

Документация на Web-сайт “Aircrack: WPA Handshake”

Информация о проекте

Сайт “Aircrack: WPA Handshake” является учебным проектом, созданным для изучения принципов работы инструментов для тестирования безопасности Wi-Fi сетей стандартов WEP/WPA/WPA2. Сайт посвящен практическому применению пакета программ Aircrack-ng.

Проект специализируется в области информационной безопасности, а именно в демонстрации процесса перехвата и взлома handshake (рукопожатия) Wi-Fi сетей. Сайт предоставляет следующие виды информации и услуг: теоретические сведения о процессе аутентификации в Wi-Fi сетях, пошаговые практические руководства (гайды) по использованию утилит airodump-ng, aireplay-ng, aircrack-ng, консультирование (через контактную форму) по вопросам, связанным с оборудованием и софтом, а также обзор совместимого оборудования (Wi-Fi чипсетов).

Консультирование пользователей позволяет оказывать дополнительные информационные услуги. К ним относятся: помочь в выборе Wi-Fi адаптера с поддержкой режима монитора, объяснение сложных технических моментов, формирование рекомендаций по использованию словарей паролей и т.д.

Цели web-сайта:

- Предоставить энтузиастам и студентам структурированную информацию о высокоеффективных инструментах для тестирования безопасности Wi-Fi сетей из пакета Aircrack-ng.
- Обеспечить проекту постоянный приток заинтересованных пользователей, что предполагает увеличение числа уникальных посетителей и формирование небольшого, но активного сообщества вокруг темы этичного хакинга.
- Обеспечить понятный и наглядный учебный материал, чтобы заинтересовать новичков в сфере кибербезопасности.
- Обеспечить поддержку репутации (имиджа) автора проекта как человека, разбирающегося в теме сетевой безопасности.

Задачи web-сайта:

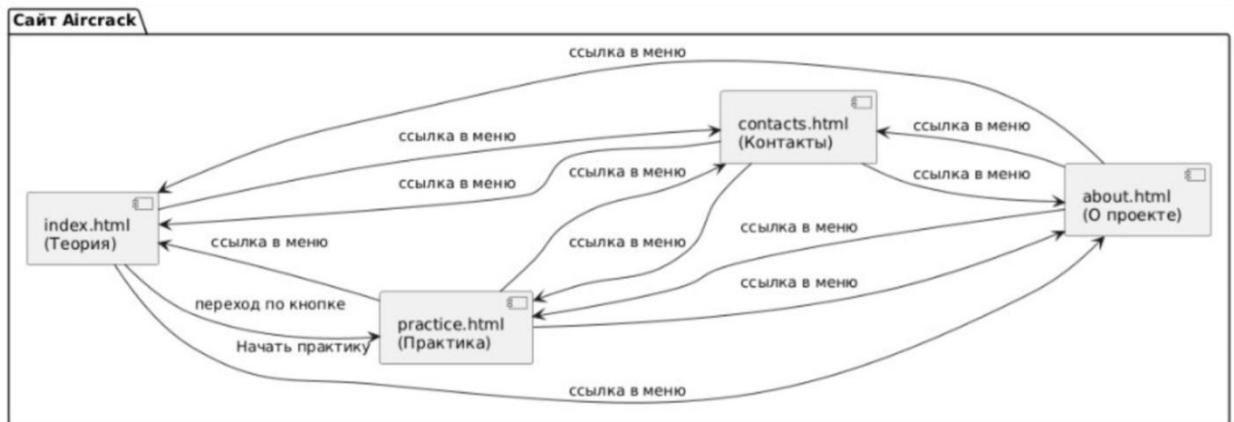
- Предоставить информацию о проекте и его целях.
- Предоставить информацию о теоретических основах WPA2 handshake.
- Предоставить пошаговые инструкции (практику) по захвату handshake.
- Предоставить контактную информацию для обратной связи.
- Предоставить информацию о необходимом оборудовании и словарях.
- Обеспечить круглосуточный доступ к информации.

