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

Безопасность и шифрование в общедоступном Wi-Fi

Атаки «человек посередине», поддельные точки доступа, перехват пакетов, VPN-туннели и шифрование HTTPS.

ОБЗОР ОБУЧЕНИЯ: БЕЗОПАСНОСТЬ ОБЩЕДОСТУПНОГО WI-FI

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 безопасность общедоступного Wi-Fi. Вы изучите незашифрованные сети, атаки «человек посередине» (MitM), поддельные точки доступа, перехват пакетов, VPN-туннели и защиту передачи данных по HTTPS.

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/bezopasnost-publichnogo-wifi/

Ваша дорожная карта обучения: безопасность общедоступного Wi-Fi

- Определите распространённые риски общедоступного Wi-Fi, включая перехват пакетов и поддельные точки доступа.
- Внедрите шифрующие VPN-туннели для защиты передаваемых данных.
- Принудительно используйте HTTPS и безопасные настройки веб-браузера для удалённых сотрудников.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО БЕЗОПАСНОСТИ ОБЩЕДОСТУПНОГО WI-FI

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: безопасности удалённого доступа. Завершите работу дополнительным заданием «Думай быстро».

БЕЗОПАСНОСТЬ ОБЩЕДОСТУПНОГО WI-FI И ЗАЩИТА ПЕРЕДАВАЕМЫХ ДАННЫХ (ВВЕДЕНИЕ)

Незашифрованные общедоступные точки доступа Wi-Fi оставляют сетевой трафик открытым для перехвата пакетов и подмены Evil Twin. Пропуск трафика через защищённые шифрованные туннели VPN и применение правил HSTS только для HTTPS защищают сеансы от перехвата в локальной сети.

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

Контрольная точка 1: Задание с выбором ответа

1 **1. Что такое атака «человек посередине» (MitM)?**

- A. Перехват и изменение связи между двумя сторонами в общей сети
- B. Метод извлечения данных из базы, нацеленный на записи пользователей
- C. Перегрузка веб-серверов запросами сетевого трафика
- D. Очистка томов хранения локального жёсткого диска

2 **2. Что такое поддельная точка доступа (Evil Twin)?**

- A. Вредоносная точка доступа Wi-Fi, настроенная с тем же SSID, что и у легитимной сети
- B. Административный инструмент для мониторинга резервных копий баз данных
- C. Защищённая конфигурация шлюза VPN
- D. Запись DNS, сопоставляющая авторизованные почтовые серверы

3 **3. Как VPN защищает трафик в общедоступном Wi-Fi?**

- A. Оборачивает все сетевые пакеты в зашифрованный туннель, делая их нечитаемыми для снифферов
- B. Он автоматически блокирует все входящие запросы на подключение
- C. Меняет MAC-адрес физической сетевой карты
- D. Удаляет кэшированные cookie в веб-браузере

4 **4. Что такое перехват пакетов (sniffing)?**

- A. Использование аппаратных или программных средств для перехвата и записи сетевых пакетов
- B. Сканирование локальных каталогов на наличие дубликатов файлов
- C. Ограничение прав чтения базы данных в зависимости от ролей пользователей
- D. Шифрование дисков хранения с помощью ключей AES-256

5 **5. Какова роль HTTPS?**

- A. Шифрование сеансового трафика между браузером и веб-сервером
- B. Фильтрация входящих сообщений электронной почты на шлюзе
- C. Сжатие изображений для ускорения загрузки страниц
- D. Управление файловыми структурами в сетевых хранилищах данных

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Подключённые пользователи могут легко перехватывать данные в открытом виде в открытых общедоступных сетях Wi-Fi.

○ Верно ○ Неверно

7 Вопрос 7

7. Мошеннические точки доступа (Evil Twin) всегда авторизованы администраторами сети.

