АННОТАЦИЯ
диссертационной работы Хомпыш Ардабека на тему
«Разработка и исследование алгоритма защиты информации с использованием непозиционных систем счисления»,
представленной на соискание степени доктора философии (PhD) по специальности «6D100200- Системы информационной безопасности»

Актуальность темы исследования. В настоящее время Казахстан сталкивается с исторической необходимостью перехода от индустриального общества к принципиально новому уровню общественного и экономического развития, определяемому жесткими требованиями современной научно-технологической революции. Учитывая высокий уровень развития информационного общества и информационной экономики во многих развитых странах, вопросы дальнейшего развития в Казахстане становятся одним из приоритетов. Так как материальной базой информационного общества является информационная экономика, то информационные ресурсы приобретают особую значимость. При этом информационные ресурсы рассматриваются как стратегические ресурсы страны, требующие постоянной защиты от несанкционированного доступа других пользователей.

Высокая степень автоматизации, широкое внедрение компьютерных систем в различные сферы деятельности человека делают автоматизированные системы обработки данных очень уязвимыми к киберугрозам, а общество становится зависимым от уровня безопасности используемых информационных технологий. Поэтому безопасность циркулирующей и передаваемой информации становится важной характеристикой любой компьютерной системы независимо от ее сложности и назначения.

Одним из приоритетов стратегии развития любого государства является национальная безопасность, а одним из важнейших ее элементов является информационная безопасность. Поэтому актуальными задачами становятся создание новых технологий защиты информации, ограничение доступа к ней, обеспечение необходимого уровня защиты информации и создание средств защиты информации, отвечающих современным требованиям.

В Концепции кибербезопасности «Киберщит Казахстана» (от 30 июня 2017 года) указано, что необходимы «Предоставление приоритета исследованиям и собственной школе прикладной математики по разработке **средств криптографической защиты информации, криптологии**, разработок по программируемым логическим интегральным схемам, квантовой криптографии и разработке защиты систем передачи, обработки и хранения информации, а также систем информационной безопасности» и «Преодоление проблемы невысокой востребованности отечественных разработок, т. к. кибербезопасность в конечном итоге зависит от уровня развития отечественной IT-отрасли и электронной промышленности».

В связи с этим, НИР направленные на развитие отечественных систем обеспечения информационной безопасности являются актуальными для нашей страны.

В первую очередь это связано с постоянно растущими темпами научно-технического прогресса, который ведет к совершенствованию компьютерных технологий. Их появление не только поднимает новые вопросы безопасности, но и предлагает новые решения проблем, а на сложность решения проблемы информационной безопасности влияют:

- увеличение объема информации, собираемой, хранимой и передаваемой с использованием компьютерных технологий;
- расширение круга пользователей, имеющих доступ к ресурсам компьютерной системы;
- усложнение режимов работы аппаратной части компьютерной системы;
- увеличение количества технических средств и коммуникаций в автоматизированных системах обработки данных;
- широкое использование новых инфокоммуникационных технологий.

Чтобы минимизировать последствия несанкционированного доступа, необходимо создать систему безопасности. Целью создания такой системы является предотвращение последствий умышленного или случайного деструктивного воздействия, в результате которого информация может быть уничтожена, модифицирована или похищена. При этом эффективная система безопасности должна обеспечивать:

- конфиденциальность всей информации или ее важной части;
- достоверность информации (полнота, точность, достоверность, целостность, аутентичность), работоспособность компонентов системы в любое время;
- своевременный доступ пользователей к необходимым им информационным и системным ресурсам;
- дифференциация ответственности за нарушение установленных правил информационных отношений;
- оперативный контроль процессов управления, обработки и обмена информацией.

Следует отметить, что среди описанных свойств системы безопасности в зависимости от объекта защиты могут быть разные расстановки приоритетов. В условиях защиты государственных секретов особое внимание уделяется конфиденциальности информации. Это определяет встречные риски, целью которых является снижение вероятности возникновения угрозы или минимизация последствий реализации угрозы. Эти меры совместно формируют политику безопасности. Исследования многих зарубежных и отечественных ученых показывают, что среди организационных, методических и технических мероприятий важное место занимают методы криптографической защиты информации.

