

# ИНФОРМАЦИОННЫЙ ПЕРИМЕТР WI-FI



# Назначение

---

**Информационный периметр Wi-Fi** - система для обнаружения и противодействия атакам на сети Wi-Fi. Автоматически выявляет угрозы безопасности и блокирует атаки.

**Сайт:** [wifisecurity.ru](http://wifisecurity.ru)

## Актуальность

---

- сети Wi-Fi используются повсеместно, каждое подключаемое устройство может быть атаковано (точки доступа, телефоны, устройства IoT)
- средства атаки на сети Wi-Fi распространены и доступны «новичкам» (Kali Linux, Android, Pineapple Wi-Fi)
- проведение атак на Wi-Fi - уголовное преступление (надо обнаруживать и документировать)

# Функции

- обнаружение атак и инцидентов безопасности, отображение информации о них
- автоматическая защита (путём блокирования и нарушения работы устройств и сетей злоумышленников)
- подача сигнала тревоги для заданных событий, оповещение ответственных сотрудников по Email и через SIEM (Security Information and Event Management) систему
- сохранение информации для расследования (запись трафика на внутренний накопитель или на внешнее сетевое хранилище по протоколу SMB)

# Функции

- отображение сетей, устройств и их параметров в реальном времени в виде таблицы
- отображение сетей на спектре с уровнями мощности в точке приема
- ведение базы данных обнаруженных сетей и устройств, истории их активности
- расширенный поиск по истории активности сетей и устройств, экспорт результатов поиска в CSV и Excel
- интеграция с SIEM (поддержка сетевого протокола syslog)
- обновление ПО и баз атак при подключении к Internet

# Обнаруживаемые атаки и их последствия

---

- **дешифрование трафика** (кража личных данных и паролей)
- **несанкционированное подключение к сети** (воздействие на компьютеры и устройства, подключенные к сети, передача ложной информации, несанкционированный доступ к сети Интернет)
- **создание фальшивых точек доступа** (перехват личных данных и паролей, подмена информации передаваемой в сети, заражение подключаемых устройств, перехват управления устройствами)

# Обнаруживаемые атаки и их последствия

---

- **создание несанкционированных сетей** (передача информации из контролируемой зоны, нарушение политик безопасности сотрудниками )
- **Denial of Service** (нарушение работы сети)

# Характеристики сенсора

- Поддержка 802.11 a/b/g/n/ac, 2.4/5 ГГц
- Одновременный прием 4 каналов
- Сеть 1 Гбит Ethernet
- CPU ARM 1.5 ГГц (4 ядра)
- 1 Гбайт ОЗУ (DDR3)
- Внутренний накопитель до 256 Гбайт





# Web-интерфейс

Старт Сноп Спектр Трафик Аналитика Настройки Справка

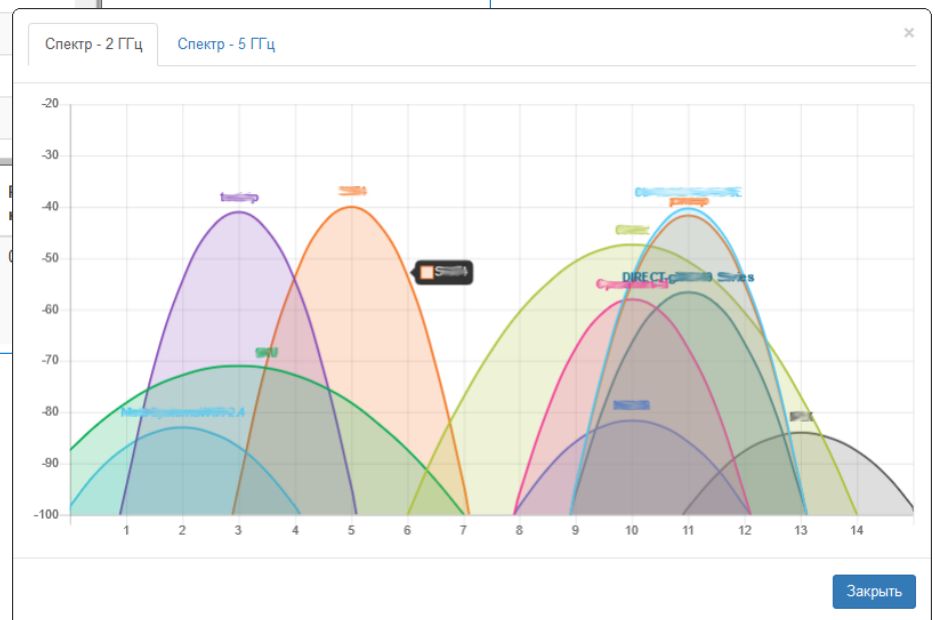
Тип	MAC	Обнаружено	Поиск SSID	Информация	dBm	Кадров
🏠	AsustekC_E6:B2:F0	desert	WPA2	7	1	18
🏠	D-Linkln_91:6A:FB	DIR-300NRU	WPA2	13	1	76
📶	62:6C:66:79:EA:0A	DIRECT-RRDESKTOP-LS7HD11msHu	WPA2	11	1	34
🏠	Netgear_81:3F:5D	HOME-NET	WPA	5	1	10
🏠	D-Linkln_33:BB:28	IPWF-T	WPA2	8 ▼	1	481
🏠	Motorola_D0:2A:15	IPWF-T	WPA2	1	1	7
🏠	ZyxeCom_03:C2:78	Keenetic-5045	WPA2	10 ▼	1	28
🏠	Sercomm_5E:1E:FE	MGTS_GPON5_2688	WPA2	36 ▲	1	56
🏠	3C:98:72:35:01:63	MGTS_GPON5_5010	WPA2	36 ▲	1	58
🏠	Zte_D9:B2:CE	MGTS_GPON_1D13	WPA2	7	1	58
🏠	Sercomm_5E:1E:FD	MGTS_GPON_2688	WPA2	1	1	13
🏠	3C:98:72:35:01:64	MGTS_GPON_5010	WPA2	1	1	6

