ИНФОРМАЦИОННЫЙ ИНТЕРФЕЙС В СИСТЕМЕ ОХРАНЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Зори А.А., Кувшинов Г. И.
Донецкий национальный технический университет,
кафедра электронной техники
E-mail: neutrino@rambler.ru

Abstract. ***Zori A A., Kuvshinov G.I. Information interface in the security system.*** *In this construction flexible in sense of a configuration of security or other information system, where it is necessary to connect gauges with the managing and analyzing centre, by best for today by the decision would be to use the uniform information-telemetering interface on the radiochannel .*

Постановка проблемы, анализ разработок. В банковской сфере отсутствуют надежные информационно-контролирующие системы охраны зданий от несанкционированного доступа. В экономически развитых странах законодательно запрещен экспорт новейших разработок. Приобретаемые зарубежные системы не имеют полной технической документации (“черный ящик”). Это делает невозможным их установку, эксплуатацию и усовершенствование отечественными специалистами, что экономически нецелесообразно.

Анализ последних достижений показывает, что в настоящее время стали доступными микроконтроллеры, позволяющие создавать интеллектуальные средства контроля. Это позволило создавать разнообразные локальные вычислительные устройства, привлекая разработчиков выгодным соотношением цена/быстродействие(мощность)/энергопотребление, удобными режимами программирования, доступностью аппаратно-программных средств поддержки и широкой номенклатурой контроллеров.

Задачи разработки. Используемые в настоящее время в банковской сфере информационно-контролирующие системы защиты от несанкционированного доступа отечественного и зарубежного производства основаны в основном на проводном принципе обмена данными между средствами контроля и системой обработки информации. Одним из недостатков является негибкость процесса установки таких систем и приспособления их к изменившимся условиям

применения. Они уязвимы, так как не имеют средств самотестирования, не имеют автоматизированного процесса контроля, а только отображают ситуацию на пульте оператора охраны.

Целью данной работы является повышение устойчивости системы к взлому путем разработки помехозащищенного алгоритма кодирования.

Основные результаты. Для построения гибкой в смысле конфигурации охранной информационной системы, где необходим обмен данными между датчиками и анализирующим центром, лучшим на сегодняшний день решением является использование единого информационно-телеметрического интерфейса (ИТИ) по радиоканалу [1]. При этом он должен удовлетворять следующим условиям:

– высокой помехоустойчивости и помехозащищенности;

– соответствию спектра сигнала в радиоканалах связи требованиям государственной инспекции электросвязи.

Рассмотрим ИТИ, применимые к системе защиты зданий от несанкционированного доступа. Структура передаваемой информации определяется выполняемыми функциями внешних устройств системы (ВУ) и их количеством. В [1] показано, что в зависимости от структуры здания и уровня защиты рекомендуется использовать от 40 до 100 ВУ.

Известные системы используют разнообразные не унифицированные протоколы передачи данных в пределах одной системы, что значительно усложняет аппаратно-программные средства, снижает их надежность, повышает себестоимость и усложняет автоматическое тестирование устройств.

Для информационно-контролирующей системы охраны здания банка от несанкционированного доступа (ИКСНД) средой передачи информации является радиоэфир, характеризующийся наличием импульсных и сосредоточенных по спектру частот помех. Для такого канала можно применить однонаправленную систему передачи информации, однако ввиду предъявляемых требований по высокой помехоустойчивости применим систему с решающей обратной связью. В помехоустойчивом алгоритме применен метод декомпозиции для декодирования m-уровневых итеративных кодов, обеспечивающий линейную зависимость сложности реализации оптимальных декодеров от длины кода, где он работает в режиме обнаружения либо исправления ошибок малой и большой кратности [2]. В системе совместно с помехоустойчивым применен помехоза-

щищенный алгоритм кодирования, устраняющий возможность доступа извне в информационно-контролирующую систему охраны здания банка от несанкционированного доступа.

Представим структурную схему информационного интерфейса (рис. 1).

