УДК 621.396.967.2

И.И. ОБОД**,** д-р техн. наук, НТУ "ХПИ" (г. Харьков),
А.А.ТЮРИН*,* НТУ "ХПИ" (г. Харьков)

ПОМЕХОУСТОЙЧИВОСТЬ АДРЕСНОГО ПО ОТВЕТУ МЕТОДА ИДЕНТИФИКАЦИИ ВОЗДУШНЫХ ОБЪЕКТОВ

Приводится исследование помехоустойчивости запросных систем идентификации воздушных объектов, в которых используется сложный сигнал с псевдохаотической последовательностью в качестве ответного сигнала, код которой однозначно определяется пространственным положением воздушного объекта. Показано, что предлагаемый метод построения систем идентификации позволяет повысить как помехоустойчивость, так и помехозащищенность систем идентификации .

Ключевые слова: помехоустойчивость, запросные системы идентификации, воздушный объект, сложный сигнал, псевдохаотическая последовательность, ответный сигнал.

Постановка проблемы и анализ литературы. Информационное обеспечение системы контроля использования воздушного пространства в значительной степени определяется системами идентификации (СИ) воздушных объектов (ВО), к которым относят системы вторичной радиолокации [1, 2] и системы радиолокационного опознавания [3]. Системы идентификации предназначены для решения следующих задач:

- определения координат ВО;
- получения дополнительной полетной информации, необходимой для контроля и управления полетами и наведения ВО;
- идентификации обнаруженных ВО по признаку "свой-чужой";
- диспетчерской идентификации (опознавания) ВО.

Однако принцип построения существующих СИ и система сигналов, которые используются в них, не позволяют их отнести ни к помехоустойчивым ни к помехозащищенным [4, 5]. Действительно, как показано в [5], современные СИ не возможно отнести ни к энергетически скрытным, (за счет использования простых сигналов в качестве сигналов запроса и ответа), ни к помехоустойчивым, (за счет возможности несанкционированного использования самолетных ответчиков (СО) заинтересованной стороной). В [6, 7] рассмотрены некоторые методы повышения помехоустойчивости СИ, основанные на создании синхронных сетей СИ, а также за счет использования специфических особенностей построения запросных СИ. Однако вопросам повышения скрытности работы СИ уделено незначительное внимание. В [8] предложен способ идентификации объектов, который позволяет повысить не только помехоустойчивость СИ, но и помехозащищенность, за счет использования системы сигналов в качестве ответных сигналов (ОС), код псевдослучайной последовательности которых определяется пространственными координатами ВО.

Цель работы – исследование помехоустойчивости адресных по ответу СИ, ОС которых используют сложные сигналы с псевдохаотической последовательностью, код которой однозначно определен пространственным положение ВО.

Основная часть. Рассмотрим метод повышения помехоустойчивости СИ ВО, в канале ответа которых используется сложный сигнал с псевдохаотической последовательностью. В этом случае функционирование канала запроса СИ не изменяется в сравнении с существующими системами. В ответчиках СИ ВО, реализованной по отмеченному принципу, алгоритм обслуживания запросных сигналов (ЗС) изменяется следующим образом. В ответчиках формируется некоторый временной интервал T_a анализа, в течение которого принимаются ЗС. При окончания указанного временного интервала и приеме в течение этого временного интервала хотя бы одного сигнала запроса (СЗ) излучается ОС в который закладывается координаты ответчика, то есть излучается сложный сигнал с псевдохаотической последовательностью, код которой определяется пространственным положением ВО.

Таким образом, реализация этого метода (адресного по ответу) существенным образом снижает интенсивность потока ОС и делает эту интенсивность не зависимой от интенсивности потока ЗС. Действительно, максимальная интенсивность потока ОС в этом методе определяется как $\lambda_{vid} = 1/T_a$. Она не зависит от интенсивности потока ЗС и интенсивности потока имитируемых ЗС. Так как в этом методе обслуживание осуществляется не отдельного ЗС, а всех ЗС на временном интервале анализа, то постановка преднамеренных помех с целью снижения помехоустойчивости СО становиться неуместной, так как нужно создать такую ситуацию при которой невозможно принять ни одного ЗС на интервале анализа. Это вынуждает заинтересованную сторону в переходе к постановке флуктуационных помех, что ведет к значительным энергетическим затратам. Так как ЗС другого запросчика сети (даже несанкционированного запроса заинтересованной стороной) на интервале анализа приводит к формированию ОС, в котором заложенны координаты ответчика, то это приводит к переходу от обслуживания ЗС к обслуживанию сети.

