6. *Евдокимова Е.О.* Пространственно-доплеровский алгоритм слежения за рельефом. Материалы международной научно-технической и научно-методической конференции «Проблемы современной системотехники». – Таганрог: Изд-во ТТИ ЮФУ, 2009. – 4 с.
7. *Евдокимова Е.О.* Алгоритм слежения за рельефом местности с использованием пространственно-временной обработки. Материалы международной научной конференции «Методы и алгоритмы принятия эффективных решений». – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 5.
8. *Евдокимова Е.О.* Пространственно-доплеровский алгоритм слежения за рельефом. Материалы международной научно-технической и научно-методической конференции «Проблемы современной системотехники». – Таганрог: Изд-во ТТИ ЮФУ, 2009. – С. 4.

Статью рекомендовал к опубликованию д.т.н., профессор Н.Е. Галушкин.

Евдокимова Екатерина Олеговна
Технологический институт федерального государственного автономного образовательного учреждения высшего профессионального образования «Южный федеральный университет» в г. Таганроге.
E-mail: chandy@inbox.ru.
347930, г. Таганрог, ул. Кузнечная, 142, кв. 9.
Тел.: +79515074544.
Кафедра теоретических основ радиотехники; аспирант.

Yevdokimova Katerina Olegovna
Taganrog Institute of Technology – Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education “Southern Federal University”.
E-mail: chandy@inbox.ru.
9, 142, Kuznechnaya Street, Taganrog, 347930, Russia.
Phone: +79515074544.
The Department of Fundamentals of Radio Engineering; Postgraduate Student.

УДК 621.391.1

Е.В. Апанасов, А.Г. Прыгунов, В.В. Слесарев

ПРИМЕНЕНИЕ СПОСОБА ФОРМИРОВАНИЯ И ПРИЁМА СЛУЖЕБНОЙ ИНФОРМАЦИИ ДЛЯ ПОВЫШЕНИЯ ПОМЕХОЗАЩИЩЁННОСТИ СИСТЕМ РАДИОСВЯЗИ В УСЛОВИЯХ «ИНФОРМАЦИОННОЙ ВОЙНЫ»

Задача обеспечения помехозащищённости и безопасности передаваемой информации в системах радиосвязи в настоящее время решается на этапе ведения связи, в то время как на этапе передачи служебной информации аппаратура подвержена воздействию преднамеренных помех. Целью предлагаемого способа является повышение помехозащищённости систем радиосвязи в условиях «информационной войны».

«Информационная война»; системы радиосвязи; служебная информация; нелинейные последовательности; оптимальный приём.

E.V. Apanasov, A.G. Prigunov, V.V. Slesarev

APPLICATION OF A WAY OF FORMATION AND RECEPTION OF THE OFFICE INFORMATION FOR NOISE IMMUNITY INCREASE RADIO COMMUNICATION SYSTEMS IN CONDITIONS OF “INFORMATION WAR”

The problem of maintenance of noise immunity and safety of transfer information in radio communication systems dares now at a stage of conducting communication while at a stage of transfer of the office information the equipment is subject to influence of deliberate hindrances. The purpose of an offered way is increase immunity increase radio communication systems in conditions of "information war».

«Information war»; radio communication systems; the office information; nonlinear sequences; optimum reception.

При передаче служебно-технологических команд (СТК) (сигналы синхронизации, маршрутизации и др.) в аппаратуре радиосвязи для передачи конфиденциальной информации используются детерминированные режимы формирования и структуры используемых последовательностей с низкой линейной сложностью, что позволяет информационному противнику разведать их структуру, определить тип используемой аппаратуры и другие разведпризнаки. Это позволяет криптоаналитикам, перехватив некоторое количество смежных элементов такой последовательности, применяя известные криптоалгоритмы сгенерировать такую же с целью постановки помех или ввода ложной информации [1-4].

Для обеспечения требуемой безопасности информации и помехозащищённости в условиях «информационной войны» необходимо разработать способ позволяющий увеличить линейную сложность применяемых последовательностей и скрыть сам факт передачи СТК.

Пусть псевдослучайная последовательность на передаче формируется в соответствии с алгоритмом Джеффе (рис. 1) [5]. В структуре генератора имеются три линейных рекуррентных регистра (ЛРР) и нелинейный узел усложнения (НУУ).

Формирование выходного элемента псевдослучайной последовательности (ПСП) будет осуществляться в соответствии с нелинейной функцией

$$Y(x_1, x_2, x_3) = x_1 x_2 + \overline{x}_2 x_3, \tag{1}$$

где x_1, x_2, x_3 – значения заданных элементов ПСП.

