

На правах рукописи



Борисов Алексей Игоревич

МЕТОД И АППАРАТНЫЕ СРЕДСТВА
ПОВЫШЕНИЯ ОПЕРАТИВНОСТИ
АВТОМАТИЧЕСКОЙ МОДИФИКАЦИИ
КЛЮЧЕВЫХ ДАННЫХ

05.13.05 - Элементы и устройства
вычислительной техники и систем управления
05.13.19 - Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание учёной степени
кандидата технических наук

КУРСК – 2012

Работа выполнена в Юго-Западном государственном университете

Научный руководитель: доктор технических наук, профессор,
заслуженный деятель науки РФ
Сизов Александр Семенович

Официальные оппоненты: *Добрица Вячеслав Порфирьевич*
доктор физико-математических наук,
профессор,
заведующий кафедрой «Комплексная за-
щита информационных систем»
Юго-Западного государственного
университета

Векленко Юрий Алексеевич
кандидат технических наук,
начальник отдела стендов и
технологических средств контроля
Курского ОАО «Прибор» ОКБ
«Авиаавтоматика»

Ведущая организация: Белгородский государственный
технологический университет
имени В.Г. Шухова

Защита состоится 16 марта 2012 г. в 16-00 часов в конференц-зале на заседании диссертационного совета Д 212.105.02 при Юго-Западном государственном университете по адресу: 305040, г. Курск, ул. 50 лет Октября, 94.

С диссертацией можно ознакомиться в библиотеке Юго-Западного государственного университета по адресу: 305040, г. Курск, ул. 50 лет Октября, 94

Автореферат разослан «15» февраля 2012 г.

Ученый секретарь
диссертационного совета Д 212.105.02



Е.А. Титенко

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы. Развитие средств вычислительной техники характеризуется расширением областей её применения. Среди устройств и элементов вычислительной техники и систем управления, предназначенных для решения задач в области защиты информации, особое значение имеют аппаратные средства генерации ключевых данных (КД). Использование ключевых данных (логины, идентификаторы, пароли, ключи и т.д.) необходимо для осуществления авторизации с целью определения круга пользователей, наделенных специальными полномочиями, ограничения несанкционированного доступа, селекции необходимых в работе данных и обеспечения профессиональной деятельности. Особо важна процедура авторизации в распределенных вычислительных системах (РВС) с сетевым доступом к общим конфигурируемым вычислительным ресурсам («облачные вычислительные системы»). Ключевые данные (КД) имеют ограниченный срок действия, вследствие чего возникает объективная необходимость развития средств аппаратной генерации, модификации и адресной доставки ключевых данных пользователям. С другой стороны сгенерированные КД на период своего существования должны характеризоваться устойчивостью для защиты выделяемого ресурса в РВС, что требует создания и применения вычислительно трудоемких алгоритмов и процедур. Необходимость совмещения аппаратной генерации КД и вычислительных трудоемких алгоритмов и процедур определяют основное *противоречие* данного исследования.

Ведущими учеными в области разработки специализированных устройств параллельной обработки данных являются Угрюмов Е.П., Самофалов К.Г., Сташин В.В. и др. Значимый вклад в решение проблем генерации и распределения ключевых данных был внесен такими отечественными учеными, как Баричев С.Г., Уфимцева В.Б., Ярмолик В.Н., Варфоломеев А.А. и др. Однако вместе с тем в работах вышеперечисленных ученых вопросы аппаратной генерации и модификации ключевых данных рассматривались частично.

Так в исследованиях Г. Шустера, J-P. Eeckmann приведены основные свойства дискретного треугольного отображения, показывающие возможность его использования в разработке устройства генерации КД, однако при этом не учтены особенности реализации в числах с фиксированной запятой.

В работах В. Diffie, М. Hellman рассмотрены алгоритмы передачи ключевых данных с использованием протоколов построения общего секретного ключа, которые ограничены использованием дискретного логарифмирования, что определяет существенную вычислительную сложность и объективные трудности аппаратной поддержки данных алгоритмов. В исследованиях R. Needham, М. Schroeder рассмотрено применение протоколов аутентификации и обмена ключами, использующих промежуточную доверенную сторону, что накладывает дополнительные требования к структуре РВС. Ра-

боты В. Schneier показывают целесообразность периодической модификации ключевых данных, но не дают конкретных реализаций с использованием устройства.

В целом, средства генерации, модификации и доставки КД в современных РВС в большинстве случаев имеют преимущественно программную реализацию, что объективно обуславливает поиск новых подходов и средств их реализации.

В соответствии с вышеизложенным **актуальной научной задачей** является разработка средств генерации и адресной доставки ключевых данных с использованием дискретного детерминировано-хаотического отображения.

Работа выполнялась в рамках НИР по тематическому плану 2009 года Министерства образования и науки РФ №1.5.09: «Создание продукционной алгоритмической системы быстрых символьных вычислений и языка программирования для реконфигурируемых вычислительных систем».

Объектом исследования являются многоабонентские распределенные системы управления.

Предмет исследования составляют методы и аппаратные средства автоматизации обработки ключевых данных в многоабонентских распределенных системах управления.

Цель работы заключается в создании метода, алгоритмических и технических средств генерации ключевых данных, их динамической модификации и адресной доставки, обеспечивающих повышение оперативности модификации ключевых данных и уменьшение нагрузки на администратора многоабонентской распределенной системы управления.

Для достижения поставленной цели необходимо решить следующие **задачи**:

- анализ состояния вопроса генерации и управления ключевыми данными в распределенной системе управления, обоснование направлений исследования;
- разработка метода динамической модификации ключевых данных для пользователей распределенной системы управления;
- разработка способа адресной доставки ключевых данных пользователю с осуществлением акцессорного преобразования на основе дискретного треугольного отображения;
- разработка структурно-функциональной организации устройства и его технических решений для генерации ключевых данных с использованием детерминировано-хаотических числовых рядов;
- синтез алгоритма работы и архитектуры многоабонентской распределенной системы управления и экспериментальная оценка её характеристик.

Методы исследования. Для решения поставленных задач использовались теория проектирования элементов и устройств вычислительной техники, методы разработки программного обеспечения, аппарат дискретной ма-

тематики, теории: хаотических систем, алгоритмов, математического моделирования.

