АННОТАЦИЯ

диссертационной работы **Усатовой Ольги Александровны**
на тему: «Разработка и исследование алгоритма аутентификации пользователей информационно–коммуникационных систем», представленной на соискание степени доктора философии (PhD) по специальности
6D100200 – «Системы информационной безопасности»

С момента приобретения независимости Республики Казахстан ее первый президент Нурсултан Абишевич Назарбаев неоднократно акцентировал внимание на необходимость защиты интересов граждан в Республике Казахстан. Так, в Послании Президента страны народу Казахстана от 10 октября 1997 года «Казахстан – 2030. Процветание, безопасность и улучшение благосостояния всех казахстанцев» долговременным приоритетом установлена государственная защищенность, где одним из важных направлений является информационная безопасность.

Комплексный механизм процессов обеспечения информационной безопасности нашей Республики охватывает организационные, социальные, технические и программные подходы, способные осуществлять конституционные права и свободу человека, гражданина в области получения информации, пользования ею в целях защиты конституционного строя, суверенитета и территориальной целостности Республики Казахстан, финансовой, а также общественной устойчивости, формирование выгодного интернационального партнерства в сфере информативной защищенности.

Принятый 6 января 2012 года Закон «О национальной безопасности Республики Казахстан» содержит необходимые статьи, в них даны чёткие определения с позиции государства, затрагивающих вопросы информационной безопасности страны в целом и граждан в частности.

На законодательном уровне в Республике Казахстан формируется и закрепляется национальная концепция обеспечения информационной безопасности, электронного документооборота, автоматизированных информационных систем, ресурсов, ИКТ, а также важных объектов.

При построении и эксплуатации телекоммуникационных сетей связи необходимо учитывать требования Республики Казахстан о соблюдении национальной безопасности в области связи. Об этом свидетельствует последняя действующая поправка статьи «О полномочиях государственных органов Республики Казахстан» от 27 декабря 2017 года.

21 мая 2013 года был принят закон Республики Казахстан (РК) № 94–V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 28.12.2017 г.), в нем регулируются отношения, связанные со сбором и обработкой, а также защитой персональных данных. Не маловажными являются Закон РК от 24 ноября 2015 года № 418–V «Об информатизации» (с изменениями по состоянию на 01.01.2020 г.) и Закон РК от 7 января 2003 года № 370–II «Об электронном документе и электронной цифровой подписи» (с изменениями по состоянию на 25.11.2019г.).

Развитие информационно–телекоммуникационных технологий позволяют использовать новые возможности в сети Интернет. Появилась возможность производить удалённые покупки товаров из любой точки страны, отслеживать состояние и исполнение работ, не присутствуя в местах их проведения. В настоящее время существует возможность оформить практически любую справку, не выходя из дома, благодаря электронной цифровой подписи и информационному порталу государственных услуг.

В Республике Казахстан 12 декабря 2017 года, Постановлением Правительства №827 была утверждена программа государства «Цифровой Казахстан». В данной программе основным аспектом является развитие экономики страны и повышение жизнедеятельности населения, основанной на совершенствовании и ускорении развития инфокоммуникационных технологий и также создание цифровой экономики. Основное внимание уделено обеспечению информационной безопасности в сфере информационно–коммуникационных технологий и консолидации кибербезопасности автоматизированных информационных систем в нашей стране.

С развитием технологического прогресса и общего уровня информатизации появляются также и новые угрозы. Киберпреступность позволяет злоумышленникам совершать противоправные и незаконные действия, находясь в тысячах километрах от цели их атаки. В Послании народу Казахстана «Третья модернизация Казахстана: Глобальная конкурентоспособность» Президент Республики Казахстан отмечал, что все большую актуальность приобретает борьба с киберпреступностью. В связи с этим была разработана и утверждена Постановлением Правительства Республики Казахстан от 30 июня 2017 года №407 Концепция кибербезопасности («Киберщит Казахстана»), в ней определены основные направления реализации государственной политики в сфере защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечения безопасного использования информационно–коммуникационных технологий

