УДК 004.056 Вестник УрФО № 3(49) / 2023, с. 81–89

**Швырев Б.А., Цимбал В.Н., Антонов А.С.**

DOI: 10.14529/secur230308

# *ТЕХНИЧЕСКИЙ КАНАЛ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ИМИТАЦИИ ЛЕГАЛЬНОГО КАНАЛА СТАНДАРТА IEEE 802.11*

*WiFi сети 2,4ГГц присутствуют повсеместно в том числе и в пространстве контролируемого помещения. Субъектами WiFi сети могут выступать различные сетевые устройства, узлы и точки доступа расположенные за пределами помещения. Элементы сети могут передавать данные в режиме «WiFi роутера» и «web-сервера». Для исследования возможности скрытной передачи данных и потокового аудио из контролируемого помещения используя WiFi сети 2,4ГГц в работе выполнены экспериментальные измерения. Для измерений разработана модель передатчика WiFi 2,4ГГц на основе микроконтроллера ESP. Проведенные исследования показали возможность передачи информации в узкой полосе частот одного канала WiFi 2,4ГГц. В работе показано, что присутствие на защищаемом объекте WiFi излучения является угрозой и для сокрытия передачи информации из контролируемого помещения на частотах легальных каналов WiFi сети злоумышленник может использовать как случайные WiFi сети излучение которых присутствует на объекте, так и специально развёрнутые на границе контролируемого объекта. Диапазон WiFi может быть использован не только для передачи несанкционированными передатчиками, но и для сокрытия передачи данных в режиме «web-сервера». Наибольшей опасностью обладает точка доступа в режиме web-сервера.*

***Ключевые слова:*** *технический канал утечки информации, микроконтроллер ESP, web-сервер, WiFi роутер, угроза утечки информации, IEEE 802.11.*

**Shvyrev B.A., Tsimbal V.N., Antonov A.S.**

# *TECHNICAL CHANNEL OF INFORMATION LEAKAGE DUE TO IMITATION OF THE LEGAL CHANNEL OF THE IEEE 802.11 STANDARD*

*2.4GHz WiFi networks are present everywhere, including in the space of the controlled room. The subjects of a WiFi network can be various network devices, nodes and access points located*

*outside the premises. Network elements can transmit data in the "WiFi router" and "web server" mode. Experimental measurements were performed to investigate the possibility of covert data transmission and audio streaming from a controlled room using a 2.4GHz WiFi network. A 2.4GHz WiFi transmitter model based on an ESP microcontroller has been developed for measurements. The conducted studies have shown the possibility of transmitting information in a narrow frequency band of one 2.4GHz WiFi channel. The paper shows that the presence of Wi-Fi radiation on the protected object is a threat and to conceal the transmission of information from a controlled room at the frequencies of legal WiFi network channels, an attacker can use both random WiFi networks whose radiation is present on the object and specially deployed at the border of the controlled object. The Wi-Fi range can be used not only for transmission by unauthorized transmitters, but also for hiding data transmission in the "web server" mode. The access point in the web server mode has the greatest danger.*

***Keywords:*** *technical information leakage channel, MSP microcontroller, web server, WiFi router, threat of information leakage, IEEE 802.11.*

Развитие беспроводных технологий пронизывает пространство обитания человека круглосуточно. Радиоволны практически всех диапазонов присутствуют как на рабочем месте, так и в местах отдыха. Все эти радиоизлучения законны – соответствуют нормам и ГОСТам и за ними пристально следят контролирующие органы [1]. Как известно каждый радиоканал характеризуется занимаемой полосой частот и защитным частотным интервалом от соседнего канала. В пределах полосы частот легального канала связи априори передается санкционированная информация между известными абонентами [2]. Такой канал радиосвязи так же характеризуется излучаемой в канал мощностью или радиоканал имеет энергетический спектр мощности. Все описанные параметры строго регулируются и для организации радиоканала используются либо открытые частоты, используемые обычными пользователя или радиолюбителями, и закрытые частоты, на которых осуществляется радиосвязь государственных органов, военных, а также работа различной телеметрической аппаратуры [3].