○ Верно ○ Неверно

8 Вопрос 8

8. VPN неэффективен для защиты трафика от перехвата пакетов (снифинга) в общедоступных сетях.

○ Верно ○ Неверно

9 Вопрос 9

9. HTTPS шифрует только путь в URL, оставляя содержимое пакета в открытом виде.

○ Верно ○ Неверно

10 Вопрос 10

10. Точки доступа Wi-Fi с защитой WPA3 обеспечивают более надёжную защиту, чем открытые сети без пароля.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

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

1. Захват частных паролей в общедоступном Wi-Fi — это _____ связи.
2. Анализ необработанных пакетов в локальной сети использует пакетный _____ .
3. Поддельная точка доступа, имитирующая гостиничный Wi-Fi, — это _____ .
4. Безопасная передача веб-трафика требует шифрования с помощью _____ .
5. Шифрование всего исходящего сетевого трафика выполняет _____ .
6. Зашифрованный канал связи через общедоступные сети — это _____ .

СЛОВАРНЫЙ БАНК СЛОВ

БРАНДМАУЭР ВПА ТРИ ВПН-КЛИЕНТ ЗЛОЙ ДВОЙНИК ПЕРЕХВАТ
СНИФФИНГ ТУННЕЛЬ ХТТПС

Напишите свои ответы здесь:

1.
2.
3.
4.
5.
6.

Контрольная точка 4: Сопоставление понятий о безопасности

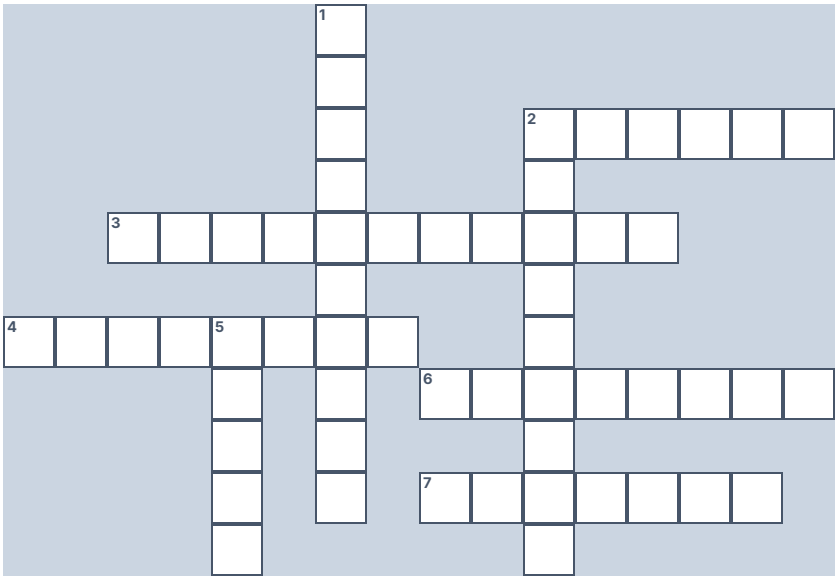
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

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

☐	1. ПЕРЕХВАТ	A	Современный стандарт безопасности Wi-Fi.
☐	2. ПЕРЕХВАТ ПАКЕТОВ	B	Защищённый путь данных при передаче.
☐	3. ЗЛОЙ ДВОЙНИК	C	Фильтрация входящего трафика.
☐	4. HTTPS	D	Мошенническая точка доступа, имитирующая Wi-Fi.
☐	5. VPN	E	Чтение трафика при передаче.
☐	6. ТУННЕЛЬ	F	Перехват сетевых пакетов данных.
☐	7. WPA3	G	Зашифрованная виртуальная частная сеть.
☐	8. БРАНДМАУЭР	H	Безопасная передача данных в вебе.

