НОВЫЕ СРЕДСТВА
КИБЕРНЕТИКИ, ИНФОРМАТИКИ,
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
И СИСТЕМНОГО АНАЛИЗА

Я.Н. НИКОЛАЙЧУК, Б.М. ШЕВЧУК, А.Р. ВОРОНИЧ, Т.А. ЗАВЕДЮК, В.Н. ГЛАДЮК

УДК 004.416.2:004.67

ТЕОРИЯ НАДЕЖНОЙ И ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ДАННЫХ В СЕНСОРНЫХ И ЛОКАЛЬНО-РЕГИОНАЛЬНЫХ СЕТЯХ

Аннотация. Проведен систематизированный анализ передачи данных в сенсорных и локально-региональных сетях. Изложены характеристики нового класса сигнальных корректирующих кодов поля Галуа, которые обеспечивают выявление и исправление ошибок на физическом уровне компьютерных сетей без дополнительного формирования и передачи кодов CRC. Изложены методы обработки гармонических сигналов цифровым процессором с нейрокомпонентами.

Ключевые слова: беспроводная сенсорная сеть, процессоры с нейрокомпонентами, сигнальный корректирующий код, теоретико-числовой базис, линейные и спиральные коды Галуа.

ВВЕДЕНИЕ

Современные тенденции развития электронной элементной базы и технологий пакетной передачи информации в беспроводных сетях, освоение новых диапазонов частот и разработка эффективных протоколов функционирования децентрализованных сетей с самоорганизацией передачи данных обеспечивают условия для широкого проникновения радиотехнологий в область построения перспективных промышленных, медицинских и бытовых систем, сетей персональной, локально-региональной и глобальной связи. Развитие пакетных радиосетей широкого применения наиболее динамично осуществляется в направлении построения mesh-сетей (ячеистых сетей) с полной децентрализацией функций управления маршрутами передачи пакетов. Примером таких сетей являются беспроводные сенсорные и локально-региональные сети [1–5].

Беспроводные сенсорные сети (Wireless Sensor Network, WSN) позволяют эффективно решать множество прикладных задач, в которых необходимо осуществлять дистанционный сбор, обработку и передачу контролируемых данных от различных удаленных объектов контроля и управления, а также передачу команд управления с применением радиочастотной связи. Построение WSN базируется на использовании информационных технологий в трех различных направлениях: сенсорного восприятия, коммуникации и компьютерной обработки данных. Структурно и функционально WSN представляют собой многоячеистую (mesh) сеть, абонентские системы которой характеризуются малыми габаритами, сверхнизким энергопотреблением устройств, большую часть времени находящихся в «спящем» режиме. В настоящее время в области WSN наиболее распространенным стандартом построения сенсорных сетей является стандарт Zigbee, спецификации которого постоянно обновляются [2–4].

Сеть Zigbee позволяет организовать передачу данных с топологией «каждый с каждым», при этом передача информации от одного узла сети к другому может осуществляться по разным маршрутам, что позволяет строить распределенные сети с надежной доставкой информации на большие расстояния. Кроме стандартных технологий Zigbee, Wireless HART для создания WSN могут также использоваться частные решения компаний, таких как Sensicast (www.sensicast.com), Millennial Net (www.millen-nial.net), Dust Networks (www.dustnetworks.com), Crossbow (www.xbow.com), а также российская разработка — платформа Meshlogic (www.meshlogic.ru). Разработана технология беспроводной передачи данных с ультранизким энергопотреблением DASH7 (www.dash7.org), стандарт беспроводной связи ISA SP100.11a для промышленной автоматизации. Отличие технологии Meshlogic заключается в наличии собственных стеков сетевых протоколов, которые обеспечивают следующие преимущества: имеется полностью многоячеистая топология сети; все узлы равноправны и являются маршрутизаторами; самоорганизация и автоматический поиск маршрутов; высокая масштабируемость и надежность доставки данных; возможность работы всех узлов от автономных источников питания.

Дальнейшим развитием Zigbee является стандарт 6loWPAN — стандарт взаимодействия по протоколу IPv6 маломощных WSN стандарта IEEE 802.15.4. Стандарт 6loWPAN ориентируется на приложения, которые требуют беспроводного подключения к Интернету с низкой скоростью передачи данных для устройств с ограниченными возможностями производительности и мощности.

Локально-региональные mesh-сети характеризуются повышенной отказоустойчивостью. Они соединяют свои узлы даже в случае выхода из строя большинства из них. Современные системы WiFi, которые работают в диапазонах 2.4 и 5 ГГц, обеспечивают высокоскоростную пакетную передачу данных при построении ad hoc- и mesh-сетей с альтернативными маршрутами доставки информации между узлами. Соответственно по скорости передачи данных на низовых уровнях компьютерных систем радиосети конкурируют с оптоволоконными сетями связи.

При развертывании WSN необходимо учитывать положительные и отрицательные свойства механизмов защиты данных в беспроводных локальных сетях (Wireless Local Area Network; WLAN). Отличительные особенности таких механизмов отображены в табл. 1 [2–4]. В беспроводных сетях с технологией стандарта Zigbee применяются механизмы доступа к каналу передачи, которые поддерживают 128-битовое AES-шифрование. Для защиты информации в беспроводных локальных сетях (WLAN) на MAC-уровне предусмотрен механизм защиты данных, включающий аутентификацию абонентских станций и собственно шифрование передаваемых данных в соответствии с алгоритмами WEP (Wired Equivalent Privacy (безопасность, аналогичная защите проводных сетей)), WPA и WPA2 (Wi-Fi Protected Access (защищенный доступ Wi-Fi)). Их основные характеристики приведены в табл. 1.

В других беспроводных технологиях, таких как сотовая цифровая передача пакетов данных (Cellular Digital Packet Data, CDPD) для мобильных телефонов, КПК, а также глобальная система мобильной связи третьего поколения (Third Generation Global System for Mobile communications, 3GSM) и множественный доступ с временным разделением каналов (Time Division Multiple Access, TDMA) для сотовых телефонов и КПК, определены свои собственные (часто закрытые) протоколы беспроводной связи и защиты информации. В системах цифрового радиовещания стандарта Eureka-147, который ориентирован на наземное, кабельное и спутниковое вещание, для защиты информации используется ее перемножение на некоторую псевдослучайную последовательность, ключом генерации которой является 8-байтовое контрольное слово, периодически изменяемое. Далее все данные кодируются в целях энергетического сглаживания сигнала, чтобы его спектр был как можно более ровным, шумоподобным.