Научная новизна результатов работы и основные положения, выносимые на защиту:

- структурно-функциональная организация специализированного вычислительного устройства генерации ключевых данных пользователя, отличающаяся использованием аналогового генератора шума и его суперпозицией с треугольным дискретным отображением, имеющим линейную вычислительную сложность, что позволяет генерировать детерминированно-хаотическую последовательность аппаратными средствами (05.13.05);

- параллельно-конвейерная организация операционной части специализированного вычислительного устройства генерации ключевых данных, реализованная на программируемой элементной базе (ПЛИС Virtex 6 XC6VLX130T), что позволяет получить технические решения с высокой надежностью функционирования, минимальными массогабаритными, энергетическими показателями (05.13.05);

- метод динамической модификации (генерация, доставка, запись на персональный носитель) ключевых данных пользователей, отличающийся введением шага предобработки исходных данных, традиционно имеющих нормальный закон распределения, в массив с равномерным распределением на основе применения n итераций треугольного отображения для каждого элемента исходных данных (05.13.19);

- способ адресной доставки ключевых данных пользователю, отличающийся использованием акцессорного (прямого-обратного) преобразования на основе мультиплексора и демультимплексора, управляемых хаотическим генератором «треугольное отображение», что позволяет автоматически шифровать и дешифровать передаваемые данные с подтверждением адресации (05.13.19);

- архитектура многоабонентской распределенной системы управления ключевыми данными, разграничивающей в клиентской и серверной частях функции акцессорного преобразования, генерации, адресной доставки и сохранения ключевых данных, что обосновывает возможность аппаратной реализации отдельных ее функций на сервере и приводит к повышению оперативности автоматической модификации ключевых данных (05.13.05).

Практическая значимость. Разработанный метод динамической модификации КД пользователей РВС реализован в виде аппаратно-программной системы, содержащей в составе серверной ЭВМ устройство генерации КД, а также программы «Сервер модификации КД» и «Клиент модификации КД». Результаты практического использования разработанной аппаратно-программной системы подтверждают снижение нагрузки на администратора в *4.3 раза* и повышение оперативности смены ключевых данных в *7 раз*. Разработанные на базе ПЛИС технические решения блоков предобработки последовательности действительных чисел могут найти применение в математических сопроцессорах и устройствах интеллектуальной

обработки числовой и символьной информации. Статистические тесты последовательностей, порождаемых разработанным генератором, удовлетворяют истинно случайному генератору на 99,5% по показателю выполнимости, что делает возможным его использование в оперативном получении индивидуальных КД для пользователей многоабонентских распределенных систем управления.

Реализация результатов работы. Основные результаты диссертации, полученные автором при выполнении исследований, внедрены в Орловско-Курском региональном центре связи ОАО «Российские железные дороги», а также применяются в составе «Системы многоабонентского доступа к документам» в ФГУП «Курский НИИ» МО РФ, что подтверждено актами о внедрении. Разработанные решения используются в учебном процессе кафедры «Программного обеспечения вычислительной техники» Юго-Западного государственного университета.

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались на следующих научно-технических конференциях: VIII Международная конференция «Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2008» (Курск, 2008); XV Международная научно-техническая конференция «Физические и компьютерные технологии» (Харьков, 2008-2009); II международная научно-практическая конференция «Васильевские чтения. Ценности и интересы современного общества» (Курск, 2008); на научно-технических семинарах кафедр «Программное обеспечение вычислительной техники», «Вычислительная техника», «Информационные системы и технологии» Юго-Западного государственного университета (2008-2012 гг.). Результаты диссертационной работы докладывались и получили положительную оценку на кафедре «Вычислительная техника» Юго-Западного государственного университета.

Соответствие паспорту специальности. Диссертационная работа соответствует паспорту научной специальности 05.13.05 – «Элементы и устройства вычислительной техники и систем управления» по пункту 2 «Теоретический анализ и экспериментальное исследование функционирования элементов и устройств вычислительной техники и систем управления в нормальных и специальных условиях с целью улучшения технико-экономических и эксплуатационных характеристик» в части разработки устройства генерации ключевых данных и разработки элемента системы управления ключевыми данными – системы динамической модификации и адресной доставки ключевых данных.

Диссертационная работа соответствует паспорту научной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» по пункту 11 «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа» в части разработки метода управления динамической моди-

фикацией и адресной доставкой ключевых данных и разработки способа адресной доставки ключевых данных.

Публикации. По материалам диссертационной работы опубликовано 12 научных работ, в том числе 3 статьи в рецензируемых научных журналах и изданиях, свидетельство о государственной регистрации программы для ЭВМ в Роспатенте № 2009613768.

Личный вклад автора. В работах, опубликованных в соавторстве и приведенных в конце автореферата, лично соискателем выполнено следующее: в [1] представлено описание разработанного устройства генерации КД; в [2,3,5] предложены для использования в РВС алгоритмы с использованием свойств треугольного отображения; в [4] представлен разработанный метод динамической модификации и адресной доставки ключевых данных; в [6] проведено статистическое тестирование числовых последовательностей, порождаемых треугольным отображением; в [7,8,9] проведен обзор алгоритмов и аппаратных средств, использующих КД для защиты информации, и произведена оценка необходимости периодической модификации КД; в [10,11] отработаны подходы проектирования специализированных вычислительных устройств, в [12] проведена реализация алгоритмов статистического тестирования числовой последовательности.

Структура диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы и 1 приложения.

Основная часть диссертации содержит 143 страницы машинописного текста, включая 39 рисунков и 3 таблицы.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, определены цели и задачи работы, ее научная новизна и практическая значимость; определены способы решения сформулированных задач; приведены сведения об апробации результатов работы.

В первой главе проведен *анализ состояния вопроса* генерации и управления ключевыми данными в распределенных вычислительных системах, распределенных системах управления, в развивающемся направлении «облачных» вычислительных системах – модели, представляющей информационные ресурсы как услуги и распределяющей их удаленным пользователям, имеющей в настоящее время высокую конкурентоспособность.

В перечисленных системах существует необходимость использования персональных КД. Проведен обзор и анализ алгоритмов и аппаратных средств динамической модификации пароля и ключа – как части КД, для архитектур РВС с многоабонентским обслуживанием клиентов. Необходимость совершенствования существующих средств показана на основе оценки функциональности названных архитектур. При этом отмечается, что оценка функциональности РВС отражает совершенство механизмов и скорость работы системы модификации и адресной доставки (СМиАД) при автоматиза-

ции функциональных обязанностей администраторов при сохранении способности программной РВС выполнять весь набор функций, определенных в ее внешнем описании. Рассмотрена возможность применения существующих подходов к проектированию механизмов преобразований для разработки акцессорного преобразования (АП). Приведены базовые решения подходов, которые использованы для разработки АП, целью которого является контроль адресации при доставке КД пользователю РВС.

