Программно-аппаратное средство мониторинга безопасности Wi-Fi сетей с применением одноплатного компьютера и набора адаптеров

Д.С. Буренок

***Аннотация* — При применении технологии Wi-Fi в рамках информационной системы согласно ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ владелец информационной системы обязан предпринять меры по защите беспроводной сети от воздействий угроз информационной безопасности, обеспечить своевременное обнаружение и фиксацию фактов реализации угроз. Распространенные средства для защиты Wi-Fi сетей обладают рядом недостатков, среди которых необходимость замены уже используемых точек доступа в основе сети на другие модели единственного производителя с функционалом по обнаружению атак, а также сложность слаженного применения автономных средств мониторинга радиоэфира для обнаружения пространственно распределенных атак. Для преодоления перечисленных недостатков автором спроектировано программно-аппаратное средство, поддерживающее сетевой режим работы с централизованным управлением и позволяющее производить обнаружение атак в пределах большого пространства без замены Wi-Fi оборудования. В основу решения заложена модульная конфигурация, обеспечивающая возможность масштабирования посредством изменения состава программно-аппаратной части для повышения производительности и добавления отдельных функций. В статье подробно описывается проектирование программно-аппаратной части, включающей одноплатный компьютер, набор сетевых устройств (Wi-Fi адаптеров с поддержкой режима мониторинга), а также интегрированный многопоточный модуль управления на языке Python. Серверная часть средства и алгоритм обнаружения атак описываются в общих чертах, являются предметом других публикаций. Новизна предложения заключается в применении набора Wi-Fi адаптеров, что позволяет использовать средство для работы на различных радиоканалах в различных режимах единовременно и способствует своевременному обнаружению атак, а также в системном подходе к управлению процессом сканирования, что позволяет централизованно управлять множеством представленных средств для увеличения пространства обнаружения атак. Элементы решения зарегистрированы в качестве объекта интеллектуальной собственности в Роспатенте.**

***Ключевые слова*—Wi-Fi, обнаружение атак на Wi-Fi сеть, сканирование, программно-аппаратное средство, датчик, Wi-Fi адаптер, режим мониторинга.**

I. Введение

Технология Wi-Fi получила широкое распространение, обеспечивая устойчивую связь средств вычислительной техники посредством беспроводной передачи данных по радиоволнам. Наряду со значимыми преимуществами, характеризующимися удобством использования и снижением издержек на прокладку кабельных линий связи, технология Wi-Fi подвержена ряду атак, в числе которых атака поддельной точки доступа и атака деаутентификации. Угрозы проведения соответствующих атак известны и включены в Банк данных угроз ФСТЭК России [1, УБИ.011 и УБИ.126].

С учетом тенденции к расширению диапазонов радиочастот и увеличению общего количества выделенных радиоканалов в стандартах семейства IEEE 802.11 практический интерес представляет средство, позволяющее осуществлять мониторинг безопасности Wi-Fi сетей и своевременное обнаружение атак в широком диапазоне радиочастот в пределах контролируемого пространства. Задачей исследования является проектирование программно-аппаратного средства (далее – датчик), поддерживающего централизованное управление и позволяющего проводить сканирование радиочастотных диапазонов Wi-Fi с использованием набора Wi-Fi адаптеров, каждый из которых производит прием пакетов на заданных радиоканалах. В работе также представлены результаты апробации экспериментального образца спроектированного датчика, реализованного на базе одноплатного компьютера Orange Pi Zero 2, а также Wi-Fi адаптеров Blueway N9000 и Alfa AWUS036ACHM, в совокупности обеспечивающих перекрытие радиочастотных диапазонов Wi Fi 2,4 и 5 ГГц. Процесс сканирования управлялся реализованным на языке программирования Python программным модулем, который был интегрирован в среду операционной системы Linux.

Пример, поясняющий применение спроектированного датчика, представлен на рисунке 1. В качестве исходной обстановки (на рисунке слева) принято, что защищаемая Wi-Fi сеть «secure-network» поддерживается двумя

Статья получена 13 мая 2024. Исследование проведено при поддержке гранта ФГБУ «Фонд содействия развитию малых форм предприятий в научно-технической сфере».

Буренок Дмитрий Сергеевич, студент 2 курса магистратуры кафедры «Информационная безопасность» НИУ «МИЭТ», Москва (e-mail: corr.dmitry@yahoo.com)

точками доступа, расположенными в помещении, в котором также установлен датчик. Датчик оснащен двумя Wi-Fi адаптерами, каждый из которых сканирует заданные радиоканалы. При изменении в составе точек доступа (добавлены две новые точки доступа – на рисунке справа) датчик зафиксирует соответствующее изменение. Так как одна из добавленных точек доступа имеет имя сети «secure-network», но ее MAC-адрес и другие параметры не известны датчику, то им будет обнаружена атака поддельной точки доступа и оповещено лицо, принимающее решение. Один из Wi-Fi адаптеров датчика может перейти на режим сканирования только того радиоканала, на котором функционирует поддельная точка доступа, а другой продолжить сканирование в широком диапазоне радиочастот. Таким образом будет возможно принимать и анализировать пакеты, адресатом и адресантом которых является устройство злоумышленника, не прекращая сканирование других радиоканалов. В том числе, будет возможно непрерывно определять силу сигнала, исходящего от устройства злоумышленника, что может быть использовано в качестве входных данных для определения его местоположения.

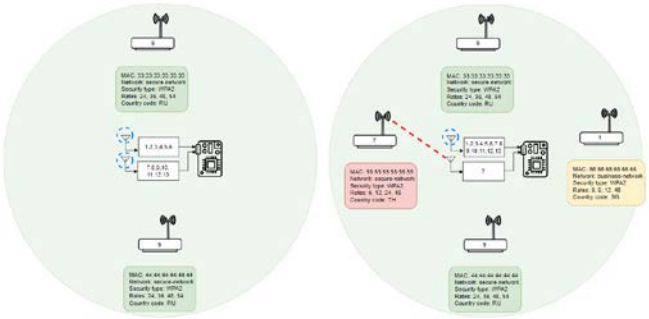


Рисунок 1 – Пример работы датчика

Посредством установки соответствующих датчиков в пределах контролируемого пространства и централизованного управления ими достигается увеличение зоны покрытия обнаружения атак. Общая схема, на которой отображено применение датчиков в сетевом варианте использования, представлена на рисунке 2. Лицо, принимающее решение, через веб-интерфейс в режиме реального времени может отслеживать сообщения об атаках, генерируемые датчиками, и на основе полученной информации предпринимать последующие действия для расследования инцидента.

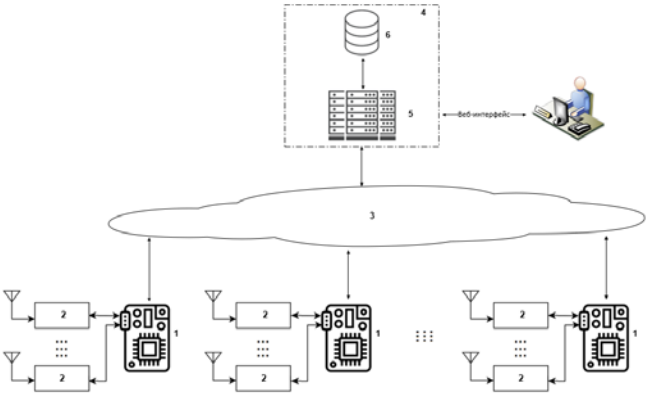


Рисунок 2 – Применение датчиков при сетевом использовании. Обозначения: 1 – датчик; 2 – Wi-Fi адаптер; 3 – общая компьютерная сеть; 4 – серверная часть; 5 – сервер приложений; 6 – база данных.

