Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

МОДЕЛИРОВАНИЕ УСТРОЙСТВА ИМИТОЗАЩИТЫ КОНТРОЛИРУЕМЫХ ОБЪЕКТОВ С ПОВЫШЕННОЙ СТРУКТУРНОЙ СКРЫТНОСТЬЮ СИГНАЛОВ-ПЕРЕНОСЧИКОВ

А.П. ЖУК, А.А. ГАВРИШЕВ

ФГАОУ ВО «Северо-Кавказский федеральный университет»

Одним из методов защиты от несанкционированного доступа (НСД) информации, передаваемой по беспроводным каналам связи, является использование хаотических сигналов (ХС). Широкополосность, сложность структуры ХС и сильная чувствительность к начальным условиям обуславливают перспективность их использования в системах связи для повышения защищенности от НСД [1]. Это подтверждает актуальность задачи исследования свойств и характеристик систем связи с ХС.

Одной из таких систем связи с ХС является устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков (далее – УИКО), предназначенное для защищенного информационного обмена в беспроводных системах безопасности, в частности в охранно-пожарных системах [2], а также, в модифицированном виде, для защищенного управления по беспроводному каналу связи робототехническим комплексом [3].

Структурная схема приемо-передающей части УИКО приведена на рис. 1. На рис. 1 введены следующие обозначения: 1 – источник информации, 2 – накопитель хаотического сигнала, 3 – модулятор-передатчик, 4 – полосовой фильтр, 5 – усилитель, 6 – первый умножитель, 7 – второй умножитель, 8 – инвертор, 9 – накопитель копии хаотического сигнала, 10 – первый интегратор, 11 – второй интегратор, 12 – вычитающее устройство, 13 – решающее устройство, 14 – получатель информации.

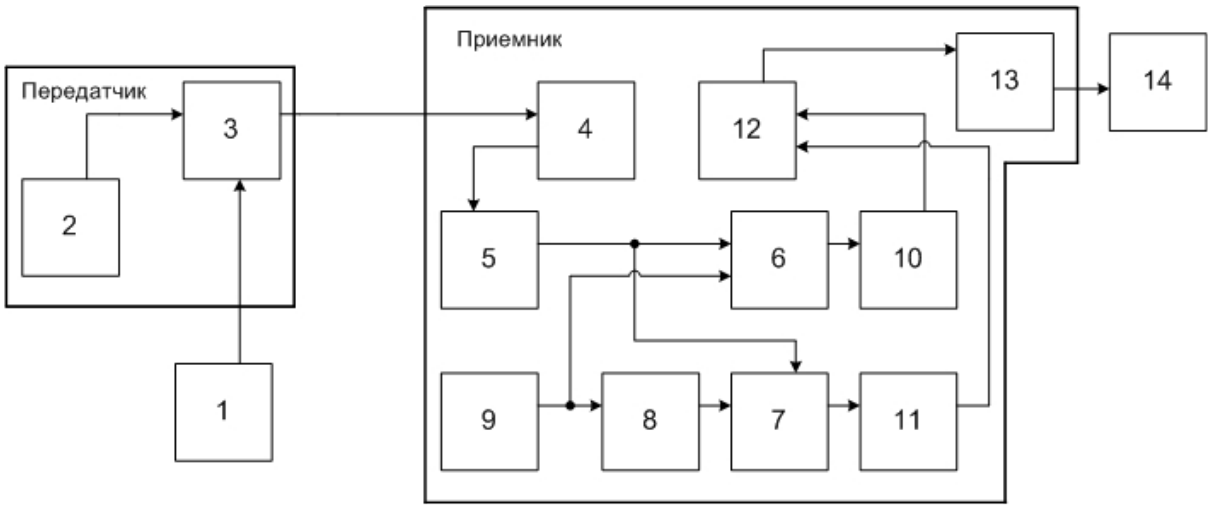

Рис. 1 – Структурная схема приемо-передающей части УИКО

Схема, изображенная на рис. 1, функционирует следующим образом [2]. Исходный информационный сигнал, представленный в виде прямоугольных импульсов из диапазона [-1; 1], перемножается в модуляторе-передатчике с хаотическими последовательностями (ХП). После этого полученные значения отправляются в линию связи. После этого сигнал последовательно проходит полосовой фильтр и усилитель. Далее, он перемножается в первом умножителе с аналогичными значениями ХП, а во втором умножителе – так же с аналогичными, но инвертированными значениями ХП. Далее полученные значения проходят через интеграторы и вычитающее устройство. По положительному или отрицательному значению сигнала определяется, какое значение пришло -1 или 1.