Целевая аудитория:

- Профессии: начинающие этичные хакеры, студенты ИТ-специальностей, системные администраторы, энтузиасты информационной безопасности, интересующиеся вопросами защиты и взлома Wi-Fi сетей.
- Интересы: Linux (особенно Arch Linux), кибербезопасность, сетевое администрирование, этичный хакинг, использование терминала.
- Местоположение: Россия и русскоязычные пользователи по всему миру.
- Возраст: от 16 лет.
- Пол: любой.
- Язык: русский.
- ОС: только Linux (Arch, Kali, Ubuntu и т.д.).
- Браузеры: современные версии Chrome, Firefox, Safari.
- Время посещения: круглосуточно.
- Уровень пользователей: beginner (начальный), medium (средний).

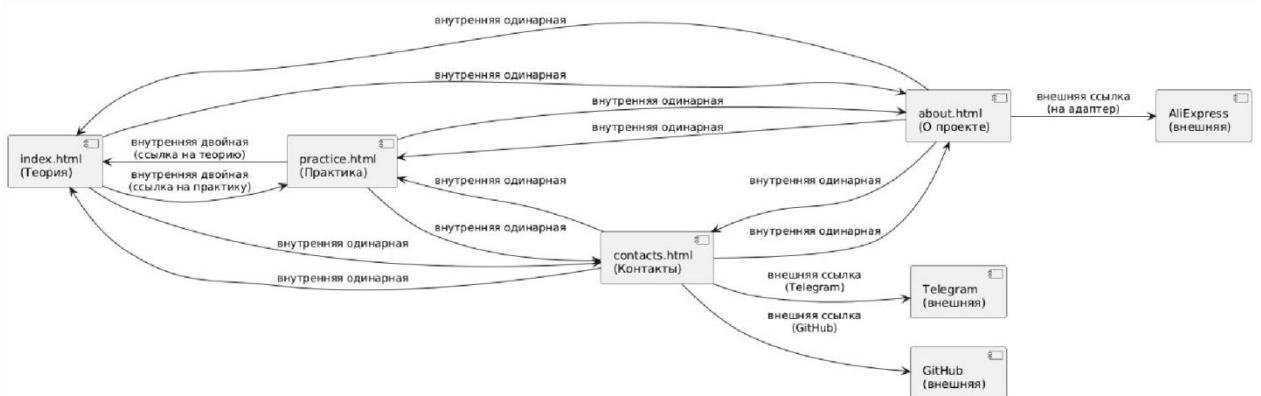
Логическая структура сайта:

Сайт имеет иерархическую логическую структуру.



Навигационная схема сайта:

Данный web-сайт использует иерархическую логическую модель организации сайта. Основная навигация осуществляется через верхнее меню. Дополнительная навигация присутствует в виде призывов к действию (СТА) на страницах, например, ссылка на страницу практики с главной страницы.



Макеты страниц

Homepage(Теория) имеет вид:

```
index.html
├── header
│   ├── строка терминала (user@arch ~ ) sudo airodump-ng wlan0
│   └── навигационная панель [ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]
└── main
    ├── заголовок H1 □ WEP/WPA/WPA2 HANDSHAKE KILLER □
    ├── заголовок H2 (описание handshake)
    ├── текстовый блок (объяснение Wi-Fi handshake)
    ├── ASCII-схема рукопожатия
    ├── терминал (пример вывода airodump-ng с handshake)
    ├── таблица сравнения словарей (rockyou, SecLists, Weakpass)
    └── кнопка [ НАЧАТЬ ПРАКТИКУ ]
└── footer
    ├── повтор навигации (текстовая)
    └── копирайт © 2026 / aircrack-handshake
```

Страница содержит заголовок, блоки с текстом, схему handshake в псевдографике (ASCII), блок с примером вывода терминала, раздел с примерами оборудования и таблицу сравнения словарей. В конце есть крупная кнопка призыва к переходу на практику.

