ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА ПДС 0200.006 ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО АВТОНОМНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ ИМЕНИ ПАТРИСА ЛУМУМБЫ» ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 22.09.2023, протокол № 19

О присуждении Алхуссайн Амани, гражданке Российской Федерации, ученой степени кандидата физико-математических наук.

Диссертация «Вероятностный анализ стойкости защиты информации методом целочисленного расщепления символов» по специальности 1.2.3. Теоретическая информатика, кибернетика в виде рукописи принята к защите 23 июня 2023 года, протокол №14 диссертационным советом ПДС 0200.006 Федерального государственного автономного образовательного учреждения высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» (РУДН) Министерства науки и высшего образования Российской Федерации (117198, г. Москва, ул. Миклухо-Маклая, д.6.; приказ от 24 октября 2022 года № 599).

Соискатель Алхуссайн Амани 1985 года рождения, в 2013 году с отличием окончила магистратуру Федерального государственного автономного учреждения высшего образования «Российский университет дружбы народов» по направлению 01.04.02 «Прикладная математика и информатика».

С 9 августа 2013 года по 8 февраля 2018 года обучалась в аспирантуре РУДН по программе подготовки научно-педагогических кадров по направлению, соответствующему научной специальности 05.13.17 «Теоретические основы информатики».

С 15 декабря 2022 года по 14 июня 2023 года прикреплена для подготовки и защиты диссертации на соискание ученой степени кандидата наук по специальности 1.2.3. Теоретическая информатика, кибернетика по которой подготовлена диссертация.

В настоящее время не работает.

Диссертация выполнена на кафедре информационных технологий факультета физико-математических и естественных наук Федерального государственного автономного образовательного учреждении высшего образования «Российский университет дружбы народов имени Патриса Лумумбы» Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук, Стефанюк Вадим Львович, профессор кафедры информационных технологий факультета физико-математических и естественных наук Российского университета дружбы народов.

Официальные оппоненты:

- **Редько Владимир Георгиевич**, гражданин Российской Федерации, доктор физико-математических наук (специальность 05.27.01 - Твердотельная электроника, микроэлектроника), старший научный сотрудник, Федеральное государственное учреждение «Федеральный научный центр Научно-исследовательский институт системных исследований Российской академии наук» ФГУ ФНЦ НИИСИ РАН, главный научный сотрудник;
- **Забежайло Михаил Иванович**, гражданин Российской Федерации, доктор физико-математических наук (специальность 05.13.17 – Теоретические основы информатики), Федеральный исследовательский центр «информатика и управление» Российской академии наук (ФИЦ ИУ РАН), главный научный сотрудник;
- **Дужин Василий Сергеевич**, гражданин Российской Федерации, кандидат физико-математических наук (специальность 05.13.18 - Математическое моделирование, численные методы и комплексы программ), Федеральное государственное автономное образовательное учреждение высшего образования Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), доцент кафедры алгоритмической математики;

дали положительные отзывы о диссертации.

В заключение отзывов оппонентов указано, что диссертационная работа полностью соответствует п.2.2 раздела II Положения о присуждении учёных степеней в федеральном государственном автономном образовательном учреждении высшего образования «Российский университет дружбы народов», утверждённого Ученым советом РУДН, протокол № 12 от 23.09.2019 г.,, а ее автор, Алхуссайн Амани заслуживает присуждения ученой кандидата физико-математических наук.

Соискатель имеет 25 опубликованных работ по теме диссертации, в том числе 5 работ в периодических научных журналах, индексируемых в МБЦ Scopus, еще 1 работа опубликована в рецензируемом издании, рекомендованном перечнем ВАК. Соискатель имеет патент на изобретение № 2643502 «Способ шифрования методом расщепления». Общий объем публикаций 3,75 п.л.

Авторский вклад — 93%.

Наиболее значимые публикации:

1. Alhussain, A.H. Comparison between integer splitting cipher and traditional substitution ciphers, based on modular arithmetic // IOP Conf. Series: Materials Science and Engineering.– 2020.– Vol. 919.– 052004 .– pp. 1-6 (Scopus).
2. Alhussain, A.H. Asymptotic secrecy of the information protection by the usage of simple integer splitting method // IOP Conference Series: Materials Science and Engineering.– 2020.– Vol. 862 .– Issue 5, pp. 052032.– pp. 1-7 (Scopus).

3. Stefanuk, V.L. Alhussain, A.H. Absolute Secrecy Asymptotic for Generalized Splitting Method // Advances in Intelligent Systems and Computing .– 2020 .– 1156 AISC .– pp. 422-431 (Scopus).