В качестве генератора ХС возьмем распространенный аттрактор Рёсслера, который описывается следующей системой нелинейных дифференциальных уравнений:

$$\frac{dx}{dt} = -y - z$$

$$\frac{dy}{dt} = x + ay$$

$$\frac{dz}{dt} = b + z(x - c)$$

где a, b, c – это положительные постоянные.

Проведем моделирование процессов, происходящих в схеме (рис. 1), с помощью пакета программ ScicosLab и приложения Modnum Toolbox. Причем, в качестве источника информации возьмем генератор равномерных прямоугольных импульсов, вырабатывающий значения [-1; 1]. На рис. 2, 3 представлены фрагменты зашифрованных информационных сигналов [4].

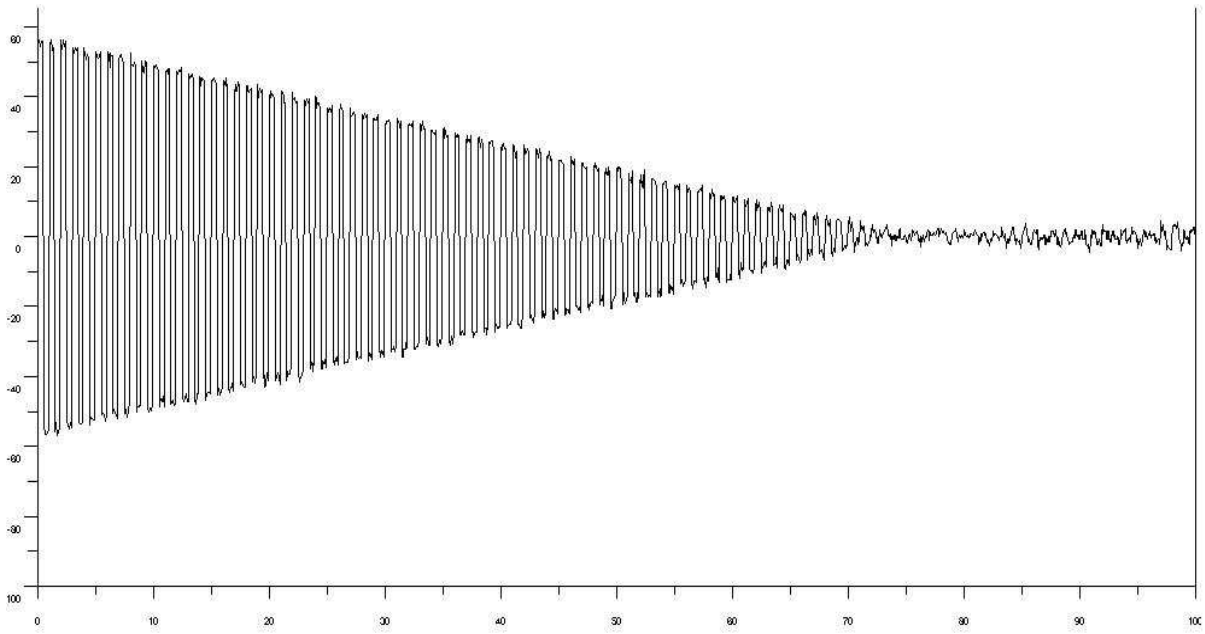

Рис. 2 – Фрагмент зашифрованного информационного сигнала, поступающего в линию связи при значениях ХС a = 0,1; b = 0,1; c = 4

