УДК 004.056.55
DOI: 10.30987/article_5c12914778c424.41687441

Н.В. Суханова, к.т.н.
(*Институт конструкторско-технологической информатики РАН, 127055, г. Москва, Вадковский пер. 18, стр. 1а*)
E-mail: n_v_sukhanova@mail.ru

Криптографическая защита информации в распределенных системах управления

Рассмотрена структура распределенной системы управления (РСУ). Поставлена задача защиты информации, которая передается между узлами сети РСУ. Для передачи информации использованы открытые каналы связи. Предложен новый способ криптографической защиты информации методом блочной шифрации с закрытым ключом.

Ключевые слова: криптография; защита информации; закрытый ключ; открытый канал связи; распределенная система управления.

N.V. Sukhanova, Can. Sc. Tech.
(*Institute of Design Technological Informatics of RAS, Building 1a, 18. Vadkovsky Alleyway, Moscow 127055*)

Cryptographic information protection in distributed control systems

The structure of the distributed control system (DCS) is considered. A problem for information protection which is transferred between the units of the DCS is specified. For information transfer there are used open communication channels. A new method for a cryptographic protection of information with the aid of the method of block encoding with a private key is offered.

Keywords: cryptography; information protection; private key; open communication channel; distributed control system.

Введение

В настоящее время создают и внедряют распределенные системы управления. В состав распределенной системы управления (РСУ) входят глобальные и локальные сети, в том числе компьютерные и промышленные сети с разными протоколами передачи данных. Рассмотрен РСУ, где для передачи данных между узлами распределенной сети используются открытые каналы передачи информации – кабельные линии и радиоканалы. Таким образом, возникает задача защиты информации в таких системах. Защита должна быть как от внешних «третьих» лиц, так и внутри системы.

Анализ структуры ИАСУ и определение каналов для защиты информации

РСУ имеет сложную многоуровневую структуру (рис. 1). Рассмотрим типовую структуру РСУ, где имеются несколько уровней:

1. Верхний уровень (персональные компьютеры, серверы, базы данных, компьютерные сети).
2. Один или несколько промежуточных уровней (компьютерные и промышленные сети, шлюзы, Интернет).
3. Нижний уровень (управляющие вычислительные системы (УВС), датчики, исполнительные механизмы).

РСУ можно рассматривать как совокупность узлов, которые соединены между собой с помощью локальных подсетей и глобальной компьютерной сети (Интернет). В свою очередь, каждый узел может представлять собой часть общей системы и иметь структуру, подобную РСУ.

На нижнем уровне регулирования имеются управляющие вычислительные системы, которые соединены с исполнительными устройствами и датчиками. Для соединения УВС с исполнительными устройствами и датчиками используется витая пара проводов. Информация на нижнем уровне передается в форме аналоговых и цифровых физических сигналов и не требует дополнительной криптографической защиты. Датчики измеряют параметры физических процессов, которые характеризуют состояние объекта управления. Объектами управления РСУ в машиностроении являются: технологическое оборудование, технологические процессы, технологические линии.

