

# ТЕОРИЯ И ПРАКТИКА ПОСТРОЕНИЯ СКРЫТЫХ РЭЛЕЕВСКИХ Wi-Fi КАНАЛОВ СВЯЗИ

Стрельницкий А. А., Шокало В. М.  
Харьковский национальный университет радиоэлектроники  
г. Харьков, пр. Ленина, 14, 61166, Украина  
тел.: 057-7021430, e-mail: stal.sivan@gmail.com

**Аннотация** — В докладе исследуются пути повышения скрытности Wi-Fi рэлеевских каналов связи, уровень которой характеризуется вероятностью обнаружения  $P_{об}$ . В результате работы предложены более совершенная модель расчета величины  $P_{об}$ , метод расчета зоны обнаружения и новый способ повышения скрытности радиоканала за счет его работы под искусственным шумом.

## I. Введение

Одно из известных направлений исследований энергетической скрытности рэлеевских каналов связи цифровых систем передачи информации (ЦСПИ) базируется на концепции отводного канала Вайнера. Исходя из этой концепции в работах [1, 2] получены соотношения вероятности обнаружения  $P_{об}$  рэлеевских каналов связи.

Скрытность рэлеевских S/SO каналов с квазистатическим затуханием исследовались во многих публикациях. Но в этих работах изложены модели анализа скрытности, в которых не учтено влияние электродинамических характеристик антенн легитимного и отводного каналов, а также разнообразие механизмов распространения радиоволн. Кроме того, в опубликованных работах не разработаны методы построения границ зон обнаружения (ЗО) для таких каналов. Однако известно, что на основе анализа границ зон обнаружения могут быть разработаны эффективные организационно-технические мероприятия по обеспечению энергетической скрытности каналов связи. Таким образом, исследование зон обнаружения рэлеевских каналов связи с квазистатическим замиранием является актуальной задачей.

Целью данной работы является усовершенствование моделей анализа скрытности многолучевых беспроводных каналов связи уровня LAN, экспериментальная проверка возможности применения их на практике, а также разработка на основе этих моделей метода построения границ зон обнаружения и нового способа повышения скрытности радиоканала за счет его работы под искусственным шумом.

## II. Результаты исследований зон обнаружения рэлеевских каналов связи

Опираясь на работы [1, 2] и вводя ряд приближений, в докладе получено следующее выражения для вероятности обнаружения:

$$P_{об} = 1 - \frac{\exp\left[-\frac{2^{R_s} - 1}{(S/N)_л}\right]}{1 + 2^{R_s} \cdot \frac{\alpha_o \cdot F_o^2(r_o, \theta_3) \cdot F_n^2(r_n, \theta_1)}{\alpha_n \cdot F_n^2(r_n, \theta_2) \cdot F_n^2(r_n, \theta_1)}}, \quad (1)$$

где  $R_s$  – секретная скорость передачи информации при которой ЦСПИ считается секретной (не обнаруживается),  $(S/N)_л$  – среднее значение сигнал/шум в легитимном канале;  $r_n, r_o$  – расстояние от антенны передатчика до антенн приемников легитимного и отводного каналов соответственно;  $\alpha_o, \alpha_n$  – функциональные

зависимости затухания сигнала в легитимном и отводном каналах;  $\theta_1, \theta_2, \theta_3$  – текущие углы отсчетов значений угловых интенсивностей напряженности поля (УЗИП) передающей антенны  $F_n(r_n, \theta_1)$  и приемных антенн легитимного  $F_n(r_n, \theta_2)$  и отводного  $F_o(r_o, \theta_3)$  каналов в местной системе координат.

Применяя выражение (1) можно построить зону обнаружения ЦСПИ, воспользовавшись понятием кривых постоянной вероятности обнаружения  $P_{об}(r, \theta) = const$ . Они ограничивают двумерное пространство на плоскости  $(r, \theta)$ , внутри и на границе которого  $P_{об}(r, \theta) \geq 0,7$ . Строятся кривые постоянной вероятности обнаружения таким образом. Вначале по формуле (1) рассчитываются кривые  $P_{об} = f(r)$  при различных углах  $\theta_{3i}$ . Рассчитанные кривые аппроксимируются полиномами, которые приравняются к заданному значению  $P_{об} = 0,7$ . Для каждого из этих уравнений находятся корни  $r_1, r_2, r_3, \dots, r_n$ . Кривая, проходящая через точки  $(r_1, \theta_{31}), (r_2, \theta_{32}), \dots, (r_n, \theta_{3n})$  и является кривой постоянной вероятности обнаружения.