Выходной элемент формируется в соответствии с функцией нелинейного преобразования трех значений ЛРР (x_1, x_2, x_3), поступающих с выводов (l, m, r).

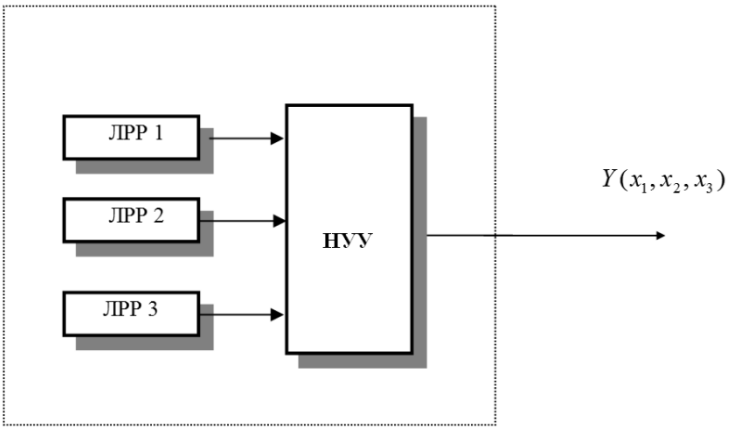

Рис. 1. Структурная схема генератора ПСП по алгоритму Джеффе

При передаче по каналу связи сигнал претерпевает изменения, например, под воздействием шумов и помех. На входе устройства обработки наблюдается смесь

$$\xi_{ij} = S(F(\overline{X}_{(lmr)ij}) + n_{ij}, \tag{2}$$

где S – целевая функция, определяемая законом модуляции; $F(\overline{X}_{(lmr)ij})$ – функция нелинейного преобразования аналоговых величин; n_{ij} – отсчеты флуктуационной гауссовской помехи.

Итак, задачу оптимального приёма и последовательной обработки СТК [1,2] можно сформулировать так: по наблюдаемым ДО принимаемой ПСП ξ_{ij} требуется осуществить обнаружение факта наличия приёма СТК и получить текущую оценку вектора состояния $\overline{X}'_{(lmr)ij}$.

Для решения задачи необходимо перейти от представления логических операций с дискретными значениями к соответствующим им арифметическим с аналоговыми значениями. О возможности такого преобразования указано в некоторых источниках, например в [1, 2].

Используя предложенный алгоритм, получим уравнения вектора состояния для моментов времени t_{ij}, лежащих внутри тактовых интервалов (ТИ), т.е. уравнения дискретизированных отсчётов (ДО):

$$x'_{lij} = K_1 x'_{li(j-1)} + K_2 \frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{li(j-1)}} \times$$
$$\times (\xi_{ij} - F(x'_{ni(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})); \quad (3)$$

$$x'_{mij} = K_1 x'_{mi(j-1)} + K_2 \frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{mi(j-1)}} \times$$
$$\times (\xi_{ij} - F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})); \quad (4)$$

$$x'_{rij} = K_1 x'_{ri(j-1)} + K_2 \frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{ri(j-1)}} \times$$
$$\times (\xi_{ij} - F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})), \quad (5)$$

где $x'_{lmri(j-1)}$ – аналоговые начальные условия для оценки внутри ТИ первого *d*, второго *r* и третьего *z* заданных элементов ОП на предыдущем $(j-1)$-м ДО; *K1 и K2* – нормировочные коэффициенты, *K1* – определяет степень доверия к откорректированным начальным условиям с каждым тактом он увеличивается так как увеличивается степень доверия к этим значениям ДО, *K2* – определяет степень доверия к оценочному значению принятому из канала связи и с каждым тактом он уменьшается, величина коэффициентов выбирается из области 0 и 1 в дробных значениях; ξ_{ij} – наблюдаемая смесь; $F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})$ – аналоговое значение нелинейной функции преобразования от заданных элементов ОП на $(j-1)$-м ДО; $\frac{\partial F(x'_{li(j-1)}, x'_{mi(j-1)}, x'_{ri(j-1)})}{\partial x'_{lmri(j-1)}}$ – значения частных производных функции *F* по соответствующим компонентам *l, m, r*

Тогда уравнения оценивания для моментов времени t_{ij}, соответствующих границам ТИ, будут иметь вид

$$x'_{lij} = x'_{l(i-1)j} + K\frac{\partial F(x'_{l(i-1)j}, x'_{m(i-1)j}, x'_{r(i-1)j})}{\partial x'_{l(i-1)j}} \times$$
$$\times(\xi_{ij} - F(x'_{l(i-1)j}, x'_{m(i-1)j}, x'_{r(i-1)j})), \quad (6)$$

где $x'_{lmr(i-1)j}$ – аналоговые начальные условия для оценки на границах ТИ первого n, второго m и третьего r заданных элементов ОП, взятые на предыдущем $(i-1)$-м ТИ; $F(x'_{l(i-1)j}, x'_{m(i-1)j}, x'_{r(i-1)j})$ – аналоговое значение нелинейной функции преобразования от заданных элементов ОП на $(i-1)$-м ТИ; $\frac{\partial F(x'_{l(i-1)j}, x'_{m(i-1)j}, x'_{r(i-1)j})}{\partial x'_{lmr(i-1)j}}$ – значения частных производных функции $\boldsymbol{G}$ по соответствующим компонентам *l, m, r* на $(i-1)$-м ТИ.

