



ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056

О МОДЕЛИРОВАНИИ ПРОЦЕССА ОБНАРУЖЕНИЯ ПЕРИОДИЧЕСКИ ИЗЛУЧАЮЩИХ УСТРОЙСТВ

ON THE MODELING OF PROCESS DETECTING THE PERIODIC RADIATING DEVICES

А.Д. Буханцов, И.В. Дружкова
A.D. Bukhantsov, I.V. Druzhkova

*Белгородский государственный национальный исследовательский университет,
Россия, 308015, Белгород, ул. Победы, 85*

Belgorod State National Research University, 85 Pobeda St, Belgorod, 308015, Russia

e-mail: bukhanstov@bsu.edu.ru, 984546@bsu.edu.ru

Аннотация. В статье предлагается подход к моделированию процесса поиска закладных устройств, излучающих сигнал периодически. Приводится выражение для определения числа периодов поиска и суммарного времени обнаружения закладки сканирующим приемником. Модель позволяет выработать рекомендации по снижению времени поиска таких устройств и соответственно повысить вероятность их обнаружения.

Resume. The article offers an approach to modeling of the process of finding embedded devices emitting a signal periodically. An expression for the number of periods and the total search time detection the embedded devices by the scanning receiver. The model allows to develop recommendations to reduce the search time of such devices and thus increase the probability of detection.

Ключевые слова: сканирующий приемник, закладка, моделирование, частотный диапазон, скорость сканирования.

Keywords: scanning receiver, bugging device, modeling, frequency range, scanning speed.

Теоретический анализ

В настоящее время вопросы совершенствования методов поиска несанкционированных радиопередающих и радиозакладных устройств (закладок) являются актуальными ввиду неуклонного возрастания роли информационной безопасности в государственной и обычной сферах деятельности, а также возможностей технических средств разведки. Современные закладки конструктивно отличаются друг от друга, но могут использовать следующие общие методы сокрытия канала передачи данных:

- метод накопления данных с последующей их передачей в течение заданного промежутка времени (до нескольких миллисекунд);
- метод накопления информации с последующей многократной передачей через определенные интервалы времени или после получения внешней команды;
- передача с возможной перестройкой частоты канала;
- использование широкополосных шумоподобных сигналов, когда энергия сигнала сосредоточена в широкой полосе частот и не имеет выраженного превышения над шумами;
- выбор диапазона частот излучения сигнала рядом с сильным источником легитимных сигналов, которые перегружают прием поиска сканирующего устройства при недостаточном диапазоне сканирования;
- маскировка под стандартные каналы связи [Хорев, 2010].

Вышеперечисленные методы не охватывают все возможные принципы маскировки, используемые закладками. Данные методы могут так же и комбинироваться друг с другом.

Какие бы сложные алгоритмы сокрытия канала передачи данных не использовали закладки, они все равно могут обнаружить себя определенной периодичностью передачи данных или использованием ограниченного диапазона частот. Данные признаки обнаруживаются оператором при



временном анализе частотного спектра. Именно частотно-временной периодичностью закладки отличаются от случайного шума, который можно принять за закладку [Ананский, 1999].

При поиске источников излучения такого типа не стоит полагаться на их мгновенное обнаружение. Чтобы найти закладку необходим радиомониторинг в течение длительного времени: до суток или более с последующим анализом всех найденных сигналов в представлении спектрограммы [Хорев, 1998]. Исходя из этого и предъявляются требования к алгоритмам, которые должны быть реализованы в программном обеспечении комплекса.

Одними из основных характеристик сканирующего приемника являются диапазон частот сканирования и скорость сканирования.

Для поиска закладок наиболее часто используется режим автоматического сканирования приемника в заданном диапазоне частот. При этом режиме устанавливаются начальная и конечная частоты сканирования исходя из возможностей сканирующего приемника, шаг перестройки по частоте, вид модуляции и порог чувствительности для обнаружения закладок с низким уровнем сигнала [Кривцун, 2012].

Исследование и его результаты

Введем следующие обозначения для параметров сканирующего приемника (СП) и закладного устройства (ЗУ), представленные в таблице 1.

