

## ТЕОРЕТИЧЕСКИЕ И АЛГОРИТМИЧЕСКИЕ ОСНОВЫ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ПАКЕТНОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ В ВЫСОКОСКОРОСТНЫХ И ЗАЩИЩЕННЫХ РАДИОСЕТЯХ

**Аннотация.** Предложен подход к повышению эффективности пакетной передачи информации в компьютерных радиосетях, основой которого является реализация абонентами сети комплекса алгоритмов оперативного компактного кодирования и защиты данных, включая криптозащиту и защиту двоичных последовательностей от действия канальных помех, формирование и адаптивную передачу высокоинформативных и помехоустойчивых пакетов информации, состоящих из интервальных кодово-сигнальных последовательностей с переменной базой.

**Ключевые слова:** компьютерные радиосети, пакетная передача информации, оперативное сжатие и защита данных, формирование и адаптивная передача интервальных кодово-сигнальных последовательностей пакетов информации.

### ВВЕДЕНИЕ

Интенсивное развитие и широкое применение беспроводных компьютерных сетей обусловлено достижениями микроэлектроники, разработкой и внедрением новых стандартов беспроводной передачи информации, конкуренцией ведущих мировых производителей процессорной техники, интеллектуальных радиомодулей и специализированного программного обеспечения. Вместе с тем удешевление производства чипов высокопроизводительных и энергоэффективных процессоров создало основу для использования в различных областях человеческой деятельности портативных абонентских систем, терминалов, станций, точек доступа и роутеров радиосетей с безлицензионным использованием рабочих полос ISM-диапазона радиочастот, включая 430, 868, 902, 2400 и 5000 МГц [1–3]. В результате, помимо мобильных средств связи 2,5G, 3G и 4G, широкое распространение получили компьютерные радиосети, построенные по технологии Ad hoc-, Mesh-, MaNET- и VANET-сетей [1], а также беспроводных сенсорных сетей WSN [1, 2]. Основой таких сетей, как правило, являются программно-аппаратные средства стандартизированных сетей WiMAX, Wi-Fi, ZigBee [2, 4], которые применяются в мониторинговых задачах, в процессе обмена данными между удаленными стационарными и подвижными объектами, а также для доступа последних к ресурсам сети Интернет. Дальнейшее внедрение сенсорных и локально-региональных радиосетей связано с развитием направлений «Интернет вещей» и «промышленный Интернет вещей» [5], которые основаны на интеллектуализации человеческой деятельности в различных сферах, включая создание разумных изделий, домов, предприятий и городов.

Важными задачами при построении сенсорных, локально-региональных и глобальных (спутниковых, микроспутниковых) радиосетей широкого применения являются задачи повышения надежности, оперативности и защищенности (криптоустойчивости и помехоустойчивости) передачи различных данных, включая видеоданные (подвижные и неподвижные изображения), речевые сообщения, массивы измерительных сигналов, величин и двоичных данных.

Поскольку входные потоки двоичных данных средствами абонентских беспроводных сетей преобразуются в выходные потоки информационных пакетов (ИП), нерешенными задачами при построении и внедрении радиосетей различного назначения являются вопросы минимизации выходных потоков ИП в местах установки абонентских и объектных систем (АС и ОС) радиосетей с учетом из-

менения уровня шумов в измерительных цепях средств ввода сигналов, условий ввода видеоданных, а также уровня шумов в радиоканале.

Целью статьи является разработка теоретических и алгоритмических основ повышения эффективности пакетной передачи информации в радиосетях с учетом ограничения на производительность процессорных средств АС и ОС (в дальнейшем АС) радиосетей, реализации надежной, высокоскоростной и защищенной передачи информации в радиосетях с доступом к ресурсам сети Интернет. Направление развития и построения таких радиосетей получило название «высокоинформативные» (high information) или «информационно-эффективные радиосети» [6–8], а базовую основу эффективного функционирования АС и терминалов радиосетей составили алгоритмы обработки, кодирования и передачи информации, оптимизированные по быстрдействию и точности [8, 9]. От качества этих алгоритмов в значительной степени зависят системные характеристики радиосетей, включая максимальную скорость передачи информации, оперативность, надежность и защищенность передачи пакетов данных удаленным абонентам сети.

