УДК 681.322, 681.51

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

Кирьянов Б.Ф., Кирьянов Д.В.

ГОУ ВПО «Новгородский государственный университет им. Ярослава Мудрого» Минобрнауки России, Великий Новгород, e-mail: NovSU@novsu.ru

Предлагается модель высоконадёжной системы передачи информации по каналам связи. Передаваемая информации скрывается от потенциальных «взломщиков» каналов связи путём случайного перемешивания её с цифровым шумом: на объекте-передатчике осуществляются замена некоторых фрагментов цифрового шума фрагментами передаваемой информации, а на объектах-приёмниках фрагменты переданной информации выделяются из цифрового шума. Компьютерное моделирование предлагаемой системы связи при различных помехах в используемых каналах, в том числе при передаче информации по интернету, показало надёжную работу этой системы.

Ключевые слова: скрытая передача информации, цифровой шум, генераторы псевдослучайных кодов (ГПСК), синхронизм ГПСК, Интернет

PROVISION OF INFORMATION IN CHANNELS OF COMMUNICATION

Kiryanov B.F., Kiryanov D.V.

SEI of HPE «The Novgorod State university it. Yaroslav Mudry» of Department of education and science of Russia, Velikiy Novgorod, e-mail: NovSU@novsu.ru

Proposes a model of a highly reliable system of data transfer via communication channels. The transmitted information is hidden from potential «intruders» channels by randomly mixing it with digital noise: on-site replacement of the transmitter are made of some fragments of digital noise fragments of information transmitted, and the receiver object fragments transmitted information extracted from digital noise. Computer simulation of the proposed system under different communication channels used in the noise, including the transmission of information on the Internet, showed a reliable operation of this system.

Keywords: hidden communication, digital noise, generators of pseudorandom codes (GPC), synchronization of GPC, Internet

В последние годы участились случаи «взлома» каналов передачи различной информации, в том числе конфиденциальной и закрытой. Вместе с тем непрерывно растёт число задач, связанных с взаимодействием между территориально удаленными объектами и соответственно число объектов, передающих по каналам связи конфиденциальную информацию. Поэтому проблема обеспечения безопасности информации, передаваемой по каналам связи, стала весьма актуальной. На важность решения данной проблемы указывалось в Указе Президента РФ № 351 от 17 марта 2008 года «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», а также в ряде документов Правительства РФ, например, в приказе № 104 от 25 августа 2009 г. по министерству связи и массовых коммуникаций РФ «Об утверждении требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования».

Решение указанной проблемы связано с решением двух задач:

1. Обеспечение практически невозможного получения кодов передаваемой информации потенциальными взломщиками каналов связи (далее – хакерами);

2. Обеспечение практически невозможной расшифровки передаваемой информации в случае приёма её хакерами.

Вторая задача – это задача выбора криптостойкого кодирования передаваемой информации [1 и др.]. В данной работе она не рассматривается.

Целью настоящей работы является разработка и исследование методов обеспечения практически невозможного получения передаваемой информации хакерами, модернизация структуры разработанной ранее модели с целью обеспечения удобства её настройки и контроля правильности её работы, а также оценка возможности использования интернета для построенная на его основе системы скрытой передачи информации, каналы которой не подвержены «взлому».

Модернизация и исследование модели системы связи

В публикациях [2–4] авторами предлагался и исследовался вариант модели системы передачи информации по каналам связи, в которой фрагменты передаваемой информации случайным образом вставлялись в последовательность цифрового шума. На принимающих информацию объектах эти фрагменты выде-

лялись из указанной последовательности. Для реализации такой передачи предлагалось использовать на связывающихся объектах синхронно идущие часы, роль которых могут выполнять генераторы псевдослучайных кодов (ГПСК), введённые в режим синхронизма. ГПСК обеспечивают синхронность моментов введения фрагментов двоичных кодов полезной информации в последовательность случайных двоичных импульсов на передающем объекте и моментов выделения фрагментов двоичных кодов полезной информации из цифрового шума на объекте, принимающем информацию.

Некоторыми недостатками указанного варианта модели системы связи являлось то, что, во-первых, последовательность псевдослучайных кодов ГПСК запрашивающего связь объекта, вводящая ГПСК вызываемых им объектов в режим синхронизма с ним, была доступна злоумышленникам, что приводило к отличной от нуля вероятности обнаружения хакерами кодов передаваемой информации, а, во-вторых, в модели отсутствовал удобный контроль правильности принятия решения о вхождении ГПСК вызываемых на связь объектов с ГПСК запрашивающего их объекта.

В работе ставятся следующие основные задачи: скрыть от возможных «взломщиков» каналов связи алгоритм ввода в цифровой шум фрагментов полезной информации, обеспечить удобный контроль правильности работы модели, исследовать её характеристики и оценить возможность использования сети Интернет для реализации предложенного способа скрытой передачи информации.

В соответствии с указанным основными отличиями усовершенствованной модели от прежнего её варианта являются введение в неё режима проверки правильности входа ГПСК в режим синхронизма и перевод ГПСК системы связи на другой алгоритм их работы после момента установления их синхронизма и, соответственно, на другое случайное расположение фрагментов полезной информации в цифровом шуме. Рис. 1 и рис. 2 поясняют работу модели в режиме исследования (10000 запусков процесса установления связи) и в режиме проверки правильности её работы при одиночных запусках этого процесса с выводом содержимого регистров ГПСК передающего и принимающего объектов. По содержимому этих регистров можно просто проверить правильность решения о вхождении ГПСК в режим синхронизма.

