Имя: _____ Дата: _____ Баллы: _____

Как настроить VPN
Рабочий лист

Настройка VPN в Windows, macOS, Android, iOS, Linux и на маршрутизаторах

ОБЗОР ОБУЧЕНИЯ ПО 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 основные принципы виртуальных частных сетей (VPN). Вы изучите то, как зашифрованные туннели защищают ваши данные, как работают сетевые протоколы и как выявлять и устранять утечки конфиденциальности.

КОНТРОЛЬНЫЕ ТОЧКИ РАБОЧЕГО ЛИСТА

- [ ] **Части 1-4: освойте понятия и протоколы VPN.**
- [ ] **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 VPN

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

Ваша дорожная карта обучения: VPN

- Сравните коммерческие VPN-приложения с настройкой встроенных клиентов.
- Настройте подключения VPN на маршрутизаторах для защиты всего дома.
- Настройка и управление файлами конфигурации, такими как OVPN или ключи WireGuard.
- Откройте и защитите определённые порты маршрутизатора для туннельного трафика.
- Проверяйте настройку клиентов с помощью проверок утечек DNS и тестов соединения.

ИНСТРУКЦИИ К РАБОЧЕМУ ЛИСТУ ПО НАСТРОЙКЕ

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: настройке и тестированию VPN-клиентов. Завершите работу дополнительным заданием «Думай быстро».

НАСТРОЙКА VPN (ВВЕДЕНИЕ)

Ручная настройка VPN даёт полный контроль над ключами шифрования и сетевой маршрутизацией. Независимо от того, настраиваете ли вы встроенный клиент на мобильном устройстве или устанавливаете туннель VPN прямо на маршрутизатор, правильная конфигурация — залог защиты от утечек DNS и безопасности всего сетевого трафика.

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

Контрольная точка 1: Задание с выбором ответа

1. Как проще всего настроить VPN на мобильных устройствах?

- A. Скачать официальное VPN-приложение из магазина приложений
- B. Вручную править файлы ядра операционной системы
- C. Прошить на устройство нестандартную прошивку
- D. Подключить телефон к компьютеру по USB

2. В чём преимущество установки VPN прямо на роутер?

- A. Повышает скорость подключения всех локальных устройств
- B. Он автоматически защищает все подключённые сетевые устройства
- C. Избавляет от платы за подписку у локального провайдера
- D. Полностью устраняет необходимость в аппаратных маршрутизаторах

3. Что подразумевает «собственная» конфигурация VPN?

- A. Настройка подключения с помощью встроенных средств ОС
- B. Использовать VPN только в родном городе
- C. Подключение только к серверам в собственной стране
- D. Написание собственного протокола на языке ассемблера

4. Что требуется для ручной внешней настройки OpenVPN?

- A. Разработка собственного логотипа для серверного подключения
- B. Импорт профиля .ovpn, содержащего ключи сертификатов
- C. Смена физического расположения домашнего маршрутизатора
- D. Полное отключение межсетевого экрана операционной системы

5. Зачем администратору использовать раздельное туннелирование в конфигурации?

- A. Полностью блокировать весь интернет-трафик
- B. Чтобы позволить отдельным безопасным приложениям обходить защищённый туннель
- C. Чтобы разделить физический маршрутизатор на два отдельных устройства
- D. Чтобы отключить шифрование для административного мониторинга

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Настройка VPN на маршрутизаторе — простой процесс, не требующий технических навыков.

○ Верно ○ Неверно

7 Вопрос 7

7. В Windows и macOS есть нативные клиенты с поддержкой IKEv2 и L2TP.

○ Верно ○ Неверно

8 Вопрос 8

8. Для настройки WireGuard необходимо сгенерировать открытый и закрытый ключи.

○ Верно ○ Неверно

9 Вопрос 9

9. VPN-туннель защищает ваши сетевые принтеры и задания печати.

○ Верно ○ Неверно

10 Вопрос 10

10. Умные замки, на которых нельзя запустить VPN-приложения, нужно защищать VPN на уровне роутера.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Устройство-шлюз, на котором можно установить VPN для защиты смарт-телевизоров и игровых консолей, называется _____ .

2. Для ручной настройки OpenVPN нужно импортировать серверный файл конфигурации, который называется _____ .

3. Настройка на уровне ОС использует _____ клиент системы.