#### РЕАЛИЗАЦИЯ НАДЕЖНОЙ И ЗАЩИЩЕННОЙ ПЕРЕДАЧИ ВЫСОКОИНФОРМАТИВНЫХ ПАКЕТОВ ИНФОРМАЦИИ В РАДИОСЕТЯХ

Эффективность передачи информации в радиосетях достигается поддержкой парой удаленных абонентов (передатчиком и приемником ИП) текущей максимальной скорости передачи информации  $R_i \rightarrow R_{\max}$  при минимально необходимом энергетическом соотношении в радиоканале  $(E_{sc} / J_0)_n$  [3, 9]. Здесь  $E_{sc} = P_{sc} \cdot T_{sc}$  — энергия кодовой последовательности ( $T_{sc}$  и  $P_{sc}$  — соответственно интервал ее длительности и мощность);  $J_0 = J / F \gg N_0$  [3], где  $J$  — средняя мощность суммарных помех в радиоканале,  $F = 1 / 2T_b$  — величина рабочей полосы частот,  $T_b = T_{sc}$  — длительность битовой (наиболее простой) кодовой последовательности. Без усложнения аппаратно-программных средств цифровых и радиотехнических модулей АС радиосетей достижение  $R_{\max}$  основано на реализации абонентскими процессорами комплекса алгоритмов обработки сигналов и изображений, выявлении наиболее информативных и достоверных данных [8–10] в местах образования информационных потоков (в местах установки ОС и АС), кодировании данных, включая их сжатие с допустимыми потерями информации и без потерь [8], криптоустойчивое и помехоустойчивое кодирование данных [11, 12], перемешивание данных ИП, а также формирование и передачу ИП в виде компактных и защищенных кодово-сигнальных последовательностей [9, 13]. Для реализации абонентами радиосети эффективных алгоритмов сжатия и защиты данных, достижения максимального коэффициента их сжатия  $K_c \rightarrow K_{c \max}$ , поддержки необходимого энергетического соотношения кодовых последовательностей  $E_{sc} / J_0 \rightarrow (E_{sc} / J_0)_n$  в радиоканале целесообразно использовать высокопродуктивные абонентские процессоры. Поддержка максимальной скорости передачи информации в радиоканале требует от абонентов сети постоянного контроля состояния уровня шумов в радиоканале, минимизации входных потоков данных, которые при передаче преобразуются в выходные потоки ИП. Следовательно, текущая скорость передачи информации  $R_{i \max}$  зависит от многих факторов и параметров, которые представлены в следующей зависимости:

$$R_{i \max} = f(F, (E_{sc} / J_0)_n, 1/k_s, K_{c \max}, L, P_{CPU}, E_a),$$

где  $k_s$  — коэффициент, учитывающий качество возобновления фронтов цифровых сигналов [3],  $1 \leq L \leq B / 4$  — количество ортогональных сигналов, позволяющих организовать соответствующее число кодовых каналов передачи информации в радиоканале,  $P_{CPU}$  — максимальная производительность абонентского процессора,  $E_a$  — эффективность алгоритмов обработки и кодирования данных.

Параметры  $P_{CPU}$  и  $E_a$  существенно влияют на время обработки и кодирования данных, при этом для построения ОС мониторинговых радиосетей пред-

почтительны алгоритмы, оптимизированные по быстродействию и точности кодирования данных [8, 13]. С учетом программной реализации процессорными средствами АС радиосетей комплексного сжатия данных (мониторинговых сигналов и видеосигналов, защищенных массивов данных) максимальная скорость передачи информации без учета служебных данных пакетов определяется выражением

$$R_{i \max} = \frac{k_1(\delta_d^N) \cdot k_2 \cdot k_3(B_{\min}) \cdot L}{k_s \cdot T_b \cdot B_{\min}(\gamma_j)},$$

где  $k_1(\delta_d^N)$  — коэффициент сжатия сигналов (видеосигналов) с контролируемыми потерями информации в зависимости от допустимого уровня входных шумов  $\delta_d^N$  в окрестности существенных отсчетов сигналов [9],  $k_2$  — коэффициент сжатия данных без потерь,  $k_3(B_{\min})$  — коэффициент уменьшения длительности ИП в процессе формирования кодово-сигнальных последовательностей (КСП) пакетов [9, 13], который соответствует дополнительному коэффициенту сжатия данных без потерь в процессе передачи пакетов минимальной длительности,  $B(\gamma_j)$  — база канального сигнала, соответствующая коэффициенту расширения спектра полезного сигнала, выбирается адаптивно в зависимости от оценки текущего энергетического соотношения  $\gamma_j$  в радиоканале [14],  $j$  — величина временного отсчета оценки энергетического соотношения  $E_{sc}/J_0$ ,  $B_{\min}$  — минимальная база канальных сигналов (как правило, шумоподобных сигналов (ШПС)), обеспечивающая поддержку абонентами сети необходимого энергетического соотношения в радиоканале.

Поскольку минимальной единицей (порцией) информации в радиосетях является ИП, длина информационного кадра (ИК) которого может изменяться в больших пределах (как правило, сотни бит — единицы Кбит), а служебная информация (поля синхропоследовательностей, начала и окончания ИП, адресного поля, а также поля управления и проверочного кода) составляет от долей до единиц процентов длины ИК, эффективность передачи ИП абонентами сети и надежность доставки информации существенно зависят от условий радиовидимости, способов защиты канальных сигналов от помех, способов помехоустойчивого кодирования и возобновления утерянной двоичной информации абонентами сети.

Передача ИП в радиосетях осуществляется централизованно или децентрализованно в режиме передачи данных с обратной связью. При централизованной передаче пакетов центральная станция сети (ячейки) в ширококешательном режиме передает управляющий пакет-квитанцию (ПК), в нем сообщается о факте успешного приема предыдущего ИП и указывается адрес абонента, который должен передавать следующий ИП. В этом случае интервал занятости радиоканала (моноканала)  $t_3 = T_{УПК} + T_{ИП}$ , где  $T_{УПК}$  — длительность управляющего ПК (УПК);  $T_{ИП} = t_{сл} + T_{ИК} + t_{прк}$  — длительность ИП,  $t_{сл}$  — длительность служебных данных ИП, включая длительность синхропоследовательностей, адресных и управляющих данных,  $t_{прк}$  — длительность проверочного кода,  $T_{ИК} = l_{ИК} \cdot T_b$  — длительность ИК,  $l_{ИК}$  — количество бит ИК. Вероятность успешной передачи ИП при централизованном управлении, от которой существенно зависит надежность доставки информации в сети,  $P_{УПК} = P_{УПК} \cdot P_{ИП}$ , где  $P_{УПК}$  — вероятность успешной передачи УПК,  $P_{ИП}$  — вероятность успешной передачи ИП.

