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

Дудка А. А., Стрельницкий А. А., Стрельницкий А. Е., Цопа А. И., Шокало В. М.
Харьковский национальный университет радиоэлектроники
Кафедра основ радиотехники
пр. Ленина, 14, г. Харьков, 61166, Украина
тел.: +8 057 702-14-79, e-mail: knure-res@kharkov.ukrtel.net

Аннотация — В докладе рассматриваются основные направления повышения защищенности каналов связи цифровых систем передачи информации для ведомственных сетей связи на физическом уровне.

I. Введение

Технологический прорыв в области микро- и наноэлектроники привел к появлению новой производительной элементной базы, позволяющей реализовывать цифровые системы передачи информации (ЦСПИ) в физически малых объемах, а также к глобальной интеграции различных технологий, как по назначению, так и по принципу действия.

Основными требованиями, предъявляемыми к ведомственным системам связи (ВСС) являются: высокая производительность и защищенность 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.

При этом также надо учитывать, что в связи с массовым внедрением 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 уровне, а также интеграции различных методов защиты информации.

В докладе основное внимание уделено определению круга нерешенных задач по защите информации на физическом (энергетическом) уровне.

II, III. 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), предложенный авторами, приведен на рис. 1 [1].

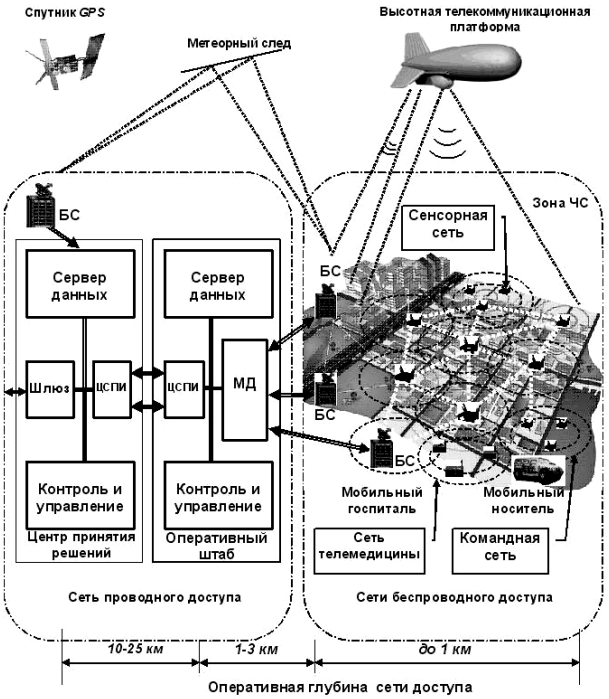

Рис. 1. Структурная схема интегрированной сети доступа, разворачиваемой в зоне ЧС.

Fig. 1. The block diagram of an integrated access network

Интегрированная сеть доступа включает в себя нескольких подсистем и сетей: сеть проводного доступа (СПД), сеть абонентского радиодоступа (САРД), сеть телемедицины, сенсорную распределенную 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 расширяя оперативную глубину зоны радиодоступа.

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.

2010 20th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2010). 13-17 September, Sevastopol, Crimea, Ukraine
 ISBN: 978-966-335-329-6. IEEE Catalog Number: CFP10788

Обеспечение защищенности ЦСПИ, входящих в эту разветвленную ведомственную сеть связи (ВСС), является одной из основных задач, которые необходимо решать при разработке, как отдельных элементов системы доступа, так и системы в целом. При этом под защищенностью системы связи мы понимаем ее помехозащищенность и скрытность.

Основоположником информационного подхода при создании безопасных систем связи является Шеннон К., положивший начало не только науки криптографии, но и науки кодирования канала связи [2]. Другой подход решения задачи повышения защищенности канала связи базируется на теории потенциальной помехоустойчивости Котельникова В.А. [3]. Дальнейшим развитием теории построения защищенных систем связи является концепция модели отводного канала связи, предложенная Вайнером А.. Развитие этой концепции дает возможность достичь высокой защищенности канала на физическом уровне модели *OSI*, без применения криптографических методов защиты информации [4].

