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

WireGuard и OpenVPN Рабочий лист

Сравнение протоколов WireGuard и OpenVPN, размеров кодовой базы, скорости и криптографических стандартов

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 сложность кодовой базы и скорость аудита протоколов.
- Проанализируйте прирост производительности при работе в пространстве ядра.
- Сравните шифры OpenSSL с современной криптографией WireGuard.
- Создайте пары открытых и закрытых ключей для рукопожатий между узлами.
- Маршрутизация VPN-трафика через порты межсетевого экрана TCP и UDP.

ИНСТРУКЦИИ К РАБОЧЕМУ ЛИСТУ ПО СРАВНЕНИЮ ПРОТОКОЛОВ

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: аудиту современных протоколов. Завершите работу дополнительным заданием «Думай быстро».

WIREGUARD И OPENVPN (ВВЕДЕНИЕ)

Выбор протокола VPN требует баланса между скоростью и возможностями настройки. OpenVPN десятилетиями был стандартом и предлагает гибкую настройку TCP/UDP. WireGuard — современная замена, работающая прямо в пространстве ядра и занимающая всего 4000 строк кода. Понимание различий между протоколами — ключ к оптимизации ваших защищённых сетей.

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

Контрольная точка 1: Задание с выбором ответа

1 **1. Каков примерный размер кодовой базы протокола WireGuard?**

- A. Примерно 70 000 строк
- B. Более 100 000 строк
- C. Менее 1000 строк
- D. Около 4000 строк

2 **2. В каком пространстве операционной системы работает WireGuard?**

- A. Пользовательское пространство
- B. Пространство ядра
- C. Прикладное пространство
- D. Виртуальное пространство

3 **3. На какую криптографическую библиотеку в основном опирается OpenVPN?**

- A. ChaCha20-Poly1305
- B. Криптографическая библиотека OpenSSL
- C. Фреймворк протоколов Noise
- D. Кодирование DES открытым текстом

4 **4. В чём главное преимущество WireGuard перед OpenVPN с точки зрения производительности?**

- A. Более быстрое установление соединения и меньшая задержка
- B. Отказом от необходимости в публичных IP-адресах
- C. Встроенная нативная поддержка устаревшего коммутируемого доступа
- D. Нулевые затраты заряда батареи на мобильных устройствах

5 **5. Как WireGuard аутентифицирует подключения пиров?**

- A. Обменом обычными паролями пользователей
- B. Проверкой сертификатов регистрации домена
- C. Использование статических пар открытых и закрытых ключей
- D. Проверкой серийных номеров оборудования

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Компактная кодовая база WireGuard значительно упрощает аудит.

○ Верно ○ Неверно

7 Вопрос 7

7. OpenVPN, как правило, быстрее WireGuard, потому что работает в пространстве ядра.

○ Верно ○ Неверно

8 Вопрос 8

8. OpenVPN хорошо настраивается и поддерживает протоколы UDP и TCP.

○ Верно ○ Неверно

9 Вопрос 9

9. WireGuard использует современную криптографию, например ChaCha20, для быстрого шифрования пакетов.

○ Верно ○ Неверно

10 Вопрос 10

10. WireGuard требует сложной настройки центра сертификации для аутентификации.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Современный протокол _____ работает непосредственно в ядре ОС.

2. Устаревший протокол _____ опирается на криптографическую библиотеку OpenSSL.

3. Выполнение кода в области, которая называется _____ , снижает накладные расходы на переключение контекста.

4. OpenVPN работает в области, называемой _____ , и маршрутизирует пакеты через виртуальные интерфейсы.

5. WireGuard использует открытые и закрытые ключи — _____ — для идентификации узлов соединения.

6. Небольшая кодовая база повышает безопасность ПО: она облегчает его _____ .

