УДК 621.391.7

А.И. ЦОПА, канд. техн. наук

КРИТЕРИИ ОЦЕНКИ И ПУТИ ПОВЫШЕНИЯ ЗАЩИЩЕННОСТИ КАНАЛОВ СВЯЗИ ЦИФРОВЫХ СИСТЕМ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ФИЗИЧЕСКОМ УРОВНЕ

Введение

Современный этап развития цифровых систем передачи информации (ЦСПИ) связан с технологическим прорывом в области микроэлектроники и глобальной интеграцией различных технологий как по назначению, так и по принципу действия [1].

При создании интегрированных производительных ведомственных систем связи (ВСС) одним из основных требований, предъявляемых к ЦСПИ, является обеспечение защищенности каналов связи. Несмотря на большое количество разработанных протоколов защиты информации на верхних ступенях семиуровневой модели взаимодействия открытых систем (*OSI*), эффективность их значительно снижается при передаче в ВСС мультимедийной информации [2]. Кроме того, при массовом внедрении цифровых технологий передачи информации обеспечить повышенные требования безопасности только одними информационными (криптографическими) методами не представляется возможным. В этих условиях необходимо искать новые пути повышения защищенности каналов связи не только на информационном, но и на физическом (энергетическом) уровне модели *OSI*.

Защищенность канала связи ЦСПИ характеризуется двумя основными параметрами: помехозащищенностью и скрытностью, которые позволяют ВВС решать задачи обеспечения связи при целенаправленных действиях нарушителя [3]. В известных работах оценка этих основных параметров защищенности ведется отдельно с использованием различных частных моделей, что не позволяет получить комплексную оценку защищенности канала связи.

Цель работы - выработка критериев и моделей оценки защищенности (помехозащищенности и скрытности) цифровых систем передачи информации, основанных на известной концепции отводного канала. Это позволяет не только определить новые пути повышения защищенности каналов связи на физическом уровне, но и оценить возможности межуровневой интеграции механизмов и средств защиты информации.

Основная часть

Одним из главных направлений развития ЦСПИ для ВСС является интеграция проводных и беспроводных технологий передачи информации.

В настоящее время в проводном сегменте ВСС доминируют различные широкополосные *xDSL* технологии, обеспечивающие высокую скорость передачи информации по существующим кабельным линиям связи (КЛС).

В сегменте беспроводных технологий абонентского доступа ведущие позиции занимают технологии *Wi-Fi*, на которых строятся ЦСПИ для локальных сетей (*WLAN*), и технологии *WiMAX*, на которых строятся ЦСПИ для городских сетей (*WMAN*).

Один из вариантов интеграции различных технологий и ЦСПИ при разворачивании информационной сети доступа в зоне кризисной или чрезвычайной ситуации (ЧС) приведен на рис. 1 [4].

Интегрированная сеть доступа включает в себя нескольких подсистем и сетей: сеть проводного доступа (СПД), сеть абонентского радиодоступа (САРД), сеть телемедицины, сенсорную распределенная радиосеть и командную радиосистему (КРС). Базовые станции (БС) системы радиодоступа подключаются по проводной сети к мультиплексору доступа (МД), который обеспечивает концентрацию информационных потоков и подключение к

серверу данных оперативного штаба. Для передачи информации на дальние расстояния в центр принятия решений используются проводные многоканальные ЦСПИ.

Также при организации связи в зоне ЧС в ряде случаев может понадобиться высотная телекоммуникационная платформа, обеспечивающая активную ретрансляцию радиосигналов и расширение оперативной глубины зоны радиодоступа.