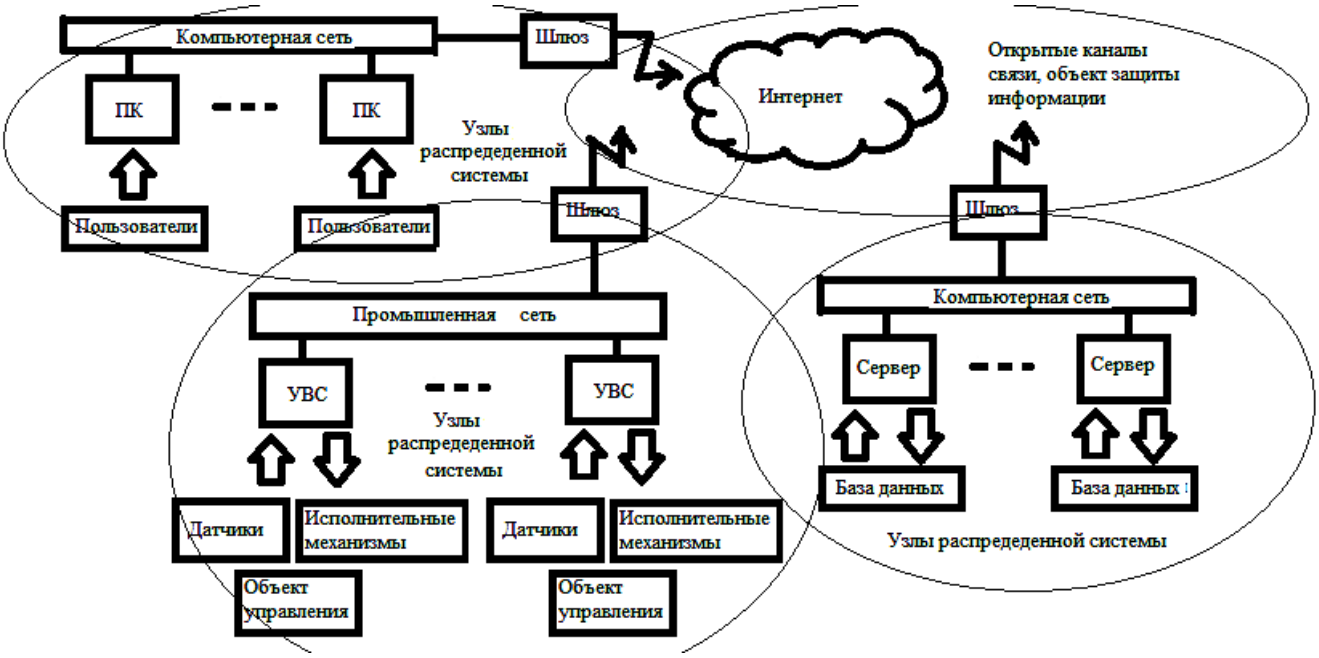

Рис. 1. Структура распределенной системы управления

В структуре РСУ на верхнем и промежуточных уровнях можно выделить глобальные и локальные компьютерные и промышленные сети, которые предназначены для приема и передачи данных между узлами. Соответственно, на верхнем и промежуточном уровнях используется различное сетевое оборудование и разные протоколы передачи данных. Серверы с базами данных, ПК и УВС являются узлами распределенной сети. Информация между серверами ПК и УВС передается в форме пакетов данных. В формате пакетов имеются сетевые адреса устройства-отправителя, устройства-получателя и поле данных. Распределенная сеть включает узлы и открытые каналы передачи данных, которые являются объектами для защиты информации.

Анализ структуры РСУ показал, что в ее состав входит распределенная сеть со сложной структурой, где информация может передаваться между разными устройствами на значительные расстояния по открытым каналам связи. Для передачи информации использованы открытые каналы связи – радиоканал, кабельная линия, сеть Интернет.

При использовании распределенных систем управления возникает задача защиты информации, которая передается между узлами РСУ.

Способы защиты информации в компьютерных и промышленных сетях

Известны разные способы защиты информации в компьютерных и промышленных сетях. К таким способам защиты относятся, прежде всего, способы криптографической защиты информации, в том числе способы блочной шифрации. В криптографии используется термин «ключ», которым обозначают информацию, которая используется при шифрации и дешифрации сообщений. Ключи разделяют на открытые общедоступные и закрытые секретные (рис. 2).

Способы шифрации разделяют на симметричные и асимметричные. При асимметричном способе используются два ключа: открытый общедоступный ключ для шифрации и закрытый секретный ключ для дешифрации сообщений. Раскрыть зашифрованное сообщение можно только с использованием закрытого секретного ключа.

При симметричном способе используется один закрытый секретный ключ для шифра
ции и дешифрации сообщений.

Криптостойкость – это способность противостоять взлому зашифрованного сообщения «третьими» лицами. Традиционный способ взлома зашифрованного сообщения состоит в подборе секретного ключа. Подобрать секретный ключ можно, например, перебором всех возможных комбинаций или используя известное приветствие, заголовок в начале и подпись в конце сообщения.

Криптостойкость измеряется количеством элементарных операций, которые необходимо выполнить для восстановления исходного информационного сообщения при знании способа преобразования, но без знания ключа. Спо-

соб преобразования при шифрации, как правило, известен. Ключ вычисляют методом перебора, с применением аппаратных и программных средств. Подбор ключа называется взломом ключа. Криптостойкость зависит от способа шифрования и длины используемого ключа. Чем длиннее ключ, тем выше криптостойкость шифрации. Для повышения криптостойкости увеличивают размер секретного ключа.

