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

VPN удалённого доступа

Защита конечных устройств удалённых сотрудников, многофакторная аутентификация и настройка туннелей IPsec.

VPN УДАЛЁННОГО ДОСТУПА: ОБЗОР ТЕМЫ

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 VPN-сети удалённого доступа. Вы изучите туннели «клиент — сайт», многофакторные входы, проверки состояния конечных точек, лимиты пропускной способности и аудит безопасности по журналам syslog.

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/udalennyy-dostup/

Ваша дорожная карта обучения: VPN для удалённого доступа

- Защищённые конечные устройства удалённых сотрудников, работающие с узлами локальной сети.
- Настройте политики многофакторной аутентификации для удалённого входа.
- Настройте конфигурации IPsec и OpenVPN по схеме client-to-site.
- Проверьте журналы удалённых подключений на нарушения контроля доступа.
- Внедрите проверки состояния устройства перед предоставлением сетевых подключений.
- Оптимизируйте пропускную способность сервера, чтобы не допустить нехватки полосы для удалённой работы.

VPN УДАЛЁННОГО ДОСТУПА: ИНСТРУКЦИИ

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: проверкам состояния устройства и многофакторному входу. Завершите работу дополнительным заданием «Думай быстро».

ТУННЕЛИ «КЛИЕНТ-САЙТ» И СООТВЕТСТВИЕ ТРЕБОВАНИЯМ КОНЕЧНЫХ ТОЧЕК (ВВЕДЕНИЕ)

VPN удалённого доступа создают защищённые туннели «клиент — сеть» для сотрудников вне офиса. Защита таких подключений требует обязательной многофакторной аутентификации (MFA) при входе, проверок соответствия состояния конечных точек и аудита журналов через центральные сборщики syslog.

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

Контрольная точка 1: Задание с выбором ответа

1 **1. Какой стандарт аутентификации должны требовать порталы удалённого доступа по VPN?**

- A) Многофакторная
- B) Один фактор
- C) Незашифровано
- D) Локальный гость

2 **2. Какой протокол является стандартом для защиты подключений удалённых сотрудников «клиент — сеть» (client-to-site)?**

- A) OpenVPN
- B) SOCKS5
- C) PPTP
- D) FTP

3 **3. Какая проверка подтверждает, что удалённый ноутбук чист, перед подключением?**

- A) Проверка состояния устройства
- B) Тест скорости
- C) Тест пинга
- D) Объём памяти

4 **4. Где хранятся журналы подключений удалённых сотрудников для аудита безопасности?**

- A) Сервер Syslog
- B) Ключ реестра
- C) Память клиента
- D) Веб-браузер

5 **5. Какая проблема возникает, когда число удалённых сотрудников превышает пропускную способность шлюза?**

- A) Ограничение пропускной способности
- B) Утечка DNS
- C) Успешное рукопожатие
- D) Раскрытие IP

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Многофакторная аутентификация добавляет второй токен проверки для защиты удалённых входов.

○ Верно ○ Неверно

7 Вопрос 7

7. Проверки состояния разрешают удалённым устройствам с отключёнными межсетевыми экранами доступ к частным серверам.

○ Верно ○ Неверно

8 Вопрос 8

8. Журналы VPN удалённого доступа необходимы для отслеживания несанкционированного входа в корпоративную сеть.

○ Верно ○ Неверно

9 Вопрос 9

9. OpenVPN и IPsec — устаревшие протоколы, которые не шифруют полезные данные удалённых клиентов.

○ Верно ○ Неверно

10 Вопрос 10

10. Перегрузка пропускной способности шлюза возникает, когда удалённый трафик превышает мощность сетевой карты.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Чтобы защитить корпоративные порталы, при удалённом входе необходимо требовать аутентификацию такого типа: _____ .

2. Удалённые клиенты шифруют полезные данные туннеля по стандартным протоколам, например _____ .

3. Прежде чем получить доступ к сети, устройство должно пройти проверку безопасности, то есть подтвердить своё безопасное _____ .