На рис. 2 показана разработанная авторами усовершенствованная структурная схема модели ЦСПИ с отводным каналом (каналом утечки).

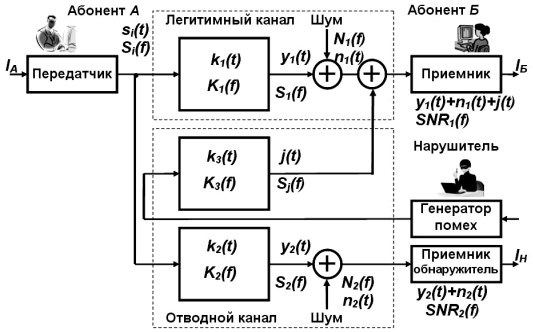

Рис. 2. Схема модели ЦСПИ с отводным каналом.

Fig. 2. The diagram of DTIS model with a wiretap channel

Для оценки защищенности такого канала связи можно применить ряд известных критериев. Один из них - помехозащищенность канала связи, который характеризует способность системы связи обеспечивать передачу информации с заданными показателями качества в условиях воздействия помех как естественного, так искусственного происхождения.

Критерием оценки помехозащищенности канала связи является допустимый уровень помех на входе легитимного приемника при обеспечении заданного уровня *BER* и *PER* при передаче информации разного вида. Учитывая случайный характер параметров сигнала и помех, критерием помехозащищенности может также служить вероятность подавления канала связи, которая зависит от уровня помех в зоне работы системы, от условий распространения радиосигнала и пространственного размещения приемо-передатчиков.

Скрытность канала связи, которая определяет способность системы сохранять в тайне факт работы системы, характеризуется формой и радиусом зоны обнаружения сигнала, вероятностью обнаружения сигнала, вероятностью вскрытия структуры сигнала и вероятностью смыслового раскрытия передаваемой информации [5]. Эти характеристики зависят от предельного отношения сигнал/шум на входе приемника обнаружителя, базы сигнала, потерь при распространении радиоволн в легитимном канале связи и канале нарушителя.

Можно также использовать информационный критерий защищенности канала связи на основе параметра секретной производительности C_S, который определяется как разность скорости передачи информации по Шеннону в легитимном канале связи C_1 и скорости передачи в отводном канале нарушителя C_2

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

Из этого выражения следует, что высокая защищенность канала связи $C_S = \max\left[C_S\right]$ 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 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 распространенными технологиями расширения спектра сигналов являются: прямое расширение спектра (*DSSS*); скачкообразная перестройка частоты сигнала (*FHSS*); случайное время выхода в эфир (*THSS*); ортогональное частотное мультиплексирование (*OFDM*).

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 (базы сигнала) 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.

Еще более существенным источником вариантности сигнальной структуры канала связи является применение *MIMO*-технологий *(Multi-Input Multi-Output)*, 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 приемопередающих 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 возможности 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. 3 представлена структура *SDR* для обработки многомерных сигналов в *MIMO* канале связи с *N* передатчиками *T* и *N* приемниками *R*.

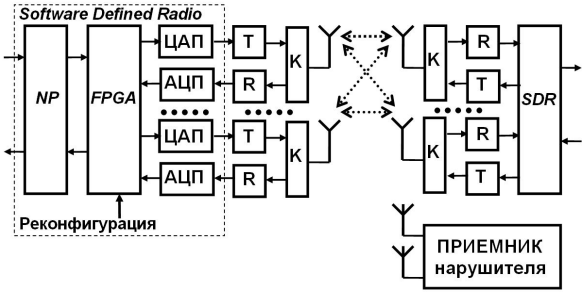

Рис. 3. Структурная схема программно-аппаратной платформы SDR.

