ЗАЩИЩЕННЫЕ ТЕЛЕКОМУНИКАЦИОННЫЕ СИСТЕМЫ И ПЕРЕДАЧА ДАННЫХ

УДК 681.3.06:519.248.681

И.Д. ГОРБЕНКО, д-р техн. наук, А.А. ЗАМУЛА, д-р техн. наук

КРИПТОГРАФИЧЕСКИЕ СИГНАЛЫ: ТРЕБОВАНИЯ, МЕТОДЫ СИНТЕЗА, СВОЙСТВА, ПРИМЕНЕНИЕ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

Введение

В условиях интенсивного информационного противодействия сторон, интересы и конкуренция которых могут проявляться в различных сферах, в том числе, как показали последние события, в сфере ведения информационных и гибридных войн, особое значение приобретает наличие и применение защищенных телекоммуникационных систем (ТКС). В существенной мере такие системы базируются на применении защищенных радиоканалов. При этом под защищенностью систем необходимо понимать, в широком смысле, прежде всего их способность обеспечивать необходимые показатели по помехозащищенности, имитостойкости, информационной, энергетической и структурной скрытности. При этом в процессе противодействия помехозащищенность радиоканалов ТКС зависит от скрытности выбора и использования параметров системы. Причем станция противодействия, как правило, ставит перед собой цель нанести максимальный ущерб ТКС и /или ее пользователям и собственникам при минимизации собственных затрат. В указанных условиях особенно важной проблемой для ТКС является обеспечение минимизации потерь при максимальных затратах станции противодействия. Эта цель достигается, в том числе, за счет обеспечения скрытности применяемых радиоканалов – структурной, энергетической и информационной скрытностей [2, 4, 5, 12].

Под скрытностью радиоканалов в целом и скрытностью используемых в них параметров будем понимать их способность противостоять мерам радиотехнической разведки, направленным на обнаружение факта работы системы (энергетическая скрытность) и определения необходимых для радиопротиводействия параметров сигнала (структурная и информационная скрытность). Энергетическая скрытность характеризует способность системы противостоять мерам, направленным на обнаружение станцией противодействия факта функционирования системы. Структурная скрытность используемых сигналов характеризует сложность достоверного предсказания сигналов или их символов (по известным предыдущим). Информационная скрытность системы характеризует сложность отождествления принятых сигналов с передаваемым сообщением.

Возможными стратегиями станции противодействия являются: определение содержания сообщений при использовании легальными абонентами алгоритмов криптографической защиты данных; фальсификация сообщений; нарушение целостности данных; постановка различных типов помех и другое. Поэтому, к ТКС, особенно к системам критичного назначения, предъявляются все более жесткие требования по обеспечению эффективности их функционирования (скорости передачи информации, помехоустойчивости приема информации, живучести, помехозащищенности, информационной безопасности) в условиях сложных внешних и внутренних воздействий.

Также повышенные требования к эффективности функционирования ТКС в условиях внутренних и внешних воздействий, в значительной мере не учитываются существующими информационными технологиями. Имеет место противоречие между жесткими требованиями по обеспечению достоверности, скрытности, конфиденциальности, целостности, подлинности данных, передаваемых по проводным и беспроводным линиям связи ТКС, с одной стороны, и существующими моделями, методами и технологиями управления телекоммуни-

кационными сетями, информационной безопасностью, услугами и качеством обслуживания – с другой.

Поэтому создание новых моделей, методов и технологий управления телекоммуникационными сетями, информационной безопасностью, услугами и качеством обслуживания с целью улучшения показателей эффективности систем, в условиях внешних и внутренних воздействий (угроз), посредством создания различных помех (ретранслированных, структурных, импульсных, широкополосных, узкополосных и т.п.), обеспечение конфиденциальности, целостности и подлинности информационного обмена является, на наш взгляд, актуальными направлениями исследований.

Постановка задачи синтеза системы нелинейных дискретных сложных сигналов

Значительное число ТКС относятся к многопользовательским системам. В таких системах множество каналов размещаются в пределах общего частотно-временного ресурса. Одним из наиболее перспективных способов множественного доступа к услугам и ресурсам системы является множественный доступ с кодовым разделением абонентов, работающих в общей полосе частот (CDMA). Указанный способ доступа является перспективным по многим характеристикам: высокая помехозащищенность каналов и обеспечение конфиденциальности передаваемых данных; высокая скорость передачи и эффективность использования полосы частот; высокая энергетическая экономичность и абонентская емкость сети. Поскольку кодовое разделение каналов ТКС основано на различии сигналов, предоставляемых абонентам системы, то построение таких систем и их характеристики определяются выбором сигналов и их свойствами. Перспективным направлением обеспечения безопасности информационных ресурсов является использование технологии распределенного спектра (широкополосных шумоподобных сигналов).

Основными путями решения указанного противоречия является повышение помехозащищенности (в частности, энергетической, структурной и информационной скрытности, помехоустойчивости приема сигналов) и информационной безопасности (в частности, имитостойкости) ТКС на основе усовершенствования методологических основ построения ТКС путем разработки методов информационного обмена, методов синтеза новых классов нелинейных сложных дискретных сигналов-переносчиков данных с необходимыми ансамблевыми, корреляционными и структурными свойствами. Процесс выбора рациональных по тем или иным критериям структур сложных сигналов тождественен синтезу соответствующих манипулирующих дискретных последовательностей (ДП). В качестве критерия выбора класса дискретных сигналов (ДС), как правило, ориентируются на критерий минимума взаимных помех (минимаксный критерий). Такой критерий подразумевает построение ансамблей сигналов объема M, манипулированных ДП, как можно заметнее отличающихся друг от друга при возможных циклических сдвигах.

Количественной мерой отличия манипулирующих ДП служат максимальные по ансамблям уровни бокового лепестка периодической функции автокорреляции (ПАКФ) и уровни бокового лепестка периодической функции взаимной корреляции (ПВКФ). Исходя из этого применяемые в ТКС широкополосные сигналы (ШПС) должны обладать такими корреляционными свойствами, когда боковые пики корреляционных функций ШПС являются как можно меньшими, т.е. в идеальном случае должны стремиться к нулю. Однако требование идеальности (нулевые значения боковых пиков) авто- и взаимокорреляционных функций между всеми циклическими сдвигами K последовательностей и различными изоморфизмами системы сигналов с периодом N невыполнимо, поскольку значение боковых пиков не может опуститься ниже $1/2\sqrt{B}$ (B – база сигнала) [2].

Используемые в ТКС методы информационного обмена, а также классы широкополосных сигналов, применяемые в качестве физического переносчика данных (множества линейных рекуррентных последовательностей (М-последовательности), Касами, Голда, Камалетдинова и др.), обладающие сравнительно небольшими значениями боковых лепестков авто- и

взаимно-корреляционных функций, не позволяют обеспечить необходимые (для критичных приложений ТКС) показатели информационной безопасности и помехозащищенности [3]. Так, в процессе информационного обмена в ТКС в течение длительного времени соответствие: бит сообщение-сигнал является фиксированным, а указанные выше сигналы обладают низкой структурной скрытностью, ограниченными ансамблевыми свойствами, а также существуют только для ограниченного числа значений периода сигнала. В случае усечения (увеличения) периода таких сигналов их корреляционные свойства ухудшаются. Поэтому актуальна задача разработки теории и практики синтеза и анализа систем дискретных сигналов с требуемыми корреляционными, структурными, ансамблевыми свойствами.