Таблица 1. Алгоритмы передачи данных в WLAN

<table>
<tr><th>WEP,
стандарт IEEE 802.11</th><th>WPA,
стандарт IEEE 802.11i</th><th>WPA2,
стандарт IEEE 802.11i-2004</th></tr>
<tr><td rowspan="2">Поточный шифр RC4, для подсчета контрольных сумм используется CRC32. Ключи статические длиной 40 бит и 104 бит для WEP-40 и WEP-104 соответственно.</td><td colspan="2">Усовершенствованная схема шифрования RC4 (стандарт AES (Advanced Encryption Standard, усовершенствованный стандарт шифрования) — обязательная аутентификация с использованием EAP (Extensible Authentication Protocol, расширяемый протокол аутентификации).
MIC (Message Integrity Check, проверка целостности сообщений) используют для предотвращения перехвата пакетов данных, содержание которых может быть изменено, а модифицированный пакет вновь передан по сети.</td></tr>
<tr><td>TKIP (Temporal Key Integrity Protocol, протокол целостности временного ключа) — ключи динамические длиной 128 бит, которые автоматически генерируются и рассылаются сервером аутентификации, специальная иерархия ключей и методология управления ключами.</td><td>CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) — протокол блочного шифрования с кодом аутентичности сообщения (MIC) и режимом сцепления блоков и счетчика.
В отличие от TKIP управление ключами и целостностью сообщений осуществляется одним компонентом, построенным вокруг AES с использованием 128-битного ключа.</td></tr>
</table>

В WiMAX (IEEE 802.16) [2] поток данных, подлежащий передаче, скремблируется — подвергается рандомизации, т.е. умножению на псевдослучайную последовательность, получаемую в 15-разрядном сдвиговом регистре.

В общедоступных беспроводных локальных сетях (даже при задействовании в точках доступа механизмов защиты данных) существенную угрозу представляет возможность несанкционированного подключения к подставной точке доступа (rogue acces point) [4]. Такая точка доступа представляет собой авторизованную точку, включенную в сеть, в которой, как правило, не активизируется система шифрования. Любой пользователь, находящийся в радиусе связи сети, может получить доступ к ресурсам корпоративной сети. Постоянная проверка наличия подставных точек доступа сети актуальна и для проводных сетей Ethernet. Для противодействия неавторизированному доступу в широко распространенных локальных сетях используется взаимная аутентификация, осуществляемая между удаленными абонентами (устройствами) и точкой доступа. В таких сетях применяются методы, благодаря которым базовая станция может удостовериться в идентичности абонента. Это позволяет убедиться в «законности» пользователя (абонента) и в установлении им соединения с легитимной точкой доступа. Вместе с тем точки доступа должны аутентифицироваться на маршрутизаторах и шлюзах, что исключает появление в сети подставных точек доступа.

Использование шифрования и аутентификации существенно повышает безопасность компьютерных сетей. Однако в беспроводных сетях определенную опасность представляют атаки «человек посередине» (man-in the middle attacks) [4]: несанкционированный пользователь сети (хакер) устанавливает устройство между легитимным абонентом (пользователем) и беспроводной сетью. При этом в процессе осуществления данной атаки используется протокол преобразования адресов (ARP, address resolution protocol), используемый во всех сетях TCP/IP. Суть проблемы, связанной с протоколом ARP, состоит в том, что

он представляет опасность для систем защиты сети из-за возможности спуфинга (spoofinf) — имитации соединения: посылая абоненту (станции) через подставное сетевое устройство фиксированный ARP-ответ, содержащий IP-адрес легитимного сетевого устройства и MAC-адрес подставного устройства, хакер вводит в заблуждение станцию. В результате все легитимные станции сети обновляют свои ARP-таблицы, внеся в них ложные данные. Таким образом, станции будут передавать пакеты подставному устройству, а не легитимной точке доступа или маршрутизатору. В результате этих действий хакер имеет возможность управлять сеансами связи пользователя, и он получит пароли и данные, а также сможет взаимодействовать с корпоративными серверами.

Действенной защитой от всех видов атак являются защита информации абонентами сети с применением цифровой подписи, маскировки факта передачи пакетов данных в шумах радиоканала методом стеганографии [1, 6]; хаотическая смена несущих частот (моноканалов передачи данных); использование направленных антенн, а также открытых оптических каналов.

Основную задачу, которая стоит перед WSN, можно сформулировать так: информацию следует передать на максимальное расстояние, с максимальной скоростью, выявлением и исправлением ошибок с заданным уровнем защиты от помех и несанкционированного доступа. Эти задачи выполняются на физическом и канальном уровнях.

На физическом уровне современных сетей используются различные методы манипуляции сигналов [2–4]. Принципиальным недостатком известных методов манипуляции сигналов является то, что они не предусматривают и не позволяют исправлять и обнаруживать ошибки в процессе приема бинарных значений передаваемых данных стандартными модемами. Это обусловлено тем, что каждый передаваемый бит в известных методах манипуляции является статистически независимым и не обладает определенными марковскими свойствами, за исключением двоичной фазовой манипуляции (BPSK, Binary Phase-Shift Keying) [3], принцип работы которой состоит в следующем: предыдущий бит является эталоном для последующего, фаза которого зеркально меняется. Использование данного метода было вызвано проблемой флуктуаций амплитуд сигналов в линии связи. Однако BPSK имеет большой недостаток — при однократной ошибке происходит прием зеркально перевернутого кода сигнала.

Анализ фреймов основных протоколов канального уровня модели OSI (рис. 1) [2] показывает, что они характеризуются наличием служебной (избыточной) информации. Зависимость объема служебной информации от общего объема информации показана на рис. 2. Здесь уровень избыточности достаточно высок при небольшом размере данных, что очень важно для низовых уровней компьютерных сетей, т.е. при создании сетей WNS. Как видно из рис. 1, приведенные протоколы не предусматривают обнаружения и исправления ошибок на физическом уровне. Здесь **PA** — Preamble (преамбула), **SD** — Start Delimiter (стартовый разделитель), **FC** — Frame Control (контроль фрейма), **DA** — Destination Address (адрес получателя), **AC** — Access Control (контроль доступа), **SA** — Source Address (адрес отправитель), **PDU** — Packet Data Unit (данные), **FCS** — Frame Check Sequence (последовательность проверки кадра), **CRC** — Cyclic Redundancy Check (циклический избыточный код), **ED**/**FS** — End Delimiter/Frame Status (разделитель конца/статус фрейма), **FT** — Frame Type (тип фрейма), **F** — Flag (флаг).