Таблица 1
Table 1

Расшифровка обозначений
Decoding of notation

Сканирующий приемник	
Диапазон частот, МГц	[a;b]
Шаг сканирования, МГц	h
Скорость сканирования, шагов/с	V
Порог чувствительности приемника, В	s
Количество шагов сканирования	N
Максимальное количество периодов поиска	M
Время прохождения одного периода поиска, с	$t_{рабСП}$
Закладное устройство	
Несущая частота, МГц	f
Ширина полосы, МГц	Δf
Период повтора, с	T
Время работы, с	$t_{рабЗУ}$
Амплитуда излучаемого сигнала, В	U

В ходе исследования моделировалась процедура поиска закладки с возможностью изменения параметров сканирования и закладки. Цель моделирования заключалась в исследовании зависимости времени сканирования приемника (количества периодов поиска) от скорости сканирования в фиксированном диапазоне частот до момента обнаружения закладки с заданными временем и периодом излучения на фиксированной несущей частоте. Упрощенная блок-схема поиска закладки сканирующим приемником представлена на рисунке 1.

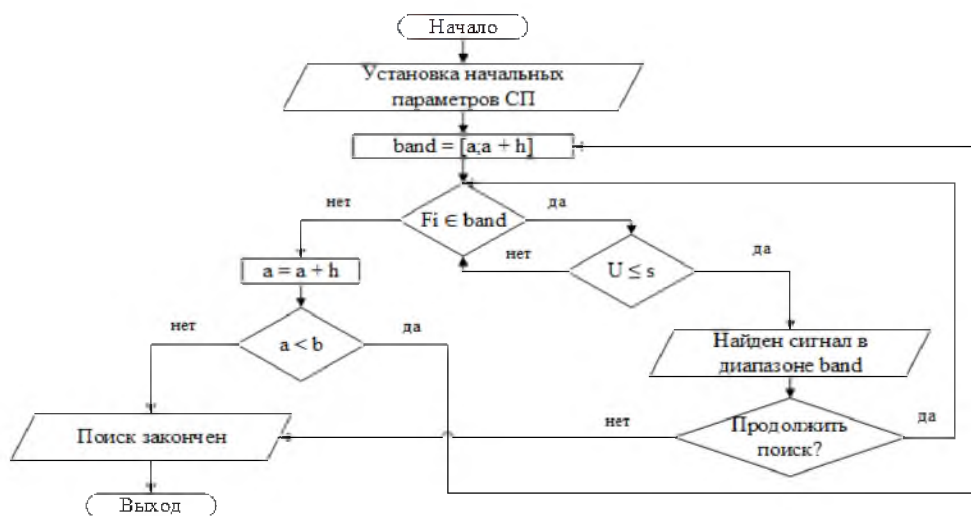


Рис. 1. Упрощенная блок-схема поиска СП
Fig. 1. The simplified block diagram of a search scanning receiver



Исходя из алгоритма поиска можно вывести зависимость для определения суммарного времени (периодов) поиска от параметров сканирующего приемника и закладного устройства.

Задавая диапазон частот от a до b и шаг сканирования h приемника, можно определить количество шагов:

$$N = \frac{b - a}{h} \tag{1}$$

В каждом СП определена скорость сканирования V , которая отражает какое количество шагов будет обработано за 1 с. Следовательно, можно определить время работы СП за один период сканирования:

$$t_{\text{рабСП}} = \frac{N}{V} \tag{2}$$

Зная время работы СП и основные параметры ЗУ, можно найти промежуток времени, при котором СП сможет обработать частотный диапазон излучения ЗУ.

Для начала найдем время, затрачиваемое на обработку одного шага:

$$t_h = \frac{t_{\text{рабСП}}}{N} \tag{3}$$

Далее можно найти нужный интервал времени по следующим формулам:

$$t_1 = t_h \cdot \text{floor} \left(\frac{f - \frac{\Delta f}{2}}{h} \right) \tag{4.1}$$

$$t_2 = t_h \cdot \text{ceil} \left(\frac{f + \frac{\Delta f}{2}}{h} \right) \tag{4.2}$$

Таким образом, для нахождения периода работы СП, при котором будет найдено ЗУ, необходимо найти время синхронизации, то есть тот момент, когда закладка будет включена на частоте, которую будет обрабатывать в это же время СП. Для этого необходимо, изменяя количество периодов работы ЗУ и его ожидания (i), найти период синхронизации, каждый раз находя время начала работы ЗУ ($t_{\text{нач. рабЗУ}}$) относительно начала периода СП:

$$t_{\text{нач. рабЗУ}} = \left[\sum_1^i (t + T) \right] \text{mod} t_{\text{рабСП}}, i = 1, 2, 3, \dots, M \tag{5}$$

Используя формулу 5, необходимо, каждый раз увеличивая i на 1, сравнивать результат, используя следующее выражение:

$$\left[t_{\text{нач. рабЗУ}}; t_{\text{нач. рабЗУ}} + t_{\text{рабЗУ}} \right] \in [t_1; t_2] \tag{6}$$

Как только ЗУ будет работать в этом интервале времени, она будет обнаружена. Тогда чтобы найти время (количество периодов) поиска, используя найденное i , необходимо:

$$T_{\text{поиска}} = \left[\sum_1^i (t + T) \right] \text{div} t_{\text{рабСП}} \tag{7}$$

Данные формулы используются при соблюдении бесперебойной и четкой работы СП и ЗУ.