Необходимо отметить, что аналоговые величины принимаются из области определения $x'_1, x'_2, x'_3 \in [0,1]$, а правило квантования, в рассматриваемом примере, имеет вид

$$F(x'_1, x'_2, x'_3) = \begin{cases} 1, \text{ если } F(x'_1, x'_2, x'_3) > 0{,}5 \\ 0, \text{ если } F(x'_1, x'_2, x'_3) \le 0{,}5. \end{cases} \quad (7)$$

Установление верного приёма фиксируется по правилу

$$\sum_{i=1}^{n}(x'_{lmr} + x_{lmr}) \bmod 2 \ge 0 \begin{cases} 0, \text{ приём СТК} \\ >0, \text{ нет приёма СТК} \end{cases}, \quad (8)$$

т.е. СТК считается верно принятой и соответствует переданной, если наблюдается совпадение состояний значений начальных условий и оценочных значений на протяжении n тактов обработки.

Сущность предлагаемого способа заключается в том, что оценка очередного элемента СТК производится в аналоговом виде с учётом предсказанного значения, сформированного на основе рекуррентных свойств ПСП.

На рис. 2,а представлены выходные элементы ПСП, формируемой в соответствии с алгоритмом Джеффе и передаваемой по каналу связи. На приеме из принимаемой смеси (рис. 2,б) выделяют тактовую частоту F_t (рис. 2,в), с частотой в *k* раз, превышающей тактовую на рис. 2,г. Для минимизации искажений принимаемый сигнал не квантуют на два уровня, а дискретизируют с частотой f_d (рис. 2,д). После дискретизации каждый ДО корректируется.

Различают обработку при смене ТИ информационного сигнала и внутри ТИ. В моменты смены ТИ на первом ДО ПСП формируют откорректированные значения заданных элементов опорной последовательности (ОП), т.е. начальные условия. В качестве значений заданных элементов ОП для первоначальной обработки могут быть использованы произвольные ненулевые значения элементов ОП (рис. 2,е). Корректировка осуществляется одновременно в трех заданных значениях, участвовавших в формировании выходного элемента ПСП. После этого откорректированные значения заданных элементов ОП, полученные на первом ДО СТК,

задерживают на время τ, равное длительности одного ДО. Далее осуществляется корректировка заданных значений элементов последовательности на последующих, вплоть до *k*-го ДО – формулы (3-5). Откорректированное значение на *k*-м т.е. последнем ДО принимают за откорректированное значение элемента в целом (ТИ) и используют в качестве начальных условий для корректировки последующего элемента, на границах ТИ используют вычисления по формуле (6).