Контрольная точка 5: Кроссворд

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



ПО ГОРИЗОНТАЛИ

2. Современный стандарт безопасности Wi-Fi. (6)

3. Поддельная точка доступа, имитирующая Wi-Fi. (11)

4. Чтение трафика при передаче. (8)

6. Захват сетевых пакетов данных. (8)

7. Защищённый путь передачи данных. (7)

ПО ВЕРТИКАЛИ

1. Фильтрация входящего трафика. (10)

2. Зашифрованная виртуальная частная сеть. (9)

5. Защищённая передача веб-данных. (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: Современный стандарт безопасности Wi-Fi. (6 букв):

3 по горизонтали: Поддельная точка доступа, имитирующая Wi-Fi. (11 букв):

4 по горизонтали: Чтение трафика при передаче. (8 букв):

6 по горизонтали: Захват сетевых пакетов данных. (8 букв):

7 по горизонтали: Защищённый путь передачи данных. (7 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Фильтрация входящего трафика. (10 букв):

2 по вертикали: Зашифрованная виртуальная частная сеть. (9 букв):

5 по вертикали: Защищённая передача веб-данных. (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.

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

СПИСОК СЛОВ СЛОВАРЯ

ПЕРЕХВАТ СНИФФИНГ ЗЛОЙДВОЙНИК ХТТПС ВПНКЛИЕНТ ТУННЕЛЬ ВПАТРИ 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. ПЕРЕХВАТ

B. СНИФФИНГ

C. ЗЛОЙДВОЙНИК

D. ХТТПС

E. ВПНКЛИЕНТ

F. ТУННЕЛЬ

G. ВПАТРИ

H. БРАНДМАУЭР

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Современный стандарт безопасности Wi-Fi.

_____ 2. Поддельная точка доступа, имитирующая Wi-Fi.

_____ 3. Захват сетевых пакетов данных.

_____ 4. Защищённый путь передачи данных.

_____ 5. Фильтрация входящего трафика.

_____ 6. Чтение трафика при передаче.

_____ 7. Зашифрованная виртуальная частная сеть.

_____ 8. Защищённая передача веб-данных.

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. **АЕХПВЕТР** _____
2. **ДКЛЗИВОНЙОЙ** _____
3. **ВИЛПЕТКНН** _____
4. **ИТАРВП** _____
5. **ФИНГФСНИ** _____
6. **ПХТСТ** _____
7. **ТЛЕЬУНН** _____
8. **ЭНМРБДРАУА** _____

Дополнительное задание: Думай быстро

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

1	Причины обновлять программы			
2	Устройства, которые подключаются к Wi-Fi автоматически			
3	Информация, которой нельзя делиться			
4	Безопасные привычки, которые можно начать уже сегодня			
5	Способы оставаться в безопасности в кафе			
6	Устройства, которые могут быть взломаны			
7	То, что хакер может увидеть в открытой сети Wi-Fi			
8	Признаки поддельной сети Wi-Fi			
9	Альтернативы общедоступному Wi-Fi			
10	Тревожные признаки в электронном письме			
11	То, чего не стоит делать в общедоступной сети Wi-Fi			
12	Места с бесплатным Wi-Fi			
13	Способы защитить свои аккаунты			
14	Признаки заражения компьютера			
15	Названия Wi-Fi, которые кажутся подозрительными			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: СДЕРЖИВАНИЕ ПЕРЕХВАТА ПАКЕТОВ В ОБЩЕДОСТУПНОМ WI-FI



Ситуация: Менеджер по продажам, работающий удалённо и подключённый к общедоступной сети Wi-Fi в аэропорту, замечает, что несколько конфиденциальных деловых писем утекли вскоре после отправки открытым текстом.

Вопрос для обсуждения: Проанализируйте риски общедоступных сетей и опишите решение по шифрованию трафика.

КЕЙС 2: ЗАЩИТА ОТ ПОДДЕЛЬНОЙ ТОЧКИ ДОСТУПА «ЗЛОЙ ДВОЙНИК»



Ситуация: Злоумышленники разворачивают поддельную точку доступа Wi-Fi под названием «CoffeeShop_Guest», имитирующую настоящую точку доступа кафе, и перехватывают сетевой трафик ничего не подозревающих гостей.

Вопрос для обсуждения: Опишите шаги проверки для обнаружения и блокировки поддельных точек доступа.

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

26	10	22	18	21	11	20	6		20	18	1	22	10	12
17	21	2	13	10	25	15	16	4	16		3	1	11	22	1	33
				25	6	18	6	9		3	17	15				

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: Почему общедоступный Wi-Fi небезопасен?

