Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

УДК 004.056:061.068

МУЛЯРЧИК
Константин Сергеевич

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации,
информационная безопасность

Минск 2013

Работа выполнена в Белорусском государственном университете.

	Сидоренко Алевтина Васильевна, доктор технических наук, доцент, профессор кафедры физики и аэрокосмических технологий Белорусского государственного университета
Официальные оппоненты:	**Чердынцев Валерий Аркадьевич**, доктор технических наук, профессор, профессор кафедры радиоприемных устройств учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
	Комликов Дмитрий Александрович, кандидат технических наук, начальник отдела государственного предприятия «Научно-исследовательский институт технической защиты информации»
Оппонирующая организация	Учреждение образования «Военная академия Республики Беларусь»

Защита состоится « 23 » января 2014 года в 14.00 на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1, ауд. 232, тел. 293-89-89, e-mail: dissovet@bsuir.by.

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

КРАТКОЕ ВВЕДЕНИЕ

Одной из устойчивых тенденций развития технических средств информатизации является их миниатюризация и мобильность. В частности, в последнее время широкое распространение получили беспроводные сенсорные сети, которые активно используются для решения задач мониторинга и управления. Эти сети являются распределенными и самоорганизующимися и состоят из множества миниатюрных узлов (сенсоров). Основным требованием, предъявляемым к узлам такой сети, является длительное время их автономной работы, что приводит к использованию в них элементов с малыми вычислительными возможностями и режимов работы с низким энергопотреблением. Так, объем памяти микроконтроллера, используемого в таких устройствах, как правило, находится в пределах 1–4 Кбайт, а частота его работы составляет 8–20 МГц. В то же время широковещательная природа беспроводных сенсорных сетей делает их уязвимыми для пассивных атак, в частности, для перехвата данных, передаваемых по беспроводному каналу.

Существующие алгоритмы шифрования, такие как BelT (СТБ 34.101.31-2007), AES, ГОСТ 28147-89, обладая известными достоинствами, неудобны для реализации в беспроводных сенсорных сетях, так как в узлах таких сетей отсутствует достаточный объем оперативной памяти микроконтроллеров, необходимый для функционирования алгоритма шифрования; длительность процесса шифрования оказывается достаточно высокой из-за низких вычислительных ресурсов системы; ограниченными являются коммуникационные возможности узлов сетей.

Одним из перспективных направлений является разработка алгоритмов шифрования с использованием динамического хаоса, что обусловлено высокой чувствительностью к начальным условиям, случайностью траекторий, высокой степенью рассеивания и запутывания систем на его основе. Среди систем шифрования на основе динамического хаоса выделяют дискретные (цифровые) системы шифрования, применяемые непосредственно в компьютерной технике. Алгоритмы, использующие динамический хаос, позволяют сократить требования к вычислительным ресурсам (быстродействие и объем оперативной памяти), необходимым для их реализации, по сравнению с упомянутыми выше традиционными алгоритмами.

В диссертационной работе решаются задачи разработки, исследования и аппаратно-программной реализации блочного симметричного алгоритма шифрования данных с использованием дискретных хаотических отображений, ориентированного на применение в беспроводных сенсорных сетях передачи данных.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Работа выполнялась в Белорусском государственном университете в период с 2011 по 2013 год в рамках научно-исследовательских работ:

1. «Исследование и разработка физико-математических принципов повышения криптостойкости и эффективности криптоалгоритмов на основе динамического хаоса» (НИР 470/15, БГУ, 2011–2013 гг.) в составе ГПНИ «Научные основы и инструментальные средства информационных и космических технологий» (шифр «Информатика и космос», 2011–2013 гг.).

2. «Исследование приемопередающих модулей для сверхширокополосных информационных систем и определение перспективных областей их применения» (НИР 15908/15, БГУ, 2012–2013 гг.).

Тема диссертационной работы соответствует следующим приоритетным направлениям научных исследований и научно-технической деятельности в Республике Беларусь.

1. Методы, средства и технологии обеспечения информационной безопасности при обработке, хранении и передаче данных с использованием криптографии, квантово-криптографические системы (п. 5.5 Постановления Совета Министров Республики Беларусь от 19 апреля 2010 г. № 585 «Об утверждении перечня приоритетных направлений научных исследований Республики Беларусь на 2011–2015 годы»).

2. Макротехнология «Производство средств связи, вычислительных средств и программного продукта; высокопроизводительные системы, технологии передачи и обработки информации», критические технологии: «обработка, передача, хранение и защита информации» (п. 34 Указа Президента Республики Беларусь от 22 июля 2010 г. № 378 «Об утверждении приоритетных направлений научно-технической деятельности в Республике Беларусь на 2011–2015 годы»).

Цель и задачи исследования

Целью диссертационной работы является разработка алгоритма шифрования на основе динамического хаоса и его аппаратно-программная реализация, ориентированная на применение в беспроводных сенсорных сетях.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Разработать алгоритм шифрования данных на основе динамического хаоса с использованием дискретных хаотических отображений для защиты информации в беспроводных сетях.

2. Разработать метод контроля хаотичности выходных последовательностей системы по параметрам корреляционной размерности и энтропии Колмогорова для осуществления минимизации числа раундов алгоритма шифрования в режиме динамического хаоса.

3. Обосновать выбор метода повышения эффективности и обеспечения стойкости алгоритма шифрования к атакам на основе дифференциального криптоанализа по показателям лавинного эффекта.

4. Разработать программные средства для мобильных систем передачи информации и осуществить аппаратно-программную реализацию разработанного алгоритма шифрования для защиты информации в беспроводных сетях на базе сверхширокополосных приемопередатчиков серии ППС-40А.

Объектом исследования являются средства защиты информации в беспроводных сетях передачи данных.

Предметом исследования являются процедуры и алгоритмы шифрования на основе динамического хаоса для беспроводных сенсорных сетей.

Положения, выносимые на защиту

1. Алгоритм шифрования данных, включающий разбиение обрабатываемого текста на последовательность блоков одинаковой длины, многократное раундовое преобразование, определение числа раундов и способа взаимосвязи блоков текста в выходной последовательности, отличающийся использованием сети Фейстеля, режима динамического хаоса, дискретного хаотического отображения, определением минимального числа раундов и режима работа блочных шифров: режима сцепления блоков либо режима обратной связи по шифртексту.