Предварительно были проведены экспериментальные исследования УЗИП для оценки вероятности обнаружения. Подробнее, описание экспериментов будет изложено в докладе. Результаты расчетов по предложенному методу зоны обнаружения Wi-Fi канала представлены на рис. 1.

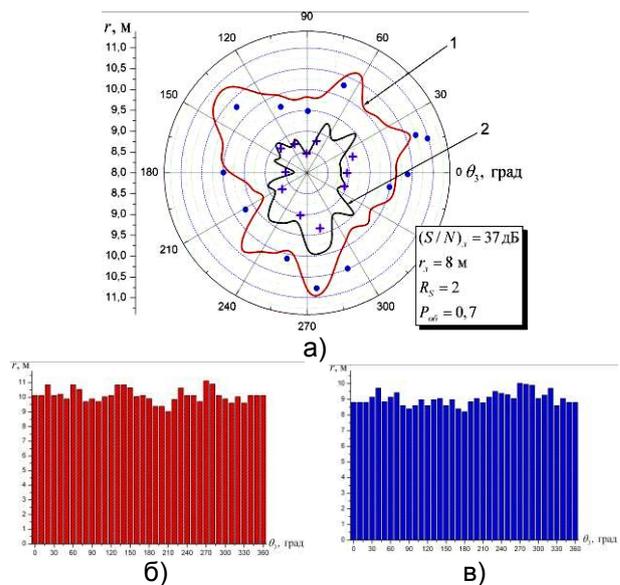


Рис. 1. Зоны обнаружения ЦСПИ для случая помещения и ближней зоны по критерию  $P_{об} = 0,7$ .

Fig. 1. Zone detection of DCS for the case of premises and a near zone as per  $P_{об} = 0,7$

Антенна отводного канала располагалась по отношению к оси легитимного канала так, что на передатчик был направлен либо максимум (кривая 1 на рис. 1, а), либо минимум ее УЗИП (кривая 2 на рис. 1, а). На рис. 1,а указаны значения длины трассы легитимного канала  $r_l$ . Кроме того, было вычислено отношение площадей зон обнаружения при ориентации на передатчик максимума УЗИП антенны отводного канала ( $S_{max}$ ) и ее минимума ( $S_{min}$ ), которое составило  $S_{max}/S_{min}=1,12$ , т.е. площадь ЗО изменяется мало. Площади  $S_{max}$  и  $S_{min}$  определялись интегрированием кривых  $r(\theta_3)$  в прямоугольной системе координат, соответственно рис. 1, б-в.

В силу неравномерности УЗИП граница зоны обнаружения имеет сложную конфигурацию. Достоверность изложенного метода построения зон обнаружения по критерию  $P_{об} = 0,7$  проверялась экспериментально. На рис. 1 точками обозначены результаты измерений  $P_{об}(r, \theta_3)$  при направлении максимума УЗИП антенны отводного канала на передатчик, а крестиками – результаты измерений  $P_{об}(r, \theta_3)$  при направлении на передатчик её минимума. По результатам проведенной экспериментальной проверки можно заключить, что между кривыми постоянной производительности и данными натурального эксперимента наблюдается хорошая согласованность.

### III. Идея нового способа обеспечения безопасной работы легитимного Wi-Fi канала связи

Цель последующих исследований состояла в разработке способа обеспечения безопасной работы легитимного Wi-Fi канала при работе генератора искусственного шума, подавляющего приемник-обнаружитель.

Рассмотрим суть предлагаемого способа (рис. 2). В точках А и В расположены модемы легитимного канала с антеннами, характеризующимися диаграммами направленности ДН1. В этих же точках находится и генераторы искусственного шума снабженные антеннами, у которых диаграмма направленности ДН2 – кардиоида.

При ориентации антенн модемов максимумами ДН1 друг на друга, а антенн генераторов искусственного шума минимумом ДН2 на максимум ДН1, на входах приемников модемов в идеальном случае будет выделяться только информационный сигнал.