Информационные технологии стали неотъемлемой частью нашей жизни, в связи с этим осуществляется автоматизация многих процессов жизнедеятельности человека. Большая часть информации хранится в информационных системах, которую необходимо защищать. В атаках на информационные системы злоумышленники используют как ошибки в написании и администрировании программ, так и методы социальной психологии для получения желаемой информации. Разработчики ресурсов, на которых предполагается работа с данными пользователей, обязаны эти данные защищать и предотвращать возможность их утечек. Одной из основных проблем РК является слабое развитие отечественной индустрии информационной безопасности, в частности, в разработке средств криптографии. В Казахстане, в настоящее время, в действующих системах защиты электронных данных используются зарубежные криптографические алгоритмы и стандарты. Исследования, касающиеся безопасности данных, непосредственно объединены с государственными секретами и применение

зарубежных готовых решений весьма рискованно, в связи с этим необходимо формировать собственные ресурсы для безопасности информации.

В ИИВТ КН МОН РК проводятся научно–исследовательские работы (НИР) по криптографической защите информации и разграничению доступа. Этими НИР занимаются сотрудники Лаборатории информационной безопасности (заведующий лабораторией, д.т.н., проф. Бияшев Р.Г., академик НАН РК Калимолдаев М.Н., д.т.н., асс. проф. Нысанбаева С.Е., ВНС, к.т.н. Капалова Н.А., PhD Бегимбаева Е.Е., научные сотрудники Рог О.А., Дюсембаев Д.С., Алгазы К.Е., Варенников А.В.и другие). На осуществление этой деятельности в ИИВТ КН МОН РК выдана государственная лицензия № 549 от 03 июля 2017 г. Комитетом национальной безопасности РК.

Одними из основных средств защиты информационных систем от постороннего вмешательства являются идентификация и аутентификация, так как механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами. Аутентификация и идентификация пользователя являются взаимозависимыми действиями распознавания и проверки подлинности.

Основной целью аутентификации пользователя информационной системы является снижение угроз безопасности, а именно нарушение конфиденциальности и целостности информации. Несанкционированный доступ – один из самых распространенных видов нарушений, представляющий непосредственную угрозу работоспособности системы.

Аутентификация используется для доступа к социальным сетям, электронной почте, интернет магазинам, интернет–банкингу, платежным системам и т.д. Аутентификация пользователя классифицируется по следующим типам:

– аутентификация на основе пароля: она проводится по одноразовым и многоразовым паролям. Многоразовый пароль задает пользователь, а система хранит его в базе данных. Он является одинаковым для каждой сессии. К ним относятся PIN–коды, слова, цифры, графические ключи. Одноразовые пароли для каждой сессии являются разными;

– комбинированная аутентификация, которая происходит с использованием нескольких методов, например, парольных и криптографических сертификатов. Она требует специальное устройство для считывания информации;

– биометрическая аутентификация: она предотвращает утечку или кражу персональной информации. Проверка проходит по физиологическим характеристикам пользователя, например, по отпечатку пальца, сетчатке глаза, распознавание лица и тембру голоса.

В настоящее время использование парольной аутентификации является доступной и распространенной из–за простоты применения. Этот метод защищенности ведет к увеличению прочности концепции защиты информации. Одним из эффективных методов защиты информации является двухфакторная аутентификация для входа в систему. Она предполагает двойную защиту данных посредством привязки аккаунта к системе защиты. После привязки

пользователю необходимо будет взаимодействовать с этой системой для верификации данных.

Задачами безопасности информации, разграничение доступа и аутентификации на основе второго фактора, занимались зарубежные ученые Эдна Элизабет, С. Нивета, Фазех Садат Бабамир, Мурвет Кирчи, И Юй, Цзинша Хе, Нафей Чжу, Фанбо Цай, Мухаммед Салман Патан и другие. Важной частью является также защита информации, хранящаяся в базах данных и программно–аппаратные средства для обработки и передачи информации. Существенный вклад в развитие этого направления был внесен также зарубежными учеными Мещеряковым Р. В., Исхаковым А.Ю., Полтавцевой М.А. и другие.

В связи с вышеуказанным, тема данной диссертационной работы по разработке и исследованию алгоритма аутентификации пользователей информационно–коммуникационных систем на основе второго фактора является актуальной. В данной диссертации в качестве второго фактора является одноразовый пароль.