В заключении раздела описывается сущность предлагаемого подхода в решении поставленной задачи и приводятся основные преимущества данного подхода по сравнению с рассмотренными аналогами. Детальное описание получаемых преимуществ приведено в последующих главах по мере детализации разработки и исследования.

Во второй главе приведен математический аппарат для решения поставленных задач. В качестве базы выбрана теория хаотических систем. Приведены ее основные положения и теоретически обоснована применимость для реализации СМиАД. Из теории хаотических систем для разработки генератора случайно-подобных чисел обоснован выбор направления, сопряженного с дискретными отображениями. В качестве генератора выбрано дискретное «Треугольное» отображение (tent map), представляющее собой итерируемую функцию (рис. 1), где x – динамическая переменная, r – параметр отображения.

$$x \text{ а } f(r, x),$$

$$x_{k+1} = f(r, x_k),$$

$$f(r, x) = \begin{cases} 2rx, & x \leq 1/2 \\ 2r(1-x), & x > 1/2, \end{cases}$$

$$f(r, x) = \Delta(r, x) = r \left(1 - 2 \left| \frac{1}{2} - x \right| \right).$$

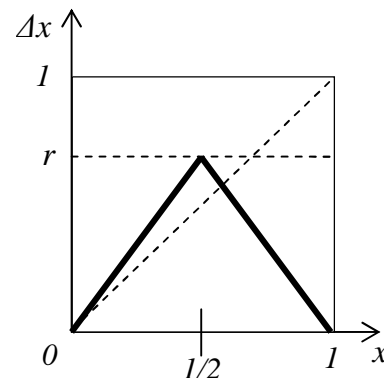


Рис. 1. Треугольное отображение

Проведен анализ свойств выбранного дискретного отображения, состоящий в определении значимых для разработки генератора параметров и указании ограничений на значения этих параметров для реализации в области действительных чисел, представленных в дискретном виде с ограниченным числом разрядов.

Для треугольного отображения показатель Ляпунова равен $\lambda = \ln 2r$ с изменением знака при $r = 1/2$. Он служит параметром, характеризующим каноническое детерминировано-хаотическое поведение. Итерируемая функция при $r > 1/2$ порождает хаотическую последовательность. При $r = 1$ хаотическое поведение характеризуется постоянной стационарной плотностью $\rho(x) = 1$ и дельта-коррелированными итерациями $C(m) = d_{m,0} / 12$.

Вычисление значений итераций треугольного отображения в области действительных чисел, представленных в дискретном виде с ограниченным числом разрядов (например, 8 байт double) имеет ряд особенностей. Так как хаотическое поведение треугольного отображения зависит от параметра r , то выбор значения данного параметра не произволен. Как показано, требуемые свойства выходной последовательности генератора наблюдаются при параметре r равном 1, однако в области действительных чисел, представленных в дискретном виде с фиксированной запятой, такое значение параметра r делает поведение треугольного отображения подобным битовому сдвигу с потерей значащих разрядов генерируемого значения. Для предотвращения процесса потери значащих разрядов выбор параметра r ограничивается интервалом $(1 \cdot 10^{-6}; 1)$, а значение динамической переменной x_0 – интервалом $(0; 0.5)$.

Таким образом, анализ свойств дискретного отображения показал возможность использования данного дискретного отображения для решения основной задачи диссертационного исследования и выявил ограничения на значения вычислительного параметра r .

Главным итогом раздела является доказательство возможности использования треугольного отображения для построения генератора случайных-подобных (детерминировано-хаотических) чисел с отсутствием корреляции между итерациями и значениями, равномерно распределенными в интервале $(0; 1)$. Отмечена необходимость проверки статистической пригодности выходных последовательностей генератора для формирования адресной составляющей КД.

В третьей главе рассмотрены метод, основные алгоритмы и устройство, обеспечивающие функционирование системы управления КД РВС.

Метод динамической модификации КД состоит из следующих этапов.

1. Для каждого пользователя РВС администратором выбираются период смены КД, генерируется и сохраняется на индивидуальный носитель информации инициализационные КД.

2. По окончании периода использования КД автоматически в процессе регистрации пользователя с использованием устройства выполняется операция генерации новых КД.

3. Новые КД с использованием адресной доставки передаются пользователю и заменяют на индивидуальном носителе информации предыдущие. Для осуществления контроля корректности проведенной замены в заключение операции производится повторная контрольная инициализация соединения с использованием новых КД пользователя.

Существенными для предложенного метода является использование операции автоматической генерации КД и адресной доставки, описание которых приводится ниже. С использованием распределенных индивидуальных КД функционируют сторонние схемы защиты информации, установленные в организации, для выполнения текущих задач в системе управления.

Для автоматизации получения новых КД, его парольной и адресной части, разработано *устройство генерации ключевых данных (УГКД)*. В уст-

ройте используется генерация КД пользователя, состоящая в следующей совокупности шагов.

1. Накопление оцифрованного сигнала аналогового генератора шума с преобразованием в массив чисел в интервале $(0; 1)$.

2. Преобразование массива чисел с использованием разработанного случайно-подобного генератора в массив с равномерным распределением.

3. Формирование парольной и адресной части КД по равномерно распределенным данным.

В генерации КД существенным является использование случайных данных и равномерность исходных данных для выполнения требований предъявляемых к статистической составляющей парольной и адресной части КД пользователя.

Пример трансформации исходных данных, получаемых от аналогового генератора шума, традиционно распределенных нормально, в массив с равномерным распределением с использованием треугольного отображения показан на рисунке 2. В качестве трансформации используется для каждого элемента массива n итераций треугольного отображения.