4. Для аутентификации WireGuard используется криптографическая пара открытого и закрытого ключей, то есть _____ .

5. Простую установку обеспечивает программа от провайдера, то есть _____ .

6. Чтобы запросы шли через серверы VPN и не отслеживались при разрешении имён, нужна _____ .

СЛОВАРНЫЙ БАНК СЛОВ

ВПН-ПРИЛОЖЕНИЕ	ВСТРОЕННЫЙ	ЖУРНАЛЫ	КЛЮЧЕВАЯ ПАРА
НАСТРОЙКА ДНС	ОВПН-ПРОФИЛЬ	РОУТЕР	СПЛИТ-ТУННЕЛЬ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление сетевых понятий

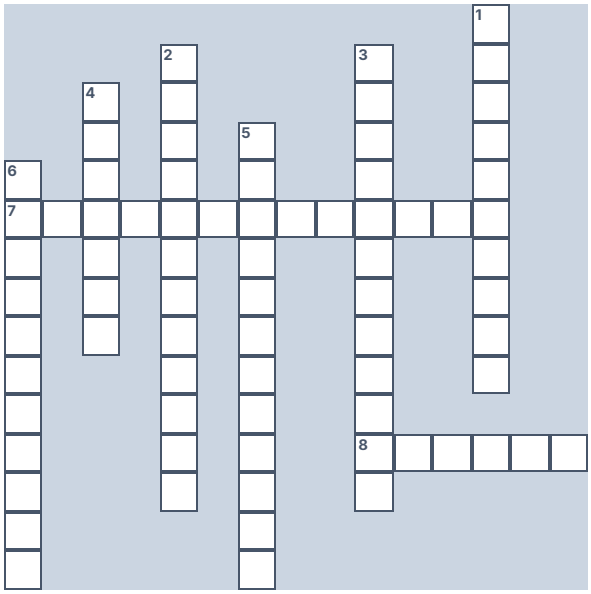
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. VPN-приложение	A	Шифрование на уровне шлюза, защищающее всю умную бытовую технику в локальной сети.
☐	2. VPN на маршрутизаторе	B	Программный пакет от сервиса подписки для простой настройки в один клик.
☐	3. Нативный клиент	C	Проверка вывода ошибок и журналов состояния клиента для отладки неудачных настроек.
☐	4. Профиль .ovpn	D	Разделение маршрутов трафика, чтобы отдельные приложения обходили зашифрованный туннель.
☐	5. Пара ключей	E	Защита трафика во встроенных настройках операционной системы без установки приложений.
☐	6. Раздельное туннелирование	F	Настройка адресов сетевых преобразователей для предотвращения утечек доменных запросов.
☐	7. Настройка DNS-сервера	G	Криптографические токены (открытые/закрытые), необходимые для установления рукопожатий WireGuard.
☐	8. Журналы подключений	H	Формат файла OpenVPN, содержащий серверы, настройки портов и ключи сертификатов.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

7. Программа от сервиса по подписке для простой настройки в один клик (13)

8. Шифрование на уровне шлюза, защищающее все умные устройства в локальной сети (6)

ПО ВЕРТИКАЛИ

1. Защита трафика средствами настроек операционной системы без установки приложений (10)

2. Задание адресов сетевых преобразователей имён, чтобы избежать утечек при поиске доменов (12)

3. Криптографические токены (открытый и закрытый), необходимые для установления рукопожатий WireGuard (12)

4. Проверка вывода ошибок и журналов состояния клиента для отладки неудачной настройки (7)

5. Разделение маршрутов трафика, при котором отдельные приложения обходят зашифрованный туннель (12)

6. Формат файла OpenVPN с серверами, настройками портов и ключами сертификатов (11)

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

7 по горизонтали: Программа от сервиса по подписке для простой настройки в один клик (13 букв):

8 по горизонтали: Шифрование на уровне шлюза, защищающее все умные устройства в локальной сети (6 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Защита трафика средствами настроек операционной системы без установки приложений (10 букв):

2 по вертикали: Задание адресов сетевых преобразователей имён, чтобы избежать утечек при поиске доменов (12 букв):

3 по вертикали: Криптографические токены (открытый и закрытый), необходимые для установления рукопожатий WireGuard (12 букв):

4 по вертикали: Проверка вывода ошибок и журналов состояния клиента для отладки неудачной настройки (7 букв):

