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

Лучший VPN для бизнеса

Практический обзор безопасности, масштабируемости и централизованного администрирования бизнес-VPN.

УЧЕБНЫЙ ОБЗОР: ЛУЧШИЙ VPN ДЛЯ БИЗНЕСА

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 Business VPN и сети удалённого доступа. Вы изучите архитектуры Zero Trust, туннели IPsec между площадками, платформы SASE, многофакторный вход и проверки безопасности конечных точек.

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/luchshiy-vpn-dlya-biznesa/

Ваша дорожная карта обучения: бизнес-VPN

- Определите ведущих провайдеров бизнес-VPN и их функции для команд.
- Проанализируйте различия между конфиденциальностью потребительских VPN и административными средствами управления для бизнеса.
- Различайте VPN удалённого доступа и корпоративные туннели «сеть — сеть».

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО БИЗНЕС-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: корпоративным решениям для удалённого доступа. Завершите работу дополнительным заданием «Думай быстро».

КОРПОРАТИВНЫЙ УДАЛЁННЫЙ ДОСТУП И ЗАЩИЩЁННАЯ ГРАНИЦА СЕТИ (ВВЕДЕНИЕ)

Для защиты корпоративного удалённого доступа необходимо перейти от традиционных VPN-моделей на основе периметра к архитектурам нулевого доверия (Zero Trust). Строгая многофакторная аутентификация (MFA) и модели Secure Access Service Edge (SASE) защищают важные активы от скомпрометированных конечных устройств.

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

Контрольная точка 1: Задание с выбором ответа

1. Какой тип бизнес-VPN соединяет сети целых офисов друг с другом?

- A. VPN между площадками (Site-to-Site)
- B. VPN для удалённого доступа
- C. Потребительский VPN
- D. Smart DNS

2. Какой вариант выделен как лучший в целом для бизнес-команд?

- A. NordLayer
- B. Surfshark
- C. Proton VPN
- D. Private Internet Access

3. От чего защищает бизнес-команды выделенный статический IP-адрес?

- A. Занесение IP-адресов в чёрный список
- B. Скорость маршрутизатора падает
- C. Сжатие данных
- D. Обновления клиента

4. Какой провайдер отмечен как лучший для выделенной инфраструктуры?

- A. Proton VPN
- B. NordLayer
- C. Surfshark
- D. Private Internet Access

5. Какая функция предоставляет централизованную панель администратора для управления пользователями?

- A. Административные средства управления
- B. Перенаправление портов
- C. Эмуляция маршрутизатора
- D. Раздельное туннелирование

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. VPN удалённого доступа позволяют отдельным сотрудникам подключаться из любого места.

○ Верно ○ Неверно

7 Вопрос 7

7. Потребительские VPN защищают всю организацию с помощью одной панели администратора.

○ Верно ○ Неверно

8 Вопрос 8

8. Выделенные IP-адреса отделяют трафик компании от общего публичного трафика.

○ Верно ○ Неверно

9 Вопрос 9

9. Private Internet Access выделяется как лучший вариант для крупных предприятий.

○ Верно ○ Неверно

10 Вопрос 10

10. SASE объединяет маршрутизацию WAN с облачными системами безопасности.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Лучший по общему рейтингу провайдер для бизнес-команд — это _____ .

2. Для объединения нескольких филиалов компании используется туннель типа _____ .

3. Чтобы адрес не попал в чёрный список, команды разворачивают выделенный _____ .

4. Администраторы управляют разрешениями устройств через центральную _____ .

5. Динамическое добавление рабочих мест для растущих команд — это _____ .

6. Выполнение нормативных требований и стандартов аудита данных называется _____ .

СЛОВАРНЫЙ БАНК СЛОВ

МАРШРУТИЗАЦИЯ МАСШТАБИРУЕМОСТЬ ПАНЕЛЬ УПРАВЛЕНИЯ САЙТ-САЙТ
СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СТАТИЧНЫЙ АДРЕС ШЛЮЗ NORDLAYER

Напишите свои ответы здесь:

