УДК 004.716
Doi: 10.31772/2712-8970-2022-23-4-657-670

Для цитирования: Басан Е. С., Прошкин Н. А., Силин О. И. Повышение защищенности беспроводных каналов связи для беспилотных летательных аппаратов за счет создания ложных информационных полей // Сибирский аэрокосмический журнал. 2022. Т. 23, № 4. С. 657–670. Doi: 10.31772/2712-8970-2022-23-4-657-670.

For citation: Basan E. S., Proshkin N. A., Silin O. I. [Improving the security of wireless communication channels for unmanned aerial vehicles by creating false information fields]. *Siberian Aerospace Journal.* 2022, Vol. 23, No. 4, P. 657–670. Doi: 10.31772/2712-8970-2022-23-4-657-670.

Повышение защищенности беспроводных каналов связи для беспилотных летательных аппаратов за счет создания ложных информационных полей

Е. С. Басан*, Н. А. Прошкин, О. И. Силин

Южный федеральный университет
Российская Федерация, 347922, Таганрог, ул. Чехова, 2
*E-mail: ebasan@sfedu.ru

На сегодняшний день проблемы, связанные с безопасностью беспилотных летательных аппаратов (БПЛА), стоят достаточно остро. Как правило, когда речь идет о коммерческих малогабаритных БПЛА, то для управления ими используются беспроводные каналы связи. Чаще всего организация связи реализуется на частоте 2,4 ГГц с применением протокола Wi-Fi. Такой БПЛА достаточно легко обнаружить, проанализировав радиочастотный диапазон или канальный уровень передачи данных, при этом не нужно обладать специализированным оборудованием и использовать открытое программное обеспечение. Обнаруженный БПЛА становится целью для проведения атак. Если известно, что БПЛА работает как беспроводная точка доступа, то все атаки, характерные для Wi-Fi, становятся актуальными для БПЛА. В данном исследовании предлагается для повышения устойчивости БПЛА к атакам в качестве первой линии защиты использовать технологию создания ложных информационных полей. Данная технология позволит скрыть легитимный БПЛА за множеством поддельных. Целью является создание поддельных точек доступа с характеристиками реальных и эмуляция передачи данных по каналам, на которых данные точки доступа развернуты. Кроме возможности скрыть легитимный БПЛА, данная технология позволяет вводить противника в заблуждение и заставлять думать, что на него надвигается ни один БПЛА, а группа. При попытке атаки ложных целей, противник себя скомпрометирует и может быть обнаружен. Таким образом, можно использовать БПЛА как приманку. В результате экспериментального исследования были выявлены каналы, на которых создание поддельных точек доступа наиболее эффективно. Используя небольшие вычислительные мощности и необходимую антенну, можно добиться высоких результатов. В данной статье продемонстрирована эффективность создания девяти поддельных точек доступа. Также проведено сравнение с реальным трафиком беспроводной сети. Можно сказать, что эмулированная активность является достаточно приближенной к реальной.

Ключевые слова: беспроводные каналы связи, точка доступа, радиоразведка, безопасность, уязвимости.

Improving the security of wireless communication channels for unmanned aerial vehicles by creating false information fields

E. S. Basan*, N. A. Proshkin, O. I. Silin

Southern Federal University
2, Chekhov St., Taganrog, 347922, Russian Federation
*E-mail: ebasan@sfedu.ru

To date, the problems associated with the safety of unmanned aerial vehicles (UAVs) are quite acute. As a rule, when it comes to commercial small-sized UAVs, wireless communication channels are used to control them. Most often, communication is implemented at a frequency of 2.4 GHz using the Wi-Fi protocol. Such a UAV is quite easy to detect by analyzing the radio frequency range or the data link layer. An attacker, however, may not even have specialized equipment and use open source software. The detected UAV becomes the target for attacks. If it is known that the UAV operates as a wireless access point, then all Wi-Fi-specific attacks become relevant for the UAV. In this study, it is proposed to use the technology of creating false information fields as the first line of defense to increase the resistance of the UAV to attacks. This technology will allow to hide a legitimate UAV communication channel behind a lot of fake ones. The goal is to create fake access points with the characteristics of real ones and emulate data transmission over the channels on which these access points are deployed. In addition to the fact that the technology allows to hide a legitimate UAV communication channel, it will also allow to mislead the attacker. It is important to make the intruder think that not a single UAV is approaching him, but a group. If the intruder attempts to attack decoys, attacker will compromise himself and be able to be detected. Thus, you can use the UAV as a bait. As a result of the pilot study, channels were identified on which the creation of fake access points is most effective. Using small computing power and the necessary antenna, you can achieve high results. This article demonstrates the effectiveness of creating 9 fake access points. A comparison was also made with real wireless network traffic. We can say that the emulated activity is quite close to the real activity.

Keywords: wireless communication channels, access point, radio intelligence, security, vulnerabilities.

Введение

Беспилотные летательные аппараты (БПЛА) сегодня становятся все более популярным решением для выполнения различных задач [1]. Более того, такие задачи часто бывают критическими [2]. В то же время БПЛА весьма уязвимы для атак злоумышленника, поскольку они физически незащищены [3]. Наиболее часто применяемые атаки используют уязвимости каналов связи. Можно попытаться спрятать БПЛА, обеспечив некоторую физическую защиту [4]. Многие страны используют БПЛА в военных целях, следовательно, страны потенциального противника также активно отслеживают наличие поблизости летающих беспилотников. Обнаружение малоразмерных БПЛА, в частности, ведется с помощью радиолокационного и оптического метода. В литературе были предложены различные методы обнаружения беспилотных летательных аппаратов с различными подходами, например, основанными на анализе аудиоинформации [5–7], видеоизображения с использованием камер [8–10] и радиочастотном зондировании [11; 12]. Однако каждый из этих подходов имеет свои достоинства и ограничения. Звуковые методы не действенны в шумной обстановке, имеют ограниченный диапазон и не могут обнаруживать БПЛА, использующие методы шумоподавления. Принимая во внимание, что подходы, основанные на использовании камер, требуют хороших условий освещения, высококачественных объективов и камер со сверхвысоким разрешением для обнаружения БПЛА на больших расстояниях, что, безусловно, обходится значительно дороже и сложнее реализуемо. Радиочастотные методы, основанные на использовании активного радара, уязвимы к радиочастотным помехам [13]. Тем не менее использование методов глубокого обучения дает большое

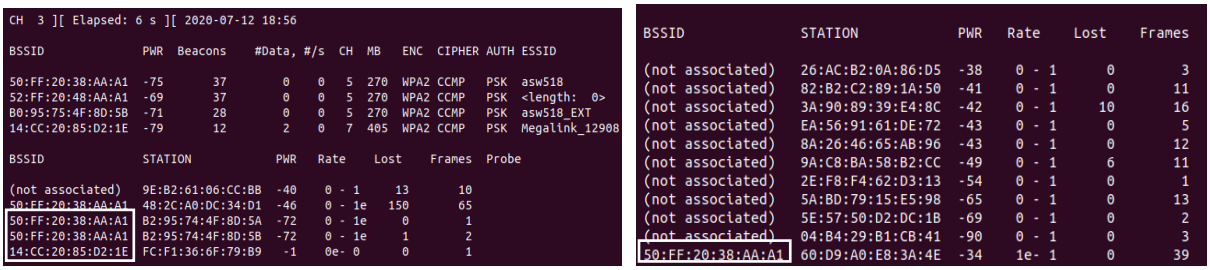
преимущество в обнаружении и классификации БПЛА с использованием глубоких нейронных сетей (DNN), которые также известны как многослойный персептрон (MLP). Более новые архитектуры глубокого обучения, такие как сверхточные нейронные сети (CNN), используются при обнаружении БПЛА. CNN используются для обнаружения БПЛА с использованием видеокамер CCTV [14] по изображениям наблюдения [15] и сигнатурам Доплера [16].