Наибольший интерес представляет открытые частотные диапазоны по причине своей доступности как в плане аппаратуры, так и отсутствие ответственности за его использование. В настоящее время наиболее распространенным радиодиапазоном является WiFi на частоте 2,4 ГГц. Этот диапазон разрешен для организации беспроводного радиоканала для передачи цифровых данных. Практически в любом месте крупного города присутствуют сигналы WiFi. В каждой квартир или офисе располагается WiFi роутер, на улице можно встретить роутеры WiMax, в транспорте или на тротуаре всегда обнаружится человек со смартфоном в режиме роутера WiFi, а если добавить скрытые сети WiFi обслуживающие городское или частное видеонаблюдение, различные датчики телеметрии включая относящиеся к ЖКХ то получается повсеместная достаточно плотная компоновка передачи сингалов в интервале 2.4 ГГц. Отследить передачу данных в легальных каналах WiFi диапазона достаточно сложно. Каждый канал WiFi 2,4 Гц имеет ширину 20 МГц и на половину перекрывается со следующим каналом, исключая крайние каналы все внутренние 9 каналов перекрываются с соседними каналами (Рис.1.) [4].

Такая картина обусловлена используемым стандартом WiFi и обеспечивает плотную компоновку радиоканалов без потери качества передачи данных. Выделение своего канала WiFi осуществляется по процедурам стандарта связи IEEE 802.11 и не вызывает вопросов у легальных пользователей. Плотная

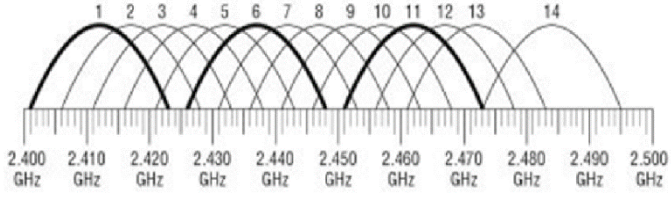


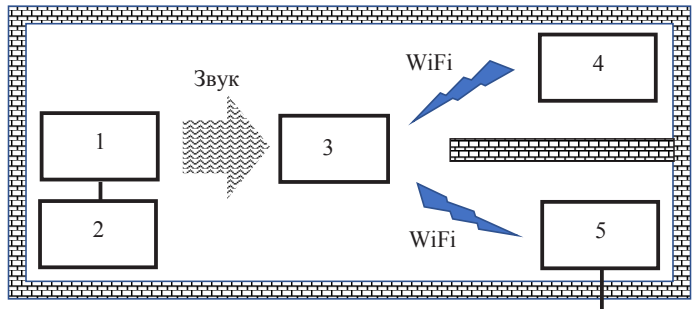

Рис. 1. Частотные каналы Wi-Fi в диапазоне 2.4 ГГц

компоновка сигналов в диапазоне WiFi 2,4ГГц создает возможность скрытной передачи информации, что потенциально может быть использовано для организации технического канала утечки информации (ТКУИ) [5]. В рассматриваемом диапазоне WiFi 2,4 ГГц может располагаться передатчик акустический разведки (АР) как стандарта IEEE 802.11, так и любой радиопередатчик с несущей частотой принадлежащей диапазону WiFi 2,4 ГГц.

В открытой литературе отсутствует исследование формирование ТКУИ на защищаемом объекте за счет использование легального канала стандарта IEEE 802.11 [6]. Простота реализации передатчика в диапазоне частот WiFi 2,4 ГГц и высокая плотность радиоизлучения WiFi 2,4 ГГц в пределах защищаемого объекта обуславливает актуальность исследования канала утечки акустической информации по средствам имитации легального канала WiFi 2,4 ГГц.

Для исследования ТКУИ за счет радиоканала стандарта IEEE 802.11 выполнены экспериментальные исследования возможности скрытной передачи телеметрической и акустической информации из контролируемого помещения. Экспериментальные исследования проводились на альтернативной измерительной площадке «Безэховая экранированная камера» (БЭК) для обеспечения радиотишины и исключения внешних наводок и помех. Для измерения использовался анализатор спектра «Rohde&Schwarz FSH13» и широкополосная измерительная рупорная антенна П6-223 обеспечивающая прием в диапазоне 800 МГц – 18 ГГц. Схема эксперимента приведена на рис.2.

