УДК 004.056

Обобщённый алгоритм защищённого информационного обмена

А. А. Гавришев, А. П. Жук

В данной статье авторами обобщаются в виде алгоритма известные технологии защищённого информационного обмена в беспроводных системах безопасности, основанные на перезаписываемых накопителях хаотических последовательностей. Разработанный алгоритм может найти применение в различных областях беспроводных систем безопасности, в которых требуется защита передаваемых по радиоканалу тревожных и служебных сообщений от несанкционированного доступа.

Ключевые слова: алгоритм, системы безопасности, радиоканал, хаотические сигналы, защищённость, информационный обмен.

1. Введение

Защита от несанкционированного доступа (НСД) тревожных и служебных сообщений в системах безопасности при их передаче по беспроводному каналу связи является актуальной задачей. Основными методами защиты информационного обмена при этом выступают криптографические методы и технологии на основе шумоподобных сигналов (ШПС) [1, 2]. Развитие технологий защиты радиоканала систем безопасности на основе ШПС представляет значительный интерес [1, 2].

Перспективной технологией повышения защищённости информационного обмена на основе ШПС является использование хаотических сигналов (ХС) [2, 3]. Их использование в защищённой радиосвязи позволяет добиться повышенной защищённости от НСД за счёт повышенной структурной и информационной скрытности по сравнению с другими видами ШПС [4].

Также по отношению к любым видам ШПС должны применяться общие правила, которые позволяют сделать передачу информации с их помощью более защищённой [5]: необходимо обладать максимальным уровнем априорной неопределённости используемых параметров сигналов; необходимо обладать большим числом сигнальных конструкций.

По отношению к ХС такой технологией, обеспечивающей обладание достаточно большим количеством сигналов и их периодической сменой, может стать использование перезаписываемых накопителей хаотических последовательностей [6–8].

На рис. 1 приведена структурная схема приёмо-передающей системы, основанной на использовании перезаписываемых накопителей хаотических последовательностей [9].

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.

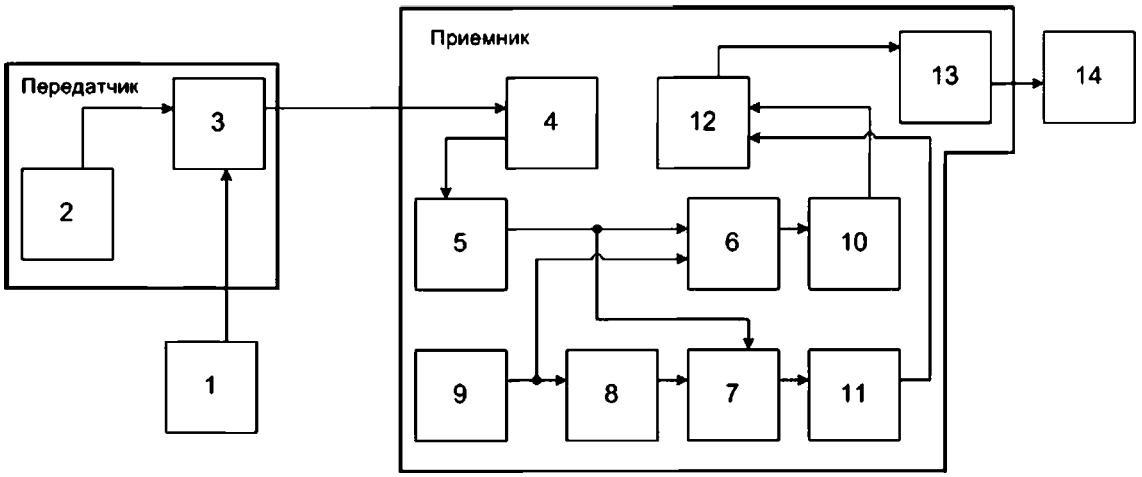

Рис. 1. Структурная схема приёмо-передающей системы, основанной на использовании перезаписываемых накопителей хаотических последовательностей