Fig. 3. The block diagram of SDR software and hardware platform

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 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. 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 проблематичной даже при использовании самых современных сигнальных процессоров и *FPGA*.

Общая структурная схема устройства цифровой обработки сложных широкополосных сигналов на основе *FPGA* приведена на рис. 4. Данная схема реализует принцип свертки сложного сигнала в частотной области, включая 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 [5], дополнительно повышая защищенность канала связи.

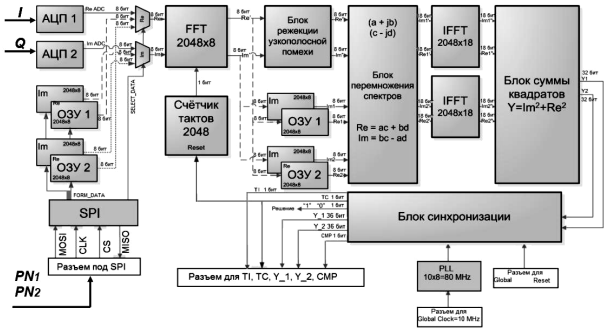

Рис. 4. Обобщенная структурная схема блока цифровой обработки широкополосных сигналов.

Fig. 4. The generalized block diagram of a broadband signal digital processing unit

Для прогнозирования 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*.

В ХНУРЭ разработано целый ряд программ моделирования беспроводных каналов связи уровня *LAN* и *MAN*. Они основаны на отражательной трактовке и использовании метода микроволновых волновых каналов, что дает возможность с достаточно высокой точностью прогнозировать параметры и производительность канала связи в зоне развертывания системы радиодоступа [6]. В докладе рассматривается пример модели отводного канала для беспроводных *Wi-Fi* и *WiMAX* систем, анализируются результаты расчета и эксперимента.

Рассмотрена также модель отводного канала для проводных ЦСПИ. Обсуждаются результаты исследования защищенности современных *VDSL* каналов связи [7].

В докладе показан пример создания отечественного защищенного центра обслуживания вызовов (ЦОВ) службы «102» ГУМВД г. Харькова (рис. 5). Структура ЦОВ включает в себя нескольких подсистем и сетей: станционное оборудование (ЦАТС) службы «102», центральный информационный сервер (ЦИС) службы «102», рабочие места оператора (РМО) службы «102», сеть проводного доступа (СПД) для связи станционного оборудования службы «102» с районными отделениями ГУМВД на основе ЦСПИ и с узлом экстренных и информационно-справочных служб Харьковского филиала ОАО «Укртелеком», рабочие места дежурных (РМД) районных отделений ГУМВД.

2010 20th Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2010). 13-17 September, Sevastopol, Crimea, Ukraine
 ISBN: 978-966-335-329-6. IEEE Catalog Number: CFP10788

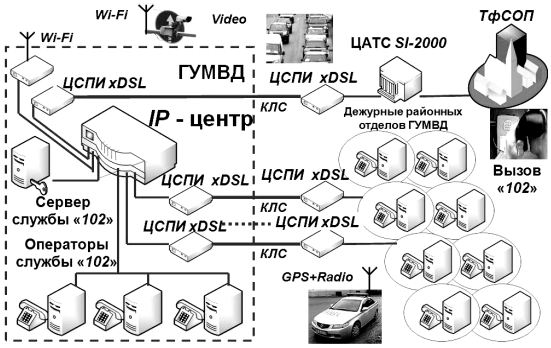

Рис. 5. Обобщенная структурная схема ЦОВ службы «102» ГУМВД г. Харькова.

Fig. 5. The structural diagram of «102» service call center

Основной отличительной особенностью разработанной ВСС является использование разработанных в ХНУРЭ новых защищенных многоканальных ЦСПИ *«Quadro»* на основе симметричных *SHDSL* технологий, в которых реализована интеграция процессов кодирования, модуляции, шифрования, преобразования и обработки сигналов в одном едином цифровом процессе обработки.

