УДК 681.322, 681.51

К ПРОБЛЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

Кирьянов Б. Ф., Кирьянов Д. В.

ГОУ ВПО «Новгородский г*осударственный университет им. Ярослава Мудрого» (НовГУ) МИНОБРНАУКИ России, Россия (816003), Великий Новгород, ул. Большая Санкт-Петербургская, 41, e-mail: NovSU@novsu.ru*

В последние годы президентом и правительством РФ неоднократно указывалось на необходимость обеспечения защиты информации, передаваемой по каналам связи. Одним из вариантов обеспечения указанной безопасности является использование скрытой передачи полезной информации в смеси её с цифровым шумом (со случайными битами). Для реализации такого обмена информацией по каналам связи на объектах системы связи необходимо иметь синхронно работающие генераторы управляющих сигналов. Идея защиты информации в каналах связи путём перемешивания её с цифровым шумом была предложена Б. Ф. Кирьяновым ещё в 60-х годах прошлого столетия. В последнее десятилетие под его руководством были исследованы характеристики различных вариантов систем скрытой передачи информации. Описываемая в данной статье модернизированная модель, реализующая систему скрытой передачи информации, не оставляет «взломщикам» каналов связи никаких шансов выделения бит полезной информации из смеси их с цифровым шумом.

Ключевые слова: М-последовательность, генератор псевдослучайных кодов (ГПСК), синхронизм нескольких ГПСК, ложный синхронизм, цифровой шум.

TO THE PROBLEM OF PROTECTION OF INFORMATION IN COMMUNICATION CHANNELS

Kiryanov B. F., Kiryanov D. V.

SEI of HPE «The Novgorod state university it. YaroslavMudry» (NovSU) of Department *of education and scienceof Russia, Russia (816003), Great Novgorod, street Greater Sankt-Petersburg, 41,e-mail: NovSU@novsu.ru*

The Russian president and the Russian Federation government had in recent years pointed out the requirement to support channel transmitted data security. A certain method of attaining that is transmitting the mix of usable data and stochastic bit noise. To implement such a method, there must be the synchronously operating deterministic random bit generators producing control signals in the transmitter and in the receiver.
Theconcept of mixing usabledataandstochastic bit noise has been propounded by B.F. Kir'yanovin 1960th. During the past decade, it was analyzing descriptions of some various versions of steganographical data transmitting system under the direction of him. This article generally focuses on the model of steganographical data transmitting system, which was improved for prevention of a cracker's possibility of useful data's bits separation from the transmitting mix.

Key words: M-sequence, generator of pseudo-casual codes (GPSK), synchronism of several GPSK, false synchronism, digital noise.

Введение

В последние годы в связи с непрерывным ростом числа задач, связанных с взаимодействием между территориально удаленными объектами и соответственно необходимостью передачи по каналам связи конфиденциальной информации, весьма актуальной становится проблема обеспечения безопасности этой информации. 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 обеспе-

чению целостности, устойчивости функционирования и безопасности информационных систем общего пользования». Разработка моделей и методов обеспечения безопасности информации, передаваемой по каналам различной физической природы и соответственно с помощью различных технических средств, представляет собой важную задачу.

Для решения проблемы обеспечения безопасности информации, передаваемой по каналам связи, автором ещё в конце прошлого века был предложен способ передачи этой информации в смеси с цифровым шумом [2, 3], обеспечивающий скрытие передаваемой зашифрованной или незашифрованной от потенциальных взломщиков каналов связи. Различные аспекты реализации указанного способа исследовались автором и его учениками в работах [1–5, 7]. Была разработана и исследована компьютерная модель, реализующая предложенный способ передачи, которая продемонстрировала достаточно высокую надёжность выделения полезной информации из смеси её с цифровым шумом на приёмном конце канала связи. В 2011–2012 годах были выяснены и сформулированы [6, 8–10] задачи, которые необходимо проработать для реализации предложенной модели в реальных системах, рекомендованы и методы, позволяющие свести вероятность выделения «взломщиками» каналов связи передаваемой информации из её смеси с цифровым шумом практически к нулю. К указанным задачам относится решение проблем начала и окончания передачи и приёма полезной информации.

В данной публикации поясняются сущность указанных задач и методов совершенствования систем связи с передачей полезной информации в смеси с цифровым шумом, приводится вариант решения проблемы выбора моментов начала передачи информации и её окончания; предлагается вариант системы связи с практически нулевой вероятностью извлечения взломщиком канала связи кодов передаваемой информации из последовательности кодов цифрового шума.

