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

Корпоративный VPN

Внедрение доступа к сети с нулевым доверием, выделенных шлюзовых узлов и централизованного корпоративного администрирования.

ОБЗОР ТЕМЫ: КОРПОРАТИВНЫЕ VPN-СЕТИ

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 корпоративные VPN-сети. Вы изучите архитектуры нулевого доверия, выделенные шлюзы со статическими IP, консоли администратора, предоставление доступа и туннели IPsec «сеть — сеть».

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/korporativnyy/

Ваша дорожная карта обучения: корпоративная VPN-сеть

- Внедрите системы доступа к сети с нулевым доверием (ZTNA).
- Настройте IP-адреса шлюзов выделенных серверов для фильтров белых списков.
- Управляйте централизованными корпоративными административными панелями и списками мест пользователей.
- Проверьте журналы доступа к сети и историю подключений пользователей.
- Настройте правила единого входа (SSO) и многофакторной аутентификации.
- Настройте туннели IPsec между филиалами по схеме site-to-site.

ИНСТРУКЦИИ: КОРПОРАТИВНЫЕ VPN-СЕТИ

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: Zero Trust и IPsec между сетями. Завершите работу дополнительным заданием «Думай быстро».

АРХИТЕКТУРЫ НУЛЕВОГО ДОВЕРИЯ И ВЫДЕЛЕННЫЕ ШЛЮЗЫ (ВВЕДЕНИЕ)

Корпоративные VPN защищают корпоративные активы за счёт перехода на модели Zero Trust Network Access (ZTNA) и внесения в белый список выделенных статических IP-шлюзов. ИТ-менеджеры используют централизованные консоли администратора для управления туннелями IPsec «сеть — сеть» и ссылками единого входа (SSO).

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

Контрольная точка 1: Задание с выбором ответа

1 **1. Какая модель безопасности приходит на смену устаревшим корпоративным VPN?**

- A) Zero Trust
- B) Multi-hop
- C) Одноранговая сеть
- D) Единый шлюз

2 **2. Какая функция нужна, чтобы ограничить доступ к базе данных серверами компании?**

- A) Выделенный IP-адрес
- B) Динамическая маршрутизация
- C) Раздельный туннель
- D) DNS-прокси

3 **3. Какой протокол является стандартом для корпоративных туннелей между офисами (site-to-site)?**

- A) IPsec
- B) PPTP
- C) SOCKS5
- D) SSL v3

4 **4. Какой центральный инструмент позволяет администраторам управлять местами сотрудников?**

- A) Консоль администратора
- B) Ключ реестра
- C) Прошивка маршрутизатора
- D) Системный журнал

5 **5. Какой стандарт аутентификации позволяет входить через Okta или Microsoft Entra ID?**

- A) Единый вход (SSO)
- B) Общий секрет
- C) Аутентификация EPP
- D) Ключ WEP

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Доступ к сети с нулевым доверием предоставляет вход в сеть только после проверки постоянного доверия к устройству.

○ Верно ○ Неверно

7 Вопрос 7

7. Шлюзы с выделенным IP направляют трафик сотрудников вместе с трафиком случайных публичных пользователей.

○ Верно ○ Неверно

8 Вопрос 8

8. Централизованные консоли администратора позволяют IT-менеджерам мгновенно отзывать места отдельных сотрудников.

○ Верно ○ Неверно

9 Вопрос 9

9. IPsec — лёгкий протокол, который не поддерживает туннели «сеть-сеть» (site-to-site).

○ Верно ○ Неверно

10 Вопрос 10

10. Единый вход (SSO) обеспечивает безопасную аутентификацию сотрудников через корпоративные поставщики удостоверений.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Современные архитектуры безопасности заменяют устаревшие туннели доступом по принципу « _____ **».**

2. Чтобы ограничить доступ к базам данных, компании настраивают для шлюза так называемый _____ **.**

3. Филиалы безопасно соединяют туннелями «сайт–сайт» на основе протокола _____ **.**

4. ИТ-администраторы распределяют лицензии сотрудников в центральном портале, который называется _____ **.**

5. Интеграция с Okta позволяет сотрудникам проходить аутентификацию через корпоративный _____ **.**