Открытый общедоступный Wi-Fi не шифрует трафик в эфире, поэтому находящиеся рядом люди могут перехватить любые незащищённые данные. [2]

Q2: Что такое перехват пакетов (packet sniffing)?

Анализатор пакетов (сниффер) перехватывает необработанные данные, передаваемые через сетевой интерфейс, раскрывая пароли в открытом виде и сведения о трафике.

Q3: Что такое Evil Twin?

Мошенническая точка доступа, созданная хакерами, которая имитирует название и настройки надёжной местной точки Wi-Fi.

Q4: Как VPN меня защищает?

Направляет ваш трафик через зашифрованный туннель, скрывая вашу активность в сети от локальных снифферов.

Q5: Защищает ли меня HTTPS в общедоступном Wi-Fi?

Да, он шифрует данные, которыми обмениваются ваш браузер и сайт, а VPN добавляет ещё один уровень защиты.

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

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Что такое WPA3?

Современный стандарт защищённого доступа к Wi-Fi, обеспечивающий более надёжное шифрование и защиту от автономных атак по словарю. [1]

Q7: Может ли общедоступный Wi-Fi доставить вредоносное ПО?

Да, злоумышленники могут перехватывать трафик и внедрять в сеанс вашего браузера вредоносные запросы на загрузку (drive-by загрузки).

Q8: Чем опасен обмен файлами?

Если включён общий доступ к файлам, другие пользователи в общедоступной сети могут читать или изменять каталог вашей локальной папки.

Q9: Что такое страница авторизации (captive portal)?

Страница входа, которую сети отелей или кафе используют для предоставления доступа в интернет и которую иногда могут подделывать злоумышленники.

Q10: Нужно ли отключать Wi-Fi, когда он не используется?

Да, отключение Wi-Fi не даёт устройству автоматически подключаться к ненадёжным сетям.

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 атака «человек посередине» использует DNS?

Используя подмену DNS на подставном маршрутизаторе, чтобы направлять браузеры жертв на похожие фишинговые страницы вместо нужных доменов.

Q2: Что такое перехват сеанса?

Злоумышленник перехватывает незашифрованный файл cookie сеанса в общедоступном Wi-Fi и импортирует его, чтобы обойти вход по учётным данным.

Q3: Что такое SSL stripping?

MitM-атака, при которой злоумышленник понижает защищённый HTTPS-запрос пользователя до незашифрованного HTTP и перехватывает логины в открытом виде.

Q4: Как HSTS защищает от SSL stripping?

HTTP Strict Transport Security заставляет браузеры подключаться только по HTTPS и отклонять возврат к незашифрованному HTTP. [3]

Q5: Что такое VPN с раздельным туннелированием?

Конфигурация, при которой через VPN направляется только корпоративный трафик, а публичный интернет-трафик идёт напрямую, что может создать риск утечки.

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

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

Q6: Почему WPA2 уязвим для KRACK?

Атака Key Reinstallation использует четырёхэтапное рукопожатие WPA2 для расшифровки пакетов без пароля Wi-Fi.

Q7: Что такое изоляция клиентов?

Настройка безопасности роутера, не позволяющая подключённым по Wi-Fi устройствам напрямую обмениваться данными друг с другом и блокирующая локальный перехват.

Q8: Как злоумышленники используют поддельные DNS-серверы?

Они настраивают поддельные маршрутизаторы, которые назначают клиентам фальшивые DNS-серверы, что позволяет перехватывать и подменять все веб-запросы.

Q9: Может ли VPN скрыть мой локальный MAC-адрес?

Нет. MAC-адреса — это локальные идентификаторы уровня 2; вместо этого используйте встроенную в устройство настройку рандомизации MAC (частный адрес).

Q10: Что такое атака с подменой captive portal?

Злоумышленник размещает поддельный портал аутентификации на мошеннической точке доступа, чтобы украсть учётные данные под видом бесплатного доступа в Wi-Fi.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

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

1. АНАЛИЗ БЕЗОПАСНОСТИ

Удалённые сотрудники часто используют Wi-Fi в кафе, отелях и аэропортах, где не могут контролировать безопасность сети.