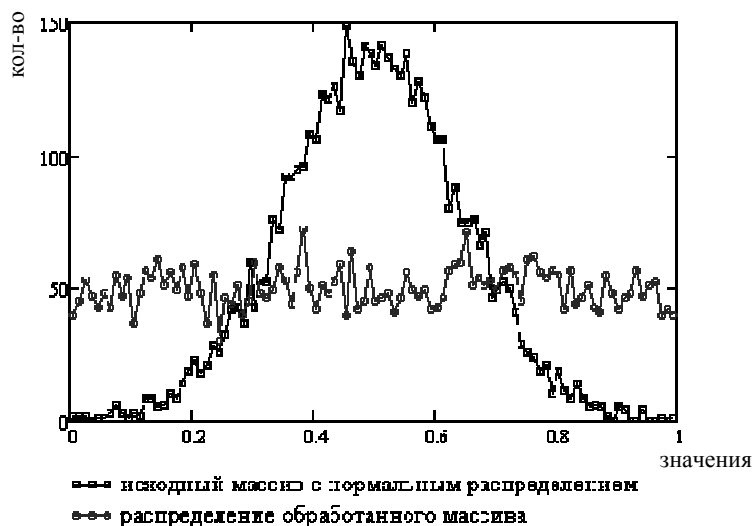


Рис. 2. Распределения исходного и обработанного массивов

Разработана математическая модель УГКД $M_{сч} = C(S_{||i}(B(G(\cdot))))$, где $i \in \mathbb{N}$; $C(\cdot)$ – функция накопления и преобразования получаемых действительных чисел в битовый массив с сохранением в энергонезависимой памяти; $S_{||i}(\cdot)$ – функция параллельных для элементов входного массива преобразований чисел с использованием треугольного отображения с параметром $1-10^{-6}$; $B(\cdot)$ – функция накопления битов информации и преобразования в массив действительных чисел в интервале $[0; 1)$; $G(\cdot)$ – функция генерации шумовых битов с использованием оцифровки сигнала с генератора шума. На основе математической модели УГКД разработана *структурно-функциональная организация специализированного вычислительного устройства генерации КД* (рис. 3). УГКД включает блоки: ПДЧ, П№1-П№N, УР. Блок ПДЧ (преобразования в действительные числа) осуществляет выборку из Блока ЗУ (запоминающего устройства) битов, инициализированных Бло-

ком АЦП (аналогово-цифровой преобразователь), и преобразование их в действительные числа с сохранением в Блоке ЗУ. Далее под управлением Блока контроллера обмена исходные действительные числа из Блока ЗУ передаются на параллельную предобработку в Блоки П №1 ... П №N (преобразование с использованием треугольного отображения), которые осуществляют преобразование действительных чисел с использованием хаотического перемешивания и сохраняют результат в Блоке ЗУ. Блок УР (управления результатами) преобразовывает результирующие действительные числа в массив битов и сохраняет их в ЭСППЗУ (электрически стираемое перепрограммируемое ПЗУ). Блок интерфейса PCI по команде пользователя осуществляет чтение ЭСППЗУ и передачу случайной битовой последовательности для прикладного использования.

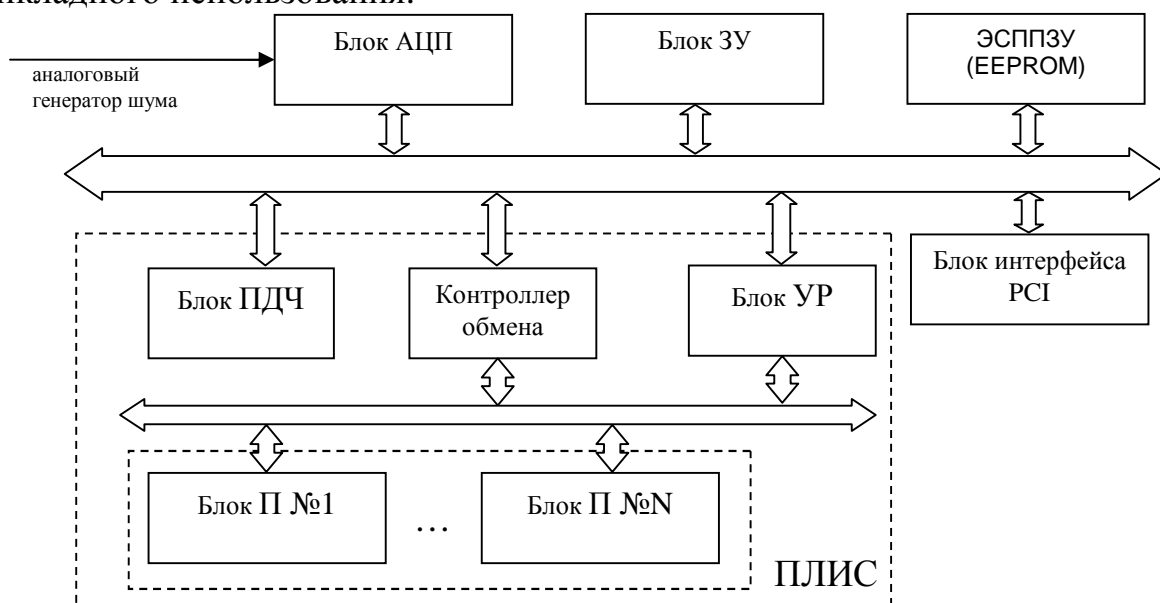


Рис. 3. Структурно-функциональная организация устройства генерации ключевых данных

Основополагающим в работе устройства является использование параллельно исполняющихся Блоков П, каждый из которых представляет собой десятиступенчатый конвейер, на каждой ступени которого вычисляется описанная во второй главе функция треугольного отображения с параметром r (рис. 4,5). Повышение оперативности автоматической модификации ключевых данных основывается на разделении функции работы, с одной стороны, блоков АЦП и ПДЧ и, с другой стороны, N блоков П. Кроме того, реализация N блоков П, Блока УР и контроллера обмена в рамках одной ПЛИС на выделенной шине также позволяет снизить затраты времени на обмен между ПЛИС и Блоком ЗУ.

Операционная часть УГКД реализована на базе программируемой логической интегральной схемы (ПЛИС) Virtex 6 XC6VLX130T, генератора 50МГц, 528 RAM 18Kb, работающей на частоте ПЛИС, что позволяет получить на серверной части системы технические решения с высокой надежностью функционирования, минимальными массогабаритными, энергетическими показателями. Устройство ГКД устанавливается в стандартную шину

PCI компьютера, с которого производится загрузка рабочих конфигураций ПЛИС. Выходные данные забираются из устройства посредством стандартного контроллера PCI с использованием режима прямого доступа к памяти (ПДП). Для взаимодействия с операционной системой Windows написан драйвер, обеспечивающий процедуры инициализации и передачи данных.

