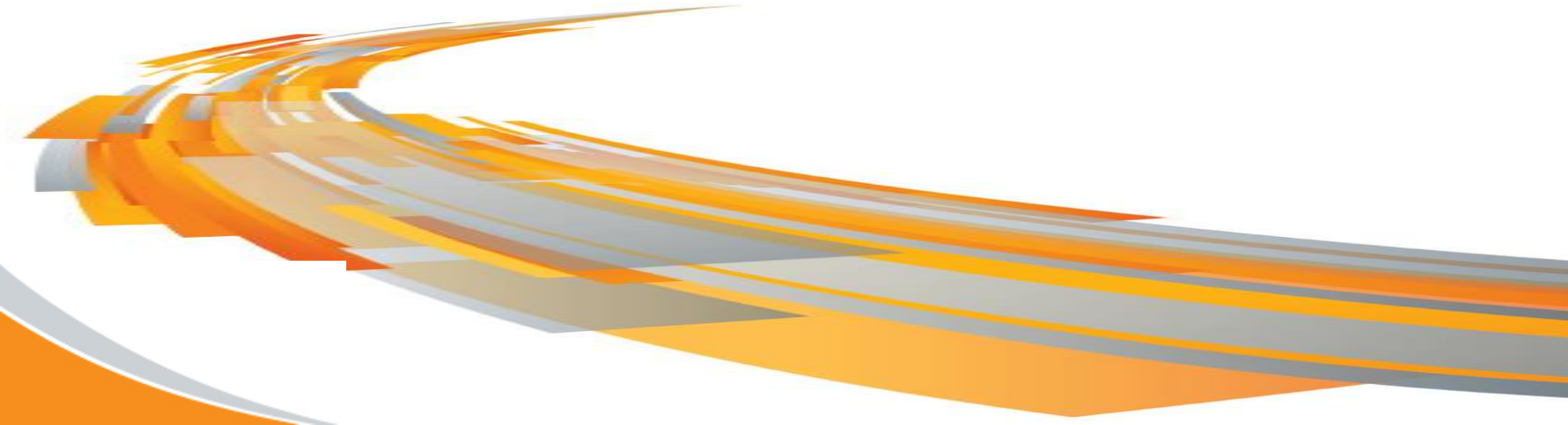
ИНФОРМАЦИОННЫЙ ПЕРИМЕТР WI-FI



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

СИНТЕЛС

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)

СИНТЕЛС

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

СИНТЕЛС

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

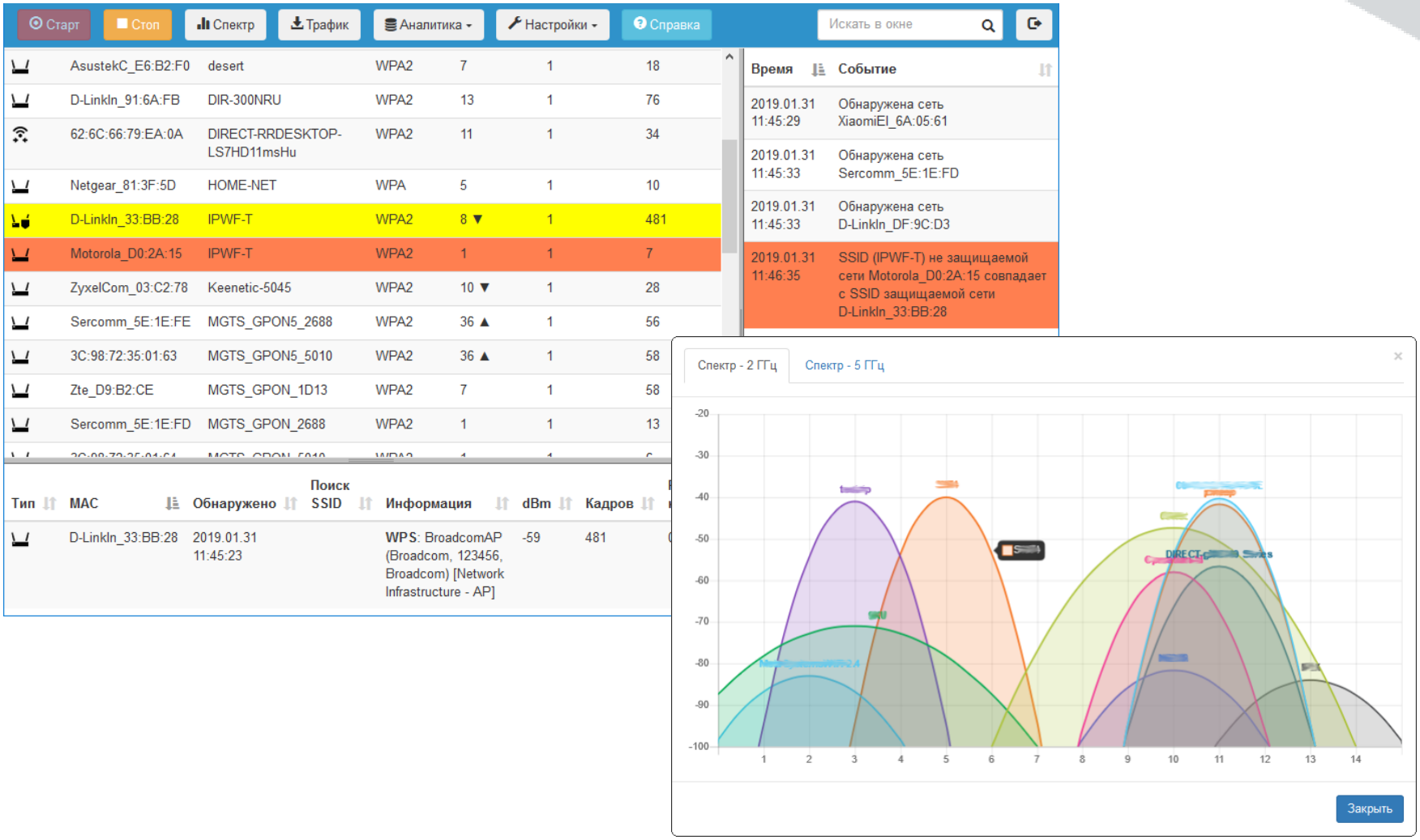
- **создание несанкционированных сетей** (передача информации из контролируемой зоны, нарушение политик безопасности сотрудниками)
- **Denial of Service** (нарушение работы сети)