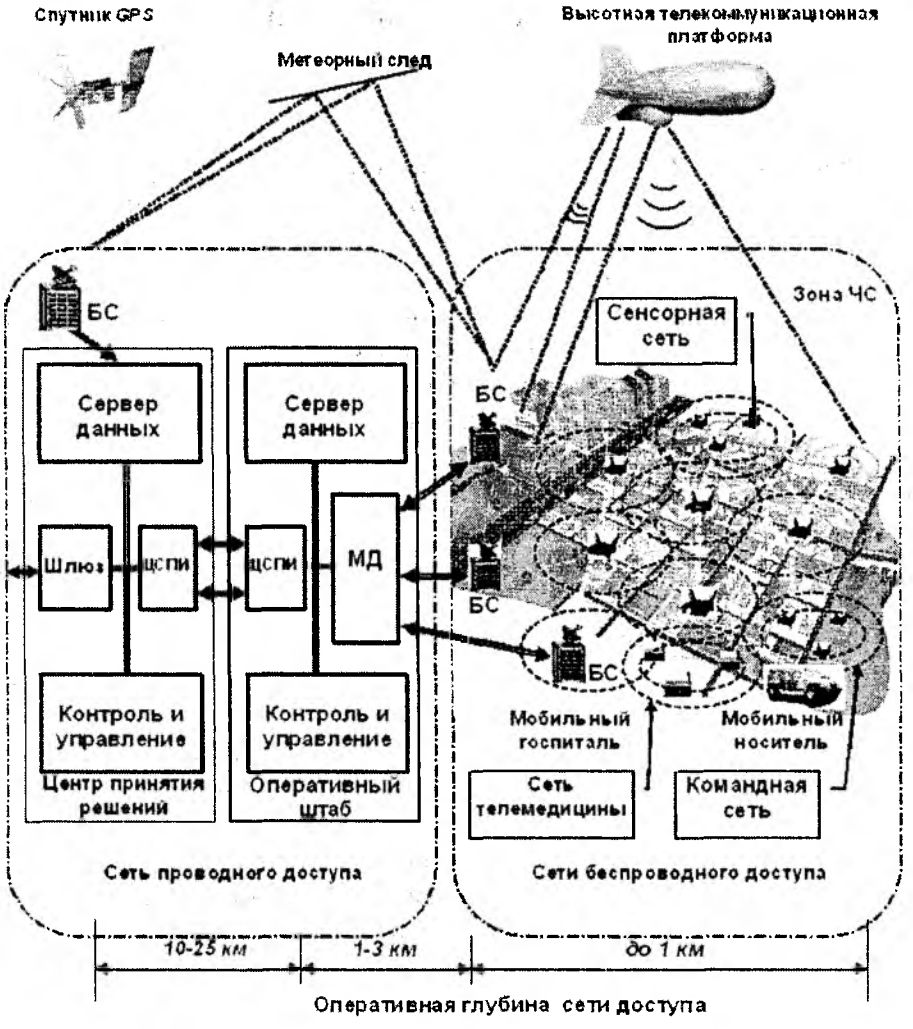

Рис. 1

В значительно мере повысить надежность связи в зоне ЧС, особенно в труднодоступных районах, может также интеграция в ЦСПИ метеорного радиоканала (МРК). Благодаря направленному характеру распространения отражённых от метеорных следов радиоволн заметно повышается энергетический потенциал линии связи и ограничивается возможность перехвата сообщений, передаваемых по метеорному каналу связи [5].

Обеспечение защищенности ЦСПИ, входящих в эту разветвленную ведомственную сеть связи (ВСС), является одной из основных задач, которые необходимо решать при разработке отдельных элементов системы доступа и системы в целом.

Основоположником информационного подхода при создании безопасных систем связи является Шеннон К., положивший начало не только науке криптографии, но и науке кодирования канала связи. В своих работах он ввел понятие совершенной секретной системы связи и указал на способ построения не раскрываемого ключа [6].

Другой подход решения задачи повышения защищенности канала связи базируется на теории потенциальной помехоустойчивости, которая определяет предельную помехоустойчивость системы связи при разных видах модуляции сигнала. Котельников В.А.

предложил повышать помехоустойчивость системы связи на основе учета статистических свойств помех и ввел оценку защищенности канала связи на основе вероятности правильного приема символа оптимальным приемником [7].

Дальнейшим развитием теории построения защищенных систем связи является модель отводного канала, предложенная Вайнером А. В этой модели рассматривается ситуация, когда в канале связи имеется шум и вероятность ошибки в канале противника (отводном канале) выше, чем для основного канала, по которому легитимные абоненты обмениваются сообщениями [8]. При таком предположении и применении специальной системы кодирования возможно достижение совершенной стойкости криптосистемы с существенно меньшими требованиями к длине ключевой информации, чем в модели Шеннона.

Развитие концепции отводного канала дает возможность достичь высокой защищенности канала на физическом уровне модели *OSI* без применения криптографических методов защиты.

Для более полной оценки параметров защищенности каналов связи необходимо учитывать то, что нарушитель может не только перехватывать информацию, передаваемую в легитимном канале связи, но и целенаправленно воздействовать на этот канал генератором помех. На рис. 2 показана структурная схема модели ЦСПИ с отводным каналом (каналом утечки), учитывающая эти особенности.

