УДК 004.056; 621.391.26

ФОРМИРОВАНИЕ ХАОТИЧЕСКИХ ИМПУЛЬСНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЛЯ МАСКИРОВАНИЯ ИНФОРМАЦИОННЫХ СИГНАЛОВ

д-р техн. наук, проф. В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО
(Полоцкий государственный университет)

Анализируются методы маскирования информационных сигналов. Исследуются основные параметры маскирующих сигналов. Предложен новый метод маскирования информационных сигналов с использованием формируемой хаотической импульсной последовательности, адаптивной к аналоговым и цифровым сигналам. Метод основан на использовании белого гауссового широкополосного шумового сигнала для формирования многоуровневых случайных по длительностям и паузам между ними хаотических импульсных последовательностей.

Переход от простых двоичных сигналов к многомерным конструкциям [1] для передачи цифровых *m*-ичных информационных потоков обусловил необходимость рассмотрения методов активного маскирования двоичных и *m*-ичных информационных потоков. В работе [1] проанализированы и представлены результаты помехоустойчивости сигналов от преднамеренных помех в виде подобных *m*-ичных потоков [2] и белого шума. Маскирование такими сигналами предусматривает значительные энергетические запасы при отношении сигнал/шум больше 1. Для маскирования широко используют белый шум с ограниченной полосой, функция распределения плотности вероятности которой имеет вид [3, 4]:

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-A)^2}{2\sigma^2}}, \qquad (1)$$

где σ^2 – дисперсия; A – математическое ожидание случайной величины при отсутствии систематических составляющих.

Этим распределением полностью описываются свойства случайного процесса. Методика обработки результатов наблюдений случайного процесса на статистическую устойчивость наблюдений известна [5–7]. Функция распределения и ее числовые характеристики являются полными характеристиками случайных величин. Для нормального закона распределения плотности вероятности основными параметрами являются дисперсия и математическое ожидание. Для принятия решения о возможности использования случайного процесса необходимо оценить ряд дополнительных параметров.

Важным свойством маскирующего шума является отсутствие аддитивных смесей в виде дополнительных сигналов. Существенной характеристикой маскирующего шума выступает энтропия как мера неопределенности [8], определяемая для белого шума:

$$\hat{H}=\ln\sqrt{2\pi e}\sigma=\ln\sqrt{2\pi e}\cdot\sqrt{Д_э}.$$

Тогда энтропийная мощность шума $Д_э=\frac{e^{2\hat{H}}}{2\pi e}$.

Из сравнения по энтропийному коэффициенту функций распределения плотностей вероятности, представленных в работе [8], следует, что его значение максимально и равно 1 при нормальном распределении. Композиция нормального закона распределения плотности вероятности с синусоидальным распределением со случайной фазой с энтропийным коэффициентом, равным 0,54, снизит суммарный коэффициент по отношению к нормальному закону. Снижение коэффициента определяется отношением мощности синусоидального сигнала к мощности белого шума.

Структура маскирующих шумов представляет собой «смесь» флуктуационной (шумовой) и импульсной компонент [3]. В импульсной компоненте сосредоточена значительная часть энергии, поэтому она оказывает существенное влияние на прием и обработку информационного сигнала в канале утечки:

$$f(x)=\frac{1-\alpha}{\sqrt{2\pi}\sigma_ф}\exp\left(-\frac{x^2}{2\sigma_ф^2}\right)+\frac{\alpha}{\sqrt{2\pi}\sigma_и}\exp\left(\frac{x^2}{2\sigma_и^2}\right). \qquad (2)$$

Функция $f(x)=f(x;t)$ состоит из двух гауссовских плотностей вероятности, параметры которых $\sigma_ф^2$ и $\sigma_и^2$ характеризуют соответственно дисперсии флуктуационной и импульсной компонент. Коэффициент α определяет импульсную составляющую шума.

Нами рассматриваются ансамбли n импульсных потоков, сформированных из случайного нормального процесса. Каждый из n потоков формируется при превышении заданных пороговых значений опорного напряжения при переходе снизу вверх мгновенного значения амплитуды случайного процесса. Причем импульсы случайных последовательностей совпадают в зависимости от их временных параметров. Амплитуды импульсов импульсных потоков нормированы, а их длительности уменьшаются по мере увеличения опорного напряжения на величину U каждого заданного порогового значения.