СЛОВАРНЫЙ БАНК СЛОВ

ВАЙРГАРД КЛЮЧЕВЫЕ ПАРЫ ОПЕНВПН ОПЕНЭСЭСЭЛЬ ПРОВЕРЯЕМОСТЬ ПРОСТРАНСТВО ЯДРА ТЦП ЮДИПИ ЮЗЕРСПЕЙС

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление сетевых понятий

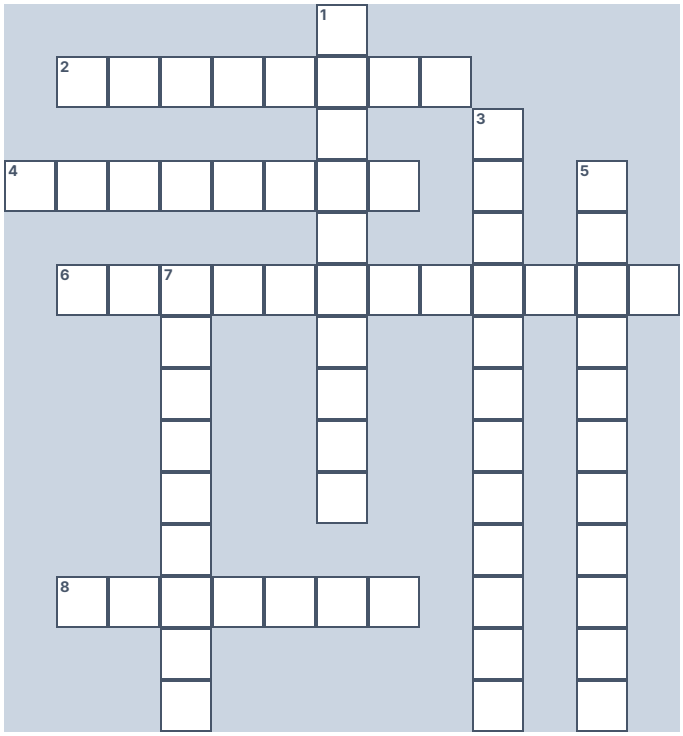
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. WireGuard	A	Область выполнения, в которой работает OpenVPN и которая создаёт накладные расходы на переключение контекста.
☐	2. OpenVPN	B	Компактный размер кодовой базы WireGuard, благодаря которому её гораздо проще проверять.
☐	3. Пространство ядра	C	Криптографическая библиотека, на которую OpenVPN опирается для алгоритмов шифрования.
☐	4. Пользовательское пространство	D	Транспортные протоколы, которые поддерживает OpenVPN; сам WireGuard работает только по UDP.
☐	5. 4,000 строк	E	Область выполнения в операционной системе, в которой для скорости работает WireGuard.
☐	6. OpenSSL	F	Асимметричные токены, которые WireGuard использует для проверки подключений узлов.
☐	7. Пара ключей	G	Современный VPN-протокол, рассчитанный на высокую скорость и простой аудит кода.
☐	8. TCP/UDP	H	Надёжный устаревший протокол с большой и сложной кодовой базой конфигурации.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

2. Транспортные протоколы, поддерживаемые OpenVPN; сам WireGuard работает только по UDP (8)

4. Современный VPN-протокол для высокой скорости и простого аудита кода (8)

6. Асимметричные токены, с помощью которых WireGuard проверяет соединения узлов (12)

8. Надёжный устаревший протокол с большой и сложной кодовой базой настроек (7)

ПО ВЕРТИКАЛИ

1. Преобразование данных в нечитаемый вид с помощью криптографических алгоритмов (10)

3. Небольшой размер кодовой базы WireGuard, благодаря которому аудит намного проще (12)

5. Область выполнения операционной системы, где для скорости работает WireGuard (11)

7. Область выполнения, где работает OpenVPN, создающая накладные расходы на переключение контекста (9)

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

2 по горизонтали: Транспортные протоколы, поддерживаемые OpenVPN; сам WireGuard работает только по UDP (8 букв):

4 по горизонтали: Современный VPN-протокол для высокой скорости и простого аудита кода (8 букв):

6 по горизонтали: Асимметричные токены, с помощью которых WireGuard проверяет соединения узлов (12 букв):