2. АНАЛИЗ БЕЗОПАСНОСТИ

Мошенническая точка доступа Evil Twin может скопировать точное название и MAC-адрес доверенной сети, вводя устройства в заблуждение.

3. АНАЛИЗ БЕЗОПАСНОСТИ

Программы для перехвата пакетов, например Wireshark, бесплатны и могут показывать нешифрованные HTTP-пароли открытым текстом.

4. АНАЛИЗ БЕЗОПАСНОСТИ

Защита WPA3 использует протокол одновременной аутентификации равных (SAE) для защиты от локальных атак полным перебором.

5. АНАЛИЗ БЕЗОПАСНОСТИ

Атаки с удалением SSL обходят базовую защиту HTTPS, перехватывая первоначальные HTTP-редиректы на шлюзе.

6. АНАЛИЗ БЕЗОПАСНОСТИ

Заголовки ответа HTTP Strict Transport Security (HSTS) не позволяют браузерам возвращаться к незашифрованным HTTP-подключениям. [3]

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Отключение функции «Автоподключение» не позволяет смартфонам подключаться к похожим поддельным сетям в общественных местах.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Корпоративные конфигурации VPN «всегда включён» направляют весь сетевой трафик удалённых сотрудников через корпоративные брандмауэры.

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Мошеннические точки доступа могут выдавать поддельные ответы DNS, перенаправляя целевые домены на фишинговые серверы.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Без VPN другие пользователи открытой точки доступа могут видеть, к каким сайтам и серверам обращается ваше устройство.

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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] 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

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

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

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое атака «человек посередине» (MitM)? → Перехват и изменение связи между двумя сторонами в общей сети

2 Вопрос 2 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое поддельная точка доступа (Evil Twin)? → Вредоносная точка доступа Wi-Fi, настроенная с тем же SSID, что и у легитимной сети

3 Вопрос 3 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Как VPN защищает трафик в общедоступном Wi-Fi? → Оборачивает все сетевые пакеты в зашифрованный туннель, делая их нечитаемыми для снифферов

4 Вопрос 4 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что такое перехват пакетов (sniffing)? → Использование аппаратных или программных средств для перехвата и записи сетевых пакетов

5 Вопрос 5 — **Правильный ответ: A**

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какова роль HTTPS? → Шифрование сеансового трафика между браузером и веб-сервером

Ответы: контрольная точка 2 – верно или неверно

6 Вопрос 6

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Подключённые пользователи могут легко перехватывать данные в открытом виде в открытых общедоступных сетях Wi-Fi.

7 Вопрос 7

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: Evil Twin — это несанкционированная точка доступа, которую злоумышленник создаёт, чтобы имитировать настоящую.

8 Вопрос 8

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: VPN шифрует трафик в туннеле, поэтому локальные снифферы не могут его прочитать.

9 Вопрос 9

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: HTTPS шифрует весь обмен по HTTP, включая путь URL-адреса и содержимое страницы.

10 Вопрос 10

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Точки доступа Wi-Fi с защитой WPA3 обеспечивают более надёжную защиту, чем открытые сети без пароля.

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

E 1. ПЕРЕХВАТ	F 2. ПЕРЕХВАТ ПАКЕТОВ	D 3. ЗЛОЙ ДВОЙНИК	H 4. HTTPS
G 5. VPN	B 6. ТУННЕЛЬ	A 7. WPA3	C 8. БРАНДМАУЭР

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ПЕРЕХВАТ	2 СНИФФИНГ	3 ЗЛОЙ ДВОЙНИК	4 ХТТПС
5 ВПН-КЛИЕНТ	6 ТУННЕЛЬ		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 G – ВПАТРИ	2 C – ЗЛОЙДВОЙНИК	3 B – СНИФФИНГ	4 F – ТУННЕЛЬ
5 H – БРАНДМАУЭР	6 A – ПЕРЕХВАТ	7 E – ВПНКЛИЕНТ	8 D – ХТТПС

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить ПЕРЕХВАТ, ПЕРЕХВАТ ПАКЕТОВ и ЗЛОЙ ДВОЙНИК и привести пример для каждого термина.