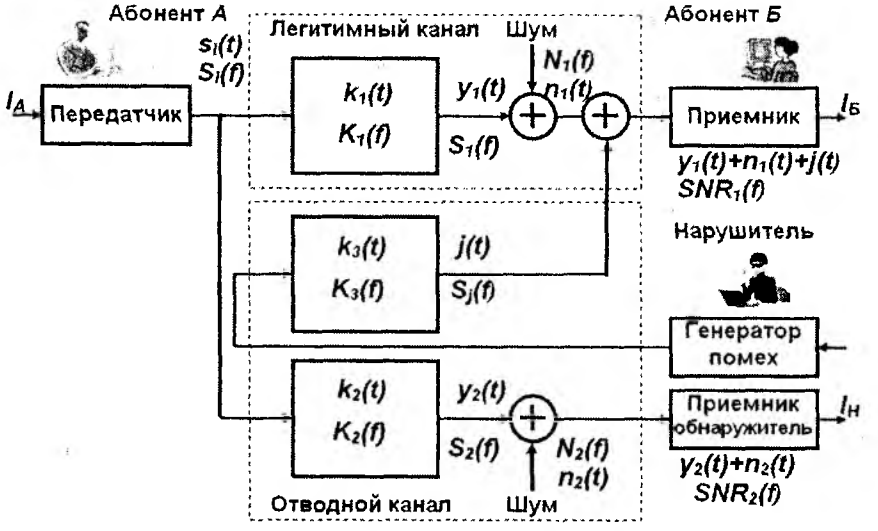

Рис. 2

Если в качестве критерия оценки эффективности работы ЦСПИ принять вероятностный критерий оценки меры успешности выполнения поставленной задачи [9], то в качестве критерия защищенности целесообразно использовать вероятность выполнения задачи передачи информации с заданными показателями качества в условиях радиоэлектронного противодействия (РЭП). Такой подход устанавливает взаимосвязь между эффективностью работа системы связи и ее защищенностью. Учитывая случайный характер характеристик канала связи и возможностей нарушителя по противодействию работы легитимного канала, критерий защищенности канала связи можно представить в форме вероятности сложного события $P_З$, являющегося суммой двух элементарных событий: вероятности скрытной работы $P_{СКР}$, и помехозащищенности канала $P_{ПЗ}$ [10]:

$$P_З = P_{СКР} + P_{ПЗ} - P_{СКР} \cdot P_{ПЗ} = 1 - P_Р \cdot P_П . \qquad (1)$$

где $P_Р = (1 - P_{СКР})$ – вероятность разведки канала связи; $P_П = (1 - P_{ПЗ})$ – вероятность подавления канала связи помехой.

Так как эффективность мер РЭП нарушителем в значительной мере зависит от выполнения этапа разведки канала связи, то рассмотрим сначала критерии оценки скрытности системы связи и определим пути ее увеличения.

Как правило, радиотехническая разведка предполагает последовательное выполнение трех основных задач: обнаружение факта работы радиосистемы (обнаружение сигнала), определение структуры обнаруженного сигнала (на основе ряда его параметров) и раскрытие содержащейся (передаваемой) в сигнале информации [11].

Перечисленным задачам разведки канала связи нарушителем могут быть противопоставлены три вида скрытности сигналов: энергетическая, структурная и информационная [12]. В этом случае скрытность работы канала связи можно оценить вероятностью скрытной работы

$$P_{СКР} = 1 - P_{Р} = 1 - P_{ОБН} \cdot P_{СТР} \cdot P_{ИНФ}, \qquad (2)$$

где $P_{ОБН}$ – вероятность обнаружения сигнала или факта работы канала связи; $P_{СТР}$ – вероятность раскрытия структуры сигнала; $P_{ИНФ}$ – вероятность раскрытия смысла передавае-мой информации.

Нужно заметить, что кроме энергетической скрытности существует еще ряд видов скрытности, направленных на исключение или существенное затруднение обнаружения сигналов системы связи. Это – частотная, временная, поляризационная, пространственная, маскировочная и другие виды скрытности, которые могут проявляться в различных сочетаниях и реализуются на физическом уровне канала связи.

Основными критериями оценки энергетической скрытности канала связи кроме вероятности обнаружения сигнала $P_{ОБН}$ при заданной вероятности ложной тревоги является отношение сигнал/шум на входе приемника обнаружителя SNR_2, обеспечивающее заданную вероятность обнаружения $P_{ОБНЗ}$, и радиус обнаружения сигнала $R_{ОБН}$ при задан-ном отношении сигнал/шум на входе приемника обнаружителя $SNR_{2\ ЗАД}$.

Последний показатель находит применение при решении целого ряда практических задач, связанных с разработкой организационно-технических мероприятий и определением размеров контролируемых зон. Если предположить, что в приемнике-обнаружителе реализованы оптимальные или квазиоптимальные алгоритмы обнаружения сигналов, то радиус обнаружения можно приближенно определить из выражения

$$R_{ОБН} = \frac{\lambda}{4\pi} \cdot \left[\frac{P_{ПЕР} \cdot G_{ПЕР} \cdot G_{ПР\ О}}{P_{ПР\ О} \cdot PL_{О} \cdot SNR_2} \right]^{1/2}, \qquad (3)$$

где λ – длина волны передатчика ВСС; $P_{ПЕР}$ – мощность передатчика ВСС; $G_{ПЕР}$ – коэффициент направленного действия антенны передатчика ВСС; $G_{ПР\ О}$ – коэффициент направленного действия антенны приемника-обнаружителя; $P_{ПР\ О}$ – чувствительность приемника-обнаружителя; $PL_{О}(Path\ Loss)$ – величина потерь на радиотрассе между ВСС и приемником-обнаружителем, связанными с условиями распространения сигнала; SNR_2 – отношение сигнал/шум на входе приемника-обнаружителя при заданных параметрах качества обнаружения сигнала ВСС.

Для оценки уровня энергетической скрытности радиолинии в зависимости от ее параметров и характеристик приемника-обнаружителя рассмотрим более детально структурную схему отводного канала в режиме перехвата, приведенную на рис. 3.

Будем считать, что ЦСПИ работает со скоростью передачи информации $R = 1/T$ (*бит/с*), с заданными показателем качества (с требуемой вероятностью битовой ошибкой P_b) и при определенном виде модуляции сигнала, которая задает значение энергии сигнала на бит информации E_B.