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

СИНТЕЛС

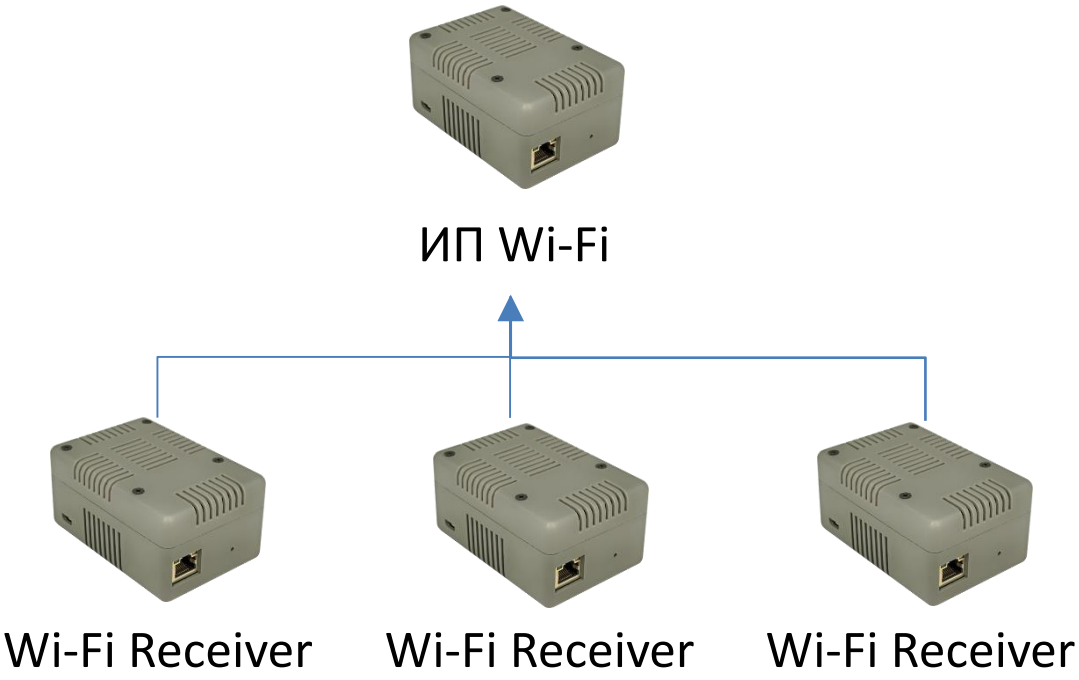
Web-интерфейс



СИНТЕЛС

Варианты построения СОА

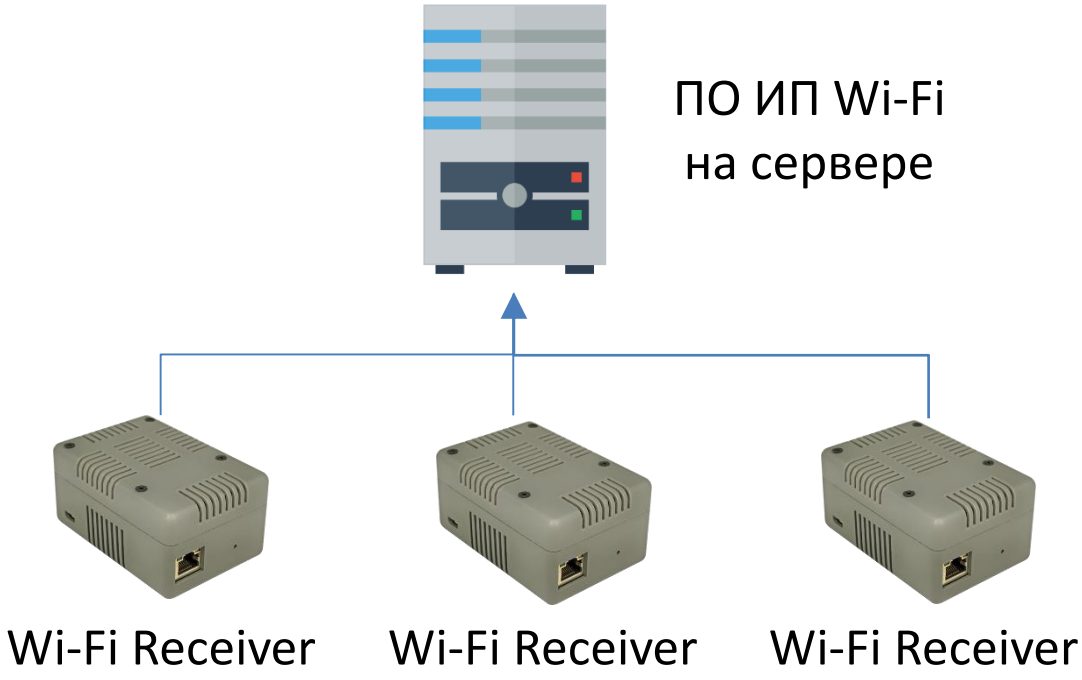
1. Автономный сенсор ИП Wi-Fi
2. Сенсор ИП Wi-Fi + расширители канальности «Wi-Fi Receiver»



СИНТЕЛС

Варианты построения СОА