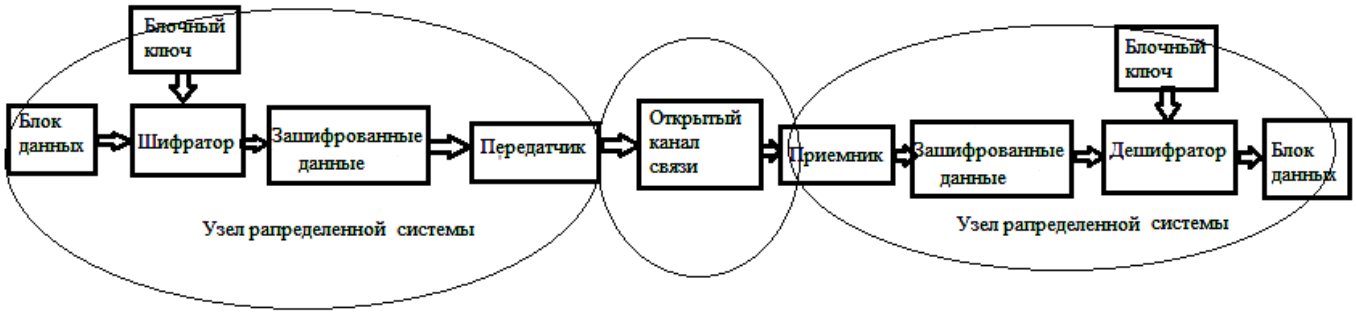

Рис. 2. Блочная шифрация с закрытым ключом

Для повышения криптостойкости используют блочное шифрование данных, когда выполняют разбиение информации на отдельные блоки фиксированного размера. Секретный ключ разбивают на подключи. Затем эти блоки шифруют, причем для шифрования каждого блока используют свой подключ, который называю блочным ключом.

К способам блочного шифрования с закрытым ключом относятся стандарты ГОСТ 28147-89 (Россия) [1], Data Encryption Standard DES (США) [2], способы блочного шифрования Молдовяна [3 – 5], способы, разработанные автором статьи [6 – 8] и др.

Недостатки способов блочной шифрации с закрытым ключом

Проведен анализ известных способов блочной шифрации с закрытым ключом [1 – 5].

Алгоритм криптографического преобразования ГОСТ 28147-89 использует блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками[1]. В ГОСТ-28147-89 не описан процесс генерации ключей и таблиц замен. Существуют «слабые» и «сильные» ключи и таблицы замен, но в стандарте не описываются критерии выбора и отсева «слабых». Недостаток этого алгоритма – использование постоянного 256-битного закрытого ключа, из которого формируются блочные ключи.

При программной реализации этот способ шифрования не обеспечивает высокую скорость (более 1 Мбит/с) из-за необходимости преобразования форматов данных. Современные процессоры оперируют данными, размер которых кратен 1 байту (8, 16, 32, 64, 128 битов). В указанном способе используется большое число операций подстановки над 4-битовыми блоками данных (до 32 раундов). При выполнении каждого раунда процессор выполняет преобразование форматов данных. Сначала в байте выделяют 4-битовые тетрады (8 битов → 4+4 бита), а затем выполняют подстановку по таблице и обратное преобразование (8×4 бита → 32 бита). Преобразование форматов данных снижает скорость шифрования.

В стандарте США DES [2] (Digital Encripting Standart) каждый блок данных шифруется независимо от других. Для всех *i*-тых входных блоков данных будет использован одинаковый *i*-й блочный ключ, что снижает уровень криптозащиты. DES использует ключ малого размера, что делает его уязвимым к криптоанализу на основе подбора ключа.

В способах блочного шифрования Молдовяна для формирования блочного ключа используется операция подстановки, зависящая от *j*-го блока данных и секретного ключа шифрования [3 – 5].

Недостатком всех рассмотренных способов блочной шифрации является использование одного исходного закрытого ключа, из которого с помощью подстановок, перестановок, преобразований, функций и т.п. получают последовательность подключей для подблоков. Зная правило преобразования, можно подобрать ключ.

Секретный ключ можно не только подобрать, но также его можно похитить или утратить в результате отказа компьютера или устройства хранения информации. Создание и хранение копий секретных ключей снижает уровень их безопасности.

Стандарт блочного шифрования DES

В стандарте США DES [3] (Digital Encripting Standart) выполняется шифрование блоков данных. Сначала вводят секретный ключ. Затем разделяют блок данных на два подблока L и R, после чего поочередно изменяют блоки. Для этого выполняют операции поразрядного суммирования по модулю два над подблоком L и двоичным вектором, который формируется как выходное значение некоторой функции F от значения подблока R.

