**УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ "БЕЛОРУССКИЙ ГОСУДАРСТВЕНЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ"**

**УДК 681.3.05; 681.324.067; 681.325.3**

**ПАЦЕЙ**

**Наталья Владимировна**

# МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ И АЛГОРИТМЫ ФУНКЦИОНИРОВАНИЯ УСТРОЙСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ КРИПТО-КОРРЕКТИРУЮЩИХ ПРЕОБРАЗОВАНИЙ

Специальности 05.13.05 - Элементы и устройства вычислительной техники и систем управления,
05.13.15 – Вычислительные машины и системы

Автореферат диссертации
на соискание ученой степени кандидата технических наук

МИНСК 2001

Работа выполнена в Белорусском государственном технологическом университете.

Научный руководитель –

д.т.н., проф. Урбанович П.П.,
кафедра Информатики и
вычислительной техники, БГТУ

Официальные оппоненты:

д.т.н., проф. Петровский А.А.,
кафедра Электронных
вычислительных средств, БГУИР

к.т.н. Анищенко В.В.,
НИО "Кибернетика" НАН Беларуси

Белорусский государственный
университет

Защита состоится 20 декабря 2001 г. в 15 часов на заседании совета по защите диссертаций Д 02.15.01 в Учреждении образования "Белорусский государственный университет информатики и радиоэлектроники" по адресу: 220027, г.Минск, ул. П. Бровки, 6, БГУИР, 1 уч. корпус, ауд. 232, тел.239-89-89.

С диссертацией можно ознакомиться в библиотеке Учреждения образования "Белорусский государственный университет информатики и радиоэлектроники".

Автореферат разослан 19 ноября 2001 г

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

***Актуальность темы диссертации.*** Защита информации не является новой областью научных исследований и практических разработок. Первые теоретические и прикладные работы в этом направлении появились достаточно давно. С расширением сферы применения компьютерных технологий в предпринимательской деятельности и в области банковских технологий проблема защиты информации стала выходить за рамки традиционных исследований и разработок.

В республике ведутся достаточно интенсивные исследования по разработке новых алгоритмов и систем криптозащиты (Государственный центр безопасности информации, Институт технической кибернетики НАНБ, НИИ Проблем защиты информации, БГУ и др.), однако при этом, как правило, не принимается во внимание надежность элементной базы, реализующей эти алгоритмы, и влияние используемых каналов передачи на целостность конфиденциальной информации. Из анализа доступных литературных источников следует, что как в странах СНГ, так и за их пределами практически не проводятся исследования, в комплексе рассматривающие надежность каналов и аппаратуры шифрования/дешифрования передаваемых сообщений с алгоритмами криптопреобразований.

Вместе с тем, наблюдаемое в последние годы резкое увеличение информационных потоков и связанное с этим ужесточение требований к целостности обрабатываемой информации обострили проблему надежной передачи конфиденциальной информации. Таким образом, разработка методов и алгоритмов, обеспечивающих конфиденциальность, а также помехо- и отказоустойчивость данных, является актуальной научно-технической задачей.

***Связь работы с крупными научными программами, темами.*** Выполнение работ в данном направлении соответствует республиканской научно-технической программе "Информатика" (Постановление комиссии Президиума Совета Министров Республики Беларусь по вопросам научно-технического прогресса, протокол №5/116 от 30 июня 1992 года). Исследования проводилось в рамках научно-исследовательских госбюджетных тем №ГР 19971627 “Теоретические основы прогнозирующего расчета надежности канала, синтеза специализированных корректирующих кодов и устройств кодирования/декодирования информации в защищенных компьютерных сетях” (1997-1998гг.) и №ГР 19991132 “Разработать методы и алгоритмы функционирования отказоустойчивых систем передачи и устройств криптографического преобразования информации для сетей телекоммуникаций” (1999-2000гг.), выполненных на кафедре Информатики и вычислительной техники БГТУ.

***Цель и задачи исследования.*** Целью работы является создание и исследование новых эффективных методов защиты информации в

компьютерных сетях на основе криптопреобразований и избыточного кодирования данных, обеспечивающих повышенный уровень надежности устройств криптографической защиты.

В соответствии с поставленной целью в диссертационной работе решаются следующие основные задачи:

- проведение экспериментального исследования и анализ характера распределения отказов в устройствах криптографического преобразования информации и ошибок в дискретных каналах передачи данных;
- разработка методов построения отказоустойчивых криптографических устройств защиты информации с учетом полученных статистических характеристик сбоев и отказов аппаратуры преобразования;
- разработка крипто-корректирующих алгоритмов преобразования информации, обеспечивающих повышенную надежность, целостность информации и адаптированных под реальную помехоустойчивость каналов передачи данных;
- оценка эффективности крипто-корректирующих устройств защиты информации, построенных на основе разработанных методов и алгоритмов.

***Объект и предмет исследования.*** Объектом исследования являются современные устройства криптографического преобразования информации. Предмет исследования – методы и алгоритмы повышения надежности этих устройств.

***Методология и методы проведенного исследования.*** При исследовании использовались методы анализа и синтеза крипто-корректирующих устройств на основе вероятностно-статистического и имитационного моделирования, а также математический аппарат теории помехоустойчивого кодирования, криптологии, теории надежности и эксперимент.

***Научная новизна и значимость полученных результатов.***

1. Экспериментально обоснована необходимость использования методов корректирующего кодирования данных в криптографических системах. Установлены характер распределения ошибок и зависимость распределения вероятности появления ошибок в телефонных каналах передачи дискретной информации от времени.
2. Впервые исследовано влияние отказов элементной базы криптосхем на достоверность преобразования информации, что позволило определить требования к отказоустойчивым криптоустройствам.
3. Созданы новые методы построения устройств криптографического преобразования информации, основанные на использовании кодовых методов обнаружения и исправления ошибок и обеспечивающие отказоустойчивость и надежность преобразования данных.
4. Разработаны новые методы построения и алгоритмы функционирования крипто-корректирующих устройств и систем защиты информации, основанные на интеграции корректирующего кодирования и

криптографических преобразований, позволяющие повысить эффективность обработки критической информации при высоком уровне помех. Предложены структурно-функциональные схемы крипто-корректирующих устройств.

5. Теоретически обоснована и доказана относительная эффективность использования разработанных крипто-корректирующих устройств в составе систем защиты информации.