Анализ показал, что в настоящее время отсутствуют регулярные методы синтеза дискретных последовательностей (ДП) оптимальных по минимаксному критерию. Задача синтеза ДП оказывается еще более сложной, если выдвигаются требования к размерности (объему) системы сигналов, структурным свойствам и числу элементов ДП. Поскольку для технологии распределенного спектра свойства сигналов-переносчиков данных полностью определяются свойствами ДП, манипулирующих информационными битами данных пользователей системы [3], актуальной проблемой остается поиск эффективных методов синтеза дискретных сигналов (последовательностей), отвечающих потенциально достижимым граничным характеристикам (минимаксным свойствам или границе «плотной упаковки»).

Сформулируем в общем виде задачу синтеза сигналов с заданными корреляционными ансамблевыми и структурными свойствами, обеспечивающими требуемые значения помехозащищенности, имитостойкости и скрытности функционирования системы передачи информации. Потребуем, чтобы такие системы сигналов обладали свойством «размытости» по корреляционным свойствам. Указанное свойство означает, что увеличение или уменьшение длины дискретной последовательности не изменяет корреляционные свойства, присущие исходной дискретной последовательности.

Под задачей синтеза сигналов будем понимать задачу построения словарей (подмножеств, векторов) $(W_m^q), q=\overline{1,N}$, $m=\overline{1,M}$ вся $M_k << p^L$, совокупность которых образует систему сигналов размерности $M_k = N \times M_x$ таких, что в каждом из словарей выполняются следующие условия.

1. Автосвертка или периодическая функция автокорреляции (ПФАК) каждого из W_m^q дискретных сигналов (ДС) удовлетворяет системе нелинейных параметрических неравенств (СНПН)

$$R_{a_1}^q(l) \le \sum_{i=1}^{L-1} W_i^q (W_{i+c}^q)^* \le R_{a_2}^q(l), \quad l=\overline{1,L-1}, \; q=\overline{1,N}, \tag{1}$$

где $R_{a_1}^q(l)$ и $R_{a_2}^q(l)$ – заданные (требуемые) реализации ПФАК.

2. Взаимная свертка или стыковая функция взаимной корреляции (СФВК) ($W^q W^p$) ДС со стыковыми словами W^{qp} и W^{pq} удовлетворяет совокупности систем нелинейных параметрических неравенств:

$$R_{b_{1,1}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,1}}^{qp}(l);$$

$$R_{b_{1,2}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^p)^* \le R_{b_{2,2}}^{qp}(l);$$

$$R_{b_{1,3}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^q \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^q \times (W_{i-l+K}^q)^* \le R_{b_{2,3}}^{qp}(l);$$

$$R_{b_{1,4}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^p)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^q)^* \le R_{b_{2,4}}^{qp}(l);$$

$$R_{b_{1,5}}^{qp}(l) \le \sum_{i=0}^{L-K} W_i^p \times (W_{i+l}^q)^* + \sum_{i=L-K+1}^{L-1} W_i^p \times (W_{i-l+K}^p)^* \le R_{b_{2,5}}^{qp}(l); \quad (2)$$

причем $l=\overline{1,L-1}$ для всевозможных сочетаний q и p, $q=\overline{1,N}$, $p=\overline{1,N}$, $q \ne p$, где $R_{b_{1,j}}^{qp}(l)$ и $R_{b_{2,j}}^{qp}(l)$ – заданные (требуемые) реализации ПФВК и СФВК.

3. Исследования показывают, что существенные затруднения в преодолении скрытности функционирования радиоканалов могут быть созданы за счет придания сигналам свойства «размытости». Введем понятие размытости. Причем вначале сформулируем задачу синтеза одиночного сигнала W^q, обладающего размытостью по циклической свертке. Определим интервал размытости Δx по длительности

$$L - x_2 \le \Delta x \le L + x_1, \quad (3)$$

Полагая, что в общем случае $|x_1| \ne |x_2|, |x_1|, |x_2| < L$, интервал размытости Δy относительно истинных значений цикловой частоты в виде

$$L - y_2 \le \Delta y \le L + y_1 \quad (4)$$

причем $|y_1| \ne |y_2|, |y_1|, |y_2| < L$.

Положим, что на основе обработки потока сигналов $W^{\nu}W^{\nu}...W^{\nu}$ принимается как истинный сигнал

$$W_{x_L}^{\vartheta} = W_{L-\delta}^{\vartheta} W_L^{\vartheta} W_{x_1-L-\delta}^{\vartheta}, \quad (5)$$

либо

$$W_{x_1}^{\vartheta} = W_{L-\delta}^{\vartheta} W_{X_1+\delta}^{\vartheta}, \quad (6)$$

при $\Delta x \ge L$, либо сигнал

$$W_{x_2}^{\vartheta} = W_{L-X_2}^{\vartheta}, \quad (7)$$

либо

$$W_{x_{21}}^{\vartheta} = W_{\delta}^{\vartheta} W_{L-x_2-\delta}^{\vartheta}, \quad (8)$$

при $\Delta x < L$, где индексы x_1 и x_2, δ, L, $x_1+\delta_1-L$, $L-\delta$, $x_1+\delta$, $L-x_2-\delta$ указывают на число символов усеченного сигнала W^{ϑ} (первых или последних, соответственно расположению его символов, $W_{x_1}^{\vartheta}$ или $W_{x_2}^{\vartheta}$. Тогда, размытость сигналов, заданных (5) – (8), будем представлять совокупностью систем нелинейных параметрических неравенств:

$$R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \sum_{i=1}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right) + \\ + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \sum_{i=1}^{x_1-L+\vartheta} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* \le R'_{a_2}(k); k = \overline{0, L+x_2}, \quad (9, \text{а})$$

$$R_{a_1}(k) \le \sum_{i=\delta}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* + \sum_{i=1}^{L-K} W_i^{\vartheta} \left(W_{i+k}^{\vartheta}\right) + \\ + \sum_{i=L-k+1}^{L} W_i^{\vartheta} \left(W_{i-L+K}^{\vartheta}\right)^* \le R'_{a_2}(k); k = \overline{0, L+x_1}, \quad (9, \text{б})$$

$$R_{a_2}(k) \le \sum_{i=1}^{L-x_1} W_i^{\vartheta} \left(W_{i-k}^{\vartheta}\right)^* \le R'_{a_2}(k), k = \overline{0, L-x_2}, \quad (9, \text{в})$$

$$R_{a_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^{\vartheta}\left(W_{i+k}^{\vartheta}\right)^* + \sum_{i=L-k+1}^{L} W_i^{\vartheta}\left(W_{i-L+K}^{\vartheta}\right)^* +$$

$$+ \sum_{i=1}^{L-x_2+\vartheta} W_i^{\vartheta}\left(W_{i+k}^{\vartheta}\right)^* \le R'_{a_2}(k); k = \overline{0, L-x_2}, \qquad (9, \text{г})$$

где $R'_{a_1}(k)$ и $R'_{a_2}(k)$ – различные реализации ПФАК, задаваемые при синтезе сигналов.