2. Метод контроля степени хаотичности выходных последовательностей алгоритма шифрования, заключающийся в автоматическом определении степени и направления изменения хаотичности и использующий в качестве критерия корреляционную размерность и энтропию Колмогорова, что в целом обеспечивает минимизацию числа раундов алгоритма шифрования в режиме динамического хаоса и повышает стойкость шифрования.

3. Способ определения эффективности алгоритма шифрования данных на основе динамического хаоса, отличающийся учетом управляющего параметра хаотического отображения при определении показателя лавинного эффекта, что подтверждает увеличение эффективности базового преобразования разработанного алгоритма до шести раз.

4. Аппаратно-программная реализация алгоритма шифрования с характеристиками: объем памяти для хранения программного кода 762 байта, объем памяти для хранения данных 241 байт, максимальная скорость обработки данных алгоритмом шифрования 88,2 Кбит/с при тактовой частоте микроконтроллера 20 МГц, основанная на использовании сверхширокополосных приемопередатчиков для обеспечения конфиденциальной передачи информации в беспроводных сетях.

Личный вклад соискателя

Содержание диссертационной работы отражает личный вклад автора. Основные научные и практические результаты работы, а также положения, выносимые на защиту, получены лично автором.

Определение целей и задач исследований, анализ методик проведения исследований, интерпретация и обобщение научных результатов проводились совместно с научным руководителем, д-м техн. наук, доц. А. В. Сидоренко. Соавтором опубликованных работ также является А. В. Сидоренко.

Апробация результатов диссертации

Основные научные положения и результаты диссертации докладывались и обсуждались на следующих научных конференциях и симпозиумах: XVI Annual seminar «Nonlinear dynamics and applications: fractals, chaos, phase transitions, self-organization» NPCS'2009 (Минск, 2009), VII Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (Минск, 2009), Международная конференция «Информационные системы и технологии» IST'2009 (Минск, 2009), VIII Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (Минск, 2010), 15th International School-Conference «Foundations & Advances in Nonlinear Science»: Nonlinear Dynamics and Application (Минск, 2010), XV Международный молодежный форум «Радиоэлектроника и молодежь в XXI веке» (Харьков, 2011), XI Научно-практическая конференция «Комплексная защита информации» (Гродно, 2011), Международный конгресс

по информатике «Информационные системы и технологии» CSiST'2011 (Минск, 2011), XIV Республиканская научно-методическая конференция молодых ученых (Брест, 2012), X Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (Минск, 2012), 16th International Conference-School Foundations «Advances in Nonlinear Science» (Минск, 2012), Международная научная конференция «Информационные технологии и системы» ИТС'2012 (Минск, 2012), VII Международная научно-техническая конференция «Средства медицинской электроники и новые медицинские технологии: Медэлектроника-2012» (Минск, 2012), XI Белорусско-российская научно-техническая конференция «Технические средства защиты информации» (Минск, 2013), 10th International Conference «Computer Data Analysis & Modeling 2013: Theoretical & Applied Stochastics» (Минск, 2013), Международный конгресс по информатике «Информационные системы и технологии» CSIST'2013 (Минск, 2013).

Опубликованность результатов диссертации

Основные результаты диссертации опубликованы в 25 научных работах. Из них 7 статей в научных рецензируемых журналах в соответствии с пунктом 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, 9 статей и 7 тезисов докладов в сборниках материалов научных конференций. Общее число страниц опубликованных материалов – 96 страниц (5,5 авторских листа).

По результатам диссертационной работы подана заявка на выдачу патента Республики Беларусь «Способ шифрования данных на основе дискретных хаотических систем и отображений» (МПК H04L 9/00, G06F 13/0, № a 20121007, 06.07.2012).

Структура и объем диссертации

Диссертационная работа состоит из введения, общей характеристики работы, четырех глав, заключения, библиографического списка и шести приложений. Общий объем диссертации составляет 163 страницы, из них 96 страниц основного текста, 42 рисунка на 14 страницах, 17 таблиц на 5 страницах, библиографический список из 158 наименований на 13 страницах, список собственных публикаций автора из 25 наименований на 4 страницах, приложения на 31 странице.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Первая глава работы посвящена принципам разработки, криптоанализа и реализации алгоритмов шифрования; обзору традиционных алгоритмов и алгоритмов шифрования на основе динамического хаоса, а также выявлению существующих проблем в области защиты информации в беспроводных сенсорных сетях.

В работе рассматриваются основные принципы построения блочных симметричных алгоритмов шифрования, проведен анализ общих подходов к построению таких алгоритмов шифрования, предполагающих реализацию принципов рассеивания и запутывания, принципа Кирхгофа, а также выполнение ряда требований, обеспечивающих надежность и стойкость шифра. Проводится обзор существующих традиционных алгоритмов шифрования и алгоритмов шифрования с использованием динамического хаоса, на основании которого предложена их классификация по общности структурных схем и способу реализации хаотического поведения в алгоритме. Обоснован выбор блочного симметричного типа алгоритма шифрования как предпочтительного для использования в узлах беспроводной сенсорной сети.

Обсуждаются особенности разработки и применения алгоритмов шифрования для беспроводных сенсорных сетей. Основным отличием беспроводных сенсорных сетей от традиционных, таких как Wi-Fi, GSM, LTE, является использование миниатюрных приемопередатчиков с автономным источником питания и, как следствие, с ограниченными вычислительными и коммуникационными возможностями: средний размер пакета данных – 20–30 байт, тактовая частота микроконтроллера – до 30 МГц, а объем оперативной памяти в нем – до 4 Кбайт.