Рассмотрим, как функционирует система, представленная на рис. 1. При вхождении в синхронизм передающей и приёмной сторон на передающей стороне от источника информации информационный сигнал, находящийся в диапазоне [-1; 1], поступает в модулятор-передатчик, куда также поступает ХС с накопителя ХС. В модуляторе-передатчике осуществляется перемножение информационного сигнала с ХС. С выхода модулятора-передатчика сформированный сигнал поступает в канал связи. Затем сигнал поступает последовательно в полосовой фильтр, усилитель и умножители. На другие входы умножителей одновременно с этим с накопителя копии ХС поступают копии ХС, идентичные ХС передающей стороны, причём на второй умножитель копия ХС поступает через инвертор. Далее с выходов умножителей сигналы через интеграторы подаются на вычитающее устройство. С выхода вычитающего устройства разностный сигнал поступает на решающее устройство, в котором происходит сравнение принятых уровней с пороговым значением напряжения. С выхода решающего устройства информация поступает к получателю информации [8].

В настоящее время по отношению к беспроводным системам безопасности известно несколько приложений приёмо-передающей системы, изображенной на рис. 1. Рассмотрим их далее более подробно и попытаемся их обобщить.

Целью данной статьи является обобщение в виде алгоритма известных технологий защищённого информационного обмена в беспроводных системах безопасности.

2. Основная часть

На рис. 2 приведена структурная схема устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков [10]. Данная технология предназначена для защиты информационного обмена между блоком контроля и оконечными датчиками в охранно-пожарных системах за счет использования перезаписываемых накопителей хаотических последовательностей [6]. Концептуально данное устройство имитозащиты состоит из блока контроля, включающего в себя генератор первой псевдослучайной последовательности (ПСП-1), генератор второй псевдослучайной последовательности (ПСП-2), накопитель хаотической последовательности (НХП), накопитель копии хаотической последовательности (НКХП), устройство сравнения (УС), и контролируемого объекта (датчика), включающего в себя генератор ПСП-2, НХП, НКХП [10].

