ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА ДМ 003.046.01 НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ ИНСТИТУТА ВЫЧИСЛИТЕЛЬНЫХ ТЕХНОЛОГИЙ СИБИРСКОГО ОТДЕЛЕНИЯ РОССИЙСКОЙ АКАДЕМИИ НАУК ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 04.12.2015 г. № 25

О присуждении Лысяку Александру Сергеевичу, гражданину РФ, **учёной степени** кандидата технических наук.

Диссертация «Разработка и исследование теоретико-информационных методов прогнозирования» **по специальности** 05.13.18 – «Математическое моделирование, численные методы и комплексы программ» **принята к защите** 28 сентября 2015 **года**, протокол № 23, **диссертационным советом** ДМ 003.046.01 на базе Федерального государственного бюджетного учреждения науки Института вычислительных технологий Сибирского отделения Российской академии наук, 630090, Россия, г. Новосибирск, пр. Академика Лаврентьева, 6, приказ Минобрнауки России № 717/нк от 09 ноября 2012 г.

Соискатель Лысяк Александр Сергеевич 1989 года рождения, гражданин РФ, в 2012 году окончил Федеральное государственное автономное образовательное учреждение высшего образования «Новосибирский национальный исследовательский государственный университет», в 2015 году – аспирантуру Федерального государственного автономного образовательного учреждения высшего образования «Новосибирский национальный исследовательский государственный университет» (НГУ), работает ассистентом на кафедре Компьютерных систем факультета информационных технологий НГУ.

Диссертация выполнена на кафедре Компьютерных систем факультета информационных технологий в Федеральном государственном автономном образовательном учреждении высшего образования «Новосибирский национальный исследовательский государственный университет».

Научный руководитель – доктор технических наук Рябко Борис Яковлевич, заведующий лабораторией информационных систем и защиты информации

Федерального государственного бюджетного учреждения науки Института вычислительных технологий Сибирского отделения Российской академии наук.

Официальные оппоненты:

1. Дьячков Аркадий Георгиевич, доктор физико-математических наук, профессор кафедры теории вероятностей Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет им. М.В. Ломоносова»;
2. Лемешко Борис Юрьевич, доктор технических наук, профессор кафедры теоретической и прикладной информатики Федерального государственного бюджетного образовательного учреждения высшего образования «Новосибирский государственный технический университет»

дали положительные отзывы на диссертацию.

Ведущая организация: Федеральное государственное бюджетное учреждение науки Институт математики им. С.Л. Соболева Сибирского отделения Российской академии наук, г. Новосибирск, в своем положительном заключении, составленном Соловьевой Фаиной Ивановной, доктором физико-математических наук, профессором, ведущим научным сотрудником Лаборатории совершенных комбинаторных структур, **указала, что** работа Лысяка А.С. полностью соответствует паспорту специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ», а сам соискатель заслуживает присуждения степени кандидата технических наук.

Соискатель имеет 10 опубликованных научных работ (в скобках в числителе указан общий объём этого типа публикаций в печатных листах, в знаменателе – объём, принадлежащий лично автору), в том числе 4 статьи (8.2/5.8) в изданиях, рекомендованных ВАК для представления основных результатов диссертации на соискание ученой степени доктора или кандидата наук, 4 труда (4.6/4.2), опубликованных в материалах всероссийских и международных конференций и 1 монография (8.3/8.3).

Наиболее значимые научные работы по теме диссертации:

Лысяк А.С. Методы прогнозирования временных рядов с большим алфавитом на основе универсальной меры и деревьев принятия решений. / А.С. Лысяк, Б.Я. Рябко // Вычислительные технологии. – 2014. – Т. 19, №2. – С. 75–92.

Лысяк А.С. Прогнозирование многомерных временных рядов. / А.С. Лысяк, Б.Я. Рябко // Вестник СибГУТИ. – 2014. – №4. – С.75–88.

Лысяк А.С. Анализ эффективности градиентной статистической атаки на блоковые шифры RC6, MARS, CAST-128, IDEA, Blowfish в системах защиты информации. / А.С. Лысяк, А.Н. Фионов, Б.Я. Рябко // Вестник СибГУТИ. – 2013. – №1. – С. 85–109.

Лысяк А.С. Теоретико-информационные методы прогнозирования временных рядов. / А.С. Лысяк. – LAP Lambert Academic Publishing, 2014, ISBN 978-3-659-59737-4. – 72 с.

Помимо отзывов от оппонентов и ведущей организации, на диссертацию и автореферат поступило 10 отзывов (все отзывы положительные, из них 2 без замечаний). Это отзывы от 1) к.т.н. Приставки А.Ф. (СибГУТИ, г. Новосибирск); 2) к.т.н. Нечты И.В. (СибГУТИ, г. Новосибирск); 3) Ракитского А.А. (СибГУТИ, г. Новосибирск); 4) к.т.н., доцента Пищика Б.Н. (КТИ ВТ СО РАН, г. Новосибирск); 5) к.ф.-м.н. Монарева В.А. (ИВТ СО РАН, г. Новосибирск); 6) д.т.н., профессора Габидулина Э.М. (МФТИ (государственный университет), г. Москва); 7) д.т.н., профессора Крука Е.А. (Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), г. Санкт-Петербург); 8) д.т.н. Кручинина В.В. (Томский государственный университет систем управления и радиоэлектроники, г. Томск); 9) д.ф.-м.н., профессора Малютова М.Б. (Северо-Восточный университет, г. Бостон, США); 10) д.т.н. Родионова А.С. (ИВМиМГ СО РАН, г. Новосибирск).