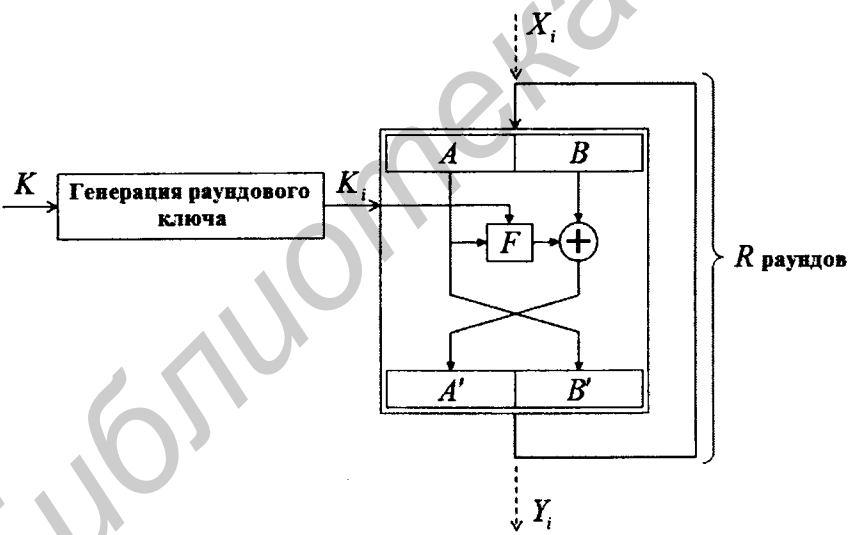
Показаны преимущества использования динамического хаоса, а именно дискретных хаотических отображений, при разработке алгоритмов шифрования, работающих в условиях ограниченных вычислительных ресурсов и коммуникационных возможностей. Установлено, что применение динамических хаотических систем с дискретными хаотическими отображениями позволит снизить потребности в вычислительных ресурсах. Будучи нелинейными, такие отображения являются хорошими кандидатами на применение вместо таблиц подстановки в алгоритмах шифрования, что значительно снизит объем оперативной памяти. Существенным является инвариантность математического выражения для вычисления хаотического отображения по отношению к множеству, на котором определены его аргументы. Это позволит использовать одну и ту же структуру отображения при реализации его вариантов в зависимости от доступных ресурсов и даст

возможность изменять длину блока в алгоритме шифрования, что будет способствовать повышению надежности и увеличению пропускной способности канала при передаче зашифрованной информации.

Таким образом, обоснована необходимость разработки алгоритма шифрования блочного симметричного типа на основе динамического хаоса; разработки метода для управления параметрами алгоритма шифрования и анализа его криптостойкости; определения способа анализа лавинного эффекта в разработанном алгоритме для определения эффективности шифрования и аппаратно-программной реализации алгоритма шифрования для защиты информации в беспроводных сетях.

Вторая глава работы посвящена разработке алгоритма шифрования, ориентированного на реализацию в условиях дефицита вычислительных ресурсов и ограниченной скорости передачи данных.

Описывается структурная схема разработанного блочного симметричного алгоритма шифрования на основе динамического хаоса (рисунок 1), в которой использованы итеративная схема Шеннона и в качестве базового преобразования – сеть Фейстеля.



X_i – блок открытого текста; A, B – входные подблоки сети Фейстеля; K – ключ шифрования; K_i – раундовый ключ; F – нелинейная функция; A', B' – выходные подблоки сети Фейстеля; Y_i – блок зашифрованного текста; R – количество раундов базового преобразования

Рисунок 1 – Структурная схема разработанного алгоритма шифрования

Принципиальным отличием разработанного алгоритма от известных, основанных на сети Фейстеля, является использование в качестве нелинейного блока F *дискретного хаотического отображения* – преобразования, заданного на конечном целочисленном множестве мощностью M, обладающего хаотической динамикой и управляемого параметром A:

$$F = F(A, M, X), \tag{1}$$

где X – входное значение отображения;

A – управляющий параметр отображения;

M – мощность множества, на котором определено отображение.

Использование дискретных хаотических отображений вместо таблиц подстановки в алгоритмах шифрования, позволяет: 1) уменьшить объем оперативной памяти, требуемый для реализации алгоритма шифрования; 2) варьировать мощность множества, на котором определено нелинейное преобразование (дискретное хаотическое отображение), что в целом способствует обеспечению надежности передаваемой информации в устройствах с ограниченными ресурсами.

Показано, что в разработанном алгоритме шифрования раундовый ключ определяет выбор конкретного вида нелинейного преобразования, а длина блока текста – мощность множества, на котором оно определено. В связи с этим для обеспечения надежности алгоритма шифрования используемое дискретное хаотическое отображение должно обладать схожими хаотическими свойствами при различных значениях управляющего параметра.

Установлены преимущества использования дискретных хаотических отображений в качестве нелинейной функции в сети Фейстеля, заключающиеся в использовании раундового ключа как управляющего параметра отображения, что существенно затрудняет дифференциальный криптоанализ такого базового преобразования.

Приведены результаты исследований в вычислительном эксперименте хаотических свойств дискретных отображений, характеризующихся дискретным показателем Ляпунова и дискретной энтропией. Дискретный показатель Ляпунова измеряет расходимость двух траекторий дискретного хаотического отображения, выходящих из соседних точек, после одного раунда. Дискретная энтропия применяется для количественной оценки неопределенности поведения дискретных отображений.

Показано, что значения дискретного показателя Ляпунова и дискретной энтропии дискретного тент-отображения изменяются плавно в пределах небольшого интервала, что говорит о практически постоянных хаотических свойствах во всем интервале значений управляющего параметра, что в большей

степени удовлетворяет требованиям при разработке алгоритма шифрования с использованием динамического хаоса.

На основании полученных результатов сформулирован критерий хаотичности динамики дискретного отображения, заключающийся в близости значений дискретного показателя Ляпунова и дискретной энтропии к их максимальным значениям в пределах малых отклонений для различной мощности множества, и их равномерном распределении во всем интервале значений управляющего параметра дискретного отображения для данной мощности множества.

Обоснован выбор дискретного тент-отображения, описываемого выражением (2) в качестве наиболее предпочтительного из исследованных для использования в алгоритмах шифрования данных на основе динамического хаоса.

$$F(X)=\begin{cases}\left\lceil \dfrac{M}{A}X \right\rceil & при \quad 0 \le X \le A, \\ \left\lfloor \dfrac{M}{M-A}(M-X) \right\rfloor + 1 & при \quad A < X \le M-1, \end{cases} \tag{2}$$

где X – входное значение;

A – управляющий параметр;

M – мощность множества, на котором определено отображение;

$\lceil\ \rceil$ – операция округления в большую сторону;

$\lfloor\ \rfloor$ – операция округления в меньшую сторону.

Таким образом, предложен и обоснован алгоритм шифрования, отличающийся использованием сети Фейстеля, режима динамического хаоса, дискретного хаотического отображения, определением минимального числа раундов и режима работы блочных шифров: режима сцепления блоков либо режима обратной связи по шифртексту.