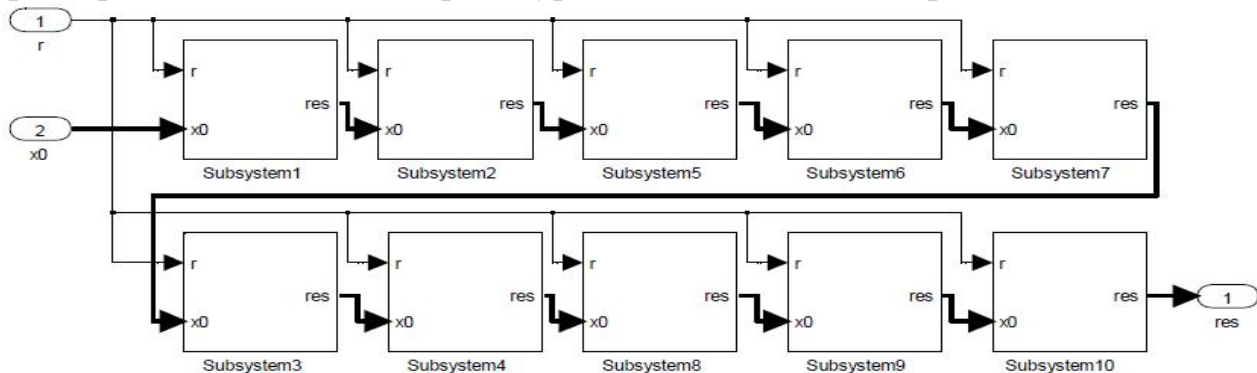


Рис. 4. Функциональная схема Блока II

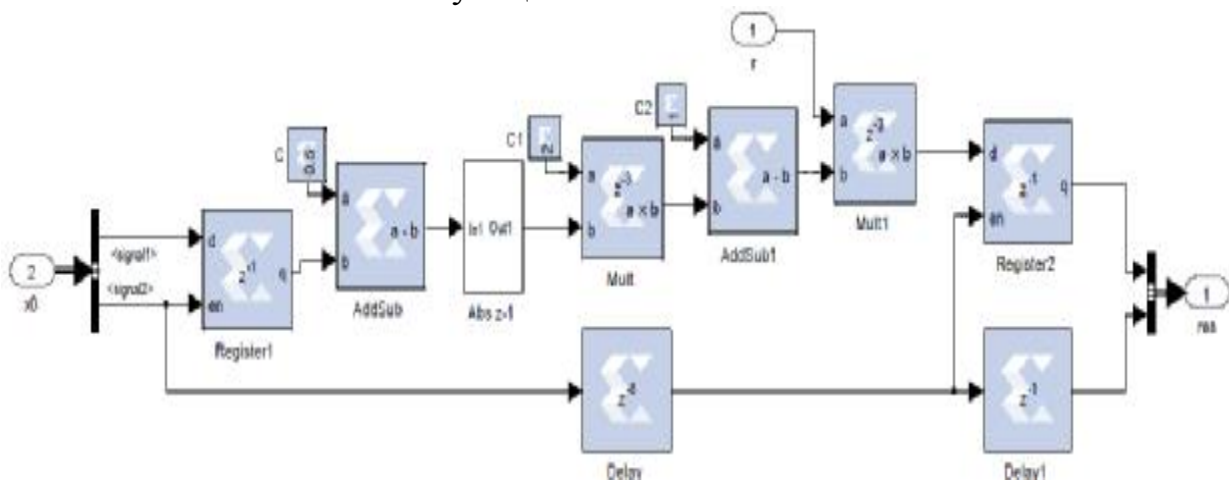


Рис. 5. Функциональная схема Блока дискретного треугольного отображения

В диссертационной работе для целей поддержки адресации распределения разработан *способ адресной доставки*, в котором осуществляются следующие операции.

1. Подтверждение адресата по текущему значению адресной части КД с формированием инициализационных значений для АП.
2. Преобразование с использованием АП передаваемых новых КД.
3. Преобразование полученных данных с использованием обратного АП с проверкой соответствия отправителю.

Для реализации данного способа разработан детерминированно-хаотический генератор на основе треугольного отображения. Важной особенностью и отличием предлагаемого способа и устройства является то, что в детерминированно-хаотическом генераторе в качестве стартового значения, являющегося частью адресной составляющей КД, принимается значение x_0 и параметр r . Кроме того в целях противодействия восстановлению адресной составляющей КД используется механизм срыва детерминированно-хаотической траектории генератора. Для этого один раз в K итераций гене-

ратора выполняется операция $x_{n+1} = x_n + 0.1$ для $x_n < 0.5$ и $x_{n+1} = x_n - 0.1$ для $x_n \geq 0.5$, где $K \hat{I} [80; 100]$ для предотвращения разглашения информации о положении более 100 подряд идущих точек траектории.

С использованием разработанного генератора псевдослучайных чисел разработано прямое АП, основанное на схеме, показанной на рис. 6-а.

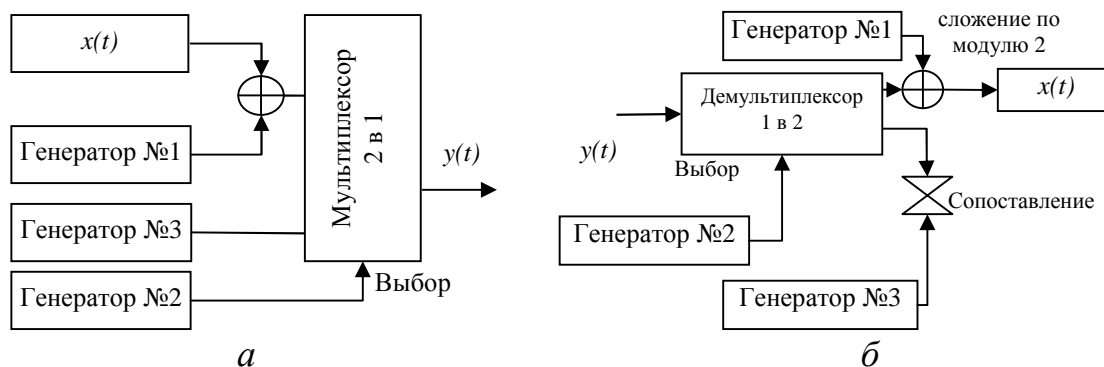


Рис. 6. Схема акцессорного преобразования

В АП использовано три разработанных генератора. Выходная последовательность генератора №1 совмещается с исходными данными с применением операции сложения по модулю 2; генератор №3 является источником прореживающих шумовых и вместе с тем проверочных данных; и генератор №2 выбирает один из двух указанных источников.