Модернизированный вариант системы связи

В предложенном ранее варианте реализации системы связи предлагалось устанавливать на концах каждого канала связи генераторы псевдослучайных кодов (ГПСК) на основе М-последовательностей. По короткой настраивающей последовательности кодов ГПСК передающего информацию объекта системы связи (ГПСК-1) ГПСК на приёмном конце канала связи (ГПСК-2) быстро вводился в режим синхронизма с ГПСК-1, то есть начинал работать в фазе с ГПСК-1. После этого по каналу связи начинал передаваться цифровой шум – случайные числа, вырабатываемые с использованием генератора физического шума. По установленным заранее кодам ГПСК в канал связи вместо передаваемого случайного кода вставлял-

ся код полезной информации, который на приёмном конце канала связи выделялся из последовательности цифрового шума.

В связи с тем, что настраивающая последовательность кодов ГПСК-1, а следовательно, и последовательность кодов ГПСК-2, вошедшего в синхронизм ГПСК-1, были доступны потенциальным взломщикам канала связи, для выделения кодов полезной информации из последовательности цифрового шума им необходимо было только выяснить коды ГПСК (не обязательно полноразрядные), при появлении которых осуществлялась передача очередного фрагмента полезной информации. При шифровании передаваемой полезной информации и обнаружении её взломщикам канала связи им необходимо было пытаться расшифровать эту информацию. Тем не менее, в рассматриваемой ранее модели для скрытия полезной информации использовался только один параметр-пароль, а именно – совокупность кодов управляющей передачей полезной информации М-последовательности, при появлении которых эта информация вставляетсяв цифровой шум и соответственно выделяется из него.

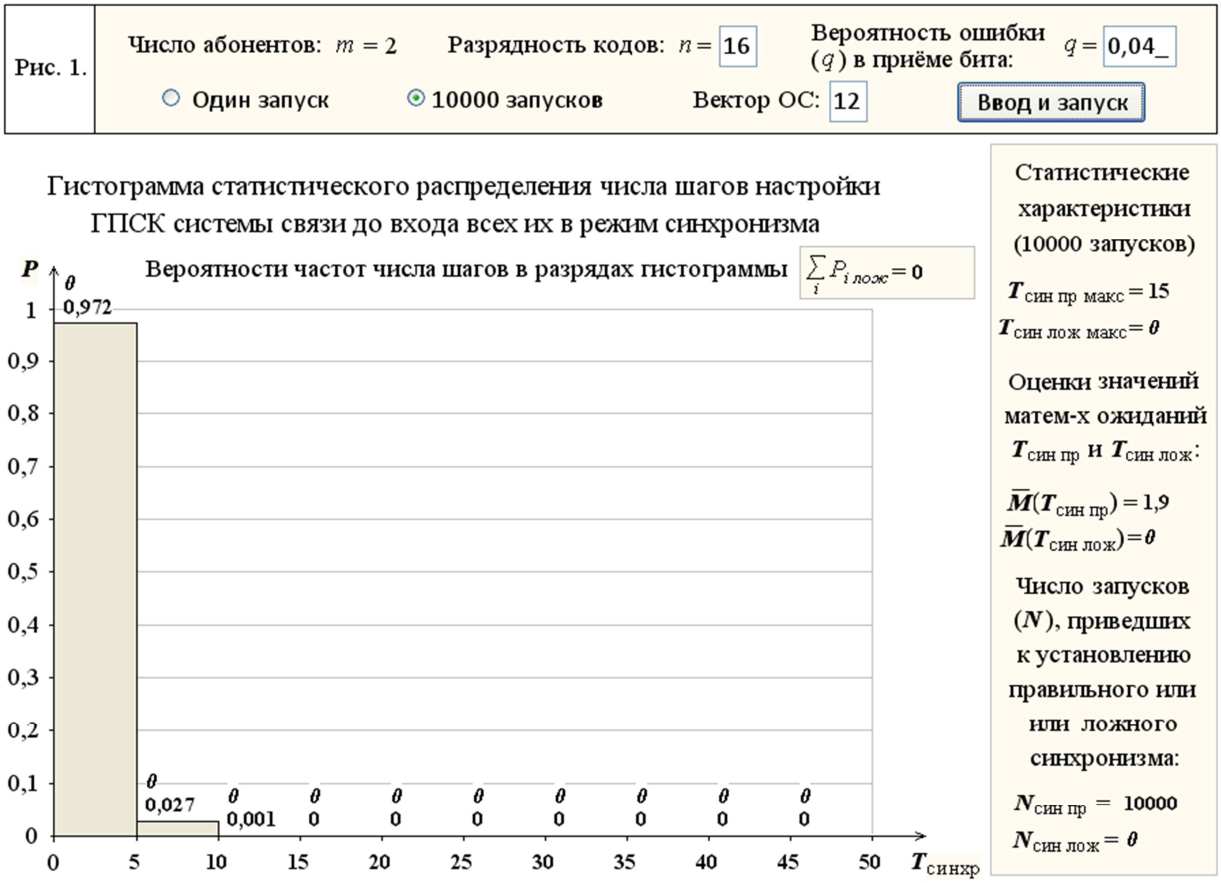
В модернизированной модели системы связи после установления синхронизма указанных ГПСК при появлении в них определённого полноразрядного кода осуществляется синхронный переход обоих ГПСК на другую управляющую передачей полезной информации М-последовательность, которая в канал связи не передавалась и, следовательно, не известна потенциальным взломщикам канала связи. Новая М-последовательность является вторым параметром-паролем модернизированного варианта системы связи. Эта последовательность может выбираться случайным образом. В результате вероятность обнаружения взломщиками канала связи полезной информации, передаваемой набольшими фрагментами в смеси с цифровым шумом, оказывается практически нулевой (как известно, равной нулю такая вероятность не может быть).