При децентрализованном управлении абоненты радиосети анализируют состояние радиоканала (занят/свободен) и в случае его освобождения реализуют процедуру множественного доступа к нему [1, 3, 14]. После успешной реализации последней абонент передает ИП и принимает ПК. Интервал занятости радиоканала в этом режиме  $t_3 = t_{др} + T_{ИП} + T_{ПК}$ , где  $t_{др}$  — интервал множественного доступа в радиоканал,  $T_{ПК}$  — длительность ПК. Вероятность успешной передачи ИП при децентрализованном управлении  $P_{УПК} = P_{др} \cdot P_{ИП} \cdot P_{ПК}$ , где  $P_{др}$  — вероятность успешного доступа абонента в радиоканал, что является основой бескон-

фликтной передачи ИП,  $P_{\text{ПК}}$  — вероятность успешной передачи ПК. Поэтому для реализации надежной, защищенной и высокоскоростной передачи ИП средствами АС необходимо максимальное сжатие входных потоков мониторинговых данных с выявлением наиболее информативных участков сигналов и видеосигналов (в дальнейшем сигналов), отсчеты которых кодируются наиболее точно и с максимально допустимой частотой выборки, а также преобразование сжатых и защищенных двоичных последовательностей массивов данных с длительностью  $T_b$  в выходные интервальные КСП ИП. Криптоустойчивое кодирование данных средствами АС осуществляется в процессе сжатия данных и при формировании КСП ИП. При этом кодовые ключи генерации криптоустойчивых псевдослучайных последовательностей, которые применяются в процессе кодирования данных по методу одноразового блокнота, а также коды формирования КСП текущих пакетов известны только абоненту-передатчику и абоненту-приемнику ИП. В результате комплексного кодирования входных потоков данных формируются выходные пакеты с повышенной информационной емкостью, при этом длительность ИП вычисляется выражением

$$T_{\text{ИП}} \approx \sum_{s=1}^{l_{sc}} T_{sc}^s < \sum_{i=1}^l T_{bi},$$

где  $T_{sc}^s$  — длительность  $s$ -й КСП ИП,  $T_{bi} = T_b$  — длительность  $i$ -й битовой последовательности закодированного массива данных,  $l_{sc}$  — максимальное количество КСП ИП.

При заданной рабочей полосе частот  $F$  и количестве бит ИК  $l_{\text{ИК}}$  эффективность передачи ИП тем выше, чем меньшая длительность интервала занятости радиоканала  $t_3$ , которая с учетом того, что  $t_{\text{др}} \ll t_{\text{сл}} \ll T_{\text{ПК}} \ll T_{\text{ИП}}$ , существенно зависит от длительности  $T_{\text{ИП}}$ .

В процессе преобразования двоичных последовательностей закодированных данных в интервальные КСП длительность  $T_{\text{ИП}}$  уменьшается приблизительно в 1,6–2,3 раза [9, 16]. Поскольку  $T_{\text{ИП}}$  существенно зависит от базы сигнала, важной задачей при повышении эффективности передачи ИП является выбор текущей минимальной базы КСП  $B_{sci} = B_{\min}$ , которая определяет необходимое энергетическое соотношение  $(E_{sc} / J_0)_n$  в радиоканале. Для независимого выбора  $B_{sci}$  абонент-передатчик ИП в первом тестовом пакете передает шумоподобные КСП (ШПС-КСП) с различными базами, выбранными в диапазоне  $1 \leq B_{sci} \leq B_{\max}$ , где  $B_{sci} = 1$  соответствует передаче  $n$ -битовых последовательностей в виде интервальных двухуровневых сигналов минимальной длительности. Данные КСП применяются при отсутствии заметных шумов в радиоканале. Выбор необходимого количества тестовых ШПС-КСП существенно влияет на сложность построения цифрового абонентского приемника ИП и зависит от количества независимых каналов корреляционной обработки принимаемых данных. Увеличение количества различных по величине тестовых ШПС позволяет оптимизировать выбор минимально необходимой базы  $B_{sci}$ , что в конечном итоге обеспечивает поддержку максимальной скорости передачи  $R_{i\max}$ . Поэтому количество тестовых ШПС целесообразно выбирать с учетом заданных параметров формирования, передачи и приема  $k_l$ -интервальных КСП, включая ШПС-КСП [9]. Здесь  $k$  определяет минимальное количество интервалов КСП ИП, а  $l$  задает максимальное количество возможных интервалов кодовых последовательностей ИП в диапазоне от  $T_{\min} = T_b$  до  $T_{\max} = T_b + (l-1)\Delta T$ , где  $\Delta T = k_s T_b$ ,  $k_s < 1$ , и выбирается в зависимости от вычисленного уровня шумов в радиоканале [14]. Величина  $k$  существенно зависит от выбора величины  $n$ ,  $n = 4, 8$ , и определяет количество независимо и одновременно работающих анализаторов принимаемых интервальных КСП и корреляционных вычислителей ШПС-КСП ( $k = 2, 3$ ) [9]. Количество тестовых ШПС зависит от  $k$  и, например, выбирается из ряда величин:  $B_{\min} = 7, 11, 13, 15, 31$ .