II. Сканирование радиочастотных диапазонов Wi-Fi

A. Классы программно-аппаратных средств, обеспечивающих обнаружение атак на Wi-Fi сеть

Обнаружение атак на Wi-Fi сети может быть реализовано посредством анализа передаваемых по радиочастотным диапазонам Wi-Fi пакетов (по тексту статьи слово "пакет" синонимично слову "кадр") на предмет наличия признаков осуществления атаки. В результате изучения источников в предметной области, в том числе [2, 3], было выделено два укрупненных класса средств, которые позволяют осуществлять мониторинг безопасности Wi-Fi сетей – таблица 1.

Таблица 1 – Классы средств мониторинга безопасности Wi-Fi сетей

Класс средства	Ключевые особенности
Специализированные точки доступа Wi-Fi	Точка доступа может осуществлять анализ адресованных ей пакетов на предмет наличия признаков атаки. Кроме того, точка доступа может быть оснащена дополнительным приемо-передатчиком, который будет осуществлять сканирование радиочастотных диапазонов Wi-Fi, захват и анализ пакетов, адресованных абонентским устройствам и другим точкам доступа. Для соответствующей цели может также использоваться только основной приемопередатчик, который будет поочередно работать как точка доступа либо проводить сканирование.
Внешние датчики	Применяются внешние приемо-передающие устройства, осуществляющие сканирование радиочастотных диапазонов Wi-Fi, захват пакетов и их анализ на предмет наличия признаков осуществления атаки.

Следует отметить, что применение специализированных точек доступа для обнаружения атак может быть результативно, если для поддержания Wi-Fi сети применяются совместимые точки доступа единого вендора. В таком случае будут отсутствовать зоны, в которых не обеспечено покрытие специализированными точками доступа и не осуществляется обнаружение атак. Следовательно, при применении данных средств потребуется замена оборудования в основе Wi-Fi сети, что повлечет дополнительные материальные издержки и выделение

рабочего времени.

Применение внешних датчиков в данном контексте обладает рядом преимуществ, в том числе не требуется замена уже функционирующих точек доступа и иного телекоммуникационного оборудования в основе Wi-Fi сети. Внешние датчики устанавливаются вблизи уже функционирующих точек доступа Wi-Fi и работают независимо от них.

Дальнейшее исследование сконцентрировано на проектировании программно-аппаратного средства (внешнего датчика), позволяющего результативно осуществлять сканирование радиочастотных диапазонов Wi-Fi, принимать пакеты и обеспечивать их последующий анализ.

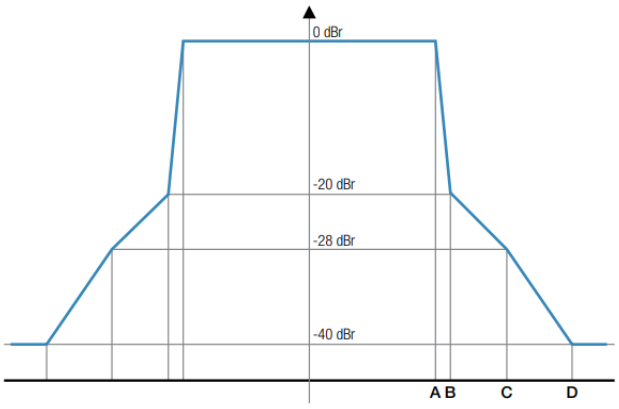
B. Канальное деление радиочастотных диапазонов Wi-Fi

Наиболее распространены радиочастотные диапазоны Wi-Fi 2,4 и 5 ГГц. В последнем поколении приемо-передающего оборудования также поддерживается радиочастотный диапазон 6 ГГц, сертифицированный организацией Wi-Fi Alliance в рамках стандартов IEEE 802.11ax, IEEE 802.11be.

Каждый радиочастотный диапазон Wi-Fi разделен на радиоканалы, сводный перечень номеров и радиочастот соответствующих радиоканалов представлен в [4]. В России решениями Государственной комиссии по радиочастотам одобрена к применению большая часть из определенных стандартами семейства IEEE 802.11 радиоканалов.

Согласно стандартам IEEE 802.11n и IEEE 802.11ac в диапазоне 2,4 ГГц выделено 13 каналов, в диапазоне 5 ГГц выделено до 25 каналов. Каждый канал имеет номинальную ширину 20 МГц, причем для стандарта IEEE 802.11n допускается объединение каналов (channel bonding) с результирующей номинальной шириной 40 МГц, для стандарта 802.11ac – с результирующей номинальной шириной 40 МГц, 80 МГц или 160 МГц.

Ширина радиоканала определяется маской [5], применяемой к спектру радиосигнала – рисунок 3. При подстройке приемо-передающего устройства на частоты заданного радиоканала им, как правило, будет возможно принимать пакеты, отправленные в пределах данного радиоканала, а передаваемые по другим радиоканалам пакеты не будут захвачены.



Channel Size	A	B	C	D
20 MHz	9 MHz	11 MHz	20 MHz	30 MHz
40 MHz	19 MHz	21 MHz	40 MHz	60 MHz
80 MHz	39 MHz	41 MHz	80 MHz	120 MHz
160 MHz	79 MHz	81 MHz	160 MHz	240 MHz

Рисунок 3 – Спектральная маска Wi-Fi

Отметим, что возможны ситуации, когда настроенный на заданный радиоканал в диапазоне 2,4 ГГц Wi-Fi адаптер может принимать передаваемые по другим смежным радиоканалам пакеты ввиду просачивания сигнала (bleed-through signal). На рисунке 4 представлено наложение спектральных масок для непересекающихся каналов 1, 6 и 11. Разница уровня сигнала на пересекающихся каналах может быть меньше 20 дБ по отношении к опорному уровню, что может привести к приему пакета, передаваемого по смежным радиоканалам.

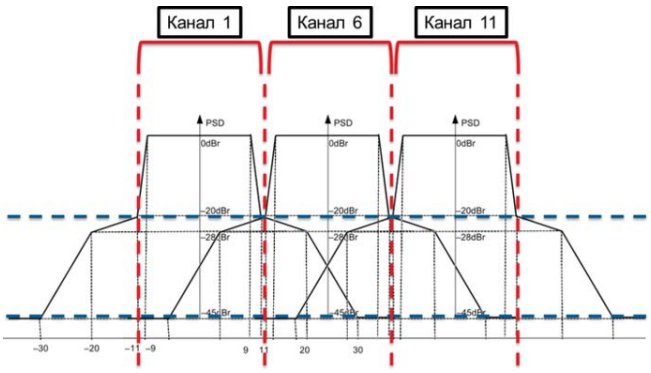


Рисунок 4 – Наложение спектральных масок в диапазоне 2,4 ГГц

Таким образом, проектируемый датчик для сканирования всех радиочастотных диапазонов Wi-Fi должен осуществлять переключение между каналами (channel hopping). Для увеличения общей доли принимаемых пакетов предлагается использовать несколько единовременно работающих приемо-передатчиков, каждый из которых сканирует заданный набор радиоканалов.

C. Совместимые приемо-передающие устройства, работающие в радиочастотных диапазонах Wi-Fi

Проведение сканирования радиочастотных диапазонов Wi-Fi возможно с применением приемо-передающего устройства, поддерживающего работу в соответствующем частотном диапазоне, а также способного демодулировать радиосигнал. В таблице 2 представлен перечень типов устройств, с

использованием которых возможно [6, 7, 8] осуществлять сканирование радиочастотных диапазонов Wi-Fi.