6. Для защиты входа корпоративные порталы требуют аутентификацию такого типа: _____ **.**

СЛОВАРНЫЙ БАНК СЛОВ

ВЫДЕЛЕННЫЙ IP-АДРЕС ЕДИНЫЙ ВХОД КОНСОЛЬ АДМИНИСТРАТОРА
МНОГОФАКТОРНАЯ НУЛЕВОЕ ДОВЕРИЕ ПРЕДОСТАВЛЕНИЕ ШЛЮЗ IPSEC

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление ключевых понятий

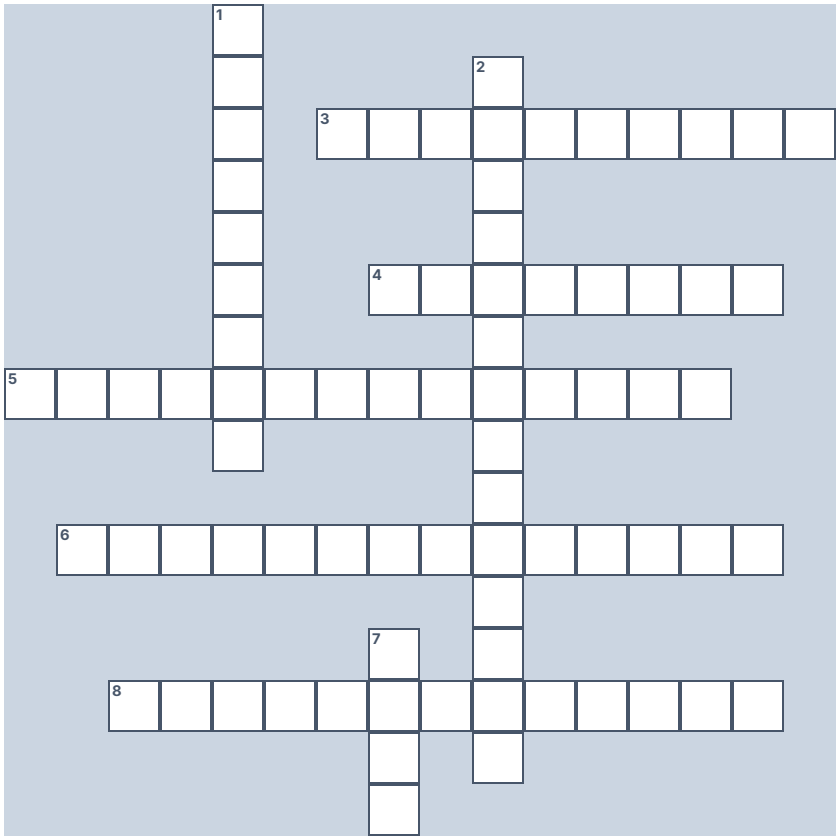
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. НУЛЕВОЕ ДОВЕРИЕ	**A**	Распределение лицензий на VPN-доступ для сотрудников.
☐	2. ВЫДЕЛЕННЫЙ IP	**B**	Связка идентификации Okta и Entra ID.
☐	3. IPSEC	**C**	Защита входа, требующая дополнительных токенов.
☐	4. КОНСОЛЬ АДМИНИСТРАТОРА	**D**	Статический адрес шлюза из белого списка.
☐	5. ЕДИНЫЙ ВХОД	**E**	Стандарт туннеля между сетями (site-to-site).
☐	6. МНОГОФАКТОРНЫЙ	**F**	Входной узел маршрутизации сети.
☐	7. ШЛЮЗ	**G**	Центральный портал IT-менеджера для управления местами.
☐	8. ПРЕДОСТАВЛЕНИЕ	**H**	Структура непрерывной проверки доверия.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

3. Связь удостоверений Okta и Entra ID (10)

4. Стандарт туннеля «сайт–сайт» (8)

5. Постоянный адрес шлюза для белого списка (14)

6. Модель непрерывной проверки доверия (14)

8. Центральный портал рабочего места ИТ-менеджера (13)

ПО ВЕРТИКАЛИ

1. Распределение лицензий на доступ сотрудников к VPN (9)