В работе [3] проведена систематизация развития отдельных разрозненных результатов по практическим применениям характеристик пересечений уровней случайными процессами. Любой случайный непрерывный процесс полностью определяется своими реализациями. Несмотря на достигнутые результаты, современное состояние исследований этой теории в решении конкретных практических задач нельзя считать законченным.

Из наиболее распространенных характеристик случайных процессов наибольший интерес представляют относительные длительности нахождения реализации при превышении ею заданных уровней. Превышение этих уровней формирует хаотические разноуровневые импульсные последовательности. Порог срабатывания формирующего устройства формируется автоматически на априорно определенных уровнях. Эти уровни задаются делителями уровней. Каждый уровень реализуют из импульсной последовательности, полученной на предыдущем уровне.

При воздействии нормального случайного процесса на вход идеального ограничителя при уровне срабатывания $C \neq 0$ (несмещенный идеальный симметричный ограничитель (рис. 1)) выражение для функции корреляции на его выходе [9] можно представить следующим образом:

$$k_{\eta} = 1 - \frac{2}{\pi}\arccos p(\tau) = 1 - \frac{2}{\pi}\left(\frac{2}{\pi} - \arcsin p(\tau)\right) = \frac{2}{\pi}\arcsin p(\tau), \qquad (3)$$

где $p(\tau)$ – коэффициент корреляции.

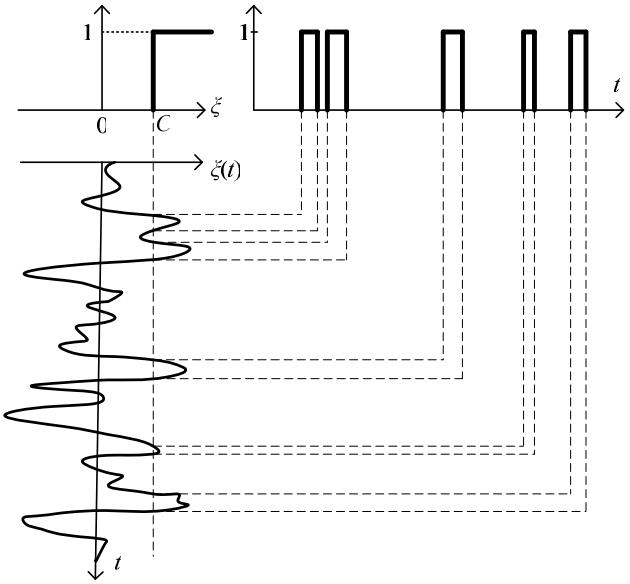

Рис. 1. Способ формирования хаотической импульсной последовательности

Неинерционный нелинейный преобразователь вида

$$\eta(t) = \begin{cases} 1, \text{ при } \xi(t) > C, \\ 0, \text{ при } \xi(t) < C. \end{cases}$$

Данное преобразование трансформирует положительные выбросы входного процесса $\xi(t)$ на уровне C или $\xi(t) > C$ в последовательность прямоугольных импульсов. Число выбросов, длительности выбросов и интервалы между ними полностью зависят от характеристик случайного процесса $\xi(t)$.

Хаотические импульсные последовательности (ХИП) [10] формируются с амплитудами, длительностями, а также с интервалами между импульсами по случайному закону. На практике ХИП реализуют с постоянной амплитудой и случайными по длительности импульсами и временными интервалами между ними. Хаотические импульсные последовательности формируют, подавая на вход, например, триггер-