Макет страницы “Практика” имеет вид:

```
practice.html
├── header
│   ├── строка терминала (user@arch ~ ) sudo ./break_wifi.sh
│   └── навигационная панель [ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]
└── main
    ├── заголовок H1 □ AIRCRACK В ДЕЛЕ □
    ├── заголовок H2 (5 шагов к захвату handshake)
    ├── пошаговая инструкция (блоки с командами)
        ├── шаг 1: airmon-ng start wlan0
        ├── шаг 2: airodump-ng wlan0mon
        ├── шаг 3: airodump-ng -c 6 --bssid ... -w capture
        ├── шаг 4: aireplay-ng -0 2 ...
        └── шаг 5: aircrack-ng capture-01.cap -w словарь
    ├── терминал (пример вывода airodump-ng с BSSID и handshake)
    ├── таблица полезных опций aircrack
    └── изображения (примеры оборудования — ASUS, Digma)
└── footer
    ├── повтор навигации (текстовая)
    └── копирайт © 2026 / aircrack-handshake
```

Структура схожа со страницей теории, но основной контент — это пошаговая инструкция, оформленная в виде команд в терминале с комментариями.

Страницы “О проекте” имеют схожую структуру:

```
about.html
├── header
|   ├── строка терминала (user@arch ~❯ whoami)
|   └── навигационная панель [ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]
└── main
    ├── заголовок H1 « ОБ ЭТОМ САЙТЕ »
    ├── заголовок H2 (Проект создан для изучения WPA2 handshake)
    ├── текстовый блок (описание целей проекта)
    ├── сетка основных инструментов
        ├── airodump-ng
        ├── aireplay-ng
        ├── aircrack-ng
        └── hashcat
    ├── таблица Wi-Fi чипсетов с поддержкой режима монитора
        ├── Atheros AR9271
        ├── Ralink RT3070
        ├── Realtek RTL8812AU
        └── Intel (большинство)
    └── карточка адаптера AR9271 со ссылкой на AliExpress
└── footer
    ├── повтор навигации (текстовая)
    └── копирайт © 2026 / aircrack-handshake
```

Заголовок, краткое описание, затем контент в виде сетки (grid) карточек (для инструментов) или формы (для контактов).

Страницы “Контакты” имеет структуру:

```
contacts.html
├── header
|   ├── строка терминала (user@arch ~❯ mail -s "hello" admin)
|   └── навигационная панель [ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]
└── main
    ├── заголовок H1 « СВЯЗАТЬСЯ »
    ├── заголовок H2 (Задай вопрос или предложи идею)
    ├── форма обратной связи
        ├── поле "Имя"
        ├── поле "Email"
        ├── поле "Сообщение"
        └── кнопка [ ОТПРАВИТЬ ]
    └── сетка ссылок
```

```
├── Telegram: @linux_x64
└── GitHub: /DarkUser1onion/site
└── footer
    ├── повтор навигации (текстовая)
    └── копирайт © 2026 / aircrack-handshake
```

Средства реализации Web-сайта:

Web-сайт реализован вручную с помощью HTML5 и CSS3 в vscode на Linux системе. Шрифты подключены через Google Fonts (Audiotwide, Share Tech Mono). Вёрстка адаптивная, с использованием Flexbox и Grid. Иконки (favicon) подготовлены в формате SVG.

Ключевые слова:

Ключевые слова, используемые для поиска: aircrack-ng, WPA2 handshake, взлом wifi, airodump-ng, aireplay-ng, захват рукопожатия, словарь паролей, rockyou.txt, монитор режим, этичный хакинг, информационная безопасность, Kali Linux, Arch Linux.

Цветовая палитра Web-сайта:

Для дизайна была использована тёмная (дарк) цветовая гамма, имитирующая интерфейс терминала и хакерскую эстетику.

Фон

Основной фон страницы - очень тёмный синий (#0a0e12). Текстовая область выделяется не цветом, а контрастностью текста и рамками.

Область текста

Область контента растягивается на всю ширину, но имеет отступы от краёв. Цвет текста светлый, что обеспечивает высокую контрастность на тёмном фоне. Для выделения блоков (например, вывода терминала) используются полупрозрачные фоны и рамки.

Текст

Для данного сайта выбраны два основных шрифта: Share Tech Mono для основного текста и Audiotwide для заголовков. Оба шрифта относятся к моноширинным и рубленым (sansserif), что ассоциируется с компьютерным кодом и терминалом. Это обеспечивает стилистическое единство и удобство чтения технической информации.

В качестве основного цвета текста выбран светло-серый (#a9b1d6). Ключевые элементы (команды, BSSID, предупреждения) выделяются яркими цветами: розовым (#ff79c6), жёлтым (#f1fa8c) и голубым (#8be9fd). Текст на тёмном фоне имеет достаточный контраст, что обеспечивает удобство чтения.