В случае размытости по ПФВК и СФВК в интервале Δx, определяемого как

$$L - x_2 \le \Delta x \le L + x_1,$$

размытость может быть задана совокупностью систем нелинейных неравенств

$$R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^q\left(W_{i+k}^{\vartheta_1}\right)^* + \sum_{i=L-k+1}^{L} W_i^q\left(W_{i-L+K}^{\vartheta_2}\right)^* + \sum_{L=1}^{L-K} W_i^p \times \left(W_{L+k}^{\vartheta_2}\right)^* +$$

$$+ \sum_{i=L-K+1}^{L} W_i^p\left(W_{i-L+K}^{\vartheta_3}\right)^* + \sum_{i=1}^{L-K} W_i^r \times \left(W_{i+K}^{\vartheta_3}\right)^* \le R'_{b_2}(k); k = \overline{0, L+x}, \qquad (10, \text{а})$$

$$R'_{b_1}(k) \le \sum_{i=\delta}^{L-K} W_i^q\left(W_{i+k}^{\vartheta_1}\right)^* + \sum_{i=L-k+1}^{L} W_i^q\left(W_{i-L+K}^{\vartheta_2}\right)^* + \sum_{L=1}^{L-K} W_i^p \times \left(W_{L+k}^{\vartheta_2}\right)^* +$$

$$+ \sum_{i=L-K+1}^{L} W_i^p\left(W_{i-L+K}^{\vartheta_3}\right)^* \le R'_{b_2}(k); k = \overline{0, L+x}, \qquad (10, \text{б})$$

$$R'_{b_2}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q * (W_i^{\vartheta_1} + k)^* \le R_{b_2}(k), k = \overline{0, L-x_2}, \qquad (10, \text{в})$$

$$R'_{b_1}(k) \le \sum_{i=L-\delta}^{L-K} W_i^q\left(W_{i+k}^{\vartheta_2}\right)^* + \sum_{i=L-k+1}^{L} W_i^q\left(W_{i-L+K}^{\delta_2}\right)^* + \sum_{i=1}^{L-x_2+\delta} W_i^p\left(W_{i+k}^{\vartheta_2}\right)^* \le$$

$$\le R'_{b_2}(k), k = \overline{0, L-x_2} \qquad (10, \text{г})$$

Таким образом, условие, которое должно выполняться для синтезируемой системы сигналов W_m^q, может быть сформулировано следующим образом: словарь $\{W_m^q\}$ удовлетворяет совокупности систем нелинейных параметрических неравенств (9) – (10), т.е. словарь $\{W_m^q\}$ обладает в интервалах Δx и Δy разностью по длительности и цикловой частоте.

4. В каждом из М словарей существуют сигналы $W_{m_1}^{q_1}$ и $W_{m_2}^{q_2}$, авто- и взаимная свертка которых удовлетворяет совокупности неравенств вида (1) и (2).

5. Закон формирования каждого из сигналов W_m^q может быть определен при перехвате не менее L сигналов, то есть – W_m^q обладает идеальной структурной скрытностью.

6. Апериодическая нормированная автосвертка W_m^q удовлетворяет системе нелинейных неравенств:

$$r_{a_1}^q(l) \le \sum_{i=1}^{L-m} W_i^q\left(W_{i+1}^q\right)^* \le r_{a_2}^q(l);\ l = \overline{1, L},\ m = \overline{1, L}, \qquad (11)$$

где $r_{a_1}^q(l)$ и $r_{a_2}^q(l)$ – заданные реализации АФАК.

7. Апериодическая взаимная свертка удовлетворяет двум системам нелинейных параметрических неравенств

$$r_{b_{1,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^q \left(W_{i+1}^q\right)^* \le r_{b_{1,2}}^{qp}(l);$$

$$l = \overline{1,L},\ m = \overline{1,L},$$

$$r_{b_{2,1}}^{qp}(l) \le \frac{1}{L-m}\sum_{i=0}^{L-m} W_i^p \left(W_{i+1}^q\right)^* \le r_{b_{2,2}}^{pq}(l);$$

$$l = \overline{1,L},\ m = \overline{1,L}. \qquad (12)$$

8. Целевая функция

$$Int(E) = \sum_{j=1}^{n} C_j S_j \qquad (13)$$

принадлежит интервалу (A,B), где S_j – значения реализаций функций системы передачи информации, описывающих законы распределения величин апериодических и периодических функций корреляции, определяющих структурную скрытность сигналов, алгоритмы построения ДС и др., а C_j – соответствующие им штрафы.

Качество услуг, которые предоставляет ТКС, предлагается оценивать, в том числе, уровнем обеспечения информационной безопасности. При этом под информационной безопасностью будем понимать способность ТКС обеспечивать защиту от уничтожения, модификации, блокирования информации, ее несанкционированной утечки или от нарушения установленного порядка ее маршрутизации. Также под информационной безопасностью следует понимать состояние защищенности систем обработки и хранения данных, при котором обеспечено сохранение конфиденциальности, целостности и доступности информации, а также других свойств информации и услуг: аутентичности, отслеживаемости, неопровержимости и надежности [1].

Решение задачи синтеза системы нелинейных дискретных сложных криптографических сигналов

Необходимость применения защищенных радиоканалов вынуждает исследователей по-новому посмотреть на режимы функционирования защищенных радиоканалов и на аспекты формирования и применения сложных сигналов. Поэтому, на наш взгляд, необходимы новые подходы и новые взгляды на процессы применения и функции непосредственно самих сложных сигналов. Основополагающим здесь, на наш взгляд, является новое понимание методов обеспечения информационной скрытности и имитостойкости, то есть функций, которые в традиционных системах возлагаются на системы и средства криптографической защиты информации. Поэтому продуктивным шагом, с точки зрения нового направления использования систем сложных сигналов, является синтез так называемых систем криптографических сигналов. Синтез таких сигналов основывается на применении ключевых данных, и при этом сигналы должны обладать: абсолютной структурной скрытностью относительно законов их формирования и смены сигналов в динамическом режиме; улучшенными ансамблевыми свойствами (существовать практически для любого значения периода, иметь значительный объем системы сигналов); необходимыми, для обеспечения требуемого значения помехоустойчивости, корреляционными свойствами. Для защищенных радиоканалов рассматриваемые системы сигналов определяются приложениями, в которых они применяются. В частности, это могут быть как отдельные сигналы или пары сигналов, так и большие множества дискретных последовательностей с необходимыми, но объективно ограниченными значениями «плотной упаковки», взаимно-корреляционными и ансамблевыми свойствами.

Под криптографическими сигналами (КС) предлагается понимать последовательности символов определенного алфавита, обладающие необходимыми ансамблевыми и корреляционными, структурными, технологическими и другими свойствами. В качестве правила по-

строения КС используются случайные или псевдослучайные процессы. КС отвечают требованиям необратимости, неразличимости, непредсказуемости, случайности [1, 4]. Применение КС, позволит улучшить показатели эффективности ТКС, в частности: помехозащищенность (помехоустойчивость приема сигналов в условиях воздействия структурных, заградительных, ретранслированных и других видов помех, скрытность функционирования) и информационную безопасность. Такие дискретные сигналы обладают необходимыми, но ограниченными (значениями «плотной упаковки»), корреляционными и ансамблевыми свойствами. При таком подходе структурная скрытность сигнала обеспечивается посредством случайности или псевдослучайности, помехоустойчивость – корреляционными свойствами синтезируемой системы сигналов, информационная безопасность ТКС обеспечивается на основе статистических свойств КС, близких к свойствам случайных последовательностей, а также использованием криптографических ключей, причем длина ключа может быть существенно меньше периода (длины) самого сигнала. Необходимо отметить особое свойство систем криптографических сигналов: возможность их восстановления в пространстве и во времени с применением ключей и ряда других параметров, которые используются в процессе синтеза сигналов.

Авторами предложен метод синтез систем сложных нелинейных криптографических сигналов, включающий следующие этапы [5]:

1. Формирование псевдослучайных последовательностей символов с использованием источников случайных (псевдослучайных) последовательностей символов.

2. Оценка статистических свойств полученных последовательностей с применением критериев и показателей качества генераторов последовательностей, определенных международными (ведомственными) стандартами FIPS PUB 140-1 [7], FIPS PUB 140-2 [8], AIS 20 [9] и AIS 31 [4], NIST 800-22 [10], NIST 800-90b [11].

3. Формирование дискретных последовательностей (ДП) символов фиксированного периода.

