УДК 621.391

К.С. Васюта, С.А. Щербинин

Харьковский университет Воздушных Сил имени Ивана Кожедуба, Харьков

МЕТОД ПОВЫШЕНИЯ СКРЫТНОСТИ СИСТЕМЫ ПЕРЕДАЧИ БИНАРНЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ МАНИПУЛЯЦИИ ПАРАМЕТРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ИМЕЮЩИХ АЛЬФА-СТАБИЛЬНЫЕ РАСПРЕДЕЛЕНИЯ

Для скрытия факта передачи и хранения бинарной информации в инфокоммуникационных системах предложено использовать сложные сигналы, фрагменты которых представляют случайные процессы с альфа-стабильными распределениями и разными параметрами показателя экспоненциальной характеристики стационарности. Показано, что данный вид сигналов при визуальном, время-частотном и нелинейном анализе не отличим от шума наблюдения. Приведен алгоритм внесения бинарного сообщения в случайный процесс и его восстановления на фоне белого шума. Проанализировано качество восстановления сообщения при различных отношениях сигнал/шум на входе приемника.

Ключевые слова: *скрытность, бинарное сообщение, ошибка восстановления, α-стабильные распределения.*

Введение

В настоящее время, когда наличие той или иной информации играет важнейшую роль в сфере экономической и политической жизни общества, в дело вступают технологии промышленного шпионажа. Государственные и коммерческие организации размышляют не только над тем, как наиболее надежно сохранить передаваемую информацию, но и о том, как эту информацию незаметно передать, поэтому скрытность процесса передачи информации выходит на первое место. Скрытию факта наличия или передачи информации посвящены методы стеганографии.

Поскольку скрытность системы связи на прямую зависит от ширены спектра сигнала и от его базы [1] то перспективными разработками в сфере хранения и передачи информации, по мнению авторов, должны стать сложные сигналы на основе случайных процессов, что обладают рядом преимуществ над детерминированными сигналами.

Целью данной работы является синтез метода повышения скрытности передачи цифровой информации в инфокоммуникационных системах, основанного на кодирование бинарной информации последовательностями альфа-стабильных распределений с разными показателями экспоненциальной характеристики стационарности.

Результаты исследований

Проанализируем принцип функционирования любой инфокоммуникационной системы приема-передачи информации. Как правило, она состоит из двух отдельных, но взаимно функционирующих трактов. Это передающий тракт (передатчик) и приемный тракт (приемник), рис. 1.

Передатчик детерминированных сигналов с точки зрения скрытности информации от радиотехнической разведки (несанкционированного доступа) вносит ряд параметров, которые понижают скрытность системы передачи информации в целом. Все эти методы основаны на усложнении формы гармонической несущей, которая легко выявляется методами нелинейного анализа в силу своей регулярности [2].

Исходя из этого, ниже предлагается использовать в качестве переносчика бинарной информации

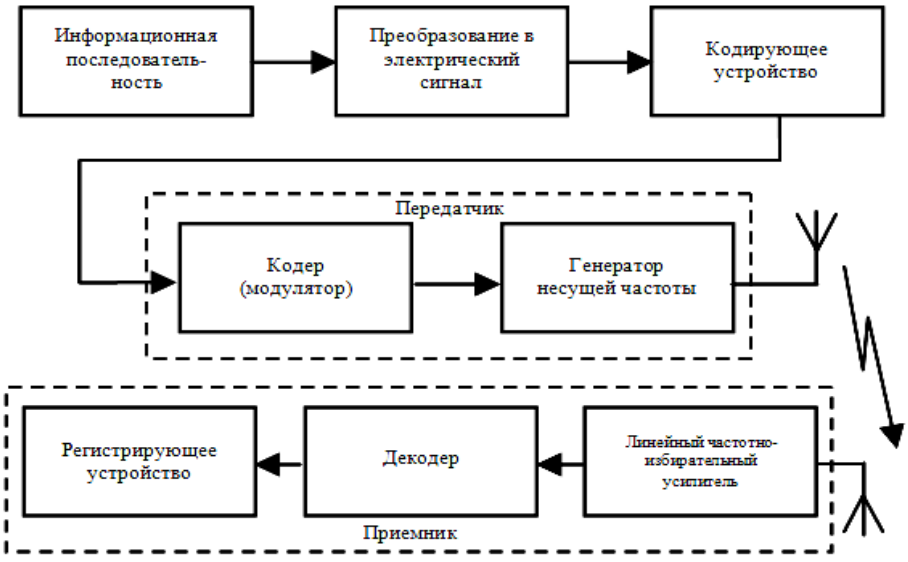


Рис. 1. Обобщенная схема телекоммуникационной системы приема-передачи информации

сложный случайный сигнал из семейства альфа-стабильных распределений. Который имеет ряд преимуществ над детерминированными сигналами. К ним можно отнести бесконечную ширину спектра (зависит только лишь от каскадов фильтров, которые имеют место в передающем тракте), отсутствие несущей частоты, сложную структуру аттрактора на выходе передатчика и схожесть работы средств связи с формирователями помех.