ТАБЛИЦА 2 – ТИПЫ ПРИЕМНЫХ И ПРИЕМО-ПЕРЕДАЮЩИХ УСТРОЙСТВ, СПОСОБНЫХ ОСУЩЕСТВЛЯТЬ МОНИТОРИНГ РАДИОЧАСТОТНЫХ ДИАПАЗОНОВ WI-FI

Тип устройства	Пример устройства
Плата на базе встроенной интегральной микросхемы, поддерживающей стандарты семейства IEEE 802.11	TP-Link TL-WN722N Alfa AWUS036 ACHM Blueway N9000
SDR-система с поддержкой диапазонов 2,4, 5 или 6 ГГц, достаточной шириной полосы пропускания и частотой дискретизации	MicroPhase ANTSDR e316 Pluto Plus Ettus USRP B210
Анализатор спектра либо широкополосный приемник с демодулятором и программным модулем анализа пакетов	Tektronix RSA306

SDR-системы и анализаторы спектра, как правило, обладают более высокими техническими характеристиками и используются для работы на уровне радиосигналов, включая поиск интерференции [9] и местоположения источника Wi-Fi сигнала. Применение соответствующих устройств для приема Wi-Fi пакетов менее распространено ввиду сравнительно высокой стоимости и массогабаритных характеристик, а также необходимости осуществлять предварительную работу с принятым радиосигналом, включая демодуляцию и передачу последовательности бит программному модулю анализа пакетов.

Наибольшее распространение для взаимодействия с Wi-Fi на уровне приема и передачи пакетов получили приемо-передающие устройства, реализованные на базе интегральных микросхем, поддерживающих стандарты семейства IEEE 802.11. Соответствующие микросхемы входят в состав Wi-Fi адаптеров, Wi-Fi роутеров, плат-расширений, обеспечивают обработку радиосигнала и позволяют через драйверы работать с данными на уровне пакетов. Микросхемы могут поддерживать один из следующих основных режимов работы: Master (точка доступа), Managed (адаптер), Ad-hoc (самоорганизующаяся сеть), Repeater (ретранслятор), Mesh (иерархичная сеть с несколькими переходами), Wi-Fi Direct (прямое подключение P2P), TDLS (туннелированное прямое подключение в пределах Wi-Fi сети), Monitor mode (режим мониторинга пакетов).

На рисунке 5 в качестве примера представлена плата Wi-Fi адаптера TP-Link TL-WN722N с приемо-передатчиком на базе микросхемы RTL8188EUS. Подобные чипы разрабатываются изготовителями для обеспечения совместимости с определенными стандартами семейства IEEE 802.11 (a, b, g, n, ac, ax, be и др.).

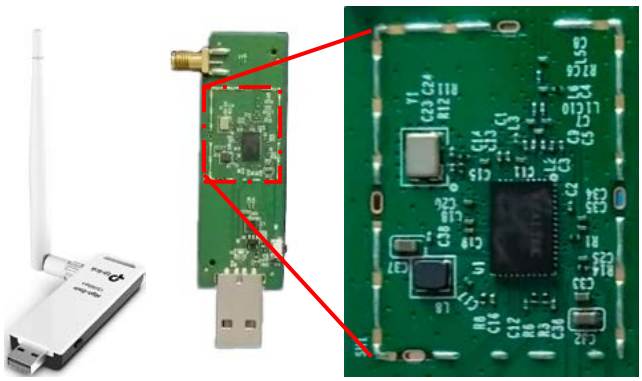


Рисунок 5 – Wi-Fi адаптер TP-Link TL-WN722N

Микросхема может совмещать в себе функции передатчика, приемника, а также контролера WLAN MAC и USB – рисунок 6. В рассматриваемом примере управление работой Wi-Fi адаптера осуществляется по интерфейсу USB 2.0. Средство вычислительной техники, управляющее работой Wi-Fi адаптера, может перевести его в стандартный режим, режим мониторинга пакетов, режим точки доступа. Также возможна отправка предварительно сформированных пакетов Wi-Fi (frame injection).

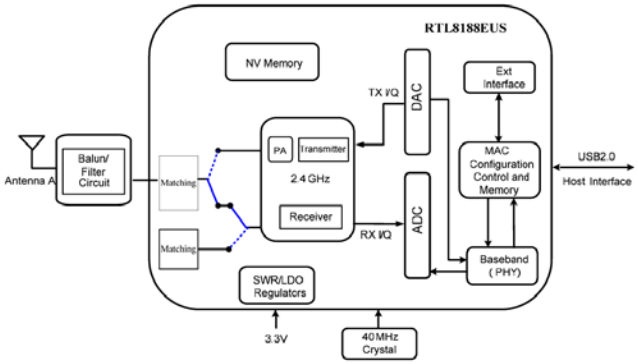


Рисунок 6 – Структура микросхемы RTL8188EUS

Для обеспечения совместимости проектируемого датчика со стандартами семейства IEEE 802.11 в части определенных радиочастотных диапазонов и типов модуляции радиосигнала принято решение в качестве приемо-передатчика применять Wi-Fi адаптеры, представленные платой со встроенной интегральной микросхемой, поддерживающей необходимые стандарты семейства IEEE 802.11.

D. Управление работой Wi-Fi адаптера при сканировании, организация приема и анализа пакетов

Схема, описывающая основные этапы проведения сканирования радиочастотных диапазонов Wi-Fi посредством внешних датчиков, сформированная на основе систематизации информации из разделов *A*, *B*, *C* настоящей главы, а также источников [10, 11], представлена на рисунке 7.

Рисунок 7 – Основные этапы проведения сканирования радиочастотных диапазонов Wi-Fi

Для управления сканированием применяется средство вычислительной техники, формирующее управляющие команды Wi-Fi адаптеру и производящее последующий анализ принятых пакетов. Результативно для данной задачи использовать компьютер, в том числе одноплатный, работающий под управлением операционной системы Linux. Указанная операционная система на уровне модулей ядра и драйверов поддерживает работу с Wi-Fi адаптерами различных производителей, позволяет производить прием и передачу пакетов в соответствии со стандартами семейства IEEE 802.11. Также в Linux может быть запущено пользовательское приложение, позволяющее посредством выполнения программного кода автоматизировать процесс.

Схема, описывающая путь пакета в операционной системе Linux от момента его приема Wi-Fi адаптером до момента передачи в пользовательское приложение [12], представлена на рисунке 8.

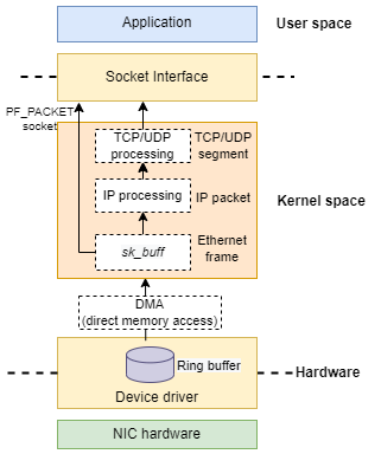


Рисунок 8 – Последовательность обработки пакетов Wi-Fi в операционной системе Linux

Инициирование сканирования и приема пакетов осуществляется переводом Wi-Fi адаптера в режим мониторинга, для чего исполняется команда *iw interface_name set monitor flags*. Командой *iw dev interface_name set channel* задаются параметры радиочастотных диапазонов, на которых производится прием пакетов.

Получение пользовательским приложением экземпляров пакетов, принятых Wi-Fi адаптером, производится через интерфейс сокетов. Для фильтрации пакетов, поступающих от конкретного Wi-Fi адаптера, в процессе привязки сокета командой *bind* может быть задан параметр *SO_BINDTODEVICE* [12]. Через сокет принятый пакет становится доступен пользовательскому приложению в виде набора байт, пользовательское приложение осуществляет их десоциализацию и переносит в структуры данных, что позволяет обращаться к полям пакетов для последующего анализа. Так как пакеты считываются через сокет по мере поступления, должна быть организована очередь пакетов и применен механизм, обеспечивающий многопоточную обработку пакетов из очереди.

