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.

Актуальность темы диссертационной работы

В последние годы, когда современные информационные технологии интенсивно внедряются во все сферы человеческой деятельности, а электронная информация определяет действия все большего числа людей и технических систем, вопросы защиты информации не могут оставаться чем-то второстепенным. Например, развитие новых банковских технологий, глобальной сети Internet, телекоммуникационной системы СВИФТ, пластиковых идентификационных карточек, которые находят применение не только в банках, но и в сфере торговли, промышленности, связи, делает чрезвычайно актуальной проблему защиты информации.

Основной параметр качества методов защиты информации – устойчивость к попыткам противника вскрыть «информацию». Такая устойчивость в криптографии называется стойкостью. Появление новых методов раскрытия информации приводит к необходимости пересмотра стойкости уже используемых методов защиты информации и разработки новых эффективных схем защиты информации в отношении действий интеллектуального агента, работающего в канале передачи и хранения информации.

Главной целью исследований автора диссертации является создание теоретических основ целочисленного расщепления, как новой математической процедуры, при которой целое число по базе другого целого представляется в виде некоторой цепочки k целых чисел. То есть, исходное число разбивается на k уровней, а затем используются соответствующие определения, понятия, утверждения, теоремы и математические модели такого целочисленного расщепления для изучения достигаемой защиты текстовой информации, а также для исследования и анализа вероятностной стойкости предложенного метода в целом.

С другой стороны, следует отметить, что разработанный метод целочисленного расщепления по своему характеру открывает новые области для применения концепции эволюции в применении к области защиты информации.

Поэтому фундаментальное исследование математических моделей метода расщепления и анализ вероятностной асимптотической стойкости этого метода является **актуальной** задачей, и можно сделать вывод, что тема диссертации соответствует специальности 1.2.3. Теоретическая информатика, кибернетика.

Содержание диссертационной работы

Диссертация Алхуссайн Амани включает в себя введение, четыре главы, заключение, библиографический список и два приложения.

Во введении дана общая характеристика диссертационной работы, обоснована актуальность темы диссертации, сформулированы цель и задачи исследования, представлено содержание основных результатов диссертации, изложена их научная новизна и практическая ценность.

В *первой главе* дан обзор состояния исследований в областях, которых касается тема диссертации. Она содержит описание существующих методов защиты, таких как методы замены, основанные на операции модульной арифметики, потоковый метод защиты, защита методом гаммирования и методом Вернама. Кроме того, дан обзор концепции эволюции, наблюдаемой в области защиты информации.

Вторая глава посвящена теоретической части исследования. В ней вводятся основные определения и понятия целочисленного расщепления. Отдельный раздел посвящен обсуждению схемы эволюции в связи с определением целочисленного расщепления – оригинального понятия, принадлежащего перу автора. В главе также представлены важные утверждения, касающиеся целочисленного расщепления, и их доказательство в связи с применением этой процедуры в области защиты информации, также принадлежащие автору.

В *третьей главе* представлено основное определение символьного расщепления и описан метод защиты информации на основе этого определения. Здесь построены математические модели применения символьного расщепления при защите текстовой информации. Важной частью этой главы является проведение вероятностного анализа математической модели использования символьного расщепления. Глава снабжена рядом шагов метода защиты и восстановления при применении разработанного в диссертации метода.

В *четвертой главе* представлено сравнение некоторых методов защиты с расщеплением. В частности, представлено сравнение между символьным расщеплением и китайской теоремой об остатках. Приведена иллюстрация работы предложенного в диссертации метода при защите информации.

В заключении сформулированы основные результаты, полученные в диссертационной работе.

Достоверность и новизна результатов диссертации

Новизна полученных результатов связана с расширением сферы применения модульной арифметики, с формулировкой на их основе новых определений, утверждений и теоретических схем, описывающих использование предложенного целочисленного расщепления в области защиты информации.

Диссертация содержит новые научные результаты, изложенные в каждой из её глав. В главе 2 автором диссертации даны определения целочисленного расщепления числа, функции отображения расщепления, обобщённого целочисленного расщепления и фактически «эволюции» целого числа на основе метода расщеплении, и доказаны строгие утверждения, позволяющие применять расщепление к защите информации. В главе 3 автором диссертации предложено новое математическое понятие – символьное расщепление, а также разработаны математические модели этапов защиты и последующего восстановления символа, кроме того доказаны строгие утверждения для исследования поведения вероятности несанкционированного восстановления символа по результату расщепления в случае простого и обобщённого расщепления. В главе 4 показано, что предложенный метод целочисленного расщепления лишен многих недостатков, присущих некоторым другим методам защиты информации в классе синхро-потоковых методов защиты, традиционным абсолютным стойким методам защиты и методам замены, основанным на операциях модульной арифметики.

Новым в диссертации является также серьезное продвижение в области модели эволюции при защите информации, обычно относимой только к природным организмам, в силу двух оригинальных аспектов работы.