В **третьей главе** работы рассматриваются вопросы оценки работоспособности алгоритмов шифрования на основе динамического хаоса при использовании известных и специализированных методов.

Приводится анализ алгоритма шифрования на основе динамического хаоса при использовании известного критерия лавинного эффекта, который заключается в значительном изменении бит в выходной последовательности преобразования при малом изменении бит во входной последовательности преобразования. В разработанном алгоритме шифрования при определении показателя лавинного эффекта вводится параметр хаотического отображения.

Новые выражения для расчета лавинных показателей имеют вид

$$\varepsilon_A(i,K) = \left|2k_{AVAL}(i,K) - 1\right|, \quad (3)$$

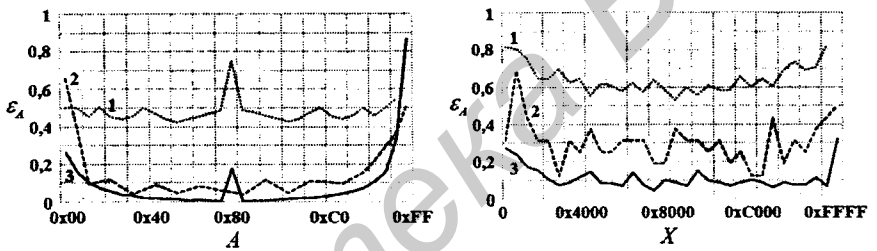
$$\varepsilon_A(i,X) = \left|2k_{AVAL}(i,X) - 1\right|, \quad (4)$$

где X – фиксированное входное значение преобразования, для которого проводится расчет лавинного показателя;

K – фиксированное значение параметра преобразования, для которого проводится расчет лавинного показателя.

Проведен анализ алгоритма шифрования как в паре «входное значение – выходное значение» ($X-Y$) для каждого фиксированного значения параметра K, так и в паре «параметр – выходное значение» ($K-Y$) для каждого фиксированного входного значения X.

На рисунке 2 представлены результаты компьютерного моделирования для определения лавинного эффекта в рассматриваемом базовом преобразовании.



1 – дискретное тент-отображение на множестве мощностью 8 бит; 2 – базовое преобразование на множестве мощностью 8 бит; 3 – базовое преобразование на множестве мощностью 16 бит

Рисунок 2 – Графики зависимости максимального значения лавинного показателя ε_A от раундового ключа A и входного значения X для базового преобразования и дискретного тент-отображения

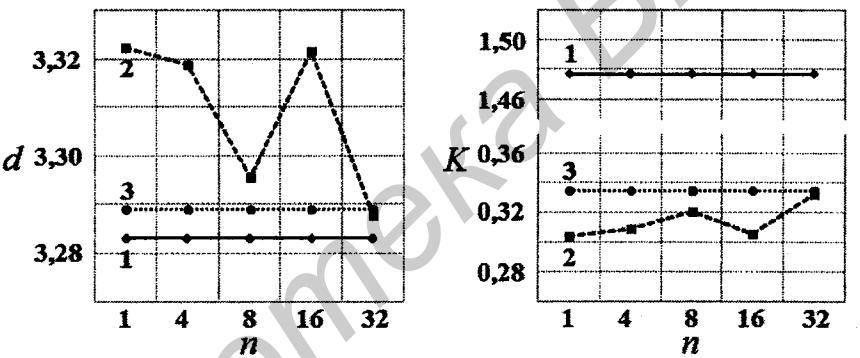
По результатам анализа сделан вывод о выполнении в предложенном автором алгоритме шифрования в рамках указанных интервалов значений раундовых ключей и входных значений требований принципов запутывания и рассеивания. Показано, что обеспечено соблюдение специальных требований при разработке алгоритма шифрования на основе динамического хаоса, заключающихся в определении ключевого пространства и исключении областей с нехаотической динамикой, а также установлении наличия лавинного эффекта в хаотической системе в рамках заданной области ключевого пространства.

Сформулирован способ определения эффективности алгоритма шифрования данных на основе динамического хаоса, отличающийся учетом

управляющего параметра хаотического отображения при определении показателя лавинного эффекта, что подтверждает увеличение эффективности базового преобразования разработанного алгоритма до шести раз за счет применения режима динамического хаоса.

Описывается алгоритм оценки работоспособности и повышения стойкости алгоритма шифрования на основе предложенного метода контроля степени хаотичности выходных последовательностей и особенности его применения в разработанном алгоритме.

С помощью метода задержанной координаты и метода построения фазовых диаграмм проводится сравнительный анализ зашифрованных последовательностей, полученных разработанным алгоритмом шифрования и традиционными, включая AES (Advanced Encryption Standard) и DES (Data Encryption Standard). На рисунках 3 и 4 проиллюстрированы результаты соответствующих вычислительных экспериментов.



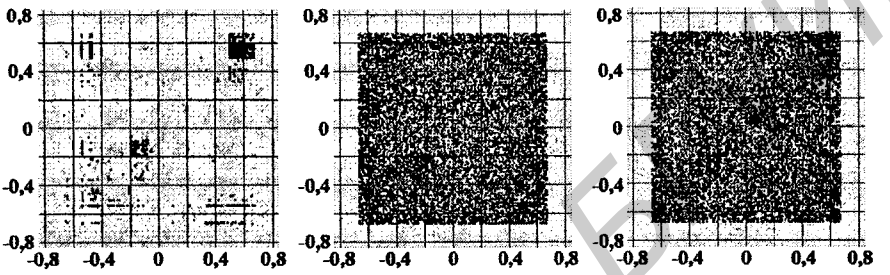
1 – открытый текст; 2 – разработанный алгоритм шифрования;
3 – алгоритм шифрования AES

Рисунок 3 – Графики зависимости корреляционной размерности d и энтропии Колмогорова K зашифрованных последовательностей, полученных разработанным алгоритмом и алгоритмом AES, от количества раундов базового преобразования n в режиме работы CBC

Для открытого текста корреляционная размерность составила 3,283, а энтропия Колмогорова – 1,476. Для режима работы CBC (Cipher Block Chaining), например, значения корреляционной размерности для зашифрованного текста превышают значение для открытого текста на 4,0 – 4,6 %, а значения энтропии Колмогорова составляют, соответственно, 20,0 – 21,8 % от значения для открытого текста. Установлено, что информационная заполняемость фазового пространства при построении фазовых диаграмм,

например, составляет для открытого текста и текста, зашифрованного при использовании режима работы CBC, 4,4 % и 67,9 % соответственно, что видно из рисунка 4.