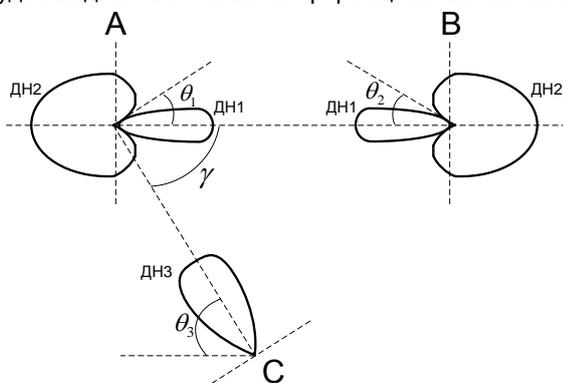


Рис. 2. Схема расположения легитимного и отводного каналов.

Fig. 2. Arrangement of legitimate and outlet channels

Искусственный шум будет воздействовать лишь на вход приемника-обнаружителя, находящегося в точке С. Его антенна имеет диаграмму направленности ДНЗ. При этом условия обнаружения легитимного канала существенно ухудшаются. Покажем это путем расчетов, взяв за основу формулу для  $P_{об}$  известную из [2]:

$$P_{об} = 1 - \frac{1}{1 + 2^{R_s} \cdot \frac{(S/N)_o}{(S/N)_л}} \cdot e^{-\left[ \frac{2^{R_s} - 1}{(S/N)_л} \right]}, \quad (2)$$

где  $(S/N)_o$  – среднее значение сигнал/шум в отводном канале.

В (2) сделаем следующие преобразования:

$$(S/N)_л = \frac{S}{N + J \cdot G_{TJ} \cdot f_{TJ}^2(\theta_1)} \cdot \alpha(r_3/r_l) \times G_{TS} \cdot f_{TS}^2(r_l, \theta_1) \cdot G_{RL} \cdot f_{RL}^2(r_l, \theta_2), \quad (3)$$

$$(S/N)_o = \frac{S}{N + J \cdot G_{TJ} \cdot f_{TJ}^2(\gamma)} \cdot \alpha(r_3/r_o) \times G_{TS} \cdot f_{TS}^2(r_o, \gamma) \cdot G_{RO} \cdot f_{RO}^2(r_o, \theta_3). \quad (4)$$

где  $S$  – мощность передатчика;  $J$  – мощность генератора искусственного шума;  $G_{TJ}$ ,  $G_{TS}$ ,  $G_{RL}$ ,  $G_{RO}$  – коэффициенту усиления антенн передатчика искусственного шума, передатчика сигнала, антенн легитимного и отводного канала соответственно, а  $f_{TJ}$ ,  $f_{TS}$ ,  $f_{RL}$ ,  $f_{RO}$  – их нормированные УЗИП;  $\gamma$  – угол прихода помехи.

Приведем результаты расчета вероятности обнаружения для случая, когда в генераторе шума используется антенна с кардиоидной диаграммой направленности  $f_{TJ} = (1 + \cos(\gamma + \pi))/2$ , а диаграммы антенн модемов и приемника-обнаружителя являются ненаправленными. На рис. 3 (кривая 1) показана зависимость  $P_{об}(\gamma)$  в полярных координатах при мощности передатчика  $S = 100$  мВт и отношении  $J/S = 0,5$ , а  $G_{TJ} = 2$ ,  $G_{TS} = G_{RL} = G_{RO} = 3$ , мощность шума  $N$  рассчитывалась при температуре  $20^\circ \text{C}$ .

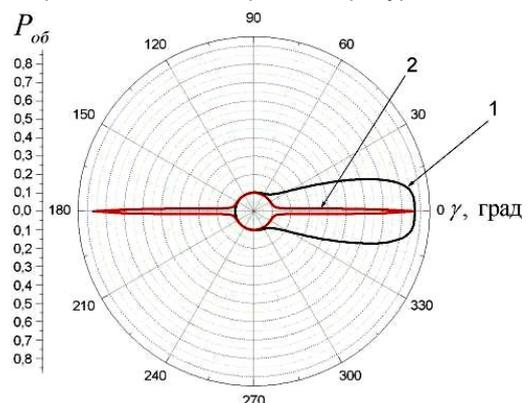


Рис. 3. Зависимость вероятности обнаружения от угла прихода помехи.