После этого блоки переставляются местами. Функция F в указанном способе реализуется путем выполнения операций перестановки и подстановки, выполняемых над подблоком R [3]. В DES каждый блок данных шифруется независимо от других. Это позволяет расшифровывать отдельные блоки зашифрованных сообщений или структуры данных. DES использует ключ малого размера, что делает его уязвимым к криптоанализу на основе подбора ключа. В DES ключ шифрования представлен в виде совокупности подключей. Для всех *i*-тых входных блоков данных будет использован одинаковый *i*-й подключ, что снижает уровень криптозащиты.

Способы блочного шифрования Молдовяна

В патентной литературе описаны способы блочного шифрования Молдовяна [4 – 6]. Этот способ включает формирование ключа шифрования в виде совокупности подключей. Производится разбиение блока данных на подблоки и поочередное преобразование подблоков путем выполнения операции шифрации над подблоком и подключом.

Перед выполнением двуместной операции шифрации над *i*-м подблоком и *i*-м подключом выполняют операцию подстановки над *i*-м подключом, зависящую от *j*-го подблока, где $j \neq i$. В качестве выполняемой над подключом операции подстановки, зависящей от *j*-го подблока, используют операцию подстановки, зависящую от ключа шифрования [4 – 6].

Недостатком известных способов блочной шифрации является использование одного исходного закрытого ключа, из которого с помощью подстановок, перестановок, преобразований, функций и т.п. получают последовательность подключей для подблоков. Зная правило преобразования, можно подобрать ключ.

Секретный ключ можно подобрать, похитить или утратить в результате отказа компьютера или устройства хранения информации. Создание и хранение копий секретных ключей снижает уровень их безопасности.

Постановка задачи защиты информации в распределенных системах управления с открытыми каналами связи

Для криптографической защиты информации в распределенной ИАСУ необходимо разработать новый способ блочной шифрации с учетом специфики открытых каналов связи. Этот способ должен подходить для разных топологий сетей, для компьютерных и промышленных сетей, для разных протоколов, размеров передаваемых пакетов и скоростей передачи данных. Таким образом, новый способ блочной шифрации должен быть надстройкой над протоколами транспортного уровня.

Способ блочной шифрации должен обеспечивать обмен данными с высокой скоростью. Новый способ блочной шифрации должен обладать повышенной криптостойкостью.

Способ блочного шифрования сообщений и передачи шифрованных данных по открытому каналу

За основу разработки был принят способ блочного шифрования сообщений с закрытым ключом и передачи шифрованных данных по открытому каналу [6, 7].

Этот способ включает разбиение сообщения в передатчике на совокупность отдельных блоков данных фиксированной длины (рис. 3). Перед передачей сообщения проводится инициализация закрытого ключа, когда в передатчике и приемнике записывают одинаковое значение закрытого секретного ключа. Для инициализации используется эталон закрытого ключа, который имеется у передатчика и приемника. Затем из закрытого ключа формируют последовательность подключей для шифрации ими блоков данных. Зашифрованная информация по блокам передается по открытому каналу связи.

Для создания блочного ключа используется генератор случайных чисел. Случайное число используется как модификатор закрытого секретного ключа. Блочный ключ для (*i*+1)-го блока добавляется к *i*-му блоку данных, после чего и ключ и данные шифруются *i*-тым блочным ключом (см. рис. 3). Размер блока увеличивается за счет присоединения к данным случайного числа. Зашифрованный блок передают по открытому каналу связи.