Решение о входе ГПСК вызываемого объекта в режим синхронизма с ГПСК вызывающего объекта принимается в том случае, если выполнено условие в котором A – матрица, реализующая один шаг работы ГПСК (рис. 2). Однако, если при выполнении этого условия $Y_1^1 X_1$, то решение о наступлении синхронизма ГПСК является ошибочным (ложный синхронизм). Для гарантированного входа в правильный синхронизм при сильных помехах в каналах связи рекомендуется переходить на передачу полезной информации после 3,5-кратного выполнения указанного условия входа ГПСК вызываемого объекта в правильный синхронизм с ГПСК вызывающего объекта.

Рис. 1. Структура модели в режиме исследования и результаты установления связи

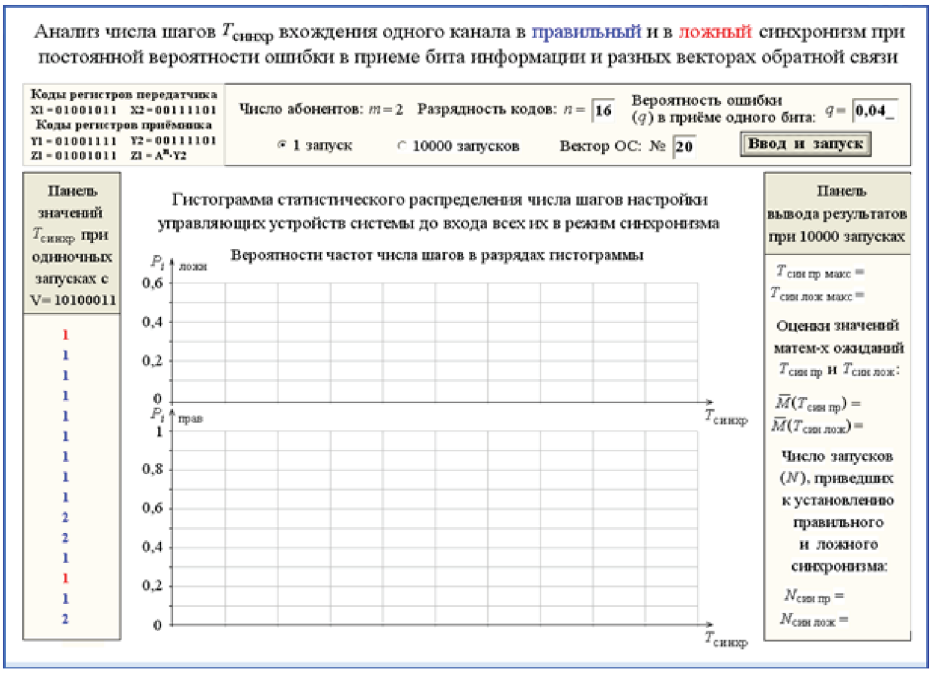

Рис. 2. Структура модели в режиме проверки правильности её работы

Как только ГПСК запрашиваемого объекта войдёт в режим синхронизма и оказывается готовым к приёму информации, он сообщает об этом вызывающему его объекту по другому каналу связи. При этом ГПСК этих объектов, управляющие каналом их связи, одновременно переводятся на другой алгоритм вставок фрагментов полезной информации в цифровой шум, гарантируя практически нулевую вероятность выделения злоумышленниками этих фрагментов из цифрового шума. Такие алгоритмы могут храниться в памяти компьютеров и выбираться из неё по адресу, учитывающему код ГПСК, на котором ГПСК вошли в режим синхронизма, то есть фактически по случайному адресу.

Об использовании Интернета для скрытой передачи информации

Интернет является, по-видимому, наиболее популярным средством обмена информацией. Он допускает и прямое соединение соответствующих объектов, организуемое, например, согласно технологии, изложенной в [6]. Для проверки надёжности установления синхронизма ГПСК объектов рассматриваемой системы связи авторами передавалась по Интернету последовательность 1000 16-разрядных двоичных кодов ГПСК с объекта-передатчика для настройки ГПСК объекта-приёмника. При приёме каждого указанного кода ГПСК объекта-приёмника входил в синхронизм с ГПСК объекта-передатчика. Это свидетельствует о том, что в каналах сети Интернет помехи практически отсутствуют. Поэтому на её основе можно строить надёжно работающие системы скрытой передачи информации.

Заключение

Усовершенствованная модель системы скрытой передачи информации надёжно защищает передаваемую информацию от попыток её вскрытия при атаках взломщиков каналов связи. Для её практической реализации может быть использована сеть Интернет.

Список литературы

1. Венбо Мао. Современная криптография. Теория и практика. – М.: Вильямс, 2005. 768 с.

2. Кирьянов Б.Ф. Математическое моделирование в среде Delphi: Монография. – М.: РАЕ. 2012. 154 с.

3. Кирьянов Б.Ф., Кирьянов Д.В. Модель системы связи с высоконадежной защитой информации в каналах её передачи // Вестник НовГУ. Сер. Технич. науки. 2011. Вып. 65. С. 73–75.

4. Кирьянов Б.Ф., Кирьянов Д.В. Модель системы обмена конфиденциальной информацией по каналам связи // Обозрение прикладной и промышленной математики. 2011. Т. 18. Вып.5: Научные доклады XII Всероссийского симпозиума по прикладной и промышленной математике. С. 777.

5. Кирьянов Б.Ф., Кирьянов Д.В. К проблеме защиты информации в каналах связи. – М.: РАЕ. Современные проблемы науки и образования. 2012. URL: http://www.science-education.ru/106-7455.

6. Создаём локальную сеть через Интернет. – URL: Testino от 6-01-2012/статьи >> Windows.