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

Тёмный и глубокий веб: безопасность и Различия

Индексирование поисковыми системами, базы данных глубокой сети, луковичная маршрутизация Tor, анонимность в сети и риски

ОБЗОР ОБУЧЕНИЯ: ДАРКНЕТ И ГЛУБОКАЯ СЕТЬ

ЗАЩИЩЁННЫЙ
ШИФРОВАНИЕ ДАННЫХ
Стандарт AES 256 бит

СООТВЕТСТВУЮЩИЙ
ГЛОБАЛЬНЫЕ СТАНДАРТЫ
Нормативные рамки GDPR и CCPA

НУЛЕВОЕ ДОВЕРИЕ
ПОЛИТИКА ДОСТУПА
Многофакторная аутентификация

Добро пожаловать! Этот пакет заданий проведёт вас через различия между глубокой сетью (Deep Web) и даркнетом (Dark Web). Вы изучите неиндексируемые базы данных, луковую маршрутизацию в браузере Tor, криптографические домены .onion и риски безопасности анонимности.

КОНТРОЛЬНЫЕ ТОЧКИ РАБОЧЕГО ЛИСТА

- [ ] **Части 1-4: освойте кибербезопасность и предотвращение угроз.**
- [ ] **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 кибербезопасности

URL: https://www.vpn.com/ru/kiberbezopasnost/temnaya-set-vs-glubokaya-set/

Ваша дорожная карта обучения: стратегия для глубокой и тёмной сети

- Сравните глубокую сеть (неиндексируемые базы данных) с даркнетом (onion-сервисы).
- Разберитесь, как луковая маршрутизация шифрует и передаёт сетевой трафик.
- Оцените риски безопасности при посещении непроверенных сайтов сети Tor.
- Разверните политики безопасного шлюза и песочницы для сбора данных об угрозах.
- Проанализируйте формат криптографического адреса доменов onion-сервисов.

ИНСТРУКЦИИ: РУКОВОДСТВО ПО ГЛУБОКОМУ И ТЁМНОМУ ВЕБУ

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: конфиденциальности в глубокой и тёмной сети. Завершите работу дополнительным заданием «Думай быстро».

БАЗЫ ДАННЫХ ГЛУБОКОГО ВЕБА И ЛУКОВАЯ МАРШРУТИЗАЦИЯ ТЁМНОГО ВЕБА (ВВЕДЕНИЕ)

Глубокий веб состоит из неиндексируемых страниц за паролями и логинами, например личной почты или корпоративных банковских порталов. Даркнет — это часть глубокого веба, намеренно скрытая; для анонимного доступа к ней нужны специализированные браузеры (например, Tor) и сети onion.

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

Контрольная точка 1: Задание с выбором ответа

1 **1. Чем глубокий веб отличается от поверхностного?**

- A. Страницы глубокой сети не индексируются публичными поисковыми системами
- B. Трафик глубокой сети незаконен и контролируется правоохранительными органами
- C. Сайты глубокой сети требуют специальных браузеров, таких как Tor
- D. Страницы глубокой сети всегда загружаются быстрее страниц поверхностной сети

2 **2. Как получить доступ к даркнету?**

- A. Через специализированные браузеры, использующие сети луковой маршрутизации
- B. Настройкой пользовательских параметров DNS на обычных маршрутизаторах
- C. Через закрытые консоли поиска по поверхностному вебу только по приглашениям
- D. Установкой стандартного расширения браузера для блокировки рекламы

3 **3. Какая структура составляет самую большую часть глубокого веба?**

- A. Защищённые паролем базы данных пользователей и личные аккаунты
- B. Нелегальные форумы чёрного рынка, торгующие незаконными товарами
- C. Незашифрованные одноранговые протоколы обмена файлами
- D. Публичные базы данных кэша поисковых систем

4 **4. Что делает луковая маршрутизация с сетевым трафиком?**

- A. Шифрует пакеты и направляет их через несколько ретрансляторов
- B. Он повышает скорость загрузки, обходя узлы провайдера
- C. Сопоставляет серийные номера оборудования с записями IP
- D. Удаляет cookie веб-браузера после каждого щелчка

5 **5. Какой суффикс домена используется исключительно в сетях Tor?**

- A. Криптографическое расширение домена верхнего уровня .onion
- B. Стандартная традиционная коммерческая зона .com
- C. Децентрализованная блокчейн-зона Web3 .eth
- D. Технологическое расширение кода страны .ai

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос «верно/неверно» 6

6. Глубокий веб и даркнет — это один и тот же сегмент сети.