На сайте используются относительные размеры шрифта (rem/em), что дает возможность при необходимости изменять размер отображаемого текста средствами браузера.

Текст имеет выравнивание по левому краю.

Ссылки

Ссылки в тексте и в навигации оформлены как кнопки в прямоугольных скобках [ТЕКСТ], что стилизовано под синтаксис терминала. При наведении цвет меняется на розовый.

Цвет ссылок (бирюзовый, розовый) хорошо виден на тёмном фоне.

Для улучшения восприятия информации используются разделители в виде ASCII символов. Списки часто оформлены маркерами в виде стрелок или отсутствуют, заменяясь отдельными блоками.

Заголовок страницы (Header)

Вместо графического заголовка используется текстовый div с классом sapper, который имитирует строку приглашения в терминале (user@arch ~» команда). Эта строка динамически меняется на каждой странице, задавая ей настроение.

Нижний колонтитул страницы (Footer)

Подвал страницы содержит дублирующую текстовую навигацию и информацию об авторских правах. Выполнен в том же стиле, что и хедер.

Изображения

На сайте используются изображения роутеров и Wi-Fi адаптеров в формате PNG, которые находятся в корне проекта (.images/*). Изображения имеют подписи и служат для визуализации примеров оборудования. Также присутствует иконка сайта в формате SVG.

Главная навигационная панель

Главная навигационная панель расположена в верхней части страницы, под строкой "терминала". Преимущества данного месторасположения:

- Стандартное и привычное для пользователя расположение.
- Находится в непосредственной близости от основного содержимого.

Navigation bar элементы - текстовые ссылки, стилизованные под кнопки.

Каждый элемент навигации может находиться в трех состояниях: пассивном, при наведении курсора и активном (текущая страница). В пассивном состоянии - серый цвет. При наведении - становится розовым. Текущая страница выделена розовым цветом и имеет анимацию пульсации.

На каждой отдельной странице элемент навигации, соответствующий текущей странице, является активным и ссылается сам на себя (хотя технически это ссылка, она ведёт на ту же страницу).

Дополнительная панель навигации по тексту

Внизу каждой страницы располагается Secondary text navigation bar. Она повторяет пункты главной навигации. Для написания использован тот же шрифт. Элементы

разделены слешем (/). Активный элемент, соответствующий текущей странице, не является ссылкой (в коде это просто текст).

Информация об авторских правах

Внизу каждой страницы расположена Copyright информация. Использован текст, выполненный в общем стиле.

Доказательства тестирования кем-либо из целевой аудитории.

Сайт был протестирован 3 пользователями из целевой аудитории. В качестве примера в приложении данного документа приведены результаты теста одного из пользователей.

Краткое описание изменений, внесенных после пользовательского тестирования.

- Были выявлены следующие ошибки и замечания:
- Найдена неверная внешняя ссылка на алиэкспресс, которая ввела на другой сайт.
- Замечено, что на мобильных устройствах neofetch съезжает. Были добавлены несколько @media для разных размеров телефона.
- Изменены виды ссылок, чтобы было понятно, что их можно нажимать.
- Добавлена опция, чтобы при нажатии на ссылки, открывалось новое окно, а не заменяло оригиналный сайтов.
- Изменена таблица со словарями. Теперь на них можно нажать, чтобы перейти на разные словари для брута.

Краткий обзор изменений, внесенных на основе отчета о проверке HTML-кода.

Все страницы были проверены HTML валидатором (The W3C Markup Validation Service <http://validator.w3.org/>), в результате были выявлены различного типа ошибки, например неверно указан , который хорошо работал на движке blink, но мог ломаться на других движках браузерах.

1. Error End tag p seen, but there were open elements.

From line 101, column 102; to line 101, column 105

дбора hash</p>
»

2. Error Unclosed element span.

From line 101, column 29; to line 101, column 47

:ss="note">Характ

Данные ошибки были устраниены и в результате для каждой из страниц получено следующее сообщение:

Check by address ▾

<https://darkuserlonion.github.io/site/index.html>

Check

Document checking completed. No errors or warnings to show.