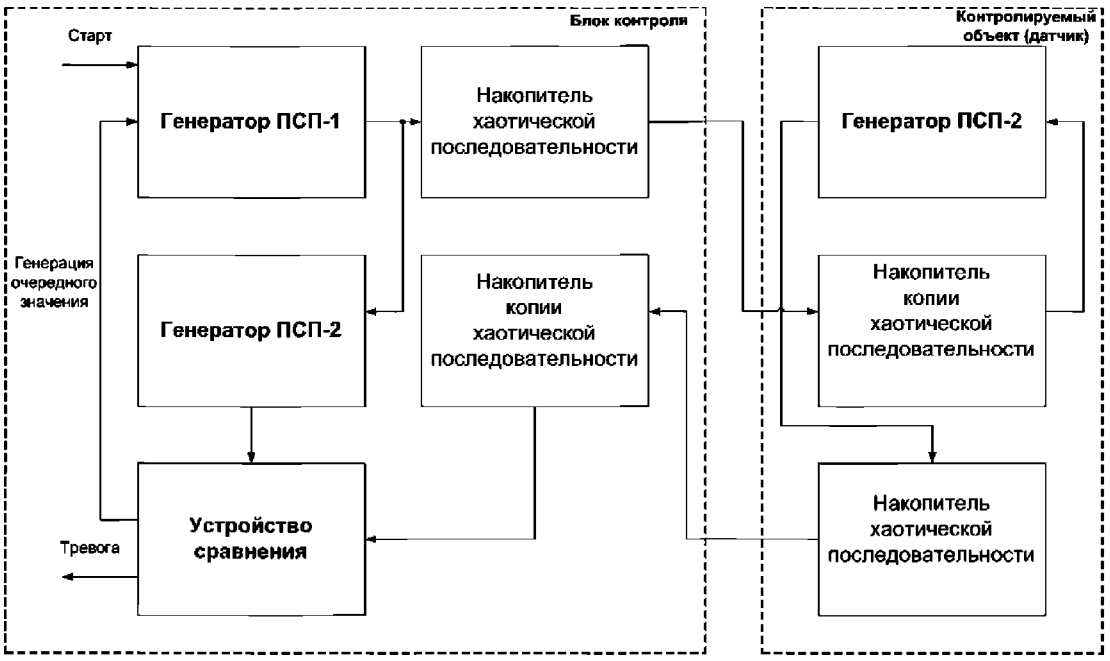

Рис. 2. Структурная схема устройства имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков

Рассматриваемое устройство имитозащиты контролируемых объектов функционирует следующим образом. Для запуска блока контроля на вход генератора ПСП-1 подаётся стартовая команда. Затем генератор ПСП-1 вырабатывает первую ПСП. Полученное значение отправляется на генератор ПСП-2 блока контроля и одновременно с этим в НХП перемножается с ХС и, после вхождения в режим синхронизации, через линию связи передается на контролируемый объект (датчик). После этого в НКХП происходит декодирование полученного сигнала с помощью копии ХС, идентичной ХС в блоке контроля, и далее декодированный сигнал в виде последовательности поступает в генератор ПСП-2, функция генерации последовательности которого идентична функции генератора ПСП-2 блока контроля. Затем в НХП происходит перемножение последовательности ПСП-2 контролируемого объекта (датчика) с ХС и, после вхождения в режим синхронизации, через линию связи передаётся на блок контроля. Далее в НКХП происходит декодирование полученного сигнала с помощью копии ХС, идентичной ХС в контролируемом объекте (датчике), и после чего декодированный сигнал в виде последовательности поступает на УС, в котором проверяется отклик ранее пришедшего значения генератора ПСП-2 блока контроля и отклик генератора ПСП-2 контролируемого объекта (датчика). В случае совпадения значений, пришедших от контролируемого объекта (датчика) и блока контроля, вырабатывается сигнал «Норма», который служит для генерации следующего псевдослучайного числа генератором ПСП-1. При несовпадении значений устройство сравнения выдает команду «Тревога».

Также в работе [3] рассмотрена схема защищённой беспроводной системы управления роботом (рис. 3), основанная на перезаписываемых накопителях хаотической последовательности [6].

Устройство состоит из сервера, в состав которого входят система управления (СУ), НКХП, генератор ПСП-1, НХП, генератор ПСП-2, УС, приёмо-передающее устройство (ППУ), и робота, в состав которого входят НКХП, ППУ, НХП, электропривод, генератор ПСП-2, актуаторы, блок формирования сигналов управления, сенсоры [3].