○ Верно ○ Неверно

7 Вопрос «верно/неверно» 7

7. Порталы корпоративных интранетов относятся к глубокой сети.

○ Верно ○ Неверно

8 Вопрос «верно/неверно» 8

8. Луковая маршрутизация полностью расшифровывает пакеты данных на каждом транзитном узле.

○ Верно ○ Неверно

9 Вопрос «верно/неверно» 9

9. Доступ к даркнету подвергает устройства высокому риску заражения вредоносным ПО.

○ Верно ○ Неверно

10 Вопрос «верно/неверно» 10

10. Стандартные веб-поисковики сканируют и индексируют сайты onion.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Частные банковские порталы находятся в неиндексируемом сегменте — _____ .

2. Специальные узлы Tor размещают скрытые службы той части сети, которая называется: _____ .

3. Сайты в сети Tor используют криптографический суффикс верхнего уровня _____ .

4. Зашифрованное многослойное прохождение трафика называется: _____ .

5. Поисковые системы поверхностного веба обходят страницы, для которых выполнена публичная _____ .

6. Сети onion шифруют IP-адреса клиентов, чтобы сохранить _____ пользователей.

СЛОВАРНЫЙ БАНК СЛОВ

.ONION АНОНИМНОСТЬ БАЗА ДАННЫХ ВХОДНОЙ УЗЕЛ ГЛУБОКИЙ ВЕБ
ИНДЕКСАЦИЯ ЛУКОВАЯ МАРШРУТИЗАЦИЯ ТЕМНЫЙ ВЕБ

Напишите свои ответы здесь:

1. **2.**

3. **4.**

5. **6.**

Контрольная точка 4: Сопоставление понятий о безопасности

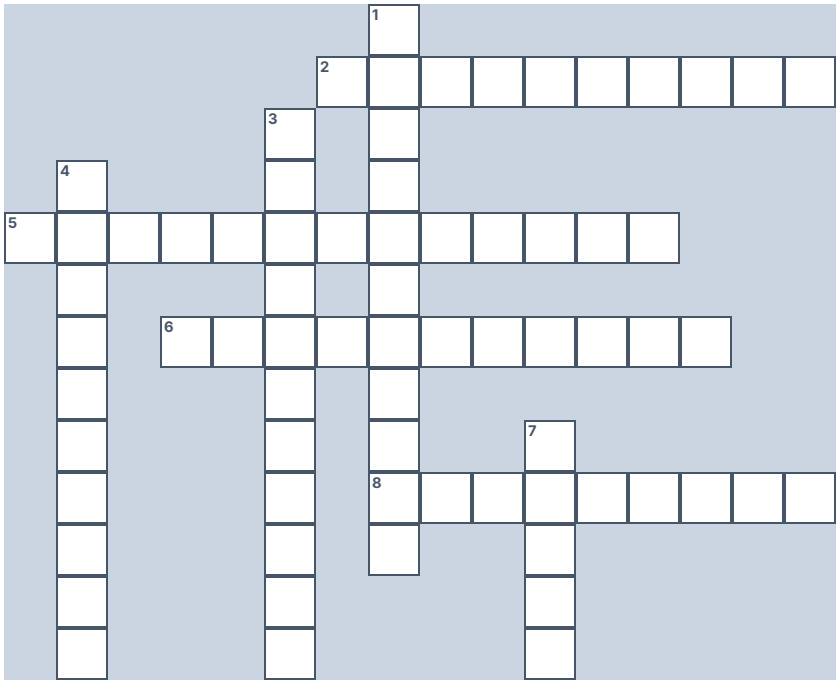
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	**1. Сегмент глубокой сети**	**A**	Зашифрованный сегмент сети, доступный только через специальные браузеры.
☐	**2. Портал даркнета**	**B**	Шифрование данных слоями и передача через три узла.
☐	**3. Расширение Onion**	**C**	Защищённое серверное хранилище, содержащее неиндексируемые системные записи.
☐	**4. Маршрутизация Tor**	**D**	Криптографический суффикс домена верхнего уровня, используемый в сетях Tor.
☐	**5. Проиндексированные страницы**	**E**	Входной узел, через который осуществляется доступ к сети Tor.
☐	**6. Анонимность пользователя**	**F**	Контент открытой части сети, собранный и доступный для поиска в Google.
☐	**7. Частная база данных**	**G**	Сокрытие публичных IP-адресов клиентов от серверов.
☐	**8. Входной шлюз**	**H**	Неиндексированный веб-контент, например частные логины, электронная почта и записи баз данных.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