***Практическая значимость полученных результатов.*** Результаты работы получены и реализованы в рамках ряда госбюджетных работ (ГБ 97-025 № ГР19971627, ГБ 78-95, ГБ 99-027 № ГР19991132, ГБ 21-064), выполненных на кафедре Информатики и вычислительной техники Белорусского государственного технологического университета.

На основе предложенных в работе решений:

- разработаны практические рекомендации по обеспечению повышенного уровня отказо- и помехоустойчивости устройств и систем защиты информации при ее хранении, преобразовании и передаче;
- сформулированы принципы построения отказоустойчивых криптографических схем, адаптированных на применение в составе современных устройств и систем защиты информации;
- разработаны структурные схемы крипто-корректирующих устройств защиты информации, снижающие вероятность возникновения ошибок при передаче и хранении конфиденциальной информации.

Полученные результаты использованы в учебном процессе по курсу "Основы информационных технологий" для аспирантов по кафедре Информатики и вычислительной техники БГТУ и Управлением прикладных и системных разработок УП "Центр Банковских Технологий", а также внедряются в управляющие подсистемы удаленного доступа и протоколы программного обеспечения служебного пользования глобальной национальной сети передачи данных РБ БелПак РО “БелТелеком”.

***Основные положения диссертации, выносимые на защиту.***

1. Результаты имитационного моделирования влияния отказов криптографических схем и ошибок каналов связи на достоверность преобразования и передачи информации.

2. Результаты экспериментального исследования характера распределения ошибок в системах передачи данных, позволяющие оптимизировать информационную и аппаратную избыточность в устройствах и системах криптографической защиты данных.

3. Методы построения и алгоритмы функционирования отказоустойчивых устройств криптографического преобразования, основанные на использовании кодовых методов обнаружения и исправления ошибок, позволяющие повысить надежность этих устройств.

4. Методы построения и системотехнические решения крипто-корректирующих систем, основанные на принципе взаимодополнения

криптографических преобразований помехоустойчивым кодированием данных, обеспечивающие конфиденциальность и целостность обрабатываемой информации.

***Личный вклад соискателя.*** Все новые результаты, изложенные в диссертационной работе, получены автором самостоятельно. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертации результатов.

***Апробация результатов диссертации.*** Основные положения и результаты диссертационной работы докладывались и обсуждались на следующих конференциях: Второй и Третьей международной конференции "Новые информационные технологии в образовании" (Минск, 1996, 1998); I, II Республиканские научно-практические конференции "Комплексная защита информации: проблемы и решения" (РСК "Раубичи", 1997, 1998); I, III МНТК "Автоматический контроль и автоматизация производственных процессов" (Минск, 1998, 2000); 62-ой и 63-ей НТК БГТУ (Минск, 1998, 1999); Третьей международной конференции "Новые информационные технологии в науке и производстве" (Минск, 1998); IV МНТК "Современные средства связи" (Нарочь, 1999); II International Conference on Computer Methods and Inverse Problem in Nondestructive Testing and Diagnostic (Berlin-Minsk, 1998); Information System for Enhanced Public Safety and Security (Munich, 2000); International symposium New Electric and Electronic Technologies and their industrial implementation (Lublin, 2001).

***Опубликованность результатов.*** По результатам выполненных исследований опубликовано 16 печатных работ, в том числе 6 статей, 10 тезисов докладов и материалов конференций, подано 2 заявки на патент Республики Беларусь. Общее количество опубликованных материалов составляет 51 стр., из них автору диссертации принадлежит 37 стр. Без соавторов опубликовано 2 работы.

***Структура и объем диссертации.*** Работа изложена на 93 страницах машинописного текста, иллюстрирована 58 рисунками, содержит 15 таблиц; состоит из общей характеристики работы, четырех глав, заключения, приложений и списка использованных источников, включающего 233 отечественных и зарубежных источника. Общий объем работы – 162 страницы.

## ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

В **первой главе** диссертации рассмотрены основные методы и средства обеспечения конфиденциальности и целостности информации в системах передачи данных.

Линии связи - один из наиболее уязвимых компонентов вычислительной системы. Существующее разнообразие протоколов и средств обеспечения конфиденциальности информации на основе алгоритмов криптографического преобразования не в состоянии обеспечить целостность потока данных. Традиционно корректирующее кодирование, гарантирующее целостность информации, и шифрование, используемое для обеспечения конфиденциальности, применяются независимо и отдельно друг от друга.

Согласно анализу литературных источников, ни один из протоколов, стандартов и средств сетевого шифрования, ни одно отдельно взятое устройство или программный пакет шифрования не в состоянии решить проблему обеспечения и конфиденциальности, и целостности информации. Однако, активное воздействие на хранимую, обрабатываемую и передаваемую в ВС конфиденциальную информацию способно нарушить ее целостность.

Одной из причин нарушения целостности информации являются отказы цифровых схем аппаратуры преобразования данных. Адекватность исходного и полученного сообщений в значительной мере определяется надежностью функционирования аппаратных средств обеспечения конфиденциальности. Возникающие в процессе эксплуатации отказы и сбои схем не позволяют обеспечить высокую надежность преобразования данных.

Другим важным фактором нарушения целостности информации являются искажения, вносимые передатчиком и каналом передачи. Несмотря на обилие моделей, общепринятой модели источника ошибок не существует. По мере разработки и совершенствования моделей вопрос о целесообразности использования той или иной из них должен решаться в каждом конкретном случае отдельно.

Согласно приведенному обзору, в системах передачи данных (СПД) применяется логическое кодирование трех видов, используемых в разных целях. Это помехоустойчивое кодирование, шифрование и сжатие данных. Они отчасти дополняют друг друга и имеют общие механизмы преобразования данных.

Известны запатентованные реализации коммуникационных криптографических систем, основанные на использовании модулей коррекции ошибок. Условно такие методы и алгоритмы, в которых пересекаются помехоустойчивое кодирование и криптографические преобразования, можно разделить на четыре группы по способу взаимодействия используемых преобразований.