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

Контрольная точка 4: Сопоставление ключевых понятий

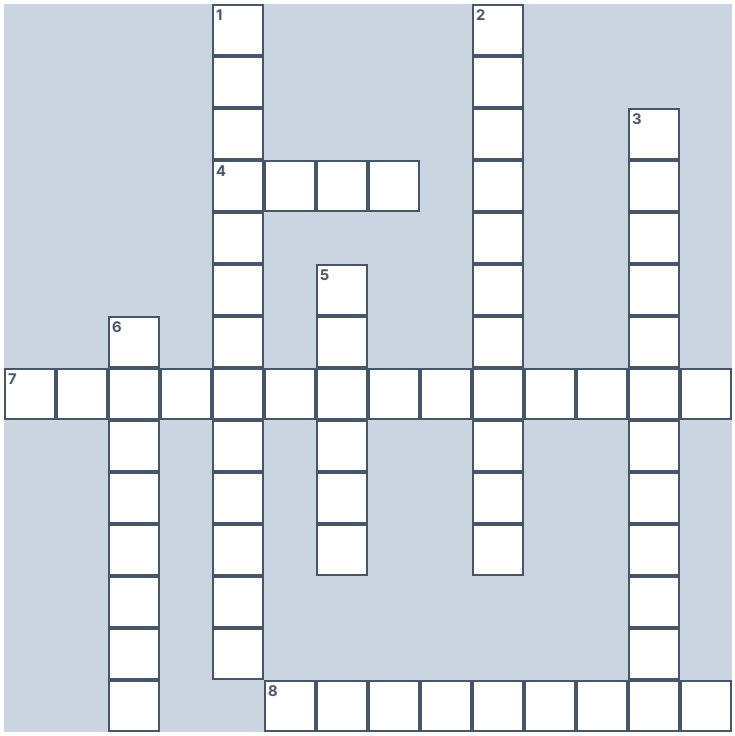
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. NORDLAYER	A	Динамический рост команды с несколькими местами.
☐	2. МЕЖДУ САЙТАМИ	B	Лучший выбор для бизнеса в целом.
☐	3. СТАТИЧЕСКИЙ IP	C	Управление трафиком с помощью раздельного туннелирования.
☐	4. ПАНЕЛЬ УПРАВЛЕНИЯ	D	Стандартный аудит по нормативным требованиям.
☐	5. МАСШТАБИРУЕМОСТЬ	E	Удалённый узел входа для аутентификации.
☐	6. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ	F	Выделенный адрес, не занесённый в чёрные списки.
☐	7. МАРШРУТИЗАЦИЯ	G	Туннель для соединения офисных сетей.
☐	8. ШЛЮЗ	H	Центральная консоль администратора.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

4. Узел удалённого входа с аутентификацией (4)

7. Выделенный адрес, не попавший в чёрные списки (14)

8. Лучший выбор для бизнеса в целом (9)

ПО ВЕРТИКАЛИ

1. Управление трафиком при раздельном туннелировании (13)

2. Динамическое добавление рабочих мест по мере роста команды (11)

3. Соблюдение нормативных требований и стандартов аудита (12)

5. Центральная консоль управления для администраторов (6)

6. Туннель для объединения сетей офисов (8)

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

4 по горизонтали: Узел удалённого входа с аутентификацией (4 букв):

7 по горизонтали: Выделенный адрес, не попавший в чёрные списки (14 букв):

8 по горизонтали: Лучший выбор для бизнеса в целом (9 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Управление трафиком при раздельном туннелировании (13 букв):

2 по вертикали: Динамическое добавление рабочих мест по мере роста команды (11 букв):

3 по вертикали: Соблюдение нормативных требований и стандартов аудита (12 букв):

5 по вертикали: Центральная консоль управления для администраторов (6 букв):

6 по вертикали: Туннель для объединения сетей офисов (8 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

НОРДЛЕЙЕР САЙТСАЙТ СТАТИЧНЫЙАДРЕС ПАНЕЛЬ РОСТКОМАНДЫ
СООТВЕТСТВИЕ МАРШРУТИЗАЦИЯ ШЛЮЗ

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. НОРДЛЕЙЕР

B. САЙТСАЙТ

C. СТАТИЧНЫЙАДРЕС

D. ПАНЕЛЬ

E. РОСТКОМАНДЫ

F. СООТВЕТСТВИЕ

G. МАРШРУТИЗАЦИЯ

H. ШЛЮЗ

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Управление трафиком при раздельном туннелировании.

_____ 2. Центральная консоль управления для администраторов.

_____ 3. Узел удалённого входа с аутентификацией.

_____ 4. Выделенный адрес, не попавший в чёрные списки.

_____ 5. Соблюдение нормативных требований и стандартов аудита.

_____ 6. Туннель для объединения сетей офисов.

_____ 7. Лучший выбор для бизнеса в целом.

_____ 8. Динамическое добавление рабочих мест по мере роста команды.

Контрольная точка 7: Задание с перепутанными словами

Расставьте буквы ниже в правильном порядке, чтобы получить ключевые понятия этого листа. Запишите ответы в предусмотренные поля.