4. Alhussain, A.H. The effectiveness of symbolic integer splitting method over both synchronous stream ciphers and perfectly secret ciphers// International Conference on Engineering Systems 2020.–Journal of Physics: Conference Series.– 2020.– Vol. 1687.– 012006.– pp. 01-08 (Scopus).

5. Alhussain A., Stefanuk V.L. The quantitative comparison between the integer splitting cipher and the traditional gamma cipher// CEUR Workshop Proceedings.– 2021.– Vol. 2899.– pp. 151–161(Scopus).

6. Алхуссайн А.Х., Некоторые результаты вероятностного анализа стойкости защиты информации методом целочисленного расщепления символов// Естественные и технические науки. – 2018.– № 12.– С. 380-381.

На автореферат диссертации поступили положительные, не содержащие критических замечаний отзывы от:

- **Фраленко Виталия Петровича**, гражданина Российской Федерации, кандидата технических наук (специальность 2.3.5 – Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей), ведущего научного сотрудника Федерального государственного бюджетного учреждения науки Институт программных систем им. А.К. Айламазяна Российской академии наук. В отзыве дана положительная оценка диссертации и указано её место в современных исследованиях защиты информации при её хранении и передаче, отзыв без замечаний.
- **Аверкина Алексея Николаевича**, гражданина Российской Федерации, кандидата физико-математических наук (специальность 01.01.09 – Дискретная математика и математическая кибернетика), доцента кафедры системного анализа и управления Федерального государственного бюджетного образовательного учреждения высшего образования «Университет «Дубна». В отзыве дана положительная оценка диссертации, отзыв без замечаний.
- **Жожикашвили Александра Владимировича,** гражданина Российской Федерации, доктора физико-математических наук (специальность 05.13.01 – Системный анализ, управление и обработка информации), старшего научного сотрудника Федерального государственного бюджетного образовательного учреждения науки «Институт проблем передачи информации им. А.А. Харкевича Российской академии наук». В отзыве дана положительная оценка диссертации и указано её место в современных исследованиях защиты информации при её хранении и передаче, отзыв без замечаний.
- **Ройзензона Григория Владимировича,** гражданина Российской Федерации, кандидата технических наук (специальность 05.13.10 – Управление в социальных и экономических системах), доцента кафедры «Прикладной математики и искусственного интеллекта» Федерального государственного

бюджетного образовательного учреждения высшего образования Национального исследовательского университета «Московский энергетический институт». В отзыве дана положительная оценка диссертации в целом и сделано замечание по поводу изложения различных дополнительных количественных оценок алгоритмов для выбора наиболее предпочтительного подхода при решении конкретной практической задачи.

Выбор официальных оппонентов обосновывается их высокой квалификацией, наличием научных трудов и публикаций, соответствующих теме оппонируемой диссертации.

Выбор **Редько Владимира Георгиевича** в качестве официального оппонента обусловлен тем, что Редько В.Г. является крупным специалистом в области исследования эволюции и вопросов, связанных с использованием математических моделей в моделировании. В частности, в сфере его научных интересов находится вопрос о модели и концепции эволюционной кибернетики, что является одним из важных аспектов диссертационного исследования соискателя, поскольку метод расщепления создает поколения чисел на основе арифметической операции деления с остатком, что приводит к новой концепции эволюции, основанной на методе расщепления.

Основные публикации Редько В.Г. по тематике диссертационного исследования:

1. Red'ko V.G., Modeling of Interaction between Learning and Evolution for Kauffman's NK Networks // Studies in Computational Intelligence, 2022, vol. 1008. Springer, Pp. 119–125. DOI: 10.1007/978-3-030-91581-0_16
2. Red'ko V.G., Some aspects of adaptation and evolution: Comment on "Dynamic and thermodynamic models of adaptation" by A.N. Gorban et al. // Physics of Life Reviews, 2021, 37, Pp.108–110. DOI:10.1016/j.plrev.2021.04.004.
3. Red'ko V.G., Model of evolution and learning of Kauffman's NK networks. Features of the interaction between learning and evolution// CEUR Workshop Proceedings, 2021, 2965, Pp. 238–243.
4. Saakian D.B., Red'ko V.G., The comparative analysis of prebiological evolution models// Chinese Journal of Physics, 2020, Vol. 66, Pp. 180-186. DOI:10.1016/j.cjph.2020.03.033
5. Red'ko V. G., Modeling of Cognitive Evolution// 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, Pp. 54-59, DOI:10.1109/IDAACS.2019.8924363.