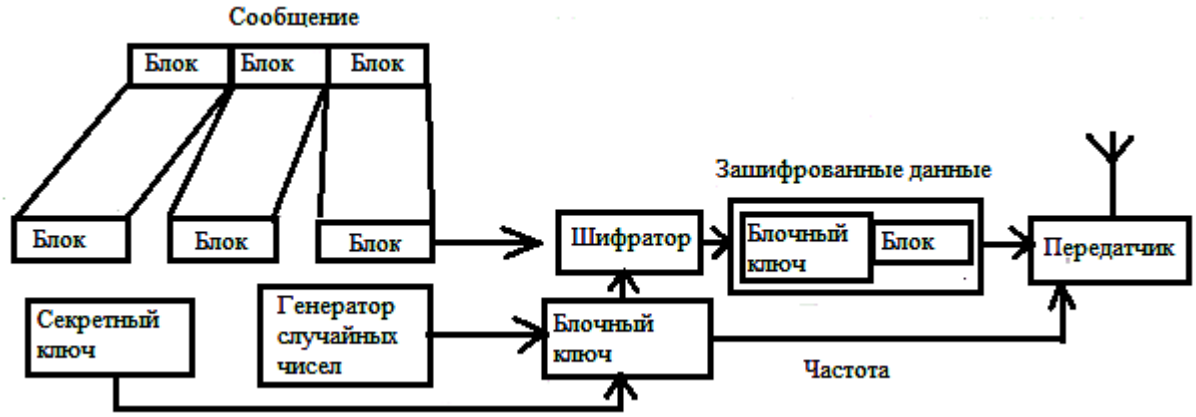

Рис. 3. Блочная шифрация с закрытым ключом и передача информации по открытому каналу связи

На приемном конце выполняют дешифрацию блоков данных с использованием подключей (рис. 4). Блочные ключи являются случайными числами, которые получают на передающей стороне с использованием секретного ключа. Эти случайные числа присоединяют к данным. К i-му блоку данных присоединен случайный (i+1)-й блочный ключ. Блочный ключ с номером (i+1) используется для дешифрации следующего по порядку (i+1)-го блока.

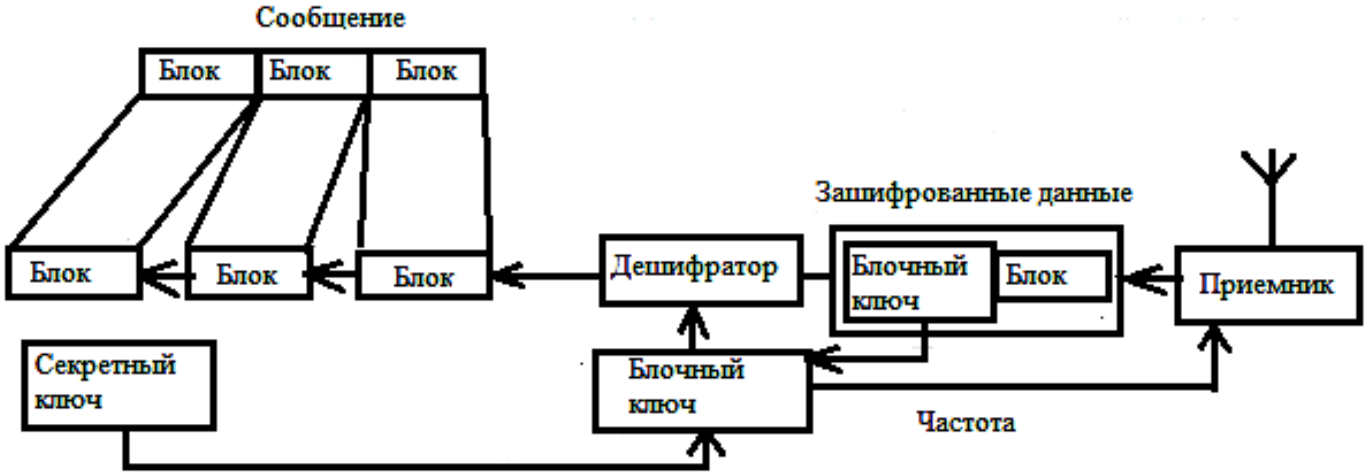

Рис. 4. Прием информации по открытому каналу связи и дешифрация с закрытым ключом

На приемном выполняют дешифрацию принятых блоков. В блоках выделяют случайные числа и полезную информацию в виде данных. Из блоков данных формируют сообщение. Случайные числа используют для модификации закрытого ключа при дешифрации следующего блока[6, 7].

Описанный выше способ блочного шифрования сообщений и передачи шифрованных данных с закрытым ключом [6, 7] может использоваться в глобальных, компьютерных и промышленных сетях.

Для взлома зашифрованного сообщения необходимо подобрать первоначальный секретный ключ для дешифрации первого блока, провести его дешифрацию и вычислить случайный блочный ключ для дешифрации следующего блока. Этот процесс надо повторить для всех блоков сообщения. Таким образом, криптостойкость блочной шифрации повышается. Если получить последовательность блоков в порядке их формирования, то достаточно подобрать только первый закрытый ключ. Подключи для всех последующих блоков можно получить с помощью случайных чисел, которые присоединяются к блоку данных. Для этого надо знать правило формирования подключа из случайных чисел.