Анализ свойств альфа стабильных распределений

Характеристическая функция альфа-стабильных распределений описывается следующим выражением [3]:

$$\Phi(t)=\begin{cases} e^{i\delta t-|\delta t|^{\alpha}(1-i\beta\frac{t}{|t|}tg\frac{\pi\alpha}{2})}, & \alpha\neq 1 \\ e^{i\delta t-|\delta t|(1-i\beta\frac{2t}{\pi|t|}\ln|t|)}, & \alpha=1 \end{cases},$$

где α – экспоненциальная характеристика стационарности ($0<\alpha\le 2$);

β – коэффициент симметрии $(-1\le\beta\le 1)$,

δ – параметр положения.

Однако моделирование данной системы уравнений в реальном масштабе времени сложно реализовать программным методом. Поэтому для генерации случайных величин с α -стабильным распределением был выбран более простой метод [3]:

для $\alpha\neq 1$

$$\xi=S_{\alpha,\beta}\frac{\sin\{\alpha(V+B_{\alpha,\beta})\}}{\{\cos(V)\}^{1/\alpha}}\left[\frac{\cos\{V-\alpha(V+B_{\alpha,\beta})\}}{W}\right]^{(1-\alpha)/\alpha}$$

где $S_{\alpha,\beta}=\left\{1+\beta^2\tan^2\left(\frac{\pi\alpha}{2}\right)\right\}^{1/(2\alpha)}$,

$$B_{\alpha,\beta}=\frac{\arctan\left(\beta\tan\frac{\pi\alpha}{2}\right)}{\alpha},$$

для $\alpha=1$

$$\xi=\frac{2}{\pi}\left\{\left(\frac{\pi}{2}+\beta V\right)\tan V-\beta\ln\left(\frac{\frac{2}{\pi}W\cos V}{\frac{2}{\pi}+\beta V}\right)\right\},$$

где V – случайная величина, сформированная на интервале $\left(-\frac{\pi}{2},\frac{\pi}{2}\right)$,

W – экспоненциальная случайная величина с единичной дисперсией.

$$X=\begin{cases}\xi+\delta & \text{if } \alpha\neq 1\\ \sigma\xi+\frac{2}{\pi}\beta\sigma\log(\sigma)+\delta & \text{if } \alpha=1\end{cases}$$

Для упрощений вычислений в работе рассматриваются только распределения, где

$$\delta=0,\ \sigma=1,\ \beta=0,$$

что, конечно же, сужает полосу возможных реализаций аттракторов, однако упрощает вычисления. Исходя из этого ограничения выражение, наведенное выше, сводится к следующему более простому виду

$$X=\xi \quad \text{if} \quad 0<\alpha\le 2.$$

Для процесса передачи бинарной информации предложено кластерное кодирование. Где передаваемым битам со значением "1" и "0" соответствует одинаковое количество отсчетов несущего сигнала, которые имеют разные значения параметра альфа-стабильных распределений.

Для обеспечения синхронизации передаваемой и принимаемой стороны в промежутке между передачей генерированных сигналов, которые отвечают соседним битам информационной последовательности, в канал связи поступают маркерные сигналы, со значением параметра $\alpha=2$.

Структурная схема кодирования и декодирования полезной информации приведена на рисунке 2.

В процессе декодирования информации возникает ряд проблем. Это проблемы связанные с оценкой правильности принятия того или иного бита информации и проблемы связанные с искажением вида сигнала за счет наблюдения на фоне аддитивных и мультипликативных помех.