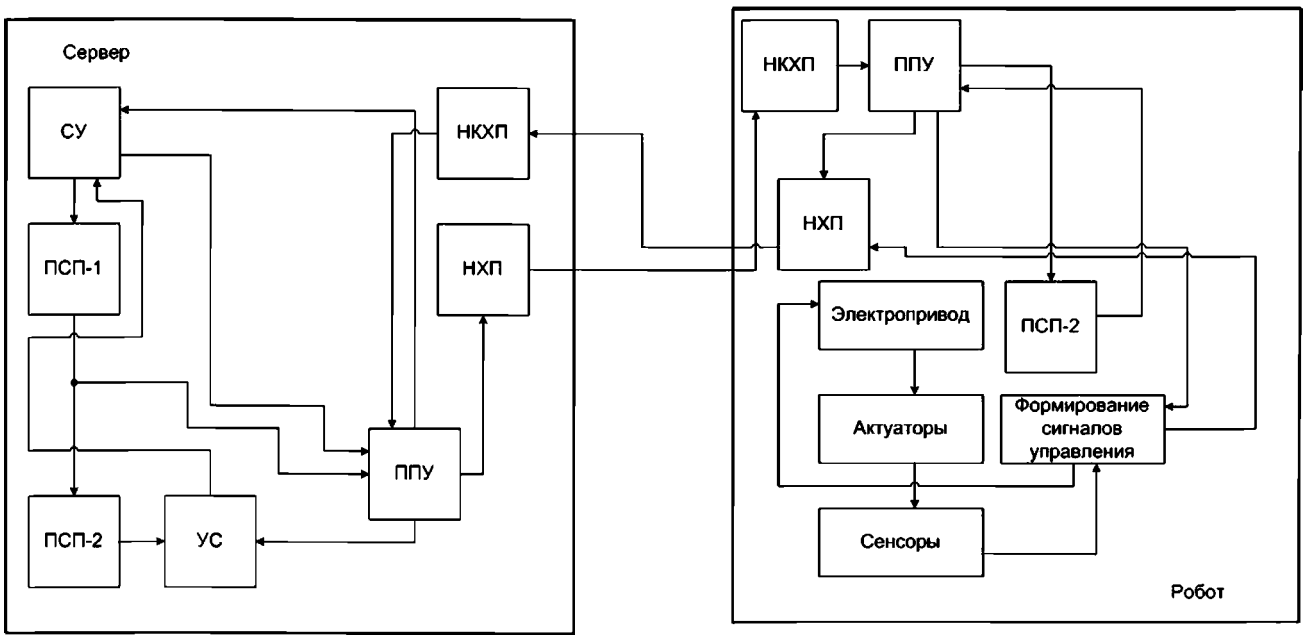

Рис. 3. Структурная схема защищённого устройства управления роботом

Функционирование беспроводной системы управления роботом осуществляется в проверочном и рабочем режимах [3]. Вначале СУ дает команду генератору ПСП-1 на генерацию первого значения ПСП-1. После этого первое значение ПСП-1 через ППУ поступает в НХП, где перемножается с ХС и, после вхождения в режим синхронизации, отправляется роботу. Робот производит декодирование переданного сообщения с помощью НКХП. После этого робот вырабатывает своё значение ПСП-2 от генератора ПСП-2 с помощью декодированного значения ПСП-1 сервера и отправляет его в ППУ. Сформированный пакет, состоящий из значения ПСП-2, отправляется в НХП, где перемножается с ХС и отправляется на сервер. На сервере после вхождения в режим синхронизации принятое сообщение проходит декодирование с помощью НКХП. Декодированные пакеты поступают в ППУ. ППУ передаёт в УС значение ПСП-2, выработанное роботом. В УС сервера происходит сравнение значений ПСП-2 сервера и ПСП-2 робота. В случае верного сравнения СУ переходит в рабочий режим управления роботом. В случае неверного сравнения выдаётся сигнал тревоги, сигнализирующий о компрометации проверяемого робота. Рабочий режим управления состоит в следующем [3]. СУ осуществляет управление роботом через ППУ, добавляя в команды управления имитовставку, состоящую из значения ПСП-1. При обработке входных команд робот отделяет от команд управления имитовставку и вычисляет значение ПСП-2, которое добавляется в команды, посылаемые роботом обратно на сервер. Сервер, как и при проверочном режиме работы, периодически проверяет истинность значения ПСП-2 робота для предотвращения несанкционированного доступа к командам управления.

Так как в описанных выше устройствах используются перезаписываемые накопители хаотических последовательностей [3, 6] и в целом логика их работы схожа, то в обобщённом виде алгоритм защищённого информационного обмена в беспроводных системах безопасности можно представить, как показано ниже:

1. Инициализация генератора ПСП-1 управляющего блока.
2. Выработка первого псевдослучайного числа генератором ПСП-1 управляющего блока.
3. Отправка полученного значения одновременно на генератор ПСП-2 управляющего блока и в НХП.
4. Передача произведения ПСП-1 и ХС из НХП на контролируемый объект.
5. Декодирование в контролируемом объекте полученного сигнала с помощью НКХП, идентичного НХП в управляющем блоке.