После приема соответствующих тестовых КСП и анализа выходных сигналов анализаторов интервальных последовательностей и выходных сигналов

корреляционных приемников ШПС абонент-приемник ИП в ПК сообщает абоненту-передатчику ИП о величине минимально необходимой базы  $B_{sci}$ , которая оптимальна для достоверной передачи КСП следующего ИП. После установления связи между абонентами ПК может передаваться для нескольких ИП. В результате после передачи одного или нескольких ИП и получения ответного ПК базу КСП последующих пакетов можно изменить с учетом уровня шумов в радиоканале.

Передача данных в радиосетях с  $R_{i\max}$ , как правило, сопровождается искажениями шумами радиоканала тех или иных КСП пакетов. Поэтому среди последовательностей верно принятых КСП возможны нераспознанные временные интервалы. Возобновление пораженных шумами кодовых последовательностей достигается на основе комплексного подхода к решению задачи исправления ошибок при передаче информации по радиоканалам с учетом априорной информации, заложенной в сжатые и защищенные массивы данных, а также с учетом значений битов проверочного кода ИП, внесенной зависимости между битами защищенного массива данных [11], результатов перемешивания битовых последовательностей ИК и КСП ИП, формирования выходных массивов данных с  $m \leq m_d$ , где  $m_d$  — допустимое количество соседних однотипных элементов в массиве данных. Для повышения вероятности достоверного возобновления искаженных данных ИП проверочные коды пакетов могут передаваться КСП с повышенной базой. В этом случае вследствие уникальности параметров последних (повышенная длительность или база сигнала) при заданных (фиксированных) длительностях ИК пакетов КСП проверочного кода ИП с учетом дополнительных данных являются признаком завершения пакета. На основе принятых и возобновленных двоичных данных искаженные битовые последовательности на коротких участках массивов данных возобновляются (угадываются) перебором соответствующих битовых последовательностей [11] при выполнении комплекса перечисленных ранее условий. В случае невозможности возобновления данных ПК запрашивает повторную передачу соответствующих КСП ИП.

Вероятность успешной передачи ИП, которая на практике определяет надежность связи, существенно зависит от выбора  $B_{\min}$  КСП пакетов. С учетом необходимости адаптации приемо-передатчиков АС к уровню шумов в радиоканале, что приводит к изменению базы КСП и длительности ИП в больших пределах, реальную скорость передачи информации в радиосети целесообразно определить для каждого пакета или группы пакетов с одинаковой текущей базой КСП ИП и ПК  $B_{sci}$ . С учетом служебных данных ИП скорость передачи информации для  $j$ -го пакета можно определить как количество полезной информации в битах (количество бит ИК пакета), переданное за время длительности текущего интервала занятости радиоканала

$$R_{\max}^j = I_{ИК}^j / t_3^j = I_{ИК}^j / (t_{др} + T_b [(l_{ИК} + l_{сл}^{ИП} + l_{ПК}) B_{\min}^j + l_{прк} B_{прк}^j]),$$

где  $I_{ИК}^j$  — количество бит ИК  $j$ -го пакета,  $l_{сл}^{ИП}$  — количество служебных данных ИП,  $l_{ПК}$  — количество бит ПК,  $l_{прк}$  — количество бит проверочного кода,  $B_{прк}^j$  — база ШПС  $j$ -го ПК.

При передаче ИП и ПК в виде КСП с заданной базой  $B_{sc}$  информационных и служебных данных, а также базой данных проверочного кода  $B_{прк} \geq B_{sc}$  скорость передачи информации в радиосети определяется формулой

$$R_{\max}^j = I_{ИК}^j / t_3^j = I_{ИК}^j / (t_{др} + \left( \sum_{i=1}^{n_{ИП}} T_{КСПи}^{ИП} + \sum_{i=1}^{n_{ПК}} T_{КСПи}^{ПК} \right) \cdot B_{\min}^j + \sum_{i=1}^{n_{прк}} T_{КСПи}^{прк} \cdot B_{прк}^j),$$

где  $n_{ИП}$  — количество КСП ИП,  $T_{КСПи}^{ИП}$  — длительность  $i$ -й КСП ИП,  $n_{ПК}$  — количество КСП ПК,  $T_{КСПи}^{ПК}$  — длительность  $i$ -й КСП ПК,  $n_{прк}$  — количество КСП проверочного кода ИП,  $T_{КСПи}^{прк}$  — длительность  $i$ -й КСП проверочного кода ИП.



Практической оценкой эффективности передачи пакетов информации может являться относительная величина  $\eta < 1$  [7], которая соответствует отношению суммарных временных потерь на передачу текущего ИП по отношению к минимальным временным затратам при передаче ИП с  $B_{sc} = 1$  ИП и ПК.