Для восстановления данных используется схема обратного акцессорного преобразования (рис. 6-б). В схеме обратного преобразования входная последовательность данных с использованием значения генератора №2 разделяется на два потока. Первый поток восстанавливается до исходных данных с использованием генератора №1 и применением операции сложения по модулю 2, а второй сопоставляется со значениями генератора №3. При обнаружении несоответствия в блоке сопоставления принимается решение о нарушении адресации полученных данных и процесс обратного преобразования прекращается с уведомлением администратора.

Для реализации первого этапа способа разработан алгоритм проверки подтверждения адресата на основе конечного числа тестов с использованием формирования по адресной части КД случайно-подобной последовательности. Алгоритм состоит в выполнении серии тестов. Каждый тест алгоритма является этапом подтверждения адресата. Тест основан на проверке знания подтверждающей стороной i -ого значения детерминировано-хаотического генератора и состоит из следующих шагов:

- проверяющая сторона определяет номер i проверяемой позиции генератора, вычисляет значение генератора в данной позиции и передает номер i проверяемой стороне;
- проверяемая сторона производит вычисление значения генератора в данной позиции i и передает его проверяющей стороне;

– проверяющая сторона производит сравнение вычисленного и полученного значения, при их равенстве алгоритм переходит к следующему тесту, иначе принимается решение о несоответствии адресата.

Проверочный генератор представляет собой объединение трех разработанных генераторов на основе треугольного отображения и выходного мультиплексора, подобного описанному в схеме АП. Вследствие применения мультиплексора на выходе появляется неопределенность принадлежности значения конкретному генератору, что усложняет подбор адресной составляющей КД для ложного подтверждения адресата.

Для выполнения одноразового подтверждения адресата необходимо подобрать n ответов для каждого из n этапов алгоритма, вероятность данного события уменьшается до приемлемого указанием администратором числа этапов, минимум которого установлен значением 128. Проверяющей стороной для каждого этапа выбирается каждый раз новая проверочная позиция, отстоящая от использованных не менее чем на M итерации, где значение M должно быть не меньше 3. При этом алгоритм подтверждения адресата выбирает последние три проверяемые позиции, и они становятся начальными позициями, используемыми в генераторах схемы АП, что является важной особенностью способа адресной доставки.

Далее в разделе рассматриваются способы подтверждения адресата пользователем, у которого нет в наличии адресной составляющей КД, и указывается высокая сложность их реализации. Единственной стратегией получения новых КД пользователя является подбор значения адресной части КД, что в силу приведенных выше положений эквивалентно полному перебору значений. Для противодействия подмене клиента вводится блокировка учетной записи при возникновении отказа в этапе подтверждения адресата.

В заключительной части раздела выполнена разработка архитектуры многоабонентской распределенной системы управления КД, которая приведена на рисунке 7.

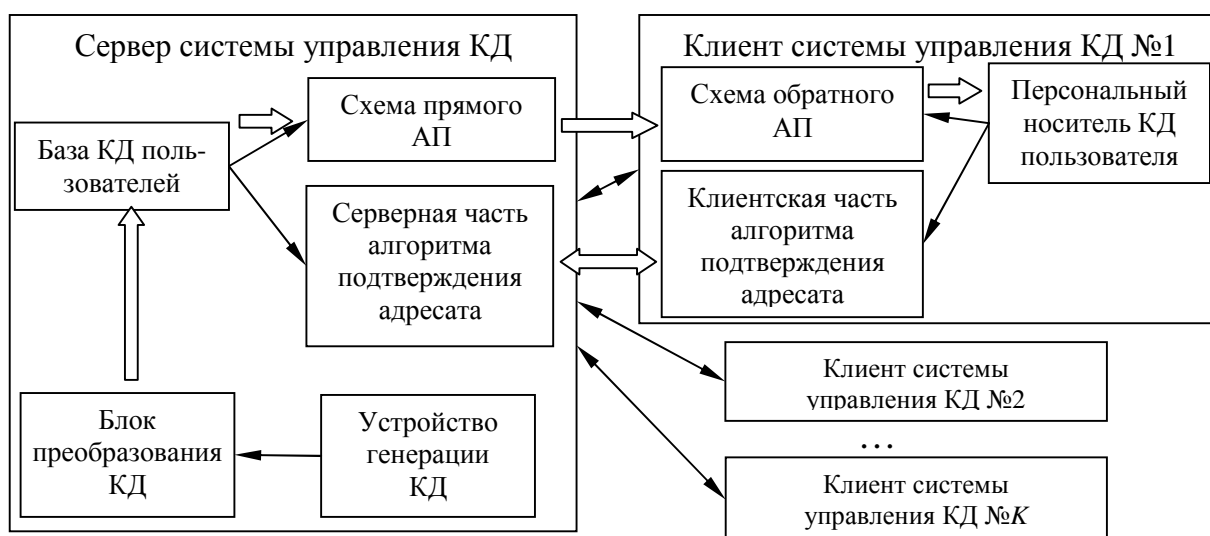


Рис. 7. Архитектура многоабонентской распределенной системы управления КД

Особенность архитектуры системы определяется клиент-серверной структурой и предложенным распределением функций. По всем ЭВМ организации распределяется приложение «Клиент СМиАД КД», запускается и контролируется работоспособность приложения «Сервер СМиАД КД». В сервере системы управления КД расположены: база данных пользователей, содержащая информацию о правах доступа каждого из них к ресурсам РВС, персональные КД и сроки их актуальности; устройство генерации КД; компоненты реализации способа адресной доставки. Клиент системы управления КД используется совместно с персональными КД пользователя, хранящимся на индивидуальном носителе информации, и также содержит компоненты для реализации способа адресной доставки.

Предлагаемая совокупность алгоритмов, устройства и компонентов архитектуры представляют собой целостную систему, позволяющую реализовать логически состоятельную и приемлемую для практики СМиАД с заявленными свойствами.

В четвертой главе приведены результаты практической реализации разработанных устройства и алгоритмов. Проект разработанного устройства генерации КД выполнен в среде MathWorks® Simulink и Xilinx ISE Design Suite 13.2. В среде MathWorks® Simulink проведено имитационное моделирование разработанных блоков устройства. Драйвер взаимодействия с устройством генерации КД выполнен в среде Microsoft Visual Studio 2003 + DDK. Для предложенных способа и алгоритмов выполнена реализация с использованием средств интерактивной среды разработки Borland® С++Builder®. При реализации был выбран язык программирования высокого уровня С++ с возможностью обособления значимых объектов предметной области в классы.