Существуют библиотеки, такие как libpcap, Scapy, dpkt, позволяющие упростить процесс взаимодействия с системными вызовами Linux, производить десериализацию байтов в объектовое представление, что может сконцентрировать разработку пользовательского приложения на управлении сканированием радиочастотных диапазонов Wi-Fi и проведении анализа пакетов.

III. Проектирование экспериментального образца программно-аппаратного средства мониторинга безопасности Wi-Fi сетей

A. Функциональные требования

Основными требованиями, предъявляемыми к датчику, являются:

– возможность осуществлять захват пакетов, передаваемых согласно стандартам семейства IEEE 802.11;

– возможность осуществлять обработку собранных пакетов и их анализ на предмет наличия признаков осуществления атаки;

– возможность сканирования радиочастотных диапазонов несколькими Wi-Fi адаптерами единовременно;

– возможность эффективно осуществлять взаимодействие с серверной частью по Wi-Fi либо Ethernet, в том числе, для передачи сообщений об обнаруженных атаках и передачи собранной телеметрии;

– возможность стационарного, переносного и перевозного применения;

– возможность питания от сети и от портативных аккумуляторов;

– возможность осуществлять обнаружение местоположения источника атаки;

– поддержка распространенных стандартизированных протоколов и интерфейсов для последующей масштабируемости.

B. Аппаратная часть датчика

Ввиду поддержки распространенных протоколов и интерфейсов, небольших массогабаритных размеров и сравнительно высокой вычислительной мощности было принято решение о применении одноплатного компьютера в качестве средства вычислительной техники, осуществляющего сканирование радиоэфира, захват и анализ Wi-Fi пакетов.

Для взаимодействия с радиоэфиром применяется

набор Wi-Fi адаптеров, подключенных по шине USB к одноплатному компьютеру. Ввиду широкой поддержки одноплатными компьютерами от 2 до 5 USB-контролеров целесообразно использовать данный интерфейс, другие шины подключения (например, PCI) получили меньшую поддержку среди одноплатных компьютеров. Wi-Fi адаптеры единовременно проводят сканирование заданных радиоканалов, таким образом достигается увеличение доли принимаемых пакетов. При увеличении доли принятых из эфира пакетов от общего их числа снижается вероятность пропустить отправленные злоумышленником пакеты, содержащие признаки проведения атаки.

С учетом вышеизложенного аппаратная часть датчика может быть представлена следующей структурной схемой (рисунок 9).

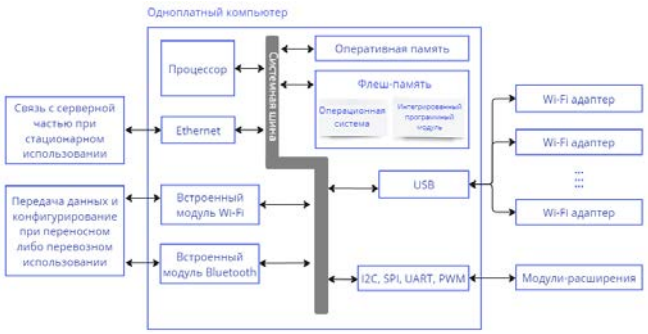


Рисунок 9 – Структурная схема аппаратной части датчика

Был осуществлен анализ доступных на рынке одноплатных компьютеров и Wi-Fi адаптеров, на основе которых возможно реализовать датчик. Подходящие одноплатные компьютеры, обладающие достаточной вычислительной мощностью и необходимыми интерфейсами, а также Wi-Fi адаптеры, совместимые с распространенными стандартами семейства IEEE 802.11, представлены в таблице 3.

Таблица 3 – Состав возможной компонентной базы датчика

Одноплатные компьютеры	Orange Pi 5 Pro / Plus Orange Pi Zero 2 / 3 Raspberry Pi 4 / 5 ASUS Tinker Board S NVIDIA Jetson Nano Radxa Rock 5 Model B + Plus Le Potato Renegade Elite Banana Pi BPI-M64 ODROID M1S FriendlyElec NanoPi M4V2 Pine64 Quartz64 Model B
Wi-Fi адаптеры	Fenvi AX5400 Alfa AWUS036ACHM Alfa AWUS036ACH Blueway N9000 TP-Link TL-WN722N ALFA AWUS036AXM ALFA AWUS036AXML CHANEVE CHW50L

Был собран экспериментальный образец датчика на основе одноплатного компьютера Orange Pi Zero 2 и Wi-Fi адаптеров Blueway N9000, Alfa AWUS036ACHM. На рисунке 10 представлена схема подключения экспериментального образца датчика, на рисунке 11 – экспериментальный образец датчика в собранном виде. Характеристики технических средств в составе датчика представлены в таблицах 4 и 5.

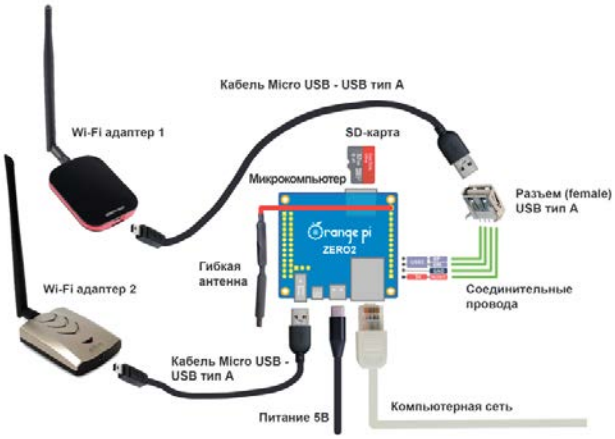


Рисунок 10 – Схема подключения экспериментального образца датчика

Рисунок 11 – Экспериментальный образец датчика в собранном виде

Таблица 4 – Характеристики Orange Pi Zero 2

Процессор	Allwinner H616
Разрядность процессора	64
Количество ядер	4
Количество потоков	4
Тактовая частота	1,5 ГГц
Объем оперативная память	2x500 МБ
Частота оперативной памяти	720 МГц
Сеть	10/100/1000 Мбит Gigabit Ethernet
USB	1x USB 2.0 (type-A), 1x USB2.0 OTG (type-C) 2x USB 2.0 (доступны через выводы на плате)

Таблица 5 – Характеристики Wi-Fi адаптеров

	Blueway N9000	Alfa AWUS036ACHM
Частотный диапазон	2,4 ГГц	2,4 ГГц, 5 ГГц
Поддерживаемые стандарты	IEEE 802.11: n, g, b	IEEE 802.11: n, g , b, a, ac
Чипсет	Ralink RT3070L	MediaTek MT7610U
Поддержка режима мониторинга	Да	Да
Поддержка беспроводных инъекций	Да	Да
Скорость передачи данных	802.11n: до 150 Мбит/с 802.11g: до 54 Мбит/с 802.11b: до 11 Мбит/с	802.11n: до 150 Мбит/с 802.11g: до 54 Мбит/с 802.11b: до 11 Мбит/с 802.11a : до 54 Мбит/с

		802.11ac: до 433 Мбит/с
Чувствительность приемника	до -90 дБм	до -90 дБм
Усиление антенны	5 дБ	5 дБ

C. Программная часть датчика

Операционная система Linux обеспечивает среду для взаимодействия одноплатного компьютера с Wi-Fi адаптерами. Для управления процессом сканирования эфира, обработки пакетов и обнаружения атак автором в ходе выполнения гранта [13] была разработана многопоточная программа [14] на языке программирования Python с использованием библиотеки Scapy. Указанная программа была обновлена для поддержки сканирования с использованием нескольких адаптеров. Программа была интегрирована в качестве программного модуля в операционную систему одноплатного компьютера. Образ программной части записан на SD-карту, через которую осуществляется загрузка одноплатного компьютера. На рисунке 12 представлена структура программной части датчика.