ной схемы с одним устойчивым состоянием, пороговым напряжением на его входе U_0 шумовое напряжение по уровню, превышающему пороговое напряжение. Плотность вероятности мгновенных значений шума подчинена нормальному закону со средним значением, равным нулю. В зависимости от порога U_0 среднее значение длительности импульсов τ, паузы между ними Δ и числа пересечений $N_{ср}$ порогового уровня в единицу времени определяют следующим образом [10]:

$$T_\tau = \frac{\pi}{\sqrt{-p_0''}}\left(1-\Phi\left(\frac{\gamma}{\sqrt{2}}\right)\right)\exp\left(\frac{\gamma^2}{2}\right), \quad (4)$$

$$T_\Delta = \frac{\pi}{\sqrt{-p_0''}}\left(1+\Phi\left(\frac{\gamma}{\sqrt{2}}\right)\right)\exp\left(\frac{\gamma^2}{2}\right), \quad (5)$$

$$N_{ср} = \frac{1}{\pi}\sqrt{-p_0''}\exp\left(-\frac{\gamma^2}{2}\right). \quad (6)$$

Здесь $p_0'' = \frac{d^2 p(\tau)}{d\tau^2}$ при τ = 0; $p(\tau)$ – коэффициент корреляции шума.

$$\Phi(\gamma) = \frac{2}{\sqrt{\pi}}\int_0^{\gamma} e^{-x^2}\,dx,$$

где $\gamma = \frac{U_0}{\sigma_ш}$; U_0 – пороговое напряжение; $\sigma_ш$ – дисперсия шума.

В работе [9] определено, что количество уровней маскирования усложняет устройство формирования маскирующего сигнала.

Для формирования ХИП разработано и предложено [11] **устройство для получения сигнала маскирования каналов утечки информации**, содержащее последовательно включенные источник шумового сигнала, фильтр нижних частот и усилитель. В устройство дополнительно включены последовательно соединенные блок формирования ХИП, сумматор, устройство масштабирования уровня совпадающих импульсных последовательностей и согласующий каскад, причем блок формирования ХИП содержит *N* формирователей ХИП положительного уровня и *N* формирователей ХИП отрицательного уровня, а также *N*–1 формирователей опорных уровней положительного уровня и *N*–1 формирователей опорных уровней отрицательного уровня. Выход усилителя подключен на первые входы каждого из формирователей ХИП; второй вход двух формирователей ХИП первого уровня соединен с землей; второй вход каждого из остальных формирователей ХИП – с выходом предшествующего формирователя ХИП через последовательно включенный формирователь опорного уровня; выходы формирователей ХИП соединены с входами сумматора.

На рисунке 2 представлен источник шумового сигнала *1*, который последовательно подключен к фильтру нижних частот *2* и усилителю *3*. Выход усилителя *3* последовательно включен с блоком формирования ХИП *5*, в котором выход усилителя *3* подключен на первые входы каждого из формирователей хаотических импульсных последовательностей *6–13*. Выходы формирователей ХИП *6–8*, *10–12* через формирователи опорного уровня *4* подключены на вторые входы формирователей ХИП следующим образом: выход формирователя ХИП первого положительного уровня *6* подключен на второй вход формирователя ХИП второго положительного уровня *7* через формирователь опорного уровня *4*, далее выход формирователя ХИП *7* подключен на второй вход формирователя ХИП *8* соответственно и т.д.; выход формирователя ХИП первого отрицательного уровня *10* подключен на второй вход формирователя ХИП второго отрицательного уровня *11* через формирователь опорного уровня *4*, далее выход формирователя ХИП *11* подключен на второй вход формирователя ХИП *12* соответственно и т.д.; выходы формирователей ХИП подключены на входы сумматора *14*, выход которого последовательно включен к устройству масштабирования уровня совпадающих импульсных последовательностей *15* и согласующему каскаду *16*, являющемуся выходом устройства.

Устройство для получения сигналов маскирования каналов утечки информации работает следующим образом. Источник шумового сигнала *2* генерирует белый шумовой широкополосный сигнал и подает его на формирователи ХИП *6–13* через фильтр нижних частот *2* и усилитель *3*. Формирователи ХИП *6–13* формируют из прошедшего через фильтр *2* и усиленного шумового сигнала хаотические импульсные последовательности. Каждый из формирователей ХИП формирует выходную последовательность одного уровня: *+U* или *–U*. Так, формирователь ХИП *6* – первый положительный уровень, *7* – второй положительный, и таких уровней может быть *N* положительных и *N* отрицательных.