Таким образом, реализация надежной и защищенной передачи высокоинформативных пакетов информации зависит от комплекса алгоритмов кодирования, передачи и декодирования данных и достигается, прежде всего, преобразованием  $n$ -битовых последовательностей сжатых и защищенных массивов данных в интервальные КСП ИП и ПК, база  $B_{sc}$  которых не превышает величины  $B_{min}$ , а база КСП проверочных кодов ИП может превышать  $B_{min}$  и выбирается с учетом гарантированной передачи последних по радиоканалам с шумами. Для повышения надежности передачи пакетов информации КСП проверочных кодов могут передаваться повторно. Помимо оптимального выбора базы канальных сигналов, важны алгоритмы перемешивания данных и КСП пакетов, а также алгоритмы внесения взаимосвязей между соседними битами ИК пакетов. Поэтому в зависимости от уровня шумов в радиоканале важен выбор соответствующих алгоритмов оперативного помехоустойчивого кодирования и декодирования данных ИП.

#### **ЭФФЕКТИВНОЕ КОДИРОВАНИЕ ДАННЫХ, ФОРМИРОВАНИЕ И ПЕРЕДАЧА ИНТЕРВАЛЬНЫХ ПСЕВДОХАОТИЧЕСКИХ И ШУМОПОДОБНЫХ ИП**

В компьютерных радиосетях каждая АС является источником информационных потоков, пакетов информации, которые подлежат передаче и ретрансляции по общему для всех абонентов радиоканалу и каналам связи межсетевое взаимодействия. Поэтому от эффективности преобразования средствами АС входных потоков данных, включая измерительные сигналы, изображения, речевые сообщения и закодированные массивы данных в выходные потоки ИП, существенно зависят ключевые характеристики всей системы передачи информации — оперативность и надежность доставки информации, крипто- и помехозащищенность передачи данных. Основой повышения эффективности пакетной передачи информации в радиосетях является отбор наиболее информативных и достоверных данных и их компактное кодирование непосредственно в местах образования сетевых информационных потоков. Поскольку информация о событиях, природных явлениях и результатах исследований вводится в сеть передачи данных в виде сигналов и измерительных величин, которые являются первичными информационными образами поведения и функционирования объектов исследования (ОИ), в процессе обработки и кодирования входных данных важно выявлять наиболее информативные и достоверные отсчеты. В сигналах такими параметрами есть экстремумы и точки перегиба кривой, которые относятся к существенным отсчетам (СО) огибающих сигналов. Точность кодирования амплитудно-временных параметров СО значительно зависит от особенностей прикладных исследований, условий ввода данных (отсутствие или наличие шумов в измерительных цепях [6, 8]), функциональной ориентации АС и ОС радиосетей и выбирается адаптивно, например, среди следующих режимов кодирования отсчетов сигналов:

— точное кодирование амплитудных значений экстремумов с  $q_{max} \geq 10-12$  бит и с  $f_{on\ min} = k_d f_{c\ max}$ , где  $f_{on\ min}$  — минимальная частота опроса (дискретизации) сигнала,  $k_d \geq 10$  — коэффициент увеличения частоты дискретизации, который задается исследователем [14],  $f_{c\ max}$  — максимальная информативная частота сигнала (этот режим применяется для обеспечения достоверных минимальных информационных потоков в сети);

— менее точное кодирование амплитудных значений экстремумов с  $q_{min} = 6,7$  бит и минимальной частотой опроса  $f_{on\ min} = 2f_{c\ max}$ , при этом низкоамплитудные экстремумы и некоторые рядом находящиеся экстремумы игнорируются с учетом минимального искажения визуальных характеристик огибающей сигнала (применяется при кодировании зашумленных участков сигналов);

— точное кодирование амплитудно-временных параметров экстремумов и точек перегиба с  $q_{max}$  и  $f_{on\ max}$ ;

— точное кодирование параметров СО и промежуточных отсчетов на наиболее информативных участках сигналов с повышенной частотой опроса.

В зависимости от задач дистанционного мониторинга состояний ОИ и контроля различных процессов возможен выбор определенных комбинаций режимов кодирования входных данных. На основе параметров СО вычисляются показатели информативности участков и фрагментов сигналов [10, 14], а также осуществляется экспресс-анализ состояний объектов с вычислением спектральных, корреляционных, энтропийных, хаотических и других показателей сигналов [14, 17].

Кодирование видеоданных при ограниченных ресурсах процессора ОС основано на реализации алгоритмов оперативного выявления объектов видеоданных с применением сигнального подхода [10], при котором из совокупности СО выделяются наиболее информативные, весомые СО. По показателям информативности весомых отсчетов выделяются наиболее информативные участки видеосигналов с последующим поиском объектов и ключевых кадров видеоданных [14]. С учетом ограниченной пропускной способности радиоканалов сенсорных сетей для эффективной передачи потокового видео с заданным качеством кадров видеоданных ОС выявляют, накапливают и передают компактные и защищенные данные ключевых кадров с высоким разрешением, например, Full HD, а также передают текущие разностные видеоданные весомых СО текущих кадров с их выбранной (максимально допустимой) частотой и разрешением. В случае необходимости передачи от ОС фрагментов высококачественного видео центральная станция сети передает запрос соответствующим абонентам, которые после компактного и защищенного кодирования видеоданных накапливают их и передают удаленным АС с текущей пропускной способностью радиоканалов. Этот режим передачи, как правило, ориентирован на качественный и выборочный видеомониторинг ожидаемых процессов и непродолжительных событий, при этом воспроизведение видеоданных осуществляется с некоторыми задержками.