6. Поступление декодированного сигнала в виде последовательности в генератор ПСП-2 контролируемого объекта, функция генерации последовательности которого идентична функции генератора ПСП-2 управляющего блока.

7. Передача произведения выработанной последовательности ПСП-2 контролируемого объекта с ХС из НХП на управляющий блок.

8. Декодирование в управляющем блоке полученного сигнала с помощью НКХП, идентичного НХП в контролируемом объекте.

9. Поступление декодированного сигнала в виде ПСП-2 контролируемого объекта в УС.

10. Выработка ПСП-2 управляющего блока и ее поступление в УС.

11. Сравнение ПСП-2 управляющего блока и ПСП-2 контролируемого объекта.

12. Если сравнение верно, то отображение сигнала «Норма» и переход к п. 1 алгоритма.

13. Если сравнение неверно, то отображение сигнала «Тревога» и переход к п. 14 алгоритма.

14. Вмешательство в работу беспроводной системы безопасности ответственных лиц.

На рис. 4 описанный алгоритм приведен в графическом виде.

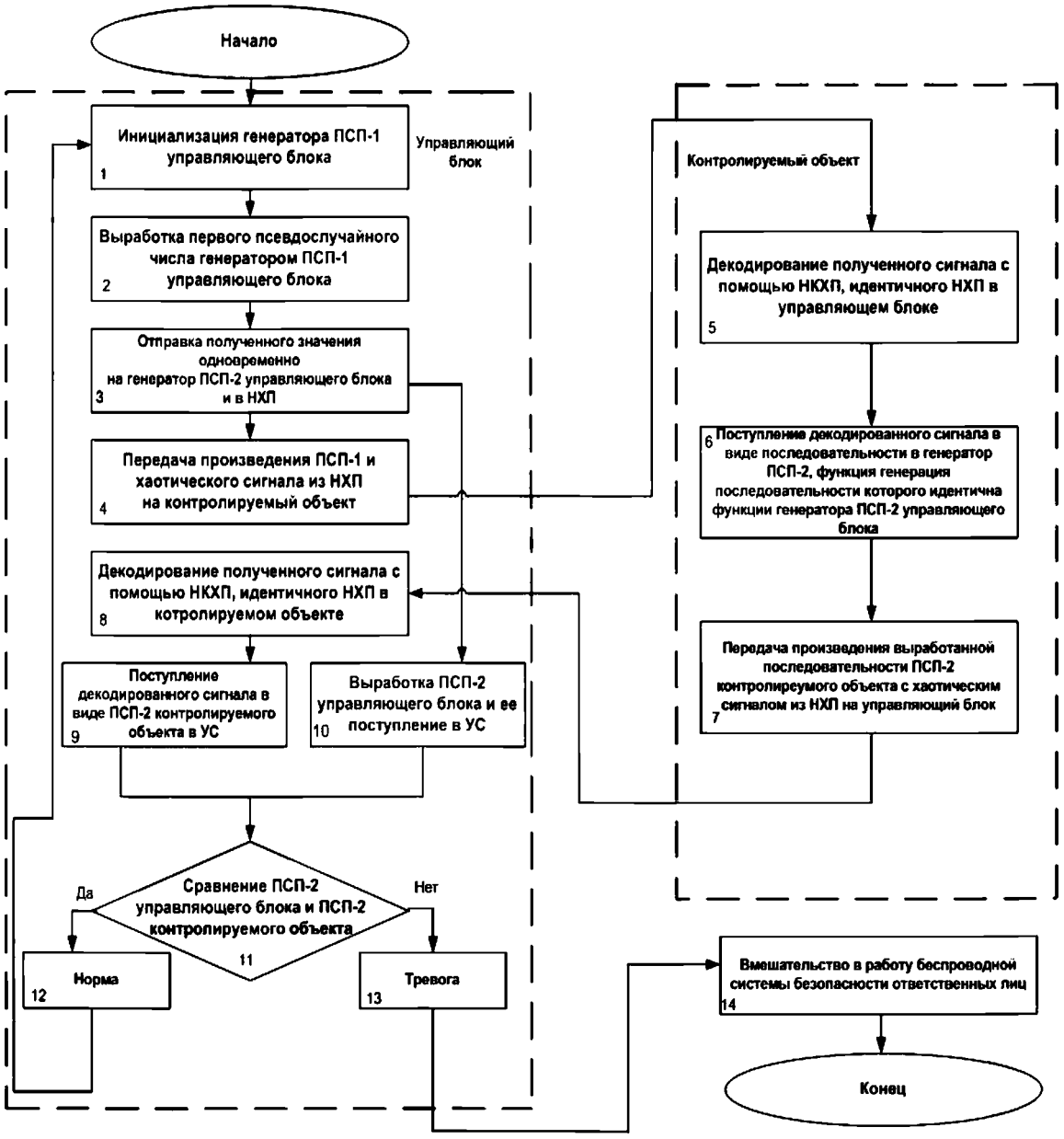

Рис. 4. Обобщенный алгоритм защищённого информационного обмена

Как видно из рис. 4, обобщённый алгоритм защищённого информационного обмена в общих чертах повторяет рис. 2–3. Таким образом, описание функционирования данных устройств также поясняет основные положения функционирования обобщённого алгоритма защищённого информационного обмена. При этом на рис. 4 приведён обобщённый вид алгоритма, то есть его возможно использовать также и в других беспроводных системах безопасности, где существует необходимость защищённого информационного обмена между несколькими объектами.

Интерес представляет краткое рассмотрение случая несанкционированного доступа к «зашифрованному» сигналу противоборствующей стороной. Как видно из описаний, приведённых выше, в НХП и НКХП потенциально возможно записать бесконечное число разнообразных реализаций ХС, отвечающих определённым требованиям для защищённых систем связи, а также периодически их перезаписывать. Поэтому, например, использование простейшего энергетического приёмника не позволит восстановить исходный