Во-первых, в данной работе определена схема эволюции при защите информации методом расщепления. В этой схеме каждый следующий уровень защиты представляет собой новое поколение для исходного символа. Процесс «рождения» выполняется с использованием математической операции деления с остатком. Функция отображения, отражающая этап создания нового поколения, определяется и подвергается исследованию. Отбор «особей» в новое поколение осуществляется в соответствии с особью предыдущего поколения, как результат частного деления с остатком в конце поколения. Кроме того, доказанные в диссертации утверждения демонстрируют, что в эволюционном процессе новое поколение определяется однозначно, а соответствующее преобразование является инъективным.

Во-вторых, в приложении к диссертации предложен термин детерминированной генетической эволюции гамм, который используется как метод повышения уровня случайности некоторых генераторов псевдослучайных чисел, благодаря найденной в работе модификации генетического алгоритма на основе концепции эволюции по Холдену, что, в свою очередь, дополнительно затрудняет использование статистических методов для попыток автоматизации процесса вскрытия текста. Этот предложный подход является примером применения концепции эволюции для создания набора гамм, которые будут использоваться при защите информации методом расщепления.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

В ходе исследования рассмотренной защиты информации методом расщепления применяются методология и методы модульной арифметики, методы теории вероятностей и методы симметричной защиты информации с использованием генераторов псевдослучайных чисел, а также некоторые модели и концепции эволюции.

Математическая часть работы написана хорошими математическими средствами, позволяющими сформулировать необходимые утверждения, касающиеся построенных моделей. Для подтверждения теоретических положений автором проведены иллюстративные исследования на основе полученных математических формул, математических моделей и теорем. Все результаты четко сформулированы и доказаны, так что их обоснованность сомнений не вызывает.

Ценность для науки и практики результатов работы

Результаты, полученные в диссертационной работе, имеют теоретическую и практическую ценность. Теоретическая значимость диссертационной работы заключается в том, что в ней получены новые научные результаты, вносящие вклад в математическую теорию защиты информации, касающиеся свойства асимптотической стойкости. Практическая ценность результатов диссертация заключается в том, что содержащиеся в исследовании материалы, сформулированные в ней выводы и рекомендации, могут быть использованы в учебной деятельности при подготовке специалистов по направлению «Информационная безопасность». Кроме того, эти результаты могут быть практически использованы в приложениях, в том числе и криптографических, а также в рамках теории защиты информации для построения, исследования и оптимизации математических моделей реальных

систем защиты информации. Построенные модели и разработанные методы могут быть использованы в научных исследованиях.

Подтверждение опубликования основных результатов диссертации в научной печати

Основные результаты диссертации отражены в 25 публикациях, включая 7 работ, которые были опубликованы в журналах из перечня ведущих изданий, рекомендованного ВАК, включая 6 работ в периодических научных журналах, индексируемых в системе Scopus, и 1 патент на изобретение. Кроме того, результаты диссертации докладывались на различных российских и международных конференциях. В публикациях отражены все основные результаты диссертации.

Соответствие содержания автореферата основным положениям диссертации

Автореферат написан ясно и четко, он в полной мере дает представление о диссертационной работе, его содержание соответствует ее основным положениям.

Замечания по диссертационной работе

По работе имеются следующие замечания:

1. В диссертации отсутствует список сокращений и выводы по главам.
2. В диссертации отсутствует оценка времени защиты информации методом целочисленного расщепления.

Однако отмеченные недостатки не снижают научную ценность полученных в диссертационной работе результатов и не препятствуют положительной оценке диссертации.

Заключение по диссертационной работе

Диссертационная работа Алхуссайн Амани на тему «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов» представляет собой законченную научно-квалификационную работу, содержащую важные результаты, имеющие теоретическую и практическую значимость в практике надёжной защиты информации. В ней дано решение актуальной задачи разработки нового метода, основанного на использовании модульной арифметики, названного в диссертации целочисленным расщеплением, и разработки новых математических моделей защиты информации, кроме того, проведен вероятностный анализ стойкости

этого метода. Диссертация выполнена на высоком научном уровне, написана технически грамотно.

Работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата физико-математических наук, согласно п.2.2. раздела II Положения о присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Российский университет дружбы народов имени Патриса Лумумбы», утвержденного Ученым советом РУДН протокол № 12 от 23.09.2019 г., а ее автор, Алхуссайн Амани, заслуживает присуждения ученой степени кандидата физико-математических наук по специальности 1.2.3. Теоретическая информатика, кибернетика.

Официальный оппонент,
доктор физико-математических наук (05.27.01 – Твердотельная электроника, микроэлектроника),
главный научный сотрудник
Федерального государственного учреждения «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» (ФГУ ФНЦ НИИСИ РАН)

(Россия,117218, г. Москва, Нахимовский просп., 36, к. 1,
Тел.: +7 (499) 124-80-42; E-mail: vgredko@gmail.com)

Редько Владимир Георгиевич

«13» июля 2023 г.

Подпись руки В.Г. Редько заверяю
Начальник отдела кадров Попова

ФГУ ФНЦ НИИСИ РАН • ОГРН 1027700384909 • ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ • ФЕДЕРАЛЬНЫЙ НАУЧНЫЙ ЦЕНТР НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ СИСТЕМНЫХ ИССЛЕДОВАНИЙ РОССИЙСКОЙ АКАДЕМИИ НАУК • МОСКВА •
ОТДЕЛ КАДРОВ