2. Контент поверхностного веба, собранный и доступный для поиска в Google (10)

5. Многослойное шифрование данных и ретрансляция через три узла (13)

6. Узел входа, используемый для доступа к сети Tor (11)

8. Зашифрованный сегмент сети, доступный только через специальные браузеры (9)

ПО ВЕРТИКАЛИ

1. Сохранение публичных IP-адресов клиентов скрытыми от серверов (11)

3. Неиндексируемый веб-контент: частные учётные записи, электронная почта и записи баз данных (11)

4. Защищённое серверное хранилище неиндексируемых системных записей (10)

7. Криптографический суффикс домена верхнего уровня, используемый в сетях Tor (5)

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: Контент поверхностного веба, собранный и доступный для поиска в Google (10 букв):

5 по горизонтали: Многослойное шифрование данных и ретрансляция через три узла (13 букв):

6 по горизонтали: Узел входа, используемый для доступа к сети Tor (11 букв):

8 по горизонтали: Зашифрованный сегмент сети, доступный только через специальные браузеры (9 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Сохранение публичных IP-адресов клиентов скрытыми от серверов (11 букв):

3 по вертикали: Неиндексируемый веб-контент: частные учётные записи, электронная почта и записи баз данных (11 букв):

4 по вертикали: Защищённое серверное хранилище неиндексируемых системных записей (10 букв):

7 по вертикали: Криптографический суффикс домена верхнего уровня, используемый в сетях Tor (5 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 Н О Н И М Н О С Т Ь Щ М Х Б

Б Ь Я И Ц А С К Е Д Н И Я О Э

Е П Ц Ф Ь К Т Д А Г М Ф Н Ы Ь

В Ь Н Л Й Ш Й З Б Ж К И Н Ч Ц

Й Ы Х Я Е Й Ж Ц Г А О О У В Я

И П М Ъ Х Щ А Ц Ь Н М П П И Й

К Р Й Х З Н Ч О Х Ь Й В Щ Ж Э

О С Ю Ь Ц Б Е В Й Ы Н М Е Т Й

Б Ш Ь А У Щ Р С Ю Т К У Ч Й Т

У Ъ Х Ы Н Н А Д А З А Б Ш Т Щ

Л М А Р Ш Р У Т И З А Ц И Я Ш

Г М А Е Т П Н Б С Ъ З И У Ф Ь

Ю Л В Х О Д Н О Й У З Е Л М Щ

Л Ю Ы Э Т М К Я К Л Р А Е К Б

Ч А Л Ж Ы Е М Я М Е Н Ф Р Л А

СПИСОК СЛОВ СЛОВАРЯ

ГЛУБОКИЙВЕБ ТЕМНЫЙВЕБ ОНИОН МАРШРУТИЗАЦИЯ ИНДЕКСАЦИЯ
АНОНИМНОСТЬ БАЗАДАННЫХ ВХОДНОЙУЗЕЛ

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. ГЛУБОКИЙВЕБ

B. ТЕМНЫЙВЕБ

C. ОНИОН

D. МАРШРУТИЗАЦИЯ

E. ИНДЕКСАЦИЯ

F. АНОНИМНОСТЬ

G. БАЗАДАННЫХ

H. ВХОДНОЙУЗЕЛ

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Сохранение публичных IP-адресов клиентов скрытыми от серверов.