Оценим помехоустойчивость СИ, реализованных на рассматриваемом методе при действии потока ЗС и хаотической импульсной помехи (ХИП). Для этого рассмотрим коэффициент готовности (КГ) СО при действии указанных потоков ЗС и ХИП. В дальнейшем определим вероятность обнаружения ВО по ОС, с учетом КГ СО.

Легко видеть, что при одновременном действии на вход анализатора СО ХИП и потока запросных сигналов (ПЗС) будут наблюдаться следующие неблагоприятные для правильного приема ЗС явления:

– подавление ЗС данной СИ из-за наложения опережающих ЗС соседних СИ и приводящих к искажению принимаемого сигнала;

– подавление ЗС данной СИ из-за наложения опережающих ЗС соседних СИ, излученных по боковым лепесткам;

– высокочастотное подавление импульсов ЗС данной СИ при совпадении по времени импульсов ХИП и ПЗС и неблагоприятных фазовых соотношениях;

– подавление ЗС в результате инерционности схем входных формирователей дешифратора.

Перечисленные ситуации приводят к невозможности правильного приема на временном интервале T_a ЗС. Кроме того, наличие ХИП приводит к ложному образованию ЗС и, при отсутствии действительных сигналов запроса, СО производит ложный ответ.

Произведем определение вероятности этих событий в предположении, что ХИП и ПЗС действует на ЗС данной СИ независимо друг от друга.

Пусть на вход СО поступает ХИП интенсивностью λ_0, ПЗС, требующие излучения ОС, интенсивностью λ_1, и ПЗС, излученные по боковым лепесткам диаграммы направленности (ДН) запросчика, интенсивностью λ_2. При этом предположим, что длительность импульсов потока ХИП и ПЗС одинакова и равна длительности импульсов полезного сигнала τ_0.

Совместное действие ХИП и ПЗС приводит к высокочастотному подавлению отдельных импульсов ХИП и ПЗС при неблагоприятных фазовых соотношениях, в результате чего уменьшается интенсивность ПЗС и ХИП.

Вероятность того, что хотя бы один импульс ХИП совпадет по времени с импульсом ПЗС и подавит его, равна:

$$P_p = \gamma[1 - \exp(-\lambda_0 \tau_0)].$$

С учетом P_p интенсивности потоков λ_1 и λ_2 можно определить как

$$\lambda_1^1 = \lambda_1 (1 - P_p)^n , \qquad \lambda_2^1 = \lambda_2 (1 - P_p)^n .$$

Вероятность того, что хотя бы один ЗС попадет в опережающий интервал и подавит ЗС данной СИ за счет наложения импульсов ПЗС, определяется как

$$P_1 = 1 - \exp(-\lambda_1^1 t_1).$$

Интенсивность потока ложных n-импульсных кодов, образованных их ХИП, можно определить из следующего соотношения:

$$\lambda_l = n\lambda_0^n (\tau_0 - \tau_c)^{n-1},$$

где τ_c – заданная величина селекции импульсов по длительности.

Вероятности того, что хотя бы один ЗС попадет в опережающий интервал и подавит дешифрацию ЗС данной СИ за счет времени приема импульсов ПЗС, излученных по боковым лепесткам ДН запросчика, а также образованных из ХИП, вычисляются соответственно как:

$$P_2^1 = 1 - \exp(-\lambda_2^1 t_2) \qquad \text{и} \qquad P_2^2 = 1 - \exp(-\lambda_l t_1) .$$

Суммарная вероятность подавления ЗС данной СИ за счет времени приема сигналов, излученных по боковым лепесткам ДН антенны запросчика и образованных из ХИП ложных ЗС, определяется как:

$$P_2 = 1 - (1 - P_2^1)(1 - P_2^2) .$$

Вероятность того, что хотя бы один импульс из потока ХИП и ПЗС наложится на импульс ЗС данной СИ и подавит его, составляет

$$P_{10} = \gamma[1 - \exp(-\lambda_c \tau_0)] ,$$

где $\lambda_c = \lambda_0 + \lambda_1^1 + \lambda_2^1$.