8 по горизонтали: Надёжный устаревший протокол с большой и сложной кодовой базой настроек (7 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Преобразование данных в нечитаемый вид с помощью криптографических алгоритмов (10 букв):

3 по вертикали: Небольшой размер кодовой базы WireGuard, благодаря которому аудит намного проще (12 букв):

5 по вертикали: Область выполнения операционной системы, где для скорости работает WireGuard (11 букв):

7 по вертикали: Область выполнения, где работает OpenVPN, создающая накладные расходы на переключение контекста (9 букв):

Контрольная точка 6: Поиск скрытых слов

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

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

СПИСОК СЛОВ СЛОВАРЯ

ВАЙРГАРД ОПЕНВПН КЕРНЕЛСПЕЙС ЮЗЕРСПЕЙС КОМПАКТНОСТЬ
ШИФРОВАНИЕ КЛЮЧЕВЫЕПАРЫ ТЦПЮДИПИ

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. ВАЙРГАРД

B. ОПЕНВПН

C. КЕРНЕЛСПЕЙС

D. ЮЗЕРСПЕЙС

E. КОМПАКТНОСТЬ

F. ШИФРОВАНИЕ

G. КЛЮЧЕВЫЕПАРЫ

H. ТЦПЮДИПИ

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Преобразование данных в нечитаемый вид с помощью криптографических алгоритмов.

_____ 2. Область выполнения операционной системы, где для скорости работает WireGuard.

_____ 3. Надёжный устаревший протокол с большой и сложной кодовой базой настроек.

_____ 4. Асимметричные токены, с помощью которых WireGuard проверяет соединения узлов.

_____ 5. Транспортные протоколы, поддерживаемые OpenVPN; сам WireGuard работает только по UDP.

_____ 6. Небольшой размер кодовой базы WireGuard, благодаря которому аудит намного проще.

_____ 7. Современный VPN-протокол для высокой скорости и простого аудита кода.

_____ 8. Область выполнения, где работает OpenVPN, создающая накладные расходы на переключение контекста.

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. РРГВААДЙ
2. ЕСЕКЙЛРЕПСН
3. КОНТТОМКЬАСП
4. РЕЕЮЫЫВАПКЛЧ
5. ВННЕОПП
6. ЙРЗЕПЮССЕ
7. ИРШАВНИЕОФ
8. ЮЦДИТПИП

Дополнительное задание: Думай быстро

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

1	Причины выбрать WireGuard			
2	Обещания, которые даёт хороший VPN-провайдер			
3	Причины выбрать OpenVPN			
4	Причины использовать VPN в путешествии			
5	То, что может видеть ваш интернет-провайдер			
6	Способы распознать поддельную сеть Wi-Fi			
7	Мифы о VPN			
8	Места, где вы пользовались бы VPN			
9	Быстрые вещи в повседневной жизни			
10	От чего VPN не может вас защитить			
11	То, что облегчает проверку кода			
12	То, что может скрыть VPN			
13	Отличия WireGuard от OpenVPN			
14	Слова, связанные с конфиденциальностью			
15	Известные вам названия шифров			

Контрольная точка 8: Кейсы по VPN

Примените изученные понятия к реальным ситуациям ниже.

САРА (СТУДЕНТКА В КАФЕ)

👩‍💻 “Привет! Я в кафе, подключена к Wi-Fi, и моё VPN-приложение позволяет выбрать WireGuard или OpenVPN. Мои видеозвонки постоянно прерываются, когда я перехожу между сетью кафе и точкой доступа телефона. Какой протокол выбрать и почему он лучше справится с переключением?”

АЛЕКС (СТУДЕНТ-ПУТЕШЕСТВЕННИК)

👩‍💻 “Я за границей в сети отеля, которая, похоже, блокирует большую часть VPN-трафика. WireGuard вообще не подключается, а мне нужно получить доступ к ресурсам моей школы дома. Что, скорее всего, блокируется и как OpenVPN может помочь это обойти?”