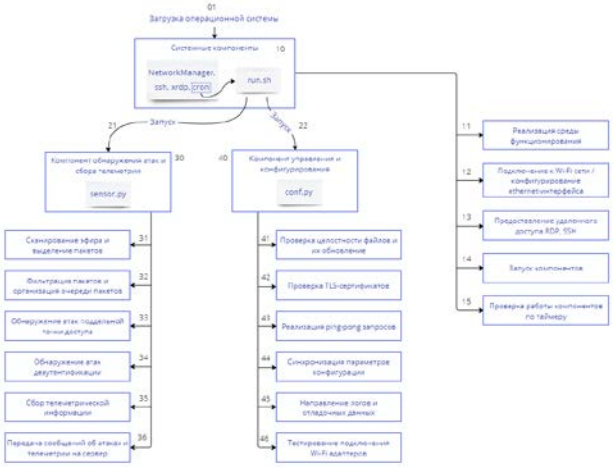


Рисунок 12 – Структурная схема программной части датчика

Описание функционала представлено с учетом обозначений на рисунке 12:

01 – передача управления программным компонентам датчика начинается после загрузки операционной системы.

10 – после загрузки операционной системы запускаются службы NetworkManager, xrdp и ssh, планировщик cron осуществляет запуск интерпретируемого bash-сценария run.sh.

11 – модули ядра, установленные пакеты операционной системы, интерпретаторы python и bash, а также дополнительные библиотеки, такие как Scapy, Requests, Threading, обеспечивают работу программного модуля датчика в целом.

12 – посредством NetworkManager осуществляется конфигурирование сетевого интерфейса ethernet либо подключение к Wi-Fi сети для последующего сетевого взаимодействия с серверной частью.

13 – посредством xrdp и ssh обеспечивается возможность подключения по протоколам RDP и SSH к датчику. Используются аутентификационные данные по умолчанию, после первого подключения к датчику предъявляется требование об изменении пароля.

14 – посредством run.sh осуществляется запуск python-сценариев sensor.py и agent.py.

15 – посредством run.sh осуществляется периодическая проверка работы сценариев sensor.py и agent.py, в случае обнаружения сбоев осуществляется их перезапуск.

21 – посредством run.sh осуществляется запуск python-сценария sensor.py.

22 – посредством run.sh осуществляется запуск python-сценария agent.py.

30 – компонент обнаружения атак и сбора телеметрии представлен исполняемым сценарием sensor.py, запускаемым через интерпретатор python.

31 – сканирование осуществляется посредством Wi-Fi адаптеров, подключенных к одноплатному компьютеру, процесс сканирования управляется python-сценарием sensor.py с использованием команды iw (для перевода адаптеров в режим мониторинга пакетов и переключения каналов) и команды sniff библиотеки Scapy с передачей в качестве параметра iface массива сетевых интерфейсов (для захвата пакетов). Перечень сканируемых радиоканалов и параметры сканирования для каждого Wi-Fi адаптера заданы в файле conf.json.

32 – очередь пакетов реализована библиотекой Queue и управляется операциями put, get, максимальный размер очереди – 10000 пакетов; фильтрация пакетов организована исключением из общего множества захваченных пакетов тех, которые не содержат заданные слои (например, представленные классами Dot11Deauth, Dot11Disas, Dot11Beacon, Dot11ProbeResp, Dot11ProbeReq); обработчики, которые анализируют извлеченные из очереди пакеты в порядке FIFO, запускаются в многопоточном режиме на основе библиотеки Thread.

33 – обнаружение атак поддельной точки доступа реализовано согласно [15].

34 – обнаружение атак деаутентификации реализовано посредством подсчета количества соответствующих пакетов в заданный период времени, при превышении заданного порогового значения детектируется атака.

35 – телеметрия собирается на основе пакетов-маяков (beacon frames) и зондирующих запросов/ответов (probe request/response), из пакетов извлекаются данные о Wi-Fi сетях и ассоциированных абонентах, соответствующие данные в совокупности с информацией о координатах места расположения датчика передаются на сервер.

36 – сообщения об обнаруженных атаках и данные телеметрии передаются на сервер по протоколу TLS (в рамках HTTPS-запросов, осуществляемых методом POST с использованием REST API). В случае, если датчик и сервер используют самоподписанные сертификаты, осуществляется верификация по корневому сертификату TLS (файл rootCA.crt, записанный на файловую систему датчика), путь до сертификата задается в переменной окружения os.environ['REQUESTS_CA_BUNDLE'].

40 – компонент управления и конфигурирования представлен исполняемым сценарием agent.py, запускаемым через интерпретатор python.

41 – обеспечивается контроль наличия файлов sensor.py и conf.json, а также загрузка обновлений программных компонентов с сервера.

42 – посредством библиотеки Requests осуществляется проверка действительности сертификата rootCA.crt и его применимости для взаимодействия с серверной частью.

43 – посредством библиотеки Requests датчик реализует ping-запросы в адрес сервера, сервер на основе соответствующих запросов осуществляет индикацию работающих на текущий момент времени датчиков в системе. Сервер дополнительно может оповестить датчик о наличии запланированной задачи, вернув в ответ на ping-запрос сообщение «cmd». Основными типами комманд, запрограммированными в датчике, являются: update (обновить прошивку), conf_update (обновить конфигурационный файл), send_logs (отправить логи), send_adapters (отправить информацию о подключенных Wi-Fi адаптерах), reboot (перезагрузка).

44 – посредством REST API (HTTPS-запрос, осуществляемый методом GET) от сервера запрашиваются актуальные данные конфигурации в формате JSON и вносятся в файл conf.json.

45 – посредством библиотеки Logging осуществляется сбор отладочных данных, сообщений об ошибках и аварийном завершении работ, данные записываются на файловую систему через класс RotatingFileHandler в папку logs (не более 200 файлов по 100000 байт каждый), данные впоследствии передаются на сервер при планировании соответствующей задачи.

46 – с использованием iwconfig и nmcli (флаги general,wifi-properties) осуществляется проверка подключения Wi-Fi адаптеров к датчику системы обнаружения атак на Wi-Fi сеть, сведения о Wi-Fi адаптерах передаются на сервер при планировании соответствующей задачи.

Методика анализа пакетов, используемая для обнаружения признаков проведения атаки, подробнее описана в [11].

IV. Апробация экспериментального образца датчика в автономном режиме

Была проведена апробация экспериментального образца датчика посредством тестового сканирования радиочастотных диапазонов Wi-Fi и приема пакетов.

Датчик был размещен в жилом помещении многоэтажного дома и переведен в режим захвата пакетов, передаваемых точками доступа Wi-Fi, которые находились на различных этажах многоэтажного дома, а также в соседних домах. Сведения о типах пакетов, передаваемых по радиоэфиру на момент проведения исследования, представлены на рисунке 13.