Время	Событие
2019.01.31 11:45:29	Обнаружена сеть XiaomiEI_6A:05:61
2019.01.31 11:45:33	Обнаружена сеть Sercomm_5E:1E:FD
2019.01.31 11:45:33	Обнаружена сеть D-Linkln_DF:9C:D3
2019.01.31 11:46:35	SSID (IPWF-T) не защищаемой сети Motorola_D0:2A:15 совпадает с SSID защищаемой сети D-Linkln_33:BB:28

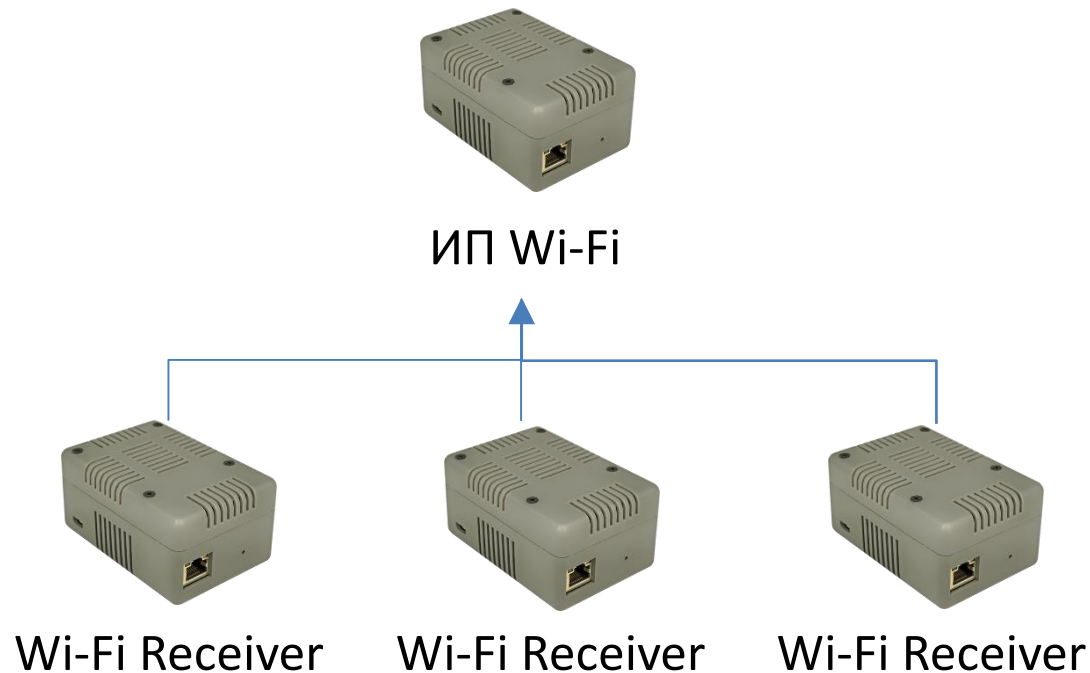
  

Тип	MAC	Обнаружено	Поиск SSID	Информация	dBm	Кадров
🏠	D-Linkln_33:BB:28	2019.01.31 11:45:23	WPS: BroadcomAP (Broadcom, 123456, Broadcom) [Network Infrastructure - AP]	-59	481	