2. Защита входа, требующая дополнительные токены (14)

7. Узел маршрутизации на входе в сеть (4)

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: Связь удостоверений Okta и Entra ID (10 букв):

4 по горизонтали: Стандарт туннеля «сайт–сайт» (8 букв):

5 по горизонтали: Постоянный адрес шлюза для белого списка (14 букв):

6 по горизонтали: Модель непрерывной проверки доверия (14 букв):

8 по горизонтали: Центральный портал рабочего места ИТ-менеджера (13 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Распределение лицензий на доступ сотрудников к VPN (9 букв):

2 по вертикали: Защита входа, требующая дополнительные токены (14 букв):

7 по вертикали: Узел маршрутизации на входе в сеть (4 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

НУЛЕВОЕДОВЕРИЕ СТАТИЧНЫЙАДРЕС ПРОТОКОЛ КОНСОЛЬАДМИНА
ЕДИНЫЙВХОД МНОГОФАКТОРНАЯ ШЛЮЗ ВЫДЕЛЕНИЕ

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. СТАТИЧНЫЙАДРЕС

C. ПРОТОКОЛ

D. КОНСОЛЬАДМИНА

E. ЕДИНЫЙВХОД

F. МНОГОФАКТОРНАЯ

G. ШЛЮЗ

H. ВЫДЕЛЕНИЕ

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Постоянный адрес шлюза для белого списка.

_____ 2. Узел маршрутизации на входе в сеть.

_____ 3. Распределение лицензий на доступ сотрудников к VPN.

_____ 4. Защита входа, требующая дополнительные токены.

_____ 5. Стандарт туннеля «сайт–сайт».

_____ 6. Модель непрерывной проверки доверия.

_____ 7. Связь удостоверений Okta и Entra ID.

_____ 8. Центральный портал рабочего места ИТ-менеджера.

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. ЕОДВЕЛУОРНИЕВЕ _____
2. ТПЛРОКОО _____
3. ЕЙОВДЫДНХИ _____
4. ЗЮШЛ _____
5. ААРТЫЙИСЧДНСЕТ _____
6. ОМЬЛИННДКОААС _____
7. РАОМТНОЯФНКГАО _____
8. ЕЛИВЕЫЕНД _____

Дополнительное задание: Думай быстро

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

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

Контрольная точка 8: Кейсы по VPN и сетям

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ПЕРЕХОД НА НУЛЕВОЕ ДОВЕРИЕ



Ситуация: Предприятие хочет защитить свои локальные серверы, постоянно проверяя сертификаты соответствия устройств, состояние межсетевого экрана и местоположение пользователя, а не доверяя любому, кто находится внутри сети.

Вопрос для обсуждения: Какую модель безопасности должен внедрить директор по ИТ-безопасности для достижения этой цели?

КЕЙС 2: ОГРАНИЧЕНИЕ ШЛЮЗА



Ситуация: Компания размещает в облаке частные финансовые базы данных. Она хочет закрыть любой публичный доступ из интернета к панелям администрирования, разрешив входы только с проверенных конечных точек компании.

Вопрос для обсуждения: Какую сетевую конфигурацию администратор базы данных должен настроить на облачном межсетевом экране?

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

17 18 16 3 6 18 33 6 20 12 1 8 5 16 6

21 19 20 18 16 11 19 20 3 16

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 корпоративный VPN?

Защищённый сетевой туннель для бизнеса, позволяющий удалённым сотрудникам получать доступ к корпоративным сетям с централизованным управлением.

Q2: Чем Zero Trust отличается от традиционных VPN?

Традиционные VPN доверяют любому внутри туннеля, а Zero Trust постоянно проверяет каждое устройство и каждое соединение пользователя.

Q3: Что такое выделенный IP-адрес в бизнес-VPN?

Статический IP-адрес, закреплённый только за вашей компанией, который можно внести в белый список для безопасного доступа к облачным базам данных.

Q4: Почему SSO важен для бизнес-VPN?

Единый вход (SSO) позволяет сотрудникам безопасно входить в систему с корпоративными учётными данными (например, Okta или Microsoft Entra ID).