На сегодняшний день имеется большое количество работ, посвященных применению методов глубокого обучения для классификации радиочастотных сигналов. Примеры включают в себя решение задач определения спектра [17], обнаружение MIMO [18], оценку канала и обнаружение сигнала [19], связь на физическом уровне [20], обнаружение помех, [21], подавление скрытности [22; 23], управление мощностью [24], обнаружение подмены сигнала [25] и планирование передатчика-приемника [26]. Классификация радиочастотных сигналов может быть использована для различного применения, например, радиозахват [27], который в итоге может использоваться в системах когнитивного радио [28], подверженных динамическим и недетерминированным помехам [29]. Классификация модуляции с использованием глубоких нейронных сетей рассмотрена в работах [30–33], где целью является классификация данного сигнала по известному типу модуляции. Различные типы наборов данных были использованы для обучения глубокой нейронной сети в целях классификации модуляции.

Противодействие радиомониторингу, конечно, есть, например, передача шума на этой частоте или ложных данных, но это не предотвращает обнаружения БПЛА.

Зачастую для решения проблемы физической незащищенности каналов связи используют добавление шума в канал связи. Такой шум не влияет на качество передаваемой информации, но позволяет скрыть поток легитимных данных.

В беспроводных сетях Wi-Fi можно достаточно просто применить подобный способ защиты путем реализации атаки. Например, атака с использованием отправки большого числа пакетамаяков (beacon) имитирует наличие множества соседних точек доступа, что должно затруднить доступ клиента к законной точке доступа. Более того, эта атака фактически не затрагивает законных пользователей. Для наглядности рассмотрим рис. 1. У легитимной точки доступа MAC-адрес 50:FF:20:38:AA:A1. Проведем атаку с помощью маяка и попытаемся найти легитимную точку доступа. На рис. 1, *б* показано, что в этом случае, помимо легитимной точки доступа, существует множество других точек без идентификатора. При этом, если подделать идентификатор точки доступа, назначив идентификатор коммерческой фирмы БПЛА, можно ввести противника в заблуждение.



CH 3][Elapsed: 6 s][2020-07-12 18:56

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
50:FF:20:38:AA:A1	-75	37	0	0	5	270	WPA2	CCMP	PSK	asw518
52:FF:20:48:AA:A1	-69	37	0	0	5	270	WPA2	CCMP	PSK	<length: 0>
B0:95:75:4F:8D:5B	-71	28	0	0	5	270	WPA2	CCMP	PSK	asw518_EXT
14:CC:20:85:D2:1E	-79	12	2	0	7	405	WPA2	CCMP	PSK	Megalink_12908

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	9E:B2:61:06:CC:BB	-40	0 - 1	13	10	
50:FF:20:38:AA:A1	48:2C:A0:DC:34:D1	-46	0 - 1e	150	65	
50:FF:20:38:AA:A1	B2:95:74:4F:8D:5A	-72	0 - 1e	0	1	
50:FF:20:38:AA:A1	B2:95:74:4F:8D:5B	-72	0 - 1e	1	2	
14:CC:20:85:D2:1E	FC:F1:36:6F:79:B9	-1	0e- 0	0	1	

BSSID	STATION	PWR	Rate	Lost	Frames
(not associated)	26:AC:B2:0A:86:D5	-38	0 - 1	0	3
(not associated)	82:B2:C2:89:1A:50	-41	0 - 1	0	11
(not associated)	3A:90:89:39:E4:8C	-42	0 - 1	10	16
(not associated)	EA:56:91:61:DE:72	-43	0 - 1	0	5
(not associated)	8A:26:46:65:AB:96	-43	0 - 1	0	12
(not associated)	9A:C8:BA:58:B2:CC	-49	0 - 1	6	11
(not associated)	2E:F8:F4:62:D3:13	-54	0 - 1	0	1
(not associated)	5A:BD:79:15:E5:98	-65	0 - 1	0	13
(not associated)	5E:57:50:D2:DC:1B	-69	0 - 1	0	2
(not associated)	04:B4:29:B1:CB:41	-90	0 - 1	0	3
50:FF:20:38:AA:A1	60:D9:A0:E8:3A:4E	-34	1e- 1	0	39

а *б*

Рис. 1. Анализ сетевой активности (*а*) в нормальных условиях (*б*) при атаке с использованием beacon-флуда

Fig. 1. Analysis of network activity (*a*) under normal conditions (*b*) during an attack using a beacon flood

В таблице представлена информация о самых популярных квадрокоптерах и характеристиках точек доступа.

В данном исследовании предлагается способ сокрытия БПЛА путем создания ложных информационных полей. Метод протестирован путем анализа радиоспектра и сравнения создаваемых поддельных полей с реальными. Результаты показали эффективность разработанного

программного обеспечения, которое позволяет создавать ложные точки доступа, которые могут быть обнаружены злоумышленником и позволяют скрыть настоящую передачу.

Характеристики БПЛА в качестве точек доступа Wi-Fi

Название БПЛА	SSID	Пароль
HUBSAN X4 STAR PRO	Hubsan_h507a_ *****	12345678
XIRO XPLORER MINI	XPLORER_Mini_0b5abe	XIRO1234
MJX X601H	MJX H ***	вшит в приложение
Parrot BEBOP	BebopDrone-BO56122	вшит в приложение
XK Innovations X300-W	XK innovat	вшит в приложение

Модуль создания ложных информационных полей вокруг БПЛА

Беспроводная среда передачи данных априори является небезопасной, так как ее практически невозможно защитить физически. Часто режим радиомолчания используется, чтобы скрыть БПЛА. В этом режиме не предусмотрена возможность передачи информации на БПЛА. В то же время, учитывая современные тенденции создания единого киберпространства, когда устройства должны не только собирать и передавать данные, но и обмениваться данными между собой для координации своих действий, работа в режиме радиомолчания может быть недопустимой [34]. Также могут быть использованы методы наложения радиопомех на канал связи, которые маскируют законную передачу информации [35]. Этот метод требует дополнительного оборудования и затрат, поэтому он не всегда применим [36].