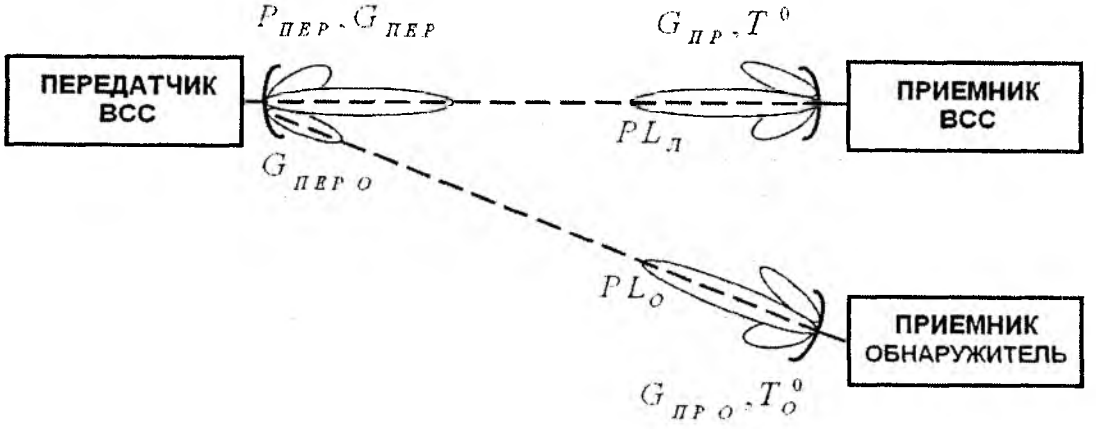

Рис. 3

Тогда условие перехвата сигнала ВСС может быть выражено неравенством [12], которое можно представить в виде нескольких сомножителей, характеризующих основные параметры канала связи

$$\underbrace{\left(\frac{G_{ПР}}{T^0}\right)}_{1}\cdot\underbrace{\left(\frac{G_{ПЕР}}{G_{ПЕР\,О}}\right)}_{2}\cdot\underbrace{\left(\frac{PL_Л}{PL_О}\right)}_{3}\cdot\underbrace{\left(\frac{1}{k_З}\right)}_{4}\cdot\underbrace{\left[\frac{1}{\left(\frac{2E_B}{N_0}\right)\cdot\frac{1}{T}\cdot\left(\frac{T_И}{F}\right)}\right]}_{5}\le\underbrace{\left[\frac{G_{ПР\,О}}{T_О^0\cdot z_О}\right]}_{6}, \qquad (4)$$

где 1 – характеристики приемника ЦСПИ: коэффициент направленного действия антенны приемника $G_{ПР}$ и шумовая температура приемника T^0; 2 – характеристики передающей антенны ЦСПИ: коэффициент направленного действия антенны передатчика $G_{ПЕР}$ и коэффициент направленного действия антенны передатчика по направлению к приемнику-обнаружителю $G_{ПЕР\,О}$; 3 – потери в линии связи: для легитимного канала $PL_Л$ и канала нарушителя $PL_О$; 4 – коэффициент запаса по мощности $k_З$; 5 – коэффициент, опреде-ляющий параметры модуляции и широкополосности сигнала: E_B – энергия сигнала на бит информации; $N_О$ – спектральная плотность шума; $F \cdot T = B$ – база сигнала; $T_И$ – время интегрирования сигнала в приемнике-обнаружителе; 6 – параметры приемника-обнаружителя, характеризующие его техническое совершенство и опасность перехвата: коэффициент направленного действия антенны приемника-обнаружителя $G_{ПР\,О}$, шумовая температура приемника-обнаружителя T^0, порог обнаружения $z_О$.

Из выражения (4) следует несколько важных выводов для практики построения защищенных каналов связи. Для увеличения энергетической скрытности легитимного канала связи, т.е. уменьшения отношения сигнал/шум на выходе линейной части приемника обнаружителя, необходимо:

- использовать передачу с минимально возможным показателем качества;

- использовать в канале направленные антенны с минимально возможным уровнем боковых лепестков;

- использовать приемник с малым уровнем собственных шумов;

- потери на распространение электромагнитной энергии сигнала на трассе легитимного канала должны быть значительно меньше, чем потери на трассе нарушителя ($PL_Л \ll PL_О$);

- использовать в качестве сигнала-переносчика сложные сигналы с наибольшим значением базы ($B_C \gg 1$) [10].

Выполнение этих условий является сложной научно-технической задачей, решение которой определяется уровнем развития различных областей радиоэлектроники.

Далее рассмотрим критерии оценки помехозащищенности ЦСПИ, показывающие способность ВСС противостоять влиянию помех естественного и искусственного происхождения. Поскольку помехозащищенность также зависит от ряда случайных факторов, то ее количественной мерой может быть вероятность подавления помехами канала связи $P_П$, которую можно определить как вероятность того, что фактическое значение отношение сигнал/шум на входе приемника ЦСПИ, станет меньше некоторого критического значения $SNR_{КР}$, при котором нарушается функционирование системы связи.

$$P_П = P\left(SNR \le SNR_{КР}\right) \tag{5}$$

Рассмотрим представленную на рис. 4 структурную схему отводного канала связи ЦСПИ при воздействии помех и определим условия подавления радиоканала при допущении, что спектральная плотность преднамеренной помехи $N_п$ значительно превышает спектральную плотность естественного шума $N_о$.