1. ЕЛДОНЙЕРР
2. ИТЧАНЕСРЫСАДЙТ
3. РМОАСОДЫКНТ
4. УИЗРИРЯТЦАМАШ
5. СААТТСЙЙ
6. ЛЕПНЬА
7. СТВСОТЕВИОЕТ
8. ШЗЮЛ

Дополнительное задание: Думай быстро

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

1	Обещания, которые даёт хороший VPN-провайдер			
2	То, что может нарушить видеовстречу			
3	Правила безопасной удалённой работы			
4	Известные вам офисные программы			
5	То, что может видеть ваш интернет-провайдер			
6	Причины предоставить сотрудникам VPN			
7	От чего VPN не может вас защитить			
8	Места, откуда работают сотрудники			
9	Инструменты, которыми компания пользуется каждый день			
10	Способы безопасного входа в систему			
11	Данные, которые компания обязана защищать			
12	Роли в ИТ-отделе			
13	Устройства, которые могут быть у сотрудника			
14	Что делать после утечки данных или взлома			
15	Слова, описывающие Zero Trust			

Контрольная точка 8: Кейсы по VPN и сетям

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ВНЕСЕНИЕ ОБЩЕГО ПУБЛИЧНОГО IP В ЧЁРНЫЙ СПИСОК



Ситуация: Отдел продаж обращается к корпоративным базам данных через потребительский VPN, но оказывается заблокирован, потому что общий выходной IP попал в чёрный список систем защиты от мошенничества.

Вопрос для обсуждения: Предложите конфигурацию бизнес-инфраструктуры VPN, чтобы устранить эту блокировку.

КЕЙС 2: СОЕДИНЕНИЕ КОРПОРАТИВНЫХ ОФИСОВ



Ситуация: Крупная компания с офисами в Мюнхене и Бостоне должна безопасно обмениваться данными на локальных файловых серверах, не пуская трафик через открытые веб-пространства.

Вопрос для обсуждения: выберите подходящую топологию бизнес-VPN.

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	21	13	6	3	16	6		5	16	3	6	18	10	6

9	1	27	10	27	1	6	20		19	6	20	10

17	18	6	5	17	18	10	33	20	10	11

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 бизнес-VPN?

Защищённое сетевое подключение, позволяющее удалённым сотрудникам и офисам безопасно получать доступ к частным корпоративным данным.

Q2: Чем потребительские и бизнес-VPN отличаются?

Потребительские VPN скрывают личный веб-серфинг; бизнес-VPN защищают корпоративные системы с помощью центральных консолей администратора.

Q3: Что такое VPN типа «сеть — сеть»?

Туннель, соединяющий сети целых физических офисов друг с другом через интернет.

Q4: Что такое VPN удалённого доступа?

Туннель, позволяющий отдельным удалённым сотрудникам безопасно подключаться к сети компании.

Q5: В чём польза выделенного статического IP-адреса?

Отделяет корпоративный трафик от публичных пулов и позволяет избежать попадания общих IP-адресов в чёрные списки.

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

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

Q6: Какой провайдер лучше всего подходит для малого бизнеса?

Private Internet Access (PIA), отмечаемый доступностью для небольших команд и простотой настройки.

Q7: Какой бизнес-VPN занимает 1-е место в общем рейтинге?

NordLayer, получивший от VPN.com 92/100 за функции и инструменты администрирования.

Q8: Что такое масштабируемость VPN для команд?

Возможность динамически добавлять рабочие места пользователей, лицензии и шлюзы по мере роста компании.

Q9: Почему так важно централизованное управление?

Позволяет администраторам применять политики безопасности и отзывать доступ сотрудников в одной панели.

Q10: Что такое SASE?

Secure Access Service Edge — архитектура, объединяющая маршрутизацию WAN с облачными службами безопасности.

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

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

Q1: Как раздельное туннелирование защищает команды?

Оставляет частный трафик SaaS внутри защищённого туннеля, а публичный веб-доступ направляет локально.

Q2: Что Proton VPN предлагает бизнесу?

Инфраструктура выделенных серверов, оценка VPN.com — 88/100 (базируется в Швейцарии).

Q3: Какие стандарты соответствия требуют использования VPN?

PCI DSS требует надёжного шифрования в общедоступных сетях; HIPAA и GDPR ожидают его как меру защиты.