Актуальность исследования заключается в необходимости:

– реализации задач, поставленных в Государственной программе правительства Республики Казахстан и Концепции кибербезопасности («Киберщит Казахстана»), направленных на развитие государственной политики в сфере защиты электронных информационных ресурсов, систем и сетей телекоммуникаций, обеспечения безопасного использования информационно–коммуникационных технологий;

– разработки отечественных Казахстанских систем обеспечения информационной безопасности;

– применения политики парольной двухфакторной аутентификации с целью повышения надежности систем защиты информации.

Цель диссертационной работы: разработка, исследование и реализация алгоритма двухфакторной аутентификации для обеспечения защиты информации в информационно–коммуникационных системах.

Задачи исследования, реализующие цель диссертационного исследования:

1. Проведение обзора и анализа существующих систем защиты информации в информационно–коммуникационных системах и алгоритмов многофакторной аутентификации.
2. Разработка алгоритма аутентификации пользователей информационно–коммуникационных систем с использованием одноразового пароля.
3. Создание информационной системы для обеспечения целостности и защиты информации в информационно–коммуникационных системах.

Объект исследования: система защиты информации от несанкционированного доступа при аутентификации пользователя на основе второго фактора.

Предметом исследования являются процессы информационного взаимодействия пользователей информационно–коммуникационных систем и их аутентификация с помощью цифрового одноразового пароля.

Научная новизна проведенных исследований и полученных в работе

результатов:

– разработан алгоритм двухфакторной аутентификации пользователя, основанный на генерации тригонометрических функций путем усложнения масштабирования функций при вычислении одноразового пароля. Масштабирование выполняется матричным представлением вариантов тригонометрических функций и использованием хеш–функций для вычисления координат и параметров, генерируемой тригонометрической функцией по текущему времени, секретной строке, логину и паролю первого аутентификационного кода;

– разработана модель процесса двухфакторной аутентификации пользователя на основе второго фактора, отличающаяся от известных тем, что она открытая и может генерировать наборы функций получения второго аутентификационного кода для каждой отдельной системы;

– предложена схема информационной системы программной реализации двухфакторной аутентификации с использованием мобильного устройства для ее внедрения и использования в закрытой сети.

Личный вклад исследователя. Разработан алгоритм аутентификации пользователя в информационной системе на основе второго фактора. Проведены численные исследования и экспериментальная оценка предлагаемых моделей и алгоритмов. Разработана архитектура клиент–серверной системы аутентификации и осуществлена программная реализация предложенной системы аутентификации пользователя при генерации одноразового пароля с использованием компьютерной программы аутентификатора и мобильного телефона.

Апробация работы. Результаты диссертационной работы докладывались и обсуждались на семинарах и конференциях ИИВТ и на кафедре «Информационные системы» КазНУ им.аль–Фараби, в том числе на международной научно–практической конференции «Инновационные технологии на транспорте: образование, наука, практика» в рамках реализации Послания Президента РК Н. Назарбаева «Новые возможности развития в условиях четвертой промышленной революции» (Каз АТК, Казахстан, Алматы, 2018); научной конференции «Современные проблемы информатики и вычислительной технологий» (ИИВТ КН МОН РК, Казахстан, Алматы, 2018); международной научной конференции «Информатика и прикладная математика» (ИИВТ КН МОН РК, Казахстан, Алматы, 2018); международной научно–методической конференции посвященной 90–летнему юбилею Казахского национального педагогического университета имени Абая (Каз НПУ, Казахстан, Алматы, 2018); International Conferenceon Wireless Communication, Network and Multimedia Engineering (WCNME2019) (Guilin, China, 2019); научной конференции «Инновационные IT и Smart–технологии» (ИИВТ КН МОН РК, Казахстан, Алматы, 2019); научной конференции «Современные проблемы информатики и вычислительных технологий» (ИИВТ КН МОН РК, Казахстан, Алматы, 2019); международной научно–практической конференции «Информатика и прикладная математика» (ИИВТ КН МОН РК, Казахстан, Алматы, 2019); международной научно–

практической конференции «Актуальные проблемы информационной безопасности в Казахстане» (ИИВТ КН МОН РК, Казахстан, Алматы, 2020).