В качестве модели источника Wi-Fi 2,4 ГГц




1 – Экранированная акустическая колонка,
2 – генератор сигналов звуковой частоты,
3 – МП (МП 1 или МП 2), 4 – WiFi роутер,
5 – антенна П6-223, 6 – анализатор спектра FSH13.

Рис. 2. Схема экспериментальных измерений

радиосигнала использовалось специально разработанное устройство - модель передатчика (МП). Для реализации МП использовалось две модели собранных на микроконтроллере ESP в двух режимах передачи в диапазоне Wi-Fi 2,4 ГГц – в режиме роутера и режиме Web – сервера. Одна модель МП1 на контроллере ESP8266 для передачи телеметрической информации, в качестве которой использовался уровень запечатлённой громкости на контролируемой территории и вторая модель МП2 на ESP32 для передачи акустической речевой информации из контролируемой территории (WiFi микрофон) [7].

Режим web-сервера МП состоит в приёме WiFi сети от иного источника (Wi-Fi роутера или мобильного телефона) [8]. После того как МП1 получает питание от аккумулятора, модуль подключается к существующей на контролируемой территории WiFi сети, создаётся Web-сервер, на который в виде html-страницы выводятся значения громкости, запечатлённые микрофоном (Рис.3). Для просмотра уровня громкости, необходимо обратиться к IP-адрес web-сервера, при этом устройству-клиенту разведчика необходимо находится в той же сети, к которой подключен МП1.

Режим WiFi точки или роутера МП1 работает как точка доступа WiFi по аналогии с роутером или режимом модема на мобильном телефоне (рис.4) [9]. Для реализации режима необходимо задать параметры SSID и пароль сети в контроллер МП. Рассматриваемый режим позволяет создать локальную сеть по стандарту IEEE 802.11 без выхода в глобальный интернет.

МП 2 по аналогии с МП1 состоит из двух модулей: микроконтроллера ESP 32 и всенаправленного микрофона I2S INMP441. МП2