Моделирование рассмотренного метода организации систем связи с высоконадёжной защитой информации в каналах связи с 16-ти и с 32-разрядными настраивающими кодами показало, что он обеспечивает быструю установку ГПСК-2 на объектах связи в режим синхронизма с ГПСК-1 (рис. 1 и 2). При малом уровне помех в канале связи (вероятность неверного приёма одного бита настраивающей последовательности не более 0,01) случаев неверного принятия решения о вхождении ГПСК-2 в синхронизм с ГПСК-1, обусловленных выполнением условия $\boldsymbol{X}2 = \boldsymbol{A}\cdot\boldsymbol{X}1,$ не наблюдалось. В приведённом выражении $\boldsymbol{X}1$ и $\boldsymbol{X}2$ – 16-разрядные или 32-разрядные части настраивающих кодов, а $\boldsymbol{A}$ – матрица, преобразующая код $\boldsymbol{X}1$ в код $\boldsymbol{X}2$, перестраиваемая с помощью задаваемых векторов обратной связи (ОС).

Статистические данные по вводу ГПСК в режим синхронизма показывают, что при наличии помех в каналах связи с увеличением разрядности настраивающих кодов вероятность установления ложного синхронизма ГПСК уменьшается, а среднее число шагов, при

которых возможно его установление, увеличивается. Для каналов связи с разным уровнем помех можно выбрать разрядность ГПСК, обеспечивающую надёжную их работу.

Рис. 1.