Нерешенными проблемами остаются необходимость повторных передач, сложные алгоритмы кодирования/декодирования **CRC**, незащищенность кода **FCS**, практическое снижение скорости передачи данных на низовых уровнях на 30–40 %, невозможность исправлять ошибки на физическом уровне, а только на канальном после приема полного пакета данных.

Ethernet

PA	SD	DA	SA	FT	PDU	FSC
56 bits	8 bits	48 bits	48 bits	16 bits	512–32000 bits	32 bits

Token Ring

SD	AC	FC	DA	SA	PDU	CRC	ED	FS
8 bits	8 bits	8 bits	48 bits	48 bits	up to 18200 × 8 bits	32 bits	8 bits	8 bits

FDDI

PA	SD	FC	DA	SA	PDU	FCS	ED/FS
16 bits	8 bits	8 bits	48 bits	48 bits	up to 4478 × 8 bits	32 bits	16 bits

HDLC

F	Address	FC	Information	FCS	F
8 bits	8 bits	8 or 16 bits	Variable length, 0 or more bits × 8 bits	16 or 32 bits	8 bits

PPP

F	Address	FC	Protocol	Information	FCS	F
8 bits	8 bits	8 bits	8 or 16 bits	Variable length, 0 or more bits ×8 bits	16 or 32 bits	8 bits

Frame Relay

F	Address	Information	FCS	F
8 bits	8 or 16 bits	Variable length, 0 or more bits ×8 bits	16 bits	8 bits

Рис. 1. Структура фреймов различных протоколов канального и физического уровней

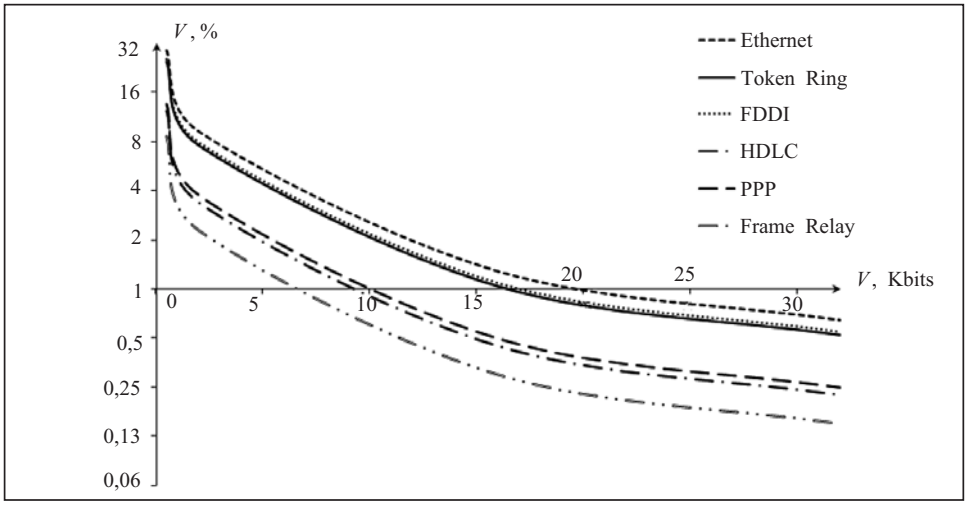


Рис. 2. Зависимость объема служебной информации от общего объема информации в различных протоколах

Существует большое количество помехоустойчивых корректирующих кодов. Из них следует выделить коды Боуза–Чоудхури–Хоквингема (BCH, Bose–Chaudhuri–Hocquenghem), Рида–Соломона (RS, Reed–Solomon) [7].

Анализ фреймов протоколов, которые используются в компьютерных сетях на канальном уровне, оценка избыточности служебной информации, а также аутентификация особенностей широкоиспользуемых корректирующих кодов позволяют классифицировать следующие атрибуты известных способов:

1) информация на передающей станции защищается от ошибок путем вычисления кода CRC, который добавляется и совместно с данными передается по каналам связи;

2) на приемной станции из переданного пакета данных вычисляется код CRC, который сравнивается с переданным;

3) при обнаружении несоответствия этих кодов реализуется алгоритм исправления ошибок согласно применяемым корректирующим кодам;

4) при невозможности исправления ошибок реализуется требование повторной передачи пакета данных.

Принципиальным недостатком такого способа обнаружения и исправления ошибок в передаваемых пакетах данных есть отсутствие процедур контроля ошибок на физическом уровне сетей и их исправление в процессе передачи данных. Этот недостаток обусловлен тем, что передаваемые данные шифруются только с целью ограничения возможности несанкционированного доступа. Способ не предусматривает шифрования данных с возможностями контроля каждого бита данных, а не пакета в целом.Так, передача каждого бита с помощью шумоподобных сигналов приводит к увеличению объема сигнальных бит-ориентированных кодов и соответствующему снижению скорости передачи данных и характеристик быстродействия приемопередатчиков. Предлагаемое решения такой задачи с нулевой избыточностью используемых корректирующих кодов вытекает из фундаментальных основ математики теоретико-числовых базисов, которые порождают системы исчисления.

МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОДОВЫХ СИСТЕМ РАЗНЫХ ТЕОРЕТИКО-ЧИСЛОВЫХ БАЗИСОВ

Теоретико-числовые базисы (ТЧБ) являются фундаментальными теоретическими основами систем исчисления и методов кодирования данных. Базис порождается системами ортогональных функций. Математической основой теоретико-числовых базисов являются системы ортогональных функций на некотором интервале изменения аргумента [8–10].

В современных компьютерных и телекоммуникационных системах широко используются ТЧБ на основе кусочно-постоянных дискретных функций, которые обеспечивают более простую реализацию цифровых генераторов, а также упрощают алгоритмы цифрового приема сигналов. Представление известных базисов отражены в табл. 2.