Разработка нового способа блочного шифрования сообщений и передачи шифрованных данных по открытому каналу.

Предложен новый способ блочной шифра-

ции с закрытым ключом [8]. Закрытый ключ состоит из конечной последовательности подключей.

Предложено повысить криптостойкость шифрации за счет следующих преобразований, которые препятствуют накоплению последовательных блоков сообщения третьими лицами, с целью их последующего криптоанализа:

– перемешивание блоков сообщения с блоками такого же размера, содержащими случайные числа;

– выбор разных частот для передачи блоков;

– выбор частоты для передачи каждого блока на основе генератора случайных чисел.

Блочная шифрация с закрытым ключом и передача информации по радиоканалу показана на рис. 3, 4.

В начале передачи сообщения в передатчике и приемнике выполняют инициализацию закрытого ключа, т.е. вводят начальное значение ключа (при $i = 0$) для шифрации-дешифрации первого блока. Этот ключ одинаковый у приемника и передатчика. Затем сообщение разделяют на отдельные блоки данных. Блоки данных перемешивают с блоками, содержащими случайные числа.

В передатчике к i-му блоку присоединяют служебную информацию для следующего (i+1)-го блока, которая включает номер текущего блока в составе сообщения, случайное число для формирования подключа, кодовый признак, указывающий, что блок содержит случайные числа, а также случайное число, задающее частоту передачи по радиоканалу. Затем i-й блок и служебную информацию шифруют i-м подключом и в зашифрованном виде передают по радиоканалу на выбранной частоте.

Таким образом, блоки, содержащие данные, шифруют с помощью закрытого ключа.

Каждый блок шифруют своим уникальным подключом.

Первый подблок данных шифруют введенным секретным ключом. Затем к каждому (i+1)-му блоку формируют новый (i+1)-й подключ. Для создания (i+1)-го подключа используют предыдущий i-й подключ и случайное число из i-го блока. Случайное число формируется в передатчике с помощью генератора случайных чисел (см. рис. 3).

Прием и дешифрация информации блоков данных показана на рис.3

Приемник получает и дешифрует i-й блок, используя i-й подключ. После дешифрации i-й блок разделяют на данные и служебную информацию для следующего (i+1)-го блока. Служебная информация включает номер блока, случайное число для формирования следующего (i+1)-го ключа, кодовый признак, указывающий, что блок содержит случайные числа, а также число, задающее частоту для передачи по радиоканалу следующего (i+1)-го блока данных. Затем приемник формирует новое значение подключа для (i+1)-го блока данных, используя i-й подключ и случайное число из i-го блока данных. Таким образом, после передачи и приема очередного блока данных, закрытый ключ синхронно меняется у передатчика и приемника данных. Обеспечивается случайная модификация блочных ключей и при этом сохраняется эквивалентность закрытых ключей на передающей и принимающей сторонах.

Приемник пропускает без обработки блоки, содержащие случайные числа. Приемник дешифрует с помощью подключа блоки, содержащие данные, и подсоединяет эти блоки к сообщению в порядке их номеров (см. рис. 3).

Разработанный способ блочной шифрации обеспечивает эквивалентные переменные ключи у передатчика и приемника данных. При приеме-передаче данных закрытый ключ постоянно меняется, причем случайным образом. По радиоканалу передают только отдельные фрагменты закрытого ключа в зашифрованном виде. Закрытый ключ остается секретным и недоступен для третьих лиц.

При перехвате информации, передаваемой по радиоканалу, у «третьих» лиц будет только часть секретного подключа. Этого не достаточно для дешифрации даже одного блока, и тем более, всего сообщения. Блоки данных перемешиваются с блоками случайных чисел и передаются на разных частотах.

Передача зашифрованных данных и случайных чисел по радиоканалу на разных частотах показана на рис. 5. На рис. 5 представлена передача зашифрованной информации одновременно на нескольких частотах $F1,\ldots, F3$ в течение времени $t1..t4$.

Попытка дешифрации блока, содержащего случайные числа, дает бессмысленный набор знаков и затрудняет криптоанализ.

Описанная выше процедура изменения закрытого секретного ключа позволяет использовать простые алгоритмы шифрации, такие как алгоритм Цезаря и др. Размер секретного ключа превышает размер шифруемых данных, и сложные алгоритмы не требуются. Упрощение алгоритма шифрации позволяет повысить скорость передачи информации по сети, вы-

свобождает ресурсы вычислительной системы для выполнения управляющей программы. Использование простых алгоритмов шифрации снижает затраты ресурсов и повышает эффективность РСУ.