Предлагаемый программный модуль обеспечивает сокрытие законного канала связи путем создания множества точек беспроводного доступа. Исследование позволило определить параметры гражданских БПЛА для сетевой связи и смоделировать эти параметры, чтобы скрыть легитимный БПЛА [37]. Гражданские БПЛА работают следующим образом: сетевой адаптер БПЛА переключается в режим создания точки доступа после того, как оператор создал точку доступа и, зная параметры подключения (как правило, это MAC-адрес точки доступа и ее идентификатор), может подключиться к нему с авторизованного устройства [38]. Таким образом, задача программного модуля – создать несколько точек доступа, которые бы уведомляли гражданский БПЛА о параметрах. Программный модуль позволяет изменять количество создаваемых информационных полей. Такой подход позволит минимизировать риски, связанные с возможностью реализации атак по каналам беспроводной связи БПЛА [39]. Поэтому при информационном сканировании сети противник будет видеть картину, представленную на рис. 2.

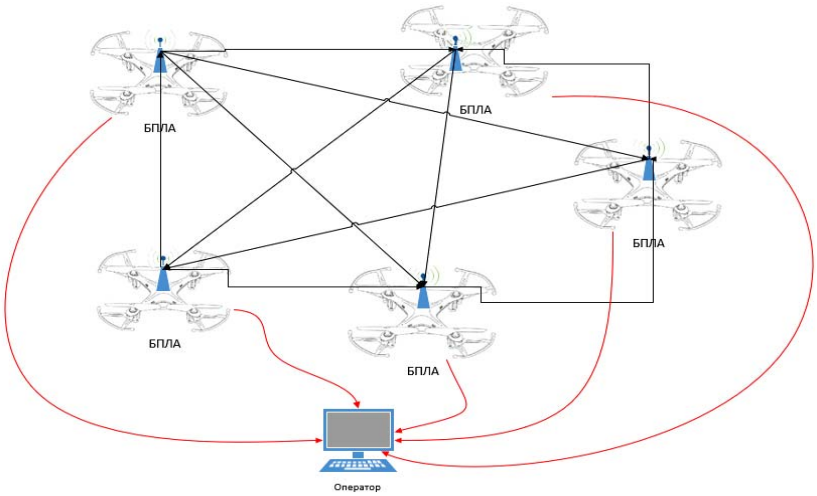


Рис. 2. Абстракция представления БПЛА для противника при радиоразведке

Fig 2. Abstraction of the representation of the UAV for the enemy in radio intelligence

Каждая точка доступа работает на отдельном радиоканале, стандарт IEEE 802.11 реализован таким образом, что вещание на определенном канале происходит постоянно, поэтому анализ частоты Wi-Fi при включенном модуле покажет активность нескольких устройств (БПЛА), как показано на рис. 2 [40]. Таким образом, создаются ложные информационные поля вокруг БПЛА. Данные информационные поля предназначены для нескольких целей. Во-первых, программный модуль позволяет скрыть реальный БПЛА от противника, который использует метод радиоразведки. Кроме того, модуль позволяет ввести противника в заблуждение путем представления ложной информации, что на противгика надвигается ни один, а группа БПЛА. Во-вторых, программный модуль позволяет создать для противника «приманку», чтобы тот попытался получить доступ к поддельному БПЛА, тем самым выдав себя. Программный модуль реализован для одноплатного компьютера Raspberry Pi 3 модели B и требует использования внешнего адаптера Wi-Fi для создания ложных точек беспроводного доступа. Модуль эмуляции состоит из микрокомпьютера Raspberry Pi 3 модели B, батареи микрокомпьютера для возможности автономной работы, ОС Linux Raspbian для Raspberry Pi, беспроводного USB-адаптера Wi-Fi ZyXEL G-202 EE и реализованного программного обеспечения. Разработанный программный модуль запускает сценарий для создания множество поддельных точек доступа Wi-Fi автоматически при наступлении события [41]. Утилита airbase-ng [42] в ОС Linux используется для создания поддельных точек доступа [43]. Разработанный программный модуль состоит из трех подсистем:

1) подсистема инициализации интерфейса – необходима для правильного определения сетевого интерфейса, на котором будут созданы ложные информационные поля;

2) подсистема генерации ложных информационных полей – служит для перевода нужного интерфейса в режим монитора и создания на нем поддельных точек доступа;

3) подсистема реагирования на события – действует как связующая оболочка между двумя предыдущими подсистемами, выполняет функции приема и передачи данных от одной подсистемы к другой, а также автоматически включается при необходимых условиях.

Анализ частотного спектра, излучаемого модулем для создания ложных информационных полей

Эксперименты проводились с использованием анализатора спектра GW In-stek (GSP827) в условиях слабого воздействия излучающих антенн. Лабораторный стенд представлен на рис. 3 [44]. Стандарт беспроводной связи 2,4 ГГц допускает только 14 каналов с шириной канала 20–22 МГц. Оптимальными для одновременного использования являются каналы 1, 6, 11; 2, 7, 12; 3, 8, 13 или 4, 9, 14. Но в этом исследовании будем считать, что нет необходимости передавать полезные данные. Активный радио трафик генерируется дополнительными флагами эмуляции, установленными в программе. Стандарт 5 ГГц имеет 140 разделенных по частоте каналов, соответственно можно развернуть в 10 раз больше ТД, но при этом радиус излучения уменьшается в два раза. В данном исследовании проведен эксперимент с частотой 2,4 ГГц с радиусом излучения до 150 м на открытой местности с мощностью передатчика 18 дБ. Максимальное число в 14 каналов на частоте 2,4 ГГц не означает, что может быть развернуто только 14 точек доступа. Две и более точки доступа, работающие на одном канале, просто накладываются друг на друга и передают трафик поочередности. Это представлено на рис. 4 [3].

На рис. 5 представлено сравнение дальности связи Wi-Fi 2,4 и 5 ГГц на открытой местности.

В легитимной реализации множества точек доступа, конечно, возможна потеря эффективности связи, но это не важно. В радиочастотном методе эмулирования нескольких БПЛА, наоборот, приветствуется активный радиотрафик на радиорадаре, который схож с активным TCP-соединением и передачей пакетов.

Для начала проанализируем спектр частоты работающего телефона в качестве точки доступа, но без подключения к нему никаких устройств, т. е. точка доступа отсылает с определенным периодом Beacon-пакеты (маячковые пакеты), но радиотрафик отсутствует. Отметим общие

пояснения терминов на рис. 6 для каждого спектра сигналов на примере спектра двух точек доступа, работающих на разных каналах с шириной спектра 75 МГц.