Fig. 3. The dependence of the probability of detection of the angle of arrival of noise

Как видно из рис. 3 Wi-Fi канал может быть обнаружен ( $P_{об} > 0,7$ ) только в небольшом секторе углов. Фактически тогда, когда приемник обнаружитель находится на оси легитимного канала. Если базовая станция должна обеспечивать связь с двумя абонентами, то в качестве антенн генератора шума следует

использовать вибраторы с ДН  $\sin \gamma$  (рис. 3. кривая 2). Используя вибраторные антенны с длиной плеч  $> 0,5\lambda$  можно, как известно [3], реализовать ДН с количеством максимумов больше двух, что позволяет обеспечить работу базовой станции под шумом от трех до шести абонентов.

Об эффективности предложенного способа обеспечения безопасной работы легитимного Wi-Fi канала связи можно судить из рассмотрения показанных на рис. 4 зон обнаружения при выключенном (кривая 1) и включенном (кривая 2) генераторе искусственно-го шума.

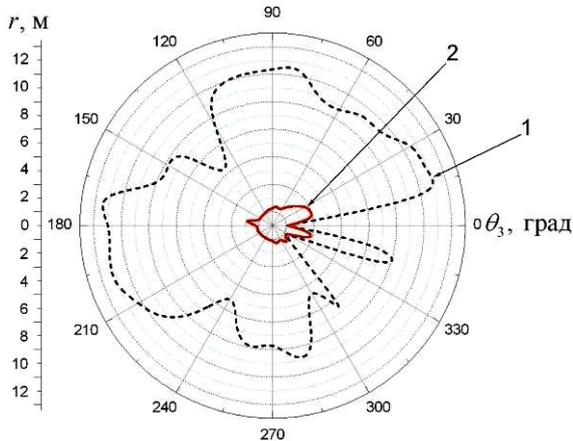


Рис. 4. Зоны обнаружения ЦСПИ для случая открытого пространства и ближней зоны по критерию  $P_{об} = 0,7$ .

Fig. 4. Zone detection DCS for the case of open space and a near zone as per  $P_{об} = 0,7$

Кривая 1 заимствована из [4, стр. 182, рис. 1]. Кривая 2 рассчитывалась при тех же условиях распространения радиоволн, что и кривая 1. Нетрудно видеть, что при работе под искусственным шумом максимальный радиус зоны обнаружения уменьшился более чем в 5 раз. Это обстоятельство существенно упрощает организацию контроля несанкционированного доступа к информации, передаваемой по легитимному каналу. Таким образом, из результатов численных исследований можно заключить, что предложенный способ обеспечения безопасной работы легитимного Wi-Fi канала может быть реализован на практике, если помехозащищенность легитимных приемников будет достаточной.

Об уровне помехозащищенности приемников модемов можно судить по величине вероятности битовой ошибки [5].

$$P_B = 0,5 \cdot Q \left[ \sqrt{\frac{E_b}{J} \cdot \alpha \left( \frac{r_L}{r_S} \right)^n \cdot \frac{G_{TS} \cdot f_{TS}^2(\theta_1) \cdot G_{RL} \cdot f_{RL}^2}{G_{TJ} \cdot f_{TJ}^2(\theta_1)}} \right] \quad (5)$$

где  $Q(x) \approx \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left[-\frac{u^2}{2}\right] du$  – функция ошибок (ин-

теграл вероятности),  $E_b$  – энергия бита,  $\alpha$  – функциональная зависимость затухания сигнала,  $r_S$ ,  $r_L$  – расстояние (разнесение) между передающими и приемными антеннами соответственно данной системы связи и постановщика помех,  $n$  – показатель степени затухания (показатель степени затухания  $n$  указывает, насколько быстро растут потери при распространении с увеличением расстояния).