В процессе компактного кодирования двоичных данных амплитудно-временных параметров СО сигналов и видеосигналов (в дальнейшем сигналов) последовательно формируются сжатые массивы данных с кодированием участков сигналов с применением максимального количества бит АЦП  $q_{\max}$  (кодирование наиболее достоверных и информативных участков сигналов) и с применением минимального количества бит АЦП  $q_{\min}$  (кодирование менее информативных участков сигналов). Битовые потоки выходных компактных данных чередующихся достоверных и менее достоверных участков сигналов формируются с полем общей служебной информации  $\{СИ_0^j\}$ , а также с полями  $\{СИ_{ПА}^j\}$  служебной информации параметров адаптации  $j$ -го участка сигнала и с полями  $\{КК_{СО}^{jn_j}\}$  компактных кодов СО  $j$ -го участка сигнала [9], где  $n_j$  — максимальное количество СО  $j$ -го участка сигнала. При потоковом компактном кодировании СО участков текущих выборок сигналов с определением служебной информации параметров адаптации  $\{СИ_{ПА}^j\}$  компактные коды СО кодируются с учетом того, что амплитудное значение первого СО участка кодируется полноразрядным кодом с  $q_{\max}$  или  $q_{\min}$ , а коды амплитудных значений и номера последующих СО кодируются разностными кодами. Компактные данные  $j$ -го участка текущей выборки сигнала кодируются следующей последовательностью двоичных кодов:

$$\{СИ_{ПА}^j\} \{КК_{СО}^j\} = \{(BK)(N)(m)(b)(N_{СО}^j)\} \{(A_{СОn})(\Delta N_{iHO})(\Delta A_{iCO})$$

$$(\Delta N_{2HO})(\Delta A_{2CO}) \dots (\Delta N_{iHO})(\Delta A_{iCO}) \dots (\Delta N_{(w-1)CO})(\Delta A_{(w-1)CO})\},$$

где BK — вид кодирования;  $N$  —  $N$ -битовый код для кодирования предварительно вычисленного количества  $R_{i\max}(N_{СО}^0)СО$   $j$ -го участка;  $m$  —  $m$ -битовый код количества  $\Delta n$  бит для кодирования разностных (со знаком) амплитудных значений соседних СО;  $b$  —  $b$ -битовый код количества  $\Delta l$  бит для кодирования разности между номерами соседних СО, что соответствует

количеству промежуточных несущественных отсчетов (НО) между соседними СО, увеличенному на единицу;  $A_{CO_n}$  — амплитудное значение первого СО полноразрядного;  $\Delta N_{iHO}$  —  $\Delta l$ -битовый код для кодирования разности между номерами  $i$ -го и  $(i-1)$ -го СО;  $\Delta A_{iCO}$  —  $\Delta n$ -битовый код со знаком для кодирования разности амплитудных значений между  $i$ -м и  $(i-1)$ -м СО;  $w$  — максимальное количество СО текущего участка ( $w = N_{CO}^j$ ).

Для минимизации служебных данных код  $\{СИ_{ПА}^0\}$  состоит из  $\nu$ -битового кода ВК, длина которого зависит от проблемной ориентации ОС радиосетей. Параметры детализации  $\nu$ -битового кода содержатся в поле  $\{СИ_0\}$ .

Дальнейшее сжатие массивов избыточных данных достигается в процессе программной реализации оперативных методов сжатия  $n$ -битовых последовательностей массивов данных [8, 9]. Для защиты сжатых данных от доступа к ним и их подмены несанкционированными абонентами сенсорных и локально-региональных радиосетей с учетом ограниченной производительности процессоров АС радиосетей криптозащита данных осуществляется в процессе сжатия данных без потерь [10, 14], преобразования сжатых и защищенных (криптоустойчивых и помехоустойчивых) массивов данных в последовательности битов с  $m \leq m_d$  [9, 16], а также в процессе формирования интервальных КСП (ШПС-КСП), где  $m_d$  — максимальное количество соседних однотипных битов. Основой криптозащиты данных является асимметричная криптография, алгоритмами которой обеспечивается шифрование сеансовых ключей. Первичные закрытые ключи абоненты радиосетей получают автоматически, например, на этапе установки ОС на объектах мониторинга, и могут их периодически менять с учетом наличия свободного времени на выполнение вычислительных операций при решении задач дискретного логарифмирования. Таким образом, два абонента радиосети, принимающих участие в передаче и приеме текущих пакетов, с учетом данных сеансового ключа генерируют криптоустойчивые псевдослучайные последовательности, которые применяются для шифрования передаваемых данных [12, 15]. В результате такого подхода на информационном уровне вычислительными ресурсами абонентов формируются и передаются в радиоканал последовательности зашифрованных интервально-импульсных или шумоподобных сигналов, которые невозможно принять и расшифровать без знания закрытых абонентских ключей.