Современные криптографические методы, включая итерационные блочные шифры, являются одним из самых популярных инструментов для безопасного обмена информацией в высокоскоростных сетях передачи данных. Широкое использование информационных технологий и быстрый рост вычислительной мощности создают угрозу криптоанализа известных шифров.

Исследования по созданию средств криптографической защиты данных зачастую направлены на защиту конфиденциальной информации, поэтому использование готовых зарубежных решений небезопасно. Исследования по развитию отечественной криптографической защиты информации, в том числе разработка алгоритмов шифрования, актуальны и необходимы.

Целью диссертации является создание алгоритма шифрования информации с использованием возможностей непозиционных полиномиальных систем счисления (НПСС), анализ криптографической стойкости созданного алгоритма, программная реализация алгоритма.

Для достижения целей исследования были поставлены следующие задачи:

- Обзор и анализ методов криптографической защиты информации;
- Анализ требований и критериев эффективности систем криптографической защиты информации;
- Разработка алгоритма симметричного блочного шифрования на основе непозиционной полиномиальной системы счисления;
- Программная реализация созданного алгоритма симметричного блочного шифрования;
- Исследование криптостойкости разработанного алгоритма симметричного блочного шифрования.

Объект исследования - алгоритмы криптографической защиты и методы их анализа.

Предмет исследования - алгоритмы шифрования и генерации раундовых ключей на основе непозиционных полиномиальных систем счисления.

Методы исследования - модульная арифметика, непозиционные полиномиальные системы счисления, статистические тесты, критерии рассеяния битов, методы криптоанализа.

Научная новизна исследования. Проблема обеспечения информационной безопасности остается на сегодняшний день нерешенной. В связи с этим было проведены исследование, достигнут ряд успехов, а научные результаты опубликованы в высокорейтинговых журналах. Новизна этих научных результатов являются основой диссертации. В частности:

- создан новый алгоритм симметричного блочного шифрования с использованием метода преобразования EM;
- создана таблица замены S-блока, отвечающая требованиям защиты от криптоанализа;
- разработан алгоритм генерации раундовых ключей;
- для оптимизации скорости шифрования создана индексная таблица выбранных рабочих оснований.

Теоретическая и практическая значимость работы. Результаты диссертационного исследования могут быть использованы для защиты информации в телекоммуникационных и информационных системах и сетях, системах электронного документооборота, а также программных продуктах отечественных информационно-коммуникационных технологий, для защиты конфиденциальной информации государства и физических лиц от

несанкционированного доступа и хищения. Кроме того, их можно использовать в образовательном процессе в высшей школе, а также при разработке новых систем криптографической защиты.

Главный вывод защиты. Новый алгоритм симметричного блочного шифрования был разработан для защиты информации на основе метода преобразования EM, который отвечает основным требованиям современных алгоритмов симметричного блочного шифрования.

Кроме того, использованные в алгоритме таблицы подстановки S-блока исследовались путем линейного и дифференциального криптоанализа предложенного S-блока, а результаты сравнивались с известными алгоритмами. Для увеличения скорости шифрования алгоритма использовалась непозиционная полиномиальная система счисления и индексная таблица выбранных рабочих оснований.

Рекомендуемые результаты для защиты. Разработан новый алгоритм блочного шифрования. Криптографическая стойкость алгоритма проверялась с использованием различных методов криптоанализа и представлением результатов.

Внедрение результатов исследований. Результаты диссертационного исследования прошли апробацию в «Институте информационных и компьютерных технологий», «Лаборатории информационной безопасности» и реализованы в рамках проекта BR05236757-«Разработка программных и программно-аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения».