5 по вертикали: Разделение маршрутов трафика, при котором отдельные приложения обходят зашифрованный туннель (12 букв):

6 по вертикали: Формат файла OpenVPN с серверами, настройками портов и ключами сертификатов (11 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

ВПНПРИЛОЖЕНИЕ РОУТЕР ВСТРОЕННЫЙ ОВПНПРОФИЛЬ КЛЮЧЕВАЯПАРА
СПЛИТТУННЕЛЬ НАСТРОЙКАДНС ЖУРНАЛЫ

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. ВПНПРИЛОЖЕНИЕ

B. РОУТЕР

C. ВСТРОЕННЫЙ

D. ОВПНПРОФИЛЬ

E. КЛЮЧЕВАЯПАРА

F. СПЛИТТУННЕЛЬ

G. НАСТРОЙКАДНС

H. ЖУРНАЛЫ

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

1. Задание адресов сетевых преобразователей имён, чтобы избежать утечек при поиске доменов.

2. Разделение маршрутов трафика, при котором отдельные приложения обходят зашифрованный туннель.

3. Шифрование на уровне шлюза, защищающее все умные устройства в локальной сети.

4. Криптографические токены (открытый и закрытый), необходимые для установления рукопожатий WireGuard.

5. Защита трафика средствами настроек операционной системы без установки приложений.

6. Проверка вывода ошибок и журналов состояния клиента для отладки неудачной настройки.

7. Формат файла OpenVPN с серверами, настройками портов и ключами сертификатов.

8. Программа от сервиса по подписке для простой настройки в один клик.

Контрольная точка 7: Задание с перепутанными словами

Расставьте буквы ниже в правильном порядке, чтобы получить ключевые понятия и термины VPN. Запишите ответы в заполняемые поля.

1. ЛНЖИИПОЕВ НЕРП
2. ЫРВСОЙННЕТ
3. КЛЯАРПЮВАЕ АЧ
4. НКРСЙСОДА НАТ
5. ТУРРЕО
6. ПЬРФЛИОВОП Н
7. ННТСПУЬЕЛЛ ТИ
8. УНЫЖЛАР

Дополнительное задание: Думай быстро

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

1	Что проверить после настройки			
2	Устройства, которые могут использовать VPN			
3	Известные вам VPN-сервисы			
4	Причины использовать VPN в путешествии			
5	Ошибки, которые люди допускают при настройке			
6	Слова из этого рабочего листа, которые вы хотите запомнить			
7	Настройки, которые включают в первую очередь			
8	Обещания, которые даёт хороший VPN-провайдер			
9	Шаги при настройке VPN			
10	Места, где вы пользовались бы VPN			
11	Способы распознать поддельную сеть Wi-Fi			
12	То, что может скрыть VPN			
13	То, что может видеть ваш интернет-провайдер			
14	Места, где можно найти помощь			
15	То, что нужно для начала работы			

Контрольная точка 8: Кейсы по VPN

Примените изученные понятия к реальным ситуациям ниже.

САРА (СТУДЕНТКА В КАФЕ)

👩‍💻 “Привет! Я сижу в Coffee & Bytes. Здесь есть незащищённая общедоступная сеть «Free_Wi-Fi_No_Password». Я хочу войти в школьную почту и загрузить задание, но боюсь хакеров. Какие риски у использования этой сети без VPN и как VPN защищает мои данные?”

АЛЕКС (СТУДЕНТ-ПУТЕШЕСТВЕННИК)

👩‍💻 “Ой! Я в поездке за границей по проекту и пытаюсь посмотреть биологический документальный фильм, размещённый на сервере в моей стране. Но сайт пишет «Это видео недоступно в вашем текущем местоположении». Почему меня блокируют и как VPN поможет посмотреть его?”

Контрольная точка 9: Расшифруйте шифр

Чтобы завершить обучение по настройке серверов, расшифруйте это скрытое сообщение о настройке защищённых туннелей.

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	19	20	1	15	16	3	10	20	6		19	3	16	11		26	13	32	9

19		9	1	27	10	27	7	15	15	29	14		5	6	14	16	15	16	14

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 потенциальных клиентов об использовании виртуальных частных сетей.

Q1: Что такое VPN и как он работает?