К первой группе относятся системы с последовательным применением схем кодирования и шифрования (либо в обратном порядке). Такое применение не дает существенных преимуществ перед методом использования коррекции ошибок и криптографии на разных уровнях ISO/OSI модели или в разных протоколах. Значительно эффективнее, с точки зрения повышения надежности, является вторая группа методов, основанная на добавлении в модули или системы криптографического преобразования логических схем проверки корректности работы. Основные недостатки - достаточно высокая схематическая избыточность и отсутствие механизмов исправления ошибок. Третья группа включает системы обеспечения конфиденциальности, построенные на основе элементов кодов коррекции ошибок или использующие механизмы помехоустойчивого кодирования. К четвертой группе относятся непосредственно системы интеграции корректирующих кодов и криптографического преобразования, обеспечивающие конфиденциальность и целостность информации. Данное направление слабо изучено и практически не имеет аналогов. Очевидно, что, несмотря на некоторые недостатки и не достаточную исследованность, существующие методы и алгоритмы считаются в последнее время перспективным направлением в области криптографической защиты информации.

Таким образом, существующее разнообразие протоколов и средств обеспечения конфиденциальности информации на основе алгоритмов криптографического преобразования не в состоянии обнаруживать и исправлять возникающие в процессе эксплуатации отказы и сбои аппаратных схем и искажения, вносимые каналом передачи данных. Установлено, что практически любая криптографическая система должна содержать дополнительные схемы контроля и коррекции выполнения преобразований, не замедляющие существенно ее работу.

**Во второй главе** проанализированы собранные статистические данные распределения ошибок передачи информации и влияния ошибок преобразования в криптографических системах для введения адекватной избыточности в оптимальных пределах.

Экспериментально исследовано свойство общей диффузии криптографических блочных алгоритмов, а именно: влияние случайных одиночных, двух-, трех- и четырехкратных ошибок, возникающих в каналах при передаче информации, зашифрованной с помощью симметричных криптографических систем MMB, 3-Way, IDEA, FEAL8, RC5 и Blowfish. Установлено, что вероятность искажения бит открытого текста при введении ошибок в шифротекст описывается схемой Бернулли и может быть представлена в следующем виде: $P(x) = C_n^x p^x (1-p)^{n-x}$. При доверительной вероятности $\gamma = 0.95$, интервальная оценка $p$ по экспериментальным данным: $0.49 \le p \le 0.51$. Тогда вероятность нахождения любого определенного числа изменений $b$ бит в $n$-битном блоке будет иметь следующий стандартный вид:

$$P(b) = \frac{\binom{n}{b}}{2^n} = \frac{n!}{2^n (n-b)! b!}.$$

Установлено, что расхождения между эмпирическими и теоретическими вероятностями не превышают уровня значимости $\alpha = 0.025$.

Анализ полученных данных показывает, что исследуемая зависимость характеризуется относительным постоянством, независимо от кратности вводимых ошибок. Согласно результатам проведенных исследований, при дешифрировании шифротекстов со случайным искажением бита (или бит) информации, приблизительно от одной до двух третей открытого текста оказывается искаженным. Фактически это означает потерю блока информации и является решающим аргументом в пользу добавления процедур коррекции ошибок в криптосистемы.

С целью исследования влияния отказов аппаратуры криптосхем на достоверность преобразования информации было проведено имитационное моделирование единичных сбоев различных функциональных элементов криптосхемы. Исследования проводились на модели криптосхемы ГОСТ 28147-89 в режиме простой замены.

Полученная функция вероятности $P_q$ искажения $q$ бит блока при сбое работы криптосхемы аппроксимируется тремя периодическими гармониками. Однако, для описания полученных данных через основные параметрические законы распределения, применяемые в теории надежности, удобнее перейти к рассмотрению смеси распределений. Тогда анализируемая генеральная совокупность будет состоять из смеси трех нормальных распределений (рис.1):

$$P(q) = 0.25 \frac{1}{3.06\sqrt{2\pi}} e^{\frac{-(q-16)^2}{18.72}} + 0.5 \frac{1}{2.66\sqrt{2\pi}} e^{\frac{-(q-32)^2}{14.15}} + 0.25 \frac{1}{3.08\sqrt{2\pi}} e^{\frac{-(q-48)^2}{18.97}}.$$

Полученные экспериментальные данные и статистические закономерности их распределения свидетельствуют о необходимости применения методов повышения эксплуатационной надежности криптосхем, таких как оптимальные методы отыскания неисправностей и прогнозирование сбоев и отказов с использованием оборудования контроля.

Для изучения статистических характеристик распределения ошибок и установления их соответствия известным характеристикам были протестированы синхронные и асинхронные выделенные телефонные каналы передачи дискретной информации и магистрали. Хотя испытания охватывали отдельные периоды, эти периоды были достаточно продолжительными для того, чтобы результаты испытаний можно было считать статистически достоверными. Установлено, что средняя вероятность ошибки не является

стабильной во времени и изменяется в диапазоне от $10^{-4}$ до $8*10^{-7}$, что подтверждает отмеченные в первой главе тенденции.

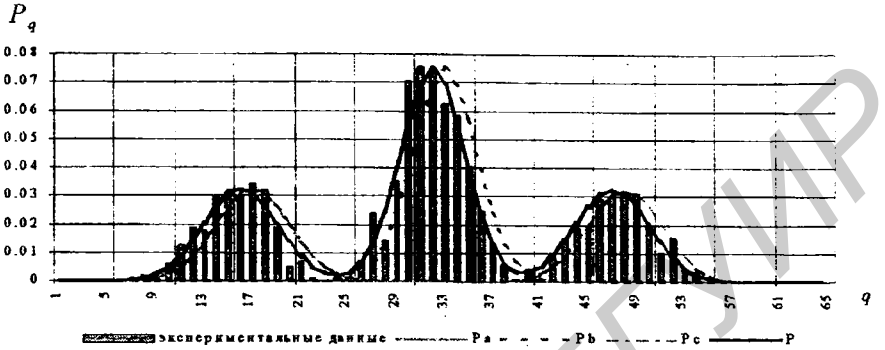


Рис.1. Гистограмма экспериментального и теоретических распределений вероятности искажения $q$ бит открытого текста при сбое регистра циклического сдвига

Так как в качестве передающей среды в последнее время наиболее часто используют телефонные каналы, то рассматривался именно этот класс линий. Согласно полученной статистике, случайные единичные ошибки составляют 34% из всех зарегистрированных в ходе тестирования каналов ошибок. Самые распространенные группы ошибок имеют размер 2 (18%) и 3÷4 (13%) бита. Около 64% составляют одиночные и группы ошибок в 2, 3 и 4 бита, 9% - ошибки от 5 до 10 бит, 15% - группы размером 11÷40 бит и 12% - свыше 40 бит. Все вышесказанное позволяет сделать вывод, что при передаче дискретной информации ошибки возникают неравномерно, и, как правило, носят случайный характер. Полученные результаты дают основание сформулировать требование к крипто-корректирующим системам защиты. Они должны исправлять случайные одиночные ошибки, а также пакеты ошибок длины от 2 до 10 бит.