С учетом *n*-импульсного ЗС вероятность подавления ЗС составит

$$P_3 = 1 - (1 - P_{10})^n .$$

Вероятность подавления ЗС данной СИ в результате появления на позиции сигнала подавления ложного импульса подавления, образованного из помех, можно записать как:

$$P_4 = (1 - P_p) P_{10} .$$

Вероятность подавления ЗС вследствие инерционности входных формирователей СО P_5 может быть определена по выражению

$$P_5 = 1 - \exp(-\lambda_c \tau_f).$$

Вероятность однократной дешифрации ЗС можно определить как

$$P_a = \prod_{i=1}^{5} (1 - P_i). \qquad (1)$$

Расчеты по выражению (1) представлены на рис. 1 для *n* = 3. Расчеты произведены при $\lambda_0 = 10000,\ 20000,\ 30000$. Как следует из рис. 1, при увеличении интенсивности ПЗС вероятность неискаженного приема ЗС уменьшается и достигает 0,65 при $\lambda_1 = 5000$ и $\lambda_0 = 20000$ и 0,58 при $\lambda_1 = 5000$ и $\lambda_0 = 30000$. Расчеты произведены при $\lambda_2 = 5\lambda_1$.

Вероятность излучения ответа СО, т.е. КГ СО, рассматриваемой СИ, с учетом интервала времени анализа, можно определить из следующего соотношения:

$$P_o = 1 - (1 - P_a)^m . \qquad (2)$$

Расчеты по выражению (2) представлены на рис. 2 для *n* = 3 при *m* = 3. На рис. 3 представлены зависимости вероятности излучения ответа при *n* = 3 и *m* = 7. Как следует из представленных зависимостей, при *m* > 7 КГ СО при рассмотренных интенсивностях потоков ЗС практически составляет единицу, что указывает на высокую помехоустойчивость предложенного способа реализации СИ. Приведенные зависимости указывают на существенную зависимость КГ СО запросных СИ с кодированием только сигналов ответа от *n* и *m*.

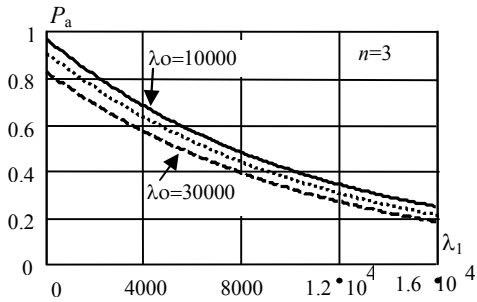

Рис. 1. Вероятность приема СЗ

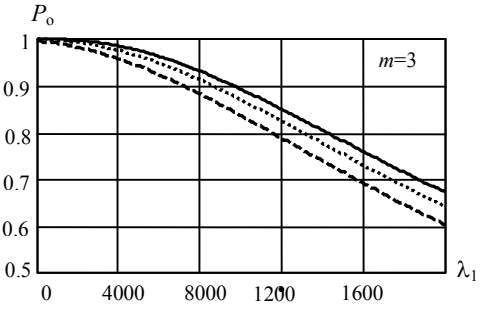

Рис. 2. КГ СО

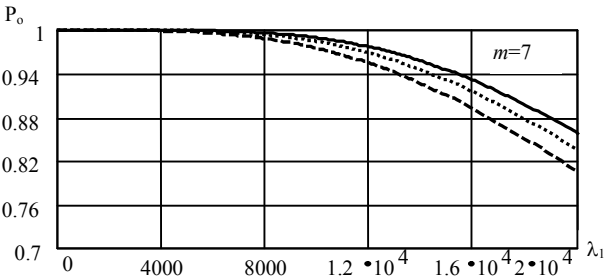

Рис. 3. Коэффициент готовности СО

Вероятность ложного излучения ОС СО, за счет образования ложного ЗС из ХИП и отсутствия на временном интервале T_a действительного ЗС, можно определить из следующего соотношения