Выбор **Забежайло Михаила Ивановича** в качестве официального оппонента обусловлен тем, что Забежайло М.И. является крупным специалистом в области теории вероятностей, криптографии и защиты информации. В частности, в сферу его научных интересов входят проблема информационной безопасности,

методы оценки защищенности компьютерных систем, а также вероятностные оценки достоверности эмпирических выводов, что является одним из важных аспектов диссертационного исследования соискателя.

Основные публикации Забежайло М.И. по тематике диссертационного исследования:

1. Грушо А.А., Грушо Н.А., Забежайло М.И., Тимонина Е.Е. Безопасность обработки больших данных// Проблемы информационной безопасности. Компьютерные системы,2021, № 4, с. 137-143
2. Grusho A.A., Zabezhailo M.I., Piskovski V.O., Timonina E.E. Industry 4.0: Opportunities and Risks in the Context of Information Security Problems// Automatic Documentation and Mathematical Linguistics, издательство Allerton Press Inc. (United States), 2020, Vol. 54, p. 55-63 DOI:10.3103/S000510552002003X
3. Грушо А.А., Забежайло М.И., Смирнов Д.В., Тимонина Е.Е. О вероятностных оценках достоверности эмпирических выводов// Информатика и ее применения, 2020, том 14, № 4, с. 3-8 DOI: 10.14357/19922264200401
4. Grusho A.A., Grusho N.A., Zabezhaylo M.I., Timonina E.E. Protection of Valuable Information in Information Technologies// Automatic Control and Computer Sciences, издательство Allerton Press Inc. (United States), 2018, Vol. 52, N 8, p. 1076-1079 DOI: 10.3103/S0146411618080138

Выбор **Дужин Василий Сергеевич** в качестве официального оппонента обусловлен тем, что Дужин В.С. является крупным специалистом в области компьютерной алгебры, алгоритмической математики и теории вероятностей. В частности, в сфере его научных интересов находится исследование проблем асимптотики вероятностей процессов и моделирование асимптотики процессов, что является одним из важных аспектов исследования кандидатской диссертации в части асимптотической стойкости расщепления.

Основные публикации Дужин В.С. по тематике диссертационного исследования:

1. Васильев Н.Н., Дужин В.С., Кузьмин А.Д. О сходимости путей выталкиваний в алгоритме RSK к их предельной форме: численные эксперименты // Информационно-управляющие системы. 2021. № 6. С. 2-9. DOI: https://doi.org/10.31799/1684-8853-2021-6-2-9
2. V. Duzhin, N. Vassiliev , Randomized Schützenberger's Jeu De Taquin and Approximate Calculation of the Cotransition Probabilities of a Central Markov Process on the 3D Young Graph// Journal of Mathematical Sciences, 2020, Vol. 251, No. 3, pp. 363-374. DOI:10.1007/s10958-020-05097-1
3. V. Duzhin, N. Vassiliev, Randomized Schützenberger's jeu de taquin and approximate calculation of co-transition probabilities of a central Markov process on the 3D Young graph //Zapiski Nauchnykh Seminarov POMI, 2019, Vol. 485, Pp.90–106.

4. Васильев Н.Н., Дужин В.С., Кузьмин А.Д., Исследование свойств классов эквивалентности перестановок с помощью обратного преобразования Робинсона - Шенстеда - Кнута// Информационно-управляющие системы.2019, 1, С. 11-22 . doi:10.31799/1684-8853-2019-1-11-22.
5. Duzhin V., Vasilyev N., Modeling of an Asymptotically Central Markov Process on 3D Young Graph // Mathematics in Computer Science, 2017, Vol. 11, Pp. 315–328. https://doi.org/10.1007/s11786-017-0314-4

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

– предложены

- новые процедуры модулярной арифметики — целочисленное расщепление и обобщенное целочисленное расщепление, обобщающие известную арифметическую операцию деления с остатком;
- оригинальный подход к защите информации на основе целочисленного расщепления;

– разработаны:

- новый математический метод защиты информации, состоящий в замене каждого символа передаваемого текста на последовательность k целых чисел;
- алгоритм защиты информации на основе целочисленного расщепления, позволяющий управлять уровнем защиты информации;

– доказаны

- единственность целочисленного расщепления числа по базе, а также инъективность и обратимость процедуры целочисленного расщепления;
- ослабление возможности раскрытия исходного текста за счет учета его содержания при применении метода расщепления;
- асимптотическая стойкость расщепления с увеличением числа k, названном в диссертации уровнем расщепления.