4. Журналы входов, пригодные для аудита, постоянно передаются на центральный сервер _____ .

5. Интенсивный трафик в рабочее время может приводить к перегрузке шлюза, когда исчерпывается его _____ .

6. Драйверы виртуальных адаптеров обеспечивают в Windows и macOS инкапсуляцию данных в соединении «клиент–сайт», называемую _____ .

СЛОВАРНЫЙ БАНК СЛОВ

БРАНДМАУЭР МНОГОФАКТОРНАЯ ПРОПУСКНАЯ СПОСОБНОСТЬ СОСТОЯНИЕ
ТУННЕЛИРОВАНИЕ ШИФРОВАНИЕ OPENVPN SYSLOG

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление ключевых понятий

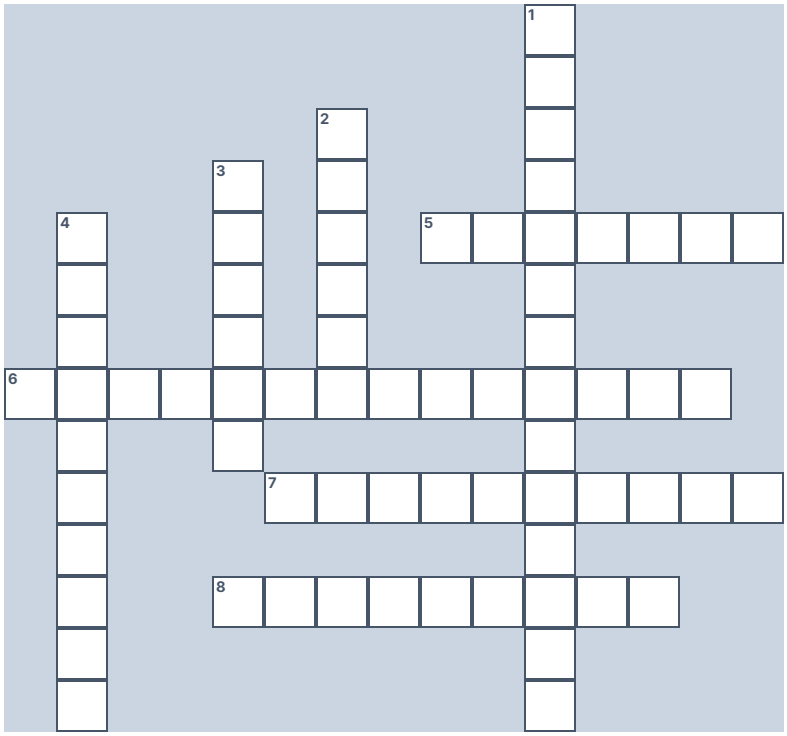
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. МНОГОФАКТОРНЫЙ	A	Инкапсуляция данных в защищённый путь.
☐	2. OPENVPN	B	Центральный сборщик журналов безопасности.
☐	3. СОСТОЯНИЕ	C	Предел пропускной способности сети.
☐	4. SYSLOG	D	Стандартный протокол «клиент — сеть» (client-to-site).
☐	5. ПРОПУСКНАЯ СПОСОБНОСТЬ	E	Проверка состояния удалённого устройства.
☐	6. ШИФРОВАНИЕ	F	Правила системы фильтрации трафика.
☐	7. ТУННЕЛИРОВАНИЕ	G	Криптографическое искажение пакетов.
☐	8. БРАНДМАУЭР	H	Защита входа, требующая дополнительных токенов.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

5. Стандартный протокол «клиент–сайт» (7)

6. Защита входа, требующая дополнительные токены (14)

7. Криптографическое преобразование пакетов (10)

8. Проверка исправности и безопасности удалённого устройства (9)

ПО ВЕРТИКАЛИ

1. Инкапсуляция данных в защищённый путь (14)

2. Предел ёмкости сети для потока данных (6)

3. Центральный сборщик журналов безопасности (6)

4. Правила системы фильтрации трафика (10)

Контрольная точка 5, альтернативный вариант: Доступные подсказки к кроссворду

Пользователи программ чтения с экрана и клавиатуры могут вводить ответы на кроссворд прямо в текстовые поля ниже.