Виртуальная частная сеть (VPN) шифрует ваше интернет-соединение и направляет трафик через защищённый удалённый сервер. Это скрывает ваш публичный IP-адрес и ограничивает то, что наблюдатели в локальной сети и ваш провайдер могут узнать о трафике, проходящем через VPN-туннель.

Q2: Что нужно, чтобы начать?

Вам нужны действующая подписка на VPN или собственный VPN-сервер, поддерживаемое устройство и либо приложение провайдера, либо данные для ручной настройки: адрес сервера, протокол и ваши учётные данные, ключи или сертификаты. Большинство людей просто устанавливают официальное приложение, входят в аккаунт и нажимают «Подключить».

Q3: Как настроить VPN в Windows без приложения?

Откройте «Настройки» > «Сеть и Интернет» > VPN, выберите «Добавить VPN» и введите имя сервера провайдера, тип VPN (например, IKEv2 или L2TP/IPsec) и данные для входа. Затем нажмите «Подключить».

Q4: Замедлит ли VPN скорость моего интернета?

Да, незначительно. Процесс шифрования и физическое расстояние до VPN-сервера добавляют задержку и накладные расходы. Влияние зависит от провайдера, протокола, удалённости сервера, устройства и условий сети.

Q5: Как настроить macOS?

Установите приложение провайдера для macOS или откройте System Settings > VPN, добавьте конфигурацию VPN, выберите IKEv2, L2TP поверх IPSec или Cisco IPSec и введите адрес сервера и учётные данные от вашего провайдера.

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

Просмотрите самые частые вопросы и ответы потенциальных клиентов об использовании виртуальных частных сетей.

Q6: Можно ли пользоваться бесплатным VPN?

Бесплатные VPN могут опираться на рекламу, ограниченные функции, аналитику использования, лимиты данных или другие модели монетизации. Перед использованием пользователям следует изучить политику конфиденциальности провайдера, его владельцев, аудиты и бизнес-модель.

Q7: Как использовать файл .ovpn?

Установите клиент OpenVPN, импортируйте профиль .ovpn от вашего провайдера или администратора и подключитесь. В файле хранятся адрес сервера, порт, настройка UDP или TCP, а часто и сертификаты с ключами.

Q8: Как выбрать лучший VPN?

Ищите проверенные аудитом политики отсутствия журналов, надёжные протоколы (WireGuard, OpenVPN), безопасные расположения серверов, высокую скорость, серверы только на ОЗУ, функцию kill switch и юрисдикцию вне альянсов обмена разведданными (например, 5/9/14 глаз).

Q9: Можно ли использовать VPN на телефоне и смарт-телевизоре?

Да. Современные VPN-провайдеры предлагают отдельные приложения для iOS, Android, macOS, Windows, Linux и смарт-телевизоров, а также настройки для роутеров, защищающие все устройства в вашей домашней сети.

Q10: Что такое Kill Switch?

Kill Switch — это функция безопасности, которая автоматически отключает ваше устройство от интернета при обрыве VPN-соединения. Это предотвращает утечку ваших незашифрованных данных или реального IP-адреса.

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

Изучите технические и структурные аспекты виртуальных частных сетей и защищённых протоколов туннелирования.

Q1: В чём разница между WireGuard, OpenVPN и IKEv2?

WireGuard — современный лёгкий протокол (всего около 4000 строк кода), обеспечивающий высокую скорость и быстрое подключение. OpenVPN — очень безопасный, проверенный временем протокол с открытым исходным кодом. IKEv2 отлично подходит для мобильных устройств благодаря способности быстро переподключаться при смене сети.

Q2: Как вручную настроить WireGuard?

Создайте пару ключей командами wg genkey и wg pubkey, передайте свой открытый ключ серверу и напишите конфигурацию с вашим закрытым ключом, открытым ключом пира, разрешёнными IP-адресами и конечной точкой. Инструмент wg-quick поднимает туннель. [2]

Q3: Что такое утечка WebRTC и как VPN её предотвращает?

WebRTC — это браузерный протокол, который может раскрыть ваши настоящие локальный и публичный IP-адреса, даже если VPN активен. Премиальные VPN блокируют или подменяют запросы WebRTC в своих приложениях для компьютеров и смартфонов и в расширениях для браузеров.

Q4: Как безопасно настроить VPN на домашнем маршрутизаторе?