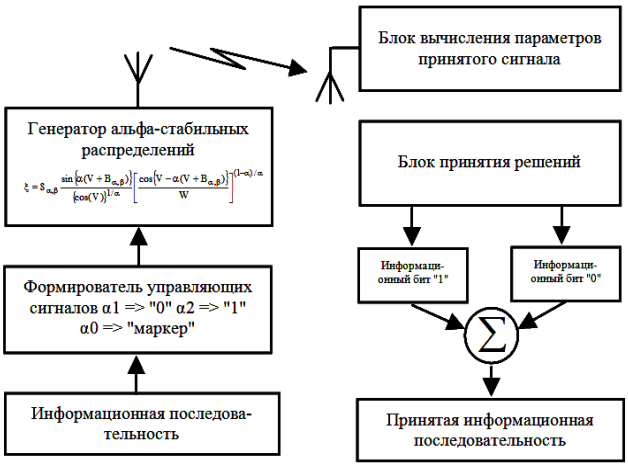


Рис. 2. Структурная схема кодирования-декодирования полезной информации

Поскольку, в общем, случаи отсутствуют достаточно простые выражения для плотности распределений сигналов на основе семейства альфа-стабильных распределений. Было предложено решать проблему оценки правильности принятия того или иного бита информации на основе оценки показателя экспоненциальной характеристики стационарности альфа-стабильных распределений. Для этого было рассмотрено несколько методов оценки параметров альфа-стабильных распределений: метод на основе квантилей распределений; метод основанный на измерении характеристической функ-

ции; а также метод основанный на фракционном моменте низкого порядка.

Границы возможностей методов оценки показателя экспоненциальной характеристики стационарности приведены в таблице 1. Из таблицы видно, что наиболее быстродействующим и эффективным методом для оценивания параметров альфа-стабильных распределений в реальной масштабе времени является метод оценивания квантилей распределения (метод McCullocha) [4].

Таблица 1

Методы оценки показателя экспоненциальной характеристики стационарности

Название метода	α
McCulloch	(0,6;2)
Kogon	(0;2)
Ma	(0;2)
Tsihrintzis	(0;2)

Этот метод имеет наибольшую скорость функционирования. Однако, основным его недостатком является не полная полоса возможности оценки показателя экспоненциальной характеристики стационарности альфа-стабильных распределений, поскольку на практике очень сложно сформировать сигналы с показателем экспоненциальной характеристики стационарности альфа-стабильных распределений ниже $\alpha = 0{,}7$. По этому такой недостаток, не несет за собой существенных ограничений в возможностях практической реализации.

Метод McCullocha заключается в оценке параметров распределений на основе вычисления процентилей случайных реализаций [3]. Так для определения параметра альфа сначала вычисляется индекс:

$$\nu_\alpha = \frac{X_{0,95} - X_{0,05}}{X_{0,75} - X_{0,25}},$$

а также

$$\nu_\beta = \frac{X_{0,95} + X_{0,05} - 2X_{0,5}}{X_{0,95} - X_{0,05}}.$$

Затем с помощью вспомогательных таблиц наведенных в [3] определяется $\alpha = \Psi_1(\nu_\alpha, \nu_\beta)$ и $\beta = \Psi_2(\nu_\alpha, \nu_\beta)$ учитывая что

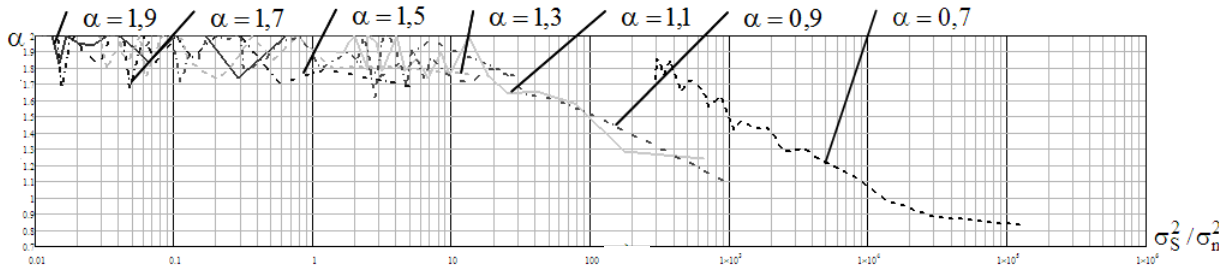
$$\Psi_1(\nu_\alpha, -\nu_\beta) = \Psi_1(\nu_\alpha, \nu_\beta);\ \Psi_2(\nu_\alpha, -\nu_\beta) = -\Psi_2(\nu_\alpha, \nu_\beta).$$

Для решения проблем, связанных с искажением вида сигнала, за счет влияния аддитивных и мультипликативных помех было проведено имитационное моделирование скорости искажения оценки показателя экспоненциальной характеристики стационарности альфа-стабильных распределений.