ПО ГОРИЗОНТАЛИ

5 по горизонтали: Стандартный протокол «клиент–сайт» (7 букв):

6 по горизонтали: Защита входа, требующая дополнительные токены (14 букв):

7 по горизонтали: Криптографическое преобразование пакетов (10 букв):

8 по горизонтали: Проверка исправности и безопасности удалённого устройства (9 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Инкапсуляция данных в защищённый путь (14 букв):

2 по вертикали: Предел ёмкости сети для потока данных (6 букв):

3 по вертикали: Центральный сборщик журналов безопасности (6 букв):

4 по вертикали: Правила системы фильтрации трафика (10 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

МНОГОФАКТОРНАЯ ОПЕНВПН СОСТОЯНИЕ СИСЛОГ ПОЛОСА
ШИФРОВАНИЕ ТУННЕЛИРОВАНИЕ БРАНДМАУЭР

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. МНОГОФАКТОРНАЯ**
- **B. ОПЕНВПН**
- **C. СОСТОЯНИЕ**
- **D. СИСЛОГ**
- **E. ПОЛОСА**
- **F. ШИФРОВАНИЕ**
- **G. ТУННЕЛИРОВАНИЕ**
- **H. БРАНДМАУЭР**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

1. Центральный сборщик журналов безопасности.
2. Правила системы фильтрации трафика.
3. Инкапсуляция данных в защищённый путь.
4. Криптографическое преобразование пакетов.
5. Стандартный протокол «клиент–сайт».
6. Предел ёмкости сети для потока данных.
7. Проверка исправности и безопасности удалённого устройства.
8. Защита входа, требующая дополнительные токены.

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. РФКОАОНТНМ АЯОГ _____
2. ЕСИТОЯНОС _____
3. ПЛОАСО _____
4. УИИВНОЛЕРН АТНЕ _____
5. ВННЕОПП _____
6. ОЛССГИ _____
7. ИРШАВНИЕОФ _____
8. ЭНМРБДРАУ А _____

Дополнительное задание: Думай быстро

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

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

Контрольная точка 8: Кейсы по VPN и сетям

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ОБЯЗАТЕЛЬНОЕ ИСПОЛЬЗОВАНИЕ MFA



Ситуация: Бизнес-аналитик пытается войти в корпоративную базу данных, работая удалённо. Он вводит правильные имя пользователя и пароль, но портал VPN блокирует доступ и требует код с физического токена.

Вопрос для обсуждения: какая политика безопасности требует этот шаг двойной проверки?

КЕЙС 2: СООТВЕТСТВИЕ ТРЕБОВАНИЯМ К СОСТОЯНИЮ ЗАЩИТЫ



Ситуация: Подрядчик подключает свой личный ноутбук к удалённой корпоративной сети. VPN-клиент сразу разрывает соединение и уведомляет пользователя, что определения его антивируса устарели.

Вопрос для обсуждения: Какая специализированная проверка на VPN-шлюзе заблокировала эту попытку подключения?

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

21	5	1	13	6	15	15	29	11		5	16	19	20	21	17

9	1	27	10	27	1	6	20		21	19	20	18	16	11	19	20	3	1

12	16	14	17	1	15	10	10

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 VPN удалённого доступа?

Защищённый способ подключения, позволяющий сотрудникам, работающим вне офиса, напрямую подключаться к частным корпоративным серверам.

Q2: Чем соединение «клиент — сеть» отличается от соединения «сеть — сеть»?

Режим «клиент-сайт» соединяет отдельные устройства пользователей, а «сайт-сайт» связывает целые физические офисы.

Q3: Что такое проверка состояния устройства?