Апробация результатов диссертации. Основные результаты исследования были представлены и обсуждены на следующих конференциях и семинарах:

- Материалы XLI Международной научно-практической конференции КазАТК им. М. Тынышпаева на тему: «Инновационные технологии на транспорте: образование, наука, практика» (3-4 апреля 2017 г., Алматы, Казахстан).
- Научная конференция «Современные проблемы информатики и компьютерных технологий» института информационных и вычислительных технологий (29-30 июня 2017 г., Алматы, Казахстан);
- II Международная научно-практическая конференция «Информатика и прикладная математика» (27-30 сентября 2017 г., Алматы, Казахстан);
- III Международная научно-практическая конференция «Информатика и прикладная математика» (26-29 сентября 2018 г., Алматы, Казахстан);
- «Наука XXI века: новый подход»: Материалы XXIII молодёжной международной научно-практической конференции студентов, аспирантов и молодых учёных. (22-23 май 2019 г., Санкт-Петербург, Россия);
- IV Международная научно-практическая конференция «Информатика и прикладная математика» (25-29 сентября 2019 г., Алматы, Казахстан);

- Материалы международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020» (15 января 2020 г., Алматы, Казахстан);

- Научно-практические семинары на тему «Актуальные проблемы информатики, математики и управления» института информационных и вычислительных технологий (2017-2020 гг., Алматы, Казахстан);

- Научные семинары факультета «Информационные технологии» Казахского национального университета им. аль-Фараби (2017-2020 гг., Алматы, Казахстан).

По теме диссертации опубликованы 14 статей и получено 1 авторское свидетельство:

1. Хомпыш А. Позициялық емес санау жүйесін қолданылуы, «Көліктегі инновациялық технологиялар: білім, ғылым, тәжірибе" атты XLI Халықаралық ғылыми-практикалық конференцияның материалдары. – Алматы, 2017. – 64-66 б.

2. Капалова Н.А., Хомпыш А. Позициялық емес санау жүйесін қолданып, Эль-Гамаль шифрлау алгоритмінің модификациясын құру, Қ.И. Сәтбаева атындағы Қазақ Ұлттық техникалық зерттеу университетінің, Хабаршысы – Алматы, 2017. – №4 (122). – 506-510 б.

3. Хомпыш А. Эль-Гамаль шифрлау алгоритмінің мобильдік қосымшасын құру, «Есептеуіш технологиялар және информатиканың заманауи мәселелері» атты ғылыми конференция материалдары. – Алматы, 2017. – 281-284 б.

4. Хомпыш А. Позициялық емес санау жүйесін негізінде құрылған Эль-Гамаль шифрлау алгоритмін мәліметтер алмасу желісінде пайдалану, II Халықаралық «Информатика және қолданбалы математика» ғылыми конференция материалдары. – Алматы, 2017. – 157-161 б.

5. Капалова Н.А, Хомпыш А., Алгазы К.Т. Модуль бойынша дәрежеге шығару негізінде ақпаратты криптографиялық қорғау алгоритмінің модификациясы, М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясының, Хабаршысы – Алматы, 2018. – №4 (107). – 247-253б.

6. Хомпыш А. Модуль бойынша дәрежеге шығару операциясы негізінде ақпаратты криптографиялық қорғау алгоритмін бағдарламалық жүзеге асыру, III Халықаралық «Информатика және қолданбалы математика» ғылыми конференция материалдары. – Алматы, 2018. – 167-171 б.

7. Хомпыш А. Криптостойкость S-блоков в алгоритме шифрования на основе ЕМ, «Наука XXI века: новый подход»: Материалы XXIII молодёжной международной научно-практической конференции студентов, аспирантов и молодых учёных. – г. Санкт-Петербург, 2019. – С. 15-19.

8. Дюсенбаев Д.С., Сақан Қ.С., Хомпыш А., Алгазы К. «MODNPSS14» шифрлау алгоритміне криптографиялық талдау, М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясының, Хабаршысы – Алматы, 2019. – №3 (110). – 235-243б.