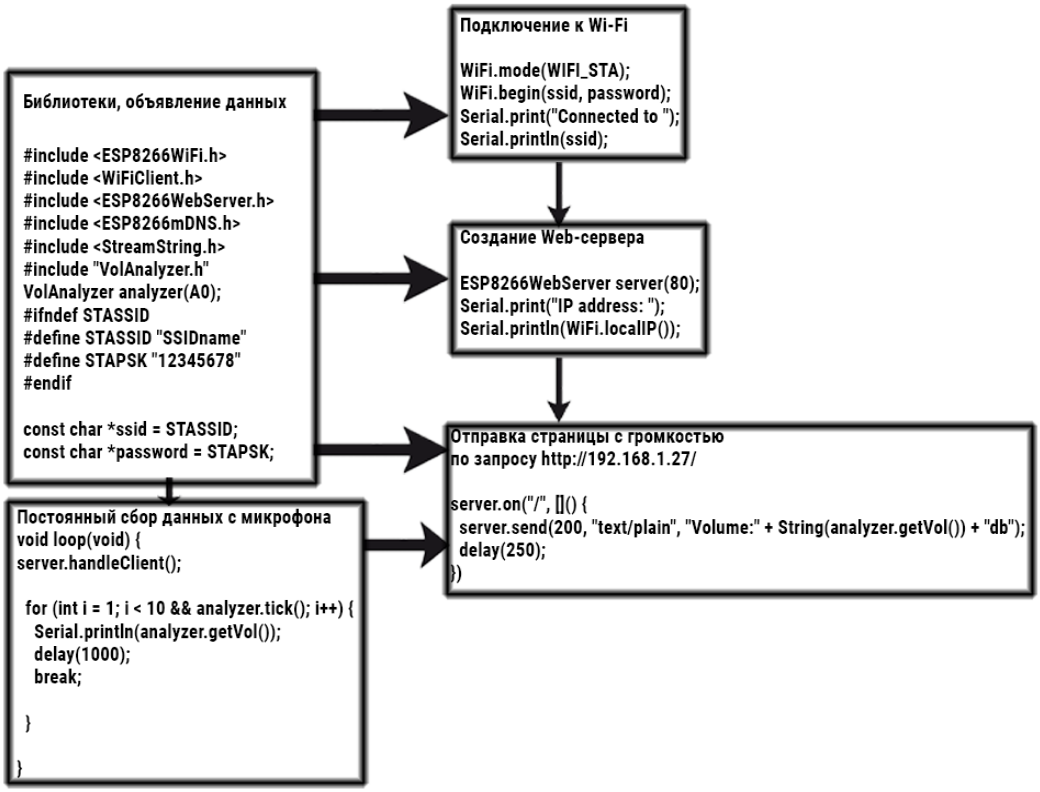



Рис. 3. Схема работы МП1 в режиме веб-сервера

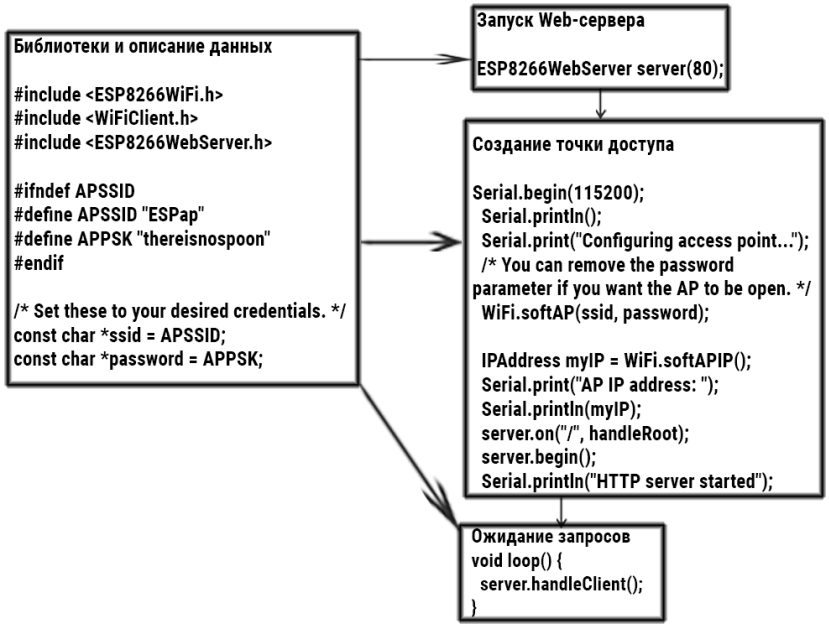



Рис. 4. Схема работы в режиме WiFi точки доступа

начинает свою работу с подключения к уже существующей сети WiFi в диапазоне 2.4 ГГц SSID и пароль введен в контроллера ESP 32 (рис.5) [7].

После соединения с сетью устройство получает IP адрес, на котором создаётся веб-сервер. Микрофон переходит в режим ожидания клиента, и не передаёт информацию, пока у веб-сервера нет клиента. Чтобы обратиться к веб-серверу Wi-Fi микрофона необходимо подсоединить устройство-клиент в ту же сеть, далее воспользоваться веб-


Рис. 5. Схема сеанса связи между клиентом и сервером

браузером или плеером с возможностью открывать URL.

Для расчёта объёма переданных данных в единицу времени воспользуемся выражением:

$$V = b f t C,$$

где V – объём данных, b – глубина кодирования (количество бит на дискретизацию), t – единица времени, C – количество каналов, $f$ – частота дискретизации.

Наиболее оптимальные параметры для ESP32 следующие: b – 16 бит, t – 1 с, C – 2, $f$ – 22050 Гц, тогда V = 16*1*2*22050 = 705600 бит. Следовательно, МП2 передает 88200 байта аудиоданных.

Прослушать аудио сигнал с МП2 можно вторым способом с помощью утилиты VLC. Для этого в ней необходимо обратиться к URL web-сервера. Плеер начнёт получать поток данных с микрофона, при этом показатели качества звука будут на слух гораздо лучше, чем в браузере.

Экспериментальные измерения проводились в два этапа:

Первый этап включал исследование спектральных характеристик электромагнитного излучения МП1 при передаче уровня громкости (телеметрические данные) в режиме «WiFi роутера» и «web-сервера».

Второй этап включал исследование спектральных характеристик электромагнитного излучения МП2 при передаче акустического речевого сигнала (поток данных) в режиме «WiFi роутера» и «web-сервера».

