

## О ВОЗМОЖНОСТИ ОРГАНИЗАЦИИ МНОГОПОЛЬЗОВАТЕЛЬСКОГО ДОСТУПА В СИСТЕМАХ ПЕРЕДАЧИ С ХАОТИЧЕСКИМИ СИГНАЛАМИ

*Аннотация.* Предложен метод организации многопользовательского доступа в системах передачи конфиденциальной информации на основе хаотических сигналов. Показано, как с помощью корреляционного приема из группового сигнала выделяются сигналы индивидуальных абонентов.

На современном этапе развития телекоммуникационных технологий возникла необходимость в создании новых систем, обладающих повышенной информационной емкостью, высокой помехозащищенностью и обеспечивающих конфиденциальность передаваемого сообщения [1]. При построении таких систем передачи информации в последнее время все чаще используется явление динамического хаоса [2]. Под динамическим хаосом понимают сложные непериодические колебания, порождаемые нелинейными системами, вид которых полностью определяется только параметрами динамической системы. Такие колебания обладают всеми свойствами шумоподобного сигнала, так как для них характерно:

- 1) Непериодичность траекторий во времени.
- 2) Экспоненциально спадающая корреляционная функция.
- 3) Сплошной непрерывный спектр мощности.

В литературе приводятся алгоритмы для формирования выходного сигнала одноканальных систем передачи, однако интерес представляет организация многопользовательского доступа, когда сигналы всех абонентов объединяются в групповой сигнал и им предоставляется возможность одновременной работы в общей полосе частот. В данном докладе рассматривается возможность организации многопользовательского доступа в системах конфиденциальной передачи информации с использованием в качестве сигнатур ортогональных многоуровневых кодовых последовательностей сформированных на реализации хаотического процесса.

В работе методом перебора был осуществлен поиск семи ортогональных сигнатур на базе одной из реализаций хаотического сигнала. Предварительно, прошедший дискретизацию по времени и квантование по уровню хаотический сигнал  $x(t)$  преобразовывается в многоуровневую кодовую последовательность  $x_n$ . Кодовая последовательность  $x_n$  разбивается на сегменты определенной длины, например,  $s = 30$  элементов (чипов) и путем их сравнения находятся взаимно-ортогональные кодовые последовательности, которые и будут использоваться в качестве сигнатур.

Пусть имеется некоторое количество  $N$  источников цифрового сигнала, использующих избыточные коды, и соответствующее им количество двоичных каналов. Каждому  $i$ -му каналу присваивается своя многоуровневая кодовая последовательность в качестве сигнатуры  $c_i$ . Формирование сигнала в индивидуальном канале осуществляется путем замены единичных посылок сигнатурой, разной по структуре, но равной длительности в чипах для каждого канала (в нашем случае  $s = 30$ ). С целью обеспечения эффективности корреляционного приема в каждом индивидуальном канале на приемной стороне отдельные элементы (посылки) индивидуальных каналов должны быть синхронизированы между собой.

Следует заметить, что если для замены каждой “1” в исходном двоичном потоке данных используется некоторая сигнатура определенной длины, то для замены “-1” применяют ту же сигнатуру, но с инвертированием значений чипов. Использование прямой и инвертированной сигнатуры обеспечивает не только определение полярности передаваемых

посылок, но и позволяет регистрировать их передние и задние фронты при корреляционном приеме в каждом индивидуальном канале.

Так как групповой сигнал  $X_{ГР}$  формируется в результате суммирования сигнатур  $c_i$  всех индивидуальных каналов

$$X_{ГР} = \sum_{i=1}^N x_i c_i, \quad (1)$$

то надежность разделения каналов определяется степенью ортогональности сигнатур  $c_1, c_2, \dots, c_N$ .

На приемной стороне каждый разряд группового сигнала  $X_{ГР}$  умножается на соответствующий элемент “своей” прямой (используемой на передаче для замены “+1”) сигнатуры  $c_i$ , в результате получаем сигнал, в котором заложена информация индивидуального  $i$  канала. Результаты каждого умножения с учетом амплитуды и значения полярности интегрируются в накопителе в пределах одного периода последовательности. В конечном счете, по окончании периода сигнатуры на выходе интегратора формируется уровень напряжения, полярность которого будет соответствовать полярности принятой посылки “1” или “-1” в каждом индивидуальном канале. При этом сигналы других пользователей с их сигнатурами воспринимаются как аддитивные шумы для данного канала.

Попытка разделения группового сигнала с использованием сигнатур, неиспользуемых на передаче, не приведет к положительному результату, так как значения уровня напряжения каждого периода интегрирования будут близким к нулю.

Предполагая линейность системы и наличие идеальной синхронизации в каналах на рис. 1 показано выделение элементарных посылок одного индивидуального канала из группового сигнала при корреляционном приеме.