Q5: Что такое VPN типа «сеть — сеть»?

Туннель, соединяющий два физических офиса (например, филиал и штаб-квартиру) через публичный интернет с помощью IPsec.

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

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

Q6: Для чего нужна консоль администратора?

Панель для ИТ-администраторов, позволяющая добавлять и удалять рабочие места сотрудников, назначать шлюзы и отслеживать активные подключения.

Q7: Как MFA защищает бизнес-VPN?

Требуя второй код (например, токен приложения-аутентификатора), чтобы предотвратить несанкционированный вход по скомпрометированным паролям.

Q8: Могу ли я проверять историю подключений сотрудников?

Да, корпоративные VPN записывают время подключений, их длительность и назначенные IP-адреса для аудита соответствия требованиям.

Q9: Что такое ZTNA?

Доступ к сети с нулевым доверием — модель безопасности, при которой доступ предоставляется только к определённым приложениям, а не ко всей сети.

Q10: Какова роль шлюзовых узлов?

Они служат защищёнными точками входа для удалённого трафика и направляют данные прямо на частные корпоративные серверы.

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

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

Q1: Как IPsec защищает корпоративные коммуникации между площадками?

IPsec шифрует трафик на сетевом уровне с помощью Encapsulating Security Payload (ESP), обеспечивая конфиденциальность и целостность данных.

Q2: Почему устаревшая защита по периметру не справляется с удалёнными сотрудниками?

Потому что сотрудники получают доступ к данным из разных мест и с разных устройств, из-за чего единый периметр сетевого межсетевого экрана устарел.

Q3: Как ИТ-менеджеры внедряют автоматическое предоставление доступа?

Сопоставляя протоколы SCIM между поставщиками удостоверений (Okta) и консолью администратора VPN для синхронизации каталогов пользователей.

Q4: В чём польза раздельного туннелирования в корпоративной среде?

Направляет локальный трафик SaaS (например, Microsoft 365) вне VPN-туннеля, сохраняя пропускную способность корпоративного шлюза для частных баз данных.

Q5: Как проверки состояния устройства подтверждают безопасность конечных точек?

Клиент VPN сканирует устройство перед подключением, чтобы убедиться, что межсетевой экран активен, антивирус работает, а исправления ОС актуальны.

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

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

Q6: Какую роль играет прохождение NAT в настройке бизнес-VPN?

NAT-T инкапсулирует пакеты IPsec в UDP, чтобы они могли проходить через домашние маршрутизаторы и брандмауэры без разрыва соединений.

Q7: Как компании предотвращают перегрузку пропускной способности шлюза?

Развёртывая несколько региональных шлюзовых узлов и распределяя входящий пользовательский трафик между ними с помощью балансировщиков нагрузки.

Q8: Почему статические белые списки IP-адресов предпочтительнее динамических?

Статические белые списки не позволяют несанкционированным внешним IP-адресам пытаться выполнить рукопожатие подключения, что резко уменьшает поверхность атаки.

Q9: Какую роль играет аутентификация на основе сертификатов в корпоративных VPN?

Проверяет уникальные цифровые сертификаты, установленные на управляемых компанией устройствах, блокируя неуправляемые личные компьютеры.

Q10: Как ZTNA снижает риск бокового перемещения?

Изолируя сеансы пользователей определёнными разрешёнными ресурсами, чтобы хакеры не могли перемещаться по сети, если один узел взломан.

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

Архитектуры нулевого доверия постоянно проверяют состояние безопасности каждого устройства, пытающегося подключиться к сети.

2. АНАЛИЗ VPN

Шлюзы с выделенным IP позволяют компаниям закрыть облачные базы данных, внеся статические адреса в белый список.

3. АНАЛИЗ VPN

IPsec — отраслевой стандартный протокол для настройки защищённых туннелей «сеть-сеть» между офисными сетями.

4. АНАЛИЗ VPN

Консоли администратора позволяют ИТ-отделам выделять, администрировать и проверять рабочие места VPN-доступа сотрудников.

5. АНАЛИЗ VPN

Единый вход (SSO) интегрирует доступ к VPN с корпоративными поставщиками удостоверений, такими как Okta и Entra ID.