Измерения спектрального состава электромагнитного излучения МП1 и МП2 в режиме «WiFi роутера» имеет одинаковый спектр и приведено на рис.6. Представленная спектрограмма является нормальным излучением практически со сплошным спектром в диапазоне 2,401-2,423 ГГц, что соответствует первому каналу сети WiFi 2,4 ГГц. Таким образом передача телеметрических данных и потоковых аудио данных имеет одинаковый спектр излучения и по спектральному составу подобны [10]. Такая трансляция легко обнаруживается не только специализированными комплексами или анализатором спектра, но и общедоступными инструментами, к которым можно отнести свободное программное обеспечение по анализу WiFi сетей. Для устройств на базе операционной системы (ОС) Андроид, приложение «Wi-Fi Analyzer», позволяет демонстрировать находящиеся рядом точки WiFi, частоты их работы, наименование SSID, каналы на которых ведется радиосвязь, используемые алгоритмы защиты (тип безопасности), уровень мощности сигнала и примерное расстояние до них [11]. Для устройств на базе ОС Apple iOS, приложений, обладающих подобным функционалом, практически нет [12], более эффективным для обнаружения, анализа наличия беспроводных сетей стандарта связи IEEE 802.11 и определения иных характеристик являются устройства на ОС Андроид. Для устройств на базе ОС Windows аналогичным выше является ПО «WiFi Analyzer», которое также позволяет демонстрировать находящиеся рядом точки WiFi, частоты их работы, наименование SSID и BSSID, каналы на которых ведется радиовещание, используемые алгоритмы защиты (тип безопасности) и уровень мощности сигнала, однако не показывает расстояние до них [13].

Работа МП1 и МП2 в режиме «WiFi роутера» полностью использует спектр одного канала WiFi сети на частоте 2.4ГГц.

Рассмотрим передачу данных МП1 в режиме «web-сервер» при передачи телеметрических данных. Измеренная спектрограмма приведена на рис. 7.

Из рис.7 видно, что диапазон частот одного канала WiFi имеет линейчатый спектр, состоящий в нашем эксперименте из нескольких узких полос с интенсивность порядка 37 дБмкВ. Увеличение объема передаваемых телеметрических данных не привело с существенному изменению спектра излучения сигнала WiFi.

На рис.8 представлен спектр излучения МП2 в режиме «web-сервер» при передачи потокового аудио 16 бит с частотой дискретизации 22050 Гц. На рисунке графики желтого и белого цветов соответствуют передачи данных в разные моменты времени. Передаваема полоса частот составляет порядка 1,4 МГц и произвольно появляется в одном из 10 субканалов первого канала WiFi 2,4 ГГц с интервалом в 5с.

Спектр радиосигнала (рис.8) передачи звука из контролируемого помещения занимает узкую полосу частот в интервале первого канала WiFi, что позволяет передаче скрываться за излучениями других сетей в аналогичном интервале частот.

**Выводы.**

Стоит отметить, что программы обнаружения WiFi сетей не отображают точки в режиме «web-сервер» как при передаче телеметрии, так и при передачи потокового аудио сигнала, то есть оперативно подобным спосо-

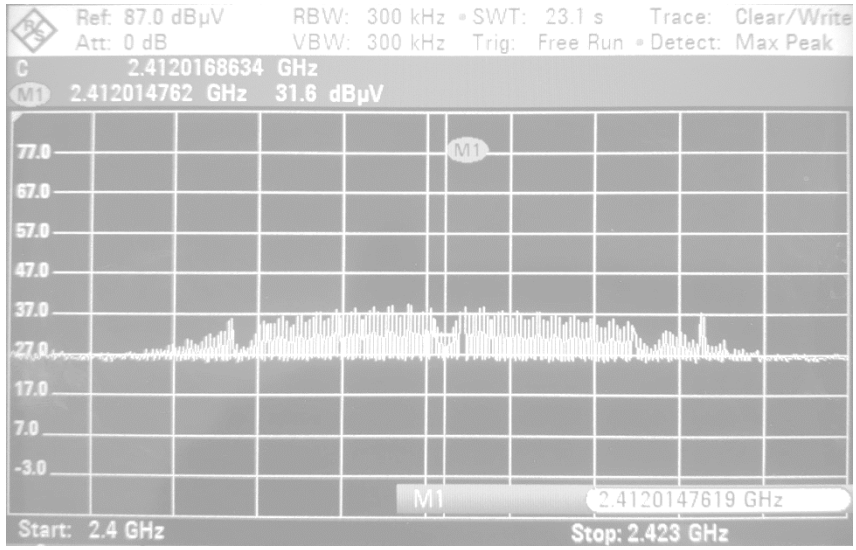



Рис.6. Спектр сигнала Wi-Fi, излучаемого МП1 (МП2) в режиме «WiFi роутера»