Used the HTML parser. Externally specified character encoding was UTF-8.
Total execution time 32 milliseconds.

Выводы:

Данный сайт отвечает всем предъявленным к нему требованиям, обеспечивает удобный способ просмотра необходимой информации. Информация хорошо структурирована и визуально выделена, что позволяет быстро найти необходимые команды и пояснения. Выбор цветов и шрифтов создаёт правильную атмосферу и позволяет легко воспринимать техническую информацию.

Дальнейшие планы:

- Добавить страницу с картой сайта (sitemap).
- Добавить интерактивный тест для проверки знаний.
- Расширить раздел "Практика" информацией о взломе WEP и атаке на WPS.
- Добавить страницу с обзором и ссылками на самые эффективные словари паролей.

Внешний вид страниц

index.html

The screenshot shows a web browser window with the title "Aircrack :: Handshake Killer". The URL in the address bar is "darkuseronion.github.io/site/index.html". The page content is as follows:

- Terminal Command:** user@arch ~> sudo airodump-ng wlan0
- Navigation Bar:** [ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]
- Section Header:** ✎ WEP/WPA/WPA2 HANDSHAKE KILLER ✎
- Text:** Ловишь пакеты – получаешь бесплатный WiFi (оффлайн)
- Text:** Wi-Fi НЕ передаёт пароль по воздуху. Вместо этого происходит **рукопожатие (handshake)** между твоим устройством и роутером. Если ты **перехватишь это рукопожатие**, то сможешь **уйти домой** и перебирать пароли на своём компе – сеть больше не нужна.
- Diagram:** A sequence diagram illustrating the WiFi handshake between an Access Point (AP) and a Client. It shows four frames:
 - [AP] -> [Client]: ANonce
 - [Client] -> [AP]: SNonce + MIC
 - [AP] -> [Client]: GTK + MIC
 - [Client] -> [AP]: ACK
- Note:** Базовые пакеты – то, что нужно сохранить. Внутри MIC – слепок пароля.
- Text:** В перехваченном handshake есть:
 - **RMK** – УЗЫ от пароля в виде сети

Aircrack :: Handshakes

darkuserionion.github.io/site/index.html

user@arch ~> sudo aircrack-ng capture-wi.cap -w /usr/share/wordlists/rockyou.txt

[ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]

user@arch ~> sudo airodump-ng wlan0

→ Пример подбора пароля, через aircrack-ng →

TP-Link Archer D714 поддерживает монитор-режим

D-Link DIR-825 работает с aircrack

Сравнение словарей

Словарь	Размер	Скорость подбора
rockyou.txt	14 млн	>2 мин
Seclists	~500 МБ	>30 мин
Weakpass	>1 млрд	часы

Aircrack :: Handshakes

darkuserionion.github.io/site/index.html

user@arch ~> sudo airodump-ng wlan0

[ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]

```
Packages: 1700 (распаковано)
Shell: fish 4.4.0
Resolution: 1080x1920, 1920x1080
WM: bspwm
Theme: TokyoNight-zk [GTK2], Dracula-pink-accent [GTK3]
Icons: TokyoNight-SE [GTK2], dracula-icons-main [GTK3]
Terminal: alacritty
CPU: Intel Xeon E5-2666 v3 (20) @ 3.50GHz
GPU: NVIDIA GeForce RTX 2060 SUPER
Memory: 8550MiB / 31924MiB
CPU Usage: 12%
Disk (/): 137G / 234G (62%)
```

Хочешь хакнуть WiFi соседа свой?

Переходи на страницу практики – там пошаговая инструкция с командами.

[НАЧАТЬ ПРАКТИКУ]

Применение инструмента для взлома чужих сетей без разрешения владельца незаконно и может повлечь за собой административную ответственность. А за эксплуатацию уязвимостей в сети, взлом устройств и снiffинг – это уже уголовное (Статья 272,273,274) сроком до 4 лет.

practice.html

Aircrack :: Практика + https://darkuserionion.github.io/site/practice.html

```
user@arch ~> sudo aircrack-ng capture.cap -w rockyou.txt
```

[ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]

✗ AIRCRACK В ДЕЛЕ ✗

5 шагов к захвату handshake

Всё делается в терминале от root (или под sudo). Убедись, что Wi-Fi адаптер поддерживает режим монитора.