Для выявления характера распределения ошибок во времени было протестировано около 45 различных телефонных каналов передачи данных. Испытания проводились в разное время, на линиях различной протяженности и скорости передачи, с использованием разных типов тестов. В качестве передающей среды использовался подземный медный кабель. Установлено, что в 36% случаев распределение вероятности появления ошибок постоянно во времени или наблюдается кратковременное увеличение числа ошибок, в 18% ошибки в линиях отсутствовали, а в 46% вероятность появления ошибок имела характерное распределение в зависимости от времени суток (рис.2).

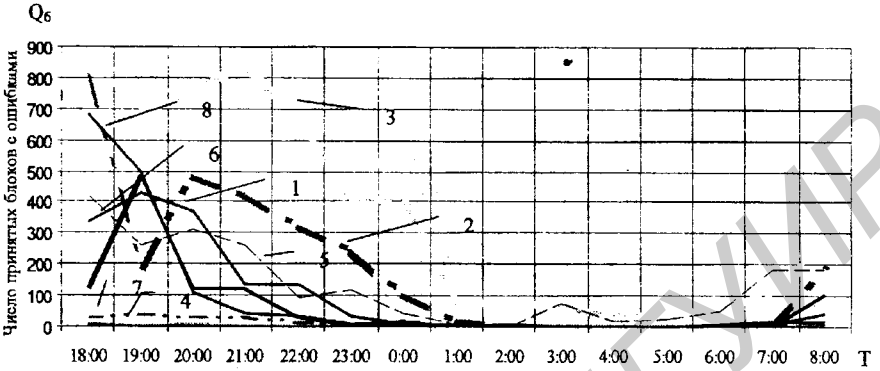


Рис.2. Распределение частоты ошибочно принятых блоков данных в зависимости от времени суток

Несмотря на разные даты испытаний, среднюю вероятность ошибки, протяженность каналов, на разную скорость передачи, размер блока и тип теста, наблюдается устойчивая картина распределения ошибок в зависимости от времени суток. Так на линиях, начиная с 23.00, средний коэффициент ошибок за час начинает уменьшаться; примерно с 1.00 до 6.00 ошибок становится значительно меньше, а с 7.00 уровень ошибок снова возрастает.

Таким образом, согласно статистическим данным, в большинстве тестируемых каналов в дневное время суток частота появления ошибочных битов увеличивается. Характер распределения ошибок свидетельствует о преобладающем влиянии внешних индустриальных помех, не возникающих в ночное время суток, на каналы передачи информации. Однако, достоверно определить источники зафиксированных в процессе измерений ошибок не удалось.

Исследования показали, что могут появляться одинарные ошибки и ошибки, называемые интенсивными, объединенные в пакеты с произвольной длительностью и структурой. Согласно ограничениям проведения эксперимента, наиболее правдоподобный результат дают показательная и гиперболическая полиномиальные модели. Испытываемые каналы математически можно описать как каналы со сложной аддитивной структурой помех (флуктуационной, импульсной). Эта модель наиболее полно описывает реальные каналы связи. Однако, ввиду ее сложности будем рассматривать исследуемые каналы как каналы с аддитивным гауссовским шумом - случайный процесс с нормальным распределением, в котором сигнал на выходе имеет вид:

$$Z(t) = kU(t-\tau) + N(t),$$

где $U(t)$- входной сигнал; $k$ и $\tau$- постоянные; $N(t)$- гауссовский аддитивный шум с нулевым математическим ожиданием и заданной корреляционной функцией.

Сравнивая полученные результаты исследований с опубликованными данными, можно отметить, что качество телефонных каналов передачи дискретной информации в течение нескольких десятилетий улучшилась незначительно.

**В третьей главе** предлагаются методы повышения отказоустойчивости устройств криптографической защиты информации, основанные на добавлении к криптографическим схемам элементов устойчивости функционирования.

Из-за возникновения какого-либо нарушения нормального функционирования логических или арифметических элементов внутри криптосхемы конечный результат преобразования может быть неверным. При этом, как правило, ошибки остаются необнаруженными либо, в случае обнаружения, требуется полное повторение прямого и/или обратного преобразования. Указанные недостатки снижают надежность функционирования криптографических алгоритмов и, соответственно, устройств преобразования информации.

Для того, чтобы устройство обладало свойством отказоустойчивости, в нем должна быть предусмотрена возможность выполнения определенной функции обнаружения возможных неисправностей, выявления их места и перестраивание системы с целью их устранения.

Сущность предлагаемых методов повышения надежности систем криптографического преобразования информации заключается в добавлении к стандартным криптографическим устройствам двух типов компонент устойчивости: детекторов и корректоров, и обеспечение на их основе отказоустойчивости устройства в целом.

Пусть $X$, $V$ и $U$ предикаты состояния детектора. Тогда, спецификация детектора $dt$ может быть представлена как "$V$ обнаруживает $X$ в $dt$ для $U$". Подразумевается, что $U$ заключено в $dt$. Аналогично, если $X$, $V$ и $U$ - предикаты состояния корректора, то спецификация корректора $ct$ может быть представлена как "$V$ корректирует $X$ в $ct$ для $U$". Подразумевается, что $U$ заключено в $ct$.

**Определение**: Пусть $\Psi$ - инварианта криптографической системы $Cs$, $F_1,...,F_n$ - классы отказов, а $l_1,...,l_n$ - типы отказоустойчивости (т.е. маскированный, не маскированный или нечувствительный к отказам). Тогда криптосистема $Cs$ - мультиотказоустойчива к $F_1,...,F_n$ для $\Psi$, если для каждого класса отказов $F_j$, $1 \le j \le n$, система $Cs$- является $l_j$- устойчивой.

Данное определение задает способ построения отказоустойчивых криптосхем. Введение вышеуказанных компонентов устойчивости позволяет сохранить работоспособность схем при возникающих в них отказах заранее

определенного класса и типа, дает возможность свести к минимуму время поиска отказа и значительно сократить время восстановления.