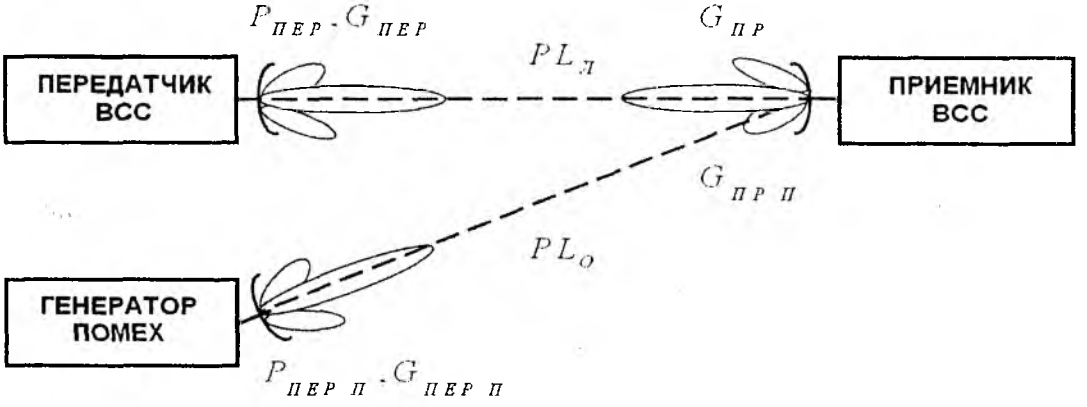

Рис. 4

Если в качестве приемника сложного сигнала ЦСПИ использовать приемник с равномерным усилением в полосе частот F, то помехозащищенность радиоканала будет обеспечена при соблюдении следующего неравенства [12]:

$$\underbrace{\left(P_{ПЕР} G_{ПЕР}\right)}_{1} \cdot \underbrace{\left(\frac{G_{ПР}}{G_{ПР\,О}}\right)}_{2} \cdot \underbrace{\left(\frac{PL_О}{PL_Л}\right)}_{3} \cdot \underbrace{\left(\frac{1}{k_З}\right)}_{4} \cdot \underbrace{\left[\frac{r^2 \cdot B \cdot R}{F} \cdot \frac{E_В}{N_П}\right]^{-1}}_{5} \ge \underbrace{\left[P_{ПЕР\ П} G_{ПЕР\ П}\right]}_{6}, \tag{6}$$

где 1 – характеристики передатчика ЦСПИ: мощность передатчика $P_{ПЕР}$, коэффициент направленного действия антенны передатчика $G_{ПЕР}$; 2 – характеристики приемной антенны ЦСПИ: коэффициент направленного действия антенны приемника $G_{ПР}$ и коэффициент направленного действия антенны приемника по направлению к генератору помех $G_{ПР\,О}$; 3 – потери в линии

связи: для канала нарушителя PL_{Θ} и легитимного канала $PL_{Л}$; 4 – коэффициент запаса по мощности k_3; 5 – критическое отношение помеха/сигнал: $E_в$ – энергия сигнала на бит информации; $N_П$ – спектральная плотность помехи; $F \cdot T = B$ – база сигнала; r^2 – среднее значение коэффициента взаимной корреляции сигнала и помехи; 6 – характеристики передатчика помех: мощность передатчика $P_{ПЕР\ П}$ и коэффициент направленного действия антенны передатчика генератора помех $G_{ПЕР\ П}$.

Из совместного сравнения неравенств (4) и (6) следует, что одновременное повышение скрытности и помехозащищенности ЦСПИ достигается увеличением базы сигнала B, направленности антенн передатчика и приемника, что может быть обеспечено применением *MIMO*-технологий *(Multi-Input Multi-Output)* и эффективным использованием радиоканала, за счет более точной модельной оценки канала распространения на радиотрассе.

С учетом того, что современные ВСС ориентированы на передачу мультимедийной информации, для оценки защищенности канала связи можно также использовать и такой параметр, как секретная производительность c_s [8], который определяется как разность скорости передачи информации по Шеннону в легитимном канале связи C_1 и скорости передачи в отводном канале нарушителя C_2.:

$$C_S = \begin{cases} W \log_2(1+SNR_1) - W \log_2(1+SNR_2), при\ SNR_1 > SNR_2 \\ 0, при\ SNR_1 \le SNR_2 \end{cases}, \quad (7)$$

где SNR_1 и SNR_2 – отношение сигнал/шум в легитимном канале связи и в канале нарушителя соответственно; W – ширина полосы пропускания канала.

Из этого выражения следует, что высокая защищенность канала связи $C_S = \max[C_\cdot]$ может достигаться за счет увеличения скорости передачи информации в легитимном канале связи и повышения SNR_1 за счет знания параметров канала распространения по отношению SNR_2 в канале нарушителя ($SNR_1 >> SNR_2$).