_____ 2. Защищённое серверное хранилище неиндексируемых системных записей.

_____ 3. Многослойное шифрование данных и ретрансляция через три узла.

_____ 4. Неиндексируемый веб-контент: частные учётные записи, электронная почта и записи баз данных.

_____ 5. Зашифрованный сегмент сети, доступный только через специальные браузеры.

_____ 6. Криптографический суффикс домена верхнего уровня, используемый в сетях Tor.

_____ 7. Узел входа, используемый для доступа к сети Tor.

_____ 8. Контент поверхностного веба, собранный и доступный для поиска в Google.

Контрольная точка 7: Задание с перепутанными словами

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

1. ОИЕЛКЙГВУББ
2. ОНОИН
3. ИСИАНКЯЕЦД
4. АЫДХАННБАЗ
5. ВЫЕБЙНТЕМ
6. РАТУЦРИЗМАИЯШ
7. ОИАННЬСТОМН
8. ЗЙЛООВНХЕУД

Дополнительное задание: Думай быстро

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

1	Причины держаться подальше от даркнета			
2	То, что поисковая система найти не может			
3	Устройства, которые могут быть взломаны			
4	Законные причины использовать Tor			
5	Причины обновлять программы			
6	Тревожные признаки в электронном письме			
7	То, что незаконно продают в даркнете			
8	Люди, у которых можно попросить помощи по ИТ			
9	Безопасные привычки, которые можно начать уже сегодня			
10	Что делать после утечки данных			
11	То, что относится к глубокому вебу			
12	Сайты, которыми вы пользуетесь с помощью логина			
13	Слова, связанные с анонимностью			
14	Информация, которой нельзя делиться			
15	То, что находится «под поверхностью»			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ВЫЯВЛЕНИЕ УТЕЧКИ ДАННЫХ



Ситуация: Корпоративный аудит безопасности обнаруживает, что записи конфиденциальной клиентской базы данных продаются на onion-маркетплейсе. В Google эти данные не проиндексированы.

Вопрос для обсуждения: Объясните, какие сегменты сети затронуты и как произошла эта утечка.

КЕЙС 2: АНОНИМНОСТЬ И РИСКИ ВРЕДОНОСНОГО ПО



Ситуация: Аналитик хочет проверить ленты данных об угрозах на сайте в сети Tor. Он скачивает браузер Tor и заходит на сайт.

Вопрос для обсуждения: Оцените преимущества анонимности и опишите шаги по снижению риска вредоносного ПО.

Контрольная точка 9: Расшифруйте шифр

Специалист по кибербезопасности защищает сетевые ресурсы от онлайн-злоумышленников. 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

						13	21	12	16	3	1	33
14	1	18	26	18	21	20	10	9	1	24	10	33
			19	16	23	18	1	15	33	6	20	
1	15	16	15	10	14	15	16	19	20	30		

Расшифрованное сообщение:

СОВЕТ: КАЖДОЕ ЧИСЛО ОБОЗНАЧАЕТ ПОЗИЦИЮ ЭТОЙ БУКВЫ В АЛФАВИТЕ (НАПРИМЕР, 1 = А, 2 = Б, 33 = Я).

Контрольная точка 10: Базовые вопросы о кибербезопасности (Часть A)

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q1: Что такое глубокий веб?

Глубокий веб состоит из всех веб-страниц, которые поисковые системы не могут проиндексировать, включая онлайн-банкинг, базы данных электронной почты и журналы с платным доступом.

Q2: Что такое даркнет?

Даркнет — небольшая часть глубокого веба, намеренно скрытая и доступная только через специализированные браузеры, использующие сети onion.

Q3: Как поисковые системы индексируют страницы?

Поисковые системы запускают автоматические программы (пауки), которые переходят по публичным ссылкам и индексируют страницы, не запретившие обход директивами для роботов.

Q4: Почему онлайн-банкинг считается частью глубокого интернета?

Банковские порталы находятся за страницами входа и паролями, что не позволяет публичным поисковым системам индексировать страницы с выписками по счетам.

Q5: Что такое луковая маршрутизация в браузере Tor?

Луковая маршрутизация — это способ передачи, при котором трафик шифруется слоями и проходит через несколько реле, скрывая IP-адреса пользователей.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Является ли доступ к даркнету незаконным?

Нет. Доступ к даркнету законен в большинстве стран, хотя участие в незаконных торговых площадках или киберпреступной деятельности запрещено.

Q7: Почему сайты даркнета медленно загружаются?

Трафик маршрутизируется и расшифровывается как минимум через три глобальных ретранслятора (входной, средний, выходной), что увеличивает задержку передачи.