Теоретическая значимость исследования обоснована тем, что:

– предложены

- новая процедура в модулярной арифметике, названная целочисленным расщеплением;
- новый подход к исследованию защиты информации, который усложняет задачи злоумышленника по сравнению с традиционными известными методами защиты информации, использующими математическую модульную арифметику;
- новый подход к исследованию эволюционной модели, основанный на целочисленном расщеплении, который очень близок к эволюционной модели, используемой в генетическом алгоритме Дж. Холланда.

– исследованы

- свойства целочисленного расщепления;
- асимптотическая стойкость предложенного метода шифрования.

Применительно к проблематике диссертации результативно

– использованы

- теоремы и методы модулярной арифметики;
- методы вероятностного анализа стойкости методов защиты текстовой информации;
- генераторы псевдослучайных чисел для создания потока гамм, которые используются в процессе шифрования и дешифрования;
- эволюционные принципы в системах информационной безопасности;
- пакеты Matlab, Minitab и IBM SPSS Statistics для проведения тестов;
- объектно-ориентированный язык программирования C# для создания криптографической системы, основанной на предложенном методе целочисленного расщепления.

– раскрыты

- возможности использования предложенной процедуры целочисленного расщепления в задачах защиты информации.

– проведено

- сравнение предложенного метода и хорошо известного синхронного потокового метода защиты информации;
- исследование поведения вероятности несанкционированного восстановления исходного текста при различных значениях уровня расщепления.

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

– разработана и реализована

- на объектно-ориентированном языке программирования C# и протестирована на серии примеров криптографическая система, основанная на оригинальной концепции целочисленного расщепления.

– определены

- условия, при которых возможно извлечение исходного целого числа из последовательности чисел на основе процедуры целочисленного расщепления.

– представлены

- иллюстрации защиты информации при различных уровнях расщепления;
- методические указания по эффективному использованию метода расщепления в задачах защиты информации;

- рекомендации по выбору параметра, названного базой, обеспечивающего возможность использования целочисленного расщепления для защиты текстовой информации.

Оценка достоверности результатов исследования выявила:

– теория

- дополняет известные результаты по численному и аналитическому исследованию криптографических систем и хорошо согласуясь с ними.

– идея базируется

- на применении известных математических методов модулярной арифметики, математической теории вероятностей и математической статистики, методов генетических алгоритмов, а также методов симметричной защиты информации с использованием генераторов псевдослучайных чисел.

– установлено

- качественное и количественное совпадение авторских результатов с результатами других авторов, а также с аналитическими решениями в тех случаях, когда это возможно;
- результаты работы достаточно полно представлены в публикациях в авторитетных рецензируемых изданиях.

Личный вклад соискателя состоит в разработке новых процедур модулярной арифметике и исследовании их свойств, а также в разработке на их основе метода защиты информации и его реализации в виде криптографического комплекса, написанного на объектно-ориентированном языке программирования C#.

Диссертационное исследование Алхуссайн Амани является законченной научно квалификационной работой, в которой решена актуальная задача проектирования асимптотически стойкого метода защиты текстовой информации на основе оригинальной концепции целочисленного расщепления. Полученные автором результаты достоверны, основные выводы и заключения обоснованы.

Заключение диссертационного совета подготовлено доктором физико-математических наук, и.о. заведующего кафедрой математического моделирования и искусственного интеллекта РУДН М.М. Малых, доктором физико-математических наук, профессором, профессором Математического института им. С.М. Никольского РУДН Е.Б. Ланеевым и доктором физико-математических наук, доцентом, профессором Департамента математики Финансового Университета при Правительстве РФ Е.Ю. Щетининым.

На заседании 22 сентября 2023 г. диссертационный совет принял решение присудить Алхуссайн Амани ученую степень кандидата физико-математических наук.

При проведении тайного голосования диссертационный совет в количестве 10 человек, из них 3 доктора наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 15 человек, входящих в состав совета, проголосовали: за – 10, против – 0, недействительных бюллетеней – 0.

Председательствующий на заседании:
заместитель председателя диссертационного
совета ПДС 0200.006, доктор
физико-математических наук, профессор Кулябов Д. С.

Учёный секретарь диссертационного совета
ПДС 0200.006, кандидат физико-
математических наук, доцент Демидова А. В.

«22» сентября 2023 г.