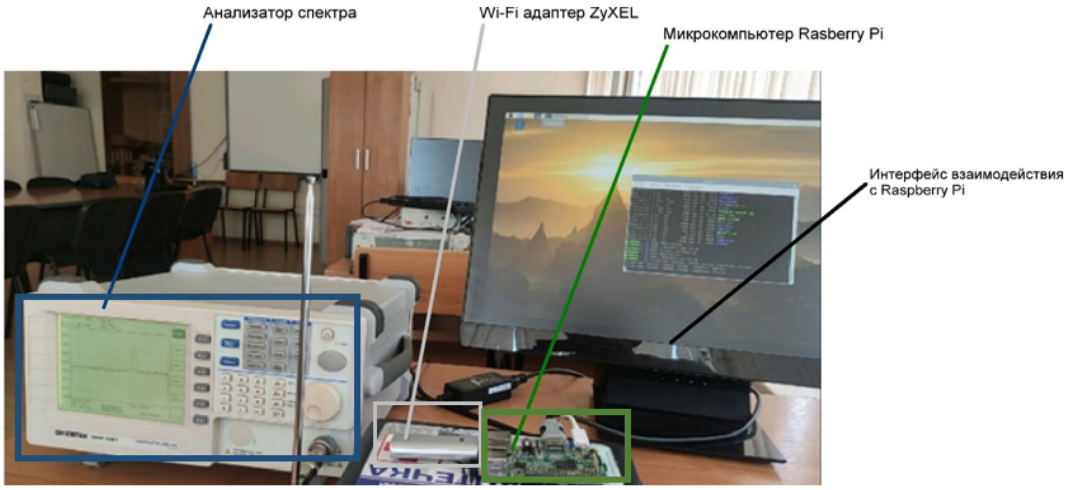


Рис. 3. Экспериментальный стенд для анализа спектра

Fig. 3. Experimental stand for spectrum analysis

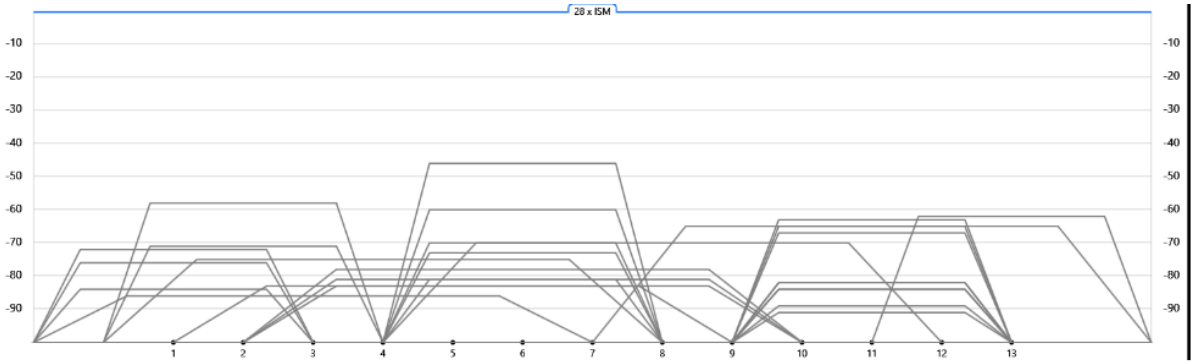


Рис. 4. Эффект наложения друг на друга точек доступа

Fig. 4. The effect of overlapping access points

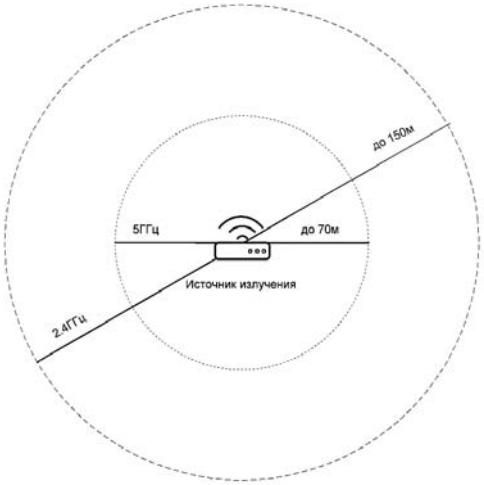


Рис. 5. Дальность связи Wi-Fi

Fig. 5. Wifi range

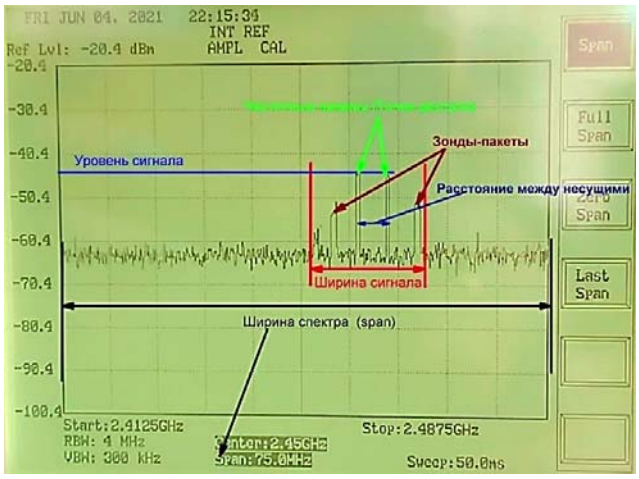
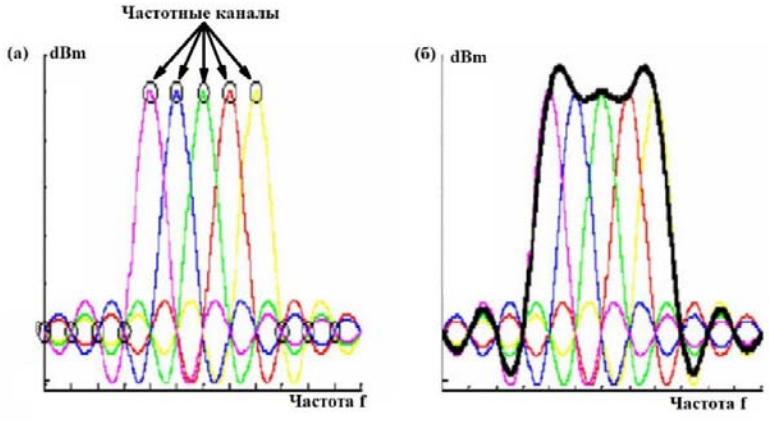


Рис. 6. Пояснение к терминам, использованным при анализе

Fig. 6. Explanation of the terms used in the analysis

Ширина полосы частот 400 МГц, средняя несущая частота 2,4 ГГц, начальное значение спектра 2,2 ГГц. Максимальный уровень сигнала достигает примерно –30 дБ с частотой примерно 2,46 ГГц, что соответствует каналу 11 в стандарте Wi-Fi. Частота появления несущих примерно 2 раза в секунду. Разница между отправкой пакетов Beacon и активным TCP-соединением на анализаторе спектра заключается в том, что ширина сигнала и частота появления несущих увеличились, сигнал стал непрерывным, это указывает на то, что какое-то устройство обменивается данными через беспроводную сеть в конкретный момент с другим устройством. Теперь, когда понятно, как выглядит сигнал простой точки доступа и точки доступа с подключенным к нему устройством и активным обменом пакетами, перейдем к анализу поддельных точек доступа, как количество и разделение по каналам влияет на тип сигнала, частоту появления пиков и ширину радиотрафика в целом.

С повышением количества точек доступа мы должны наблюдать такую картину, как на рис. 7: каждый отдельный канал, т. е. отдельная точка доступа, должен выглядеть как один пик на спектре (одна несущая) (рис. 7, *а*), но из-за несовершенства антенны и физических свойств электромагнитной волны, можно увидеть объединение этих пиков (рис. 7, *б*).