$$F = P_{ol}(1 - P_o), \tag{3}$$

где P_{ol} определяется как

$$P_{ol} = 1 - (1 - P_2^2)^m. \tag{4}$$

Расчеты по выражению (3) с учетом (4) для различных n и m представлены на рис. 4. Как следует из приведенных зависимостей, предложенный способ СИ характеризуется приемлемыми вероятностями ложной тревоги. Необходимо отметить, что ложные ответы данного способа приводят к ситуации беззапросного варианта СИ и не влияют на вероятность получения ОС, в частности сигналов идентификации ВО. Приведенные расчеты показали на существенную зависимость вероятности ложной тревоги от n (при увеличении n с 2 до 3 вероятность ложной тревоги снижается на

порядок) и m (при увеличении m с 3 до 7 – снижается с 0,18 до 0,13 при $\lambda_1 = 20000$).

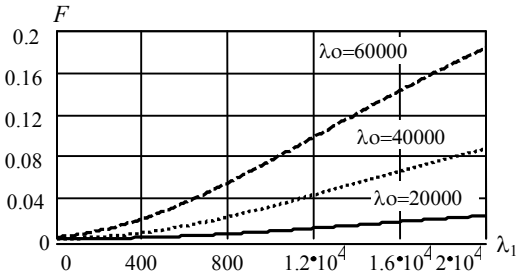

Рис. 4. Вероятность ложной тревоги

Рассмотрим влияние потока ЗС на вероятность обнаружения ВО рассматриваемой СИ. Аппаратура обработки принимаемых ОС запросчика реализует, как правило, алгоритм обнаружения пачки поступающих ОС, заключающийся в обнаружении "k из m" ответных сигналов. Если рассматривать КГ СО постоянным для всей пачки ОС, то вероятность первого обнаружения пачки ОС аппаратурой запросчика можно определить из следующего соотношения

$$P_{ob} = \sum_{i=k}^{m} C_k^m P_o^i (1 - P_o)^{m-i} . \qquad (5)$$

Исходя из того, что за время сканирования антенны запросчика СИ, происходит облучение СО пачкой из N ЗС, то вероятность обнаружения ВО СИ может быть определена из следующего соотношения

$$P_c = \sum_{j=m}^{N} C_m^N P_{ob}^j (1 - P_{ob})^{N-j} . \qquad (6)$$

Подставляя (5) в (6) окончательно получаем выражение для оценки вероятности обнаружения ВО рассматриваемой СИ

$$P_c = \sum_{j=m}^{N} C_m^N \left[\sum_{i=k}^{m} C_k^m P_o^i (1 - P_o)^{m-i} \right]^j \left[1 - \sum_{i=k}^{m} C_k^m P_o^i (1 - P_o)^{m-i} \right]^{N-j} . \qquad (7)$$

Расчеты по выражению (7) с учетом вышеизложенного приведены на рис. 5 и 6. На рис. 5 и 6 представлены зависимости вероятности обнаружения ВО при действии потока ЗС при n = 2, m = 3, 5, 7, N = 10 и 20 и k/m = 4/4. Как следует из представленных зависимостей, при m > 7 наблюдается достаточно высокая вероятность обнаружения ВО рассматриваемой СИ.

Как следует из рис. 5 и 6 помехоустойчивость предложенного способа реализации СИ значительно превосходит помехоустойчивость существующих запросных СИ [4], что указывает на высокую его эффективность.