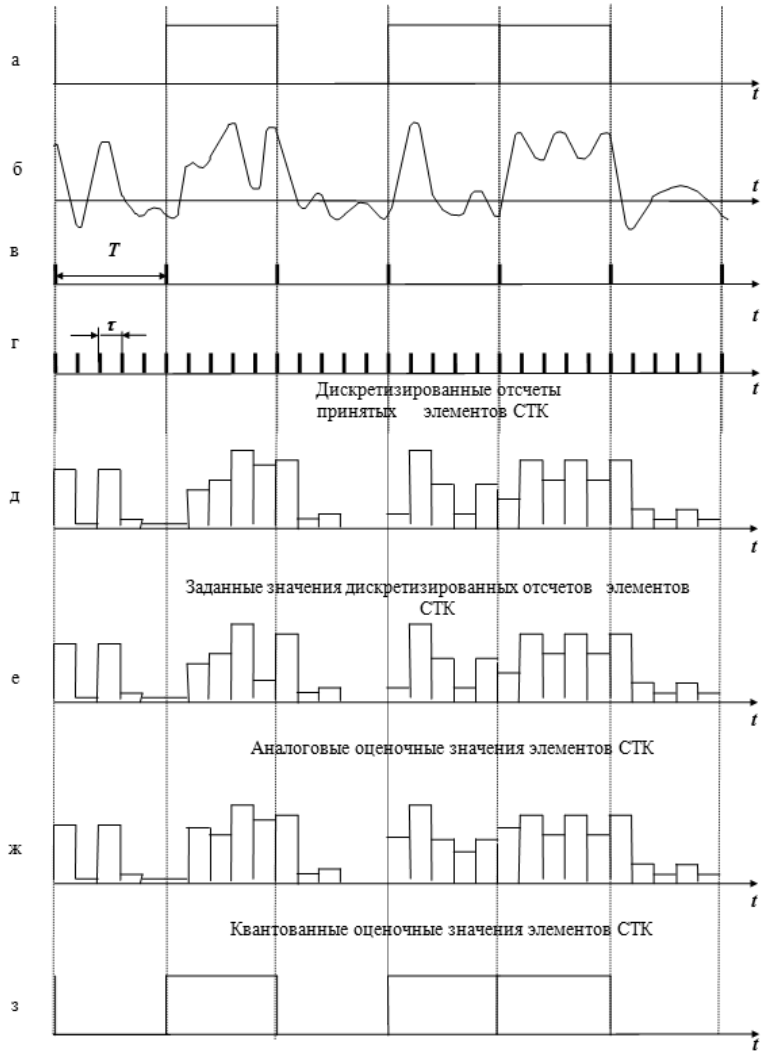

Рис. 2. Графики, поясняющие сущность способа оптимального приёма СТК

Аналогично первой ветви осуществляется корректировка во второй и третьей ветвях обработки (рис. 2,ж). После корректировки производится квантования сигнала согласно (7) (рис. 2,з). Таким образом, формируется СТК, в точности аналогичная с передаваемой. Кроме того, получение откорректированных значений сигнала, с учётом принимаемых предсказанных не прекращается и производится непрерывно с целью получения предсказанных значений сигнала для сокращения времени при повторном приёме.

Отличие предложенного способа от известных заключается в том, что не требуется многократная передача последовательности СТК по каналу связи с последующей мажоритарной обработкой на приёме. Проведение имитационных исследований подтверждает возможность повышения помехозащищённости систем радиосвязи в условиях «информационной войны».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Апанасов Е.В., Прыгунов А.Г.* Способ и устройство синхронизации псевдослучайных последовательностей для повышения безопасности связи // Вопросы защиты информации. – 2005. – № 1 (68). – С. 27-29.
2. *Баранов А.П., Борисенко Н.П., Зежда П.Д.* Математические основы информационной безопасности. – Орёл: ВИПС, 1997. – 354 с.
3. Введение в криптографию / Под общ. ред. В.В. Ященко. – М.: МЦНМО, "ЧеРо", 1998. – 272 с.
4. *Диффи У., Хеллман М.Э.* Защищённость и имитостойкость. Введение в криптографию. ТИИЭР, 1979. – Т. 67, № 3. – С. 71-109.
5. *Уорд Р.* Различение псевдослучайных сигналов методами последовательной оценки // Зарубежная радиоэлектроника. – 1966. – № 8.

Статью рекомендовали к опубликованию: к.т.н., доцент В. Калюка; к.т.н., доцент А. Онышко.

Апанасов Евгений Викторович
Филиал военной академии связию (г. Новочеркасск).
E-mail: apanev1@ yandex.ru.
г. Новочеркасск, ул. Щорса, 18.
Тел.: 88635279427; 88635222763; +79045084127.
К.т.н.; доцент.

Слесарев Владимир Владимирович
г. Новочеркасск, ул. Калинина, 45, кв. 47.
Тел.: +79198734708.
Лаборатория радиосвязи; инженер.

Прыгунов Александр Германович
Ростовский военный институт РВ.
E-mail: apanev1@ yandex.ru.
г. Ростов-на-Дону, пр. Малиновского, д. 38/29, кв. 68.
Тел.: 88632450239; 88632284861.
Кафедра связи; к.т.н.; доцент.

Apanasov Evgenie Viktorovich
Branch of Military Academy of Communication (Novocherkassk).
E-mail: apanev1@ yandex.ru.
18, ShChorsa Street, Novocherkassk, Russia.
Phone: +78635279427; +78635222763; +79045084127.
Cand. of Eng. Sc.; Associate Professor.

Slesarev Vladimir Vladimirovich
45, sq. 47, Kalinin Street, Novocherkassk, Russia.
Phhone: +79198734708.
Laboratory of a Radio Communication; Engineer.

Prigunov Alexander Germanovich
The Rostov Military Institute RV.
E-mail: apanev1@ yandex.ru.
38/29, sq. 68 Avenue of Malinovsky, Rostov-on-Don; Russia.
Phone: +78632450239; +78632284861.
The Department of Communication; Cand. of Eng. Sc.; Associate Professor.