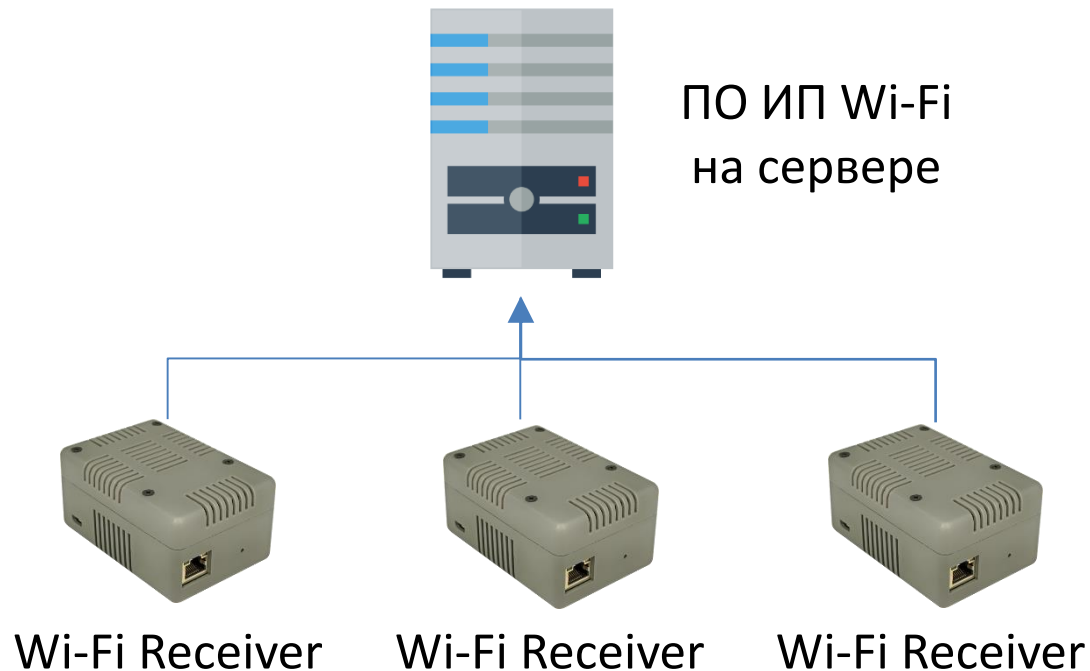
# Варианты построения СОА

1. Автономный сенсор ИП Wi-Fi
2. Сенсор ИП Wi-Fi + расширители каналности «Wi-Fi Receiver»



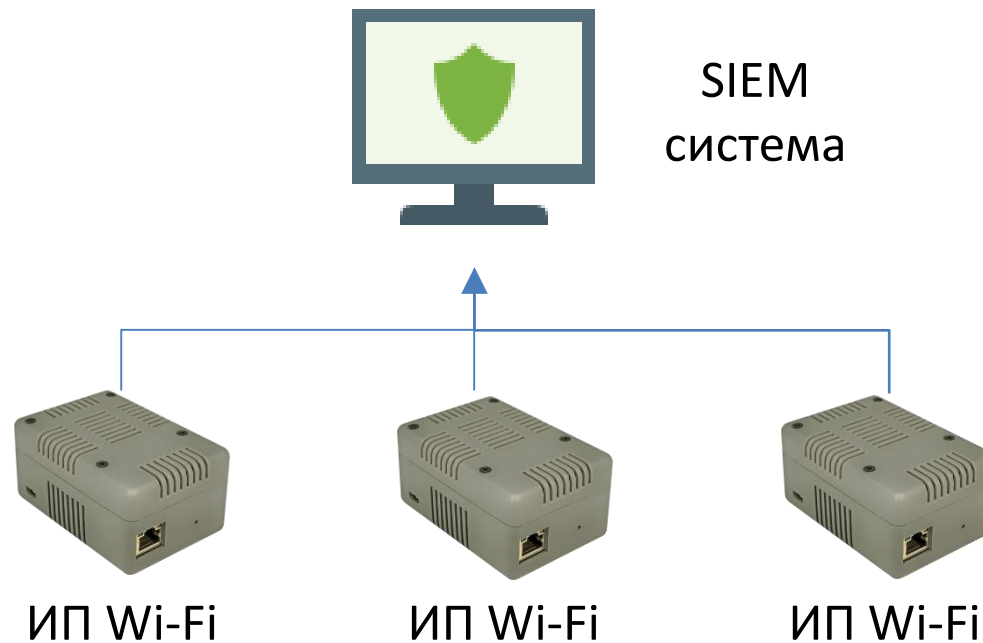
# Варианты построения СОА

3. Клиент-сервер (ИП Wi-Fi на сервере + приемники «Wi-Fi Receiver»)



# Варианты построения СОА

4. Подключение нескольких систем ИП Wi-Fi к SIEM системе (Security Information and Event Management)



# Уникальные преимущества

---

- ✓ Для работы не требуется компьютер и установка ПО. Все функции реализованы в устройстве, взаимодействие с пользователем через Web-интерфейс
- ✓ В базе данных сохраняются интервалы активности устройств и сетей, их идентификационная информация. Расширенный поиск по базе данных с возможностью построения отчетов.
- ✓ Собственная разработка ПО и схемотехники сенсора (используется элементная база общего назначения зарубежного производства)
- ✓ Готовность к проведению проверки на НДС

**Спасибо за внимание!**

wifisecurity.ru