Убедитесь, что ваш маршрутизатор поддерживает режим VPN-клиента, войдите на его страницу администрирования и загрузите файл OpenVPN или WireGuard от провайдера. Некоторым маршрутизаторам сначала нужно обновить прошивку; после этого туннель используют все устройства в сети.

Q5: Как обфускация обходит блокировки VPN?

Обфускация (или «скрытый VPN») маскирует VPN-трафик так, что он выглядит как обычный HTTPS-трафик (порт 443). Это может помочь обойти глубокую проверку пакетов (DPI), которую используют правительства или школьные и офисные сети для блокировки VPN.

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

Изучите технические и структурные аспекты виртуальных частных сетей и защищённых протоколов туннелирования.

Q6: Что такое раздельное туннелирование и когда его следует использовать?

Раздельное туннелирование позволяет выбрать, какие приложения передают трафик через зашифрованный туннель VPN, а какие подключаются к интернету напрямую. Используйте его, чтобы направлять банковские приложения через VPN, а локальные игры подключать напрямую и избегать задержки, добавляемой VPN.

Q7: Как проверить, что моя новая настройка VPN работает?

Подключитесь, затем зайдите на сайт проверки IP: он должен показывать IP-адрес и местоположение VPN-сервера. Запустите тесты на утечки DNS и WebRTC и ненадолго разорвите соединение, чтобы убедиться, что kill switch блокирует трафик.

Q8: Что проверить, если VPN не подключается после настройки?

Проверьте логин или ключи, адрес сервера и то, что выбранные порт и протокол не заблокированы. Попробуйте переключиться между UDP и TCP или выбрать другой сервер и просмотрите журналы подключения приложения на предмет ошибок.

Q9: Что такое защита от утечек DNS?

Защита от утечек DNS заставляет ваше устройство отправлять запросы на поиск сайтов (DNS-запросы) через частные зашифрованные DNS-серверы VPN, а не через серверы вашего провайдера. Это не позволяет провайдеру отслеживать, какие сайты вы посещаете.

Q10: Должен ли VPN запускаться автоматически?

Обычно да. Большинство приложений могут запускаться при старте системы и подключаться автоматически, в том числе в ненадёжной сети Wi-Fi, поэтому вы защищены до того, как другие приложения начнут отправлять данные.

Часть 11: 10 интересных фактов о VPN и выводов из реальной практики

Ознакомьтесь с этими очень ценными реальными фактами и сведениями об истории, рынке и технологиях VPN.

1. НАТИВНЫЕ КЛИЕНТЫ

В Windows и macOS есть встроенные VPN-клиенты с поддержкой IKEv2 и L2TP/IPsec, поэтому многие подключения можно настроить без дополнительного приложения.

2. ГЕНЕРАЦИЯ КЛЮЧЕЙ

В кратком руководстве WireGuard закрытый ключ создаётся командой wg genkey, а открытый ключ выводится из него командой wg pubkey. [2]

3. РЕВОЛЮЦИЯ WIREGUARD

У WireGuard очень компактная кодовая база, рассчитанная на эффективность, поэтому её проще проверять на уязвимости безопасности, чем традиционные протоколы. [1]

4. ФАЙЛЫ ПРОФИЛЕЙ

Профиль .ovpn объединяет адрес сервера, порт, протокол и сертификаты, поэтому один импорт настраивает подключение OpenVPN.

5. ПОРТЫ ПО УМОЛЧАНИЮ

OpenVPN обычно использует порт 1194, а в официальных примерах WireGuard используется UDP-порт 51820; для подключения туннеля в межсетевых экранах и маршрутизаторах может потребоваться разрешить эти порты.

6. ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ

Глубокая инспекция пакетов (DPI) может обнаруживать и блокировать распространённые VPN-протоколы; переход на OpenVPN через TCP-порт 443 или на обфусцированный режим может помочь.

7. ПОКРЫТИЕ РОУТЕРОВ

VPN на роутере защищает все устройства за ним, включая консоли и смарт-телевизоры, на которых нельзя запустить VPN-приложение, без установки чего-либо на каждое устройство.