Повышение скорости передачи и защиты информации в легитимном канале связи связано с использованием многоуровневых линейных кодов (*TC-PAM*) и дискретной мультитоновой модуляции (*DMT*) в проводных каналах связи, а также применением многоуровневых видов модуляции (*M-QAM*) и различных технологий расширения спектра *SS* (*Spread Spectrum*) в беспроводных каналах связи.

Наиболее распространенные технологии расширения спектра сигналов:

- прямое расширение спектра (*DSSS*);
- скачкообразная перестройка частоты сигнала (*FHSS*);
- случайное время выхода в эфир (*THSS*); ортогональное частотное мультиплексирование (*OFDM*) [9].

Основной особенностью этих технологий является использование псевдослучайных величин *PN* (*pseudo noise*) для установки уровня и кратности модуляции M, базы сигнала B, числа поднесущих частот f_n, времени T и последовательности выхода в эфир и др. В качестве *PN* последовательностей применяются коды Баркера, *M*-последовательности, коды Уолша, алгебраические коды и другие, обладающие хорошими автокорреляционными свойствами.

Значительное увеличение длины (разрядности) этих последовательностей *PN* (*более* 1000) создает значительный массив вариантности структуры сигнала в канале связи, что также может быть использовано для повышения защищенности канала связи на сигнальном уровне. Это обусловлено тем, что переборный механизм обработки в реальном масштабе времени таких сложных сигналов в канале перехвата будет сопряжен с большими аппаратными затратами и временем обработки.

Для оценки возможностей существующих программно-аппаратных платформ нами был разработан цифровой блок обработки широкополосных сигналов с большой базой с использованием платформы разработчика *DK-DSP-2C70N* (*Altera*).

Как известно, одним из эффективных методов обработки широкополосного сигнала на приеме является согласованная фильтрация, которая максимизирует отношение сигнал/шум в канале связи [13]. Программируемый цифровой согласованный фильтр для свертки сигналов в частотной области является одним из наиболее сложных для реализации элементов помехозащищенной ЦСПИ. Это обусловлено необходимостью очень высокого быстродействия спецпроцессора, которая для сигнала с базой более 1000 становится пробле-матичной даже при использовании самых современных сигнальных процессоров (*DSP*) и программируемых логических матриц (*FPGA*). Общая структурная схема устройства цифровой обработки сложных широкополосных сигналов на основе *FPGA* приведена на рис. 5. Данная схема реализует принцип свертки сложного сигнала в частотной области, обеспечивает режекцию узкополосных помех и формирует квадрат модуля свертки отсчетов принимаемого сигнала и двух опорных последовательностей *PN1* и *PN2*, которые могут оперативно изменяться от одного сеанса связи к другому, дополнительно повышая защищенность канала связи [14].

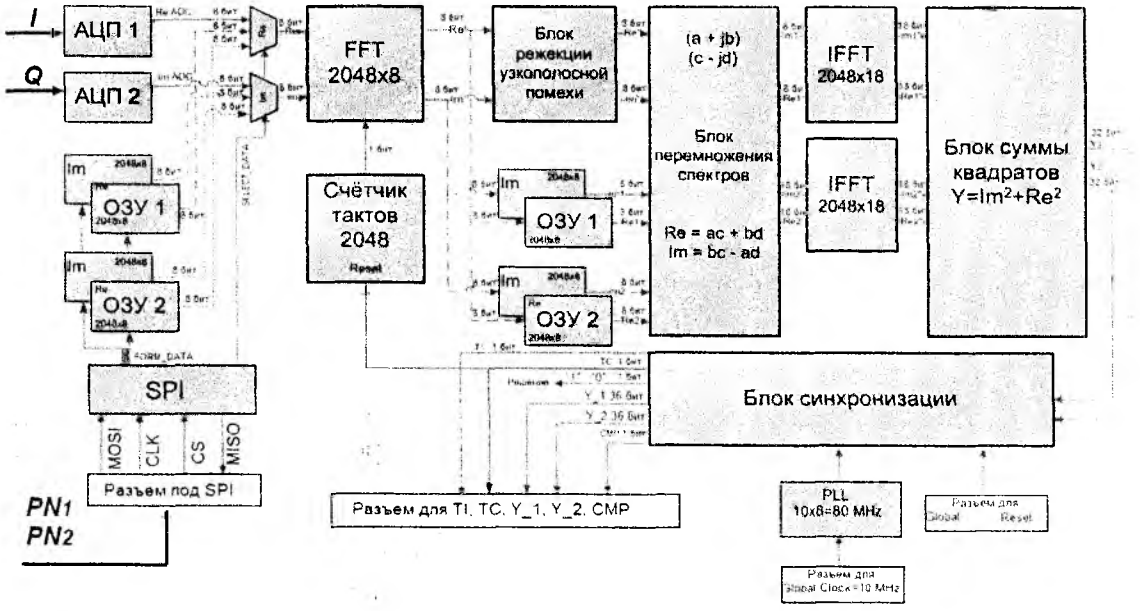

Рис. 5

На осциллограмме (рис. 6) показано положение автокорреляционной функции *АКФ* входного сигнала по отношению к тактовому импульсу *ТИ*, поступающего с выхода блока синхронизации, при отношении сигнал/шум SNR_{INP}= - 6 *дБ* на входе фильтра. Эти данные подтверждают высокую скрытность широкополосного канала связи.