Проверка, оценивающая состояние безопасности удалённого устройства (антивирус, уровень обновлений ОС) перед предоставлением доступа.

Q4: Почему OpenVPN используют для удалённого доступа?

Из-за надёжного протокола безопасности, кросс-платформенной совместимости и способности обслуживать отдельные подключения.

Q5: Как MFA защищает удалённый доступ?

Добавляет вторичный токен проверки, не давая получить доступ, даже если пароли сотрудников утекли или украдены.

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

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

Q6: Что такое сервер syslog?

Централизованное хранилище журналов, в котором записываются события подключения, входы в систему и системные оповещения для аудитов соответствия требованиям.

Q7: Что вызывает перегрузку пропускной способности?

Когда совокупные потребности удалённых сотрудников в пропускной способности превышают ограничение скорости интернета корпоративного шлюза.

Q8: Можно ли подключить домашний компьютер к рабочему VPN?

Только если устройство проходит аудит проверки состояния корпоративной политики и разрешено ИТ-администраторами.

Q9: Что такое инкапсуляция в сети?

Упаковка передаваемых пакетов данных в зашифрованные заголовки протокола для защиты передачи.

Q10: Как раздельное туннелирование оптимизирует удалённый доступ?

Позволяет сотрудникам использовать местного провайдера для обычного просмотра сайтов, а рабочие файлы направлять через VPN.

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

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

Q1: Как аутентификация на основе сертификатов улучшает удалённый доступ?

Привязывает разрешения на подключение к заранее установленным локальным цифровым сертификатам, блокируя неуправляемые или несанкционированные устройства.

Q2: В чём риск безопасности раздельного туннелирования при удалённой работе?

Создаёт потенциальный мост, по которому скомпрометированное локальное устройство может проводить внешние угрозы в частную сеть.

Q3: Как проверки состояния устройства анализируют параметры реестра?

Клиент VPN запускает локальные скрипты, которые проверяют пути реестра, чтобы убедиться, что корпоративное ПО безопасности работает.

Q4: Почему системные журналы по умолчанию используют UDP-порт 514?

Чтобы быстро передавать журналы с минимальными накладными расходами, хотя в защищённых конфигурациях теперь обязательна инкапсуляция TLS поверх TCP.

Q5: Как компании устраняют узкие места в пропускной способности шлюза?

Внедряя балансировщики нагрузки и распределяя удалённый трафик между региональными серверными узлами.

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

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

Q6: Какова функция виртуальных адаптеров TAP/TUN на удалённых клиентах?

Они работают как виртуальные сетевые карты и направляют TCP/IP-трафик устройства прямо в зашифрованный VPN-туннель.

Q7: Как IKEv2 MOBIKE поддерживает мобильность удалённых сотрудников?

Динамически обновляет привязки IP-адресов, сохраняя VPN активным при переходе пользователя между Wi-Fi и мобильными данными.

Q8: Чем раздельная маршрутизация отличается от полной маршрутизации через туннель?

Полная маршрутизация направляет весь интернет-трафик устройства через VPN, тогда как раздельная отправляет туда только IP-адреса корпоративных назначений.

Q9: Как устройства NAT обрабатывают удалённые VPN-подключения?

Сопоставляя диапазоны локальных портов с публичными IP-адресами шлюза, чтобы направлять возвращающиеся зашифрованные пакеты данных.

Q10: Какие стандарты соответствия требуют аудита удалённого доступа?

Стандарты вроде HIPAA, SOC 2 и PCI DSS требуют вести журналы и отслеживать все сеансы удалённых подключений.

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

VPN удалённого доступа создают защищённые туннели «клиент — сеть» для сотрудников вне офиса.

2. АНАЛИЗ VPN

Многофакторная аутентификация требуется правилами соответствия для защиты удалённых бизнес-порталов.

3. АНАЛИЗ VPN

Проверки состояния подтверждают локальные настройки безопасности клиента до предоставления доступа к частной сети.