а *б*

Рис. 7. Спектр множества точек доступа: *а* – совершенные несущие; *б* – огибающая несущих

Fig. 7. Spectrum of multiple access points: *a* – perfect carriers; *b* – envelope of carriers

В следующем эксперименте было создано 25 точек доступа, их количество постепенно увеличивалось без отключения предыдущих. Сигнал полностью аналогичен сигналу на рис. 6, но с более низким уровнем, равным –50 дБм. Из-за меньшей мощности передатчика был установлен канал 12, который соответствует средней частоте сигнала. На рис. 8 показан спектр сигнала 1 точки доступа, но с включенными флагами активной эмуляции. Частота пиков увеличилась примерно в 2 раза, а уровень сигнала немного увеличился на 0,2–0,4 дБ. Появился еще один носитель, созданный опцией отправки дополнительных зондовых пакетов для известных устройств. На рис. 8 показаны спектры сигналов от разного количества ложных точек доступа. Количество несущих увеличивается, расстояние между ними уменьшается, а трафик становится более активным за счет увеличения количества точек доступа.

Можно сделать вывод, что прирост эффективности эмулирования становится меньше после девяти точек доступа. Однако, при повышении числа точек доступа до двадцати пяти, средняя несущая частота сигнала сместилась на частоту 2,46 ГГц и ширина сигнала стала равна около 25 МГц.

Для определения диапазона эффективного количества поочередно включенных ТД на рис. 9 и 10 продемонстрированы спектры сигналов 5-и, 3-х, 2-х, и 1-й точек доступа на ширине спектра 75 МГц.

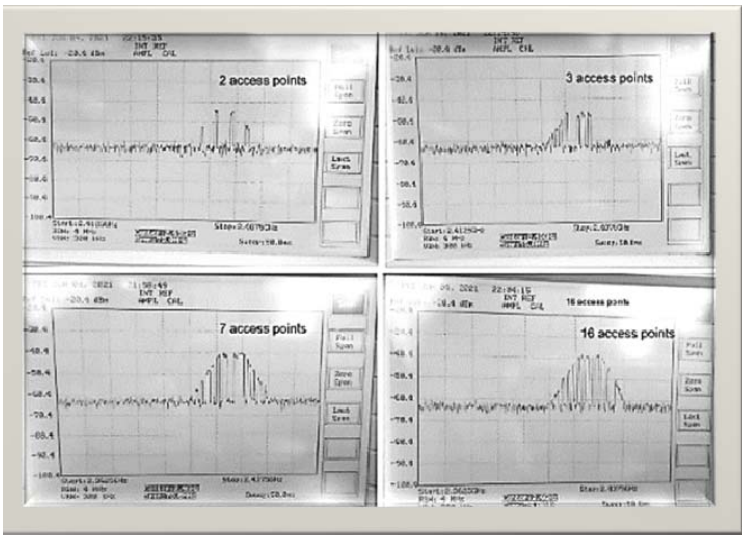
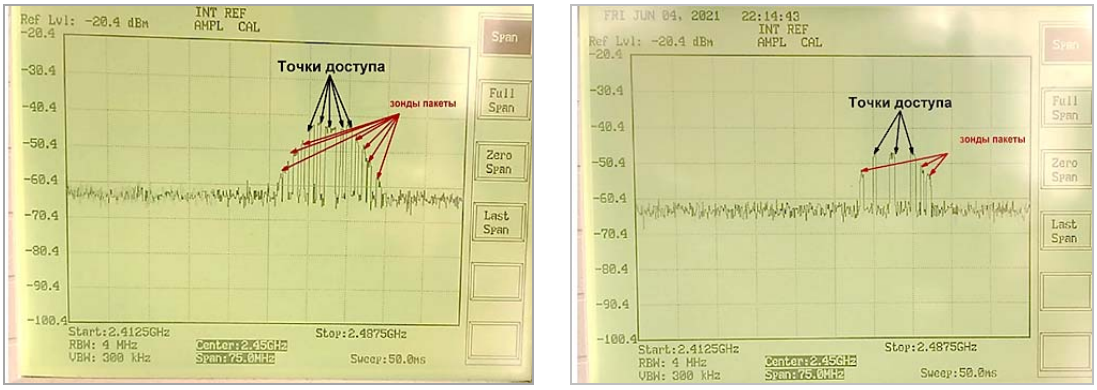


Рис. 8. Сигналы разного количества точек доступа

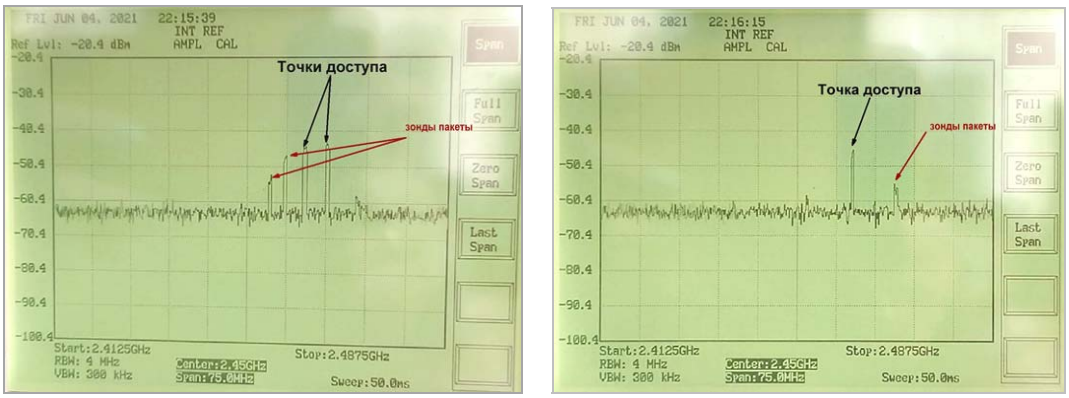
Fig. 8. Signals of a different number of access points



а *б*

Рис. 9. Сравнение сигналов 5-и и 3-х точек доступа. Ширина спектра 75 МГц:
а – 5 точек доступа; *б* – 3 точки доступа

Fig. 9. Comparison of signals of 5 and 3 APs. Spectrum width 75 MHz:
a – 5 access points; *b* – 3 access points



а *б*

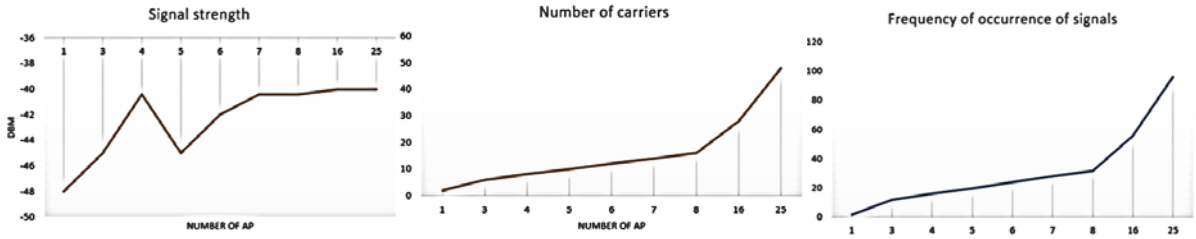
Рис. 10. Сравнение сигналов 2-х и 1-й точек доступа. Ширина спектра 75 МГц:
а – 2 точки доступа; *б* – 1 точка доступа