Q4: Можно ли запускать бизнес-VPN на маршрутизаторах?

Да, настройка VPN-туннелей на роутерах автоматически защищает все устройства в офисе.

Q5: Что такое многофакторная аутентификация?

Требование нескольких факторов (например, смарт-карт или SMS-кодов) для подтверждения входа.

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

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

Q6: Почему общие IP-адреса попадают в чёрные списки?

Потому что ими пользуются тысячи людей, среди которых могут быть те, кто совершает вредоносные действия.

Q7: Как шлюз аутентифицирует пользователей?

Проверяя клиентские сертификаты, пароли и коды многофакторной аутентификации по активным каталогам.

Q8: Что Surfshark предлагает командам?

Лучший выбор VPN.com среди пакетов безопасности с оценкой 84/100 и серверами только на RAM.

Q9: Как проводить аудит бизнес-VPN-подключений?

Просматривая журналы подключений, показатели использования данных и историю входов в консоли администратора.

Q10: Что такое контроль доступа Zero Trust?

Парадигма, в которой все устройства считаются недоверенными и для каждого сеанса требуется проверка.

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

Бизнес-VPN шифрует трафик и защищает корпоративные системы от перехвата в общедоступных сетях.

2. АНАЛИЗ VPN

VPN типа «сеть — сеть» (Site-to-Site) безопасно объединяют сети целых филиалов, не открывая локальные узлы.

3. АНАЛИЗ VPN

Потребительские VPN маскируют личный веб-серфинг, тогда как бизнес-VPN защищают шлюзы корпоративных ресурсов.

4. АНАЛИЗ VPN

VPN.com оценивает NordLayer в 92/100 как лучший VPN для бизнеса в целом.

5. АНАЛИЗ VPN

VPN.com оценивает Proton VPN в 88/100 и называет его лучшим для выделенной инфраструктуры.

6. АНАЛИЗ VPN

VPN.com оценивает Private Internet Access в 76/100 и ставит его на первое место для команд малого бизнеса.

7. VPN: ВАЖНО ЗНАТЬ

Центральные панели администратора позволяют специалистам по безопасности управлять правами пользователей и правилами доступа.

8. VPN: ВАЖНО ЗНАТЬ

Выделенные статические IP-адреса не дают антифрод-системам блокировать команды из-за общих IP.

9. VPN: ВАЖНО ЗНАТЬ

GDPR называет шифрование одной из надлежащих мер защиты персональных данных.

10. АНАЛИЗ VPN

Архитектуры нулевого доверия проверяют все удалённые конечные точки независимо от их расположения и учётных данных.

Технические ссылки и источники

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

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.
https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.
https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.
https://nordlayer.com/

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Топология туннеля** МЕЖДУ САЙТАМИ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN типа «сеть — сеть» (Site-to-Site) безопасно соединяют друг с другом целые удалённые филиалы. Источник: NIST Zero Trust.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN.com оценивает NordLayer в 92/100 и ставит его лучшим в целом для бизнес-команд.

3 **Белый список IP** ВЫДЕЛЕННЫЙ IP — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Выделенные статические IP не дают командам потерять доступ из-за общих чёрных списков IP. Источник: NIST Remote Access.

4 **Вопрос 4** — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN.com оценивает Proton VPN в 88/100 и называет его лучшим для выделенной инфраструктуры.

5 **Центральная консоль** АДМИНИСТРАТИВНЫЕ ЭЛЕМЕНТЫ УПРАВЛЕНИЯ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Централизованные панели позволяют специалистам по безопасности управлять правами пользователей и местами. Источник: NIST Remote Access.

Ответы: контрольная точка 2 – верно или неверно

6 **Удалённые подключения** УДАЛЁННЫЙ ДОСТУП — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN удалённого доступа позволяют отдельным удалённым сотрудникам подключаться к частным серверам. Источник: NIST Remote Access.

7 **Корпоративные туннели** ПОТРЕБИТЕЛЬСКИЕ ЛИМИТЫ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В потребительских VPN нет централизованных средств управления администратора, и они не подходят для аудита организаций. Источник: CISA Infrastructure.

8 **Изоляция шлюза** ВЫДЕЛЕННЫЙ ТУННЕЛЬ — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Выделенные IP отделяют трафик компании от общего шума, защищая базы данных. Источник: NIST Zero Trust.

9 **Вопрос 9** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN.com ставит PIA (76/100) лучшим для малого бизнеса, а не для крупных предприятий.