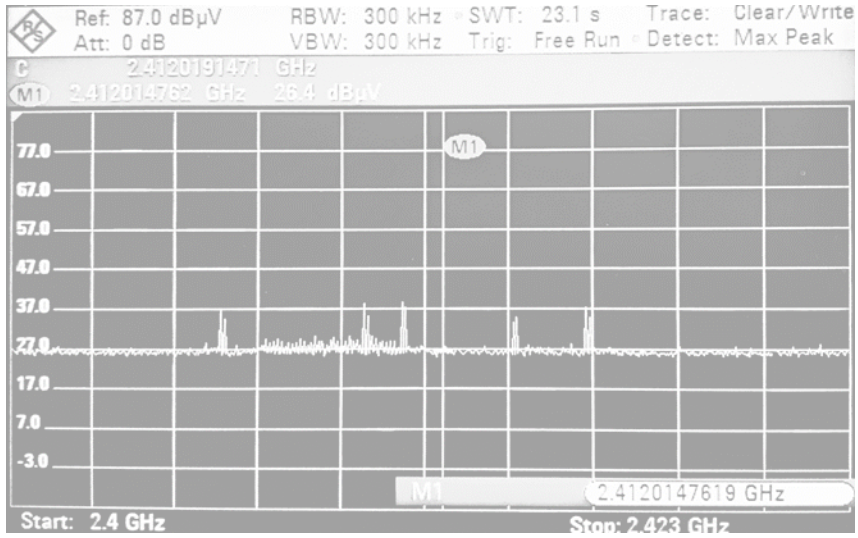



Рис.7. Спектр сигнала WiFi, излучаемого МП1 в режиме «web-сервер»

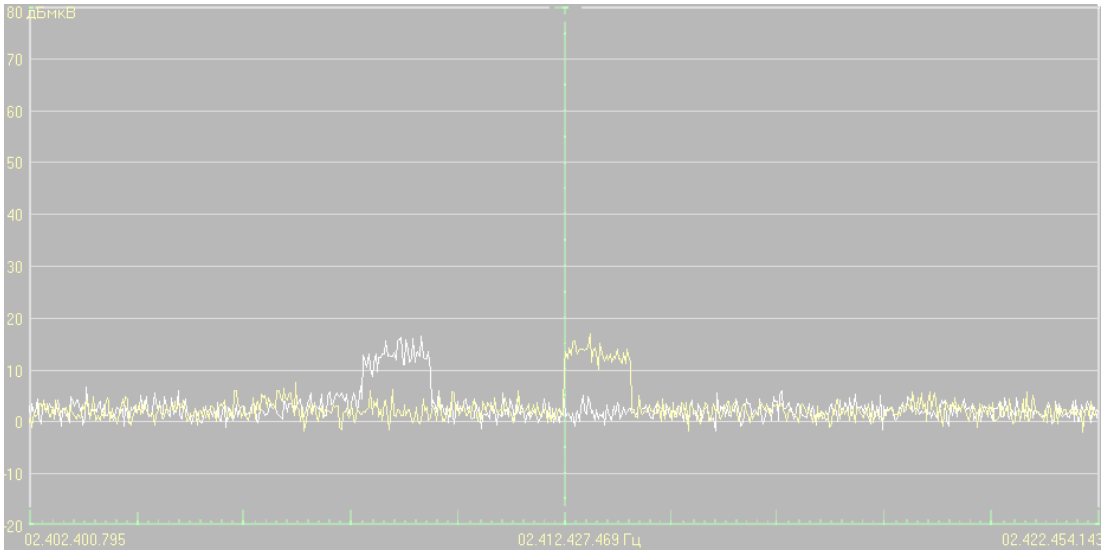



Рис.8. Спектр сигнала WiFi, излучаемого МП2 в режиме «web-сервер»

бом установить наличие МП на объекте или рядом с ним невозможно. Обнаружить передачу становиться возможным только с использование специального измерительного оборудования.