Результаты вычислительных экспериментов позволили осуществить выбор режимов работы предложенного алгоритма, а также установить минимальное количество раундов базового преобразования алгоритма шифрования в режиме динамического хаоса.



а б в

а – открытый текст; б – зашифрованный текст (разработанный алгоритм);
в – зашифрованный текст (AES)

Рисунок 4 – Фазовые диаграммы входной и выходных последовательностей

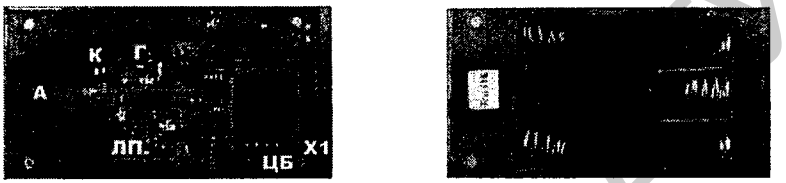
На основании полученных результатов сформулирован метод контроля степени хаотичности выходных последовательностей алгоритма шифрования, заключающийся в автоматическом определении степени и направления изменения хаотичности и использующий в качестве критерия корреляционную размерность и энтропию Колмогорова для установления минимального числа раундов алгоритма шифрования в режиме динамического хаоса.

Таким образом, разработаны способ определения эффективности алгоритма шифрования данных на основе динамического хаоса, отличающийся учетом управляющего параметра хаотического отображения при определении показателя лавинного эффекта, и метод контроля степени хаотичности выходных последовательностей алгоритма шифрования при использовании в качестве критерия параметров корреляционной размерности и энтропии Колмогорова, которые могут быть использованы для оценки работоспособности и криптоанализа алгоритмов шифрования на основе динамического хаоса.

Четвертая глава посвящена описанию структуры и элементов аппаратно-программного комплекса конфиденциальной передачи данных в беспроводной сенсорной сети на базе приемопередатчиков серии ППС-40А.

Рассматриваются программные средства системы передачи данных на основе динамического хаоса. В диссертационной работе при построении беспроводных сенсорных сетей в качестве узлов используются сверхширокополосные прямохаотические приемопередатчики серии ППС-40А (рисунок 5).

Приемопередатчик серии ППС-40А относится к классу устройств с ограниченными ресурсами и коммуникационными возможностями, следовательно, для обеспечения в нем функций шифрования требуется использовать специально предназначенные для этого алгоритмы, к числу которых относится разработанный алгоритм шифрования.



а б

а – вид сверху; б – вид снизу

Рисунок 5 – Приемопередатчик для беспроводных сенсорных сетей

Программные средства для систем передачи данных на базе приемопередатчиков серии ППС-40А включают в себя программный код микроконтроллера, координирующий работу самого приемопередающего устройства; разработанную программную библиотеку, обеспечивающую внешнее управление приемопередатчиком посредством независимого интерфейса.

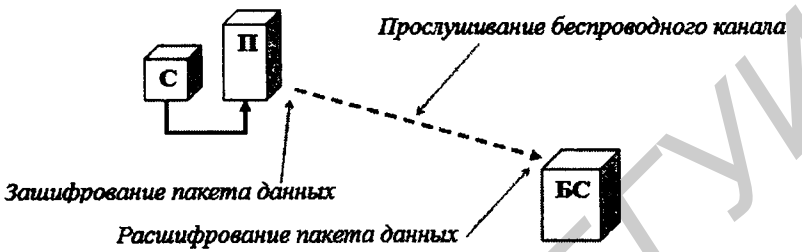
С одной стороны, программная библиотека реализует процесс взаимодействия с приемопередатчиком, подключенным к компьютеру. С другой стороны, программная библиотека реализует независимый интерфейс для взаимодействия стороннего программного обеспечения с приемопередатчиком.

Описывается аппаратно-программная реализация разработанного алгоритма шифрования и моделирование его работы при использовании программного обеспечения Atmel AVR Studio 5.0 на языке программирования AVR Assembler. Проведенный сравнительный анализ показал, что объем памяти микроконтроллера, необходимый для реализации разработанного алгоритма шифрования, по крайней мере в два раза меньше по сравнению со стандартными алгоритмами шифрования.

Разработана структура аппаратно-программного комплекса с использованием предложенного алгоритма шифрования и созданного

программного обеспечения для конфиденциальной передачи данных в беспроводной сенсорной сети на базе приемопередатчиков серии ППС-40А.

Функционирование сети при шифровании данных схематически изображено на рисунке 6.



С – сенсор; П – приемопередатчик; БС – базовая станция; пунктирная линия – беспроводная связь; сплошная линия – проводная связь

Рисунок 6 – Схема зашифрованной передачи информации в сенсорной сети

Для аппаратно-программного комплекса разработан новый программный код микроконтроллера, который включает в себя:

1) введение подпрограммы шифрования данных разработанным алгоритмом;

2) новую подпрограмму отправки и приема пакета в/из эфира путем добавления вызова функции шифрования;

3) введение подпрограммы настройки параметров шифрования (ключа шифрования), которая позволяет только записывать параметры шифрования в приемопередатчик, исключая их считывание во время настройки приемопередатчика при помощи управляющего программного обеспечения.

В функциях приема и отправки пакета реализовано шифрование тела пакета данных целиком, не затрагивая при этом заголовок пакета и байты контрольной суммы. Выбор такой схемы преобразования продиктован необходимостью защиты информации о маршрутизации, поскольку одной из целей пассивного прослушивания является извлечение идентификаторов узлов. Отметим, что контрольная сумма пакета вычисляется после применения к нему процедуры зашифрования.