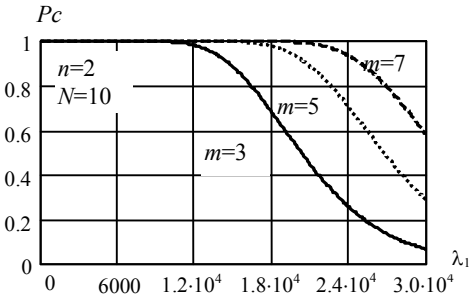

Рис.5. Вероятность обнаружения ВО

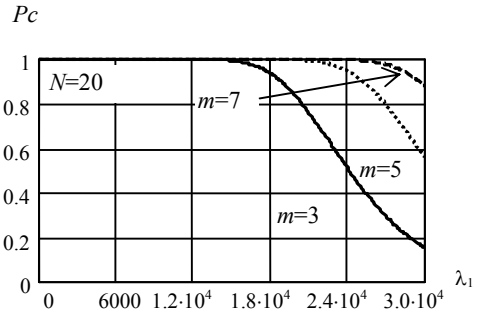

Рис. 6. Вероятность обнаружения ВО

Выводы. Вышеизложенное позволяет утверждать, что создание адресных по ответу СИ на основе формирования ответного сигнала в виде сложного сигнала с псевдохаотической последовательностью, код которой однозначно определяется пространственным положением ВО, позволит существенным образом повысить помехоустойчивость систем идентификации воздушных объектов.

Список литературы: 1. *AAP-28(B)* NATO Glossary of Identification. – NATO Standardization Agency, 2002. **2.** *Давыдов П.С., Сосновский А.А., Хаймович И.А.* Авиационная радиолокация: Справочник. – М.: Транспорт, 1984. – 224 с. **3.** *Маляренко А.С.* Системы вторичной радиолокации для управления воздушным движением и государственного радиолокационного опознавания: Справочник. – Харьков: ХУПС, 2007. – 78 с. **4.** *Обод И.И.* Помехоустойчивые системы вторичной радиолокации: – М.: ЦНТИ, 1998. – 119 с. **5.** *Обод И.И., Тюрин А.А., Яровая А.В.* Сравнительный анализ существующих систем идентификации воздушных объектов // Системи управління, навігації та зв'язку: Збірник наукових праць. – Вип. 2 (6). – К.: ЦНДІ НіУ, 2008. – С. 21-25.

6. Теоретичні основи побудови завадозахищених систем інформаційного моніторингу повітряного простору / *В.В. Ткачев, Ю.Г. Даник, С.А. Жуков, І.І. Обод, І.О. Романенко.* – К.: МОУ, 2004. – 271 с. **7.** Комплексне інформаційне забезпечення систем управління польотами авіації та протиповітряної оборони / *В.В. Ткачев, Ю.Г. Даник, С.А. Жуков, І.І. Обод, І.О. Романенко.* – К.: МОУ, 2004. – 342 с. **8.** *Обод І.І., Тюрін О.О.* Спосіб ідентифікації об'єктів. Патент на корисну модель № 32641 від 26.05.2008.

УДК 621.396.967.2

Перешкодостійкість адресного по відповіді методу ідентифікації повітряних об'єктів / Обод І.І., Тюрін А.А. // Вісник НТУ "ХПІ". Тематичний випуск: Інформатика і моделювання. – Харків: НТУ "ХПІ". – 2008. – № 49. – С. 126 – 133.

Наводиться дослідження перешкодостійкості запитних систем ідентифікації повітряних об'єктів, в яких використовується складний сигнал з псевдохаотичной послідовністю, як у відповідь сигнал, код якої однозначно визначається просторовим положенням повітряного об'єкту. Показано, що запропанований метод побудови систем ідентифікації дозволяє підвищити як перешкодостійкість, так і перешкодозахищеність систем ідентифікації. Іл.: 6. Бібліогр.: 8 назв.

Ключові слова: перешкодостійкість, запитні системи ідентифікації, повітряний об'єкт, складний сигнал, псевдохаотична послідовність, відповідний сигнал.

UDC 621.396.967.2

Antijammingness of address on answer method of authentication of air objects / Obod I.I., Tyurin A.A. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modeling. – NTU "KhPI". – 2008. – № 49. – P. 126 – 133.

Research over of noise-immunity of the air objects authentication query systems, in which a difficult signal is used with a pseudo-chaotic sequence as a backward signal, the code of which is simply determined spatial position of air object, is brought. It is rotined that the offered method of construction of the systems of authentication allows to promote both antijammingness and noise immunity of the authentication systems. Figs: 6. Refs: 8 titles.

Keywords: noise-immunity, authentication query systems, air object, difficult signal, pseudo-chaotic sequence, backward signal.

Поступила в редакцию 05.10.2008