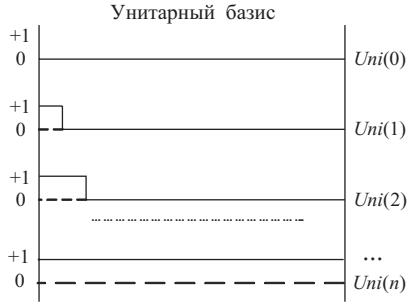
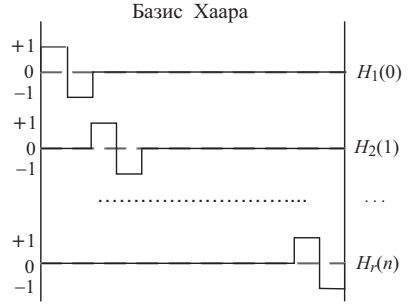
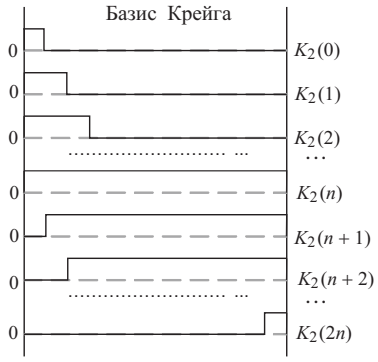
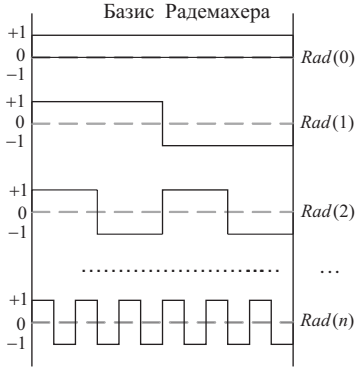
Массовое распространение в современных компьютерных системах получила реализация известных базисов, таких как унитарный, Хаара, Крейга, Радемахера, Крестенсона и Галуа. Эти базисы порождают системы исчисления, что обеспечивает существенное упрощение цифровой обработки базисных функций на основе их представления в виде логических кодовых матриц [8–12]. Важной характеристикой каждого базиса являются объем V_i его кодовой матрицы M и число активных элементов (независимых кодовых значений) N_i (см. табл. 2), что определяет характеристики избыточности представления информации на основе аналитической оценки:

$$V_i = n_i \cdot N_i, \tag{1}$$

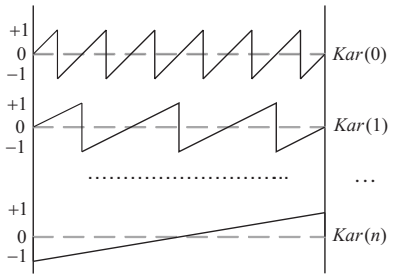
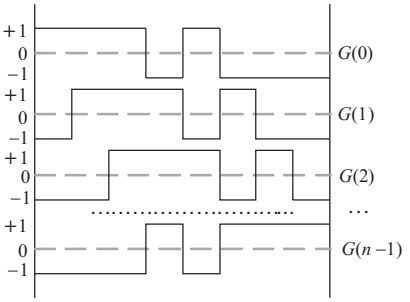
где n_i — разрядность числа.

Анализ показывает, что унитарный базис, базис Хаара и базис Крейга, которые обладают возможностью обнаружения ошибок, имеют высокий уровень избыточности по сравнению с другими базисами, использование которых неэффективно и нецелесообразно. ТЧБ Радемахера и Крестенсона являются неизбыточными, однако для защиты от ошибок требуют дополнительной служебной информации. Кодовая матрица ТЧБ Галуа наиболее плотно упакована и за счет рекуррентных свойств обеспечивает обнаружение всех одиночных ошибок, а в случае отсутствия стираний и вставок битов — исправление всех ошибок.

Таблица 2. Кодовые матрицы обнаружения и исправления ошибок сравниваемых базисов

Ортогональные функции базисов	Характеристики базиса
1	2
Унитарный базис 	$M_{Uni} = \begin{vmatrix} 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 \end{vmatrix}$, $V = N^2$, $Uni(m, \theta, i) = \text{sign}\ (\sin\ (2^m \pi (\theta + i \cdot 2^{-n})))$, базис порождает унитарную систему исчисления, обнаруживает $N^2 - N$ ошибок
Базис Хаара 	$M_{Har} = \begin{vmatrix} 0 & 0 & 0 & \dots & 0 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix}$, $V = N^2$, $Har(n, \theta, i) = \text{sign}\ [\sin(i 2^n \pi, \theta)]$, базис порождает систему исчисления Хаара, обнаруживает N^2 ошибок
Базис Крейга 	$M_{Crg} = \begin{vmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 & 0 \\ 1 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 1 \end{vmatrix}$, $V = N^2 / 2$, $Crg(n, \theta) = \text{sign}\ [\ 2^{n-1} \pi, \theta]$, базис порождает систему исчисления Крейга, обнаруживает $(N^2 - 4N) / 2$ ошибок
Базис Радемахера 	$M_{Rad} = \begin{vmatrix} 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 & 1 \end{vmatrix}$, $V = N \cdot \log_2 N$, $Rad(n, \theta) = \text{sign}\ [\ 2^n \pi, \theta]$, базис порождает двоичную систему исчисления и двоичные коды, не обнаруживает ошибок

Продолжение табл. 2

1	2
Базис Крестенсона  	$M_{Gres} = \begin{vmatrix} P_1 & P_2 & \dots & P_x \\ 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ 2 & 2 & \cdots & 2 \\ 0 & 3 & \cdots & 3 \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \cdots & a_x \end{vmatrix}$, $V = \sum_{i=1}^{m} \log_2(P_i)$, $N_i = res \sum_{i=1}^{n} (B_i \cdot b_i) \bmod P$, базис порождает систему остаточных классов, не обнаруживает ошибок
Базис Галуа  	$M_G = \lvert 0\ 0\ \dots\ 0\ 1\ 1\ 1 \rvert^{\mathrm{T}}$, $V = N$, $N_i = f(C_{j-n-1}, \dots, C_{j-1}, C_j)$, $C_j = \sum_{j=0}^{n-1} C_{j-1} \cdot a (\bmod 2)$, базис Галуа порождает коды поля Галуа и систему исчисления Галуа, обнаруживает и исправляет N ошибок

Анализ корректирующих свойств кодовых матриц ТЧБ, приведенных в табл. 2, показывает, что все базисы, кроме Галуа, не обладают рекуррентными свойствами и для защиты данных требуют формирования дополнительной служебной информации, например метод четности в ТЧБ Радемахера, когда к семибитовой последовательности добавляется бит четности, который позволяет выявить однократные ошибки. В базисе Крестенсона обнаружение или исправление ошибок достигается путем расширения системы взаимно простых модулей, что также увеличивает избыточность информационных данных.

Фундаментальной теоретической основой кодовых систем и кодов Галуа является теория абелевых групп и расширенных полей Галуа [10].