4. Отбор ДП, значения боковых лепестков периодической функции автокорреляции (ПФАК) которых близки к границе «плотной упаковки» [2].

5. Получение матрицы состояний взаимно-корреляционных функций всех возможных пар последовательностей, прошедших отбор по результатам предыдущего шага.

6. Обработка матрицы, заключающаяся в том, что осуществляется отбор последовательностей, удовлетворяющих границам «плотной упаковки» (предельно достижимым значениям) для соответствующих корреляционных функций.

С учетом необходимости обеспечения криптографической стойкости и структурной скрытности (сложности) криптографического сигнала, в качестве источника псевдослучайных последовательностей символов (1-й этап метода) *обоснован выбор алгоритма симметричного блочного шифрования со счетчиком: Национальный криптографический стандарт блочного симметричного преобразования ДСТУ 7624:2014, определяющий шифр «Калина» и режимы его работы для обеспечения конфиденциальности и целостности информации* [6]. В качестве альтернативы такому источнику может быть предложен источник на основе алгоритма AES (международный стандарта ISO/IEC 18033). Предпочтение при выборе отдано ДСТУ 7624:2014 с учетом следующих факторов.

Блочные симметричные шифры (БСШ) являются одним из наиболее распространенных криптографических примитивов. Кроме обеспечения конфиденциальности (шифрования) основных объемов информации, передаваемых по сети или хранимых локально, они применяются как конструктивный элемент других примитивов (функций хеширования, кодов аутентификации сообщений, генераторов псевдослучайных последовательностей и пр.). Значение этого криптографического преобразования подчеркивает и ряд международных конкурсов, таких как AES, NESSIE, CRYPTRACK, которые были ориентированы на разработку блочного шифра (как основной цели или в составе набора перспективных решений).

Национальный стандарт поддерживает размер блока и длину ключа шифрования 128, 256 и 512 бит (длина ключа равна размеру блока или в два раза превышает его), обеспечивая нормальный, высокий и сверхвысокий уровень стойкости (сейчас это единственный в мире стандарт блочного шифрования, поддерживающий 512-битовые симметричные ключи). Разные варианты стандарта обеспечивают гибкость выбора параметров для разработчиков систем криптографической защиты, что позволяет получить как наивысший уровень быстродействия, так и наибольший запас стойкости преобразования. Высокоуровневая конструкция использует хорошо исследованную Square-подобную SPN-структуру, применяемую в алгоритмах AES/Rijndael, Whirlpool, «Стрибог» и многих других. Цикловое преобразование построено на базе таблиц подстановки (S-блоков) и умножения на МДР-матрицу над конечным полем, обеспечивая необходимые криптографические свойства. Применение именно такой конструкции позволяет обеспечить доказуемую стойкость по отношению к дифференциальному, линейному и другим видам криптоанализа, одновременно обеспечивая эффективную реализацию для широкого спектра программных и программно-аппаратных платформ. При выборе размера МДР-матрицы был принят во внимание размер кэша L1 современных и перспективных процессоров, что позволило оптимизировать быстродействие программной реализации шифра. Стандарт Украины обеспечивает наибольшую нелинейность булевых функций, что дает дополнительный запас стойкости по отношению к линейному криптоанализу. Кроме того, по нашему мнению, стандарт блочного симметричного преобразования ДСТУ 7624:2014 относится к постквантовым алгоритмам, т.е. – он будет обеспечивать (при выборе соответствующих параметров) криптографическую стойкость против атак с применение квантовых компьютеров.

В табл. 1 – 4 представлена реализация этапов предложенного метода синтеза нелинейных дискретных КС. В табл. 1 приведены последовательности символов с периодом N=32, полученные на выходе криптографического алгоритма «Калина» и прошедшие процедуру тестирования на соответствие требованиям стандарта NIST 800-22 [25] (в соответствии с шагом 2 метода). В табл. 1 указано также число символов {1,0} в последовательности. В табл. 2 – 3 приведены матрицы состояний взаимно-корреляционных функций (ПФВК) (значения максимальных и минимальных выбросов взаимно-корреляционных функций) некоторых пар псевдослучайных последовательностей и периодических функций автокорреляции последовательностей (ПФАК), полученных при реализации шагов 1–2 предлагаемого метода. В табл. 4 представлены (в соответствии с шагом 5 метода) результаты отбора пар последовательностей. Другими словами, в табл. 4 приведены номера пар и собственно пары последовательностей, боковые пики взаимно-корреляционной функции которых удовлетворяют границе «плотной упаковки». Целесообразность отбора сигналов, обладающих хорошими автокорреляционными свойствами в периодическом режиме (ПФАК) для синтеза системы сигналов (с целью их использования в различных приложениях телекоммуникационных систем) обусловлена рядом факторов.

Применение широкополосных сигналов (ШПС) позволяет повысить помехоустойчивость телекоммуникационных систем (ТКС) при воздействии структурных (взаимных) и организованных помех. Реальная помехоустойчивость будет ниже потенциальной. Причинами снижения помехоустойчивости при вхождении в синхронизм и при различении сигналов является наличие боковых пиков корреляционных функций (КФ). В качестве критерия выбора класса ДС, как правило, ориентируются на критерий минимума взаимных помех (минимаксный критерий). Такой критерий подразумевает построение ансамблей сигналов объема M, манипулированных ДП, как можно заметнее отличающихся друг от друга при возможных циклических сдвигах. Минимизация уровня боковых лепестков автокорреляционной функции (АКФ) имеет наибольшее значение при конструировании сигнала для таких приложений как измерение времени запаздывания, временное разрешение и др. Предпочтительными являются кодовые последовательности с наименьшим значением максимального бокового лепестка. Таким образом, требования, предъявляемые наилучшему сигналу, могут быть

сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей длины N с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка апериодической АКФ. Сформулированная выше оптимизационная задача, как и многие другие задачи дискретной оптимизации, не имеют общего аналитического решения, и типичной процедурой ее выполнения является осуществление исчерпывающего поиска. Гарантированное нахождение глобально оптимального (т.е. имеющего минимально возможное значение бокового лепестка АКФ $p_{a,\max} > 2/N$ при заданном N) бинарного кода может быть осуществлено только путем полного перебора возможных комбинаций. При этом вычислительный объем, необходимый для такой оптимизации, экспоненциально возрастает с увеличением длины N и становится нереализуемым при величинах N, превышающих 50 [12]. *Очевидно, что нахождение оптимальных бинарных последовательностей большой длины практически нереализуемо. Тогда указанная выше задача оптимизации может быть сформулирована так: найти бинарный код с удовлетворительно малым уровнем периодического бокового лепестка* $p_{a,\max}$. *Общая идея алгоритмов, направленных на решение этой задачи, состоит в предварительном отборе некоторого ограниченного множества последовательностей, которое кажется многообещающим в плане корреляционных свойств, и последующем поиске кода с минимальным значением* $p_{a,\max}$ *только среди последовательностей, вошедших в указанное множество.* Одним из примеров подобной стратегии является использование соотношения (14), связывающего апериодическую АКФ со своим периодическим аналогом.