Q8: Что означает суффикс домена .onion?

Это специальный суффикс домена верхнего уровня, используемый в сетях Tor, указывающий на криптографически сгенерированные адреса вместо стандартных DNS-серверов.

Q9: Какие риски связаны со ссылками даркнета?

На сайтах нет проверок безопасности, из-за чего пользователи подвергаются высокому риску заражения вредоносным ПО, фишинговых скриптов и мошенничества с платежами.

Q10: Кто создал протокол маршрутизации сети Tor?

Технологию первоначально разработала Военно-морская исследовательская лаборатория США в 1990-х годах для защиты правительственной связи.

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

Изучите продвинутые технические аспекты систем безопасности, анализа вредоносного ПО и соответствия требованиям к данным.

Q1: Как промежуточные узлы защищают анонимность в Tor?

Каждый узел расшифровывает только один слой данных маршрутизации, зная лишь предыдущий и следующий переход, но никогда не источник и получателя одновременно.

Q2: Какова роль выходного узла?

Выходной узел расшифровывает последний слой шифрования и отправляет трафик на публичный сервер назначения или сервер onion.

Q3: Что такое шлюз мостов Tor?

Мосты (bridges) — это не внесённые в список входные реле Tor, используемые для обхода блокировок провайдера и цензуры в регионах, ограничивающих доступ к браузеру Tor.

Q4: Как злоумышленники даркнета используют криптовалюту?

Злоумышленники используют анонимные криптовалюты для финансовых операций на теневых торговых площадках, обходя стандартные банковские проверки.

Q5: Почему обычные поисковые системы не сканируют глубокие базы данных?

Поисковые роботы не могут вводить учётные данные для входа, решать защитные CAPTCHA или выполнять серверные скрипты SQL-запросов, необходимые для доступа к глубоким базам данных.

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

Изучите продвинутые технические аспекты систем безопасности, анализа вредоносного ПО и соответствия требованиям к данным.

Q6: Что такое сервер каталогов в сетях Tor?

Это доверенный сервер, который ведёт список активных входных, промежуточных и выходных ретрансляторов, используемых клиентами для построения маршрутов.

Q7: Как злоумышленники перехватывают данные на выходных узлах?

Операторы вредоносных выходных узлов могут перехватывать незашифрованный HTTP-трафик при выходе из сети Tor, похищая имена пользователей и файлы cookie.

Q8: Чем Tor отличается от I2P?

Tor использует централизованный каталог ретрансляторов и выходные узлы для доступа к публичным сайтам, а I2P — децентрализованную одноранговую структуру для внутреннего хостинга.

Q9: Как правоохранительные органы отслеживают торговые площадки даркнета?

Ведомства используют анализ блокчейна, находят физическое размещение серверов и проводят операции с приманками, чтобы выявить операторов.

Q10: Как утечка DNS ставит под угрозу анонимность клиента?

Утечки DNS возникают, когда DNS-запросы браузера отправляются напрямую через локального провайдера, а не маршрутизируются через зашифрованную сеть Tor.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

Ознакомьтесь с реальными фактами об инцидентах безопасности, механизмах защиты и стандартах соответствия.

1. АНАЛИЗ БЕЗОПАСНОСТИ

Глубокий веб намного больше доступного для поиска поверхностного веба, поскольку большая часть контента находится за логинами и в базах данных.

2. АНАЛИЗ БЕЗОПАСНОСТИ

Даркнет — небольшая, намеренно скрытая часть глубокого веба, доступная с помощью таких средств, как Tor.

3. АНАЛИЗ БЕЗОПАСНОСТИ

Маршрутизация Tor шифрует пакеты данных трижды, снимая слои шифрования, как слои луковицы, на каждом ретрансляторе.

4. АНАЛИЗ БЕЗОПАСНОСТИ

Tor вырос из проекта луковой маршрутизации Научно-исследовательской лаборатории ВМС США, а его код был выпущен как свободное ПО. [1]

5. АНАЛИЗ БЕЗОПАСНОСТИ

Адреса onion — это 56-символьные буквенно-цифровые строки, криптографически сгенерированные из пар открытых ключей.