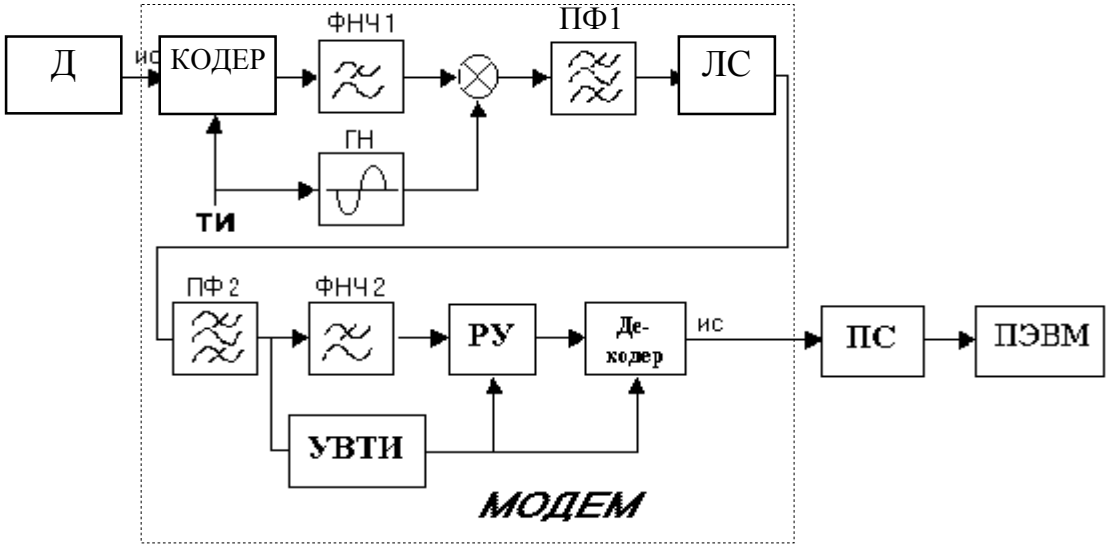

Рисунок 1 — Структурная схема информационно-телеметрического интерфейса системы

Для наглядности информационный интерфейс подключен к плате согласования с ПЭВМ и одному из ВУ - датчиков. Каждое ВУ имеет интеллектуальную часть — микроконтроллер и специальное программное обеспечение. От датчика Д на вход кодера поступает последовательность информационных символов ИС. Кодер вырабатывает последовательность модулирующих символов, обеспечивающих формирование информационной составляющей сигнала. В кодер поступает также колебание тактовой частоты. Фильтрация с целью обеспечения спектра сигнала производится как по низкой (ФНЧ1), так и по радиочастоте (ПФ1). Посредством линии связи сигнал поступает на полосовой фильтр ПФ2, где ослабляется действие флуктуационных помех и помех от соседних по частоте каналов; фильтром ФНЧ2 производится дополнительная фильтрация по низкой частоте. При поэлементном приеме в схеме решающего устройства (РУ) производится анализ сигнала и выносится решение о передаче символа. Устройство выделения тактовых импульсов (УВТИ) определяет момент вынесения решения. На основе решений декодер вырабатывает последо-

вательность информационных символов, которые через плату сопряжения ПС поступает в ПЭВМ, где происходит их обработка.

Для передачи сигнала по радиоканалу необходимо модулировать несущий сигнал информационным. На практике в подобных информационно-измерительных системах применяют амплитудную, частотную и фазовую модуляции [1]. Однако амплитудная модуляция не обеспечивает требуемых помехоустойчивости и помехозащищенности, частотная — имеет широкий спектр сигнала, что не соответствует требованиям государственной инспекции электросвязи, фазовая — усложняет приемо-передающий тракт, поскольку нужно дополнительное устройство измерения абсолютного значения начальной фазы.

Применив фазовую манипуляцию при небольшом числе возможных значений начальной фазы, как правило, 2, 4 или 8, стало возможно обеспечить высокую помехоустойчивость ($d_{min}/\sigma \cong 0.39$) при достаточно простой аппаратно-программной реализации, доступной для уровня контроллеров, с помощью которой относительно просто определить фазовый сдвиг между двумя соседними символами. Предложено использовать фазоразностную манипуляцию (синонимы — дифференциальная фазовая манипуляция, относительная фазовая манипуляция). График сигнала с 4-позиционной фазовой манипуляцией приведен на рис. 2.

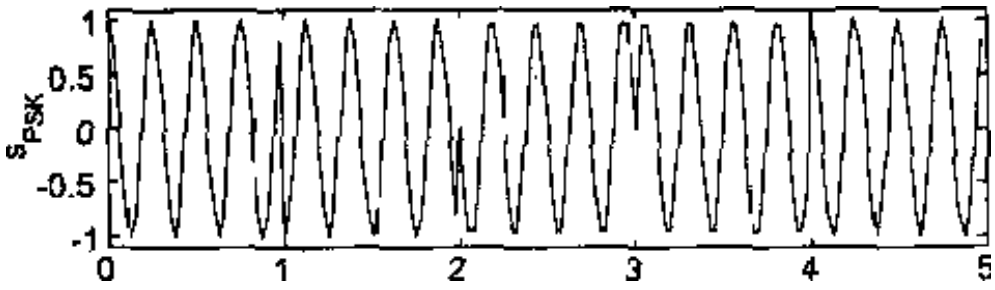

Рисунок 2 — Сигнал с 4-позиционной фазовой манипуляцией

Для защиты передаваемой в системе информации применяем помехозащищенное кодирование. Для выбора класса криптографирования необходимо проанализировать гипотетические возможности злоумышленника. Например, для злоумышленника, вооруженного вычислительной техникой, приемопередатчиком, работающем в том же диапазоне, что и ИТИ, устройством демодуляции и ввода информационного сигнала в компьютер, при использовании в системе симметричного криптографирования, стойким окажется лишь шифр с одноразовым ключом, что невыполнимо с технологической стороны. Использова-

ние многоразового (то есть "зашитого" в системе) ключа приведет к тому, что злоумышленник может попытаться восстановить ключ, используя знания о перехваченных сообщениях и детерминированные алгоритмы вычисления.