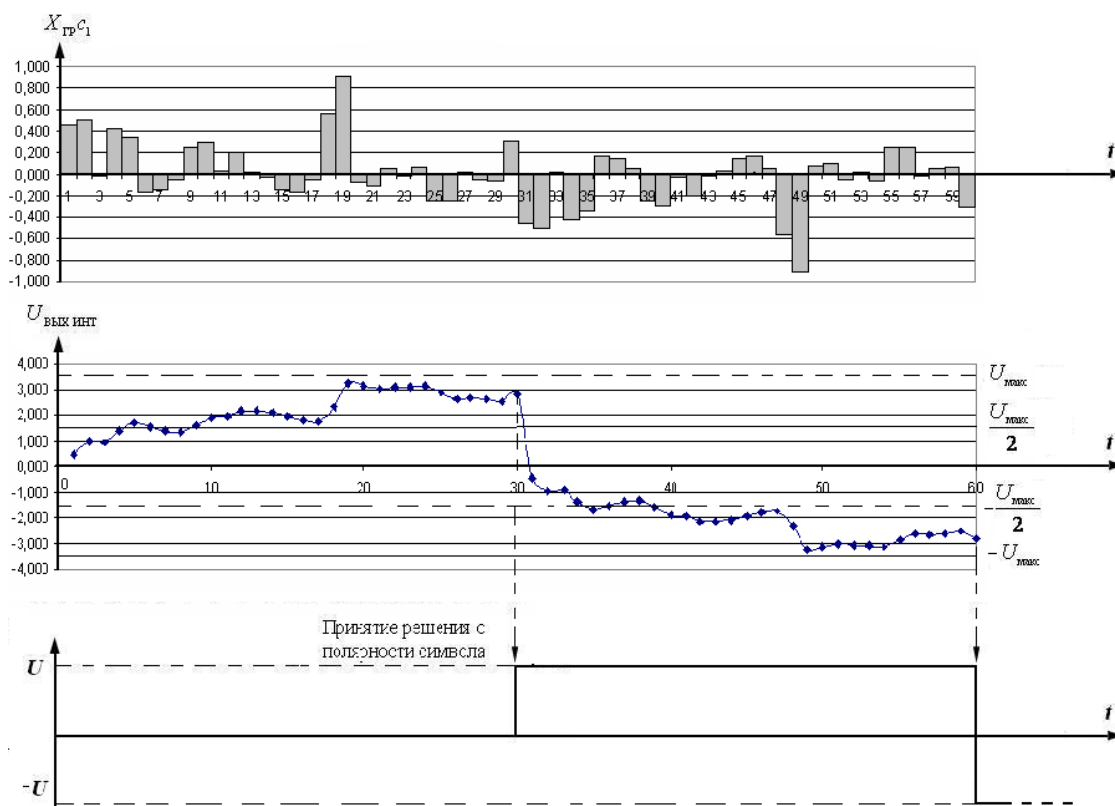


Рисунок 1 — Выделение элементарной посылки одного индивидуального канала из группового сигнала

Из рисунка видно, что уровень сигнала на выходе интегратора  $U_{\text{ВЫХ ИНТ}}$  значительно превышает порог принятия решения  $U_{\text{макс}}/2$ , чем обеспечивается надежное выделение сигнала каждого индивидуального канала. Кроме того, если  $U_{\text{ВЫХ ИНТ}} > U_{\text{макс}}/2$ , тогда принята посылка положительной полярности, если  $U_{\text{ВЫХ ИНТ}} < -U_{\text{макс}}/2$ , то – отрицательной.

Предложенные методы формирования многоуровневых ортогональных последовательностей на базе хаотического процесса и группового сигнала на их основе показали возможность организации многопользовательского доступа в современных конфиденциальных системах связи. При построении таких систем возникает задача поиска достаточного количества взаимно – ортогональных кодовых последовательностей с хорошими корреляционными свойствами.

#### Список литературы:

1. Гуляев, Ю.В. Информационные технологии на основе динамического хаоса для передачи, обработки, хранения и защиты информации / Ю.В. Гуляев, Р.В. Беляев, Г.М. Воронцов и др. // Радиотехника и электроника. – 2003. – Т. 48, №10. – С 1157-1185
2. Капранов, М. В. Регулярная и хаотическая динамика нелинейных систем с дискретным временем / М. В. Капранов, А. И. Томашевский. – М.: Издательский дом МЭИ, 2010. – 256 с.

*Захарченко Н.В., Корчинский В.В., Радзимовский Б.К.  
Одесская национальная академия связи им. А.С. Попова*

## **СИНТЕЗ СИГНАЛЬНО-КОДОВЫХ КОНСТРУКЦИЙ НА ОСНОВЕ ХАОТИЧЕСКИХ И ТАЙМЕРНЫХ СИГНАЛОВ**

*Аннотация. Предложен метод синтеза сигнальных конструкций на основе хаотических и таймерных сигналов. Приведен алгоритм формирования сигнала для передачи и показан метод его приема в системах конфиденциальной связи.*

Надежная защита передаваемых данных от несанкционированного доступа (НСД) является одним из главных критериев эффективности конфиденциальных систем связи [1]. Поэтому поиск и исследование методов передачи, направленных на увеличение скрытности (энергетической, структурной и информационной) передаваемой информации является актуальной задачей.

Известно [1], что применение в системах связи широкополосных сигналов с большой базой  $B \gg 1$  при разрядно-цифровых методах кодирования обеспечивает значительное повышение скрытности передачи, по сравнению с сигналами  $B=1$ . В свою очередь, исследования, проведенные в работах [2,3], показали, что структурная и информационная скрытность таймерных сигнальных конструкций (ТСК) выше, чем при разрядно-цифровых методах кодирования. Эти факторы обосновывают целесообразность поиска и синтеза новых сигнальных конструкций, обладающих более высокой помехозащищенностью. С целью повышения скрытности передаваемых сигналов в данной работе предложен метод формирования сигнальных конструкций на основе широкополосных хаотических [4] и информационных таймерных сигналов.

В известных алгоритмах передачи на основе динамического хаоса [4] формирование выходного сигнала осуществляется модуляцией информационной последовательностью хаотического сигнала на каждом единичном интервале  $t_0$  разрядно-цифрового кода. Если в качестве информационной последовательности использовать ТСК, то применить такие