8. KEEPALIVE-ПАКЕТЫ

За NAT или межсетевым экраном параметр WireGuard PersistentKeepalive, обычно равный 25 секундам, сохраняет доступность туннеля. [2]

9. ДРАЙВЕРЫ TUN/TAP

OpenVPN рассчитан на работу с виртуальным сетевым интерфейсом TUN/TAP, доступным на большинстве платформ и настраиваемым при установке клиента. [3]

10. РАЗДЕЛЬНОЕ ТУННЕЛИРОВАНИЕ

Во время настройки раздельное туннелирование позволяет исключить из VPN выбранные приложения или адреса, что помогает с локальными принтерами или приложениями, блокирующими IP-адреса VPN.

Технические ссылки и источники

Цитируемые публикации, криптографические спецификации и официальные стандарты документов, использованные в этом рабочем листе.

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

[2] WireGuard. (n.d.). Quick Start.
https://www.wireguard.com/quickstart/

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

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

[5] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

Ответы: настройка VPN в Windows, macOS, Android, iOS, Linux и на маршрутизаторах

1 **Вопрос 1** **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Как проще всего настроить VPN на мобильных устройствах? → Скачать официальное VPN-приложение из магазина приложений

2 **Настройка шлюза маршрутизатора** ЗАДЕРЖКА **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN на роутере шифрует трафик на шлюзе, защищая IoT-устройства, консоли и умную бытовую технику, на которые нельзя установить VPN-приложение. Источник: DD-WRT OpenVPN Clients, Linksys Router Config. [3]

3 **Вопрос 3** **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В Windows и macOS есть встроенные клиенты для протоколов вроде IKEv2 и L2TP/IPsec, поэтому соединение можно настроить без установки дополнительного ПО.

4 **Импорт профиля OpenVPN** УПРАВЛЕНИЕ МАРШРУТИЗАЦИЕЙ **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Для ручной настройки нужно скачать ключи профилей.ovpn, содержащие порты целевых серверов, параметры протокола (UDP/TCP) и криптографические сертификаты. Источник: клиенты DD-WRT OpenVPN.

5 **Маршрутизация по раздельному туннелю** КОНФИДЕНЦИАЛЬНОСТЬ **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Раздельное туннелирование позволяет направлять рабочие приложения с конфиденциальными данными через зашифрованный туннель, а локальный стриминг или игры подключать напрямую без накладных расходов VPN. Источник: IETF IKEv2 RFC.

Ответы: контрольная точка 2 – верно или неверно

6 **Вопрос 6** **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Настройка на роутере означает вход на страницу администрирования, проверку поддержки VPN и загрузку файлов конфигурации.

7 **Нативная интеграция с ОС** СКОРОСТИ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Основные операционные системы имеют встроенную поддержку протоколов, чтобы обеспечить беспроблемную настройку защищённых подключений. Источник: Microsoft Native Gateway, профили поддержки Apple.

8 **Сопряжение ключей WireGuard** РИСК ПЕРЕХВАТА **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard использует асимметричные ключи для установления защищённых P2P-рукопожатий вместо паролей или цепочек центров сертификации. Источник: WireGuard CLI Specifications.

9 **Блокировки локального трафика** БРАНДМАУЭРЫ **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

VPN обычно маршрутизируют трафик публичного интернета и иногда могут блокировать доступ к принтерам локальной сети, если не настроены иначе. Источник: Microsoft Native Gateway.

10 **Вопрос 10** **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Умные замки, на которых нельзя запустить VPN-приложения, нужно защищать VPN на уровне роутера.

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. VPN-приложение	A 2. VPN на маршрутизаторе	E 3. Нативный клиент	H 4. Профиль .ovpn
G 5. Пара ключей	D 6. Раздельное туннелирование	F 7. Настройка DNS-сервера	C 8. Журналы подключений

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 РОУТЕР	2 ОВПН-ПРОФИЛЬ	3 ВСТРОЕННЫЙ	4 КЛЮЧЕВАЯ ПАРА
5 ВПН-ПРИЛОЖЕНИЕ	6 НАСТРОЙКА ДНС		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 G – НАСТРОЙКАДНС	2 F – СПЛИТТУННЕЛЬ	3 B – РОУТЕР	4 E – КЛЮЧЕВАЯПАРА
5 C – ВСТРОЕННЫЙ	6 H – ЖУРНАЛЫ	7 D – ОВПНПРОФИЛЬ	8 A – ВПНПРИЛОЖЕНИЕ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить VPN-приложение, VPN на маршрутизаторе и Нативный клиент и привести пример для каждого термина.