Реализация алгоритма шифрования при использовании блока размером 8 байт характеризуется следующими параметрами: объем памяти для хранения программного кода составляет 762 байта, объем памяти для хранения данных – 241 байт, максимальная скорость обработки данных – 88,2 Кбит/с при тактовой частоте микроконтроллера 20 МГц.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Предложен и обоснован алгоритм шифрования на основе динамического хаоса, включающий разбиение обрабатываемого текста при блочном проведении шифрования на последовательность блоков одинаковой длины, многократное раундовое преобразование каждого блока текста, определение числа раундов и способа взаимосвязи блоков текста в выходной последовательности, основанный на использовании сети Фейстеля, режима динамического хаоса, дискретного хаотического отображения, определении минимального числа раундового преобразования и режима работы блочных шифров CBC (режим сцепления блоков) либо CFB (режим обратной связи по шифртексту), что обеспечивает при конфиденциальной передаче информации в беспроводных сетях повышение эффективности шифрования [1–А, 2–А, 4–А, 8–А, 9–А, 10–А, 11–А, 12–А, 13–А, 17–А, 18–А, 19–А, 20–А].

2. Использование метода задержанной координаты при шифровании предложенным алгоритмом позволяет повысить криптостойкость алгоритма и выявить отличия в выходной последовательности относительно входной, которые могут быть выражены качественными параметрами в виде фазовых диаграмм и количественными параметрами в виде корреляционной размерности и энтропии Колмогорова. В частности, введена возможность визуализации фазовых диаграмм последовательностей, что позволяет определить информационную заполняемость фазового пространства фазовыми траекториями динамической системы, которая для входной и выходной последовательностей составляет 4,4 % и 69,7 %, соответственно, для режимов CBC и CFB. Значения корреляционной размерности d и энтропии Колмогорова K для выходных последовательностей, например, в режиме работы CBC превышают значения для входных на 4,0–4,6 %; а энтропии Колмогорова – снижаются относительно значений для входных на 20,0–21,8 %, что демонстрирует повышение эффективности шифрования.

Метод задержанной координаты в отличие от известного, основанного на определении показателей Ляпунова, позволяет для повышения стойкости шифрования перейти в качественно новый диапазон определения хаотичности. В режиме CBC, например, ограничение значения корреляционной размерности до 3,40±0,05, а энтропии Колмогорова – до 0,37±0,01 при оптимизации числа раундов базового преобразования показывает возможность исключения появления только детерминированной компоненты сигнала в выходной последовательности при шифровании [3–А, 5–А, 21–А].

3. Выбор новых параметров – корреляционной размерности и энтропии Колмогорова на основе метода задержанной координаты при анализе выходных последовательностей алгоритма шифрования позволяет установить оптимальное число раундов в процессе шифрования, при котором наблюдается максимальная степень хаотичности последовательностей. В оптимальном режиме информационные параметры выходной последовательности в виде фазовых диаграмм, корреляционной размерности и энтропии Колмогорова согласуются с результатами анализа того же открытого текста при использовании стандартных алгоритмов шифрования DES (Data Encryption Standard) и AES (Advancend Encryption Standard). Фазовые диаграммы выходных последовательностей, как при использовании предложенного алгоритма, так и стандартных алгоритмов, не отличаются и характеризуются практически 69,7 % информационной заполняемостью. Установлено, что если при определении параметров выходной последовательности после очередного раунда базового преобразования блока текста наблюдается увеличение информационной заполняемости фазовой диаграммы свыше 10 % и параметра корреляционной размерности до 3,55±0,05 и снижение значения энтропии Колмогорова до 0,35±0,01 в режиме СВС, например, то необходимо ограничить число раундов предыдущим значением. Анализ методом задержанной координаты позволяет использовать корреляционную размерность и энтропию Колмогорова в качестве критерия для метода контроля степени хаотичности для автоматического определения степени и направления изменения хаотичности выходных последовательностей [3–А, 5–А, 21–А].

4. Предложен способ определения эффективности алгоритма шифрования с использованием при оценке показателя лавинного эффекта алгоритма дополнительно в качестве управляющего параметр хаотического отображения. Для случая вариации управляющего параметра в диапазоне $0x18-0x78$ и $0x88-0xF8$ значения лавинного показателя устанавливаются в промежутке 0–0,16. Для случая вариаций значений бит входных последовательностей в диапазоне $0x1800-0xF800$ значения лавинного показателя составляют 0,04–0,15. Это позволяет при формировании характеристик для проведения дифференциального криптоанализа получить данные, характеризуемые более высокой по сравнению с традиционными способами повторяемостью и воспроизводимостью [4–А, 7–А, 15–А, 16–А].

5. Предложен способ для оценки работоспособности алгоритма шифрования, сочетающий: 1) определение степени и направления изменения хаотичности выходной последовательности алгоритма шифрования по параметрам: корреляционной размерности и энтропии Колмогорова; 2) определение показателя лавинного эффекта алгоритма шифрования с учетом влияния управляющего параметра хаотического отображения, применяемого в

виде аргумента при оценке показателя, в качестве критериев для проведения эффективной оценки работоспособности и криптоанализа алгоритмов шифрования, использующих динамический хаос.

Значения корреляционной размерности составляют 3,40–3,55, а значения энтропии Колмогорова изменяются в диапазоне 0,35–1,55 для СВС режима шифрования. Установлено, что при наличии лавинного эффекта значения лавинного показателя варьируют в пределах 0–0,16 и 0,04–0,15 в зависимости от управляющего параметра и значений бит входных последовательностей соответственно. В то же время для исходного отображения в отсутствие хаоса в первом случае величина лавинного показателя составляет 0,42–0,51, а во втором соответственно – 0,52–0,83. Таким образом, предложенный способ для анализа работоспособности и криптоанализа алгоритма шифрования позволяет разработать способ шифрования на основе динамического хаоса с эффективностью базового преобразования в четыре – шесть раз выше, чем в традиционном методе [5–А, 7–А, 21–А].

6. Разработаны программные средства для мобильных систем передачи информации на сверхширокополосных хаотических сигналах, шифрование данных при этом реализуется путем модификации основного кода прошивки микроконтроллера и использованием разработанной программной библиотеки. Библиотека в виде отдельного компонента обеспечивает управление приемопередающим устройством и его доступ к стороннему программному обеспечению посредством независимого интерфейса. Это позволяет снизить структурную сложность программного кода, а также повысить надежность функционирования программной библиотеки и всего интерфейса взаимодействия за счет уменьшения количества возможных вариантов переключения режима работы интерфейса [6–А, 14–А].

