ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу Алхуссайн Амани
«Вероятностный анализ стойкости защиты информации
методом целочисленного расщепления символов»,
представленную к защите в Диссертационном Совете ПДС 0200.006
на базе Российского университета дружбы народов имени Патриса Лумумбы
на соискание ученой степени кандидата физико-математических наук
по специальности 1.2.3. – «Теоретическая информатика, кибернетика».

Проблема обеспечения конфиденциальности контактов (в частности, как проблема обеспечения конфиденциальности сообщений, которыми обмениваются контактирующие стороны) известна уже не один десяток столетий. Переписка между государственными деятелями, дипломатическая почта, донесения разведки и многое другое дали миру массу примеров применения достаточно развитых приемов и методов, использующих как особые технические средства, так и (порою весьма глубокие и элегантные) математические конструкции. Столетия размеренного и постепенного совершенствования искусства шифрования в противоборстве с искусством криптоаналитика (цель которого – «взломать» защиту и получить несанкционированный доступ к содержанию зашифрованного послания) в первой трети прошлого века сменились бурным ростом: началось активное развитие технических средств криптозащиты и криптоанализа. При этом в их разработке стали использовать все более изощренные математические методы и алгоритмы. Приход в эту область компьютеров вывел криптозащиту и криптоанализ на принципиально новый уровень: развитие проблемно-ориентированных математических методов и алгоритмов, интегрируемых со все более продвинутыми компьютерными технологиями, помимо усиления позиций в традиционных сферах применения систем и средств шифрования (см. выше) вывел такие инструментальные решения в широкий спектр индустриальных применений. В новейшие времена это – широко понимаемые потребности в конфиденциальной связи: цифровая телефония, в т.ч. – мобильная GSM-связь, электронная почта, удаленный режим доступа к различным системам и сервисам, а также электронная коммерция, телемедицина, технологическая связь на транспорте и многое другое.

Постоянно растущие требования индустриальных приложений при естественных ограничениях уже эксплуатируемых решений (см. в частности, специфику хранения и распределения ключей симметричного шифрования в массовых приложениях, которая предоставляет крипто-аналитику при несанкционированном декодировании дополнительные «подсказки» по линии семантических особенностей некоторых систем шифрования и др.) – вот очевидный стимул развивать теоретические основания, на которых базируются актуальные крипто-решения. (Все более существенную роль при этом играет ускоряющийся прогресс в области соответствующей технической базы - вычислительной техники, телекоммуникационных решений и др.).

Потребности в современных технологиях, а также системах обеспечения и управления конфиденциальностью конкретных процедур коммуникаций определяют **актуальность** разработки новых математических моделей, которые могли бы служить надежной теоретической основой для эффективных решений в рассматриваемой области, удовлетворять актуальным требованиям приложений, преодолевать (опираясь в т.ч. и на новейшие достижения науки и технологий) ограничения ранее уже введенных в использование подходов и решений. Диссертационное исследование Амани Алхуссейн «Вероятностный ана-

лиз стойкости защиты информации методом целочисленного расщепления символов» может быть отнесено именно к такой категории научно-квалификационных работ. **Практическая значимость** этого исследования обусловлена разработкой математических оснований для технических систем и решений, ориентированных на массовое использование в сфере цифровых сервисов и телекоммуникаций - цифровой телефонии, системах электронной почты, удаленного режима доступа к компьютерным системам и сервисам и т.п.

В диссертационной работе Амани Алхуссайн предложена **новая** теоретико-методологическая концепция – использующее модульную арифметику так называемое целочисленное расщепление, разработан и исследован **оригинальный** набор средств (методов и алгоритмов) защиты информации. Очевидным аргументом в пользу **научной новизны** данной работы являются развитые соискателем математические основания предлагаемого подхода, **теоретическая значимость** определяется доказательством ряд базовых утверждений, демонстрирующих корректность и стойкость соответствующих процедурных средств защиты, а также проведенным вероятностным анализом стойкости реализующего целочисленное расщепление инструментария защиты. Соискателем намечены пути практического применения сформированного математического и алгоритмического инструментария как одной из платформ для защиты информации при её передаче и хранении. Продемонстрированы преимущества предлагаемого в данной диссертационной работе подхода и инструментария в сравнении с рядом известных методов защиты информации.

Структура диссертационной работы сформирована Введением, четырьмя Главами, Заключением и Приложениями. Во **Введении** обоснованы актуальность, новизна, теоретическая и практическая значимость проводимых исследований, дан литературный обзор текущего состояния дел в рассматриваемой предметной области, обозначены цели и задачи работы. В **Первой главе** дан обзор методов защиты информации, представлены классы соответствующих систем (в том числе – требования к стойким шифрам), дан перечень недостатков известных методов шифрования (что существенно для демонстрации в последующих главах того, как предлагаемые автором данной диссертационной работы подход и процедурная конструкция позволяют обойти эти ограничения). **Вторая глава** посвящена детальному описанию математической техники целочисленного расщепления – процедурной схеме реализующего его преобразования. Определяются: функция целочисленного расщепления, понятие обобщенного целочисленного расщепления по векторной базе, а также доказывается ряд утверждений о свойствах целочисленного расщепления (в т.ч. – базовое утверждение о единственности целочисленного расщепления для заданного исходного элемента). Представлено детальное описание алгоритмической конструкции целочисленного расщепления заданного числа по заданной базе расщепления и заданному уровню расщепления. Демонстрируется связь между эволюционными вычислениями и процедурой расщепления, в которой используются псевдослучайные числа. В **Третьей главе** исследованы возможности использования метода целочисленного расщепления, предложенного автором данной диссертационной работы, как платформы для построения систем защиты текстовой информации. Представлено описание математической модели соответствующего метода защиты, которая базируется на использовании известного и отправителю, и получателю передаваемых закодированных сообщений стойкого генератора псевдослучайных чисел (ГПСЧ). Показано, как в ключ защиты при формировании конкретных параметров реализуемого целочисленного расщепления «встраивается» информация о выбранных эволюционном алгоритме (детерминированном генетическом алгоритме) и ГПСЧ. Дан детальный вероятностный анализ стойкости процедур защиты, формируемых таким способом. Представлены результаты выполненных соискателем численных расчетов вероятности взлома предлагаемых средств защиты для различных уровней расщепления. Получены аналитические