Рассмотрен пример построения отказоустойчивого устройства криптографического преобразования информации в соответствии с описанным методом на основе криптосхемы алгоритма ГОСТ 28147-89. Для исправления ошибок при считывании информации в блоках запоминающих устройств и проверки корректности выполнения операций преобразования основного алгоритма до его завершения введены дополнительные схемы корректоров $ct_{1,\dots,}$ и детекторов $dt_{1,\dots,j}$. А именно: блоки контроля/коррекции арифметических и логических операций, блоки обнаружения/исправления ошибок (или кодеры/декодеры), дополнительные накопители хранения проверочных разрядов для ключевого запоминающего устройства, блока подстановки и накопителей. Для обеспечения контроля арифметических и логических операций предлагается применение следующих методов: метода дублирования, мажоритарного резервирования и метода, основанного на применении кодов контроля и коррекции.

Наиболее эффективный метод повышения отказоустойчивости криптосхем - использование кодов контроля. Сущность метода заключается во введении блоков контроля, осуществляющих проверку выполнения основных арифметических и логических операций алгоритма при помощи методов контроля, основанных на свойствах сравнений (или контроля по модулю). Контрольный код числа (свертка) образуется суммированием цифр числа по выбранному модулю $p$:

$$r \equiv \sum_i (-1)^i a_i (\mathrm{mod}\, p),$$

где $a_i$ - двоичное изображение цифр в системе с основанием $q = 2^s$, $p = (2^s \pm 1)/m$, а $m$ и $s$ - некоторые целые положительные числа ($s \geq 2$).

Предложенный метод контроля по модулю позволяет эффективно обнаруживать одиночные ошибки. Для обнаружения и корректировки одиночных и пакетов ошибок, а также для контроля операций записи и считывания информации в накопителях могут быть использованы арифметические коды. Операнды контролируемого блока представляются в $AN$-коде (где $N$ - выбранный модуль) или в $BN$-коде (причем $B = (2^{N-1} - 1)/N$) с арифметическим расстоянием между ними $d > q$ и, следовательно, с минимальной избыточностью $\log_q(q+1)$ и $N-1$ для $AN$ и $BN$-кода соответственно. После выполнения операции результат сравнивают с образцами разрешенных комбинаций. При получении запрещенной комбинации выполняется коррекция результата путем перехода к наиболее близкой разрешенной. Таким образом, арифметический контроль позволяет не только зафиксировать наличие ошибки, но и исправить ее.

Кроме того, при кодовом методе контроля каждое информационное слово данных, хранимое в запоминающих блоках, дополняется проверочными (контрольными) разрядами в процессе записи информации, формируемыми предварительно на основе используемого корректирующего кода или кодерами при записи информации, и записывается в соответствующие дополнительные накопители. С помощью контрольных разрядов и аппаратуры декодирования возможно обнаружение и исправление возникающих в информационных разрядах накопителей ошибок при считывании информации.

Для определения эффективности кодового метода построения отказоустойчивых устройств криптографического преобразования оценена вероятность безотказной работы рассмотренного примера отказоустойчивой криптосхемы. Обозначим через $Q_j$ вероятность ошибки в $j$-ом функциональном блоке криптосхемы (пусть отказы любого из элементов равновероятны). Тогда вероятность отказа устройства равна

$$P_{yc} = 1 - \exp\left[-\sum_{j=1}^{s} Q_j\right].$$

Если предположить, что ошибки накопителей имеют биномиальный закон распределения со средней вероятностью $p_0$ на бит информации, то с учетом корректирующей способности используемого кода (для исправления $t$-кратной ошибки) для 32-разрядных накопителей величина $Q_j$ вычисляется как

$$Q_j = \sum_{i=t+1}^{32+r} C_n^i p_0^i (1-p_0)^{32+r-i} = 1 - \sum_{i=0}^{t} \frac{(32+r)!}{(32+r-i)!\,i!} p_0^i (1-p_0)^{32+r-i}.$$

Установлено, что корректоры блоков запоминающих устройств криптосхемы снижают общую вероятность отказа устройства на 3÷6 порядков. Анализ зависимости $P_{yc}$ от вероятности ошибки $p_0$ ЗУ показывает, что вероятность отказа устройства с корректорами для блоков ЗУ значительно снижается при дублировании операционных блоков схемы и может быть еще больше снижена при мажоритарном резервировании арифметических и логических блоков схемы.

Введенные корректоры арифметических и логических операций снижают общее быстродействие криптосхемы. Разница в быстродействии предложенного избыточного устройства по сравнению с оригинальным будет определяться временем формирования проверочных разрядов для блоков ЗУ в режиме записи и длительностью периода декодирования в режиме считывания, что меньше, чем в схемах с дублированием и мажоритарным резервированием, за счет формирования сигналов контроля операционных блоков параллельно с выполнением операций.

Таким образом, несмотря на увеличение времени криптопреобразований, преимущество отказоустойчивого устройства состоит в увеличении среднего

времени безотказной работы, по крайней мере, в несколько раз по сравнению с безызбыточной криптосхемой, а следовательно, - в повышении надежности функционирования и получении более корректных результатов реализации алгоритма. Кроме того, ошибки, возникающие в устройствах криптопреобразований, могут оставаться необнаруженными, а в случае обнаружения достаточно трудно локализуемы, что устраняется при использовании отказоустойчивого метода построения криптографических схем.

**В четвертой главе** рассмотрены принципы построения и алгоритмы функционирования крипто-корректирующих систем защиты.

Для нейтрализации ошибок, возникающих при передаче дискретной информации по каналам связи, предлагается использование в криптографических системах дополнительных избыточных схем, принцип работы которых основан на реализации алгоритма обнаружения и исправления определенного типа ошибок с помощью корректирующих кодов. Для снижения информационной избыточности сообщения и повышения эффективности передачи потока данных в последовательную систему крипто-корректирующего преобразования информации добавлен блок сжатия данных. Разработана структурная схема системы, реализующая три вида преобразования: сжатие, шифрование и помехоустойчивое кодирование, в которой преобразование информации может быть представлено как

$$Ck = G_{\zeta}(Y_c(m) \oplus Z(K)),$$

где $Ck$ - крипто-кодовая последовательность, $G_{\zeta}$ - порождающая матрица линейного корректирующего кода $\zeta$ $[n,k]$, $Y_c$ - функция сжатия, $m$ - исходная последовательность данных, $Z$ - функция формирования псевдослучайной последовательности, $K$ - секретный ключ.