Рис. 5. Передача зашифрованных данных и случайных чисел на разных частотах

Выводы

Разработан новый способ криптографической защиты информации на основе известных способов блочной шифрации с закрытым ключом.

Рассмотрена передача зашифрованных сообщений по радиоканалу. Обычно все сообщения передаются на одной частоте. Смена частоты приводит к потере информации, которая передается на других частотах. При приеме информации на одной частоте, третьи лица могут получить только часть из общей последовательности зашифрованных блоков данных, которые перемешаны с блоками случайных чисел.

Для криптоанализа требуется знать все частоты, на которых возможна передача, и непрерывно вести прием всей информации на этих частотах.

В заявленном способе существенным отличием является передача в составе каждого передаваемого блока дополнительной служебной информации, в том числе:

– случайного числа, которое используется для формирования блочного ключа из закрытого секретного ключа;

– кодовый признак, который указывает, что данный блок содержит случайные числа или полезную информацию, данные;

– номер блока в составе сообщения;

– частота передачи для следующего блока.

Служебная информация передается в зашифрованном виде.

При шифрации и дешифрации формируется блочный ключ, и при этом длина закрытого секретного ключа превышает объем шифруемой информации.

Таким образом, заявленный способ блочного шифрования данных с закрытым ключом затрудняет криптоанализ и обеспечивает высокий уровень криптостойкости.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. **Стандарт СССР** ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования, Москва, ГК СССР по стандартам 1989 г.

2. **National** Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46, January 1977.

3. **Пат. на изобретение 2211541 РФ** МПК H04L 9/00 .. Способ криптографического преобразования блоков цифровых данных [Текст]/ Молдовян А.А., Молдовян Н.А., Еремеев М.А., заяв. Молдовян Н.А. патентообл. ГУП Специализированный центр программных систем "Спектр", Молдовян А.А., Молдовян Н.А.-№ заявки 2001130201/09**,** заявл. 08.11.2001; опубл. 27.08.2003, Бюл. № 24. – 5 с.

4. **Пат. на изобретение 2140712 РФ** МПК H04L 9/00 Способ блочного шифрования двоичной информации [Текст]/ Молдовян А.А., Молдовян Н.А., Савлуков Н.В.: заяв. Молдовян А.А. патентообладатель ОАО "Московская городская телефонная сеть", ГУП Специализированный центр программных систем "СПЕКТР", Молдовян

А.А.-№ 98107784/09; заявл. 22.04.1998.; опубл. 27.10.1999, Бюл. № 10, – 3 с.

5. **Пат. на изобретение** 2103829 РФ МПК H04L 9/20 Способ шифрования информации, представленной двоичным кодом [Текст]/ Молдовян А.А., Молдовян Н.А., Молдовяну П.А.: заяв. и патентооб. ГУП "Специализированный центр программных систем "Спектр", Молдовян А.А., Молдовян Н.А..-№ 97104754/09; заявл 02.04.1997.; опубл. 27.01.1998, Бюл. № 1, – 3 с.

6. **Пат. на изобретение 2459367 РФ** МПК H04L 9/00 Способ блочного шифрования сообщений и передачи шифрованных данных с закрытым ключом [Текст]/ Кабак И.С., Суханова Н.В., Позднеев Б.М.: заяв. и патентообл. ФГБОУ ВПО МГТУ "СТАНКИН". (RU) -№ 2010129310/08,; заявл. 16.07.2010; опубл. 20.08.2012 Бюл. № 23, – 5 с.

7. **Пат. на изобретение 2 481 715 РФ** МПК H04L 9/00 Способ блочного шифрования сообщений и передачи шифрованных данных с закрытым ключом [Текст]/ Позднеев Б.М., Кабак И.С., Суханова Н.В.: заяв. и патентообл. ФГБОУ ВПО МГТУ "СТАНКИН". -№ 2011148733/08 ; заявл. 30.11.2011; опубл. 10.05.2013, Бюл. № 13, – 6 с.

8. **Пат. на изобретение 2 631 981 РФ** МПК H04L 9/06,H04K 1/04 Способ блочной шифрации с закрытым ключом [Текст]/ Суханова Н.В., Кабак И.С., Шептунов С.А., Соломенцев Ю.М. заявитель и патентообладатель ФГБУН Институт конструкторско-технологической информатики РАН (ИКТИ РАН).№ 2016104815; заявл 12.02.2016.; опубл. 29.09.2017, Бюл. № 28, – 8 с.