Оперативность принятия вызовов, своевременное информирование о происшествиях дежурных в районных отделениях ГУМВД дало возможность более эффективно и качественно реагировать и раскрывать преступления по «горячим» следам.

IV. Заключение

1. Характерной особенностью современного этапа 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. Развитие концепции отводного канала, которая базируется на физическом уровне модели *OSI* для широкополосных технологий, несет большой потенциал, который может быть использован для повышения безопасности в ВСС.

3. Перспективным направлением повышения энергетической защищенности каналов связи ЦСПИ является использование *MIMO*-технологий и многомерного пространства сигналов.

V. Список литературы

[1] *Шокало В. М., Цопа А. И.* Концепция создания отечественных специальных цифровых систем передачи информации // Науково-технічний журнал «Захист інформації». – Київ: ДУІКТ, 2006. – Вип. № 3. – С. 51-57.

[2] *Shannon K.* Communication theory of secrecy systems // Bell Systems Tech Journal, 1949. – Vol. 28, №4. – pp. 656-715.

[3] *Котельников В. А.* Теория потенциальной помехоустойчивости. – М.: ГЭИ, 1956. – С. 151.

[4] *Wyner A. D.* The wire-tap channel // Bell System Technical Journal. – 1975. – Vol. 54, № 8. – pp. 1355 -1387.

[5] Урядников Ю.Ф., Аджемов С.С. Сверхширокополосная связь. – М.: Солон Пресс, 2005. – С. 366.

[6] *Strelnitskiy A. A.* 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.

[7] *Dudka O. O.* Cable communication system as antenna. Radiation and reception regimes / O. O. Dudka, O. I. Tsopa, V. M. Shokalo // «Telecommunication and Radio Engineering».–Begell House, 2009–Vol. 68(10).– P.865-874.

WAYS TO IMPROVE THE SECURITY OF COMMUNICATION CHANNELS OF INFORMATION TRANSMISSION DIGITAL SYSTEMS AT THE PHYSICAL LEVEL

Dudka O. O., Strelnytskyi A. A., Strelnytskyi A. E., Tsopa O. I., Shokalo V. M.
Kharkiv National University of Radioelectronics
14, Lenin Ave., Kharkiv, 61166, Ukraine
Ph.: 8057-7021479,
e-mail: knure-res@kharkov.ukrtel.net

Abstract — The report concerns the main ways of increasing security of communication channels of digital communication systems for departmental communication networks at the physical level.

I. Introduction

The main requirements for departmental communications system (*DCS*) are high performance and secure communication. The effectiveness of the protocols of information security at the upper levels of the seven-level model of open systems interconnection (*OSI*), is significantly reduced during *DCS* multimedia information transmission. The report focuses on identifying the range of unsolved problems of information security at the physical level.

II, III. Main Part

One of the main development directions of digital transmission information systems (*DTIS)* for *DCS* is the integration of wired and wireless transmission of information. Wired segment of the *DCS* is dominated by various broadband *xDSL* technologies for high speed data transmission. Segment of wireless access technologies is dominated by *Wi-Fi* and *WiMAX* technologies.

The report shows one of the options for the integration of different technologies and *DSIT* when deploying network access in the area of emergency. *DTIS* ensuring security included in this extensive network of departmental communication is one of the main tasks that must be solved. At the same time, under secure communications, we understand its noise protectability and secrecy.

The report develops the concept of wiretap channel, which allows achieving a high security channel at the physical layer of *OSI* model, without using cryptographic techniques for information protection. We present a model wiretap channels for wired and wireless *DTIS*.

IV. Conclusion

1. A special feature of modern *DTIS* development for *DSC* is the integration of technologies, which should include scope of information security, this trend will continue and deepen with time.

2. The concept of wiretap channel based on the physical layer of the *OSI* model for broadband transmission of information has great potential, it can be used to enhance security in corporate networks access.

3. The promising direction to improve energy security of *DTIS* communication channels is the use of *MIMO*-technology and multi-dimensional signal space.