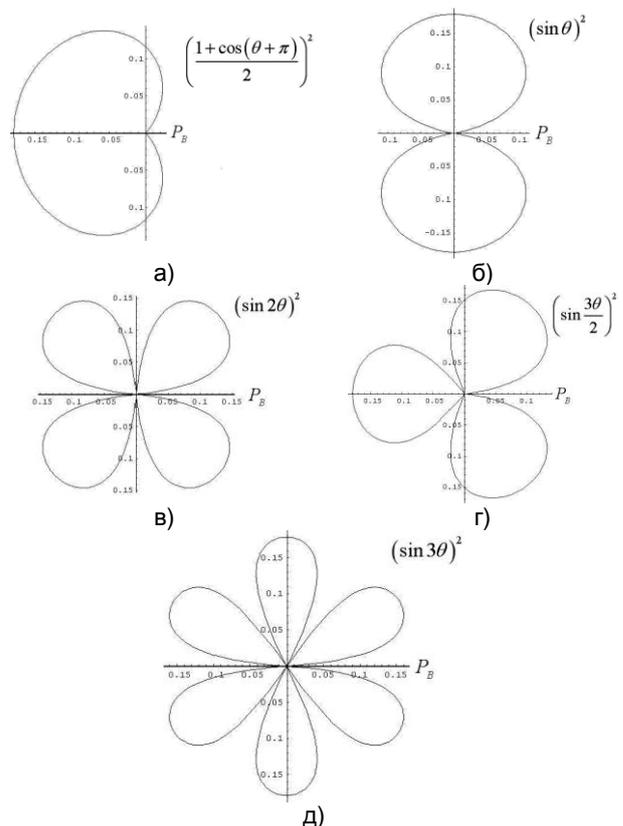


Рис. 5. Зависимость вероятность битовой ошибки от угла для разных типов ДН генератора шума.

Fig. 5. The dependence of the probability of a bit error vs. the angle for different types of RP noise generator

Рядом с графиками показаны формулы, по которым в выражении (5) рассчитывались ДН2 антенн генераторов шума. Значения вероятности битовой ошибки получились неудовлетворительными за исключением небольшого сектора углов в районе  $\theta \approx \pm(2-3)^\circ$  (см. рис. 6, случай  $\sin \theta$ ).

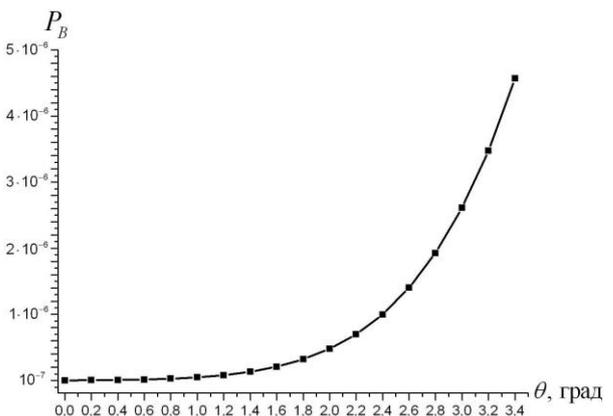


Рис. 6. Зависимость вероятность битовой ошибки от угла для случая применения в генераторе шума ДН  $\sin \theta$ .

Fig. 6. The dependence of the probability of a bit error vs. the angle for the case of the generator noise RP  $\sin \theta$

Высказанная идея проверялась экспериментально. Легитимный канал был построен на основе Wi-Fi модемов нагруженных на антенны «двойной квадрат» (рис.

7). Для излучения «искусственного шума» использовался СВЧ генератор непрерывных сигналов и укороченный вибратор (рис. 7). На рис. 8 показана зависимость уровня сигнала на входе модема легитимного канала. Как следует из результатов эксперимента, выдвинутая идея нашла подтверждение на практике.

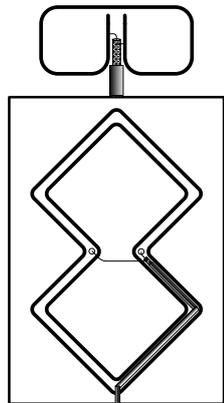


Рис. 7. Вид антенны модема и антенны генератора искусственного шума.

Fig. 7. Type of a modem antenna and an artificial noise generator antenna

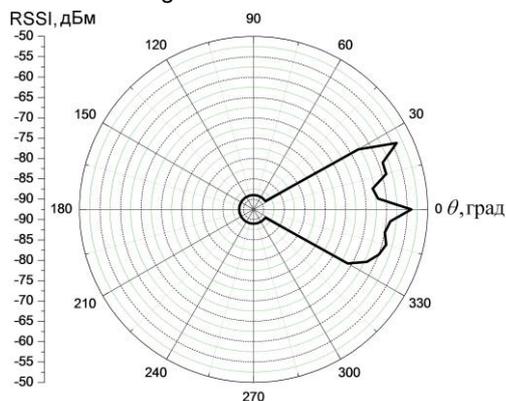


Рис. 8. Уровень сигнала на входе приемника легитимного канала связи.

Fig. 8. The signal level at the receiver input of a legitimate channel of communication

#### IV. Заключение

1. Предложен метод расчета ЗО по критерию  $P_{об} = 0,7$ .
2. Предложен новый способ обеспечения скрытой работы легитимного канала связи под искусственным шумом.