Контрольная точка 9: Расшифруйте шифр

Чтобы завершить обучение по аудиту протоколов, расшифруйте это скрытое сообщение о выполнении в пространстве ядра.

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 13 21 25 26 10 20 6 16 17 6 15 3 17 15

2 16 13 6 6 2 29 19 20 18 29 14

20 21 15 15 6 13 6 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: Почему важны протоколы?

Протокол определяет, как ваш VPN строит туннель, какая криптография защищает данные и как быстро происходит подключение и повторное подключение. WireGuard и OpenVPN — два протокола с открытым исходным кодом, которые предлагает большинство приложений VPN; у них разные компромиссы между простотой, скоростью и гибкостью настройки.

Q3: Какой из них более приватный?

Ни один из протоколов не делает вас анонимным. Оба шифруют трафик туннеля стойкими шифрами; ваша конфиденциальность зависит в основном от того, что VPN-провайдер записывает в журналы и как он управляет ключами, аккаунтами и серверами.

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: Имеют ли оба открытый исходный код?

Да. WireGuard и community-версия OpenVPN публикуют свой исходный код, поэтому независимые исследователи могут их проверять. Небольшая кодовая база WireGuard позволяет провести полную проверку гораздо быстрее.

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

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

Q6: Какой из них быстрее?

WireGuard обычно быстрее: он работает в ядре, использует лёгкое шифрование ChaCha20-Poly1305 и быстро завершает рукопожатия. У OpenVPN накладные расходы выше, но реальная скорость также зависит от нагрузки на сервер и расстояния.

Q7: Могут ли оба работать по TCP и UDP?

Нет. OpenVPN может работать по UDP или TCP, а режим TCP помогает в сетях, блокирующих UDP. WireGuard отправляет пакеты только по UDP, поэтому может не работать в сетях, допускающих только TCP. [4]

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 WireGuard и OpenVPN на телефоне?

Да. WireGuard кроссплатформенный, у него есть приложения для Windows, macOS, Linux, iOS и Android, а клиенты OpenVPN существуют для тех же систем. Большинство VPN-приложений позволяют выбрать любой из них. [1]

Q10: Почему WireGuard такой компактный?

WireGuard поддерживает один фиксированный набор современных шифров вместо множества вариантов. Его реализация для Linux занимает менее 4000 строк кода, что упрощает аудит по сравнению с более крупными кодовыми базами VPN. [3]

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: Какие шифры использует WireGuard?

WireGuard использует ChaCha20 с Poly1305 для шифрования, Curve25519 для обмена ключами, BLAKE2s для хеширования и среду Noise для рукопожатия. Согласования шифров нет, поэтому пользователи не могут выбрать слабый вариант. [2]

Q3: Какие шифры и библиотеки может использовать OpenVPN?

OpenVPN тесно интегрирован с библиотекой OpenSSL и использует TLS для обмена ключами. Администраторы могут выбирать шифры канала данных, например AES-256-GCM, что даёт гибкость, но и допускает слабые настройки. [4]

Q4: Как каждый протокол аутентифицирует участников?

Узлы WireGuard идентифицируют друг друга по статическим открытым ключам, подобно обмену ключами SSH, а каждый ключ сопоставляется с разрешёнными IP-адресами туннеля. OpenVPN обычно опирается на центр сертификации с сертификатами X.509, часто в сочетании с именем пользователя и паролем.

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 происходит при переключении с Wi-Fi на мобильную сеть?

WireGuard не использует постоянное соединение: он отправляет пакеты с нового адреса, и туннель продолжает работать после быстрого рукопожатия. OpenVPN сохраняет состояние сеанса, поэтому при смене сети может потребоваться переподключение, которое занимает чуть больше времени.

Q7: Как работает прямая секретность (Perfect Forward Secrecy)?

PFS гарантирует, что для каждого сеанса создаётся уникальный временный ключ шифрования. Даже если закрытый ключ будет скомпрометирован в будущем, его нельзя использовать для расшифровки прошлых или будущих сеансов, поскольку в них применялись независимые ключи.

