: Most Secure VPN.

4 **Защита DNS** ЗАЩИТА DNS **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Защита от утечек DNS направляет поисковые запросы через частные резолверы. Источник: Most Secure VPN.

5 **Туннели Multi-Hop** MULTI-HOP **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Маршрутизация Multi-Hop последовательно связывает два отдельных серверных узла. Источник: самые безопасные VPN.

Ответы: контрольная точка 2 – верно или неверно

6 **Сервер только на RAM** ТОЛЬКО RAM — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Серверное оборудование, работающее только на RAM, ничего не записывает на диск, а при перезагрузке данные стираются. Источник: Most Secure VPN.

7 **Скорость WireGuard** WIREGUARD — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard использует современную криптографию, которая избегает узких мест обработки. Источник: Most Secure VPN.

8 **Kill Switch** АВАРИЙНЫЙ ВЫКЛЮЧАТЕЛЬ — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Kill switch блокирует весь трафик при обрыве VPN-соединения. Источник: Most Secure VPN.

9 **Аудит третьими сторонами** АУДИТЫ НЕОБХОДИМЫ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Аудит третьими сторонами необходим для проверки заявлений компаний о конфиденциальности. Источник: Most Secure VPN.

10 **Вопрос 10** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Zero Trust не предоставляет неявного доверия на основе местоположения в сети.

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. Нулевое доверие	E 2. Multi-Hop	F 3. Сервер только на RAM	G 4. Защита DNS
H 5. Kill Switch	A 6. Система, прошедшая аудит	B 7. Шифрование	D 8. Протокол

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 НУЛЕВОЕ ДОВЕРИЕ	2 МУЛЬТИХОП	3 ТОЛЬКО ОЗУ	4 ЗАЩИТА ДНС
5 КИЛЛ-СВИЧ	6 АУДИТ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 E – КИЛЛСВИЧ	2 D – ЗАЩИТАДНС	3 B – МУЛЬТИХОП	4 H – ПРОТОКОЛ
5 G – ШИФРОВАНИЕ	6 C – ТОЛЬКООЗУ	7 F – АУДИТ	8 A – НУЛЕВОЕДОВЕРИЕ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить Нулевое доверие, Multi-Hop и Сервер только на RAM и привести пример для каждого термина.

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

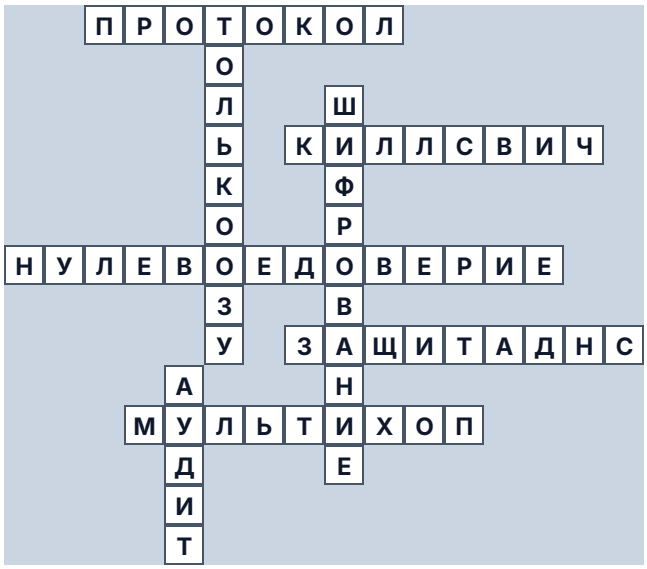
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

1 по горизонтали: ПРОТОКОЛ Набор технических правил, определяющих, как данные упаковываются и отправляются (8 букв)

4 по горизонтали: КИЛЛСВИЧ Защитный механизм, блокирующий трафик при сбое VPN (8 букв)

5 по горизонтали: НУЛЕВОЕДОВЕРИЕ Концепция безопасности, требующая постоянной аутентификации всех пользователей (14 букв)

6 по горизонтали: ЗАЩИТАДНС Принудительные приватные DNS-запросы для защиты поиска по серверам имён (9 букв)

8 по горизонтали: МУЛЬТИХОП Каскадная маршрутизация VPN, соединяющая в цепочку два серверных узла (9 букв)

ПО ВЕРТИКАЛИ

2 по вертикали: ТОЛЬКООЗУ Серверная архитектура, использующая энергозависимую память для хранения данных (9 букв)

3 по вертикали: ШИФРОВАНИЕ Криптографическое преобразование полезной нагрузки данных для защиты при передаче (10 букв)

7 по вертикали: АУДИТ Независимая проверка настроек, подтверждающая, что логи не хранятся (5 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЕОДВЕЛУОРНИЕВЕ — **НУЛЕВОЕДОВЕРИЕ**
2. УТЗЬОООКЛ — **ТОЛЬКООЗУ**
3. ЛИКСВЧИЛ — **КИЛЛСВИЧ**
4. ВИОЕРНАШИФ — **ШИФРОВАНИЕ**
5. ХТУПИЬМОЛ — **МУЛЬТИХОП**
6. НИАДАЗТСЩ — **ЗАЩИТАДНС**
7. ИТАДУ — **АУДИТ**
8. ТРОЛПОКО — **ПРОТОКОЛ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЗАЩИЩЁННЫЕ ВПН ОХРАНЯЮТ ЦЕННЫЕ ЦИФРОВЫЕ АКТИВЫ"

Ответы к кейсам

A КЕЙС 1: УКРЕПЛЕНИЕ КОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: корпоративный банк перестраивает топологию удалённого доступа. Ему нужна архитектура нулевого доверия, связывающая все клиентские устройства с защищёнными серверами.
- Рекомендуемая стратегия и решение: Критерии проверки: объясните, что микросегментация ограничивает доступ определёнными ресурсами и не позволяет угрозе распространяться по сети, если устройство скомпрометировано.

B КЕЙС 2: ЗАЩИТА СЕРВЕРОВ «ТОЛЬКО RAM»

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: VPN-провайдер, ориентированный на безопасность, модернизирует свои серверы, чтобы изъятие серверов не раскрывало историю журналов пользователей.
- Рекомендуемая стратегия и решение: Критерии проверки: укажите, что в RAM-only серверах нет физических дисков. При отключении питания все временные данные в энергозависимой памяти стираются автоматически.