6. АНАЛИЗ VPN

Многофакторная аутентификация блокирует несанкционированные попытки подключения с использованием украденных паролей.

7. VPN: ВАЖНО ЗНАТЬ

Раздельное туннелирование оптимизирует корпоративную пропускную способность, исключая публичный трафик SaaS из зашифрованного туннеля.

8. VPN: ВАЖНО ЗНАТЬ

Проверки состояния устройства подтверждают локальные настройки безопасности перед предоставлением доступа к корпоративным серверам.

9. VPN: ВАЖНО ЗНАТЬ

Синхронизация каталогов SCIM автоматизирует управление доступом при приёме и увольнении сотрудников.

10. АНАЛИЗ VPN

Доступ к сети с нулевым доверием ограничивает пользователям доступ определёнными авторизованными приложениями и предотвращает перемещение по сети в стороны.

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 **Нулевое доверие** МОДЕЛЬ ZTNA — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Модели нулевого доверия постоянно проверяют соответствие устройства требованиям перед входом в сеть. Источник: NIST Zero Trust.

2 **Выделенный IP** СТАТИЧЕСКИЙ IP — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Выделенные IP-адреса позволяют использовать шлюзы с белым списком, чтобы блокировать публичный трафик. Источник: Dedicated IP Guide.

3 **Стандарт IPsec** ТУННЕЛЬ IPSEC — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

IPsec — стандартный протокол, используемый для туннелей «сеть-сеть» между филиалами. Источник: IPsec Tunneling.

4 **Распределение ИТ-ресурсов** КОНСОЛЬ АДМИНИСТРАТОРА — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Централизованные панели администратора позволяют IT-менеджерам распределять лицензии на места. Источник: CISA Guidelines.

5 **Вопрос 5** — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой стандарт аутентификации позволяет входить через Okta или Microsoft Entra ID? → Единый вход (SSO)

Ответы: контрольная точка 2 – верно или неверно

6 **Нулевое доверие** ПРОВЕРКИ ZTNA — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Модели нулевого доверия постоянно проверяют соответствие устройства требованиям перед входом в сеть. Источник: NIST Zero Trust.

7 **Вопрос 7** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Выделенные IP закрепляются за одной компанией, поэтому её трафик не смешивается с трафиком других пользователей.

8 **Распределение ИТ-ресурсов** МЕСТО ИТ-АДМИНА — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Централизованные панели администратора позволяют IT-менеджерам распределять лицензии на места. Источник: CISA Guidelines.

9 **Стандарт IPsec** МЕЖДУ САЙТАМИ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

IPsec — стандартный протокол, используемый для туннелей «сеть-сеть» между филиалами. Источник: IPsec Tunneling.

10 **Ссылка Okta SSO** ВХОД ЧЕРЕЗ SSO — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Единый вход (SSO) интегрирует входы в VPN с корпоративными каталогами, такими как Okta. Источник: Okta SSO.

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

H 1. НУЛЕВОЕ ДОВЕРИЕ	D 2. ВЫДЕЛЕННЫЙ IP	E 3. IPSEC	G 4. КОНСОЛЬ АДМИНИСТРАТОРА
B 5. ЕДИНЫЙ ВХОД	C 6. МНОГОФАКТОРНЫЙ	F 7. ШЛЮЗ	A 8. ПРЕДОСТАВЛЕНИЕ

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 НУЛЕВОЕ ДОВЕРИЕ	2 ВЫДЕЛЕННЫЙ IP-АДРЕС	3 IPSEC	4 КОНСОЛЬ АДМИНИСТРАТОРА
5 ЕДИНЫЙ ВХОД	6 МНОГОФАКТОРНАЯ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 B – СТАТИЧНЫЙАДРЕС	2 G – ШЛЮЗ	3 H – ВЫДЕЛЕНИЕ	4 F – МНОГОФАКТОРНАЯ
5 C – ПРОТОКОЛ	6 A – НУЛЕВОЕДОВЕРИЕ	7 E – ЕДИНЫЙВХОД	8 D – КОНСОЛЬАДМИНА

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить НУЛЕВОЕ ДОВЕРИЕ, ВЫДЕЛЕННЫЙ IP и IPSEC и привести пример для каждого термина.