Обозначая через $p_{p,\max}$ максимальный боковой лепесток периодической АКФ: $P_{p,\max} = \max_{m=1,2,\ldots n-1}\left\{\left|P_p(m)\right|\right\}$ и используя неравенство

$$\max\left\{|x+y|\right\} \le \max\left\{|x|+|y|\right\} \le \max\left\{|x|\right\} + \max\left\{|y|\right\},$$

приходим к оценке $P_{p,\max} \le P_{a,\max}$ или:

$$P_{a,\max} \ge \frac{1}{2} P_{p,\max}. \qquad (14)$$

Из (14) следует, что последовательности с хорошей апериодической АКФ могут быть найдены среди последовательностей с хорошей периодической АКФ. Интерес к последовательностям с хорошей периодической АКФ не ограничивается только их ролью исходного материала для построения хороших апериодических последовательностей. Существует множество приложений, основанных на использовании периодических дискретных сигналов (CW – локация, навигация, пилотный канал и канал синхронизации в мобильных системах радиосвязи, радарные и сонарные системы с непрерывным излучением и т.п.), что предопределяет важность периодической АКФ (ПАКФ) в отношении системных характеристик. Кроме того, в теории систем сигналов известен ряд интегральных равенств, устанавливающих соотношения авто- и взаимнокорреляционных функций сигналов [13]. Использование данных равенств приводит к полезным вычислительным алгоритмам и методам построения последовательностей. В частности, показано, что среднее значение квадрата модуля функции взаимной корреляции сигналов x и y равно среднему значению произведения их автокорреляционных функций. Фактически это означает, что сигналы, обладающие хорошими автокорреляционными свойствами будут обладать и хорошими свойствами взаимнокорреляционных функций. С учетом приведенных соотношений в предложенном методе синтеза систем КС введен шаг, реализующий отбор сигналов, обладающих улучшенными автокорреляционными свойствами.

Таблица 1

Номер	Последовательность	1	0
1	01111011000011010001110001111010	17	15
2	00110000000100010111101000010111	13	19
3	00000001010101100100111100100101	13	19
4	00101001000000010010011100100000	9	23
5	00111001010010110010110001110010	15	17
6	00010100010001100011100000011001	11	21
7	00000100011110100011100100111111	16	16
8	01001001001010000010111100001010	12	20
9	01011101001001010001001100110111	16	16
10	00110000000111100011001101010111	15	17
11	00011100000000111001001100011 0010	12	20
12	00100010000010100101010100011001	11	21
13	00111110001101100011110000101101	17	15
14	01011011010111000011101110010110	18	14
15	00011101010101110011101100100000	15	17
16	01111101001001000111010100000100	14	18

Таблица 2

Номер	Значения максимальных боковых выбросов пар
1	32 -8 -12 -8 16 -12 18 10 -14 12 -18 12 -16 -10 -12 -10 8 -14 -14 12 -14 20 8 14 16 -22 8 10 -10 -14 20 16
2	8 32 -12 16 -12 12 -14 14 10 16 -10 12 -12 -14 -12 -14 16 14 14 16 14 -12 20 14 12 10 12 14 -14 14 12 16
3	12 12 32 12 -12 12 -14 14 18 12 14 12 -12 -10 12 14 8 18 14 -12 10 16 12 10 12 -10 16 14 10 10 -12 16
4	-8 16 12 32 12 12 14 14 -10 12 14 12 -12 -10 12 14 16 10 18 16 -14 12 16 14 16 -14 12 14 14 6 -8 16
5	16 -12 12 12 32 12 18 14 14 12 14 12 12 14 12 10 12 -18 18 -12 -14 12 8 14 8 14 16 14 14 14 12 12
6	-12 12 12 12 12 32 14 10 -14 12 14 16 12 -14 12 -10 12 -14 14 12 -10 16 -12 14 12 -14 12 14 -14 14 12 16
7	18 -14 -14 14 18 14 32 -12 -12 -14 -12 -14 14 -12 14 12 14 -12 -12 -14 8 14 14 16 14 -12 10 -12 16 -12 -14 14
8	-10 14 14 14 -14 10 12 32 12 10 12 14 -14 -16 -10 -12 10 16 16 14 -16 14 -14 12 14 -12 10 16 -12 -12 14 14
9	-14 -10 18 10 14 -14 -12 -12 32 14 12 -14 14 -20 10 12 10 16 12 10 -16 -10 14 16 10 -12 18 -16 12 -12 -14 -10

Таблица 3

№	Значения ПФАК сигналов
1	32 4 -4 -8 -12 0 8 0 8 4 -8 -4 -4 4 4 0 -12 0 4 4 -4 -4 -8 4 8 0 8 0 -12 -8 -4 4
2	32 4 4 0 4 0 -12 0 0 0 -8 -4 8 0 0 0 12 0 0 0 8 -4 -8 0 0 0 -12 0 4 0 4 4
3	32 -4 4 4 0 -4 4 -4 4 4 4 -8 4 -4 0 0 -4 0 0 -4 4 -8 4 4 4 -4 4 -4 0 4 4 -4
4	32 4 4 12 4 8 0 0 12 -4 0 12 0 12 8 4 12 4 8 12 0 12 0 -4 12 0 0 8 4 12 4 4
5	32 -4 -8 -4 -8 8 4 -4 -4 8 -4 4 0 -4 4 -4 4 -4 4 -4 0 4 -4 8 -4 -4 4 8 -8 -4 -8 -4
6	32 4 -4 -8 8 0 4 0 4 8 8 0 -8 4 8 8 -4 8 8 4 -8 0 8 8 4 0 4 0 8 -8 -4 4
7	32 8 0 -4 -4 -8 -8 -4 0 4 -4 0 -4 0 4 4 0 4 4 0 -4 0 -4 4 0 -4 -8 -8 -4 -4 0 8
8	32 -4 4 8 -12 0 4 -8 8 0 4 8 0 0 4 -4 8 -4 4 0 0 8 4 0 8 -8 4 0 -12 8 4 -4
9	32 -8 -4 4 8 -8 4 0 4 0 0 -8 4 -8 0 -8 8 -8 0 -8 4 -8 0 0 4 0 4 -8 8 4 -4 -8

Предложенный метод синтеза сложных нелинейных дискретных криптографических сигналов, использующий случайные или псевдослучайные процессы, позволяет формировать большие ансамбли дискретных последовательностей практически любого периода с заданными, но физически реализуемыми, значениями боковых лепестков функций авто- и взаимной и стыковой функции корреляции в периодическом и апериодическом режимах работы, а также статистическими характеристиками корреляционных функций, не уступающих аналогичным характеристикам лучших линейных классов сигналов. Так, для периода последовательности N=63 число пар криптографических дискретных последовательностей, удовлетворяющих установленному граничному значению максимальных боковых лепестков ПФВК – 17, составляет 12 214 869.

Таблица 4

Номер	Значение ПФВК / Сигналы
1	0 0 0 -4 0 0 -8 0 0 0 0 -8 -8 -4 4 8 8 0 -4 -4 -8 -4 4 4 8 -4 0 0 8 0 -4 4 Сигналы (1, 2): 01111011000011010001110001111010; 11000000010001011110100001011 7
2	4 4 0 4 -8 -8 4 -8 0 4 -8 4 -8 -4 4 0 -4 0 -8 8 8 0 0 -4 0 -4 -4 4 4 -4 0 -8 Сигналы (1, 4): 01111011000011010001110001111010 01010010000000010010011100100000
3	4 0 -4 -4 -4 0 4 0 4 4 0 0 -4 0 0 4 0 -4 0 -4 -4 -4 0 0 8 0 4 0 -8 -4 -4 4 Сигналы (1, 17): 01111011000011010001110001111010 00100001010111100010000001011110
4	4 8 -8 -4 -4 -8 8 4 4 4 -4 0 4 -4 4 4 4 0 -8 -4 0 -4 0 4 4 0 -4 -4 -4 -8 4 4 Сигналы (1, 23): 01111011000011010001110001111010 00111001001101110011000000110101
5	-4 4 0 4 0 -4 0 -4 -4 8 4 4 0 -4 -4 0 0 0 8 4 0 -8 0 -8 4 -4 4 8 4 -8 -4 -4 Сигналы (1, 27): 01111011000011010001110001111010 00100101010101110010011001000111
6	4 0 0 0 4 8 -4 4 4 -8 -4 -4 0 0 4 0 4 4 4 4 4 8 0 4 0 -4 -4 -4 4 -4 8 0 Сигналы (3, 17): 00000001010101100100111100100101 00100001010111100010000001011110
7	4 4 0 0 4 -4 4 0 4 4 0 -4 4 -4 -8 -4 8 4 0 0 -8 0 -4 4 4 0 0 4 0 -4 -4 8 Сигналы (24, 30): 00110101001100110011101000001001 00001110010101110001110000110001