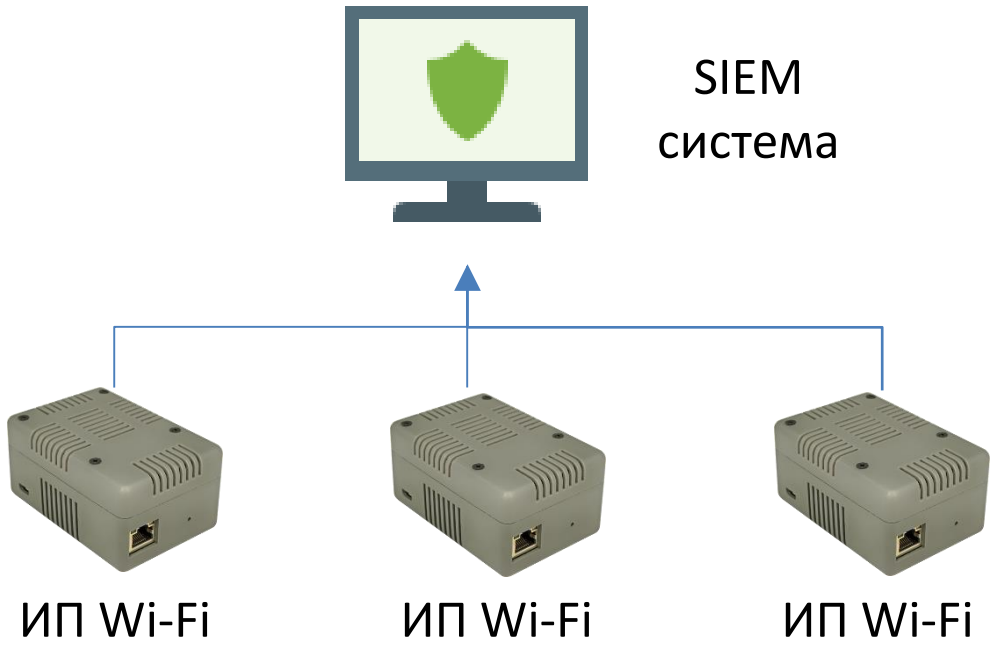
3. Клиент-сервер (ИП Wi-Fi на сервере + приемники «Wi-Fi Receiver»)



СИНТЕЛС

Варианты построения СОА

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



СИНТЕЛС

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 НДВ

СИНТЕЛС

Спасибо за внимание!

wifisecurity.ru