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

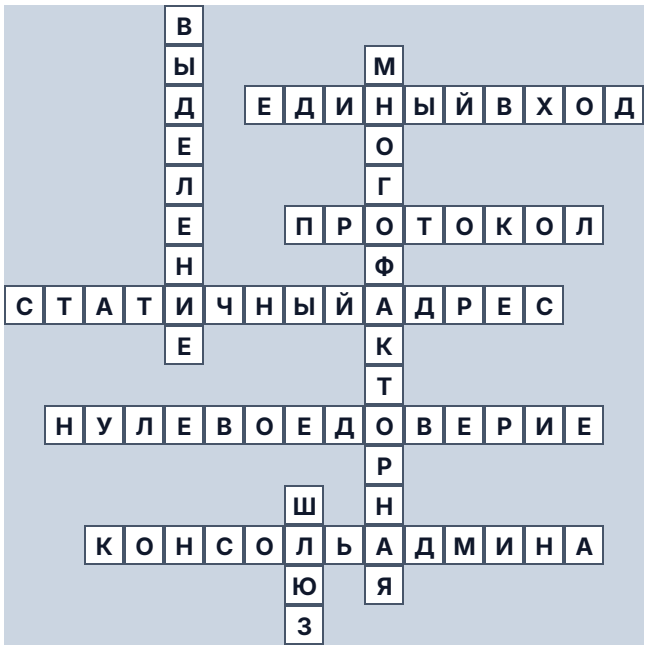
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

3 по горизонтали: ЕДИНЫЙВХОД Связь удостоверений Okta и Entra ID (10 букв)

4 по горизонтали: ПРОТОКОЛ Стандарт туннеля «сайт–сайт» (8 букв)

5 по горизонтали: СТАТИЧНЫЙАДРЕС Постоянный адрес шлюза для белого списка (14 букв)

6 по горизонтали: НУЛЕВОЕДОВЕРИЕ Модель непрерывной проверки доверия (14 букв)

8 по горизонтали: КОНСОЛЬАДМИНА Центральный портал рабочего места ИТ-менеджера (13 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ВЫДЕЛЕНИЕ Распределение лицензий на доступ сотрудников к VPN (9 букв)

2 по вертикали: МНОГОФАКТОРНАЯ Защита входа, требующая дополнительные токены (14 букв)

7 по вертикали: ШЛЮЗ Узел маршрутизации на входе в сеть (4 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. ТПЛРОКОО — **ПРОТОКОЛ**
3. ЕЙОВДЫДНХИ — **ЕДИНЫЙВХОД**
4. ЗЮШЛ — **ШЛЮЗ**
5. ААРТЫЙИСЧДНСЕТ — **СТАТИЧНЫЙАДРЕС**
6. ОМЬЛИННДКОААС — **КОНСОЛЬАДМИНА**
7. РАОМТНОЯФНКГАО — **МНОГОФАКТОРНАЯ**
8. ЕЛИВЕЫЕНД — **ВЫДЕЛЕНИЕ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"НУЛЕВОЕ ДОВЕРИЕ ПРОВЕРЯЕТ КАЖДОЕ УСТРОЙСТВО"

Ответы к кейсам

A Кейс 1: Переход на нулевое доверие

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: компания хочет защитить свои локальные серверы, непрерывно проверяя сертификаты соответствия устройств, состояние межсетевого экрана и местоположение пользователя, а не доверяя всем, кто находится внутри сети.
- Рекомендуемая стратегия и решение: Директору следует перейти на модель Zero Trust Network Access (ZTNA), которая обеспечивает постоянные проверки безопасности с учётом контекста.

B Кейс 2: Ограничение шлюза

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: компания размещает в облаке закрытые финансовые базы данных. Она хочет заблокировать весь публичный доступ из интернета к панелям администрирования и разрешить вход только с проверенных конечных точек компании.
- Рекомендуемая стратегия и решение: Администратору следует настроить на корпоративном VPN шлюз Dedicated IP и внести этот статический адрес в белый список межсетевого экрана облачной базы данных.