Для представителя класса линейных последовательностей – последовательностей с трехуровневой функцией взаимной корреляции (множеств Голда, являющегося оптимальным с точки зрения функций взаимной корреляции сигналы [14]), число пар сигналов, удовлетворяющих данной границе, составляет – 975. Превышение объема криптографических сигналов над ансамблем, составленного из М-последовательности, составляет более чем 10^7 раз. Для периода последовательности N=1023 число пар криптографических дискретных последовательностей, удовлетворяющих установленному граничному значению для боковых лепестков функций взаимной корреляции (ФВК) – 100, составляет 5 293 538, тогда как для представителя класса линейных последовательностей – М-последовательностей число пар, удовлетворяющих данной границе, составляет – 435, т.е. превышение объема системы сигналов составляет более чем 10^5 раз. Кроме того, КС являются самосинхронизирующимися.

При незначительном снижении требований к граничному значению максимального бокового пика ВКФ, в соответствии с которым осуществляется отбор сигналов (по сути, – снижение помехоустойчивости приема), могут быть существенно улучшены показатели имитозащищенности функционирования ТКС. Так, для периода последовательности N=127, увеличение значения границы на 1,2 Дб позволит увеличить объем ансамбля с М=11610 при границе $R_{бmax}$=17, до 9 006 648 сигналов, при граничном значении $R_{бmax}$=27, т.е. более чем в 700 раз.

Таким образом, варьируя граничные значения уровня боковых лепестков соответствующей функции корреляции (с учетом требований, предъявляемых к телекоммуникационной системе с точки зрения помехоустойчивости приема сигналов и имитозащищености системы), можно решить задачи достижения необходимых значений помехоустойчивости приема сигналов, имитостойкости и информационной скрытности сообщений абонентов телекоммуникационной системы.

Выполненные расчеты и имитационное моделирование свидетельствуют о том, что значения максимальных боковых выбросов корреляционных функций КС, а также статистические характеристики данного класса сигналов не уступают соответствующим характеристикам линейных М-последовательностей [15].

Помехозащищенность ТЛК системы и одна из ее составляющих – структурная скрытность системы в значительной степени определяются структурными или статистическими свойствами сигналов-переносчиков данных в системе. Для исследования указанных свойств КС мы использовали методику тестирования генераторов случайных (псевдослучайных) последовательностей, определенную стандартом NIST 800-22. Результаты тестирования приведены в табл. 5 (приведен фрагмент результатов моделирования). Как следует из данных табл. 5, статистические свойства нелинейных КС с точки зрения значений оцениваемых вероятностей (их 189) по 16 тестам данной методики находятся в пределах допустимых значений. А это, в свою очередь, означает, что КС удовлетворяют требованиям, предъявляемым к псевдослучайным последовательностям: непредсказуемости следования символов, необратимости, случайности, равновероятности, независимости, непредсказуемости, неразличимости и др. По сути, КС не отличимы от случайных последовательностей. Таким образом, использование НС в качестве физического переносчика данных позволит повысить структурную и информационную скрытность (криптостойкость) ТКС.

Таблица 5

№	c1	c2	c3	c4	c5	c6	c7	c8	c9	c10	Вер.	Результат тестирования	Название теста
1	14	5	11	10	10	12	7	14	8	9	0,574903	0,99	Frequency
2	10	8	10	11	12	5	6	13	14	11	0,574903	0,99	BlockFrequency
3	13	6	5	14	18	10	9	5	12	8	0,058984	0,99	CumulativeSums
4	14	9	4	10	8	8	15	15	12	5	0,122325	1	CumulativeSums
5	9	8	8	12	10	10	14	7	8	14	0,759756	1	Runs
6	8	14	15	8	8	7	9	12	10	9	0,657933	1	LongestRun
7	12	10	11	7	11	7	6	15	11	10	0,678686	1	Rank
8	10	7	9	12	9	11	14	10	8	10	0,935716	1	FFT
9	10	10	6	10	7	10	11	9	9	18	0,419021	1	NonOverlappingTemplate
10	11	7	9	12	9	14	9	8	11	10	0,924076	0,98	NonOverlappingTemplate
11	17	11	14	10	10	6	10	7	7	8	0,319084	1	NonOverlappingTemplate
12	16	9	7	8	6	7	10	13	9	15	0,275709	0,98	NonOverlappingTemplate
13	12	6	7	8	11	7	12	10	13	14	0,616305	0,99	NonOverlappingTemplate
14	15	15	10	9	7	11	6	9	7	11	0,455937	0,98	NonOverlappingTemplate
15	11	9	13	7	11	14	9	12	8	6	0,719747	1	NonOverlappingTemplate
16	13	12	12	9	12	12	7	8	8	7	0,816537	0,97	NonOverlappingTemplate
17	11	11	14	8	10	8	10	10	9	9	0,971699	1	NonOverlappingTemplate
18	8	12	11	11	12	7	12	12	6	9	0,851383	1	NonOverlappingTemplate
19	9	11	10	12	7	11	8	16	7	9	0,678686	1	NonOverlappingTemplate
20	14	10	13	10	12	12	6	7	11	5	0,494392	0,98	NonOverlappingTemplate
21	15	11	10	8	12	9	13	9	5	8	0,595549	0,95	NonOverlappingTemplate
22	9	5	14	10	7	6	14	9	13	13	0,334538	1	NonOverlappingTemplate
23	12	7	7	11	11	5	14	12	11	10	0,637119	0,99	NonOverlappingTemplate
24	10	12	12	11	15	10	7	10	6	7	0,657933	1	NonOverlappingTemplate
25	12	8	14	9	12	12	6	8	11	8	0,759756	0,98	NonOverlappingTemplate
26	6	7	7	10	14	7	8	15	15	11	0,249284	0,99	NonOverlappingTemplate
27	12	7	13	6	11	10	10	16	7	8	0,455937	0,98	NonOverlappingTemplate
28	12	9	9	12	9	10	6	7	17	9	0,474986	0,98	NonOverlappingTemplate
29	5	8	9	7	11	11	14	10	16	9	0,401199	1	NonOverlappingTemplate
30	6	7	12	9	9	12	12	9	12	12	0,851383	1	NonOverlappingTemplate
189	9	6	13	9	11	11	10	6	13	12	0,759756	0,99	LinearComplexity
											84,82113	186,0039	

Для практического использования нелинейных дискретных криптографических сигналов в целях улучшения общесистемных показателей эффективности систем, реализующих динамические принципы передачи данных, необходимо формировать большие массивы сигнальных конструкций и осуществлять смену соответствия бит сообщения – сложный сигнал в установленное время по закону специальных управляющих последовательностей. В таких условиях становятся критичными, в том числе, вопросы разработки методов синтеза и анализа (исследования) систем дискретных сложных сигналов с необходимыми свойствами, методы и средства их формирования и обработки. При этом методы и средства синтеза таких систем сигналов должны обеспечивать необходимую производительность.