В отзывах содержатся следующие критические замечания (приведены наиболее существенные):

1) В работе отсутствует описание того, каким образом следует подбирать коррелирующие процессы, и не может ли низкий коэффициент корреляции сделать точность, полученную с применением данного подхода, ниже, чем при классическом одномерном прогнозировании с использованием аналогичного алгоритма.

2) Работе не помешал бы более обстоятельный обзор методов прогнозирования временных рядов с включением в него для сравнения статистических методов.

3) В конце глав диссертации явно не хватает выводов по итогам исследований, описанных в соответствующей главе.

4) В обоснование предпочтительности разбиения на интервалы равной длины в разделе 2.4 автор ссылается на результаты экспериментальных исследова-

ний, при которых использовались различные способы разбиения. Здесь хотелось бы иметь и более строгое обоснование.

5) В работе не упоминается о регистрации разработанного программного обеспечения. Напрашивается необходимость реализации данного шага.

6) В автореферате недостаточно полно описана теория приложения методов прогнозирования к задаче криптоанализа блоковых шифров.

Выбор официальных оппонентов и ведущей организации обосновывается близостью тематики исследования оппонентов и ведущей организации к теме диссертации Лысяка А.С., а также тем, что результаты, полученные за последние годы оппонентами и в ведущей организацией, публикуются в ведущих мировых журналах по тематике диссертационного исследования.

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

предложены эффективные (имеющие полиномиальную сложность и не требующие большого объёма памяти) методы прогнозирования, базирующиеся на теоретико-информационных подходах, а также на теории анализа данных;

разработан метод группировки алфавита, применимый к произвольным методам прогнозирования, существенно уменьшающий вычислительную сложность и улучшающий качество получаемых прогнозов;

разработан и исследован экспериментально многомерный подход в прогнозировании, улучшающий точность получаемых прогнозов благодаря учёту в прогнозе коррелирующих между собой временных рядов;

показано, что качество работы предложенных методов при прогнозировании сложных экономических и социальных процессов выше, чем у ранее известных алгоритмов прогнозирования;

предложена градиентная статистическая атака на блоковые шифры, базирующаяся на использовании рассмотренных в работе методов прогнозирования;

предложен новый подход к исследованию криптостойкости генераторов псевдослучайных чисел, основанный на использовании вероятностных методов прогнозирования.

Теоретическая значимость исследования обоснована тем, что:

применительно к проблематике диссертации результативно (с получением обладающих новизной результатов) использованы подходы из теории ин-

формации и интеллектуального анализа данных с целью построения методов прогнозирования вещественных стационарных временных рядов;

предложен ряд универсальных модификаций (т. е. применимых к произвольным вероятностным методам прогнозирования), позволяющих повысить точность получаемых оценок статистических параметров рассматриваемых процессов, а также снизить их сложность;

предложен многомерный подход, основанный на построении полиномиальной хеш-функции со сдвигом по коррелирующим с рассматриваемым временным рядам, что позволяет находить статистические закономерности и повышает точность прогнозов для нестационарных временных рядов;

предложен новый статистический тест, базирующийся на вероятностных методах прогнозирования, эффективный при реализации градиентной статистической атаки на блоковые шифры, а также для проверки криптостойкости генераторов псевдослучайных чисел.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны численные алгоритмы для получения плотности вероятностей, квантилей распределения, а также математического ожидания временного ряда рассматриваемого процесса;

разработан программный комплекс для прогнозирования значений временных рядов прикладных процессов с учётом их взаимных корреляций.

Достоверность и обоснованность результатов исследования обеспечивается тем, что:

установлено хорошее качественное соответствие полученных численных результатов экспериментальных исследований реальным результатам реализации изучаемых процессов с отклонениями, не превышающими в среднем 10%;

установлено, что получаемые численные результаты экспериментов в большинстве случаев превосходят (по точности получаемых оценок квантилей распределения и математического ожидания) результаты других исследователей (полученные с использованием известных ранее методов прогнозирования);

использованы современные эффективные численные методы и алгоритмы математического моделирования и оптимизации при реализации комплексов программ.

Личный вклад соискателя состоит в непосредственном участии в постановке задач, самостоятельной разработке универсальных модификаций (метод усреднения, моделирование поведений, метод группировки алфавита, многомерных подход), разработке и оптимизации методов прогнозирования на основе универсальной меры и решающих деревьях, теоретической разработке и реализации приложения методов прогнозирования к анализу надёжности генераторов случайных и псевдослучайных чисел, а также к градиентной статистической атаке на блоковые шифры, реализации всех разработанных методов в виде комплексов программ, апробации разработанных методов и алгоритмов для прогнозирования реальных экономических и социальных процессов, анализе полученных результатов.

На заседании 4 декабря 2015 года **диссертационный совет принял решение присудить** Лысяку А.С. **учёную степень** кандидата технических **наук**.

При проведении тайного голосования диссертационный совет в количестве 19 человек, из них 7 докторов наук по специальности 05.13.18 – «Математическое моделирование, численные методы и комплексы программ» (технические науки), участвовавших в заседании, из 23 человек, входящих в состав совета, проголосовали: за 17, против 1, недействительных бюллетеней 1.

Заместитель председателя
диссертационного совета
д.т.н Фионов Андрей Николаевич

Ученый секретарь
диссертационного совета Лебедев Александр Степанович

«09» декабря 2015 г.