Коды поля Галуа [9, 10, 12] по общей классификации относятся к подклассу циклических блочных кодов, которые обладают всеми основными свойствами помехозащищенных кодов. В блочных кодах последовательность элементарных сообщений разбиваются на блоки символов $(B_1, B_2, B_3, \dots, B_n)$ фиксированной длины, к каждому из которых ставится в соответствие определенная комбинация символов кодового слова $(b_1, b_2, b_3, \dots, b_n)$.

Преимущества базиса Галуа наиболее эффективно можно использовать при кодировании интегральных значений, поскольку при интегрировании каждое последующее значение увеличивается на единицу. Каждое дискретное значение интеграла функции $x(t)$ вместо n-разрядного двоичного кода в отличие от базиса Радемахера фиксируется одним битом Галуа [9, 10].

Для генерации кодов поля Галуа $G\left(\begin{matrix} n \\ 2 \end{matrix}\right)$ используются примитивные алгебраические многочлены [10]:

$$4: x_1 \oplus x_4;\ 5: x_2 \oplus x_5;\ 6: x_1 \oplus x_6;\ 7: x_3 \oplus x_7;\ 8: x_2 \oplus x_3 \oplus x_4 \oplus x_8;\ 9: x_4 \oplus x_9;$$

$$10: x_3 \oplus x_{10};\ 11: x_2 \oplus x_{11};\ 12: x_1 \oplus x_4 \oplus x_6 \oplus x_{12};\ 13: x_1 \oplus x_3 \oplus x_4 \oplus x_{13};$$

$$14: x_1 \oplus x_6 \oplus x_{10} \oplus x_{14};\ 15: x_1 \oplus x_{15};\ 16: x_1 \oplus x_3 \oplus x_{12} \oplus x_{16};$$

$$17: x_3 \oplus x_{17};\ 18: x_7 \oplus x_{18};\ 19: x_1 \oplus x_2 \oplus x_5 \oplus x_{19};\ 20: x_3 \oplus x_{20};$$

$$21: x_2 \oplus x_{21};\ 22: x_1 \oplus x_{22};\ 23: x_5 \oplus x_{23};\ 24: x_1 \oplus x_3 \oplus x_4 \oplus x_{24};\ 25: x_3 \oplus x_{25};$$

$$26: x_1 \oplus x_2 \oplus x_6 \oplus x_{26};\ 27: x_1 \oplus x_2 \oplus x_5 \oplus x_{27};\ 28: x_3 \oplus x_{28},\ 29: x_2 \oplus x_{29};$$

$$30: x_1 \oplus x_4 \oplus x_6 \oplus x_{30};\ 31: x_7 \oplus x_{31};\ 32: x_2 \oplus x_6 \oplus x_7 \oplus x_{32}.$$

Существуют также примитивные алгебраические многочлены для полей более высоких порядков $G\begin{pmatrix} n \\ p \end{pmatrix}$, где p — простое число.

Важным преимуществом кодовой последовательности Галуа является простая генерация кодов на основе рекуррентного уравнения. Простейшие ключи кодов поля Галуа описываются выражением

$$G_i = G_{i-1} \oplus G_{i-m};\ m \le n. \tag{2}$$

Важным математическим и практически целесообразным свойством в последовательности Галуа есть наличие черезуровневых рекуррентных связей [10], которые обладают высокими энтропийными характеристиками.

Пусть задан код поля Галуа $G\begin{pmatrix} 4 \\ 2 \end{pmatrix}$, имеющий ключ $G_i = G_{i-1} \oplus G_{i-4}$:

$$G\begin{pmatrix} 4 \\ 2 \end{pmatrix} = 1111\ 01011\ 0010\ 0011\ 1101\ 0110\ 0100\ 0111\ 1010\ 1100\ 1000\ 1111\ 0101\ldots$$

Данный код можно упаковать в спираль (рис. 3), причем по каждой из четырех образующих формируется рекуррентная последовательность, имеющая соответствующие рекуррентные свойства кода в базисе Галуа [9].

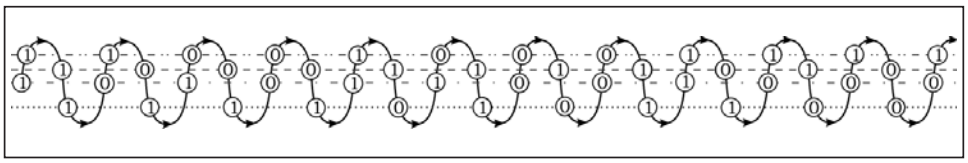


Рис. 3. Сигнальный корректирующий код, упакованный в виде спирали

После развертывания спирали, которая закодирована рекуррентным кодом поля Галуа, формируется черезуровневая рекуррентная последовательность согласно выражению

$$G_{i,j} = G_{i-4,j} \oplus G_{i-16,j},\ j = \overline{1, 4}, \tag{3}$$

или в общем случае

$$G_i = G_{i-4^v} \oplus G_{i-4^{v+1}},\ v = 0, 1, 2, 3\ldots \tag{4}$$

С учетом спиральных свойств сигнальный рекуррентный код можно использовать при обнаружении и исправлении пакетов ошибок, поскольку вначале проверяются и исправляются ошибки согласно выражению (2), а затем согласно выражению (3) по образующим спирали [11].

ПРИНЦИПЫ ФОРМИРОВАНИЯ И ОБРАБОТКИ ДАННЫХ, ОБЕСПЕЧИВАЮЩИЕ ИСПРАВЛЕНИЕ ОШИБОК НА ОСНОВЕ СИГНАЛЬНЫХ КОРРЕКТИРУЮЩИХ КОДОВ ПОЛЯ ГАЛУА

Коды поля Галуа широко используются для защиты информации от несанкционированного доступа [8–10]. Кодирование данных на основе кодовой последовательности Галуа показано на рис. 4.