Тогда, процесс обратного преобразования:

$$m = Y_d(H_{\zeta}(Ck' \oplus Z(K))) = Y_d(H_{\zeta}(Ck \oplus e \oplus Z(K))),$$

где $Y_d$ - функция развертывания, $H_{\zeta}$ - функция помехоустойчивого декодирования, $Ck'$ - искаженная крипто-кодовая последовательность, $e$ - канальный шум.

Показано, что преимущество последовательного крипто-корректирующего процесса со сжатием состоит в увеличении фактической пропускной способности системы преобразования и в более эффективном использовании каналов связи. Предварительное сжатие исходных данных позволяет использовать в криптосхемах коды с различной корректирующей способностью и соответственно - увеличивать помехоустойчивость криптографических систем. Недостатками представленной реализации является переменный размер блока крипто-кодового текста и увеличение времени прямого и обратного преобразования.

С целью устранения указанных недостатков предлагается модифицированная система корректирующего скремблера/дескремблера информации со сжатием, преимущество которой состоит в сокращении времени обратного преобразования за счет удаления блока дескремблирования и увеличении криптостойкости системы.

Предложены методы и алгоритмы функционирования интегрированных систем обеспечения защищенности, в которых ключевым элементом является наличие общего модуля кодирования и криптографического преобразования, основанного на принципе взаимодополнения, в отличие от крипто-корректирующих методов и алгоритмов, предполагающих независимость модулей криптопреобразования и кодирования.

Рассмотрен метод внутреннего кодирования, при котором криптографическое преобразование исходной последовательности осуществляется как до, так и после корректирующего кодирования. При этом, необходимым условием является отсутствие распространения ошибок в криптографическом преобразовании, осуществляемом после кодирования. Введем следующие обозначения: $m$ - исходный блок данных, $K_1, K_2$ - секретные ключи, $Ek1, Ek2$ - процессы криптографического преобразования данных, $G_\zeta$ - порождающая матрица линейного корректирующего кода $\zeta$, $Ck$ - выходной блок крипто-кодовых данных. Тогда процесс криптографического преобразования с внутренним кодированием может быть представлен как

$$Ck = \begin{cases} Ek1((G_\zeta \cdot Ek1(m, K_1)), K_1), \\ Ek2((G_\zeta \cdot Ek1(m, K_1)), K_2), \\ Ek2((G_\zeta \cdot Ek1(m, K_1)), K_1), \end{cases}$$

Различия алгоритмической структуры прямого и обратного преобразований сводятся к порядку использования процессов кодирования и шифрования.

Рассмотрен метод построения корректирующих систем с секретными элементами. Операция крипто-кодирования описывается в общем виде с помощью следующей функции:

$$Ck = f((m \cdot G_\zeta), K),$$

где $f$ - функция формирования крипто-кодовой последовательности. Тогда обратная функция восстановления:

$$\varphi_f((f(m \cdot G_\zeta), K), K) = m.$$

Данный метод отличается высокой информационной избыточностью, что может значительно снизить криптостойкость системы и упростить процедуру криптоанализа. Поэтому более приемлема модификация метода, при которой

крипто-кодовая функция $f$ - нелинейна. В этом случае увеличивается степень сложности как криптоанализа, так и алгоритма декодирования. Проанализированы основные параметры реализаций систем.

Теоретически рассчитана оценка эффективности применения крипто-корректирующих систем защиты информации на основе сравнительной характеристики, которая учитывает все представляющие интерес параметры. Общий коэффициент качества или "эффективность системы" определяется соотношением:

$$\gamma = \sum_{i=1}^{N} \beta_i \eta_i , \quad 0 \le \gamma \le 1$$

где $\beta_i$ - относительный весовой коэффициент (вес), а $\eta_i$ - "коэффициент успеха". Из перечня сравниваемых параметров наиболее существенными выбраны: пропускная способность системы, временная сложность алгоритма преобразования и помехоустойчивость (отказоустойчивость).

По данной методике расчета эффективность крипто-корректирующих систем примерно на 19-24 % выше в сравнении с традиционными криптографическими системами защиты. Таким образом, условие целесообразности создания крипто-корректирующих систем подкреплено достигаемым при этом эффектом.

## ЗАКЛЮЧЕНИЕ

Основные результаты диссертационной работы заключаются в следующем:

1. Получены статистические характеристики распределения ошибок в телефонных каналах передачи дискретной информации. Установлено, что в большинстве (64%) случаев превалируют одиночные случайные ошибки и пакеты ошибок малой длины: от 2 до 4. Впервые показано, что существует класс линий, в которых вероятность появления ошибок меняется в зависимости от времени суток, а характер распределения коэффициента ошибок соответствует нормальному закону [2, 7-9].

2. Установлено, что распределение групп ошибок в телефонных каналах передачи дискретной информации описывается показательной или гиперболической полиномиальными моделями и совпадает с одной из известных моделей [13].

3. Установлена степень влияния помех в дискретных телефонных каналах и отказов аппаратуры преобразования данных на целостность и достоверность обрабатываемой информации в распределенных системах криптографических преобразований. На основе имитационного моделирования искажения различного числа бит передаваемого блока шифротекста блочных криптоалгоритмов установлено, что вероятность искажения бит открытого

текста имеет биномиальный закон распределения. Разработана математическая модель распределение вероятности появления числа искаженных бит в блоках открытого текста при единичных отказах элементов криптосхем, соответствующая смеси трех нормальных распределений [4].

4. Разработаны методы построения отказоустойчивых систем криптографической защиты информации, основанные на введении дополнительных схем корректоров/детекторов. Установлено, что реализация кодового метода, обеспечения отказоустойчивости схемы алгоритма шифрования ГОСТ 28147-89 приводит к увеличению вероятности безотказной работы системы криптографического преобразования информации на 3÷6 порядков [1, 6, 12, 15, 18].

5. Разработаны методы и алгоритмы крипто-корректирующего преобразования, основанные на дополнении криптографических систем избыточными схемами кодирования информации, обладающими свойствами обеспечения конфиденциальности и целостности предаваемых данных одновременно, позволяющие создавать на их основе безопасную инфраструктуру внутренних коммуникаций, обеспечивающую надежную защиту обработки информации. Реализация подобных систем повышает относительную эффективность известных криптосистем на 19-24% [3, 5, 10, 11, 14, 16, 17].