сигнал, так как не будет виден переход от -1 к 1 и обратно, поскольку неизвестна копия, записанная на носитель информации. Таким образом, энергетический приёмник и в случае 1, и в случае -1 даст решение о 1, а нарушить информационную скрытность невозможно без наличия копии хаотического сигнала-переносчика [8]. Также потенциально перезаписываемые НХП могут снизить вероятность несанкционированного доступа к передаваемым сигналам с помощью BDS-статистики. В данный момент BDS-статистика находит активное применение для раскрытия информации о ХС [11].

Кроме того, использование в управляющем блоке и контролируемом объекте одинаковых генераторов ПСП-2, инициализация которых осуществляется периодически изменяющимся псевдослучайным числом, вырабатываемым генератором ПСП-1 управляющего блока, позволяет повысить защищённость от НСД передаваемых команд за счёт её использования в качестве имитовставки, а также в качестве проверки подлинности непосредственно контролируемых объектов.

В подтверждение данных тезисов в работах [2] и [3] на основе аппарата нечёткой логики на примере охранно-пожарных систем и специальной робототехники произведена оценка защищённости различных технологий защиты радиоканала. Данная оценка показала преимущество описываемого подхода, основанного на использовании перезаписываемых накопителей хаотических последовательностей, по критерию защищённости от комплексных угроз (просмотр, подмена, перехват, радиоэлектронное подавление) по сравнению с известными технологиями защиты радиоканала, применяемыми в данных областях.

3. Заключение

Таким образом, в данной работе на основе обобщения известных подходов обеспечения защищённого информационного обмена разработан обобщённый алгоритм защищённого информационного обмена в беспроводных системах безопасности. В основу данного алгоритма положено использование перезаписываемых накопителей хаотических последовательностей, а также использование одинаковых генераторов ПСП-2, инициализация которых осуществляется периодически изменяющимся псевдослучайным числом, вырабатываемым генератором ПСП-1.

