

ОРГАНИЗАЦИЯ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ, ПРАКТИЧЕСКИ НЕ ПОДВЕРЖЕННЫХ ИХ ВЗЛОМУ

Кириянов Д.В.

ГОУ ВПО «Новгородский Государственный университет им. Ярослава Мудрого» (НовГУ)
МИНОБРНАУКИ России, Великий Новгород,
e-mail: www@novsu.ru

Предлагается вариант модели скрытой передачи информации по каналам связи, практически недоступной взломщикам каналов.

На важность защиты информации в каналах связи указывалось ещё в Указе Президента РФ № 351 от 17 марта 1986 года «О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информационного обмена», а затем – в ряде документов Правительства РФ.

Для решения проблемы обеспечения безопасности информации, передаваемой по каналам связи, в конце прошлого века Б.Ф. Кирияновым был предложен способ передачи этой информации в смеси с цифровым шумом, обеспечивающий скрытие ее от потенциальных взломщиков каналов связи. Различные аспекты реализации и применения указанного способа исследовались в работах [1–13].

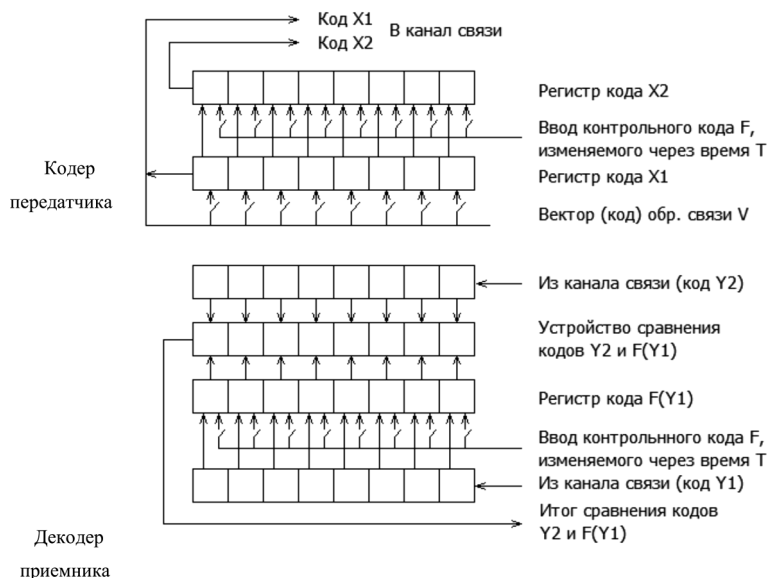
В 2015 году автором настоящей статьи модель системы скрытой передачи информации (ССПИ) была существенно модернизирована и допол-

нительно исследована. В рассматриваемом варианте системы по каналам связи передаются лишь адреса ячеек памяти аппаратуры абонентов системы связи для формирования в их компьютерах текста полученной информации. Поэтому для взломщиков каналов связи эта информация оказывается недоступной. Полученные результаты излагаются в предлагаемой публикации.

Структура модернизированной модели

Программа моделирования системы скрытой передачи информации работает в двух режимах – в режиме однократного запроса связи передающей станцией или абонентом с одним или с несколькими другими абонентами моделируемой системы и в режиме 10000 непрерывных запросов связи для получения статистических данных о правильности передачи информации по каналам связи с задаваемой интенсивностью помех, искажающих эту информацию. Предполагается, что в составе ССПИ работает несколько абонентов, число которых задаётся оператором передающей станции. Оператор может также устанавливать размер порций полезной информации, предназначенной для абонентов.

Важной особенностью нового варианта системы является то, что по каналу связи передаются только адреса X фрагментов сообщаемой информации, а тексты этой информации образуются в компьютерах абонентов с помощью адресов X . Поэтому перехват передаваемой информации хакерами исключен.