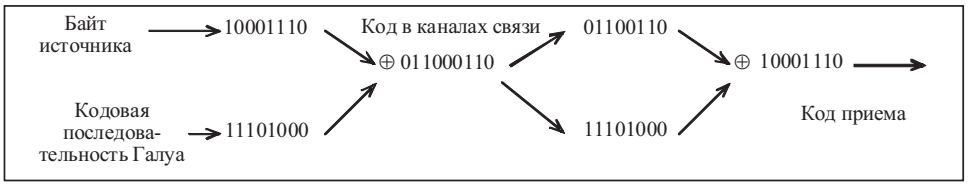


Рис. 4. Кодирование данных на основе кодовой последовательности Галуа

В работах [5, 10, 12, 13] авторами предложен способ неизбыточной защиты информационных потоков данных от ошибок на основе нового класса сигнальных корректирующих кодов, в которых используются рекуррентные свойства линейных и спиральных кодов поля Галуа. При передаче и приеме информации на основе предложенных кодов манипулируемые сигналы формируются на основе четырех признаков ($\uparrow, \downarrow, +, -$), которые поставлены в соответствие элементам информационного сообщения согласно кодам поля Галуа [9, 10, 12]. Принцип формирования сигнального корректирующего кода поля Галуа состоит в том, что биты единиц в пакете данных нумеруются рекуррентным кодом поля Галуа $G\binom{n}{2}$ [12]. Причем для единиц в пакете данных бит Галуа 1 передается фронтом нарастания ($\uparrow$), а бит Галуа 0 передается фронтом спада ($\downarrow$). Биты нулей в пакете данных также нумеруются рекуррентным кодом поля Галуа $G\binom{n}{2}$. Для нулей в пакете данных бит Галуа 1 передается потенциалом + (плюс) , а бит Галуа 0 передается потенциалом − (минус). В качестве четырех признаков манипуляции на физическом уровне могут быть соответственно использованы наборы из четырех фаз, частот, М-последовательностей, кодов Баркера, шумоподобных сигналов и других их комбинаций.

Структура формирования кодировано-манипулированных сигналов на основе кодов поля Галуа приведена на рис. 5, где G_i^1, G_i^0 — генераторы битов Галуа для символов 1 и 0 соответственно, Ф— формирователь выходных манипулированных сигналов; разграничение входного информационного потока на 0 и 1 (а); кодирование кодом поля Галуа потоков 1 и 0 (б, б′); представление битов Галуа символьными признаками (в, в′); мультиплексирование символьных признаков 1 и 0 (г); высокоэнтропийная манипуляция выходного сигнала на физическом уровне (д). Таким образом, обеспечивается эффективное симметричное кодирование в виде кодов поля Галуа последовательности нулей и единиц блока данных с однозначным определением их числа $N_0 + N_1 = N_D$, которое используется для обнаружения и исправления ошибок, т.е. выявления стирания и вставок отдельных битов или их пачек после передачи данных [12].

На рис. 6 показана схема реализации обнаружения и исправления ошибок кодировано-манипулированных сигналов на физическом уровне, где N — номер позиции битов в информационном сообщении; Д — информационные биты принятых данных с выявленными и исправленными ошибками; СгК — сигнальный код; $G_2^4(1)$, $G_2^4(0)$ — соответственно биты Галуа G_2^4 для информационных битов 1 и 0 с выявлением и исправлением ошибок; 0*, 1* — ошибочные биты. Возможны два случая идентификации битов Галуа: инвертирование Галуа-признака единичного или нулевого бита и замена сигнальных признаков $\uparrow, \downarrow$ на плюс (+), минус (–) или наоборот. Во всех случаях ошибка обнаруживается и исправляется программно-аппаратным декодером Галуа.

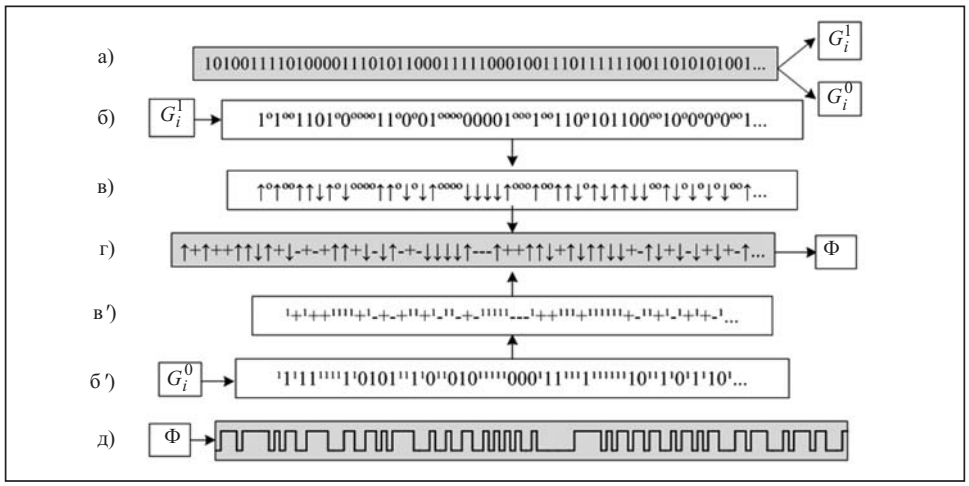


Рис. 5. Структура формирования кодировано-манипулированных сигналов на основе кодов поля Галуа

N / Биты	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	...
СгК																									
$G_2^4(1)$	1			1		1		1	0	0* /1		0	1		1	0		1	0	0	1* /0		0		...
$G_2^4(0)$		1	1		1		0* /1				0			1			1* /0					1		1	...
Д	1	0	0	1	0	1	0	1	1	1	0	1	1	0	1	1	0	1	1	1	1	0	1	0	...

Рис. 6. Схема реализации обнаружения и исправления ошибок кодировано-манипулированных сигналов

В современных системах цифровой связи на физическом уровне наиболее часто используются амплитудно-частотно-фазовые гармонические сигналы. При этом в качестве цифровых приемников достаточно эффективно используются спецпроцессоры с нейрокомпонентами. Анализ научных публикаций в области нейронных сетей и нейрокибернетики демонстрирует важные научные результаты моделирования и теоретической формализации функций нейрона, персептрона и нейронных сетей [13, 14].

Для решения широкого класса задач в области интеллектуальной обработки данных и распознавания сигналов все чаще применяются гибридные нейро-фаззи-системы и вейвлет-нейро-фаззи-системы, которые имеют улучшенные аппроксимирующие свойства и при этом не теряют способности функционировать в реальном времени. Такими системами являются архитектуры типа Ванга–Менделя, адаптивные нейро-фаззи-системы Такаги–Сугено–Канга, вейвлет-нейро-фаззи-сети, адаптивные вейвлет-нефро-фаззи-системы с *W*-нейронами [15].