6. Разработанные в диссертации методы и алгоритмы криптографической защиты информации на основе корректирующих кодов используются в учебном процессе на кафедре ИиВТ БГТУ и в управляющих подсистемах удаленного доступа на предприятии УП "Центр банковских технологий".

## СПИСОК ОПУБЛИКОВАННЫХ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

1. Урбанович П.П., Пацей Н.В. Концепция создания взаимодополняемых алгоритмов обеспечения надежности и целостности информации в компьютерных сетях// Сб. Труды БГТУ. Серия IV. Физико-математические науки и информатика. -Мн.: БГТУ.- 1997. -Вып. 5.-С.91-96.

2. Урбанович П.П., Пацей Н.В., Спиридонов В.В. Распределение ошибок в телефонных каналах передачи дискретной информации// Известия Белорусской инженерной академии. - Мн., - 1997.- №1(3)/1, С.24-26.

3. Пацей Н.В., Урбанович П.П. Комбинированное преобразование информации в каналах связи для повышения целостности и надежности данных (система 3К)//Сб. Труды БГТУ. Серия Физико-математические науки и информатика.-Мн.:БГТУ,1998.-Вып.VI.-С. 103-107.

4. Урбанович П.П., Пацей Н.В. Общие диффузионные характеристики криптографических блочных кодов // Управление Защитой Информации. -1998.-Т.2,№2.-С.139-140.

5. Пацей Н.В., Урбанович П.П. Метод построения криптокорректирующих систем на основе сверточных кодов // Управление Защитой Информации.-1999.-Т.3, №4.-С.453-454.

6. Пацей Н.В. Метод повышения отказоустойчивости криптографических схем защиты информации // Сб. Труды БГТУ. Серия Физ.-мат. науки и информатика- Мн.:БГТУ,2000.-Вып.VIII.-С. 132-138.

7. Пацей Н.В., Урбанович П.П. Основные проблемы защиты информации в сетях телекоммуникаций // Труды второй международной конференции "Новые информационные технологии в образовании" – Мн., БГЭУ, 1996.- Т.2.-С.34-36.

8. Пацей Н.В., Урбанович П.П. Некоторые вопросы применения типовых криптографических алгоритмов // Тезисы докладов и сообщений 1 РНПК "Комплексная защита информации проблемы и решения" -Мн.,1997- С. 42-44.

9. Пацей Н.В., Урбанович П.П. О распределении ошибок во времени при передаче двоичных сигналов по телефонным каналам // Материалы МНТК "Автоматизированный контроль и автоматизация производственных процессов".-Мн.:БГТУ,1998.-С.123-125.

10. P.P.Urbanovich, N.V.Patsei Combinational Methods of Increase Integrity and Confidentialy of the Information in Communication Channels// Proceedings, "2 International Conference on Computer Methods and Inverse Problems in Nondestructive Testing and Diagnostics".- Minsk, Berlin, 1998.-P.591-593.

11. Пацей Н.В., Урбанович П.П. О потоковых комбинационных крипто-корректирующих кодах защиты информации// Труды Третьей

международ. Конф. "Новые информационные технологии в образовании" - Мн.,1998.- Т.2.- С.33-35.

12. Урбанович П.П., Пацей Н.В. О создании отказоустойчивых криптографических систем// Материалы МНТК "Новые информационные технологии в науке и производстве".- Мн., 1998.- С.283-284.

13. Пацей Н.В., Скачков М.С., Урбанович П.П. Некоторые закономерности распределения ошибок в каналах передачи дискретной информации//Спец. выпуск Известия белорусской инженерной академии № 1(7)/1; Материалы IV МНТК "Современные средства связи" - Нарочь, 1999.- С.18.

14. Пацей Н.В. Формирование оценки эффективности крипто-корректирующей системы защиты каналов передачи информации // Материалы МНТК "Автоматический контроль и автоматизация производственных процессов". –Мн.:БГТУ,2000.-С.171-172.

15. Patsei N.V., Urbanovich P.P. On the Design of Error Detection and Correction Cryptography Schemes // Eurocomm 2000 Information Systems for Enhanced Public Safety and Security: Conference Record, Munich, Germany – IEEE Service Center, USA,2000 – P.266-268.

16. P.P.Urbanovich, N.V.Patsei Information scrambler/descarmbler based on combination of data compression and error-correction codes // Symposium Proceedings "New Electrical and Electronic Technologies and their Industrial Implementation" -Poland, Lublin,2001.-P.78-80.

17. Заяв. на пат. BY, МПК 6 H 04L 9/00, G 06F 11/08. Устройство крипто-корректирующего преобразования / Урбанович П.П., Пацей Н.В. - № 19990661 A; Заявл. 02.07.1999. // Афіцыйны бюлетэнь / Дзярж. пат. ведамства. Рэсп. Беларусь. –2001. -№1(28)-С.65.

18. Заяв. на пат. BY, МПК 6 H04K 1/00, H04L 9/00. Устройство криптографического преобразования информации с обнаружением и коррекцией ошибок / Урбанович П.П., Пацей Н.В. -№ 19990935 A; Заявл. 15.10.1999. // Афіцыйны бюлетэнь / Дзярж. пат. ведамства Рэсп. Беларусь. – 2001. -№2(29).

# РЭЗЮМЭ

Пацэй Наталля Ўладзіміраўна

## МЕТАДЫ ПАВЫШЕННЯ НАДЗЕЙНАСЦІ І АЛГАРЫТМЫ ФУНКЦЫЯНАВАННЯ СРОДКАЎ АХОВЫ ІНФАМАЦЫІ Ў КАМП'ЮТЭРНЫХ СЕТКАХ НА АСНОВЕ КРЫПТА-КАРЭКЦЫЙНЫХ ПЕРАЎТВАРЭННЯЎ

**Ключавыя словы**: крыптаграфічная сістэма, карэкцыйнае кадіраванне, надзейнасць, памылка, адмоваўстойлівасць, уладкаванне.

Аб'ектам даследавання з'яўляюцца сучасныя сродкі крыптаграфічнага пераўтварэння інфармацыі. Прадмет даследавання – метады і алгарытмы павышення надзейнасці гэтых сродкаў.