4. АНАЛИЗ VPN

Серверы Syslog собирают журналы подключений для аудита и обнаружения попыток несанкционированного доступа.

5. АНАЛИЗ VPN

Перегрузка пропускной способности шлюза возникает, когда совокупный удалённый трафик превышает интернет-лимиты сервера.

6. АНАЛИЗ VPN

Виртуальные сетевые адаптеры инкапсулируют сетевые запросы операционной системы внутри защищённых протоколов.

7. VPN: ВАЖНО ЗНАТЬ

Поддержка MOBIKE позволяет удалённым клиентам переключаться между сетями без разрыва VPN-туннеля.

8. VPN: ВАЖНО ЗНАТЬ

Маршрутизация через полный туннель защищает весь интернет-трафик сотрудников, но повышает нагрузку на корпоративный шлюз.

9. VPN: ВАЖНО ЗНАТЬ

Аутентификация по сертификатам привязывает авторизацию подключения VPN непосредственно к оборудованию, управляемому компанией.

10. АНАЛИЗ VPN

Стандарты вроде SOC 2 и PCI DSS предполагают ведение журналов и мониторинг сеансов удалённого доступа.

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/

[5] IETF. (2006). RFC 4555: IKEv2 Mobility and Multihoming Protocol (MOBIKE).

https://www.rfc-editor.org/rfc/rfc4555

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Токены входа** БЕЗОПАСНОСТЬ MFA **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Многофакторная аутентификация требует дополнительной проверки при входе. Источник: внедрение MFA.

2 **Туннель OpenVPN** КЛИЕНТ-САЙТ **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

OpenVPN — стандартный протокол для защиты туннелей между клиентом и сетью. Источник: OpenVPN Client.

3 **Аудиты состояния устройств** ПРОВЕРКА УСТРОЙСТВА **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Проверки состояния сканируют конечные устройства на наличие активных межсетевых экранов и антивирусных средств. Источник: Posture Compliance.

4 **Агрегатор журналов** СЕРВЕР SYSLOG **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Серверы Syslog собирают журналы событий безопасности для мониторинга нарушений доступа. Источник: Syslog Standard.

5 **Переполнение карты** ПЕРЕГРУЗКА ШЛЮЗА **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Перегрузка пропускной способности шлюза возникает, когда трафик пользователей превышает лимиты сервера. Источник: Capacity Planning.

Ответы: контрольная точка 2 – верно или неверно

6 **Токены входа** ПРОВЕРКИ MFA — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Многофакторная аутентификация требует дополнительной проверки при входе. Источник: внедрение MFA.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Проверки состояния блокируют устройства с выключенным межсетевым экраном или антивирусом, поэтому таким устройствам отказывают в доступе.

8 **Агрегатор журналов** СЕРВЕР SYSLOG — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Серверы Syslog собирают журналы событий безопасности для мониторинга нарушений доступа. Источник: Syslog Standard.

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

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

OpenVPN и IPsec — актуальные протоколы, которые действительно шифруют трафик удалённых клиентов.

10 **Переполнение карты** ПЕРЕГРУЗКА ШЛЮЗА — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Перегрузка пропускной способности шлюза возникает, когда трафик пользователей превышает лимиты сервера. Источник: Capacity Planning.

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. МНОГОФАКТОРНЫЙ	D 2. OPENVPN	E 3. СОСТОЯНИЕ	B 4. SYSLOG
C 5. ПРОПУСКНАЯ СПОСОБНОСТЬ	G 6. ШИФРОВАНИЕ	A 7. ТУННЕЛИРОВАНИЕ	F 8. БРАНДМАУЭР

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 МНОГОФАКТОРНАЯ	2 OPENVPN	3 СОСТОЯНИЕ	4 SYSLOG
5 ПРОПУСКНАЯ СПОСОБНОСТЬ	6 ТУННЕЛИРОВАНИЕ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 D – СИСЛОГ	2 H – БРАНДМАУЭР	3 G – ТУННЕЛИРОВАНИЕ	4 F – ШИФРОВАНИЕ
5 B – ОПЕНВПН	6 E – ПОЛОСА	7 C – СОСТОЯНИЕ	8 A – МНОГОФАКТОРНАЯ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить МНОГОФАКТОРНЫЙ, OPENVPN и СОСТОЯНИЕ и привести пример для каждого термина.