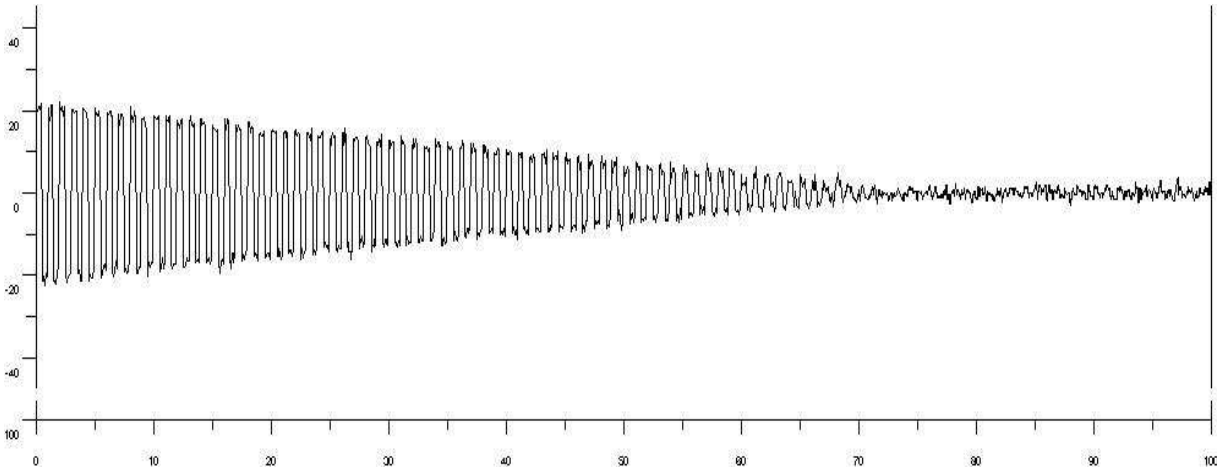

Рис. 3 – Фрагмент зашифрованного информационного сигнала,
поступающего в линию связи при значениях ХС a = 0,1; b = 0,1; c = 13

Как видно из рис. 2-3, поступающие в линию связи сигналы имеют шумоподобный вид, и из них визуально трудно выделить информационный сигнал. Это можно трактовать как подтверждение защищенности от НСД со стороны третьих лиц [4].

Далее, рассмотрим сигналы, которые были восстановлены на приемной стороне (рис. 4). Для упрощения процесса понимания функционирования приемо-передающей части УИКО, расположим вместе с восстановленными сигналами так же исходную информационную последовательность. Таким образом, на рис. 4 изображены графики следующих сигналов: а) фрагмент исходного информационного сигнала; б) фрагмент восстановленного сигнала при значениях ХС a = 0,1; b = 0,1; c = 4; в) фрагмент восстановленного сигнала при значениях ХС a = 0,1; b = 0,1; c = 13.