На первые входы каждого из формирователей ХИП *6–13* подают белый широкополосный шумовой сигнал. Другой вход формирователей ХИП *6*, *10* первого положительного и отрицательного уровней подключают к нулевому уровню («земле»). Выходы данных формирователей (*6*, *10*) подключают ко вторым входам формирователей ХИП *7*, *11* второго положительного и отрицательного уровней соответственно через формирователи опорных уровней напряжений *4* с равномерным шагом $U/(N-1)$ и $-U/(N-1)$. Выход каждого предшествующего формирователя ХИП подключают на второй вход каждого следующего формирователя через формирователи опорных уровней напряжений *4*. Длительность импульсов последовательностей формируется пересечением мгновенного значения уровня шумового сигнала с соответствующими 1, 2, …, N положительными и –1, –2, …, $-N$ отрицательными опорными уровнями. Длительность сформированных импульсов равна времени пребывания шумового сигнала над каждым опорным уровнем. Далее импульсы сформированных хаотических импульсных последовательностей с выхода формирователей подают на вход сумматора *14*, суммируют их по уровню и подают на выход устройства масштабирования уровня хаотических импульсных последовательностей *15*, которое предназначено для масштабирования и формирования суммарного потока совпадений в виде его дискретных состояний, и согласующий каскад *16*. В результате чего получают сигнал для маскирования каналов утечки речевых сигналов, видеосигналов и сигналов передачи данных (рис. 3).

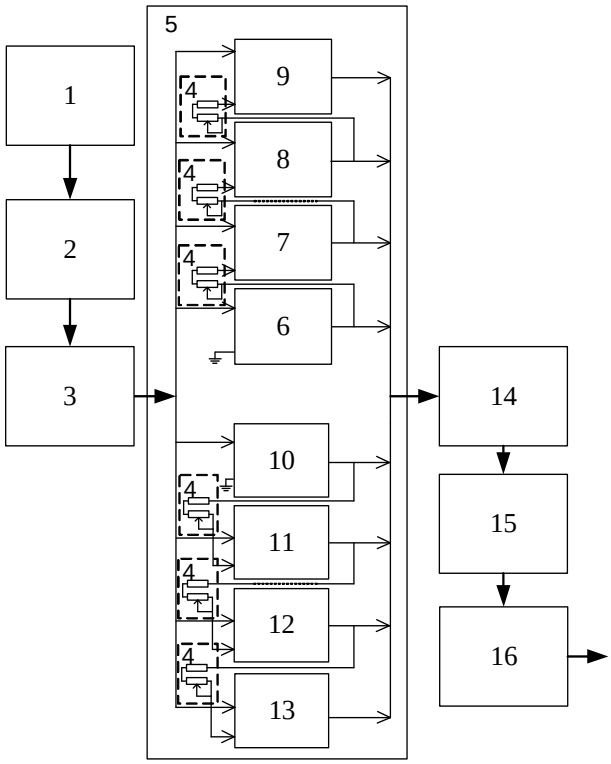

Рис. 2. Схема, реализующая способ получения сигнала маскирования каналов утечки информации при различных уровнях