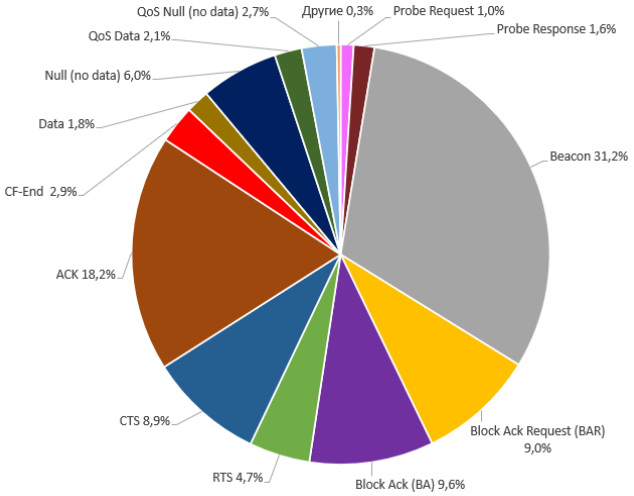


Рисунок 13 – Распределение принятых пакетов Wi-Fi по типам

Было проведено две серии наблюдений (для радиочастотного диапазона 2 ГГц, а также радиочастотных диапазонов 2 ГГц и 5 ГГц), в каждой серии осуществлялось по 20 измерений количества принятых пакетов. Ввиду помех в радиоэфире количество принятых пакетов отличалось между выборками. Измерения проводились при времени сканирования 130 секунд и интервале сканирования одного радиоканала в 1 секунду. При этом осуществлялось как сканирование посредством одного Wi-Fi адаптера, так и двух Wi-Fi адаптеров, работающих параллельно и захватывающих пакеты из различных сокетов. Датчик не осуществлял взаимодействие с серверной частью, все принятые пакеты сохранялись в оперативную память.

Результаты сканирования представлены в таблице 6. На основе проведенных тестов Шапиро-Уилка принято, что выборки соответствуют нормальному закону распределения. Пример гистограммы и квантиль-квантиль графика выборки с p-значением 0,40 при уровне значимости 5% представлен на рисунках 14 и 15.

Таблица 6 – Результаты сканирования радиочастотных диапазонов Wi-Fi экспериментальным образцом датчика

Радиочастотный диапазон	2 ГГц				2 + 5 ГГц		
Способ сканирования	Сканирование одним Wi-Fi адаптером		Сканирование двумя Wi-Fi адаптерами		Сканирование одним Wi-Fi адаптером	Сканирование двумя Wi-Fi адаптерами	
Адаптер	Blueway N9000	Alfa AWUS036ACHM	Blueway N9000	Alfa AWUS036ACHM	Alfa AWUS036ACHM	Blueway N9000	Alfa AWUS036ACHM

Сканируемые радиоканалы	1,2,3,4,5, 6,7,8,9,10 , 11,12,13	1,2,3,4,5, 6,7,8,9,10, 11,12,13	1,2,3,4,5,6	7,8,9,10, 11,12,13	1,2,3,4,5,6,7,8,9, 10,11,12,13, 36,40,44,48,52,56, 60,64,100,104,108, 112,116,120,124,128, 132,136,140,144,149, 153,157,161,165	1,2,3,4,5,6,7,8,9, 10,11,12,13	36,40,44,48,52,56, 60,64,100,104,108, 112,116,120,124,128, 132,136,140,144,149, 153,157,161,165
Общее время сканирования	130 с	130 с	130 с	130 с	130 с	130 с	130 с
Время сканирования одного радиоканала	1 с	1 с	1 с	1 с	1 с	1 с	1 с
Количество измерений	20	20	20	20	20	20	20
Среднее выборочное количество принятых пакетов	4585	4334	4542	5479	4426	6204	1507
Средне-квадратичное отклонение выборки	167	208	186	280	233	660	83
Коэффициент вариации	0,04	0,05	0,04	0,05	0,05	0,11	0,06

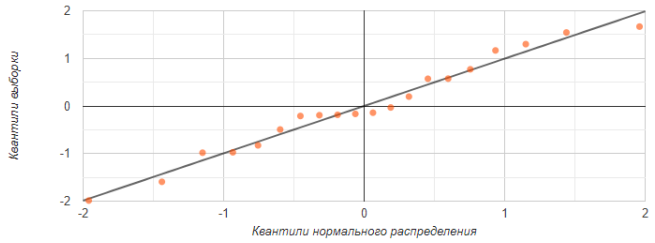


Рисунок 14 – Квантиль-квантиль график количества захваченных пакетов двумя Wi-Fi адаптерами в радиочастотных диапазонах 2,4 ГГц и 5 ГГц (промахи исключены в соответствии с правилом 3-х сигм)

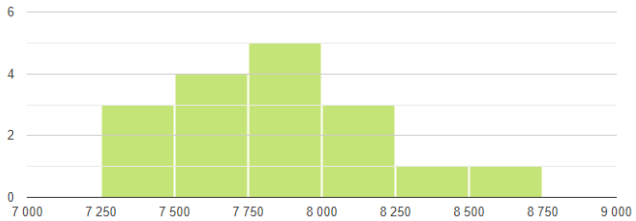


Рисунок 15 – Гистограмма количества захваченных пакетов двумя Wi-Fi адаптерами в радиочастотных диапазонах 2,4 ГГц и 5 ГГц (промахи исключены в соответствии с правилом 3-х сигм)

Графическая интерпретация результатов сканирования представлена на рисунках 16 и 17.

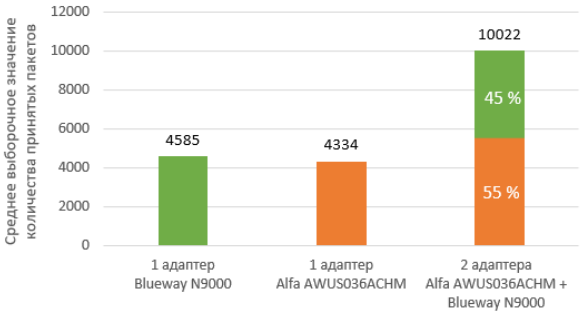


Рисунок 16 – Количество захваченных пакетов WI-Fi адаптерами в радиочастотном диапазоне 2,4 ГГц

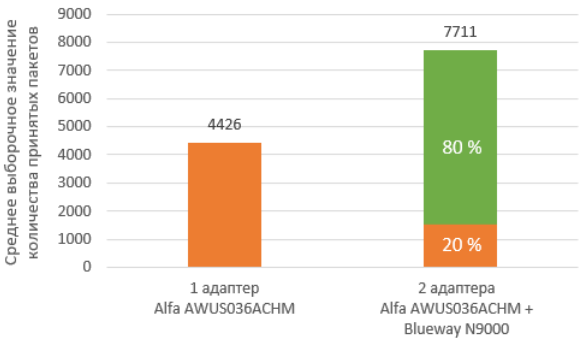


Рисунок 17 – Количество захваченных пакетов WI-Fi адаптерами в радиочастотных диапазонах 2,4 ГГц и 5 ГГц

Согласно рисункам можно сделать вывод, что увеличение количества Wi-Fi адаптеров, единовременно осуществляющих сканирование, ожидаемо приводит к увеличению доли захваченных пакетов, при этом зависимость в общем случае не является линейной. Ввиду отличий в количестве абонентских устройств и точек доступа на каждом радиоканале для повышения количества захваченных пакетов может потребоваться задание специализированных параметров сканирования. Планируется проведение дальнейшего исследования с использованием разработанного программно-аппаратного средства, дополняющего ранние работы авторского коллектива [10, 11, 16], для определения оптимальных параметров сканирования радиочастотных диапазонов Wi-Fi и максимизации количества захваченных пакетов.

Отметим, что увеличение количества Wi-Fi адаптеров также влечет увеличение потребляемого датчиком электрического тока и нагрузки на вычислительные ресурсы одноплатного компьютера, соответствующие данные представлены на рисунках 18, 19, 20.