Вейвлет-нейрон, который использовался для решения задачи on-line прогнозирования нестационарных сигналов, достаточно близок по архитектуре к формальному нейрону с n входами. При поступлении на вход вейвлет-нейрона векторного сигнала $x(k)$ ($k = 0, 1, 2, \ldots$ — текущее дискретное время) на его выходе формируется сигнал, значение которого можно найти согласно выражению

$$y(k) = \sum_{i=1}^{n} f_i(x(k)) = \sum_{i=1}^{n} \sum_{j=1}^{h_j} w_{ji}(k)\, \varphi_{ji}(x_i(k)), \qquad (5)$$

где $w_{ji}(k)$ — синаптические веса, $\varphi_{ji}(x_i(k))$ — вейвлет-функции.

В общем случае реакция формального нейрона на аналоговый входной сигнал $x(t)$ может быть достаточно адекватно описана моделью расширенного оператора ПИД-регулятора [16]

$$Z(t) = \alpha_0 x(t) + \alpha_1 \frac{dx}{dt} + \alpha_2 \int x dx + \alpha_3 \frac{d^2x}{dt^2} + \ldots + \alpha_i \int x(t)x(t+\tau)dx + \ldots, \quad (6)$$

где $\alpha_0, \alpha_1, \alpha_2 \ldots$ — весовые коэффициенты, $\int x(t)x(t+\tau)dx$ — автокорреляционная функция входного сигнала.

Недостатком описания такой модели является отсутствие в уравнении корреляционных составляющих, которые учтены в формуле Колмогорова для прогнозирования значения стационарной функции [17], что используется при реализации предусматривающего фильтра Колмогорова–Габора

$$g[x(t)] = r_0 + \sum_0^n r_0 x_n + \sum_0^n \sum_0^n x_{n_1} x_{n_2} r_{n_1 n_2} + \sum_0^n \sum_0^n \sum_0^n x_{n_1} x_{n_2} x_{n_3} r_{n_1 n_2 n_3} + \ldots, \quad (8)$$

где $g[x(t)]$ — прогнозируемое значение функции; $x_{n_1}, x_{n_2}, \ldots$ — предыдущие значения этой функции; r_{n_i} — коэффициенты влияния (веса) каждого члена.

В результате исследований было установлено, что на выходе нейрона формируется импульсный частотно-модульный сигнал, который реализуется на основе пороговой функции. В работе [18] сказано, что на уровне нейронных структур гармонический синусоидальный сигнал на входе нейрона на уровне возбуждающих и тормозящих входов трансформируется в квадратическое пространство. На рис. 7, *а* показан график модели гармонического сигнала $y(x) = \sin^2(x)$ и его производной, а на рис. 7, *б* — реакция нейрона на этот сигнал путем идентификации точек $a - h$ согласно выражению $x(t) = 0$ (для *a*, *e*); $x(t) = (dx(t))/dt$ (для *b*, *d*, *f*, *h*); $x(t) = \max$ (для *c*, *g*) и формирование соответствующей выходной импульсной последовательности.

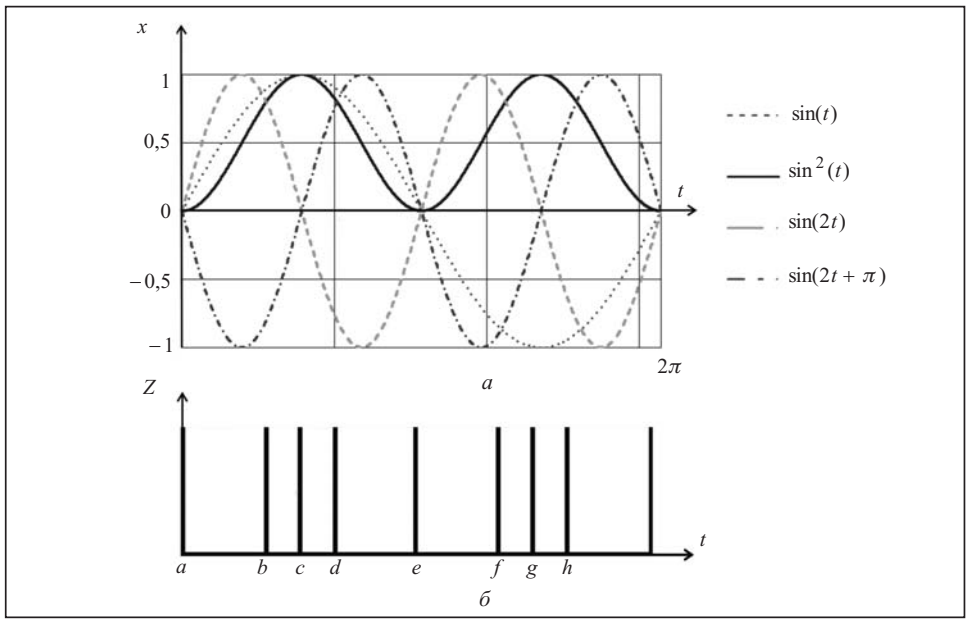


Рис. 7. График модели гармонического сигнала $y(x) = \sin^2(x)$ и его производной (*а*) и импульсная реакция нейрона (*б*)

На рис. 8 показана структура корреляционного нейропроцессора на основе модели динамического нейрона для распознавания гармонических сигналов [19], где Ф — формирователь импульсов, изображенных на рис. 7, *б*. Выходной сигнал имеет вид $H_i = \begin{cases} 1, & Z_i \geq p, \\ 0 & Z_i < p. \end{cases}$ Функция реакции нейрона на входной сигнал x_i определяется выражением $Z_i = \sum_{i=1}^{n} \alpha_i \cdot x_i$, где α_i — весовой коэффициент; p — пороговое значение.

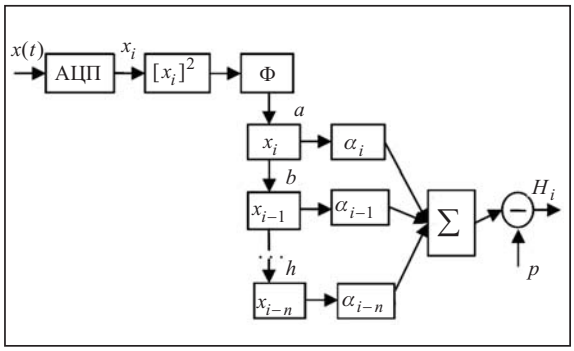
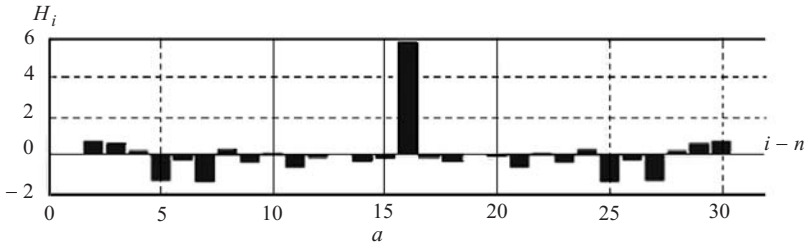


Рис. 8. Структура корреляционного нейропроцессора для распознавания гармонических сигналов на основе модели динамического нейрона

В результате обработки импульсного потока сигналов (см. рис. 7, *б*) процессором со структурой динамического нейрона (рис. 8) получен сигнальный импульсный код, приведенный на рис. 9, который соответствует корреляционной свертке известных и широко применяемых в технике связи кодов Баркера.