ШАГ 1. Включаем монитор-режим
user@arch ~> sudo airmon-ng start wlan0

| airmon-ng start | переводит интерфейс wlan0 в режим монитора (появится wlan0mon).

ШАГ 2. Смотрим эфир
user@arch ~> sudo airodump-ng wlan0mon

| airodump-ng | показывает все точки доступа и клиенты в радиусе действия.

ШАГ 3. Фокусируемся на цели
user@arch ~> sudo airodump-ng -c 6 --bssid 00:1A:2B:3C:4D:5E -w capture wlan0mon

Aircrack :: Практика + https://darkuserionion.github.io/site/practice.html

```
user@arch ~> sudo aircrack-ng capture.cap -w rockyou.txt
```

[ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]

Полезные опции aircrack

Команда	Описание
-w словарь	Указать путь к словарю
-b BSSID	Атака только на конкретную точку
-e ESSID	Фильтр по имени сети
-p	Использовать PTW-атаку (для WEP)

↔ Пример подбора пароля, через aircrack-ng ↔

```
Aircrack-ng 1.7
[00:00:02]: 23820/13244188 keys tested (1072.38 k/s)
Time left: 22 minutes, 15 seconds          0.1%  

Current passphrase: 1452044113
```

Master Key : E5 48 97 09 76 70 80 05 92 88 04 84 08 35 04 42
18 C4 50 99 0C A0 44 EE 0E 20 3C 56 09 02 48 05

Transient Key : 49 2C 02 0C F9 00 4C C3 09 42 08 06 95 09 28 00
35 04 34 00 81 23 FA 39 09 C2 F2 F3 C9 07 30 0A
56 54 30 00 0E 05 95 03 0C 00 0E 00 30 01 00 04

EAPOL HMAC : C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```
Aircrack-ng 1.7.2
[00:00:02]: 175 keys tested (131.48 k/s)
Time left: 8 seconds           100.00%
KEY FOUND! [ user@00:00:00 ]
```

Master Key : 05 38 04 01 04 04 0C 27 04 95 04 0C 27 02 02
07 75 13 01 00 00 0F 02 03 00 00 00 00 00 00 03

Transient Key : 04 09 02 02 02 02 02 02 02 02 02 02 02 02 02 02
04 09 02 02 02 02 02 02 02 02 02 02 02 02 02 02
C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 75 AE 22 49 59 00 00 01 00 11 02 02 04 0F 00 00

Digma DMR-N301
самый дешевый роутер

about.html

Aircrack :: 0 про...

https://darkuseronion.github.io/site/about.html

user@arch ~> whoami

[ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]

❶ ОБ ЭТОМ САЙТЕ ❷

Проект создан для изучения WPA2 handshake

Этот сайт – учебный проект по курсу HTML5 + CSS3. Тема: этичный хакинг, инструмент Aircrack-ng. Здесь ты найдёшь теорию, практические примеры и полезные ссылки о том, как эффективно ломать сети.

Основные инструменты

airodump-ng Захват пакетов, поиск сетей	aireplay-ng Деаутентификация, инъекции	aircrack-ng Взлом через словарь	hashcat GPU-брутфорс
--	---	------------------------------------	-------------------------

Поддерживаемые Wi-Fi чипсеты

Чипсет	Режим монитора	Инъекции
Atheros AR9271	✓	✓
Ralink RT3070	✓	✓
Realtek RTL8812AU	✓	✓
Intel (большинство)	✗	✗

Aircrack :: 0 про...

https://darkuseronion.github.io/site/about.html

user@arch ~> whoami

[ТЕОРИЯ] [ПРАКТИКА] [О ПРОЕКТЕ] [КОНТАКТЫ]

Realtek RTL8812AU	✓	✓
Intel (большинство)	✗	✗

**Powerful Chip
Atheros AR9271**
Built in high performance Chip Atheros AR9271
2.4GHz band up to 150Mbps
Adapt 802.11bgn new wireless transmission technology

Аналог легендарной
ALFA

КУПИТЬ

PCI-E wireless network card
Ralink Model: RT3070 2D

Аналог для ноутбуков

КУПИТЬ

contacts.html