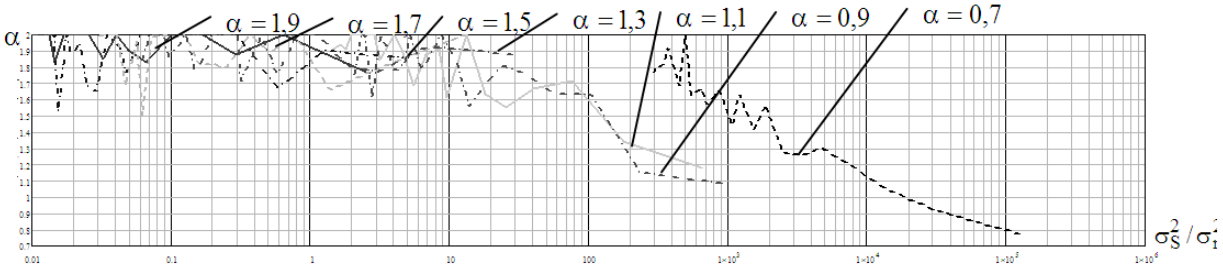
Для этого были сформированы сигналы с набором показателей $\alpha = 0{,}7; 0{,}9; 1{,}1; 1{,}3; 1{,}5; 1{,}7; 1{,}9$ и построены графики зависимости оценки значения показателя экспоненциальной характеристики стационарности альфа-стабильных распределений от отношения сигнал шум на входе приемного тракта (рис. 3).

Из рисунка видно, что помехоустойчивость сигналов на основе альфа-стабильных распределений тем выше, чем выше показатель экспоненциальной характеристики стационарности. Так же видно, что наиболее выгодных диапазон возможных параметров показатель экспоненциальной характеристики стационарности $1{,}3 \geq \alpha \leq 1{,}7$, что позволяет обеспечить правильный прием сообщения в диапазоне отношений сигнал/шум на входе приемника соответственно $100 \geq \sigma_S^2 / \sigma_n^2 \leq 0{,}2$.

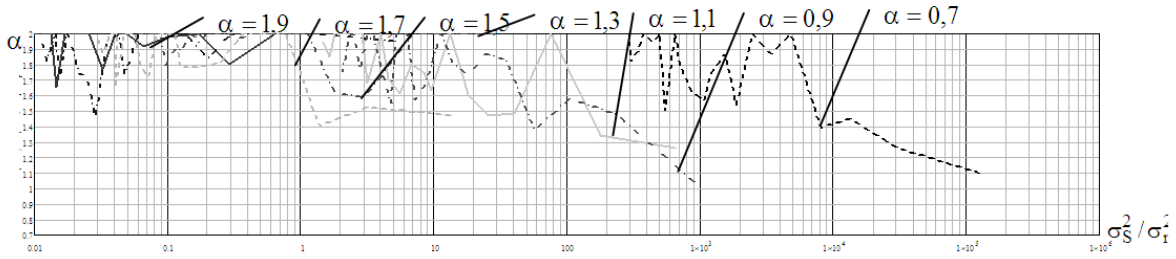
Используя, выше разработанный метод кодирования и декодирования передаваемой информации, было проведено имитационное моделирование возможностей передачи информации с такими начальными условиями: $\alpha = 1{,}7$ соответствует биту "1", $\alpha = 1{,}3$ соответствует биту "0".



а – L=500



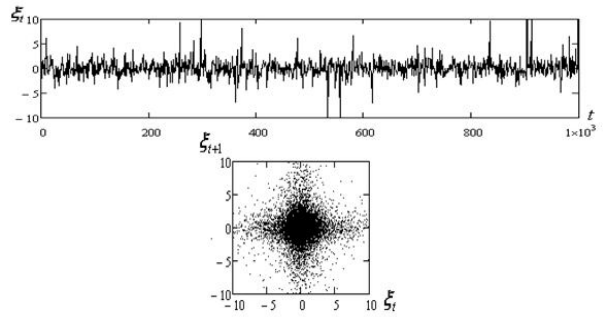
б – L=250



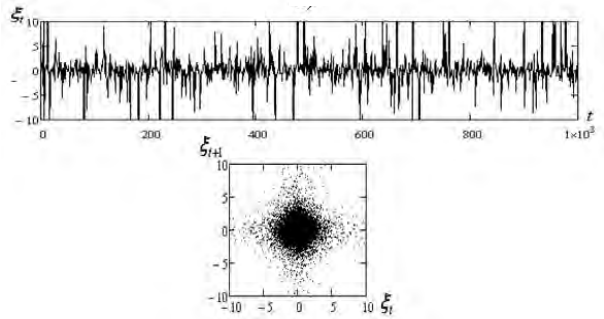
в – L=125

Рис. 3. Зависимости оценки значения показателя экспоненциальной характеристики стационарности альфа-стабильных распределений от отношения сигнал шум на входе приемного тракта

На рис. 4 приведен вид временной реализации и фазового портрета случайной величины информационных последовательностей.