Отметим, что в ряде работ, посвященных синтезу и выбору дискретных последовательностей, приводятся верхние и нижние оценки распределения максимальных и минимальных лепестков функций авто- и взаимной корреляции [2, 13]. Нахождение дискретных последовательностей с необходимыми характеристиками корреляционных функций сводится, по сути, к перебору всех возможных вариантов последовательностей, принадлежащих некоторому множеству, и отбору тех последовательностей, которые удовлетворяют известным оценкам. При этом вычислительная сложность таких методов оказывается значительной.

Оптимизация метода синтеза криптографических сигналов

Известно, что существует большая группа методов улучшенного перебора, объединенных общим названием «метод ветвей и границ» [16]. Основная идея таких методов состоит в использовании конечности множества решений и в замене их полного перебора сокращенным (направленным) перебором. Таким образом, суть методов улучшенного перебора состоит в нахождении оптимальных решений различных задач оптимизации, в частности дискретной и комбинаторной оптимизации. Для реализации методов используют процедуру нахождения оценок (границ). Процедура нахождения оценок заключается в установлении границы для решения задачи нахождения допустимых значений. Если оценка подмножества (параметра) окажется больше, чем граница значений функции подмножества, то значение исключается из дальнейшего рассмотрения. Реализация описанного выше общего принципа имеет определенные сложности, определяемые спецификой решаемой задачи оптимизации. Применительно к сформулированной выше задаче синтеза систем нелинейных дискретных криптографических сигналов указанный метод оптимизации направлен на реализацию процедуры «ветвления», состоящей в разбиении множества допустимых значений переменной x (шага сканирования) на подобласти (подмножества) меньших размеров. Полученные подобласти образуют дерево, называемое деревом поиска или деревом ветвей и границ. Узлами этого дерева являются построенные подобласти (подмножества множества значений переменной x).

В ходе исследований авторами получен усовершенствованный метод синтеза нелинейных криптографических последовательностей, основанный на использовании сокращенного (направленного) перебора на основе применения метода «ветвей и границ», посредством исключения из дальнейшего рассмотрения подобластей (реализаций дискретных последовательностей, имеющих значение боковых лепестков функции корреляции, превышающих установленную исследователем границу).

Задача выбора дискретных последовательностей, удовлетворяющих известным граничным оценкам, может быть записана в виде аналитических выражений и ограничений:

$$Ra_1^1(l) \le \sum_{i=1}^{L} W_i^1 (W_{i+l}^{\ 1})^* \le Ra_2^1(l), l = \overline{0, L'}, \qquad (15)$$

$$Ra_1^2(l) \le \sum_{i=1}^{L} W_i^2 (W_{i+l}^{\ 2})^* \le Ra_2^2(l), L' = \frac{L-1}{2},$$

если L – нечетное,

$$Ra_1^j(l) \le \sum_{i=1}^{L} W_i^j (W_{i+l}^j)^* \le Ra_2^j(l), L' = \frac{L}{2},$$

если L – четное,

$$Ra_1^N(l) \le \sum_{i=1}^{L} W_i^N (W_{i+l}^N)^* \le Ra_2^N(l),$$

где $Ra_1^i(e), Ra_2^i(e)$ – граничные значения боковых лепестков ФАК, L – период последовательности W_i^{υ}, $\upsilon = \overline{1, N}$.

Теорема 1. Пусть максимальные (минимальные) значения реализаций функций $Ra_1^1(l)$ и $Ra_2^1(l)$ в (1) являются таковыми, что величина δ, определенная как

$$\delta = \left| Ra_1'(l) - Ra_1(l) \right| \text{ либо } \delta = \left| Ra_2'(l) - Ra_2(l) \right|, \tag{16}$$

$\delta \ne 0,1,2,...P-1,P$ больше P, а W^j – сигнал определен над полем $GF(P)$ или над кольцом чисел по модулю P, тогда множество значений циклической свертки (функции автокорреляции (ФАК)) $Ra^Z(l)$ может принадлежать интервалу

$$(\min Ra_1(l), \max Ra_2(l)), \tag{17}$$

по крайней мере, при "отбрасывании" r последних и "добавлении" r первых символов сигнала W, где

$$r = \frac{\delta}{P}, \text{ если } \delta \mid P \text{ и } r = \frac{\delta + t}{P}, \text{ если } \delta \ne P.$$

Доказательство теоремы 1.

Предположив, что $Wa_1'(l) < \min Ra_1(l)$, рассмотрим ФАК сигнала. Так как символы W^j определены в кольце чисел по модулю P, либо над полем $GF(P)$, то при «отбрасывании» W_1 и «добавлении» W_{L+1}, Ra_1' возрастает по крайней мере на P. Аналогично при «отбрасывании» символа W_2 и «добавлении» W_{L+2}, Ra_1' возрастает не более чем на P. И, таким образом, после r «отбрасываний» $\min Ra_1'(l)$ и «добавлений» r символов каждый с максимальным расстоянием P

$$\min Ra'(l) \ge Ra_1'(l) + P \cdot r, \tag{18}$$

поэтому

$$r' \ge \frac{\min Ra'(l) - Ra_1'(l)}{P}. \tag{19}$$

В действительности, величина $r > r'$, а вероятность того, что за r шагов $Ra'(l)$ станет равной значению $\min Ra'(l)$ достаточно мала.

Рассмотрим второй случай, когда

$$Ra_2'(l) > \max Ra_2(l).$$

Рассуждая аналогично вышеприведенному, после r шагов получим

$$\max Ra_2(l) < \max(Ra_2'(l) - P \cdot r)$$

и

$$r \ge \frac{\max Ra_2'(l) - Ra_2(l)}{P} \tag{20}$$

С учетом (18) и (20), дополняя их величиной t, но так, чтобы $(\delta + t)$ являлось делителем P, имеем $r = \frac{\delta}{P}$, если $\delta \mid P$ и $r = \frac{|\delta| + t}{P}$, если δ не делит P.

Следствие теоремы 1. Если $W_i \in GF(P)$, то $r = \frac{\delta}{2}$, если δ – четное и $r = \frac{\delta+1}{2}$, если δ – нечетное.

Подчеркнем, что теорема 1 и ее следствие имеют важное значение, так как из них следует, что за $r < r'$ «отбрасываний» и r «дополнений» $\min Ra'(l)$, и $\max Ra'_2(l)$ не могут попасть в интервал $(\min Ra_1(l), \max Ra_2(l))$.

В ходе исследований было проведено имитационное моделирование приведенного выше метода синтеза последовательностей. Были выполнены оценки производительности (быстродействия) такого метода. В качестве источника нелинейных криптографических сигналов был использован стандарт шифрования данных Украины «Калина». В процессе моделирования с помощью представленного выше метода были выбраны последовательности с различным периодом следования символов (от 256 до 1024), функции автокорреляции которых отвечают границе «плотной упаковки» для указанных периодов. Анализ результатов исследований показал, что данный метод обеспечивает выигрыш в производительности синтеза систем нелинейных дискретных криптографических последовательностей с заданными корреляционными свойствами от 40 до 60 % по отношению к методу синтеза системы сигналов, основанному на переборе всех возможных вариантов последовательностей. При реализации рассматриваемого метода возможны пропуски (потери) в нахождении лучших с точки зрения корреляционных свойств сигналов. Но, как показали исследования, процент таких потерь – незначителен, и для указанных периодов составляет не более 8 %.