а

α_1	– 0.9014	α_5	0.5010	α_9	0.6061	α_{13}	0.2040
α_2	0.1421	α_6	0.4800	α_{10}	0.8909	α_{14}	– 0.4929
α_3	0.4017	α_7	– 0.1363	α_{11}	– 0.8322	α_{15}	0.7469
α_4	0.9246	α_8	0.2685	α_{12}	0.8319	α_{16}	0.0268

б

Рис. 9. Сигнальный импульсный код, получаемый на выходе корреляционного нейропроцессора (*а*) на основе весовых коэффициентов (*б*)

Проведенные исследования эффективности применения линейных и спиральных сигнальных корректирующих кодов в базисе Галуа позволили установить возможность полного исправления однократных ошибок в информационных потоках за счет линейных сигнальных корректирующих кодов в базисе Галуа, а также пакетов ошибок при одновременном применении линейных и спиральных сигнальных корректирующих кодов в базисе.

ЗАКЛЮЧЕНИЕ

Изложены перспективные решения проблемы усовершенствования системных характеристик сетей WNS с учетом реализации максимальной дальности передачи информационных потоков с обнаружением и исправлением ошибок, а также защиты от несанкционированного доступа. Предложены новые методы эффективного кодирования и манипуляции сообщений в кодовой системе ТЧБ Галуа путем использования нового класса сигнальных корректирующих кодов,

обеспечивающих обнаружение и исправление ошибок на физическом уровне компьютерных сетей в режиме онлайн. Разработанная технология кодированной манипуляции сигналов на физическом уровне компьютерных сетей является совместимой с известными стандартными протоколами. Совместно с технологией распознавания гармонических сигналов с использованием корреляционных нейропроцессоров существенно повышается скорость передачи информации на низовых уровнях в условиях влияния интенсивных помех.

СПИСОК ЛИТЕРАТУРЫ

1. Шевчук Б.Н., Задирака В.К., Гнатив Л.О., Фраер С.В. Технология многофункциональной обработки и передачи информации в мониторинговых сетях. — К.: Наук. думка, 2010. — 370 с.
2. Шахнович Н.В. Современные технологии беспроводной связи. — 2-е изд. — М.: Техносфера, 2006. — 288 с.
3. Sklar B. Digital communications: Fundamentals and applications. — 2nd ed. — New Jersey: Prentice Hall, 2001. — 1079 p.
4. Geier J. Wireless networks first-step. — Indianapolis: Cisco Press, 2005. — 264 p.
5. Пат. 73756 Украина, МПК (2012.01) H04W 4/00. Беспроводная сенсорная сеть / Я.Н. Николайчук, А.Р. Воронич, В.М. Гладюк. — Опубл. 10.10.2012.
6. Шевчук Б.Н. Обработка, кодирование и передача данных средствами абонентских систем информационно-эффективных радиосетей // Компьютер. средства, сети и системы. — 2010. — № 9. — С. 130–139.
7. Peterson W., Weldon E.J., Jr. Error-correcting codes. — 2nd ed. — Cambridge (Mass.): MIT Press, 1972. — 560 p.
8. Николайчук Я.Н. Теория источников информации. — 2-е изд. — Тернополь: ООО «Терно-граф», 2010. — 536 с.
9. Николайчук Я.М. Коды поля Галуа: теория и применение. — Тернополь: ООО «Терно-граф», 2010. — 576 с.
10. Артин Э. Теория Галуа: Пер. с англ. — М.: МЦНМО, 2004. — 66 с.
11. Пат. 63648 Украина, МПК (2011.01) H04J13/00. Многоканальный способ передачи и приема информации / Я.М. Николайчук, А.Р. Воронич. — Опубл. 10.10.2011. — Бюл. № 19.
12. Nykolaychuk Y.M., Voronych A.R. Entropic methods of signal processing with protection from errors in Galois base // J. Qafqaz Univ. — Baku (Azerbaijan), 2010. — N 30. — P. 69–77.
13. Николайчук Я.М., Заведюк Т.О. Структура та функції рекурентного біонейрона для розпізнавання образів у Хеммінговому просторі // Поступ в науку. — 2010. — № 6. — С. 37–39.
14. Заведюк Т.О., Николайчук Я.М., Воронич А.Р. Самовідновлювана система передавання сигналів біонейронного волокна у базисі Крестенсона // Вісн. Хмельн. нац. ун-ту. — 2012. — 4 (191). — С. 137–142.
15. Bodyanskiy Ye., Pliss I., Vynokurova O. Hybrid wavelet-neuro-fuzzy system using adaptive W-neurons // Wissenschaftliche Berichte, FH Zittau/Goerlitz. — 2010. — **106**, N 2454–2490. — S. 301–308.
16. Теория автоматического управления / Под ред. А.А. Воронова. — М.: Высш. шк., 1977. — Ч. I. — 304 с.
17. Івахненко О.Г., Лапа В.Г. Передбачення випадкових процесів. — Київ: Наук. думка, 1969. — 420 с.
18. Zavedyuk T.O. Specifics of recognition of signals are on the basis of correlation neuronlike processor // Матеріали X Міжнар. конф. TCSET'2010 «Сучасні проблеми радіоелектроніки, телекомунікації, комп'ютерної інженерії». — 23–27 лют. 2010 р., Славське. — С. 308.
19. Zavedyuk T., Shyrmovska N. Specialized data neuroprocessors and diagnostics quasi-steady objects based on cluster models // XIth Intern. Conf. "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM 2011) ", 23–25 лют. 2011 р., Львів. — Lviv Polytech. Nat. Univ., 2011. — P. 181.

Поступила 29.04.2013