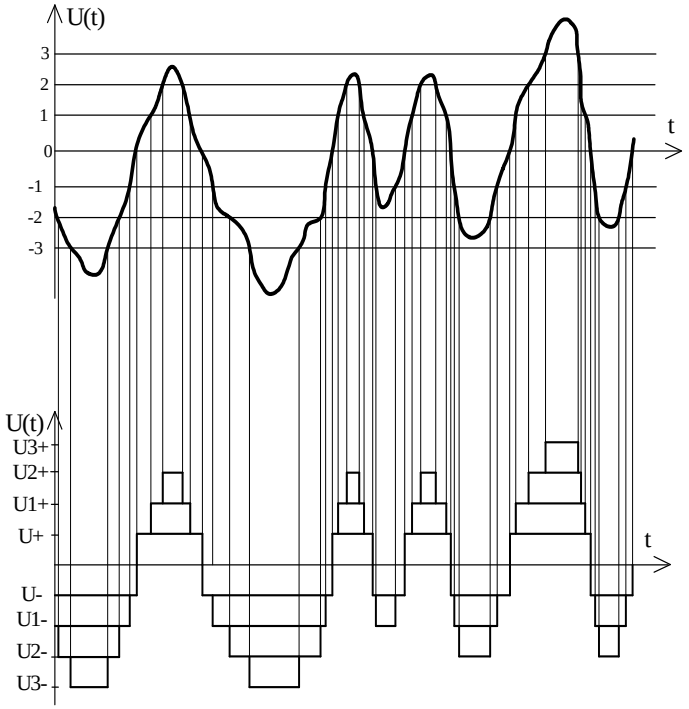

Рис. 3. Многоуровневая хаотическая импульсная последовательность маскирования каналов утечки информации

Заключение. Предлагается устройство формирования ХИП, которое обеспечит повышение степени защиты речевых сигналов в аналоговой и цифровой форме, видеосигналов и сигналов звукового сопровождения, сигналов передачи данных при преобразовании их из аналоговой в цифровую форму, передачи ее в цифровой форме по цифровым системам передачи, а также при дальнейшем преобразовании из цифровой формы в аналоговую.

С целью предотвращения перехвата конфиденциальной информации разработан и предложен **метод создания маскирующего сигнала для каналов утечки информации** (см. рис. 3), **основанный на формировании многоуровневой хаотической импульсной последовательности**. Применение многоуровневой хаотической импульсной последовательности позволило получить оптимальный маскирующий сигнал к параметрам маскируемых сигналов.

ЛИТЕРАТУРА

1. Савищенко, Н.В. Многомерные сигнальные конструкции: их частотная эффективность и потенциальная помехоустойчивость приема / Н.В. Савищенко; под ред. Д.Л. Бураченко. – СПб.: Изд-во Политехн. ун-та, 2005. – 420 с.
2. Теория передачи сигналов: учебник для вузов / Д.Д. Кловский [и др.]. – М.: Связь, 1980. – 288 с.
3. Тихонов, В.И. Проблема пересечений уровней случайными процессами / В.И. Тихонов, В.И. Хименко // Радиотехника и электроника. – 1998. – № 5, Т. 43. – С. 501–523.
4. Денисенко, А.Н. Сигналы. Теоретическая радиотехника: справ. пособие / А.Н. Денисенко. – М.: Горячая линия – Телеком, 2005. – 704 с.
5. Рабинович, С.Г. Погрешности измерений / С.Г. Рабинович. – Л.: Энергия, 1978. – 262 с.
6. Железняк, В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К. Железняк; ГУАП. – СПб., 2006. – 188 с.
7. Денисенко, А.Н. Статистическая теория радиотехнических систем / А.Н. Денисенко. – М.: АРИ, 2007. – 200 с.
8. Розенберг, В.Я. Радиотехнические методы измерения параметров процессов и систем / В.Я. Розенберг. – М.: Изд-во Комитета стандартов, мер и измерительных приборов при СМ СССР, 1970. – 308 с.
9. Тихонов, В.И. Выбросы случайных процессов / В.И. Тихонов. – М.: Наука, 1970. – 392 с.
10. Максимов, М.В. Защита от радиопомех / М.В. Максимов. – М.: Сов. радио, 1976. – 496 с.
11. Рябенко, Д.С. Применение хаотических импульсных последовательностей для маскирования аналоговых и цифровых речевых сигналов / Д.С. Рябенко, В.К. Железняк // Современные средства связи: материалы XVIII междунар. науч.-техн. конф., Минск, 15–16 окт. 2013 г.; редкол. А.О. Зеневич [и др.]. – Минск: УО ВГКС, 2013. – С. 207–208.

Поступила 04.03.2014

FORMING OF CHAOTIC PULSE PATTERNS FOR INFORMATION SIGNAL MASKING

V. ZHELEZNYAK, D. RYABENKO

Analysis of methods of information signals masking was performed in the research. Key parameters of masking signals were studied. New method of information signal masking with the usage of formed chaotic pulse pattern adaptive to analog and digital signals was suggested. The method is based on use of a white broadband noise signal for formation multilevel casual on time and pauses between them chaotic pulse sequences.