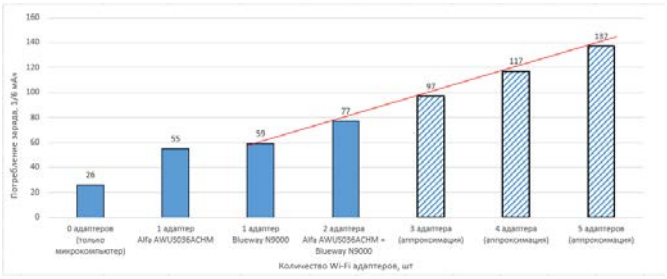


Рисунок 18 – Потребление заряда в течение 10 минут при питании датчика от портативного аккумулятора номинальным напряжением 5В

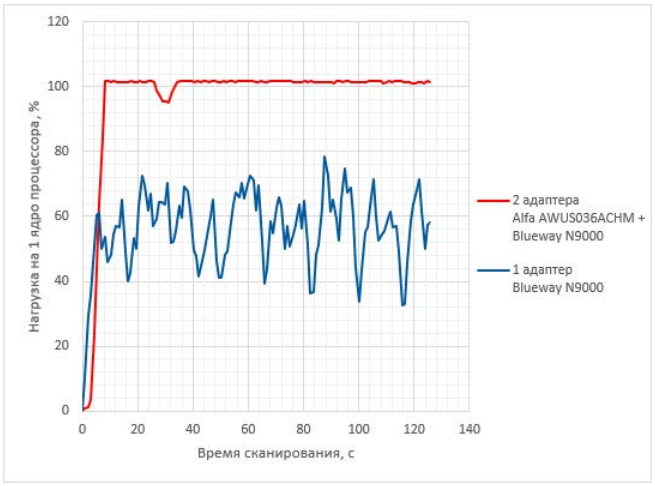


Рисунок 19 – Нагрузка на 1 ядро процессора при сканировании диапазона 2,4 ГГц. Примечание: значения свыше 100% вызваны многоядерной средой.

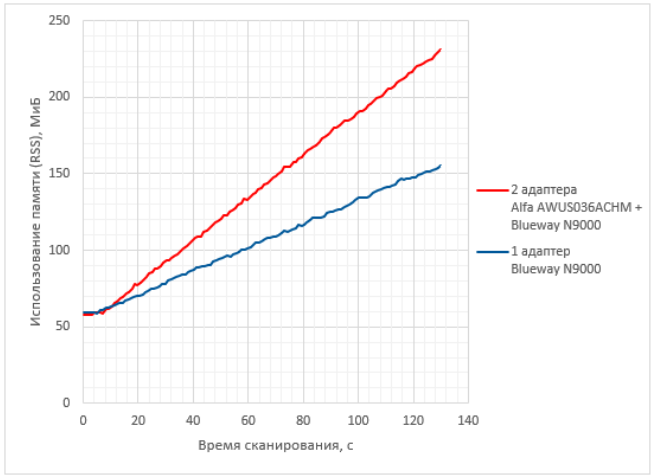


Рисунок 20 – Использование памяти при сканировании диапазона 2,4 ГГц (все захваченные пакеты были сохранены в памяти)

Возможны дальнейшие исследования в части оптимизации технических решений, дополняющие [17], для снижения загруженности системных ресурсов при приеме и последующей обработке пакетов.

V. Заключение

В статье описано программно-аппаратное средство, с использованием которого возможно осуществлять мониторинг безопасности Wi-Fi сетей: проводить сканирование радиочастотных диапазонов Wi-Fi, захват пакетов и их последующий анализ на предмет наличия признаков проведения атаки злоумышленником. Технические решения в основе разработки зарегистрированы в качестве объектов интеллектуальной собственности в Роспатенте [14, 15].

Существующие подходы, применяемые в средствах защиты Wi-Fi сетей, не предполагали произведение сканирования радиочастотных диапазонов Wi-Fi набором единовременно работающих Wi-Fi адаптеров, подключенных к датчикам, множество которых расположено в пределах контролируемого пространства и централизованно управляется. Что не позволяло увеличить долю принимаемых из радиоэфира и анализируемых пакетов, расширить покрытие пространства, в пределах которого обеспечивается обнаружение атак на Wi-Fi сеть. Одноплатный компьютер, к которому подключено несколько Wi-Fi адаптеров, при сканировании задействует больший объем вычислительных мощностей, что может потребовать его замену на более производительную и дорогостоящую модель, а также требует дополнительной проработки механизма обработки принятых пакетов, включая организацию очереди пакетов и их многопоточную обработку.

Представленные в настоящей статье результаты апробации экспериментального образца датчика свидетельствуют о его функциональности. Планируется продолжить исследование по обозначенным в статье направлениям, включая оптимизацию программно-аппаратной части разработки и определение оптимальных параметров сканирования радиочастотных диапазонов Wi-Fi. В качестве перспективного направления исследования выделено применение программно-аппаратного средства для расследования инцидентов информационной безопасности, включая обнаружение местоположения источника Wi-Fi сигнала.

Библиография

[1] Банк данных угроз безопасности информации // ФСТЭК России [Электронный ресурс]. – URL: https://bdu.fstec.ru/threat (дата обращения: 12.05.2024).

[2] Jivthesh M. R., Gaushik M. R., Adarsh P., Niranga G. H., Rao N. S. A Comprehensive survey of WiFi Analyzer Tools // 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2022, pp. 1-8, doi: 10.1109/GCAT55367.2022.9972040.

[3] Overlay vs. Integrated Wireless Security. The pros and cons of different approaches to wireless intrusion prevention. Airmagnet. Available at: https://airmagnet.netally.com/dynamic_threat_protection/assets/ AM_WP_Overlay_vs_Integrated_WIPS.pdf (accessed 12.05.2024).

[4] Перечень радиоканалов WLAN // Интернет-энциклопедия «Википедия» [Электронный ресурс]. – URL: https://en.wikipedia.org/ wiki/List_of_WLAN_ channels (дата обращения: 12.05.2024).

[5] Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. Tektronix. Available at: https://download.tek.com/document/37W-29447-2_LR.pdf (accessed 12.05.2024).

[6] WLAN (IEEE 802.11) capture setup. Wireshark. Available at: https://wiki.wireshark.org/CaptureSetup (accessed 12.05.2024).

[7] OFDM Wi-Fi Scanner Using SDR Preamble Detection. MathWorks MATLAB WLAN Toolbox. Available at: https://www.mathworks.com/help/wireless-testbench/ug/ofdm-wifi-scanner-using-sdr-scanner.html (accessed 12.05.2024).

[8] RSA306 USB Real Time Spectrum Analyzer Datasheet [SignalVu-PC application-specific licenses]. Tektronix. Available at: https://www.tek.com/en/datasheet/rsa306-usb-real-time-spectrum-analyzer-datasheet-0 (accessed 12.05.2024).

[9] Поиск интерференции с помощью портативного анализатора спектра R&S FSH // Rohde & Schwarz [Электронный ресурс]. – URL: https://rohdeschwarz.su/pics/Поиск интерференции с помощью портативного анализатора спектра FSH.pdf (дата обращения: 12.05.2024).

[10] D. S. Burenok. Experimental Study of Sequential and Random Channel Hopping for Detecting Wi-Fi Access Points // 2022 International Siberian Conference on Control and Communications (SIBCON), Tomsk, Russian Federation, 2022, pp. 1-8, doi: 10.1109/SIBCON56144.2022.10003009.

[11] Burenok D. S., Voevodin V. A., Cherniaev V. S. Technique for Detecting Computer Attacks on a Wi-Fi Networks // 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2022, pp. 487-492, doi: 10.1109/ElConRus54750.2022.9755703.