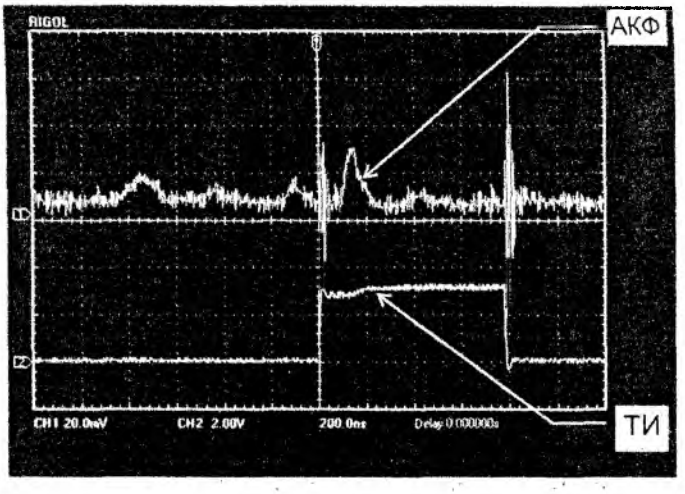

Рис. 6

Еще более существенным источником вариантности сигнальной структуры канала связи является применение *MIMO*-технологий, которые дополнительно вносят пространственную координату, создавая в канале связи многомерное пространство сигналов. Интеграция технологий расширения спектра сигналов и *MIMO*-технологий (*xDSL+MIMO*, *DSSS+MIMO*, *FHSS+MIMO*, *OFDM+MIMO* и т.п.) создает реальную основу построения защищенных ЦСПИ на физическом уровне.

Кроме многоуровневых методов модуляции сигнала и пространственного размещения приемо-передающих антенн важной особенностью современных технологий связи является наличие развитых механизмов адаптации к каналу связи. Эти механизмы дают возможность не только повысить производительность системы, но и улучшить качество передачи информации на канальном уровне (за счет применения различных методов коррекции ошибок). Отсутствие у противника полной информации о параметрах, механизмах адаптации и коррекции ошибок не даст ему возможность получать достоверную информацию на сигнальном уровне, а значит и возможность информационного вскрытия канала связи будут значительно уменьшены.

Для аппаратной реализации защищенных ЦСПИ необходимо использовать концепцию «цифрового радио» *SDR* (*Software Defined Radio*), представляющую собой программно-аппаратную платформу, в которой интегрированы сетевой процессор *NP*, блок потоковой цифровой обработки сигналов на основе программируемой логической матрицы *FPGA*, аналого-цифровые АЦП и цифро-аналоговые преобразователи ЦАП.

На рис. 7 представлена структура *SDR* для обработки многомерных сигналов в *MIMO* канале связи с *N* передатчиками *T* и *N* приемниками *R*.

Учитывая большое различие в принципах работы беспроводных технологий передачи информации, изменение только программного обеспечения (ПО) *SDR* недостаточно для эффективной интеграции, поэтому необходима еще достаточно сложная реконфигурация аппаратных средств, реализующих взаимодействие абонентов сети на канальном уровне.

Для повышения энергетического потенциала легитимного канала связи важно также знать параметры затухания РРВ в канале связи при различном пространственном расположении абонентов в зоне доступа. Эффективная работа адаптационного алгоритма настройки ЦСПИ напрямую зависит от оценки параметров канала связи в реальном масштабе времени, что требует разработки упрощенных моделей для реализации их на программно-аппаратной платформе *SDR*.

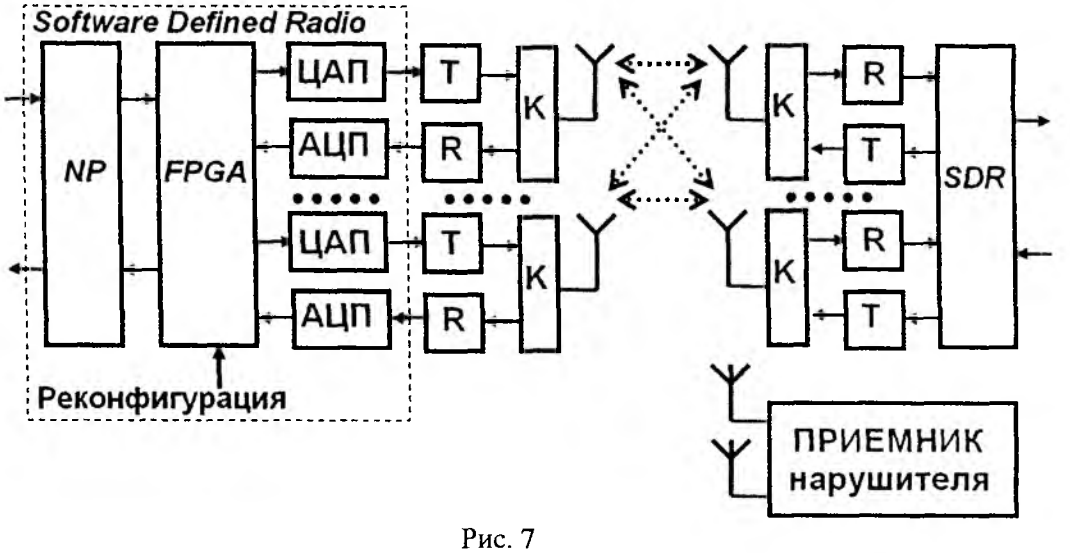

Рис. 7

В ХНУРЭ разработано целый ряд программ моделирования беспроводных каналов связи уровня *LAN* и *MAN* [15,16]. Они основаны на отражательной трактовке и использовании