Для исключения возможности взлома системы необходимо использовать асимметричное криптографирование, характеризующееся тем, что для шифрования и расшифрования используются разные ключи, связанные между собой некоторой зависимостью. При этом данная зависимость такова, что установить один ключ, зная другой, с вычислительной точки зрения очень трудно. Один из ключей (например, ключ шифрования) может быть сделан общедоступным, и в этом случае проблема получения общего секретного ключа для связи отпадает. Если сделать общедоступным ключ расшифрования, то на базе полученной системы можно построить систему аутентификации передаваемых сообщений.

Алгоритм генерации ключей открыт, необходимо подать ему на вход случайную строку r надлежащей длины и получить пару ключей (k_1,k_2). Один из ключей (например, k_1) передается вместе с сообщением, он называется открытым, а второй, называемый секретным, встроен в алгоритм шифрования-дешифрования. Алгоритмы шифрования E_{k1} и дешифрования D_{k2} таковы, что для любого сообщения m $D_{k2}(E_{k1}(m))=m$.

Рассмотрим теперь гипотетическую атаку злоумышленника на эту систему. Противнику известен открытый ключ k_1, но неизвестен соответствующий секретный ключ k_2. Противник перехватил криптограмму d и пытается найти сообщение m, где $d=E_{k1}(m)$. Поскольку алгоритм шифрования открыт, противник может просто последовательно перебрать все возможные сообщения длины n, вычислить для каждого такого сообщения m_i криптограмму $d_1= E_{k1}(m_1)$ и сравнить d_1 с d. То сообщение, для которого $d_1=d$ и будет искомым открытым текстом. В худшем случае перебор будет выполнен за время порядка $2^nT(n)$, где $T(n)$ — время, требуемое для шифрования сообщения длины n. Если сообщения имеют длину порядка 1000 битов, то такой перебор неосуществим на практике ни на каких самых мощных компьютерах.

В помехоустойчивом алгоритме кодирования предложена криптосистема Ривеста-Шамира-Эйделмана (RSA). RSA представляет собой криптосистему, стойкость которой основана на сложности решения задачи разложения числа на простые сомножители. Кратко алгоритм можно описать следующим образом: пользователь А выбирает пару различных простых чисел p_a и q_a, вычисляет

$n_a=p_aq_a$ и выбирает число d_a, такое что НОД(d_a, $\varphi(n_a)$)=1, где $\varphi(n)$ — функция Эйлера (количество чисел, меньших n и взаимно простых с n. Если $n= pq$, где p и q — простые числа, то $\varphi(n)=(p-1)\cdot(q-1)$. Затем он вычисляет величину e_a, такую, что $d_ae_a=1$ (mod ($\varphi(n_A)$), и размещает в общедоступной справочной таблице пару (e_A, n_A), являющуюся открытым ключом пользователя А.

Время выполнения наилучших из известных алгоритмов разложения при $n>10^{145}$ на сегодняшний день выходит за пределы современных технологических возможностей [5].

Выводы.

1. Предложен новый информационно-телеметрический интерфейс системы охраны здания банка от несанкционированного доступа.

2. Проанализирован и предложен помехоустойчивый алгоритм передачи данных.

Литература

1. Харотишвили Н. Г. Дифференциальная импульсно-кодовая модуляция в системах связи. — М.: Радио и связь, 1982. — 133 с.
2. Бронников В. Н., Зори А. А., Кувшинов Г. И. Научные труды. Оптимальный метод получения мягких решений относительно символов кодов с помощью декомпозиции информации в проверочных соотношениях. — ДонДТУ, вип. 20, 2000. — 231 с.
3. Кларк Дж., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи. — М.: Радио и связь, 1987. — 390 с.
4. Баричев С. Г., Гончаров В.В., Серов Р. Е.. Основы современной криптографии. — М.: Горячая линия - телеком, 2001. — 120 с.
5. Щербаков А. Ю. Компъютерная безопасность. Теория и практика. — М.: Молчагаева, 2001. — 351 с.

Сдано в редакцию: 11.03.2003г.

Рекомендовано к печати: д.т.н., проф. Зори А.А.