REFERENCES

1. Standard of the USSR RSS 28147-89. *System of Information Processing. Cryptographic Protection. Algorithm of Cryptographic Transformation*, Moscow SC of the USSR for Standards 1989.

2.National Bureau of Standards. Data Encryption Standard. Federal Information Processing Standards Publication 46, January 1977.

3. Pat for Invention 2211541 RF IPC H04L 9/00.. *Method for Cryptographic Transformation of Digital Data Blocks* [Text] / Moldovyan A.A., Moldovyan N.A., Eremeev M.A., applicant: Moldovyan N.A., patent holder: SUC Specialized Center of Program Systems “Spectrum”, Moldovyan A.A., Moldovyan N.A. – Application No. 2001130201/09, applied 08.11.2001; published 27.08. 2003, Bull. No.24. – pp. 5.

4. Pat. for Invention 2140712 RF IPC H04L 9/00 *Method for Block Encryption of Binary Information* [Text] / Moldovyan A.A., Moldovyan N.A., Savlukov N.V.: applicant: Moldovyan A.A., patent holder PC “Moscow Municipal Telephone Network”, SUC Specialized Center of Program Systems “Spectrum”. Moldovyan A.A. – No. 98107784/09; applied: 22.04.1998; published: 27.10.1999, Bull. No.10, - pp. 3.

5. Pat. for Invention 2103829 RF IPC H04L 9/20 *Method for Encryption of Information Presented as Binary Code* [Text] / Moldovyan A.A., Moldovyan N.A., Moldovyanu P.A.: applicant and patent holder: SUC “Specialized Center of Program Systems “Spectrum”, Moldovyan A.A., Moldovyan N.A. – No. 97104754/09; applied: 02.04.1997.; published: 27.01.1998, Bull. No.1, - pp. 3.

6. Pat. for Invention 2459367 RF IPC H04L 9/00 *Method for Block Encryption of Messages and Encoded Data Transfer with Private Key* [Text] / Kabak I.S., Sukhanova N.V., Pozdneev B.M.: applicant and patent holder: FSBEI HVE MSTU “STANKIN”. (RF) – No.2010129310/08,; applied: 16.07.2010; published: 20.08.2012, Bull. No. 23, - pp. 5.9. Sukhanova N.V. Development of intelligent automated control systems in mechanical engineering // Science intensive technologies in mechanical engineering. – 2018. – №11(89). – pp. 42-48.

7. Pat. for Invention 2 481 715 **RF** IPC H04L 9/00 *Method for Block Encryption of Messages and Digital Data Transfer with Private Key* [Text] / Pozdneev B.M., Kabak I.S., Sukhanova N.V.: applicant and patent holder: FSBEI HVE MSTU “STANKIN”. – No. 2011148733/08; applied: 30.11.2011; published: 10.05.2013, Bull. No.13, - pp. 6.

8. Pat. for Invention 2 631 981 RF IPC H04L 9/06, H04K 1/04 *Method for Block Encryption with Private Key* [Text] / Sukhanova N.V., Kabak I.S., Sheptunov S.A., Solomentsev Yu.M. applicant and patent holder: FSBEI Institute of Design-Technological Informatics of RAS (IDTI RAS). No. 2016104815; applied: 12.02.2016.; published: 29.09.2017, Bull. No. 28, - pp. 8.

Рецензент д.т.н. А.Б. Барский

Учредитель: Федеральное государственное бюджетное образовательное учреждение
высшего образования "Брянский государственный технический университет"
Адрес редакции и издателя: 241035, Брянская область, г. Брянск, бульвар 50 лет Октября, 7
ФГБОУ ВО «Брянский государственный технический университет»
Телефон редакции журнала: 8-903-592-87-39. E-mail: naukatm@yandex.ru
Вёрстка А.А. Алисов. Технический редактор А.А. Алисов. Корректор Н.В. Дюбкова.
Сдано в набор 05.12.2018. Выход в свет 31.01.2019.
Формат 60 × 88 1/8.Бумага офсетная. Усл. печ. л. 5,88.
Тираж 500 экз. Свободная цена.
Отпечатано в лаборатории оперативной полиграфии
Федерального государственного бюджетного образовательного учреждения высшего образования
"Брянский государственный технический университет"
241035, Брянская область, г. Брянск, ул. Институтская, 16