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

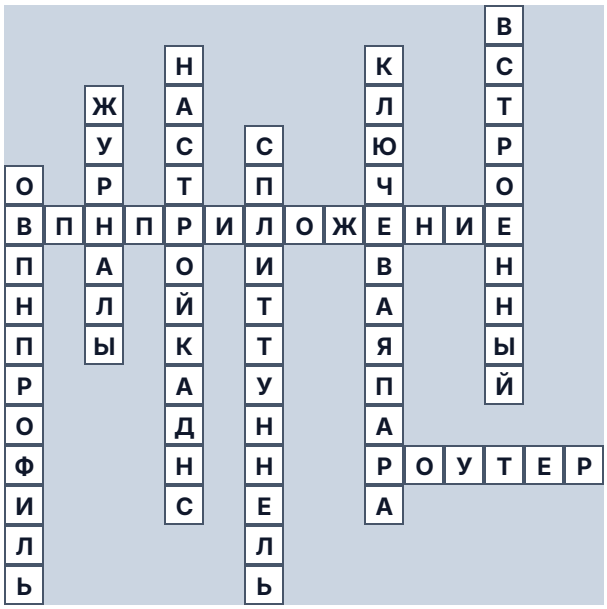
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

7 по горизонтали: ВПНПРИЛОЖЕНИЕ Программа от сервиса по подписке для простой настройки в один клик (13 букв)

8 по горизонтали: РОУТЕР Шифрование на уровне шлюза, защищающее все умные устройства в локальной сети (6 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ВСТРОЕННЫЙ Защита трафика средствами настроек операционной системы без установки приложений (10 букв)

2 по вертикали: НАСТРОЙКАДНС Задание адресов сетевых преобразователей имён, чтобы избежать утечек при поиске доменов (12 букв)

3 по вертикали: КЛЮЧЕВАЯПАРА Криптографические токены (открытый и закрытый), необходимые для установления рукопожатий WireGuard (12 букв)

4 по вертикали: ЖУРНАЛЫ Проверка вывода ошибок и журналов состояния клиента для отладки неудачной настройки (7 букв)

5 по вертикали: СПЛИТТУННЕЛЬ Разделение маршрутов трафика, при котором отдельные приложения обходят зашифрованный туннель (12 букв)

6 по вертикали: ОВПНПРОФИЛЬ Формат файла OpenVPN с серверами, настройками портов и ключами сертификатов (11 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ЛНЖИИПОЕВНЕРП — **ВПНПРИЛОЖЕНИЕ**
2. ЫРВСОЙННЕТ — **ВСТРОЕННЫЙ**
3. КЛЯАРПЮВАЕАЧ — **КЛЮЧЕВАЯПАРА**
4. НКРСЙСОДАНАТ — **НАСТРОЙКАДНС**
5. ТУРРЕО — **РОУТЕР**
6. ПЬРФЛИОВОПН — **ОВПНПРОФИЛЬ**
7. ННТСПУЬЕЛЛТИ — **СПЛИТТУННЕЛЬ**
8. УНЫЖЛАР — **ЖУРНАЛЫ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"УСТАНОВИТЕ СВОЙ ШЛЮЗ С ЗАЩИЩЁННЫМ ДЕМОНОМ"

Ответы к кейсам

A Ситуация A: безопасность общедоступной сети

ПЕРЕХВАТ И ШИФРОВАНИЕ | Дилемма Сары

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Риски: перехват пакетов, перехват данных и атаки «человек посередине». Кто-то в той же сети кафе мог бы перехватить её данные для входа или файл с домашним заданием.
- Защита VPN: шифрует полезную нагрузку сетевых пакетов, делая перехваченный трафик туннеля нечитаемым для пассивных наблюдателей в локальной сети при правильной настройке VPN.

B Ситуация B: доступ к заблокированным ресурсам

ГЕОБЛОКИРОВКА И IP | Дилемма Алекса

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Почему заблокировано: стриминговый хост использует геоблокировку, которая сопоставляет локальный IP-адрес путешественника с его физической страной и блокирует его по территориальным лицензиям.
- Чем помогает VPN: скрывает его реальное местоположение, направляя трафик через сервер в его родной стране. Сайт видит IP-адрес родной страны, и доступ разрешается.