а



б

Рис. 4. Временная реализация и фазовый портрет случайной величины: а – α=1,3; б – α=1,7

При этом на выходе кодера будет иметь место закодированная информационная последовательность с временной реализацией и фазовым портретом, представленными на рис. 5.

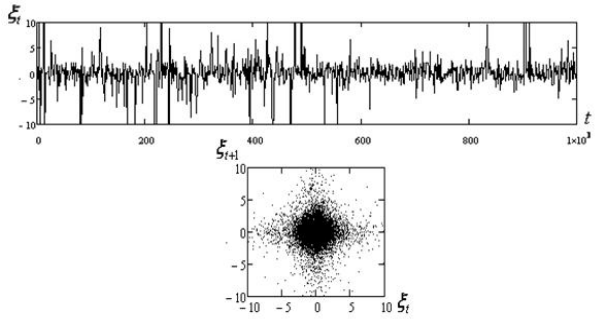


Рис. 5. Временная реализация и фазовый портрет закодированной последовательности

Проанализируем качество восстановления бинарной информации.

Для решения данной задачи на основании метода оценки показателей экспоненциальной характеристики стационарности (McCullocha) был построен график зависимости вероятности правильной оценки

$$P_{\vec{r}}(L,q) = 1 - P_{err.\vec{r}}(L,q)$$

сообщения $\vec{r}$ от количества элементов L бинарного сообщения и отношения сигнал/шум на входе приемника

$$q = \sigma_S^2 / \sigma_n^2 \quad \text{(рис. 6).}$$

Величина $P_{err.\vec{r}} = d_H(\vec{r}, \hat{\vec{r}})/Q$ определяет долю ошибок в оценках элементов сообщения и равна отношению расстояния Хемминга $d_H(\vec{r}, \hat{\vec{r}})$ между передаваемой бинарной последовательностью $\vec{r}$ и её оценкой $\hat{\vec{r}}$ к общему числу L ее элементов.

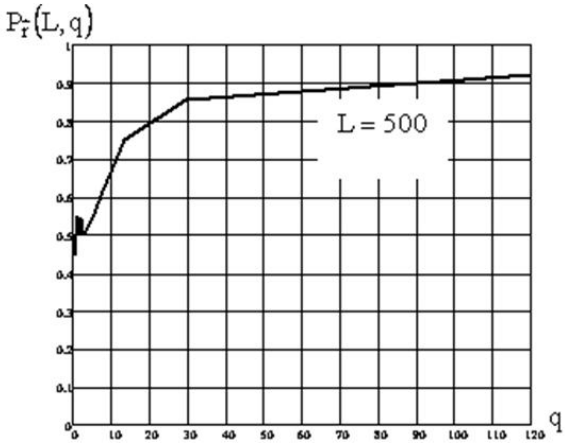


Рис. 6. Зависимости вероятности правильной оценки от отношения сигнал/шум на входе приемника

Из рисунка видно, что для обеспечения качества приема и восстановления цифровой информации в предложенном методе необходимо иметь на входе приемника большие значения отношения сигнал/шум. Это обусловлено "тяжелыми хвостами" альфа-стабильных распределений.

Анализ альфа-стабильных распределений нелинейными методом анализа [4], основанным на

применении BDS-статистики, которая обладает высокой чувствительностью к мере зависимостей между значениями наблюдения показывает (рис. 7), что сформированные сигналы на их основе не будут отличимые от шума наблюдения.