Параметр i меняется, пока не закончится заданное количество периодов поиска. Если за это время закладка не была обнаружена, то говорят о синхронизации работы ЗУ и СП. Поэтому для обнаружения меняют начальные установки СП.

В таблице 2 приведены параметры экспериментов.

Таблица 2
Table 2

Параметры моделирования
The modeling parameters

№	Диапазон сканирования, МГц	Шаг перестройки частоты, МГц	Скорость сканирования, каналов/с	Время работы закладки, с	Период работы закладки, с	Полоса частот закладки, МГц
1	0 – 1000	1	от 10 до 100	1	5	99.5 – 100.5
2	0 – 1000	1	от 10 до 100	0.5	5	99.5 – 100.5
3	0 – 500	1	от 10 до 100	1	5	99.5 – 100.5
4	0 – 200	1	от 10 до 100	1	5	99.5 – 100.5

Результаты моделирования отражены на рисунках 1-4. В каждом эксперименте скорость сканирования изменялась от 10 до 100 каналов/с. Такими параметрами скорости обладают большинство современных сканирующих устройств.

Эксперименты 1, 3, 4 отличаются по сканируемому диапазону частот, каждый последующий эксперимент уменьшает его относительно полосы частот закладного устройства.

Эксперименты 1, 2 отличаются по времени работы закладки, где время работы во втором случае уменьшено в 2 раза.

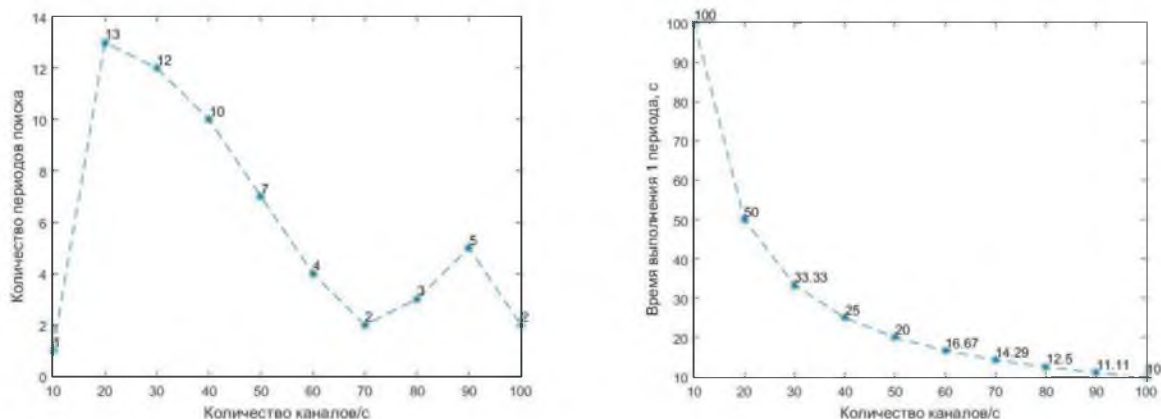


Рис. 1. Графики зависимости количества периодов поиска от скорости сканирования (эксперимент №1)

Fig. 1. The charts showing how the number of search periods depends on the scanning speed (the experiment No1)

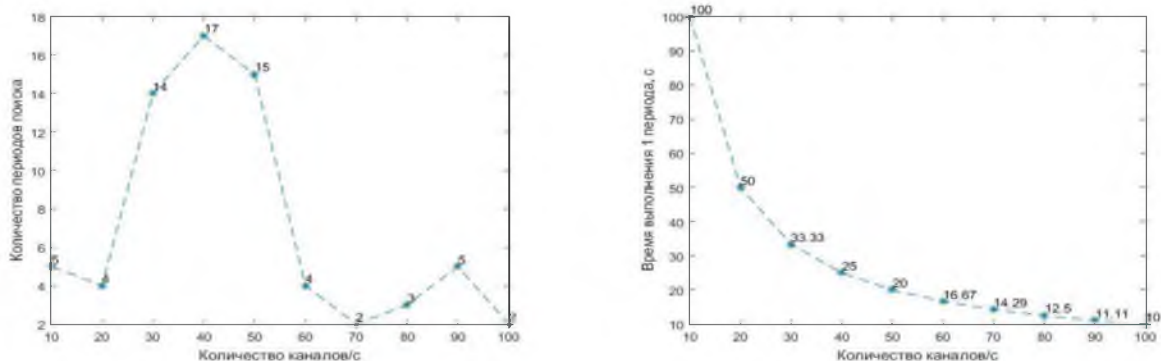


Рис.2. Графики зависимости количества периодов поиска от скорости сканирования (эксперимент №2)