Мэтай працы з'яўляюцца распрацоўка і даследаванне новых эфектыўных метадаў аховы інфармацыі ў камп'ютэрных сетках на аснове крыптапераўтварэнняў і лішкавага кадавання даных, дазваляючых павялічыць ўзровень надзейнасі сродкаў крыптаграфічнай аховы.

У працы эксперыментальна абгрунтавана неабходнасць выкарыстання метадаў карэкцыйнага кадавання даных ў крыптаграфічных сістэмах. Устаноўлены характар размеркаванне памылак і залежнасць размеркавання імавернасці з'яулення памылак у тэлэфонных каналах перадачы дыскрэтнай інфармцыі ад часу. Упершыню даследаваны ўплыў адмоў элементнай базы крыптасхем на дакладнасць пераўтварэння інфармацыі, што дазваляе вызначыць патрабаванні да адмоваўстойлівых крыптасродкаў.

Прапанаваны новыя метады пабудовы крыптасродкаў на аснове выкарыстання выяўлення і выпраўкі памылак і забеспячэння адмоваўстойлівасці і надзейнасці пераўтварэння даных.

Прапанаваны новыя метады пабудовы і алгарытмы функцыянавання крыпта-карэкцыйных сродкаў і сістэм аховы інфармацыі на аснове інтэграцыі карэкцыйнага кадавання і крыптаграфічных пераўтварэнняў, якія дазваляюць павялічыць эфектыўнасць апрацоўкі крытычнай інфармацыі пры высокім узроўне перашкод. Прапанаваны структурна-функыянальныя схемы крыпта-карэкцыйнах сродкаў. Тэарэтычна абгрунтавана і даказана адносная эфектыўнасць выкарыстання распрацаваных сродкаў у складзе сістэм аховы інфармацыі.

Атрыманыя вынікі можна выкарыстоўваць пры распрацоўцы бяспечнай інфраструктуры ўнутраных камунікацыяў падсістэм кіравання сетак прадпыемства.

## РЕЗЮМЕ

Пацей Наталья Владимировна

# МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ И АЛГОРИТМЫ ФУНКЦИОНИРОВАНИЯ УСТРОЙСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ КРИПТО-КОРРЕКТИРУЮЩИХ ПРЕОБРАЗОВАНИЙ

**Ключевые слова:** криптографическая система, корректирующее кодирование, надежность, ошибка, отказоустойчивость, устройство.

Объектом исследования являются современные устройства криптографического преобразования информации. Предмет исследования – методы и алгоритмы повышения надежности этих устройств.

Целью работы является создание и исследование новых эффективных методов защиты информации в компьютерных сетях на основе криптопреобразований и избыточного кодирования данных, обеспечивающих повышенный уровень надежности устройств криптографической защиты.

В работе экспериментально обоснована необходимость использования методов корректирующего кодирования данных в криптографических системах. Установлены характер распределения ошибок и зависимость распределения вероятности появления ошибок в телефонных каналах передачи дискретной информации от времени. Впервые исследовано влияние отказов элементной базы криптосхем на достоверность преобразования информации, что позволило определить требования к отказоустойчивым криптоустройствам.

Предложены новые методы построения криптографических устройств, основанные на использовании кодовых методов обнаружения и исправления ошибок и обеспечивающие отказоустойчивость и надежность преобразования данных.

Предложены новые методы построения и алгоритмы функционирования крипто-корректирующих устройств и систем защиты информации, основанные на интеграции корректирующего кодирования и криптографических преобразований, позволяющие повысить эффективность обработки критической информации при высоком уровне помех. Предложены структурно-функциональные схемы крипто-корректирующих устройств. Теоретически обоснована и доказана относительная эффективность использования разработанных устройств в составе систем защиты.

Полученные результаты могут быть использованы при создании безопасной инфраструктуры внутренних коммуникаций в управляющих подсистемах сети предприятия.

## SUMMARY

Patsei Natallia Vladimirovna

# METHODS OF RELIABILITY GROWTH AND OPERATION ALGORITHMS OF INFORMATION PROTECTION DEVICES IN COMPUTER NETWORKS ON THE BASE OF CRYPTO-CORRECTION TRANSFORMATIONS

**Key words**: cryptography system, error-correcting coding, reliability, error, fault-tolerance, noiseproof feature, devices.

The object of researche are modern cryptography systems of information transformation. The subject of research – methods and algorithms of reliability growth this devices.

The purpose of work is the research and development of new effective methods of information protection in computer networks on the base of crypto transformations and redundancy coding, providing increased level of reliability cryptography protection devices.

Experimentally prove the necessity of error-correcting methods use in crypto systems. Characters of error distribution and dependence of error probability distribution in telephony channel of discrete information transmission dependent upon time established. For the first time faults influence of crypto schemes element bases on information transformation reliability investigated. That allow to determine requirements to fault-tolerance crypto devices.

The new methods of crypto devices construction on the base of code methods of error determine and correction and ensuring data transformation fault-tolerance and reliability are offered.

The new construction methods and operation algorithms of crypto-correction devices and information protection systems on base of error correction coding and crypto transformation integration are offered, what allow to increase critical information processing efficiency on high level of noise. Structurally-function schemes of crypto-correction devices are offered. Theoretically prove and demonstrated comparative effectiveness of using elaborated devices in consisting of protection system.

The obtained results can be used for safe infrastructure of inner management subsystems communication in enterprise networks creation.

**ПАЦЕЙ**

**Наталья Владимировна**

# МЕТОДЫ ПОВЫШЕНИЯ НАДЕЖНОСТИ И АЛГОРИТМЫ ФУНКЦИОНИРОВАНИЯ УСТРОЙСТВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ НА ОСНОВЕ КРИПТО-КОРРЕКТИРУЮЩИХ ПРЕОБРАЗОВАНИЙ

Специальности 05.13.05 - Элементы и устройства вычислительной техники и систем управления,

05.13.15 – Вычислительные машины и системы

Автореферат диссертации

на соискание ученой степени кандидата технических наук

| | | |
|---|---|---|
| Подписано в печать | 13.11.2001. | Формат 60x84 1/16 |
| Бумага офсетная. | Печать ризографическая. | Усл.печ.л. 1,63. |
| Уч.-изд.л. 1,2. | Тираж 90 экз. | Заказ 536. |

Издатель и полиграфическое исполнение:
Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
Лицензия ЛП № 156 от 05.02.2001.
Лицензия ЛВ № 509 от 03.08.2001.
220013, Минск, П. Бровки, 6.