метода микроволновых волновых каналов, что дает возможность с достаточно высокой точностью прогнозировать параметры производительности и защищенности канала связи в зоне развертывания системы радиодоступа.

Заключение

1) Из изложенного следует, что характерной особенностью современного этапа научно-технического прогресса в области развития ЦСПИ для ВСС является интеграция технологий, которая должна захватить и сферу защиты информации, и эта тенденция в дальнейшей перспективе будет сохраняться и углубляться.

2) Анализ различных критериев оценки защищенности каналов связи (скрытности и помехозащищенности) показывает, что физический уровень современных цифровых технологий передачи информации несет большой потенциал, который может быть использован для повышения безопасности в ведомственных сетях доступа.

3) Основными направлениями повышения энергетической защищенности каналов связи ЦСПИ являются: использование широкополосных сигналов с большой базой, *MIMO*-технологии, многомерного пространства сигналов и разработка моделей прогнозирования затухания сигналов в зоне развертывания системы радиодоступа.

4) Развитие теории отводного канала позволяет определить новые возможности повышения защищенности каналов связи на физическом уровне и найти механизмы их интеграции с информационными методами защиты информации.

Список литературы: 1. *Коновалов Г.В.* Многомерные сети – будущее инфокоммуникационных сетей // Электросвязь. М, 2008. №4. С.28-32. 2. *Мао В.* Современная криптография. Теория и практика. М.: Вильямс, 2005. 768 с. 3. *Сердюков П.Н., Бельчиков А.В., Дронов А.Е.* и др. Защищенные радиосистемы цифровой передачи информации. М.: АСТ, 2006. 403 с. 4. *Шокало В.М., Цопа А.И.* Концепция создания отечественных специальных цифровых систем передачи информации // Захист інформації. Київ: ДУІКТ, 2006. Вип. № 3. С. 51 - 57. 5. *Коваль Ю.А. Бавыкина В.В.* Развитие теории и совершенствование метеорных систем связи и синхронизации. Харьков: Коллегиум, 2006. 308 с. 6. *Shannon K.* Communication theory of secrecy systems // Bell Systems Tech Journal, 1949. Vol. 28, №4. P. 656-715. 7. *Котельников В.А.* Теория потенциальной помехоустойчивости. М.: ГЭИ, 1956. 151 с. 8. *Wyner A.D.* The wire-tap channel // Bell System Technical Journal. 1975. Vol. 54, № 8. P. 1355 -1387. 9. *Зюко А.Г.* Помехоустойчивость и эффективность систем связи. М.: Связь, 1972. 358 с. 10. *Урядников Ю.А., Аджемов С.С.* Сверхширокополосная связь. Теория и применение. М.: Солон-Пресс, 2005. 368 с. 11. *Куприянов А.И., Сахаров А.В.* Теоретические основы радиоэлектронной борьбы. М.: Вузовская книга, 2007. 356 с. 12. *Тузов Г.И. и др.* Помехозащищенность радиосистем со сложными сигналами / Г.И. Тузов, В.А. Сивов, В.И. Прытков, Ю.Ф. Урядников, Ю.А. Дергачев, А.А. Сулиманов. М.: Радио и связь, 1985. 264 с. 13. *Варакин Л.Е.* Системы связи с шумоподобными сигналами. М.: Радио и связь, 1985. 384 с. 14. *Tsopa O.I.* Signal Processing Verification System Programmable Digital Matched Filter / *H.V. Kharchenko, S.O. Makovetskiy, I.O. Tkalich, O.I. Tsopa, Y.I. Vdovychenko* // Proc. 6th IEEE East-West Design & Test Symposium /*EWDTS-2008*/. Lviv: Ukraine, 2008. P. 243-250. 15. *Цопа А.И.* Вариант модели затухания широкополосного сигнала в радиолинии при расчете защищенности локальной сети связи / А.А. Стрельницкий, А.Е. Стрельницкий, А.И. Цопа, В.М. Шокало// Захист інформації. Киев: ГУИКТ, 2008. №3(39). С. 38-43. 16. *Tsopa O.I.* Approximate Model for Estimation of Efficiency and Noise Immunity of Branched Street and Corridor *Wi-Fi* and *WiMAX* Communication Channels / A.A. Strelnitskiy, O.I. Tsopa, V.M. Shokalo // International journal «Telecommunication and Radio Engineering». Begell House, 2009. Vol. 68(17). P. 1511-1528.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 05.02.2010