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

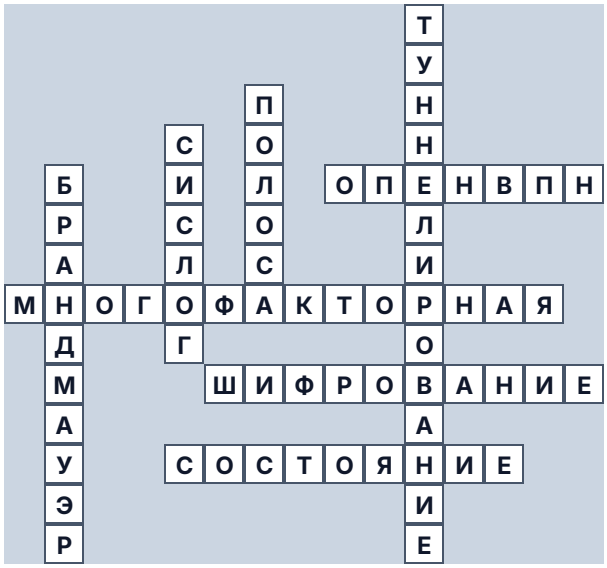
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

5 по горизонтали: ОПЕНВПН Стандартный протокол «клиент–сайт» (7 букв)

6 по горизонтали: МНОГОФАКТОРНАЯ Защита входа, требующая дополнительные токены (14 букв)

7 по горизонтали: ШИФРОВАНИЕ Криптографическое преобразование пакетов (10 букв)

8 по горизонтали: СОСТОЯНИЕ Проверка исправности и безопасности удалённого устройства (9 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ТУННЕЛИРОВАНИЕ Инкапсуляция данных в защищённый путь (14 букв)

2 по вертикали: ПОЛОСА Предел ёмкости сети для потока данных (6 букв)

3 по вертикали: СИСЛОГ Центральный сборщик журналов безопасности (6 букв)

4 по вертикали: БРАНДМАУЭР Правила системы фильтрации трафика (10 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. РФКОАОНТНМАЯОГ — **МНОГОФАКТОРНАЯ**
2. ЕСИТОЯНОС — **СОСТОЯНИЕ**
3. ПЛОАСО — **ПОЛОСА**
4. УИИВНОЛЕРНАТНЕ — **ТУННЕЛИРОВАНИЕ**
5. ВННЕОПП — **ОПЕНВПН**
6. ОЛССГИ — **СИСЛОГ**
7. ИРШАВНИЕОФ — **ШИФРОВАНИЕ**
8. ЭНМРБДРАУА — **БРАНДМАУЭР**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"УДАЛЕННЫЙ ДОСТУП ЗАЩИЩАЕТ УСТРОЙСТВА КОМПАНИИ"

Ответы к кейсам

A Кейс 1: Обязательное использование MFA

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: бизнес-аналитик пытается войти в корпоративную базу данных во время удалённой работы. Он вводит верные имя пользователя и пароль, но VPN-портал блокирует доступ и требует код с физического токена.
- Рекомендуемая стратегия и решение: Корпоративный VPN-портал применяет строгую политику многофакторной аутентификации (MFA) для защиты удалённых входов.

B Кейс 2: Соответствие требованиям к состоянию защиты

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: подрядчик подключает личный ноутбук к удалённой корпоративной сети. VPN-клиент сразу разрывает соединение, уведомив пользователя, что определения его антивируса устарели.
- Рекомендуемая стратегия и решение: Шлюз удалённого доступа выполнил проверку состояния конечной точки и заблокировал устройство из-за устаревших настроек безопасности.