Fig. 10. Comparison of signals of the 2nd and 1st AP. Spectrum width 75 MHz: *a* – 2 APs; *b* – 1 AP

Проанализировав рис. 8–10, становится отчетливо видно, что с повышением количества точек доступа расстояние между несущими уменьшается, частота появления пиков увеличивается, ширина сигнала увеличивается до количества точек доступа равного 7. На рис. 11 показаны зависимости параметров: уровня сигнала, количества несущих и частоты появления несущих от количества точек доступа. Адаптер ZyXEL Wi-Fi может транслировать только 14 каналов шириной 20–22 МГц каждый. Программное обеспечение используется для установки номеров каналов 1, 6, 11, 16, 21, 26, 31, 36, 41, 46 и т. д. Следовательно, канал с номером больше 14 будет иметь номер, рассчитанный по формуле (1):

$$Nk = NPk \ mod \ 14, \tag{1}$$

где Nk – это актуальный номер канала; NPk – программируемый номер канала; mod – это целочисленный остаток от деления.



а *б* *в*

Рис. 11. Зависимость уровня сигнала от количества точек доступа (*а*), количества несущих от количества точек доступа (*б*), частоты появления несущих от количества точек доступа (*в*)

Fig. 11. Dependence of (*a*) signal level on the number of access points (*b*) the number of carriers on the number of access points (*c*) the frequency of occurrence of carriers on the number of access points

Из рис. 12 видно, что фактические каналы перекрывают друг друга, особенно зашумленными каналами являются 2, 7, 12.

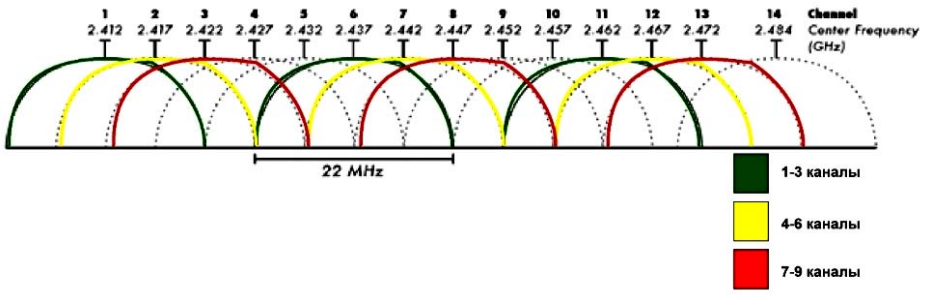


Рис. 12. Перекрытие каналов поддельных точек доступа

Fig. 12. Overlapping fake AP channels

Из этого следует, что создаваемые каналы перекрывают друг друга. Однако, поскольку адаптер не может транслировать одновременно по 14 каналам, трансляция происходит поочередно, но очередь состоит не из реальных каналов, а из каналов, которые были указаны программно, т. е. передача пакетов происходит сначала по 1, потом 6, потом 11, 2, 7 каналам и т. д. За счет такой организации очереди отправки пакетов интерференция волн намного меньше. На рис. 13 показано сравнение реального TCP-соединения на частоте 2,4 ГГц и 5 фиктивных точек доступа. По форме параметры сигнала похожи друг на друга, что даст ошибочное представление об объекте разведки.

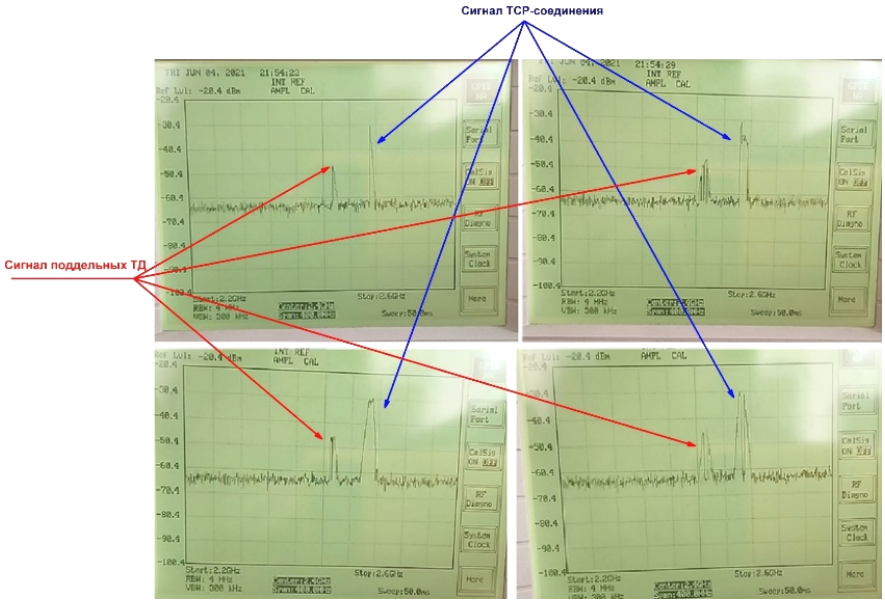


Рис. 13. Сравнение сигналов пяти точек доступа и TCP-соединения

Fig. 13. Comparison of the signals of five access points and a TCP connection

После активации модуля в течение нескольких секунд происходит создание 14 поддельных точек доступа Wi-Fi. Это можно пронаблюдать с помощью любого устройства с Wi-Fi (рис. 13).

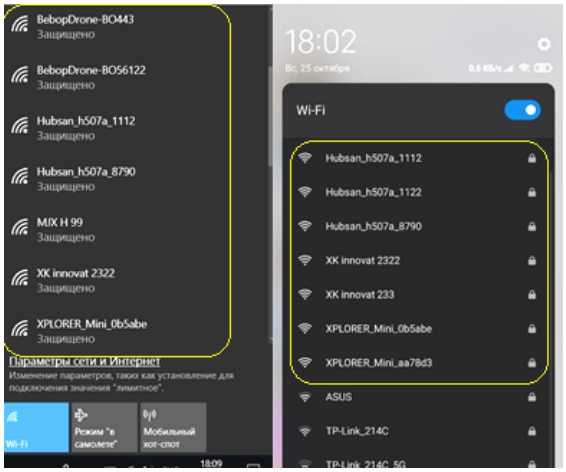


Рис. 14. Демонстрация работы модуля

Fig. 14. Demonstration of the module

Из рис. 14 видно, что Wi-Fi телефона (рис. 14, справа) и адаптер компьютера (рис. 14, слева) одинокого видят поддельные точки доступа, причем они находятся по списку раньше легитимных.