7. Разработана структура аппаратно-программного комплекса передачи информации в беспроводной сети на базе сверхширокополосных прямохаотических приемопередатчиков ППС-40А, в котором реализация алгоритма шифрования осуществляется использованием разработанного программного кода прошивки микроконтроллера приемопередатчика, отличающегося исключением функции считывания во время настройки шифрования, что позволяет обеспечить конфиденциальность передаваемой информации. Аппаратная реализация алгоритма шифрования характеризуется сокращением рабочего объема памяти микроконтроллера по сравнению с традиционными (BelT, AES, ГОСТ 28147-89) в два – пять раз. При этом объем памяти для хранения программного кода составляет 762 байт; объем памяти для хранения переменных 241 байт; скорость обработки данных 88,2 Кбит/с при тактовой частоте микроконтроллера 20 МГц [6–А, 13–А, 14–А, 22–А].

9–A. Sidorenko, A.V. The algorithms of the encryption based on the dynamic chaos construction using discrete mapping / A.V. Sidorenko, K.S. Mulyarchik // Nonlinear Dynamics and Application: Proceedings of the 15th International School-Conference "Foundations & Advances in Nonlinear Science", Minsk, Sept. 20–23, 2010 / Belarusian State University. – Minsk, 2010. – P. 133–138.

10–A. Мулярчик, К.С. Построение алгоритмов шифрования данных на основе цифровых хаотических систем / К.С. Мулярчик // Радиоэлектроника и молодежь в XXI веке : материалы XV Междунар. молодеж. форума, Харьков, 18–20 апр. 2011 г. / Харьковский национальный университет радиоэлектроники. – Харьков, 2011. – С. 173–174.

11–A. Сидоренко, А.В. Цифровые отображения для систем шифрования на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Комплексная защита информации : материалы XVI науч.-практ. конф., Гродно, 17–20 мая 2011 г. – Минск, 2011. – С. 152–155.

12–A. Сидоренко, А.В. Цифровые системы и отображения на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Международный конгресс по информатике: информационные системы и технологии: материалы междунар. науч. конгресса, 31 окт.–3 нояб. 2011 г.: в 2 ч. – Минск, 2011. – Ч. 1. – С. 139–144.

13–A. Мулярчик, К.С. Средства защиты в информационных системах на основе дискретного динамического хаоса / К.С. Мулярчик // XIV республиканская научно-методическая конференция молодых ученых : сб. материалов, [Брест], 11 мая 2012 г.: в 2 ч. / М-во образования Респ. Беларусь, Брест. гос. ун-т им. А.С. Пушкина ; под общ. ред. В.В. Здановича. – Брест, 2012. – Ч. 1. – С. 69–71.

14–A. Сидоренко, А.В. Организация сенсорных защищенных сетей для систем управления / А.В. Сидоренко, А.И. Ходасевич, К.С. Мулярчик, Ю.В. Андреев // Информационные технологии и системы 2012 (ИТС 2012) : материалы Междунар. науч. конф, Минск, 24 окт. 2012 г. / БГУИР. – Минск, 2012. – С. 34–35.

15–A. Sidorenko, A.V. Analysis of the avalanche effect in discrete chaotic maps for block ciphers / A.V. Sidorenko, K.S. Mulyarchik // Theoretical & Applied Stochastics: Proceedings of the 10th International Conference «Computer Data Analysis & Modeling 2013», Minsk, Sept. 10–14, 2013 / Research Institute for Applied Problems of Mathematics and Informatics, Belarusian State University. – Minsk, 2013. – P. 32–35.

16–A. Сидоренко, А.В. Лавинный эффект в алгоритмах шифрования на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Международный конгресс по информатике: информационные системы и технологии: материалы междунар. науч. конгресса, Минск, 4–7 нояб. 2013 г. /

редкол. : С.В. Абламейко (отв. ред.), В.В. Казаченок (отв. ред.) [и др.]. – Минск, 2013. – С . 105–109.

Тезисы докладов

17–А. Сидоренко, А.В. Применение хаотических отображений в алгоритмах шифрования данных / А.В. Сидоренко, К.С. Мулярчик // Технические средства защиты информации : материалы VII Белорус.-российск. науч.-техн. конф., г. Минск, 23–24 июня 2009 г. / БГУИР. – Минск, 2009. – С. 64.

18–А. Сидоренко, А.В. Анализ криптостойкости систем шифрования на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Информационные системы и технологии (IST'2009) = Informational systems and technologies : материалы V Междунар. конф.-форума, Минск, 16–17 ноября 2009 г.: в 2 ч. / БГУ [и др.] ; [редкол.: Н. И. Листопад и др.] – Минск, 2009. – Ч. 2. – С. 75–76.

19–А. Сидоренко, А.В. Целочисленные хаотические отображения, их свойства и особенности применения в алгоритмах шифрования данных на основе динамического хаоса / А.В. Сидоренко, К.С. Мулярчик // Технические средства защиты информации: труды VIII Белорус.-российск. науч.-техн. конф., г. Минск, 24–28 мая 2010 г. / БГУИР. – Минск, 2010. – С. 50.

20–А. Сидоренко, А.В. Шифрование данных на основе дискретных хаотических систем и отображений / А.В. Сидоренко, К.С. Мулярчик // Технические средства защиты информации: тез. докл. X Белорус.-российск. науч.-техн. конф., Минск, 29–30 мая 2012 г. / БГУИР. – Минск, 2012. – С. 50.

21–А. Sidorenko, A.V. The control of chaotic regimes in encryption algorithm based on dynamic chaos / A.V. Sidorenko, K.S. Mulyarchik // Advances in Nonlinear Science: Proceedings of 16th International Conference-School Foundations, Minsk, Sept. 24–28, 2012 / Belarusian State University. – Minsk, 2012. – P. 55.

22–А. Сидоренко, А.В. Защита биоэлектрической информации / А.В. Сидоренко, А.В. Крупенин, К.С. Мулярчик // Средства медицинской электроники и новые медицинские технологии: Медэлектроника–2012: тр. VII междунар. науч.-техн. конф., Минск, 13–14 дек. 2012 г. / БГУИР. – Минск, 2012. – С. 337.

23–А. Мулярчик, К.С. Анализ лавинного эффекта в алгоритмах шифрования на основе дискретных хаотических отображений / К.С. Мулярчик // Технические средства защиты информации: тез. докл. XI Белорус.-российск. науч.-техн. конф., Минск, 5–6 июня 2013 г. / БГУИР. – Минск, 2013. – С. 74.