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

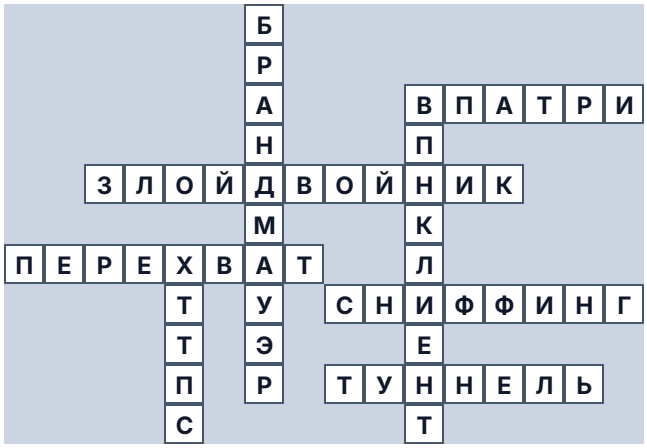
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

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

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

2 по горизонтали: ВПАТРИ Современный стандарт безопасности Wi-Fi. (6 букв)

3 по горизонтали: ЗЛОЙДВОЙНИК Поддельная точка доступа, имитирующая Wi-Fi. (11 букв)

4 по горизонтали: ПЕРЕХВАТ Чтение трафика при передаче. (8 букв)

6 по горизонтали: СНИФФИНГ Захват сетевых пакетов данных. (8 букв)

7 по горизонтали: ТУННЕЛЬ Защищённый путь передачи данных. (7 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: БРАНДМАУЭР Фильтрация входящего трафика. (10 букв)

2 по вертикали: ВПНКЛИЕНТ Зашифрованная виртуальная частная сеть. (9 букв)

5 по вертикали: ХТТПС Защищённая передача веб-данных. (5 букв)

Ключ к словам-перевёртышам и шифру

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

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1.	АЕХПВЕТР	ПЕРЕХВАТ	5.	ФИНГФСНИ	СНИФФИНГ
2.	ДКЛЗИВОНЙОЙ	ЗЛОЙДВОЙНИК	6.	ПХТСТ	ХТТПС
3.	ВИЛПЕТКНН	ВПНКЛИЕНТ	7.	ТЛЕЬУНН	ТУННЕЛЬ
4.	ИТАРВП	ВПАТРИ	8.	ЭНМРБДРАУА	БРАНДМАУЭР

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ШИФРУЙТЕ ТРАФИК ПУБЛИЧНОГО ВАЙФАЯ ЧЕРЕЗ ВПН"

Ответы к кейсам

A Кейс 1: Сдерживание перехвата пакетов в общедоступном Wi-Fi

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: руководитель отдела продаж, работающий удалённо и подключённый к публичному Wi-Fi в аэропорту, замечает, что несколько важных деловых писем утекли вскоре после отправки в открытом виде.
- Рекомендуемая стратегия и решение: Обяжите использовать корпоративный VPN-клиент на всех удалённых рабочих станциях. Разрешите только браузерные расширения с HTTPS и блокируйте незашифрованные протоколы (такие как HTTP и FTP) на клиентском межсетевом экране.

B Кейс 2: Защита от поддельной точки доступа «злой двойник»

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: злоумышленники разворачивают поддельную беспроводную точку доступа с именем «CoffeeShop_Guest», имитирующую настоящую точку доступа кафе, и перехватывают сетевой трафик ничего не подозревающих гостей.
- Рекомендуемая стратегия и решение: проверьте MAC-адреса BSSID точек доступа, чтобы убедиться в подлинности сети. Включите проверку состояния клиента, чтобы блокировать подключение к открытым сетям, и требуйте использовать мобильные точки доступа для конфиденциальной работы.