Для сокрытия передачи информации из контролируемого помещения на частотах легальных каналов WiFi сети злоумышленник может использовать как случайные WiFi сети излучение которых присутствует на объекте, так и специально развёрнутые на границе контролируемого объекта. Следовательно, присутствие на защищаемом объекте WiFi излучения является угрозой. Диапазон WiFi может использоваться не только для передачи несанкционированными ТСПИ, но и для сокрытия передачи данных в режиме «web-сервера». Этот режим позволяет, используя легальные радиоэлектронные средства и частоты скрытно передавать потоковый звуковой сигнал и телеметрические данные. Передача телеметрии может использоваться для передачи перехваченной цифровой информации обрабатываемой вычислительной техникой, не имеющей непосредственного подключения к компьютерным сетям, такие вычислительные системы в литературе называют с «воздушным зазором».

**Литература**

1. Бабурин А. В. Физические основы защиты информации: учеб. пособие / А. В. Бабурин, А. С. Пахомова. – Воронеж: ФГБОУ ВПО «Воронежский государственный технический университет», 2015.

2. Шатуновский В.Л. Проектирование устройств для дистанционного мониторинга и управления в системах локальной автоматизации на базе микроконтроллерных плат, типа «ARDUINO» и «ESP»: учеб. пособие / В.Л. Шатуновский, Электронное текстовое издание / Санкт-Петербург, 2021.

3. Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам: Справочное пособие / Бузов Г.А. - М.: Горячая линия-Телеком, 2015.

4. IEEE-SA, IEEE Standard for Ethernet, IEEE Standards Authority, 2012.

5. Зайцев, А. П. Технические средства и методы защиты информации. Учебник для вузов - 7-е изд., испр. / А.П. Зайцев, Р.В. Мещеряков, А.А. Шелупанов. - М.: Горячая Линия-Телеком, 2018.

6. Поршнев С.В. Скрытые технические каналы утечки информации, обрабатываемой в средствах вычислительной техники: анализ действующей нормативно-методической базы, терминология / С.В. Поршнев, Д.О. Беляев // Вестник УрФО. Безопасность в информационной сфере. 2021. № 1 (39). С. 5-13.

7. Diao W., Liu X., Zhou Z., Zhang K. Your voice assistant is mine: How to abuse speakers to steal information and control your phone; Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices; Scottsdale, AZ, USA. 3–7 November 2014; pp. 63–74.

8. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, T. Thomas, LTE-advanced: next-generation wireless broadband technology, IEEE Wirel. Commun. 17 (3) (2010) 10–22.

9. Heartfield R., Loukas G., Budimir S., Bezemskij A., Fontaine J.R., Filippoupolitis A., Roesch E. A taxonomy of cyber-physical threats and impact in the smart home. Comput. Secur. 2018; 78:398–428. doi: 10.1016/j.cose.2018.07.011.

10. G. Wilkinson, Digital Terrestrial Tracking: The Future of Surveillance, DEFCON 22.

11. M. Gruteser, D. Grunwald, Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis, Mob. Netw. Appl. 10 (3) (2005) 315–325.

12. Butun I., Pereira N., Gidlund M. Security Risk Analysis of LoRaWAN and Future Directions. Future Internet. 2019; 11:3. doi: 10.3390/fi11010003.

13. R. Flickenger, S. Okay, E. Pietrosemoli, M. Zennaro, C. Fonda, Very long distance Wi-Fi networks, in: Networked systems for developing regions-NSDR'08, ACM Press, New York, New York, USA, 2008, p. 6.

## References

1. Baburin A. V. Fizicheskie osnovy zashchity informatsii: ucheb. posobie / A. V. Baburin, A. S. Pakhomova. – Voronezh: FGBOU VPO «Voronezhskiy gosudarstvennyy tekhnicheskiy universitet», 2015.