6. АНАЛИЗ БЕЗОПАСНОСТИ

Выходные узлы могут читать трафик в открытом виде, поэтому для защиты данных сеанса в Tor по-прежнему нужен TLS/HTTPS.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Сайты интрасети, облачные диски и частные базы данных составляют крупнейшие сегменты хранения данных в глубоком вебе.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Специализированные поисковые системы, такие как DuckDuckGo, используют onion-порталы для анонимного поиска в сетях Tor.

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Более 2 миллионов пользователей ежедневно подключаются к сети Tor, чтобы обходить цензуру и сохранять конфиденциальность общения.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Глобальные операции правоохранительных органов (например, Operation Bayonet) закрывают крупные даркнет-рынки, изымая оборудование хостинга.

Технические ссылки и источники

Учебное пособие и интерактивные головоломки составлены на основе мировых стандартов NIST, OWASP и требований к соблюдению правил конфиденциальности данных.

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] Tor Project. (n.d.). Why is it called Tor?

https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?

https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.

https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 **Индексирование поиском** ГЛУБОКИЙ ВЕБ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Страницы глубокого веба скрыты за формами входа и базами данных, поэтому поисковые роботы не могут их обходить. Источник: IETF RFC 3986.

2 **Доступ к Tor** ДАРКНЕТ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Даркнет состоит из скрытых onion-сервисов, доступных только через такие браузеры, как Tor. Источник: IETF RFC 3986.

3 **Глубокие базы данных** БАЗЫ ДАННЫХ — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Защищённые паролем учётные записи и корпоративные документы составляют самую большую часть глубокого веба. Источник: NIST Digital Identity.

4 **Луковая маршрутизация** СЕТЬ TOR — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Луковая маршрутизация шифрует пакеты данных слоями и передаёт их через несколько узлов для обеспечения анонимности. Источник: IETF RFC 3986.

5 **Домен onion** СУФФИКС — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Криптографический суффикс домена.onion направляет трафик внутри Tor без публичного DNS. Источник: IETF RFC 3986.

Ответы: контрольная точка 2 – верно или неверно

6 **Веб-сегменты** СТРУКТУРА — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Глубокий веб охватывает все неиндексируемые страницы, а даркнет — это небольшой зашифрованный сегмент сетей onion. Источник: IETF RFC 3986.

7 **Корпоративные интранеты** ГЛУБОКИЙ ВЕБ — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Сайты интрасети находятся за порталами с паролем и не индексируются, то есть относятся к глубокому вебу. Источник: NIST Digital Identity.

8 **Многослойное шифрование** РЕТРАНСЛЯТОРЫ — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Луковые реле расшифровывают только один уровень маршрутизации, чтобы защитить анонимность пользователя, но никогда не весь пакет. Источник: IETF RFC 3986.

9 **Заражение вредоносным ПО** УГРОЗЫ — **Правильный ответ: Верно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

На торговых площадках тёмного веба нет фильтрации безопасности, поэтому риск заражения вредоносным ПО чрезвычайно высок. Источник: Center for Internet Security (CIS).

10 **Вопрос 10** — **Правильный ответ: Неверно**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Обычные поисковые роботы не используют Tor, поэтому не могут добраться до сайтов .onion и проиндексировать их.

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. Сегмент глубокой сети	A 2. Портал даркнета	D 3. Расширение Onion	B 4. Маршрутизация Tor
F 5. Проиндексированные страницы	G 6. Анонимность пользователя	C 7. Частная база данных	E 8. Входной шлюз

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ГЛУБОКИЙ ВЕБ	2 ТЕМНЫЙ ВЕБ	3 .ONION	4 ЛУКОВАЯ МАРШРУТИЗАЦИЯ
5 ИНДЕКСАЦИЯ	6 АНОНИМНОСТЬ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 F – АНОНИМНОСТЬ	2 G – БАЗАДАННЫХ	3 D – МАРШРУТИЗАЦИЯ	4 A – ГЛУБОКИЙВЕБ
5 B – ТЕМНЫЙВЕБ	6 C – ОНИОН	7 H – ВХОДНОЙУЗЕЛ	8 E – ИНДЕКСАЦИЯ

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить Сегмент глубокой сети, Портал даркнета и Расширение Onion и привести пример для каждого термина.