оценки, демонстрирующие экспоненциальный характер скорости убывания вероятности взлома защиты с ростом числа уровней расщепления. Доказано утверждение об асимптотической стойкости защиты методом целочисленного расщепления. Предложенные процедурные конструкции защиты данных иллюстрируются разбором серии подробных примеров их реализации. В **Четвертой главе** представлено сравнение предлагаемого автором диссертационной работы метода защиты с наиболее популярными другими методами, использующими вычисления по модулю (в том числе – многократное вычисление по модулю и не связанность используемого модуля с размерами алфавита кодируемого сообщения). Также демонстрируются преимущества символьного расщепления по отношению к известным абсолютно стойким методам защиты информации (экономность по ресурсам и сокрытие истинных размеров защищаемого сообщения). В **Заключении** приведены все выносимые на защиту результаты выполненного диссертационного исследования.

Все **выносимые** соискателем **на защиту положения и результаты** достаточно полно **обоснованы** и аргументированы в тексте рассматриваемой диссертационной работы: обоснована актуальность тематики исследования, выполнен обзор литературы, сформулированы выносимые на защиту положения и представлена развернутая система аргументов, формирующая их обоснование. Текст диссертации содержит ряд оригинальных утверждений, доказательства которых были своевременно опубликованы в рецензируемых журналах, а также были представлены в докладах на целом ряде научных конференций. Все это может служить дополнительным подтверждением обоснованности выносимых на защиту положений и выводов. Достоверность результатов вычислений по предложенным алгоритмам подтверждается результатами расчетов в тестовых примерах.

Автореферат корректно отражает результаты диссертационного исследования.

По теме диссертационного исследования автором подготовлены 25 публикаций, 7 из которых – в изданиях из перечня ВАК Минобрнауки РФ, 6 - в периодических научных журналах, индексируемых в системе Scopus, получен 1 патент на изобретение.

Имеется несколько **замечаний** к оформлению текстов диссертации и автореферата:
1.Тексты диссертации и автореферата, к сожалению, содержат некоторое количество некорректных использований лингвистических конструкций русского языка. (Что, видимо, является следствием вполне понятного обстоятельства: автора данной диссертационной работы вряд ли можно отнести к носителям литературного русского языка).
2. Более детального представления заслуживает взаимосвязь процедурной техники целочисленного расщепления (в т.ч. – повторного деления с остатком) с алгоритмикой эволюционных вычислений (см., в частности, выигрыш во времени выполнения по сравнению с традиционными для генетических алгоритмов процедурами эволюции). Приводимые в Приложении соображения могли бы быть более детальными.
3. Список литературы не полностью оформлен в соответствии с имеющимися требованиями (см., в частности, ссылки №№ 31,34,48,79, 80 и др.)

Однако, названные замечания носят скорее редакционно-методический характер и не способны существенным образом повлиять на общую **положительную оценку** диссертационной работы Амани. Алхуссайн.

Судя по текстам диссертационной работы, автореферата и публикаций автора, рассматриваемое диссертационное исследование Амани Алхуссайн «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов» представляет собой законченное и самостоятельное научно-квалификационное исследование, в котором решена актуальная задача разработки новой теоретико-методологической и практической концепции расщепления как одной из систем защиты информации.

Диссертационное исследование соответствует паспорту специальности 1.2.3. Теоретическая информатика, кибернетика, в частности:

- п.15 (Модели данных и новые принципы их проектирования),
- п.25 (Методы высоконадежной обработки информации и обеспечения помехоустойчивости информационных коммуникаций для целей передачи, хранения и защиты информации),
- п.26 (Теория надежности и безопасности использования информационных технологий),
- п.29 (Теоретические основы программирования, создания программных систем для новых информационных технологий).

На основании вышеизложенного считаю, что диссертационная работа «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов» полностью **соответствует** требованиям п. 2.2 раздела II Положения о присуждении ученых степеней в ФГАУ ВО Российский университет дружбы народов, утвержденного Ученым советом РУДН, протокол № 12 от 23 сентября 2019 г., предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук по специальности 1.2.3 — Теоретическая информатика, кибернетика, а ее автор —Амани Алхуссайн— **заслуживает** присуждения ей степени кандидата физико-математических наук.

Официальный оппонент:

Главный научный сотрудник Отдела №16
Федерального исследовательского центра
«Информатика и управление»
Российской академии наук, д.ф-м.н. М.И.Забежайло

25 августа 2023 года

Наименование организации – места работы: Федеральный исследовательский центр «Информатика и управление» Российской академии наук. Структурное подразделение – Отдел №16 «Интеллектуальный анализ данных и автоматизированная поддержка научных исследований» Отделения №1.
Должность: д.ф-м.н., г.н.с., и.о.заведующего Отделом.
Адрес электронной почты: m.zabezhailo@yandex.ru
Телефон: 8 (499) 135-32-98
Адрес организации: 119333 г.Москва, ул. Вавилова, д.40

Подпись Забежайло Михаила Ивановича и сведения удостоверяю

Ученый секретарь ФИЦ ИУ РАН
д.т.н. В.Н.Захаров