10 **Объединение систем безопасности** СТАНДАРТ SASE — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

SASE объединяет маршрутизацию корпоративной WAN с облачной защитой по принципу нулевого доверия. Источник: Cloudflare Zero Trust.

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

B 1. NORDLAYER	G 2. МЕЖДУ САЙТАМИ	F 3. СТАТИЧЕСКИЙ IP	H 4. ПАНЕЛЬ УПРАВЛЕНИЯ
A 5. МАСШТАБИРУЕМОСТЬ	D 6. СООТВЕТСТВИЕ ТРЕБОВАНИЯМ	C 7. МАРШРУТИЗАЦИЯ	E 8. ШЛЮЗ

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 NORDLAYER	2 САЙТ-САЙТ	3 СТАТИЧНЫЙ АДРЕС	4 ПАНЕЛЬ УПРАВЛЕНИЯ
5 МАСШТАБИРУЕМОСТЬ	6 СООТВЕТСТВИЕ ТРЕБОВАНИЯМ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 G – МАРШРУТИЗАЦИЯ	2 D – ПАНЕЛЬ	3 H – ШЛЮЗ	4 C – СТАТИЧНЫЙАДРЕС
5 F – СООТВЕТСТВИЕ	6 B – САЙТСАЙТ	7 A – НОРДЛЕЙЕР	8 E – РОСТКОМАНДЫ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить NORDLAYER, МЕЖДУ САЙТАМИ и СТАТИЧЕСКИЙ IP 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

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

РЕШЕНИЕ КРОССВОРДА

			М					Р						
			А					О						
			Р					С				С		
			Ш	Л	Ю	З		Т				О		
			Р					К				О		
			У		П			О				Т		
		С	Т		А			М				В		
С	Т	А	Т	И	Ч	Н	Ы	Й	А	Д	Р	Е	С	
		Й		З		Е			Н			Т		
		Т		А		Л			Д			С		
		С		Ц		Ь			Ы			Т		
		А		И								В		
		Й		Я								И		
		Т			Н	О	Р	Д	Л	Е	Й	Е	Р	

РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

4 по горизонтали: ШЛЮЗ Узел удалённого входа с аутентификацией (4 букв)

7 по горизонтали: СТАТИЧНЫЙАДРЕС Выделенный адрес, не попавший в чёрные списки (14 букв)

8 по горизонтали: НОРДЛЕЙЕР Лучший выбор для бизнеса в целом (9 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: МАРШРУТИЗАЦИЯ Управление трафиком при раздельном туннелировании (13 букв)

2 по вертикали: РОСТКОМАНДЫ Динамическое добавление рабочих мест по мере роста команды (11 букв)

3 по вертикали: СООТВЕТСТВИЕ Соблюдение нормативных требований и стандартов аудита (12 букв)

5 по вертикали: ПАНЕЛЬ Центральная консоль управления для администраторов (6 букв)

6 по вертикали: САЙТСАЙТ Туннель для объединения сетей офисов (8 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЕЛДОНЙЕРР — НОРДЛЕЙЕР
2. ИТЧАНЕСРЫСАДЙТ — СТАТИЧНЫЙАДРЕС
3. РМОАСОДЫКНТ — РОСТКОМАНДЫ
4. УИЗРИРЯТЦАМАШ — МАРШРУТИЗАЦИЯ
5. САТТСЙЙ — САЙТСАЙТ
6. ЛЕПНЬА — ПАНЕЛЬ
7. СТВСОТЕВИОЕТ — СООТВЕТСТВИЕ
8. ШЗЮЛ — ШЛЮЗ

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"НУЛЕВОЕ ДОВЕРИЕ ЗАЩИЩАЕТ СЕТИ ПРЕДПРИЯТИЙ"

Ответы к кейсам

A Кейс 1: Внесение общего публичного IP в чёрный список

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: отдел продаж получает доступ к корпоративным базам данных через потребительский VPN, но блокируется, так как общий выходной IP попал в чёрный список систем защиты от мошенничества.
- Рекомендуемая стратегия и решение: используйте выделенные бизнес-серверы со статическим IP-адресом, чтобы отделить корпоративный трафик от общих пулов.

B Кейс 2: Соединение корпоративных офисов

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: компании с офисами в Мюнхене и Бостоне нужно безопасно обмениваться данными на локальных файловых серверах, не пропуская трафик через открытые веб-пространства.
- Рекомендуемая стратегия и решение: настройте VPN-туннель «сеть — сеть», чтобы безопасно соединить две локальные офисные сети через интернет.