Fig. 2. The charts showing how the number of search periods depends on the scanning speed (the experiment No2)

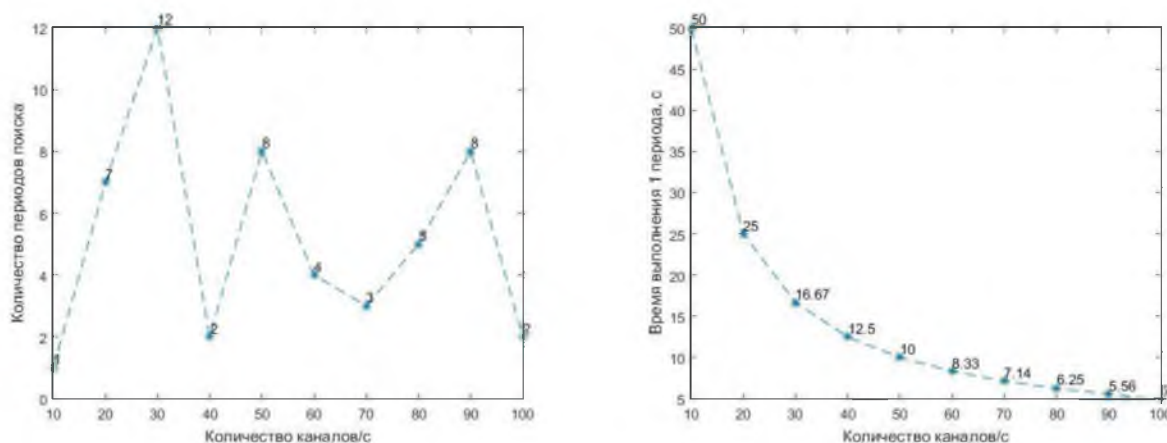


Рис. 3. Графики зависимости количества периодов поиска от скорости сканирования (эксперимент №3)
 Fig. 3. The charts showing how the number of search periods depends on the scanning speed (the experiment №3)

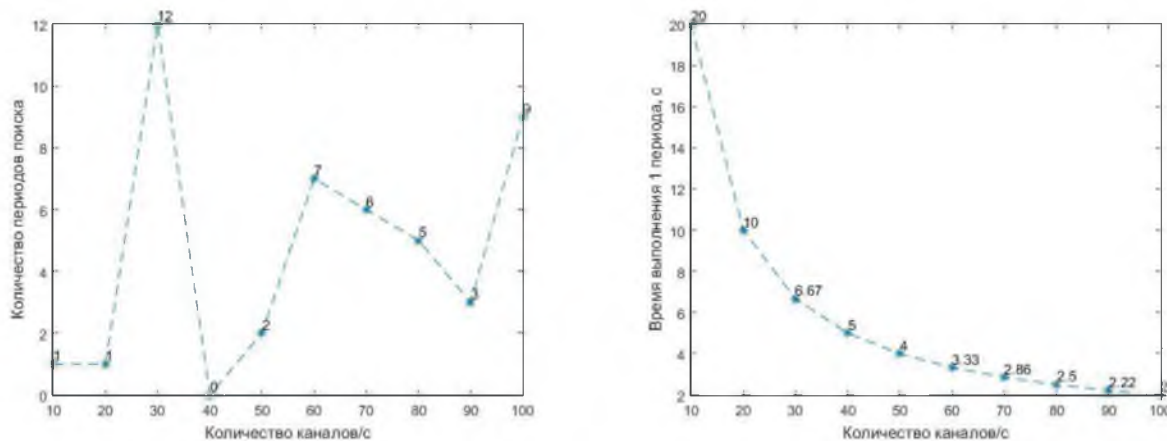


Рис. 4. Графики зависимости количества периодов поиска от скорости сканирования (эксперимент №4)
 Fig. 4. The charts showing how the number of search periods depends on the scanning speed (the experiment №4)

В ходе проведенного исследования по результатам анализа графиков, представленных на рисунках 1 - 4 можно выделить следующие особенности выявления закладок, излучающих сигнал периодически:

- с повышением скорости сканирования частотного диапазона количество периодов поиска (т.е. время сканирования заданного диапазона частот до момента обнаружения закладки) не всегда снижается, что объясняется различным соотношением периодов сканирования и работы закладки, влияющим на общую длительность ее поиска;
- скорость сканирования зависит как от ширины анализируемого диапазона частот, так и от шага перестройки частоты внутри данного диапазона;
- на рисунке 4 при скорости 40 каналов/с наблюдается синхронизация периода поиска приемника и периода работы закладки, которые составляют по 5 с, исходя из чего сканирующее устройство не может "попасть" в период работы закладки, а, следовательно, и не обнаружит данное устройство;
- значения времени поиска закладки до момента ее обнаружения, определяемого по результатам моделирования и вычисляемого согласно выражения (7), в основном сходятся, что подтверждает достоверность работы программной модели и аналитических расчетов и позволяет в дальнейшем использовать модель и полученное выражение для формирования исходных данных к параметрам сканирования частотного диапазона при поиске закладного устройства с конкретными частотно-временными параметрами излучения информационного сигнала.



Выводы

По результатам исследования можно представить следующие выводы и рекомендации по настройке программно-аппаратного оборудования поиска несанкционированных передающих устройств:

1. При поиске закладок, излучающих сигнал периодически, повышение скорости сканирования не обязательно приводит к снижению времени их обнаружения, так как для такой ситуации важным является не столько скорость, сколько число "сканирований" выбранного диапазона до совпадения сканируемой частоты и полосы частот закладки, если в данный момент она излучает.

2. Периодически излучающая закладка может быть совсем не обнаружена, если период ее срабатывания и период сканирования (время одного цикла "проверки" выбранного диапазона) оказываются кратными величинами. Такой вариант напоминает случай синхронизации двух процессов: сканирования и излучения через равные или кратные промежутки времени.

3. Для повышения вероятности выявления "пульсирующих" закладок целесообразно программно организовать возможность автоматической процедуры незначительного изменения заданного диапазона сканирования в большую или меньшую стороны для каждого последующего "прохождения" диапазона, чтобы устранить кратность периодов работы закладки и приемника и тем самым повысить вероятность обнаружения таких устройств.

Таким образом, модель позволяет обоснованно скорректировать программу управления сканирующим приемником или учесть изложенные выше рекомендации при поиске периодически излучающих закладок в "ручном" режиме сканирования для повышения вероятности их обнаружения. Результаты исследования путей повышения вероятности обнаружения сложных сигналов и их источников могут быть полезными не только в сфере информационной безопасности, но и в других смежных приложениях и сферах деятельности, например, в радиолокации [Травин, 2012].

Список литературы

References

- Хорев А.А., 2010. Аналоговые акустические радиозакладки. Спецтехника и связь. 1.
Horev A.A., 2010. Analog acoustic radiobook-marks. *Spectekhnika i svyaz*. [Special equipment and communication] 1. (in Russian)
- Ананский Е.В., 1999. Что такое радиозакладки и как их обнаружить? Служба безопасности. 10.
Ananskij E.V., 1999. What radiobook-marks and how them to find out? *Sluzhba bezopasnosti*. [Security Service] 10. (in Russian)
- Хорев А.А., 1998. Методы и средства поиска электронных устройств перехвата информации. М.: МО РФ, 224.
Horev A.A., 1998. Methods and query of electronic devices of intercept of information facilities. Moscow, MO RF, 224. (in Russian)
- Кривцун А.В., 2012. Радиомониторинг: частотный диапазон. Специальная техника. 4.
Krivcun A.V., 2012. Radiomonitoring: frequency range *Spectekhnika*. [Special equipment] 4. (in Russian)
- Травин Г.А., Горюнов В.В., Суворцев В.И., Перепелкин И.Н., 2012. Пеленгование и распознавание сложных дискретно-кодированных (шумоподобных) сигналов малозаметных РЛС на основе применения компьютерных технологий. *Научные ведомости БелГУ. Сер. История. Политология. Экономика. Информатика*. 13(132): 123-127.
Travin G. A., Goryunov V.V., Surovcev V.I., Perepelkin I.N., 2012. Direction-finding and recognition of the difficult discretely-encoded (noisesimilar) signals barely visible RLS on the basis of application of computer technologies. *Nauchnye vedomosti BelGU. Istoriya. Politologiya. Ehkonomika. Informatika* [Belgorod State University Scientific Bulletin. History. Political science. Economy. Information technologies] 13(132): 123-127. (in Russian)