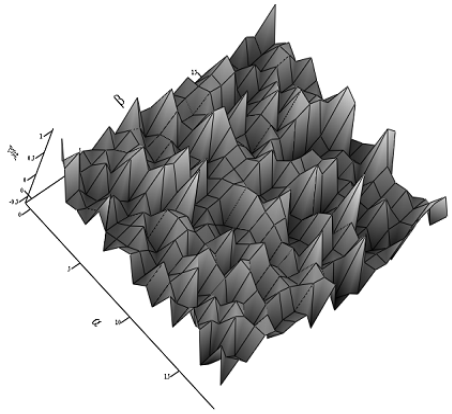


Рис. 7. BDS статистика
альфа-стабильных распределений

К достоинствам предложенного метода можно отнести то, что работа такого передатчика создает в районе функционирования дополнительные помехи и позволяет не правильно классифицировать источник передачи информации, а так же одновременно осуществлять постановку помех другим радиотехническим средствам.

Выводы

Таким образом, для повышения скрытности передачи и хранения цифровой информации возможно использование метода, основанного на кодирование бинарной информации последовательностями альфа-стабильных распределений с разными показателями экспоненциальной характеристики стационарности.

Путем имитационного моделирования определен оптимальный диапазон применимых параметров $1{,}3 \geq \alpha \leq 1{,}7$.

Опираясь на визуальные, энергетические, корреляционные, нелинейные свойства таких сигналов можно ожидать значительное повышение их скрытности при передаче цифровой информации. Для обеспечения высокого качество восстановления ($P_{\bar{r}} \geq 0{,}85$) бинарного сообщения по наблюдению требуются большие значения отношения сигнал/шум на входе приемника $q \geq 30$.

Внесение бинарной информации в случайные процессы с альфа-стабильными распределениями может осуществляться путем манипуляции и других параметров этих процессов: β , δ , σ .

Список литературы

1. Варакин Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин – М.: Радио и связь, 1985. – С. 8-9.

2. Васюта К.С. Модели нелинейных стохастических процессов в информационных системах и методы анализа на нелинейность / К.С. Васюта // Всеукр. межвед. науч.-техн. сб., 2009.

3. Bates S. The estimation of stable distribution parameters / Stephen Bates, Steve McLaughlin. – University of Edinburgh, Mayfield Rd, Edinburgh, EH9 3JL.

4. McCulloch J. H. Simple consistent estimators of stable distribution parameters / J. Huston McCulloch // Commun. Statist. – Simula. – 1986. – 15 (4) – P. 1109-1136.

5. Vasiuta K.S. Recognition of Colored Noise in Pseudo-Phase Space by Using BDS Statistics / K.S. Vasiuta // Radioelectronics and Communications Systems. – 2009 – Vol. 52. – №12. – P. 667-672.

Поступила в редколлегию 16.08.2013

Рецензент: д-р техн. наук, проф. П. Ю. Костенко, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД ПІДВИЩЕННЯ СКРИТНОСТІ СИСТЕМИ ПЕРЕДАЧІ БІНАРНИХ ПОВІДОМЛЕНЬ З ВИКОРИСТАННЯМ МАНІПУЛЯЦІЇ ПАРАМЕТРІВ ВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ, ЩО МАЮТЬ АЛЬФА СТАБІЛЬНІ РОЗПОДІЛИ

К.С. Васюта, С.О. Щербінін

Для приховання факту передачі та зберігання бінарної інформації в інфокомунікаційних системах запропоновано використання складних сигналів, фрагменти яких представляють випадкові процеси з альфа-стабільними розподілами та різними параметрами показника експоненціальної характеристики стаціонарності. Показано, що даний вид сигналів при візуальному, часово-частотному та нелінійному аналізі не відрізняється від шуму спостереження. Наведений алгоритм внесення бінарного повідомлення в випадкових процесах та його відновлення на фоні білого шуму. Проаналізовано якість відновлення повідомлення при різних відношеннях сигнал/шум на вході приймача.

Ключові слова: *прихованість, бінарне повідомлення, похибка відновлення,α-стабільні розподіли.*

METHOD OF INCREASING THE SECURITY OF TRANSMISSION SYSTEM OF BINARY MESSAGES USING MANIPULATION OF THE PARAMETERS OF RANDOM SEQUENCES WITH ALPHA-STABLE DISTRIBUTIONS

K.S. Vasyuta, S.A. Shcherbinin

To hide the fact of the transmission and storage of binary information in information and communication systems it is proposed to use complex signals, fragments of which are random processes with alpha-stable distributions and different parameters of the index of exponential stationarity characteristic. It is shown that this type of signals within the visual, time-frequency and non-linear analyses is indistinguishable from monitoring noise. An algorithm for getting a binary message into a random process and its reconstruction against the background of white noise is given. The quality of message reconstruction for various signal/noise ratios at the receiver input is analyzed.

Keywords: *security, binary message, reconstruction error, α-stable distribution.*