Эффективная передача данных по радиоканалам от удаленных ОИ и подвижных объектов основана на поддержке абонентами сети минимально необходимой энергетики в радиоканале, ретрансляции данных на большие расстояния в условиях прямой видимости абонентских приемопередающих антенн. С учетом наличия шумов в радиоканалах реализация надежной, высокоскоростной и защищенной передачи данных достигается преобразованием  $n$ -битовых последовательностей сжатых, зашифрованных и закодированных массивов данных в  $k_l$ -интервальные ШПС [9, 16]. Для построения несложных абонентских цифровых приемников ШПС  $k = 2, 3$ , т.е. соответствующие  $n$ -битовые последовательности передаются двумя или тремя интервальными ШПС длительностью  $T_{ШПС} = N_B \cdot \tau_i$ , где  $N_B$  — количество элементов ШПС,  $\tau_i \geq T_b$  — длительность элемента  $i$ -го ШПС. Путем псевдохаотического выбора параметров  $n, m_d, k, l, N_B$  и  $\tau_i$  реализуется криптоустойчивая передача шумоподобных пакетов на канальном уровне. В целях постоянной поддержки текущей максимальной скорости передачи пакетов информации в радиосети центральная станция отслеживает уровень шумов в радиоканале и в УПК сообщает абонентам о рекомендуемой величине  $B_{\min}$ .

При децентрализованной передаче ИП между удаленными абонентами сети выбор  $B_{\min}$  целесообразен после анализа пакета с тестовыми ШПС-КСП в точке приема информации [15]. Для оптимизации выбора  $B_{\min}$  из ряда возможных ШПС с различной базой при ограниченном количестве каналов приема и анализа ШПС-КСП абонентского приемника с учетом принятых управляющих данных тестового пакета каждый канал корреляционной обработки ШПС принимает и



анализирует соответствующее количество (на практике не более двух-трех) тестовых ШПС с различными по величине базами  $B_{sc}$ . Решение о выборе соответствующего ШПС с  $B_{sc} = B_{min}$  при моноканальной передаче пакетов ( $L = 1$ ) основано на анализе величины основного пика корреляционной, например, модульной функции [14], приблизительно в середине интервала последнего элемента текущего ШПС. Поскольку после передачи ШПС-КСП по радиоканалу с шумами и его приема величина базы ШПС распределяется на составляющие  $B_{max} = \Pi_{ш} + M + H$ ,  $\Pi_{ш} \approx 0,5B_{max}$  — порог распознавания полезного сигнала от шумовых составляющих радиоканала [18], условием надежной передачи информации по радиоканалам, например, КСП с уровнем логической единицы, с учетом маскирования факта передачи данных в шумах беспроводных сетей является совокупность следующих выражений:

$$\begin{cases} B_{max} / 2 + H_{min} < G(j) \leq B_{max} / 2 + H_{max} & \text{— прием единичной КСП,} \\ B_{max} / 2 - H_{max} \leq G(j) < B_{max} / 2 - H_{min} & \text{— прием нулевой КСП,} \\ B_{max} / 2 - H_{min} < G(j) < B_{max} / 2 + H_{min} & \text{— прием недостоверных данных,} \\ B_{max} / 2 + H_{max} < G(j) < B_{max} / 2 - H_{max} & \text{— прием КСП с избыточной базой,} \end{cases}$$

где  $H < M < B_{max} / 2 + H_{max}$  — оценка уровня шумов в радиоканале, в котором обеспечивается достоверный прием информации;  $H$  — оценка качества приема КСП;  $H_{min} > 1$  — минимальное значение оценки качества приема КСП ( $H_{min} = 2$ );  $G(j)$  — значение модульной функции ШПС при  $j$ -м сдвиге [14];  $H_{max}$  — максимальное значение оценки качества приема КСП ( $H_{max} < H_{max} < B_{max} / 2 - H_{min}$ ).

При передаче информации по нескольким моноканалам ( $1 < L < B_{max} / 4$ ) основной пик модульной функции уменьшается на величину  $L$ . Следовательно, для оптимального выбора  $B_{min}$  по результатам анализа приема тестовых ШПС, например, с последовательно увеличивающимися базами, за основу  $B_{sc} = B_{min}$  выбирается база того ШПС, величина которой первой отвечает требованиям маскирования передачи данных в шумах радиоканала. При этом база предыдущего тестового ШПС вследствие недостаточной величины не соответствует условиям маскирования передачи данных в шумах радиоканала, а база последующего ШПС соответствует условиям достоверной передачи данных. В результате такого подхода выбирается минимально избыточная база КСП-ШПС, достоверный прием которых позволяет организовать эффективную передачу высокоинформативных пакетов информации, а за счет реализации абонентами радиосети комплекса алгоритмов помехоустойчивого кодирования и декодирования данных обеспечивается эффективное возобновление данных, искаженных канальными помехами.