Экспериментальная оценка характеристик разработанной системы состояла в проведении оценки задействованных ресурсов ПЛИС (таблица 1), статистического тестирования разработанного генератора, сравнительного анализа скорости выполнения предложенной схемы АП с аналогами, оценки изменения нагрузки на администратора при использовании СМиАД.

Таблица 1

Использование ресурсов ПЛИС XC6VLX130T

Ресурс	Модуль преобразования	Модуль интерфейса PCI	Контроллер обмена	Доступно	Процент использования
RAM 18 Кб	34	24	39	480	20%
Регистры	72000	1592	7800	160000	51%

В статистическом тестировании использовался набор тестов позволяющих определить степень подобия генерируемой последовательности истинной случайной последовательности. Использовались следующие тесты: частотный, автокорреляционные, последовательные, выявление серий. Ста-

статистика частотного теста $f_q(s^N) = \frac{2}{\sqrt{N}} \left(\sum_{i=1}^N s_i - \frac{N}{2} \right)$ при $N \geq 30$ согласуется с нормальным распределением с нулевым средним и единичной дисперсией с приемлемыми порогами $t_1 = -t_2 \approx 2,5 \div 3,0$. Автокорреляционным тестом с задержкой t является частотный тест для $s_t^N = (s_1 \oplus s_{1+t}, s_2 \oplus s_{2+t}, \dots, s_{N-1} \oplus s_N)$. Последовательный тест с параметром L разбивает s^N на N/L отрезков длины L и определяет частоту n_i появления двоичного представления целого числа i : $(0 \leq i \leq 2^L - 1)$. При длине последовательности более $5L \cdot 2^L$ статистика последовательного теста $f_n(s^N) = \frac{L \cdot 2^L}{N} \sum_{i=0}^{2^L-1} \left(n_i - \frac{N}{L \cdot 2^L} \right)^2$ согласуется с распределением χ^2 -квadrat с $2^L - 1$ степенями свободы. Тест серий определяет число 1-серий $z_{1,r}$ ($x_i = x_{i+r+1} = 1$) и 0-серий $z_{0,r}$ ($x_i = x_{i+r+1} = 0$) длины $1 \leq r \leq L$ (например, $L = 15$), где $i \in \{0, 1, \dots, T-1\}$ и индексы рассматриваются по модулю T . Статистика теста $f_c(s^N) = \sum_{r=1}^L \frac{(z_{1,r} - N / 2^{r+2})^2}{N / 2^{r+2}} + \sum_{r=1}^L \frac{(z_{0,r} - N / 2^{r+2})^2}{N / 2^{r+2}}$ согласуется с распределением χ^2 -квadrat с $2L$ степенями свободы.

В результате при изменяемом параметре объема генерации получено, что из общего количества тестов $9801 \cdot 22 = 215622$ было выявлено невыполненных 962 теста (для $8 \cdot 10^3$ бит генерации) и невыполненных 1238 теста (для $8 \cdot 10^4$ бит), что согласуется с результатами аналогичного тестирования истинно случайного генератора. На основе этого делается вывод о возможности использования разработанного генератора в генерации адресной и паролльной части КД.

В работе проведен сравнительный анализ скорости выполнения предложенной схемы АП с алгоритмами для осуществления последующей перекодировки известными средствами. В качестве прототипов выбраны обработка с применением схемы кодировки по технологии AES с разными режимами: режим электронной книги, режим сцепления блоков, режим счетчика.

Таблица 2

Результаты сравнительного анализа времени преобразований

	Треугольное отображение <i>разработка</i>	AES Режим электронной книги	AES Режим сцепления блоков	AES Режим счетчика
10^5 байт Время, с	0.046	0.447	0.421	0.428
10^6 байт Время, с	0.433	4.244	4.255	4.254

Тестирование производилось со следующими исходными параметрами операционной среды: однопотокное исполнение алгоритмов; процессор Intel® Core™ i7 860 @ 2.8 GHz; 2.9 Гб ОЗУ. В качестве изменяемого параметра был принят объем данных. В качестве основного оценочного параметра был принят интервал времени необходимый для обработки данных заявленного объема. Результаты, приведенные в таблице 2, достаточно удовлетворительно согласуются с предварительными оценочными интервалами. Установлено, что разработанная схема акцессорного преобразования с использованием треугольного отображения выполняется с меньшими *на один порядок* затратами времени чем различные вариации схемы AES, что позволяет охарактеризовать разработанное преобразование как высокоскоростное и подтвердить возможность его использования перед применением методов стандартизированного шифрования.

Общая оценка скорости выполнения преобразования с использованием треугольного отображения с учетом использования её в сетевых распределенных системах является приемлемой при условии, что скорость выполнения преобразования имеет *один порядок* с общедоступной скоростью передачи данных в РВС (≈ 8 Мбайт/с).

Для оценки изменения нагрузки на администратора при использовании СМиАД использовалась методика С.П. Гржибовского. Среднее месячное количество рабочих часов (T_p) при еженедельной смене КД операцией занимающей 20 минут в РВС на 100 пользователей равно 120 нормо-часов. С использованием СМиАД на поддержание работоспособности затрачивается 10 нормо-часов/месяц при уровне автоматизации 85%. Трудоемкость обработки $T_m = T_p \cdot (100 - U_m) / 100 + T_{vy}$, где U_m – уровень автоматизации; T_{vy} – трудоемкость поддержания работоспособности СМиАД. $T_m = 120 \cdot (100 - 85) / 100 + 10 = 28$. Снижение трудовых затрат ($T_{ac} = T_p - T_m = 92$) в $120/28 \approx 4.3$ раза. В СМиАД операция смены КД выполняется 3 минуты, что дает повышение оперативности в 7 раз. С увеличением количества пользователей РВС увеличивается T_{ac} , что дает основание полагать, что использование СМиАД в РВС уменьшает нагрузку на администратора.

В заключении сформулированы научные и практические результаты исследования.

В приложении приведены результаты выполнения статистического пакета тестов для проверки последовательности порождаемой генератором с указанием инициализационных значений генератора, длины генерируемой последовательности и результатов прохождения каждого теста, а также листинг важных фрагментов проектов программных и аппаратных средств.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В диссертационной работе решена научная задача разработки средств генерации и адресной доставки ключевых данных с использованием дискретного детерминировано-хаотического отображения.

В ходе решения этой задачи получены следующие основные результаты.