Заключение

В этом исследовании продемонстрирована работа модуля эмуляции радиочастоты для нескольких сигналов БПЛА путем создания поддельных точек доступа, которые передают трафик, состоящий только из пакетов маяков и зондов. Анализ спектров возрастающего количества точек доступа показал, что с увеличением количества точек доступа изменяется количество несущих частот, что показывает несколько работающих отдельных устройств Wi-Fi, частота

появления пиков увеличивается – увеличивается вероятность замешательства противника – имитация активного радиотрафика, при этом 9 одновременно работающих точек доступа никак не влияют на эффективность. Анализ спектра реальной работы устройства показал, что при одновременном включении 13 точек доступа сигнал становится более непрерывным и эффективным по сравнению с 9 точками доступа. Когда 13 точек доступа создаются и запускаются одновременно, каждая из них осуществляет широковещательную передачу с равным интервалом времени от соседней, то достигается эффект непрерывного радиотрафика. В рамках исследования были решены следующие задачи:

– проведен анализ характеристик информационных полей БПЛА;

– определены ключевые характеристики информационных полей;

– обосновано соответствие характеристик ложных информационных полей характеристикам реальных точек доступа БПЛА;

– реализован процесс создания легитимных информационных полей.

В заключение отметим, что эксперимент проведен с простейшим адаптером Wi-Fi и слабой антенной. В реальных условиях следует использовать гораздо более мощный излучатель для увеличения дальности и уровня сигнала, а противник будет использовать более чувствительную антенну.

Благодарности. Работа выполнена при финансовой поддержке Совета по грантам Президента Российской Федерации за счет средств стипендии Президента Российской Федерации молодым ученым и аспирантам (Конкурс СП-2022) № СП-858.2022.5 на тему «Технология обеспечения кибербезопасности автоматизированных систем от активных информационных атак на основе принципа рефлексии».

Acknowledgements. The work was financially supported by the Council for Grants of the President of the Russian Federation at the expense of the scholarship of the President of the Russian Federation for young scientists and graduate students (Competition SP-2022) No. SP-858.2022.5 on the topic “Technology for ensuring cybersecurity of automated systems from active information attacks based on the principle of reflection”.

References

1. Xu C., Liao X., Tan J., Ye H., Lu H. Recent Research Progress of Unmanned Aerial Vehicle Regulation Policies and Technologies in Urban Low Altitude. *IEEE Access.* 2020, Vol. 8. P. 74175–74194. Doi: 10.1109/ACCESS.2020.2987622.

2. Shi Y., Bai M., Li Y. Study on UAV Remote Sensing Technology in Irrigation District Informationization Construction and Application. *10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA)*. Changsha, China, 2018, P. 252–255. Doi: 10.1109/ICMTMA.2018.00067.

3. Gao X., Jia H., Chen Z., Yuan G., Yang S. UAV security situation awareness method based on semantic analysis. *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*. Shenyang, China, 2020, P. 272–276. Doi: 10.1109/ICPICS50287.2020.9201954.

4. Basan E., Medvedev M., Teterevyatnikov S. Analysis of the Impact of Denial-of-Service Attacks on the Group of Robots. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, China, 2018, P. 63–68. Doi: 10.1109/CyberC.2018.00023.

5. Bernardini A., Mangiatordi F., Pallotti E., Capodiferro L. Drone detection by acoustic signature identification. *IS TInt. Symp. Electron. Imaging Sci. Technol.* 2017, P. 60–64.

6. Kim J., Park C., Ahn J., Ko Y., Park J., Gallagher J. C. Real-time UAV sound detection and analysis system. *IEEE Sensor Application Symposium (SAS).* United States, 2017, P. 1–5.

7. Nijim M., Mantrawadi N. Drone classification and identification system by phenome analysis using data mining techniques. *IEEE Symposium on Technologies for Homeland Security.* Waltham, MA, United States, 2016, P. 1–5.

8. Aker C., Kalkan S. Using deep networks for drone detection. *IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS).* Lecce, Italy, 2017, P. 1–6. Doi: 10.1109/AVSS.2017.8078539.

9. Saqib M., Daud Khan S., Sharma N., Blumenstein M. A study on detecting drones using deep convolutional neural networks. *14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS).* Lecce, Italy, 2017, P. 1–5. Doi: 10.1109/AVSS.2017.8078541.

10. Nguyen P., Ravindranathan M., Nguyen A., Han R., Vu T. Investigating cost-effective RF-based detection of drones. *2nd Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use (DroNet '16).* Association for Computing Machinery. New York, NY, USA, 2016, P. 17–22. Doi: https://doi.org/10.1145/2935620.2935632.

11. Ezuma M., Erden F., Anjinappa C. K., Ozdemir O., Guvenc I. Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques. *IEEE Aerospace Conference.* Big Sky, MT, USA, 2019, P. 1–13. Doi: 10.1109/AERO.2019.8741970.

12. Abeywickrama S., Jayasinghe L., Fu H., Nissanka S., Yuen C. RF-based Direction Finding of UAVs Using DNN. *IEEE International Conference on Communication Systems (ICCS).* Chengdu, China, 2019, P. 157–161. Doi: 10.1109/ICCS.2018.8689177.

13. Fonseca R., Creixell W. Tracking and following a moving object with a quadcopter. *14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS).* Lecce, Italy, 2017, P. 1–6. Doi: 10.1109/AVSS.2017.8078463.

14. Kim B. K., Kang H. S., Park S. O. Drone classification using convolutional neural networks with merged doppler images. *IEEE Geoscience and Remote Sensing Letters*. 2017, Vol. 14, No. 1, P. 38–42.

15. Davaslioglu K., Sagduyu Y. E. Generative adversarial learning for spectrum sensing. *IEEE International Conference on Communications (ICC).* Kansas City, MO, USA, 2018, P. 1–6. Doi: 10.1109/ICC.2018.8422223.

16. He H., Wen C.-K., Jin S., Li G. Y. A model-driven deep learning network for MIMO detection. *IEEE Transactions on Signal Processing.* 2018, Vol. 68, P. 1702–1715.

17. Ye H., Li G. Y., Juang B.-H. Power of deep learning for channel estimation and signal detection in OFDM systems. *IEEE Wireless Communications Letters.* 2018, Vol. 7, No. 1, P. 114–117. Doi: 10.1109/LWC.2017.2757490.

18. O'Shea T. J., Hoydis J. An introduction to deep learning for the physical layer // IEEE Transactions on Cognitive Communications and Networking (TCCN). 2017. Vol. 3, No. 4. P. 563–575. Doi: 10.1109/TCCN.2017.2758370.

19. Shi Y., Sagduyu Y. E., Erpek T., Davaslioglu K., Lu Z., Li J. Adversarial deep learning for cognitive radio security: jamming attack and defense strategies. *IEEE ICC 2018 Workshop – Promises and Challenges of Machine Learning in Comm. Networks.* 2018, P. 1–6. Doi: 10.1109/ICCW.2018.8403655.

20. Shi Y., Erpek T., Sagduyu Y. E., Li J. Spectrum data poisoning with adversarial deep learning. *IEEE Military Communications Conference.* Los Angeles, CA, USA, 2018, P. 407–412. Doi: 10.1109/MILCOM.2018.8599832.

21. Sagduyu Y. E., Shi Y., Erpek T. IoT network security from the perspective of adversarial deep learning. *IEEE International Conference on Sensing, Communication and Networking (SECON) Workshop on Machine Learning for Communication and Networking in IoT.* Boston, MA, USA, 2019, P. 1–9. Doi: 10.1109/SAHCN.2019.8824956.