Q8: Остаётся ли OpenVPN хорошим выбором, если WireGuard быстрее?

Да. OpenVPN — зрелый и широко применяемый протокол, он работает по TCP, когда UDP заблокирован, и поддерживает корпоративные решения на основе сертификатов. Многие провайдеры предлагают оба протокола, чтобы пользователи могли переключиться, если один заблокирован или работает медленно.

Q9: Какие порты они используют?

Стандартный порт OpenVPN — 1194, но его можно перенести на любой порт UDP или TCP, включая 443. WireGuard слушает UDP-порт, заданный в конфигурации; 51820 — порт, используемый в его официальных примерах.

Q10: Какой протокол проще настроить вручную?

WireGuard обычно проще: создайте пару ключей, обменяйтесь открытыми ключами и укажите разрешённые IP-адреса. OpenVPN требует сертификатов, центра сертификации и большего числа параметров, хотя профили .ovpn объединяют их в один файл.

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. ПЕРВЫЙ VPN-ПРОТОКОЛ

PPTP (Point-to-Point Tunneling Protocol) был разработан группой производителей, включая Microsoft, и опубликован как RFC 2637 в июле 1999 года для поддержки VPN удалённого доступа. [6]

2. ДВА ТРАНСПОРТА

OpenVPN может передавать туннель по UDP или TCP, а в режиме TLS его каналы управления и данных используют один порт. [4]

3. РЕВОЛЮЦИЯ WIREGUARD

У WireGuard очень компактная кодовая база, рассчитанная на эффективность, поэтому её проще проверять на уязвимости безопасности, чем традиционные протоколы. [3]

4. СОВРЕМЕННАЯ КРИПТОГРАФИЯ

WireGuard объединяет ChaCha20, Poly1305, Curve25519, BLAKE2s, SipHash24 и HKDF в рамках протокольной среды Noise, и у пользователей нет выбора шифров, в котором можно было бы ошибиться. [2]

5. OPENSSL ВНУТРИ OPENVPN

OpenVPN тесно интегрирован с библиотекой OpenSSL и берёт из неё многие криптографические возможности, включая TLS для обмена ключами. [4]

6. ГЛУБОКАЯ ИНСПЕКЦИЯ ПАКЕТОВ

Глубокая инспекция пакетов (DPI) изучает содержимое пакетов и характер трафика, а не только заголовки, и некоторые брандмауэры используют её для обнаружения и блокировки распространённых VPN-протоколов.

7. КЛЮЧИ В СТИЛЕ SSH

Соединения WireGuard настраиваются обменом простыми открытыми ключами, подобно обмену ключами SSH, и центр сертификации не нужен. [1]

8. КРОССПЛАТФОРМЕННОСТЬ

WireGuard сначала был выпущен для ядра Linux, а теперь доступен для Windows, macOS, BSD, iOS и Android, поэтому один и тот же протокол работает на большинстве устройств. [1]

9. ПРЯМАЯ СЕКРЕТНОСТЬ

WireGuard повторяет рукопожатие Noise_IK каждые несколько минут, чтобы менять симметричные сеансовые ключи, обеспечивая совершенную прямую секретность, даже если долговременный ключ позже будет раскрыт. [2]

10. ИНТЕРФЕЙСЫ TUN/TAP

OpenVPN рассчитан на работу с виртуальным сетевым интерфейсом TUN/TAP, доступным на большинстве платформ и передающим пакеты туннеля. [4]

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.). Protocol & Cryptography.

https://www.wireguard.com/protocol/

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.

https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

[4] OpenVPN. (n.d.). OpenVPN 2.6 Manual.

https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

[5] WireGuard. (n.d.). Quick Start.

https://www.wireguard.com/quickstart/

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).

https://datatracker.ietf.org/doc/html/rfc2637

Ответы: сравнение протоколов WireGuard и OpenVPN, размера кодовой базы, скорости и криптографических стандартов

1 **Размер кода WireGuard** ПРОТОКОЛЫ — **Правильный ответ: D**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard чрезвычайно компактен: он работает примерно на 4000 строк кода. Это сокращает поверхность атаки и упрощает аудит. Источник: WireGuard Project.