В настоящее время разработано программное и математическое обеспечение, реализующее методы синтеза и исследования свойств систем нелинейных криптографических сигналов, которое практически готово к возможному использованию в составе опытных образцов и элементов современных цифровых коммуникационных средств и позволяет: генерировать нелинейные криптографические сигналы для практически любого периода; определять значения минимальных и максимальных боковых выбросов различных корреляционных функций; сравнивать полученные значения с известными, потенциально достижимыми границами для соответствующих корреляционных функций; присваивать реализациям синтезированных последовательностей, а также параметрам, используемым для синтеза сигналов, уникальные идентификаторы (специальные радиоданные), которые необходимы для оптимальной обработки сигналов; рассчитывать статистические характеристики различных корреляционных функций синтезированных сигналов; проводить исследования ансамблевых характеристик синтезированных сигналов.

Применение нелинейных дискретных сложных криптографических сигналов в телекоммуникационных системах

Анализ приведенных свойств нелинейных КС показывает, что данный класс сигналов может найти широкое применение в различных системах передачи в качестве: физического переносчика данных пользователей ТКС; синхропоследовательностей, на этапе решения одной з задач теории оптимального приема – обнаружения сигнала; производящего сигнала, при построении производных ортогональных сигналов (ПОС). В частности, в стандарте UMTS (стандарт третьего поколения систем с кодовым разделением каналов – CDMA) в качестве кода первичной синхронизации используется бинарная линейная последовательность длины 256, обладающая апериодическими боковыми лепестками вплоть до ¼. Это значительные боковые пики.

В качестве альтернативы указанным последовательностям могут быть предложены нелинейные классы сигналов, в частности КС. Исследования показали [15], что за счет улучшенных корреляционных свойств нелинейных КС выигрыш (с точки зрения помехоустойчивости приема сигналов при использовании таких сигналов в качестве синхропоследовательностей (СП)) по сравнению с использованием последовательностей, применяемых в стандарте UMTS, составляет 3 дБ.

Результаты исследования характеристик ПФВК ПОС на основе КС (значения максимальных боковых лепестков, их количество, статистические характеристики функции корреляции) показывают, что число пар сигналов (период сигнала N=64), для которых значения максимальных боковых лепестков R_{max} не превышают 17 (это так называемая граница «плотной упаковки», достигаемая в классе лучших с точки зрения ПФВК последовательностей с трехуровневой ПФВК), составляет 604 пары, что составляет около 30 % из общего числа возможных сочетаний пар сигналов. Число пар сигналов, для которых значения R_{max}, не превышают 20 – 1577 пар сигналов, что составляет 77 %. При границе R_{max}=25 максимальное количество отобраных пар сигналов – 1984, что составляет 96,8 % от общего числа. Такие значения R_{max} имеют место для последовательностей, получивших наибольшее распространение в современных телекоммуникационных системах, – М-последовательности.

Выводы

Применяемые в ТКС способы информационного обмена, основанные на фиксированном соответствии: бит сообщения (m бит) – сигнал (2^m сигналов) в информационном канале и использовании (в течение продолжительного времени) в канале синхронизации одного и того же широкополосного сигнала (причем используемые сигналы построены с применением линейных законов), не позволяют достичь необходимых значений помехозащищенности и информационной безопасности функционирования телекоммуникационной системы.

Комплексное решение проблемы обеспечения помехозащищенности и информационной безопасности функционирования ТКС может быть достигнуто, в том числе, на основе реализации динамического режима передачи информации, при котором соответствие: бит сообщения – сигнал меняется с течением времени по закону, предсказание которого возможно с вероятностью, не превышающей допустимого в системе значения, и применения сигналов с необходимыми корреляционными, ансамблевыми, структурными свойствами. При этом системы сигналов должны основываться на нелинейных правилах построения.

Предлагаемые в статье сложные нелинейные дискретные криптографические сигналы, в отличие от известных классов сигналов, используемых в различных приложениях ТКС, могут быть синтезированы для любых значений периода дискретных сигналов. Синтез данного класса сигналов основывается на ограничениях, связанных с граничными значениями функций авто- и взаимной корреляции сигналов в периодическом и апериодическом режимах передачи информации.

Объем системы нелинейных криптографических сигналов (мощность кодирования) определяется, во-первых, требованиями, обусловленными применением данного класса сигналов (обнаружение и измерение параметров сигнала, режим передачи данных пользователей и др.) и, во-вторых, требованиями, предъявляемыми к системе с точки зрения таких показателей эффективности функционирования телекоммуникационной системы, как помехоустойчивость приема сигналов, информационная скрытность и имитостойкость системы. Пользователю (владельцу) системы, исходя из указанных ограничений, необходимо принимать компромиссные решения о выборе того или иного ансамбля нелинейных криптографических сигналов с необходимыми свойствами.

В статье в общем виде сформулирована и решена задача синтеза нелинейных дискретных сложных криптографических сигналов, ансамблевые, корреляционные свойства которых могут быть установлены в зависимости от требований, предъявляемых к помехозащищенности и информационной безопасности ТКС.

Предложен ряд положений оптимизации синтеза сложных нелинейных криптографических дискретных сигналов с необходимыми свойствами с помощью метода ветвей и границ. Применение таких сигналов позволит повысить помехозащищенность, скрытность и информационную безопасность функционирования телекоммуникационных систем.

Список литературы: 1. *Горбенко, І.Д., Горбенко, Ю.І.* Прикладна криптологія. Теорія. Практика. Застосування : монографія / І.Д. Горбенко, Ю.І Горбенко. – Харків : Форт, 2012. – 880 с. 2. *Варакин, Л. Е.* Системы связи с шумоподобными сигналами / Л. Е. Варакин. – М. : Радио и связь,1985. – 384 с. 3. *Замула, А.А.* Перспективы применения нелинейных дискретних сигналов в современных телекоммуникационных системах и сетях / Замула А.А., Семенко Е.А // Системи обробки інформації. – Х. : ХУПС, 2015. – Вип. 5 (130). – С. 129–134. 4. *Application* Notes and Interpretation of the Scheme (AIS) 31. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 2001. 5. *Gorbenko, I.D., Zamula, A.A., Semenko, Ye.A.* Ensemble and correlation properties of cryptographic signals for telecommunication system and network applications // Telecommunications and Radio Engineering. – Volume 75, 2016 Issue 2. pages 169–178. 6. *ДСТУ 7624:2014.* Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. : Мінекономрозвитку України, 2015. 7. *Federal* Information Processing Standards Publication (FIPS PUB) 140-1. Security requirements for cryptographic modules. NIST, 1994. 8. *Federal* Information Processing Standards Publication (FIPS PUB) 140-2. Security requirements for cryptographic modules. NIST, 1999. 9. *Application* Notes and Interpretation of the Scheme (AIS) 20. Functionality classes and evaluation methodology for physical random number generators. Certification body of the BSI in context of certification scheme. BSI, 1999. 10. *NIST 800-22* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, 2000. 11. *NIST 800-90* b Recommendation for the Entropy Sources Used for Random Bit Generation, 2012. 12. *Ipatov, Valery P.* Spread Spectrum and CDMA. Principles and Applications / Valery P. Ipatov. University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. – 2005. – 385 p. 13. *Sarvate, D.V.* Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun, 1980. – Vol. Com 68 – P. 59–90. 14. *Gold, R.* Optimal binary sequences for spread spectrum multiplexing // IEEE Trans. Inform. Theory. – 1967. – Vol. 13. – P. 619–621. 15. *Замула, А.А.* Ансамбли дискретных сигналов с минимальными значениями боковых лепестков функций корреляции / Замула А.А. // Системи обробки інформації. – Х. : ХУПС, 2015. – Вип. 10 (135). – С. 35-39. 16. *Land A.H. and Doig A.G.* An automatic method of solving discrete programming problems. Econometrica. v28 (1960), pp 497-520.

Харьковский национальный университет
имени В.Н. Каразина

Поступила в редколлегию 12.09.2016