22. Erpek T., Sagduyu Y. E., Shi Y. Deep learning for launching and mitigating wireless jamming attacks. *IEEE Transactions on Cognitive Communications and Networking.* 2019, Vol. 5, No. 1, P. 2–14. Doi: 10.1109/TCCN.2018.2884910.

23. Shi Y., Davaslioglu K., Sagduyu Y. E. Generative adversarial network for wireless signal spoofing. *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*

Workshop on Wireless Security and Machine Learning (WiseML). Miami FL USA, 2019, P. 55–60. Doi: https://doi.org/10.1145/3324921.3329695.

24. Abu Zainab N. et al. QoS and jamming-aware wireless networking using deep reinforcement learning. *IEEE Military Communications Conference (MILCOM).* Norfolk, VA, USA, 2019, P. 610–615. Doi: 10.1109/MILCOM47813.2019.9020985.

25. Restuccia F. et al. DeepRadioID: Real-time channel-resilient optimization of deep learning-based radio fingerprinting algorithms. *ACM Intl. Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc).* New York, NY, United States, 2019, P. 51–60. Doi: https://doi.org/10.1145/3323679.3326503.

26. Soltani S. Distributed cognitive radio network architecture, SDR implementation and emulation testbed. *IEEE Military Communications Conference (MILCOM).* Tampa, FL, USA, 2015, P. 438–443. Doi: 10.1109/MILCOM.2015.7357482.

27. Sagduyu Y. E., Berry R., Ephremides A. Jamming games in wireless networks with incomplete information. *IEEE Communications Magazine.* 2011, Vol. 49, No. 8, P. 112–118. Doi: 10.1109/MCOM.2011.5978424.

28. O'Shea T., Corgan J., Clancy C. Convolutional radio modulation recognition networks // Communications in Computer and Information Science. 2016, Vol. 629. Springer, Cham. Doi: https://doi.org/10.1007/978-3-319-44188-7_16.

29. O'Shea T. J., Roy T., Clancy T. C. Over-the-air deep learning-based radio signal classification. *IEEE Journal of Selected Topics in Signal Processing.* 2018, Vol. 12, No. 1, P. 168–179. Doi: 10.1109/JSTSP.2018.2797022.

30. Ali A., Fan Y. Unsupervised feature learning and automatic modulation classification using deep learning model. *Physical Communication.* 2017, Vol. 25, P. 75–84.

31. Shi Y. et al. Deep learning for signal classification in unknown and dynamic spectrum environments. *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN).* Newark, NJ, USA, 2019, P. 1–10. Doi: 10.1109/DySPAN.2019.8935684.

32. Kiranyaz S., Zabihi M., Rad A. B., Tahir A., Ince T., Hamila R. Real-time PCG Anomaly Detection by Adaptive 1D Convolutional Neural Networks. *Signal Processing.* 2016, P. 1–12. Doi: https://doi.org/10.48550/arXiv.1902.07238.

33. Zheng Y., Liu Q., Chen E., Ge Y., Zhao J. L. Exploiting multi-channels deep convolutional neural networks for multivariate time series classification. *Front. Comput. Sci.* 2016, Vol. 10, No. 1, P. 96–112.

34. Mikhalevich I. F., Trapeznikov V. A. Critical Infrastructure Security: Alignment of Views. In *Systems of Signals Generating and Processing in the Field of on Board Communications*. Moscow Technical University of Communications and Informatics, Russia, 2019, P. 1–5. Doi: 10.1109/SOSG.2019.8706821.

35. Ilioudis C. V., Clemente C., Soraghan J. Understanding the potential of Self-Protection Jamming on board of miniature UAVs. *In International Radar Conference (RADAR).* Toulon, France, 2019, P. 1–6. Doi: 10.1109/RADAR41533.2019.171405.

36. Li X., Ju R., Wang H., Sun Y. The Design and Research of Data Transmission on Remote Radio Control in Different Noise Channel. *13th World Congress on Intelligent Control and Automation (WCICA)*. Changsha, China, 2018, P. 1306–1311. Doi: 10.1109/WCICA.2018.8630340.

37. Proshkin N., Basan E., Lapina M. Radio Frequency Method for Emulating Multiple UAVs. *17th International Conference on Intelligent Environments (IE).* Dubai, United Arab Republic, 2021, P. 1–4. Doi: 10.1109/IE51775.2021.9486599.

38. Basan E., Basan A., Nekrasov A., Fidge C., Sushkin N., Peskova O. GPS-Spoofing Attack Detection Technology for UAVs Based on Kullback–Leibler Divergence. *Drones*. 2022, No. 6(1), P. 8. Doi: https://doi.org/10.3390/drones6010008.

39. Astaburuaga I., Lombardi A., La Torre B., Hughes C., Sengupta S. Vulnerability Analysis of AR. Drone 2.0, an Embedded Linux System. *IEEE 9th Annual Computing and Communication*

Workshop and Conference (CCWC). United States, 2019, P. 0666–0672. Doi: 10.1109/CCWC.2019.8666464.

40. Caballé M. C., Augé A. C., Lopez-Aguilera E., Garcia-Villegas E., Demirkol I., Aspas J. P. An Alternative to IEEE 802.11ba: Wake-Up Radio with Legacy IEEE 802.11 Transmitters. *IEEE Access.* 2019, Vol. 7, P. 48068–48086. Doi: 10.1109/ACCESS.2019.2909847.

41. Madruga S., Tavares A., Brito A., Nascimento T. A Project of an Embedded Control System for Autonomous Quadrotor UAVs. *Latin American Robotic Symposium, Brazilian Symposium on Robotics (SBR) and 2018 Workshop on Robotics in Education (WRE)*. João Pessoa, Brazil, 2018, P. 483–489. Doi: 10.1109/LARS/SBR/WRE.2018.00091.

42. Carranza A., Mayorga D., DeCusatis C. Comparison of Wireless Network Penetration Testing Tools on Desktops and Raspberry Pi Platforms. *16th LACCEI International Multi-Conference for Engineering, Education and Technology.* Boca Raton, Florida, USA, 2018, P. 1–5.

43. Abril-García J. H. et al. Application to monitoring a USB control with Python in Windows, Mac OS and Raspbian OS. *ECORFAN Journal Democratic Republic of Congo.* 2019, Vol. 5 (8), P. 1–6.

44. Korneev S. Digital spectrum analyzer GSP-7830 manufactured by GW Instek. *Components and technologies.* 2008, Vol. 1 (78), P. 158–162.

Басан Елена Сергеевна – кандидат технических наук, доцент; Южный федеральный университет. E-mail: ebasan@sfedu.ru.

Прошкин Никита Андреевич – студент; Южный федеральный университет. E-mail: nproshkin@sfedu.ru .

Силин Олег Игоревич – аспирант; Южный федеральный университет. E-mail: silin@sfedu.ru.

Basan Elena Sergeevna – Cand. Sc., Associate Professor; Southern Federal University. E-mail: ebasan@sfedu.ru.

Proshkin Nikita Andreevich – student; Southern Federal University. E-mail: nproshkin@sfedu.ru.

Silin Oleg Igorevich – post-graduate student; Southern Federal University. E-mail: silin@sfedu.ru.