2. Shatunovskiy V.L. Proektirovanie ustroystv dlya distantsionnogo monitoringa i upravleniya v sistemakh lokal'noy avtomatizatsii na baze mikrokontrollernykh plat, tipa "ARDUINO" i "ESP": ucheb. posobie / V.L. Shatunovskiy, Elektronnoe tekstovoe izdanie / Sankt-Peterburg, 2021.

3. Buzov, G. A. Zashchita informatsii ogranichennogo dostupa ot utechki po tekhnicheskim kanalam: Spravochnoe posobie / Buzov G.A. - M.: Goryachaya liniya-Telekom, 2015.

4. IEEE-SA, IEEE Standard for Ethernet, IEEE Standards Authority, 2012.

5. Zaytsev, A. P. Tekhnicheskie sredstva i metody zashchity informatsii. Uchebnik dlya vuzov - 7-e izd., ispr. / A.P. Zaytsev, R.V. Meshcheryakov, A.A. Shelupanov. - M.: Goryachaya Liniya-Telekom, 2018.

6. Porshnev S.V. Skrytye tekhnicheskie kanaly utechki informatsii, obrabatyvaemoy v sredstvakh vychislitel'noy tekhniki: analiz deystvuyushchey normativno-metodicheskoy bazy, terminologiya / S.V. Porshnev, D.O. Belyaev // Vestnik UrFO. Bezopasnost' v informatsionnoy sfere. 2021. № 1 (39). S. 5-13.

7. Diao W., Liu X., Zhou Z., Zhang K. Your voice assistant is mine: How to abuse speakers to steal information and control your phone; Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices; Scottsdale, AZ, USA. 3–7 November 2014; pp. 63–74.

8. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, T. Thomas, LTE-advanced: next-generation wireless broadband technology, IEEE Wirel. Commun. 17 (3) (2010) 10–22.

9. Heartfield R., Loukas G., Budimir S., Bezemskij A., Fontaine J.R., Filippoupolitis A., Roesch E. A taxonomy of cyber-physical threats and impact in the smart home. Comput. Secur. 2018; 78:398–428. doi: 10.1016/j.cose.2018.07.011.

10. G. Wilkinson, Digital Terrestrial Tracking: The Future of Surveillance, DEFCON 22.

11. M. Gruteser, D. Grunwald, Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis, Mob. Netw. Appl. 10 (3) (2005) 315–325.

12. Butun I., Pereira N., Gidlund M. Security Risk Analysis of LoRaWAN and Future Directions. Future Internet. 2019; 11:3. doi: 10.3390/fi11010003.

13. R. Flickenger, S. Okay, E. Pietrosemoli, M. Zennaro, C. Fonda, Very long distance Wi-Fi networks, in: Networked systems for developing regions-NSDR'08, ACM Press, New York, New York, USA, 2008, p. 6.

---

**ШВЫРЕВ Борис Анатольевич,** кандидат физико-математических наук, доцент, доцент кафедры специальных информационных технологий учебно-научного комплекса информационных технологий. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: bor2275@yandex.ru

**SHVYREV Boris Anatolyevich,** Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Special Information Technologies of the educational and scientific complex of information Technologies. Federal State Public Educational Establishment of Higher Education "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: bor2275@yandex.ru

**ЦИМБАЛ Виталий Николаевич,** кандидат юридических наук, заместитель начальника кафедры информационной безопасности учебно-научного комплекса информационных технологий, кандидат юридических наук. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: sedruk@mail.ru

**TSIMBAL Vitaly Nikolaevich,** Candidate of Legal Sciences, Deputy Head of the Department of Information Security of the educational and Scientific complex of Information Technologies, Candidate of Legal Sciences. Federal State Public Educational Establishment of Higher Edication "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: sedruk@mail.ru

**АНТОНОВ Анатолий Сергеевич,** курсант факультета подготовки специалистов в области информационной безопасности. Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В. Я. Кикотя». 117997, Москва, ул. Академика Волгина, д.12. E-mail: therafi@yandex.ru

**ANTONOV Anatoly Sergeevich,** cadet of the Faculty of training specialists in the field of information security. Federal State Public Educational Establishment of Higher Edication "Moscow University of the Ministry of Internal Affairs of the Russian Federation named after V.Y. Kikot". 117997, Moscow, Akademika Volgina str., 12. E-mail: therafi@yandex.ru