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

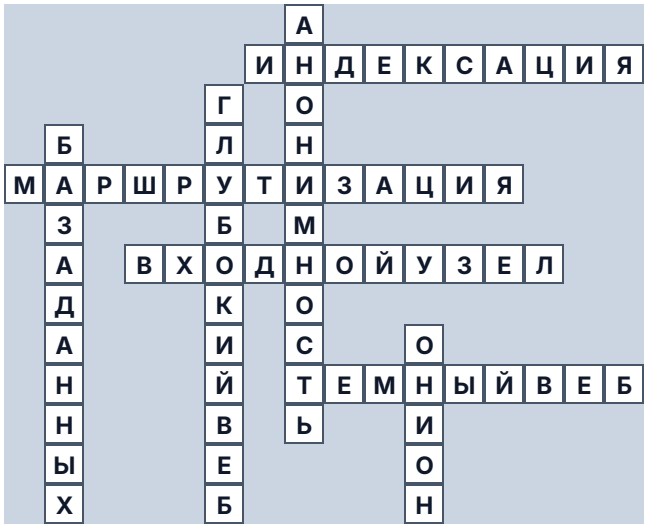
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

2 по горизонтали: ИНДЕКСАЦИЯ Контент поверхностного веба, собранный и доступный для поиска в Google (10 букв)

5 по горизонтали: МАРШРУТИЗАЦИЯ Многослойное шифрование данных и ретрансляция через три узла (13 букв)

6 по горизонтали: ВХОДНОЙУЗЕЛ Узел входа, используемый для доступа к сети Tor (11 букв)

8 по горизонтали: ТЕМНЫЙВЕБ Зашифрованный сегмент сети, доступный только через специальные браузеры (9 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: АНОНИМНОСТЬ Сохранение публичных IP-адресов клиентов скрытыми от серверов (11 букв)

3 по вертикали: ГЛУБОКИЙВЕБ Неиндексируемый веб-контент: частные учётные записи, электронная почта и записи баз данных (11 букв)

4 по вертикали: БАЗАДАННЫХ Защищённое серверное хранилище неиндексируемых системных записей (10 букв)

7 по вертикали: ОНИОН Криптографический суффикс домена верхнего уровня, используемый в сетях Tor (5 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1. ОИЕЛКЙГВУББ — **ГЛУБОКИЙВЕБ**
2. ОНОИН — **ОНИОН**
3. ИСИАНКЯЕЦД — **ИНДЕКСАЦИЯ**
4. АЫДХАННБАЗ — **БАЗАДАННЫХ**
5. ВЫЕБЙНТЕМ — **ТЕМНЫЙВЕБ**
6. РАТУЦРИЗМАИЯШ — **МАРШРУТИЗАЦИЯ**
7. ОИАННЬСТОМН — **АНОНИМНОСТЬ**
8. ЗЙЛООВНХЕУД — **ВХОДНОЙУЗЕЛ**

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ЛУКОВАЯ МАРШРУТИЗАЦИЯ СОХРАНЯЕТ АНОНИМНОСТЬ"

Ответы к кейсам

A Кейс 1: Выявление утечки данных

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: корпоративный аудит безопасности обнаруживает, что конфиденциальные записи базы данных клиентов продаются на onion-площадке. Эти данные не проиндексированы в Google.
- Рекомендуемая стратегия и решение: Задействованные сегменты: частная база данных относится к глубокой сети (deep web: не индексируется, но защищена). Площадка, торгующая украденными данными, находится в даркнете (сеть onion). Как это произошло: хакеры обошли защиту сервера, украли базу данных из глубокой сети и анонимно выставили её в даркнете, чтобы уйти от отслеживания правоохранителями.

B Кейс 2: Анонимность и риски вредоносного ПО

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: аналитик хочет проверить каналы разведданных об угрозах на сайте Tor. Он скачивает браузер Tor и заходит на сайт.
- Рекомендуемая стратегия и решение: Преимущества: Tor направляет трафик через три узла, скрывая корпоративный IP-адрес аналитика. Риски и меры по снижению: у ссылок даркнета нет проверки репутации. Аналитикам следует запускать Tor внутри изолированных виртуальных машин (ВМ), отключать JavaScript в настройках Tor и не скачивать никаких файлов, чтобы защитить корпоративную сеть.