Структура программы обработки передаваемой и принимаемой информации модели передающей станции системы ССПИ

Поясним работу модели узла настройки синхронизации ССПИ, имитирующей работу командной станции (рисунок). В канал связи она посылает указанные 16-разрядные коды X , состоящие из двух 8-разрядных частей: $X1$ и $X2$. Коды $X2$ образуются из кодов $X1$ с помощью преобразования F , установленного на текущий интервал времени во всех станциях ССПИ (поразрядное сложение по модулю 2 кодов $X1$ и F). Так как в канале связи эти коды и коды ответов на запросы могут быть искажены помехами, то в общем случае они принимаются как некоторые коды $Y1$ и $Y2$. Однако выполняемое преобразование F кода $Y1$ позволяет с высокой вероятностью определить верно ли, что $Y1 = X1$ и $Y2 = X2$. В случае несовпадения указанных кодов можно повторить запрос.

Представленная на рисунке структура программы обработки передаваемой и принимаемой информации модели передающей станции требует для её реализации около 200 Кб памяти. Аналогично могут быть реализованы программы первичной обработки принимаемой и передаваемой информации компьютеров абонентов рекомендуемой системы.

Заключение

Проверка работоспособности предлагаемого варианта построения системы связи в сети интернет показала, что реализующая её программа правильно реализует получение абонентами информации без передачи её текста по каналу связи.

Список литературы

1. Жгун Т.В., Кирьянов Б.Ф. Модель скрытой передачи цифровой информации // Вестник Новгородского госуд. ун-та, Сер. Математика и информатика, 2002, № 22, С. 50-53.
2. Жгун А.А., Кирьянов Б.Ф. Оценка вероятности синхронизации в модели скрытой передаче информации // Вестник Казанского ГТТУ им. А.Н. Туполева. Сер. Информатика и вычислительная техника, 2009, с. 78-81.
3. Жгун А.А., Жгун Т.В., Осадчий А.И. Исследование синхронизации приема и передачи в стеганографической системе // Научно-технич. ведомости СПбГПУ. Сер. Информатика. Телекоммуникации. Управление. 2010, № 2, с. 7-11.
4. Жгун А.А. Исследование ложной синхронизации приема и передачи информации в модели скрытой передачи информации // Вестник НовГУ. Сер. Технич. Науки, 2010, № 6, с. 33-35.
5. Кирьянов Б.Ф. Микро-ЭВМ как средство имитации и обработки случайных процессов в радиоэлектронных системах: Монография // Новгородский политехнический ин-т, 1986, 213 с. (Деп. В ВИНТИ 10.11.1986. Num 7646-B86).
6. Кирьянов Б.Ф., Кирьянов Д.В. Модель системы обмена конфиденциальной информацией по каналам связи // Обзорение прикладной и промышленной математики, Т. 18. Вып. 5. 2011.
7. Кирьянов Б.Ф., Кирьянов Д.В. Система связи с высоконадёжной защитой информации в каналах её передачи // Информационные технологии и их приложения. Казань: КГТУ им А.Н. Туполева. 2011, С. 207 – 211.
8. Кирьянов Б.Ф. Надёжная защита информации в каналах связи // Обзорение прикладной и промышленной математики. Том 20 (2013), Вып. 4. С. 551 -552.
9. Кирьянов Б.Ф., Кирьянов Д.В. К проблеме защиты информации в каналах связи // Современные проблемы науки и образования. – 2012. – № 6.; URL: <http://science-education.ru/ru/article/view?id=7455>.
10. Кирьянов Б.Ф., Кирьянов Д.В. Обеспечение защиты информации в каналах связи // Международный журнал прикладных и фундаментальных исследований. 2012, № 11, С. 10-12.
11. Kiryanov B.F., Kiryanov D.V. The model of a communication system guaranteeing almost zero probability of receiving by hackers of codes of the transmitted data at breaking of a communication channel is offered and investigated // INTERNATIONAL JOURNAL OF APPLIED AND FUNDAMENTAL RESEARCH // Germany. Neu-Isenburg. Publishing-house «Academy of Natural History». Num 1, 2014. 2 p.