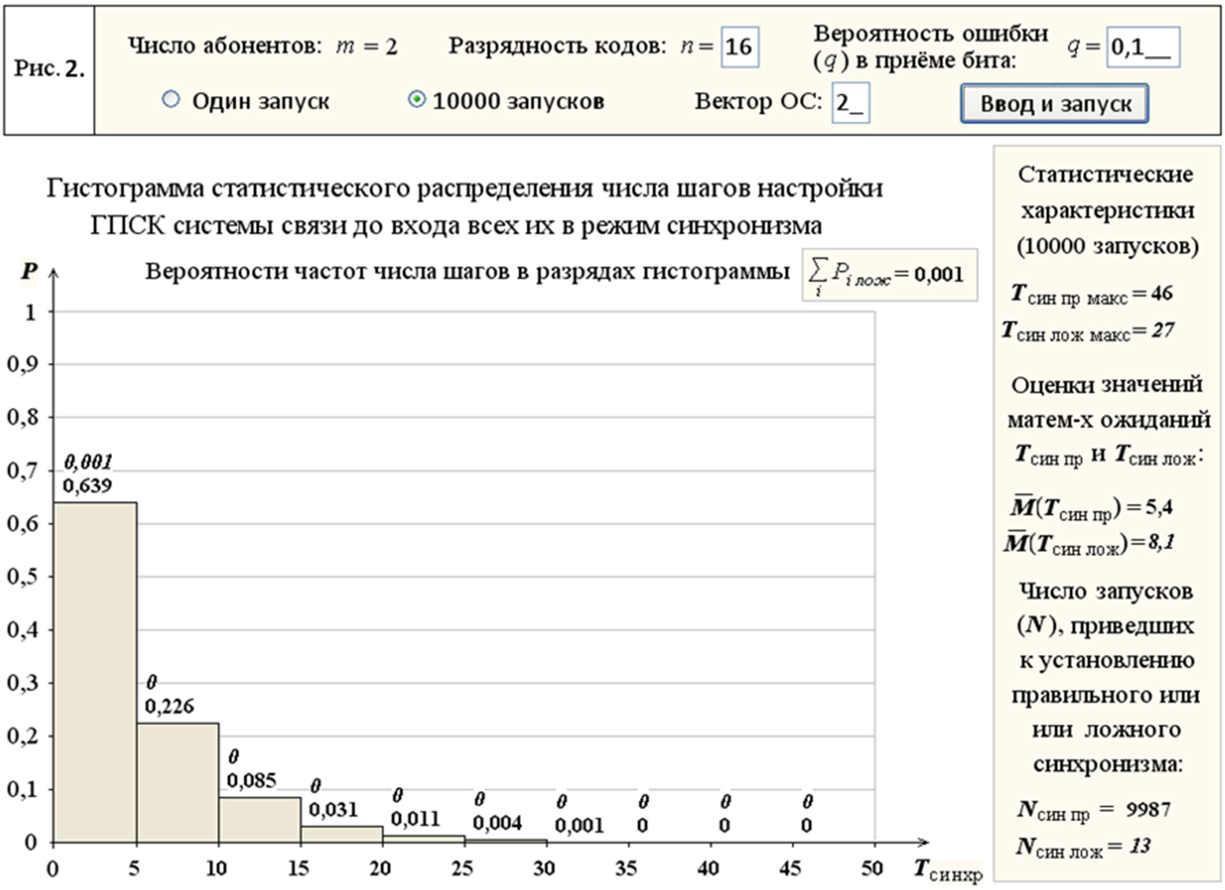


Рис. 1 и рис. 2. Вид панелей модели и результаты моделирования процесса установления синхронизма двух ГПСК при значительной вероятности q ошибки в приёме бита кода

Заключение. Разработанная модель обеспечивает надёжную защиту передаваемой информации и установку синхронизма ГПСК при высоком уровне помех в каналах связи.

Список литературы

1. Жгун А. А. Исследование ложной синхронизации приёма и передачи информации в модели скрытой передачи информации // Вестник Новгородского гос. ун-та им. Ярослава Мудрого. – 2010. – Вып. 60. – С. 33-35.

2. Жгун А. А., Жгун Т. В., Осадчий А. Н. Исследование синхронизации приёма и передачи информации в стенографической системе // Научно-технические ведомости СПбГПУ. – Сер. «Информатика. Телекоммуникации. Управление». – 2010. – № 2. – С. 7-11.

3. Жгун А. А., Кирьянов Б. Ф. Оценка вероятности синхронизации в модели скрытой передачи информации // Вестник Казанского гос. технич. ун-та им. А. Н. Туполева. – 2009. – Вып. 4. – С. 78 -81.

4. Кирьянов Б. Ф. Основы теории стохастических вычислительныхмашин и устройств: Монография.– Казанский авиац. Ин-т. Деп. в ЦНИИТЭИ приборостроения 21.05.76, № 524. – 168 с.

5. Кирьянов Б. Ф. Микро-ЭВМ как средства имитации и обработки случайных процессов в радиоэлектронных системах: Монография. – Новгородский политехнич. ин-т. Деп. в ВИНИТИ 10.11.86, № 7646-В86. – 213 с.

6. Кирьянов Б. Ф. Математическое моделирование в среде Delphi: Монография. – М.: РАЕ, 2012. –150 с.

7. Кирьянов Б. Ф., Кирьянов Д. В. Простой способ генерирования локальных баз данных и технология обращения к ним // Вестник Новгородского госуд. ун-та им. Ярослава Мудрого. Сер. Технич. науки. – 2010. – Вып. 60. – С. 41 – 42.

8. Кирьянов Б. Ф., Кирьянов Д. В. Модель системы связи с высоконадёжной защитой информации в каналах её передачи // Информационные технологии и их приложения. – Казань: КГТУ им А. Н. Туполева, 2011. – С. 207 – 211.

9. Кирьянов Б. Ф., Кирьянов Д. В. Модель системы связи с высоконадёжной защитой информации в каналах её передачи // Вестник Новгородского гос. ун-та им. Ярослава Мудрого. – 2011. – Вып. 65. – С. 73 – 75.

10. Кирьянов Б. Ф., Кирьянов Д. В. Математическая модель системы обмена конфиденциальной информацией по каналам связи // Обозрение ППМ. – Т. 128. – Вып. 5. – 2011. Научные доклады XII Всероссийского симпозиума по ППМ. – С. 777.

Рецензенты:

Песошин В. А., доктор технических наук, профессор, заведующий кафедрой компьютерных систем Казанского государственного национального исследовательского технического университета им. А. Н. Туполева, заслуженный деятель науки РФ, член-корреспондент АН Республики Татарстан.

Емельянов Г. М., доктор технических наук, профессор, профессор кафедры информационных технологий и систем Новгородского государственного университета им. Ярослава Мудрого.