2 **Скорость в пространстве ядра** ЗАДЕРЖКА — **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Работая непосредственно в пространстве ядра, WireGuard избегает издержек переключения контекста, что обеспечивает высокую пропускную способность. Источник: WireGuard Project.

3 **Вопрос 3** — **Правильный ответ: B**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

OpenVPN тесно интегрирован с OpenSSL, который предоставляет шифры вроде AES-GCM и делает его гибко настраиваемым, но более сложным.

4 **Производительность протокола** УПРАВЛЕНИЕ МАРШРУТИЗАЦИЕЙ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard устанавливает рукопожатия за миллисекунды и мгновенно реагирует на роуминг между сетями (например, при переключении с Wi-Fi на сотовую связь). Источник: Microsoft Native Gateway, Apple Support. [3]

5 **Асимметричная криптография** КОНФИДЕНЦИАЛЬНОСТЬ — **Правильный ответ: C**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard использует Cryptokey Routing, сопоставляя открытые ключи с разрешёнными IP-адресами туннеля, подобно конфигурациям SSH. Источник: WireGuard Project.

Ответы: контрольная точка 2 – верно или неверно

6 **Вопрос 6** **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Реализация WireGuard для Linux занимает менее 4000 строк, поэтому команды безопасности могут проверить её намного быстрее, чем гораздо более крупные кодовые базы VPN, такие как OpenVPN.

7 **Задержка в пользовательском пространстве** СКОРОСТИ **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

OpenVPN работает в пользовательском пространстве и передаёт пакеты туда и обратно между ядром и виртуальным интерфейсом, что добавляет издержки на переключение контекста (если не используется разгрузка в ядро, например OpenVPN DCO). Источник: DD-WRT custom firmware.

8 **Конфигурация OpenVPN** РИСК ПЕРЕХВАТА **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

OpenVPN может работать поверх TCP (для надёжности и обхода межсетевых экранов) или UDP (для скорости), что делает его совместимым со сложными корпоративными межсетевыми экранами. Источник: IETF Cryptographic Protocols.

9 **Современная криптография** БРАНДМАУЭРЫ **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard отказывается от устаревших шифров в пользу современных надёжных примитивов, таких как ChaCha20 и Poly1305, которые быстро работают на мобильных ЦП. Источник: WireGuard Project.

10 **Упрощение ключевых пар** БЕЗ ЖУРНАЛОВ **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

WireGuard не использует сертификаты и сложные иерархии центров сертификации; он опирается на простые пары открытого и закрытого ключей, которыми обмениваются узлы. Источник: WireGuard Project.

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

G 1. WireGuard	H 2. OpenVPN	E 3. Пространство ядра	A 4. Пользовательское пространство
B 5. 4,000 строк	C 6. OpenSSL	F 7. Пара ключей	D 8. TCP/UDP

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ВАЙРГАРД	2 ОПЕНВПН	3 ПРОСТРАНСТВО ЯДРА	4 ЮЗЕРСПЕЙС
5 КЛЮЧЕВЫЕ ПАРЫ	6 ПРОВЕРЯЕМОСТЬ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 F – ШИФРОВАНИЕ	2 C – КЕРНЕЛСПЕЙС	3 B – ОПЕНВПН	4 G – КЛЮЧЕВЫЕПАРЫ
5 H – ТЦПЮДИПИ	6 E – КОМПАКТНОСТЬ	7 A – ВАЙРГАРД	8 D – ЮЗЕРСПЕЙС

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить WireGuard, OpenVPN и Пространство ядра и привести пример для каждого термина.