#### V. Список литературы

- [1] Barros J., Rodrigues M.R.D. Secrecy capacity of wireless channels // In: 2006 IEEE International Symposium on Information Theory, IEEE Press, New York. – pp. 356–360.
- [2] Chrysikos T., Dagiuklas T., Kotsopoulos S. A Closed-Form Expression for Outage Secrecy Capacity in Wireless Information-Theoretic Security // Proceedings of Security in Emerging Wireless Communication and Networking Systems (SEWCN'09). – Springer, 2010. – Vol. 42 of Lecture Notes in Computer Science. – pp. 3–12.
- [3] Шифрин Я. С. Антенны. – ВИРТА им. Говорова Л. А., 1976. – С. 239-241. – 408 с.
- [4] 16-й Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке». Сб. материалов форума. Т. 3. - Харьков: ХНУРЭ. 2012. – 220 с.
- [5] Harada H. and Prasad R. Simulation and Software Radio for Mobile Communications, Norwood, MA: Artech House, 2002. – 475 p.

## THEORY AND PRACTICE OF CONSTRUCTION OF STEALTH RAYLEIGH Wi-Fi CHANNELS

Strelnitskiy O. O., Shokalo V. M.  
 Kharkiv National University of Radioelectronics  
 14, Lenina Ave., Kharkiv, 61166, Ukraine  
 Ph.: +38-063-255-02-16, e-mail: stal.sivan@gmail.com

**Abstract** — The report investigates the ways to improve the stealth Wi-Fi Rayleigh channels, the level of which is characterized by a probability of detection  $P_{об}$ . As a result of the work a more advanced model for calculating the value of  $P_{об}$ , the method of calculation of the detection zone and a new way to improve the stealth channel due to its work under artificial noise, are offered.

### I. Introduction

The aim of this work is to improve the models of analysis of multibeam stealth wireless communications of LAN level, experimental verification of the possibility of applying them in practice as well as development on the basis of these models is the method of construction zone limits of detection and a new way of increasing secrecy at the expense of his radio work under artificial noise.

### II, III. Main Part

Based on [1, 2], and introducing a number of approximations, in a report obtained by the following expression for the probability of detection:

$$P_{об} = 1 - \frac{\exp\left[-\frac{2^{R_s} - 1}{(S/N)_a}\right]}{1 + 2^{R_s} \cdot \frac{\alpha_o \cdot F_o^2(r_o, \theta_3) \cdot F_{II}^2(r_o, \theta_1)}{\alpha_a \cdot F_a^2(r_a, \theta_2) \cdot F_{II}^2(r_a, \theta_1)}}$$

Using this expression can construct a detection area of digital communication system (DCS). The results of calculations by the proposed method of detection zone Wi-Fi channels are shown in Fig. 1. The boundary of the detection zone has a complex configuration. The validity of this method of building detection zones is tested experimentally. According to the results of experimental verification it can be concluded that the curves of constant performance and field experiment data are in good accord.

The purpose of the follow-up studies is to develop the ways to ensure safe operation of a legitimate Wi-Fi channel when the generator of artificial noise operates, overwhelming the receiver-detector.

Consider the nature of the proposed method (Fig. 2). At points A and B the legitimate channel modems and antennas, radiation patterns (RP) characterized ДН1 are. In these same points an artificial noise generator is and it is equipped with antennas that have ДН2 pattern - cardioid. When the orientation of antennas of modems ДН1 maximums is at each other, and antennas of artificial noise generators of ДН2 minimum at ДН1 maximum, the receiver input of modems in the ideal case only an information signal will be. The effectiveness of the proposed method of ensuring the safe operation of a legitimate Wi-Fi channel can be seen from consideration in Fig. 4 detection areas with off (curve 1) and activated (curve 2) artificial noise generator. It is easy to see that when working under artificial noise the maximum radius of the detection area decreased for more than 5 times. This greatly simplifies the control of unauthorized access to the data transmitted through legitimate channels. Thus, using the results of numerical studies we can conclude that the proposed method of ensuring the safe operation of a legitimate Wi-Fi channel can be implemented in practice, if the immunity of the legitimate receiver will be sufficient.

### IV. Conclusion

The method for calculating the detection zone by  $P_{об} = 0,7$ . The new way of providing covert operation of a legitimate channel for artificial noise is presented.