#### ЗАКЛЮЧЕНИЕ

Основой повышения эффективности передачи ИП в радиосетях является выбор наиболее информативных и достоверных данных, включая существенные и весомые отсчеты сигналов и видеосигналов, их компактное кодирование в местах образования сетевых информационных потоков, а также реализация абонентскими процессорами комплекса алгоритмов, эффективных по быстродействию и точности кодирования, а именно алгоритмов оперативного шифрования и помехоустойчивого кодирования данных, преобразования  $n$ -битовых последовательностей сжатых, зашифрованных и закодированных массивов данных в интервальные кодово-сигнальные последовательности с переменной базой. Основой криптозащиты данных процессорными средствами абонентских систем радиосетей является асимметричная криптография, алгоритмами которой обеспечивается шифрование сеансовых ключей. При этом криптозащита данных осуществляется в процессе их сжатия без потерь и при формировании КСП ИП. В результате абонентами формируются и передаются в радиоканал

высокоинформативные пакеты данных, основу которых составляют последовательности зашифрованных интервально-импульсных или шумоподобных сигналов с минимально необходимой базой. В зависимости от уровня шумов в радиоканале важен выбор базы шумоподобных пакетов, проверочных кодов, а также алгоритмов внесения зависимостей между соседними битами зашифрованных данных, перемешивания данных и КСП ИП.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бунин С.Г., Войтер А.П., Ильченко М.Е., Романюк В.А. Самоорганизующиеся радиосети со сверхширокополосными сигналами. — К.: НПП Изд-во Наук. думка НАН Украины, 2013. — 444 с.
2. Ильченко М.Ю., Кравчук С.О. Сучасні телекомунікаційні системи. — К.: НВП Видавництво Наук. думка НАН України, 2008. — 328 с.
3. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. — 2-е изд.: Пер. с англ. — М.: Издательский дом «Вильямс», 2003. — 1104 с.
4. Шахнович И.В. Современные технологии беспроводной связи. — М.: Техносфера, 2006. — 288 с.
5. Филиппи Б. Создавая промышленный интернет вещей / [www.ua.automation.com](http://www.ua.automation.com)
6. Шевчук Б.М. Теоретичні основи побудови високоінформативних інтелектуальних радіомереж обробки і передачі інформації // Праці міжнародного симпозиуму «Питання оптимізації обчислень (ПОО-XXXIII)», присвяченого 50-річчю створення Інституту кібернетики імені В.М. Глушкова НАН України (Кацивелі, 23–28 вересня 2007 р.). — К. — С. 310–311.
7. Шевчук Б.М. Методи побудови інформаційно-ефективних комп'ютерних мереж / Праці міжнародного симпозиуму «Питання оптимізації обчислень (ПОО-XXXV)». — Т. 2. (Кацивелі, 24–29 вересня, 2009). — К. — С. 400–405.
8. Шевчук Б.М., Задірака В.К., Фраєр С.В. Алгоритмічні основи підвищення інформаційної ефективності передачі даних в сенсорних мережах // Комп'ютерні засоби, мережі та системи. — 2013. — № 12. — С. 140–149.
9. Шевчук Б.М. Оптимизированные по быстродействию и точности кодирования методы и алгоритмы повышения информационной эффективности абонентских систем беспроводных сетей // Кибернетика и системный анализ. — 2014. — № 6. — С. 137–151.
10. Шевчук Б.М., Задірака В.К., Фраєр С.В., Луц В.К. Оперативне розпізнавання фрагментів і комплексів сигналів та визначення параметрів об'єктів відеоданих засобами об'єктних систем безпроводних мереж // Штучний інтелект. — 2013. — № 3. — С. 275–283.
11. Шевчук Б.М. Системний підхід до вирішення проблем оптимізації обчислень засобами об'єктних систем сенсорних мереж // Інформаційні технології та комп'ютерна інженерія. — 2013. — № 1. — С. 88–95.
12. Шевчук Б.М. Оперативне формування і передавання компактних, криптистійких та завадостійких пакетів інформації в радіомережах // Комп'ютерні засоби, мережі та системи. — 2011. — № 10. — С. 143–152.
13. Шевчук Б.М. Формування кодово-сигнальних послідовностей об'єктними системами безпроводових сенсорних мереж // Праці міжнар. конф. Питання оптимізації обчислень (ПОО-XL), присвяченої 90-річчю від дня народження В.М. Глушкова, 30 вересня — 1 жовтня. К., 2013. — С. 277–278.
14. Шевчук Б.М., Задірака В.К., Гнатів Л.О., Фраєр С.В. Технологія багатофункціональної обробки і передачі інформації в моніторингових мережах. — К.: Наук. думка, 2010. — 370 с.
15. Шевчук Б.М. Надійна і захищена передача інформації в радіомережах промислового призначення та для зв'язку між мобільними роботами і рухомими системами // Штучний інтелект. — 2012. — № 2. — С. 80–87.
16. Шевчук Б.М., Задірака В.К., Фраєр С.В. Підвищення ефективності передачі інформації в моніторингових мережах на основі оптимізації обчислень в процесі кодування даних засобами об'єктних систем сенсорних мереж // УСиМ. — 2015. — № 3. — С. 65–71.
17. Николайчук Я.Н. Теория источников информации. — 2-е изд. — Тернополь: ООО «Терно-граф», 2010. — 536 с.
18. Гераїмчук М.Д., Івахів О.В., Паламар М.І. та ін. / Основи побудови перспективних безпроводових сенсорних мереж. — К.: ЕКМО, 2010. — 124 с.

*Поступила 03.07.2015*