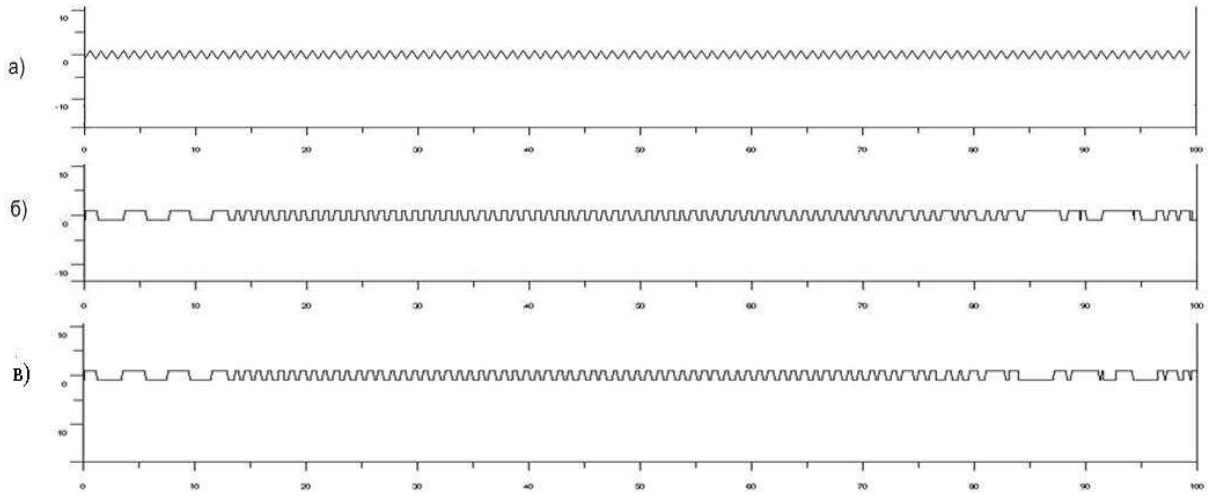

Рис. 4 – Графики исходного (4а) и восстановленных сигналов (4б-4в)

Как видно из представленных графиков, фрагменты восстановленных сигналов (рис. 4*б*, 4*в*) имеют достаточно похожий вид с исходным информационным сигналом (рис. 4*а*). Данный факт можно трактовать как подтверждение возможности практического использования УИКО при изменениях параметров хаотического сигнала [4].

Таким образом, моделирование показывает, что приемо-передающая часть УИКО в целом позволяет решить задачу по зашифровке и восстановлению информационных

сигналов для целей защищенного информационного обмена [4]. Среди основных недостатков представленной модели следует отметить необходимость наличия точной синхронизации между передающей и приемной сторонами, так же как это требуется для современных систем передачи информации [4].

Одной из особенностей описываемой схемы приемо-передающей части УИКО является возможность использования широкого класса ХС, записанных в перезаписываемые накопители хаотических последовательностей. Данный факт позволяет значительно повысить защищенность радиоканала от комплексных угроз (просмотр, подмена, перехват, радиоэлектронное подавление).

Список литературы

1. Иванюк П.В., Политанский Л.Ф., Политанский Р.Л., Элияшив О.М. Хаотическое маскирование информационных сигналов с использованием генератора на базе системы Лю // Технология и конструирование в электронной аппаратуре. 2012. № 3. С. 11-17.

2. Осипов Д.Л., Жук А.П., Гавришев А.А. Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Патент РФ № 2560824. 2015. Бюл. № 23. 15 с.

3. Жук А.П., Гавришев А.А., Осипов Д.Л. К вопросу о разработке защищенного устройства управления робототехническим комплексом посредством беспроводного канала связи // T-Comm: Телекоммуникации и транспорт. 2016. Т.10. № 12. С. 4-9.

4. Гавришев А.А., Жук А.П. Моделирование устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Прикладная информатика. 2017. Т. 12. № 1(67). С. 68-78.

ПЕРСПЕКТИВЫ РАЗВИТИЯ БЕЛОРУССКОЙ ЭЛЕКТРОННОЙ КАРТЫ

В.В. КОЗЛОВСКИЙ

ООО «Лайт Вел Организейшн»

Мировой опыт свидетельствует о широком использовании различных современных технологий оказания электронных услуг с помощью интегрированных систем на основе внедрения разного рода многофункциональных электронных карточек, включающих несколько приложений: идентификационное (идентификация личности, замена паспорта), электронно-цифровая подпись, платежное (банковская карточка для расчета за товары и услуги или снятия наличных), транспортное (для оплаты проезда), получение льгот и скидок и другие.

В настоящее время в Республике Беларусь отсутствует единая система, которая бы носила ярко выраженный интеграционный характер и обеспечивала бы работу множества разнородных государственных информационных систем с использованием единой электронной карточки. Например, отсутствует единая система идентификации и аутентификации пользователей при взаимодействии с государственными информационными ресурсами, а также не созданы инфраструктуры открытых ключей, функционирующие в рамках Государственной системы управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и обеспечивающие использование сертификатов открытых ключей пользователей.

Разработка основ создания Белорусской интегрированной сервисно-расчетной системы (БИСРС) проводится в соответствии с Указом Президента Республики Беларусь от 08.11.2011 № 515 «О некоторых вопросах развития информационного общества в Рес-