9. Бияшев Р.Г., Капалова Н.А., Алғазы К.Т., Дюсенбаев Д.С., Хомпыш А. Криптоанализ генератора псевдослучайных последовательностей и ее модификация, Вестник Казахского национального исследовательского

технического университета имени К.И. Сатпаева. – Алматы, 2019. – №3 (133). – с.179-185.

10. Хомпыш А., Капалова Н.А., Алгазы К. ЕМ түрлендіру әдісі негізінде жасалған блокты шифрлеу алгоритміне жүргізілген бағалау тесттері, IV Халықаралық "Информатика және қолданбалы математика" ғылыми конференциясы. – Казахстан, Алматы – 2019. – 2. – 580-587 б.

11. Бияшев Р.Г., Алгазы К., Хомпыш А. Исследование разработанных алгоритмов по критерию «лавинного эффекта», Материалы международной научно-практической конференции «Актуальные проблемы информационной безопасности в Казахстане АПИБК-2020». Алматы – 2020. – с.107-119.

12. Бияшев Р.Г., Смоларш А., Алгазы К.Т., Хомпыш А. Encryption algorithm ‘’Qamal NPNS’’ based on a nonpositional polynomial notation, Journal of Mathematics, Mechanics and Computer Science, «Хабаршы» ҚазҰУ – Алматы, 2020. – №1 (105). – С. 198-207.

13. Kapalova N.A., Khompysh A., Müslüm A., Algazy K. A block encryption algorithm based on exponentiation transform, Cogent engineering (2020), 7:1788292, ISSN 2331-1916, V. 7. – P. 1-12

14. Хомпыш А., Капалова Н.А., Алгазы К. Исследование разработанного алгоритма на основе преобразования ЕМ по критерию «лавинного эффекта», М.Тынышбаев атындағы Қазақ көлік және коммуникациялар академиясының, Хабаршысы – Алматы, 2020. – №3 (114). – 284-292б.

15. Хомпыш А., Капалова Н.А. Программа шифрования файлов «CryptoEM v1.0.1», ЭЕМ-ге арналған бағдарламаға алынған авторлық құқық куәлігі, №5450, 24 қыркүйек 2019 ж.

Структура и объем диссертации. Структура диссертации состоит из введения, 3 глав, заключения, списка использованных источников и 4 приложений.

Во введении обосновывается актуальность проблемы построения алгоритмов криптографической защиты информации, отвечающих требованиям, предъявляемым к современным блочным алгоритмам, формулируется цель работы, определяется общая научная задача и ее разделение на конкретные научные задачи, определяется объект и тема исследования, представляются основные положения, отражены новизна диссертационной работы, представленной на защиту, и ее результаты.

В первом разделе с учетом того, что одним из наиболее эффективных способов решения упомянутых в диссертации задач являются криптографические методы, рассматриваются основные понятия криптографических методов, термины и базовые классы криптографических преобразований, основные этапы разработки алгоритмов симметричного блочного шифрования, требования к алгоритмам блочного шифрования.

Во втором разделе описан разработанный симметричный блочный алгоритм шифрования на основе непозиционных полиномиальных систем счисления, а также подходы формирования системы рабочих оснований для алгоритма шифрования на базе непозиционных полиномиальных систем счисления, основные параметры алгоритма, схема зашифрования и

расшифрования, а также метод преобразования EM, таблица замены S-блока, порядок работы и быстрого возведения в степень, и алгоритм выработки раундовых ключей.

В третьем разделе описан созданный программный комплекс нового блочного алгоритма шифрования, представленного в диссертационной работе. Для проверки криптостойкости алгоритма были представлены результаты проверки статистической безопасности шифрованного текста с помощью оценочных и графических тестов. Кроме того, описаны результаты исследования алгоритма с помощью критерия рассеяния бит, линейного и дифференциального криптоанализа S-блока, дифференциального анализа для всех модификаций алгоритма.

В заключении были сформулированы основные итоги и результаты работы.