1. Разработана структурно-функциональная организация специализированного вычислительного устройства генерации ключевых данных пользователя, отличающегося использованием аналогового генератора шума и его суперпозицией с треугольным дискретным отображением, имеющим линейную вычислительную сложность, что позволяет генерировать детерминированно-хаотическую последовательность аппаратными средствами.
2. Получена параллельно-конвейерная организация операционной части специализированного вычислительного устройства генерации ключевых данных, реализованная на программируемой элементной базе (ПЛИС Virtex 6 XC6VLX130T), что позволяет проектировать технические решения с высокой надежностью функционирования, минимальными массогабаритными, энергетическими показателями.
3. Разработан метод динамической модификации (генерация, доставка, запись на персональный носитель) ключевых данных пользователей, отличающийся введением шага предобработки исходных данных, традиционно имеющих нормальный закон распределения, в массив с равномерным распределением на основе применения n итераций треугольного отображения для каждого элемента исходных данных. Метод позволяет уменьшить административную нагрузку и повысить надежность выбираемой для каждой конкретной организации сторонней системы защиты информации за счет автоматизации процессов распределения ключевых данных.
4. Разработан способ адресной доставки ключевых данных пользователю, отличающийся использованием акцессорного (прямого-обратного) преобразования на основе мультиплексора и демultipлексора управляемых хаотическим генератором «треугольное отображение», что позволяет автоматически шифровать и дешифровать передаваемые данные с подтверждением адресации. Произведено сравнение скорости выполнения разработанного акцессорного преобразования с прототипами, результаты которого характеризуют разработанный алгоритм как высокоскоростной, с преимуществом над аналогами до одного порядка, что позволяет использовать его в многоабонентских распределенных системах управления.
5. Создана архитектура многоабонентской распределенной системы управления ключевыми данными, разграничивающей в клиентской и серверной частях функции акцессорного преобразования, генерации, адресной доставки и сохранения ключевых данных, что обосновывает возможность аппаратной реализации отдельных ее функций на сервере и приводит к повышению оперативности автоматической модификации ключевых данных.
6. Результаты практического использования разработанной системы подтвердили уменьшение нагрузки на администратора рассмотренной РВС в 4.3 раза и повышение оперативности смены ключевых данных в 7 раз для каждого пользователя по сравнению с системами, использующими руч-

ные операции администратора и набор специализированных утилит. Статистические тесты последовательностей, порождаемых разработанным генератором, удовлетворяют истинно случайному генератору на 99,5% по показателю выполнимости, что делает возможным его использование в оперативном получении индивидуальных КД для пользователей многоабонентских распределенных систем управления.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи в рецензируемых научных журналах и изданиях

1. Борисов, А.И. Автоматизация процедуры периодической модификации и адресной доставки ключевых конструкторов / А.И. Борисов // Вестник Воронежского государственного технического университета. 2011. Том 7. №3. С.138-140.
2. Борисов, А.И. Свойства треугольного отображения в системах управления документами / А.И. Борисов, В.М. Довгаль // Вестник Воронежского государственного технического университета. 2010. Том 6. №6. С.73-74.
3. Борисов, А.И. Использование хаотических свойств треугольного отображения в системах управления документами / А.И. Борисов, В.М. Довгаль // Известия Юго-Западного государственного университета. 2010. №4 (33). С.34-38.

Публикации в других изданиях

4. Борисов, А.И. Устройство генерации последовательности случайных двоичных чисел с использованием хаотического дискретного отображения / А.И. Борисов, А.С. Сизов // Научно-технический сборник трудов НИЦ (г.Курск) ФГУП «18 ЦНИИ» МО РФ. 2011 г. №2 (176). С.32-35
5. Борисов, А.И. Система управления документооборотом с блоком генерации числовой последовательности на основе логистического отображения / А.И. Борисов, Д.Л. Жилиев, В.М. Довгаль, В.В. Гордиенко, В.В. Малых // Физические и компьютерные технологии: Труды 15-й Международной научно-технической конференции, 2-3 декабря 2009г. Харьков: ХНПК «ФЭД». 2009. С.476-478.
6. Борисов, А.И. Хаотические последовательности, порождаемые итерируемой функцией «Треугольное отображение» для систем управления документами / А.И. Борисов, Д.Л. Жилиев, В.М. Довгаль, В.В. Гордиенко, В.В. Малых // Физические и компьютерные технологии: Труды 15-й Международной научно-технической конференции, 2-3 декабря 2009г. Харьков: ХНПК «ФЭД». 2009. С.469-471.
7. Борисов, А.И. Обзор программных средств криптографии и стеганографии с использованием псевдослучайных и хаотических процессов / А.И. Борисов, В.В. Гордиенко // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2008: сб. материалов VIII Междунар. конф. Ч.1 Курск: КГТУ, 2008. С.75-76.

8. Борисов, А.И. Защита информации в социальной системе и походы к проектированию поточного шифра / А.И. Борисов, В.М. Довгаль, Д.Л. Жилиев, В.В. Гордиенко, И.В. Ильин // Васильевские чтения. Ценности и интересы современного общества: Материалы II международной научно-практической конференции. Часть I. 10 ноября 2008 г. Курск: Курский филиал РГТЭУ. 2008. С.63-66.
 9. Борисов, А.И. Электронная цифровая подпись как средство оптимизации процессов электронного документооборота в социально-экономической системе общества / А.И. Борисов, В.М. Довгаль, Д.Л. Жилиев, В.В. Гордиенко, И.В. Ильин // Васильевские чтения. Ценности и интересы современного общества: Материалы II международной научно-практической конференции. Часть I. 10 ноября 2008 г. Курск: Курский филиал РГТЭУ. 2008. С.302-306.
 10. Борисов, А.И. Анализ методов проектирования вычислительных элементов для мониторинга геоинформационной системы // Материалы 28 ВНК (Курск, 5-7 октября 2008г.) Издание ФГУП «Курский НИИ» МО РФ. 2008. С.62-66.
 11. Борисов, А.И. Синтез элементов распределенной системы // Материалы 28 ВНК (Курск, 5-7 октября 2008г.) Издание ФГУП «Курский НИИ» МО РФ. 2008. С.58-62.
- Свидетельство об официальной регистрации*
12. Борисов, А.И. Программный компонент для статистического тестирования псевдослучайной последовательности чисел, порождаемой хаотическим генератором / А.И. Борисов, В.М. Довгаль // Свидетельство о государственной регистрации программы для ЭВМ №2009613768. заявл. 26.05.2009. рег. 15.06.2009.

Подписано в печать ____2012. Формат 60x84 1/16.
Печатных листов 1,1 . Тираж 120 экз. Заказ _____.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.