РЕЗЮМЕ

Мулярчик Константин Сергеевич

Шифрование данных с использованием динамического хаоса

Ключевые слова: шифрование данных, динамический хаос, дискретные хаотические отображения, беспроводные сенсорные сети.

Цель работы: разработка алгоритма шифрования на основе динамического хаоса и его аппаратно-программная реализация, ориентированная на применение в беспроводных сенсорных сетях.

Методы исследования: принципы и методы разработки и оценки работоспособности алгоритмов шифрования, моделирования его работы и оценки характеристик его аппаратно-программной реализации.

Полученные результаты и их новизна: предложен и обоснован блочный симметричный алгоритм шифрования, отличающийся использованием сети Фейстеля, режима динамического хаоса и дискретного хаотического отображения для применения в устройствах с ограниченными вычислительными ресурсами, в частности, в узлах беспроводных сенсорных сетей; предложен новый метод оценки работоспособности алгоритмов шифрования на основе динамического хаоса, использующий метод задержанной координаты при анализе выходных последовательностей, что позволило выбрать допустимые режимы работы алгоритма и количество раундов базового преобразования; предложен способ определения эффективности алгоритма шифрования с использованием при оценке показателя лавинного эффекта алгоритма дополнительно в качестве управляющего параметр хаотического отображения; разработаны программные средства и структура аппаратно-программного комплекса передачи информации в беспроводной сенсорной сети на базе сверхширокополосных прямохаотических приемопередатчиков ППС-40А с использованием разработанного алгоритма шифрования для обеспечения конфиденциальности передаваемой информации.

Степень использования: разработанный блочный симметричный алгоритм шифрования может быть применен в аппаратно-программных средствах с ограниченными вычислительными ресурсами и коммуникационными возможностями для обеспечения конфиденциальности передаваемой информации.

Область применения: беспроводные сенсорные сети.

РЭЗЮМЭ

Мулярчык Канстанцін Сяргеевіч

Шыфраванне дадзеных з выкарыстаннем дынамічнага хаосу

Ключавыя словы: шыфраванне дадзеных, дынамічны хаос, дыскрэтныя хаатычныя адлюстраванні, бесправадныя сэнсарныя сеткі.

Мэта працы: распрацоўка алгарытму шыфравання на аснове дынамічнага хаосу і яго апаратна-праграмная рэалізацыя, арыентаваная на ўжыванне ў бесправадных сэнсарных сетках.

Метады даследавання: прынцыпы і метады распрацоўкі і ацэнкі працаздольнасці алгарытмаў шыфравання, мадэліравання яго работы і ацэнкі характарыстык яго апаратна-праграмнай рэалізацыі.

Атрыманыя вынікі і іх навізна: прапанаваны і абгрунтаваны блокавы сіметрычны алгарытм шыфравання, які адрозніваецца выкарыстаннем сеткі Фейстэля, рэжыму дынамічнага хаосу і дыскрэтнага хаатычнага адлюстравання для ўжывання ў абсталяванні з абмежаванымі вылічальнымі рэсурсамі, у прыватнасці, у вузлах бесправадных сэнсарных сетак; прапанаваны новы спосаб ацэнкі працаздольнасці алгарытмаў шыфравання на аснове дынамічнага хаосу, які выкарыстоўвае метад затрыманай каардынаты пры аналізе выхадных паслядоўнасцяў, што дазволіла выбраць дапушчальныя рэжымы работы алгарытму і колькасць раўндаў базавага пераўтварэння; прапанаваны спосаб вызначэння эфектыўнасці алгарытму шыфравання з выкарыстаннем пры ацэнцы паказчыка лавіннага эфекту алгарытму дадаткова ў якасці кіраўніка параметр хаатычнага адлюстравання; распрацаваны праграмныя сродкі і структура апаратна-праграмнага комплексу перадачы інфармацыі ў бесправаднай сэнсарнай сетцы на базе звышшырокапалосных прамахаатычных прыёмаперадатчыкаў ППС-40А з выкарыстаннем распрацаванага алгарытму шыфравання для забеспячэння прыватнасці пры перадачы інфармацыі.

Ступень выкарыстання: распрацаваны блочны сіметрычны алгарытм шыфравання можа быць ужыты ў апаратна-праграмных сродках з абмежаванымі вылічальнымі рэсурсамі і камунікацыйнымі магчымасцямі для забеспячэння прыватнасці пры перадачы інфармацыі.

Галіна ўжывання: бесправадныя сэнсарныя сеткі.

SUMMARY

Mulyarchik Konstantin Sergeevich

Data encryption using dynamic chaos

Keywords: data encryption, dynamic chaos, discrete chaotic maps, wireless sensor networks.

Research objective: to develop an encryption algorithm based on dynamic chaos and to perform its firmware implementation oriented towards the usage in wireless sensor networks.

Methods of the research: principles and methods of development and estimation of encryption algorithms, simulation and estimation of algorithm firmware implementation performance.

The results obtained and their novelty: a block symmetric encryption algorithm based on the usage of Feistel network, dynamic chaos mode and discrete chaotic maps. has been proposed and justified for the usage in the devices with limited computational resources, particularly, in wireless sensor networks; a new method for estimation of encryption algorithms based on dynamic chaos has been proposed which uses delayed coordinate method to analyze output sequences; a method for determining the effectiveness of the encryption algorithm has been proposed which additionally uses the control parameter of the chaotic map for the avalanche effect estimation; software tools and the structure of the hardware-software system using an encryption algorithm have been developed to ensure the confidentiality of the information transmitted over the wireless sensor network based on ultrawideband chaotic transceivers PPS- 40A.

Degree of use: the developed block symmetric encryption algorithm can be used in hardware and software tools with limited computational resources and communication capabilities to ensure the confidentiality of transmitted information.

Sphere of application: wireless sensor networks.

Научное издание

Мулярчик Константин Сергеевич

ШИФРОВАНИЕ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ ДИНАМИЧЕСКОГО ХАОСА

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Подписано в печать 12.12.2013.	Формат 60x84 $^1/_{16}$.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л. 1,63.
Уч.-изд. л. 1,5.	Тираж 60 экз.	Заказ 474.

Издатель и полиграфическое исполнение: учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009
220013, Минск, П. Бровки, 6