[12] Write a Linux packet sniffer from scratch: part one- PF_PACKET socket and promiscuous mode. Available at: https://organicprogrammer.com/2022/02/22/how-to-implement-libpcap-on-linux-with-raw-socket-part1/ (accessed 12.05.2024).

[13] Буренок Д. С. Система обнаружения атак на Wi-Fi сеть // Отчет о НИР в рамках Гранта Федерального государственного бюджетного учреждения «Фонд содействия развитию малых форм предприятий в научно-технической сфере». Всероссийский конкурса инновационных проектов «УМНИК». 2023 год.

[14] Буренок Д. С. Программный модуль датчика системы обнаружения атак на Wi-Fi сеть // Роспатент. Свидетельство о государственной регистрации программы для ЭВМ № 2024616189 от 18 марта 2024 г.

[15] Буренок Д. С. Способ обнаружения несанкционированных и поддельных точек доступа Wi-Fi // Роспатент. Патент на изобретение № 2810111 от 21.12.2023.

[16] Буренок Д. С., Воеводин В. А. Результат экспериментального исследования по обнаружению точек доступа Wi-Fi // The scientific heritage. 2021. № 73-1. С. 32 – 44. doi: 10.24412/9215-0365-2021-73-1-32-44.

[17] Буренок Д. С., Воеводин В. А. Об оценке своевременности обмена данными в централизованной системе мониторинга Wi-Fi сетей // German International Journal of Modern Science. 2021. № 17. С. 60 – 65. doi: 10.24412/2701-8369-2021-17-60-65.

The hardware & software sensor for wireless security monitoring based on a single-board computer and a set of Wi-Fi adapters

D.S. Burenok

***Abstract* — If Wi-Fi technology is used in an information system, according to Art. 16 of Russian Federal Law No. 149-FZ dated 27.07.2006, the owner of the information system must implement protection against wireless network threats. The owner also must ensure timely threat detection and logging. Common Wi-Fi security solutions have a few disadvantages. They may require replacing existing access points that enable the Wi-Fi network by single vendor models featuring an attack detection module. Other disadvantage may be the challenge of using autonomous sensors together to detect distributed attacks. To address these disadvantages, the author designed a hardware & software sensor. It supports pairwise network operation mode and centralized management. These features let it detect attacks across a geolocation without replacing Wi-Fi equipment. The sensor is modular. It scales by changing its hardware and software. This allows it to improve performance and add new features. The paper describes in detail the design of the hardware and software, which include a single-board computer, a set of network interfaces (represented by Wi-Fi adapters in monitor mode), as well as an integrated multithreaded control module in Python. The server side of the solution and the attack detection technique are described in general terms and are within the scope of other author's papers. The solution is novel. It uses a set of Wi-Fi adapters, allowing the sensor to work on several channels in different modes simultaneously. This ensures timely attack detection. It also uses a system approach to manage the scanning process, allowing for centralized management of such devices. This increases the coverage of attack detection. The designed elements had been patented in Rospatent (Federal Service for Intellectual Property).**

***Keywords*— Wi-Fi, detecting attacks on Wi-Fi networks, channel hopping, hardware & software sensor, Wi-Fi adapters, monitoring mode.**

REFERENCES

[1] *Bank dannykh ugroz bezopasnosti informatsii* (Information Security Threats Database). FSTEC of Russia. Available at: https://bdu.fstec.ru/threat (accessed 12.05.2024).

[2] Jivthesh M. R., Gaushik M. R., Adarsh P., Niranga G. H., Rao N. S. A Comprehensive survey of WiFi Analyzer Tools // 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT), Bangalore, India, 2022, pp. 1-8, doi: 10.1109/GCAT55367.2022. 9972040.

[3] Overlay vs. Integrated Wireless Security. The pros and cons of different approaches to wireless intrusion prevention. Airmagnet. Available at: https://airmagnet.netally.com/dynamic_threat_ protection/assets/ AM_WP_Overlay_vs_Integrated_WIPS.pdf (accessed 12.05.2024).

[4] List of WLAN channels. Internet encyclopedia "Wikipedia". Available at: https://en.wikipedia.org/ wiki/List_of_WLAN_ channels (accessed 12.05.2024).

[5] Wi-Fi: Overview of the 802.11 Physical Layer and Transmitter Measurements. Tektronix. Available at: https://download.tek.com/document/37W-29447-2_LR.pdf (accessed 12.05.2024).

[6] WLAN (IEEE 802.11) capture setup. Wireshark. Available at: https://wiki.wireshark.org/CaptureSetup (accessed 12.05.2024).

[7] OFDM Wi-Fi Scanner Using SDR Preamble Detection. MathWorks MATLAB WLAN Toolbox. Available at: https://www.mathworks.com/help/wireless-testbench/ug/ofdm-wifi-scanner-using-sdr-scanner.html (accessed 12.05.2024).

[8] RSA306 USB Real Time Spectrum Analyzer Datasheet [SignalVu-PC application-specific licenses]. Tektronix. Available at: https://www.tek.com/en/datasheet/rsa306-usb-real-time-spectrum-analyzer-datasheet-0 (accessed 12.05.2024).

[9] *Poisk interferentsii s pomoshchiu portativnogo analizatora spektra R&S®FSH* (Interference Hunting with R&S®FSH). Rohde & Schwarz. Available at: https://rohdeschwarz.su/pics/Поиск интерференции с помощью портативного анализатора спектра FSH.pdf (accessed 12.05.2024).

[10] Burenok D. S. Experimental Study of Sequential and Random Channel Hopping for Detecting Wi-Fi Access Points // 2022 International Siberian Conference on Control and Communications (SIBCON), Tomsk, Russian Federation, 2022, pp. 1-8, doi: 10.1109/SIBCON56144.2022.10003009.

[11] Burenok D. S., Voevodin V. A., Cherniaev V. S. Technique for Detecting Computer Attacks on a Wi-Fi Networks // 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2022, pp. 487-492, doi: 10.1109/ElConRus54750.2022.9755703.

[12] Write a Linux packet sniffer from scratch: part one- PF_PACKET socket and promiscuous mode. Available at: https://organicprogrammer.com/2022/02/22/how-to-implement-libpcap-on-linux-with-raw-socket-part1/ (accessed 12.05.2024).

[13] Burenok D. S. System for detecting attacks on Wi-Fi network // Report on R&D under the Grant of the Federal State Budgetary Institution «Foundation for Assistance to Small Innovative Enterprises in Science and Technology». All-Russian competition of innovative projects «UMNIK». 2023.

[14] Burenok D.S. *Programmnyi modul' datchika sistemy obnaruzheniya atak na Wi-Fi set'* [Software module of the Wi-Fi network attack detection system's sensor]. RF certificate of state registration of a computer program, no. 2024616189, 2024.

[15] Burenok D.S. *Sposob obnaruzheniya nesanktsionirovannykh i poddel'nykh tochek dostupa Wi-Fi* [Detecting rogue and unauthorized Wi-Fi access points]. RF patent, no. 2810111, 2023.

[16] Burenok D.S. Voevodin V.A. Result of experimental study on detecting Wi-Fi access points. The scientific heritage, 2021, no. 73-1, pp. 32 – 44 (in Russian). DOI: 10.24412/9215-0365-2021-73-1-32-44

[17] Burenok D.S. Voevodin V.A. On assessing the timeliness of data exchange in a centralized monitoring system for wi-fi networks. German International Journal of Modern Science, 2021, no. 17, pp. 60 – 65 (in Russian). DOI: 10.24412/2701-8369-2021-17-60-65