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

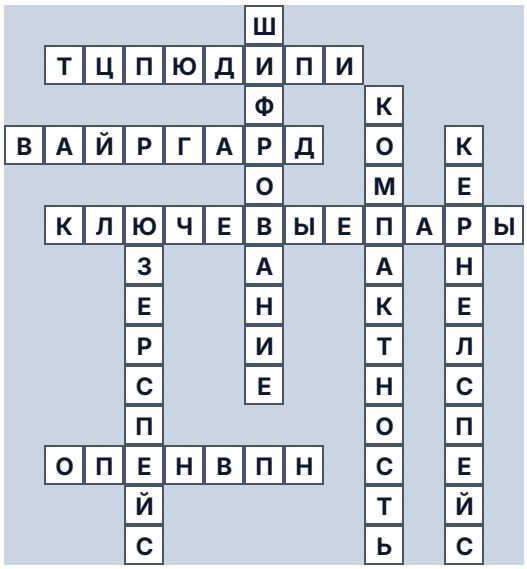
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

2 по горизонтали: ТЦПЮДИПИ Транспортные протоколы, поддерживаемые OpenVPN; сам WireGuard работает только по UDP (8 букв)

4 по горизонтали: ВАЙРГАРД Современный VPN-протокол для высокой скорости и простого аудита кода (8 букв)

6 по горизонтали: КЛЮЧЕВЫЕПАРЫ Асимметричные токены, с помощью которых WireGuard проверяет соединения узлов (12 букв)

8 по горизонтали: ОПЕНВПН Надёжный устаревший протокол с большой и сложной кодовой базой настроек (7 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: ШИФРОВАНИЕ Преобразование данных в нечитаемый вид с помощью криптографических алгоритмов (10 букв)

3 по вертикали: КОМПАКТНОСТЬ Небольшой размер кодовой базы WireGuard, благодаря которому аудит намного проще (12 букв)

5 по вертикали: КЕРНЕЛСПЕЙС Область выполнения операционной системы, где для скорости работает WireGuard (11 букв)

7 по вертикали: ЮЗЕРСПЕЙС Область выполнения, где работает OpenVPN, создающая накладные расходы на переключение контекста (9 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. РРГВААДЙ — **ВАЙРГАРД**
2. ЕСЕКЙЛРЕПСН — **КЕРНЕЛСПЕЙС**
3. КОНТТОМКЬАСП — **КОМПАКТНОСТЬ**
4. РЕЕЮЫЫВАПКЛЧ — **КЛЮЧЕВЫЕПАРЫ**
5. ВННЕОПП — **ОПЕНВПН**
6. ЙРЗЕПЮССЕ — **ЮЗЕРСПЕЙС**
7. ИРШАВНИЕОФ — **ШИФРОВАНИЕ**
8. ЮЦДИТПИП — **ТЦПЮДИПИ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"УЛУЧШИТЕ ОПЕНВПН БОЛЕЕ БЫСТРЫМ ТУННЕЛЕМ"

Ответы к кейсам

A Ситуация A: выбор протокола

ПЕРЕХВАТ И ШИФРОВАНИЕ | Дилемма Сары

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Рекомендация: WireGuard. Его лёгкая архитектура без постоянного соединения позволяет туннелю быстро восстанавливаться при смене сети, а ChaCha20-Poly1305 обеспечивает быстрое шифрование.
- Безопасность: оба протокола шифруют её трафик в сети Wi-Fi кафе, поэтому при правильной настройке любой из них защищает её учётные данные; выбор влияет в основном на скорость и стабильность.

B Ситуация B: как обойти блокировки VPN

ГЕОБЛОКИРОВКА И IP | Дилемма Алекса

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Почему заблокировано: WireGuard использует только UDP, и межсетевой экран отеля, вероятно, блокирует UDP или распознаёт пакеты WireGuard с помощью фильтрации или глубокого анализа пакетов (DPI).
- Чем помогает OpenVPN: он может работать по TCP, включая порт 443, используемый HTTPS, который гостиничные брандмауэры редко блокируют полностью, потому что от него зависит веб-сёрфинг.