Среди основных преимуществ данного подхода следует выделить повышенную защищённость от НСД [2, 3], среди недостатков – необходимость наличия точной синхронизации между передающей и приёмной сторонами [7]. Однако использование перезаписываемых накопителей хаотических последовательностей, содержащих одинаковые копии ХС на передающей и приёмной сторонах [6–8], позволяет упростить задачу обеспечения точной синхронизации между передающей и приёмной сторонами за счёт уменьшения времени извлечения ХС из блоков памяти по сравнению с их вычислением [7].

Литература

1. *Брауде-Золотарёв Ю.* Алгоритмы безопасности радиоканалов // Алгоритм безопасности. 2013. № 1. С. 64–66.
2. *Гавришев А. А., Жук А. П., Осипов Д. Л.* Анализ технологий защиты радиоканала охранно-пожарных сигнализаций от несанкционированного доступа // Труды СПИИРАН. 2016. Вып. 4 (47). С. 28–45.
3. *Жук А. П., Гавришев А. А., Осипов Д. Л.* К вопросу о разработке защищённого устройства управления робототехническим комплексом посредством беспроводного канала связи // T-Comm: Телекоммуникации и транспорт. 2016. Т. 10, № 12. С. 4–9.
4. *Сиващенко С. И.* Скрытность радиосистем со сложными и хаотическими сигналами // Системи управління, навігації та зв'язку. 2009. № 3 (11). С. 56–58.
5. *Горохов С. М., Захарченко Н. В., Корчинский В. В.* Критерии эффективности скрытых методов передачи // Цифрові технології. 2012. № 12. С. 147–150.
6. *Осипов Д. Л., Жук А. П., Гавришев А. А.* Устройство имитозащиты контролируемых объектов с повышенной структурной скрытностью сигналов-переносчиков // Патент РФ № 2560824. 2015. 15 с.
7. *Мохсени Т. И., Кикот А. М.* Когерентная передача цифровой информации с двоичной модуляцией хаотического импульса // Журнал радиоэлектроники. 2015. № 6. 24 с.
8. *Баркетов С. В., Жук А. П., Сазонов В. В., Авдеенко С. И., Жук Е. П., Лохов В. И., Голубь Ю. С.* Когерентная система передачи информации хаотическими сигналами // Патент РФ № 2326500. 2008. 6 с.
9. *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
10. *Жук А. П., Гавришев А. А.* Альтернативный подход повышения структурной скрытности сигналов-переносчиков устройства имитозащиты контролируемых объектов // Спецтехника и связь. 2015. № 2. С. 59–63.
11. *Васюта К. С., Озеров С. В., Королюк А. Н., Комин Д. С.* Оценка скрытности функционирования радиотехнических систем передачи информации военного назначения при помощи BDS-статистики // Системи озброєння і військова техніка. 2014. № 2 (38). С. 67–69.

Статья поступила в редакцию 12.09.2017.

Гавришев Алексей Андреевич
аспирант кафедры организации и технологии защиты информации СКФУ (355009, Ставрополь, ул. Пушкина, 1), тел. (8652) 95-68-08, e-mail: alexxx.2008@inbox.ru.

Жук Александр Павлович
к.т.н., профессор, профессор кафедры организации и технологии защиты информации СКФУ, тел. (8652) 95-68-08.

Generalized algorithm of secure information exchange

A. Gavrishev, A. Zhuk

In this article, the authors summarized known technologies in the form of algorithm for secure information exchange in wireless security systems, based on re-writable drives of chaotic sequences. The developed algorithm can find application in various areas of wireless security systems that require protection of the transmitted radio alarming and service messages from unauthorized access.

Keywords: algorithm, security systems, radio channel, chaotic signals, protection, information exchange.