Связь темы с планами научно – исследовательских программ. Представленные результаты получены при выполнении следующих проектов ИИВТ КН МОН РК (источник финансирования Комитет науки МОН РК):

– программно – целевого финансирования (ПЦФ) КН МОН РК «Разработка программных и программно–аппаратных средств для криптографической защиты информации при ее передаче и хранении в инфокоммуникационных системах и сетях общего назначения» в 2018–2019 годы;

– грантового финансирования (ГФ) КН МОН РК «Разработка казахстанского сегмента защищенного трансграничного информационного взаимодействия» в 2020 году.

Публикации. Основные результаты, проведенных исследований по теме диссертации, представлены в 15 публикациях, из которых 5 – в научных изданиях, рекомендуемых КН МОН РК, 2 – в международных научных изданиях, входящих в базу данных Scopus и Web of Science, 8 – в материалах международных научно практических конференций.

Структура и объем диссертации. Общий объем работы – 123 страницы. Диссертация состоит из введения, 3 разделов, заключения, списка используемых источников из 104 наименований, 4 приложений, включает 37 рисунков и 5 таблиц.

Во введении дано обоснование актуальности выбранной темы диссертационного исследования. Сформулированы цель, объект, предмет и задачи исследования. Описаны результаты проведенных исследований, показана их научная новизна и практическая значимость. Представлены данные об апробации результатов диссертационной работы.

Первый раздел посвящен исследованию известных методов и средств защиты информационных систем на основе двухфакторной аутентификации. Описаны принципы построения защиты информации в базе данных при аутентификации пользователя.

Представлена классификация распространенных методов двухфакторной аутентификации, используемых в информационных системах, рассмотрены недостатки и достоинства этих методов.

Рассмотрены алгоритмы и протоколы аутентификации с использованием одноразового кода. HOTP (HMAC – Based One – Time Password Algorithm)– алгоритм защищенной аутентификации с помощью использования одноразового кода, основанного на SHA–1 и TOTP (Time – based One – Time Password Algorithm) – алгоритм создания одноразовых паролей для защищенной аутентификации, которые являются фундаментом для разработки одноразовых паролей защищенной аутентификации. Проведен анализ систем защиты информации и их характеристики на основе двухфакторной аутентификации. Приведены статистические данные компаний, специализирующихся в области обеспечения информационной безопасности. Проведен анализ кибератак и рассмотрены некоторые компании,

предоставляющие услуги по защите информации, хранящейся в базах данных. Описаны проблемы, которые возникают при использовании готовых решений аутентификаторов.

Во втором разделе представлены результаты, полученные при разработке модели защиты информационной системы при идентификации пользователя на основе двухфакторной аутентификации.

Рассмотрены методы аутентификации с использованием одноразового пароля. Разработан и описан алгоритм генерации одноразового пароля с использованием программы аутентификатора и мобильного телефона, который основан на модели генерации одноразового ключа для аутентификации пользователя на основе второго фактора.

Разработанная модель основана на использовании комбинации двух факторов: постоянного и временного паролей.

Описана хеш–функция SHA256, которая используется в качестве входного параметра для генерации набора функций и вычисления одноразового пароля. Для формирования хеш–функции SHA256 учитываются такие данные, как логин и пароль пользователя, текущий момент времени/даты и секретная строка. Рассмотрены созданные генераторы случайных секретных слов и тригонометрических функций для формирования одноразового пароля двухфакторной аутентификации.

В третьем разделе приведены результаты программной реализации предложенного алгоритма двухфакторной аутентификации. Разработана информационная система, состоящая из 3 взаимодействующих модулей: пользователя, мобильного приложения и серверной части. Рассмотрены структуры каждого из этих модулей.

Описан алгоритм Base64 и схема его использования для защиты информации, хранящейся в базе данных с приведенным программным кодом на языке реализации JavaScript.

Рассмотрены стандартные протоколы TLS (Transport Layer Security) и SSL (Secure Socket Layer) для защиты трафика веб–сайтов и обмена файлами по сети.

Описана работа СУБД MongoDB, в которой хранятся и обрабатываются данные. Описан объектно–ориентированный подход, используемый при реализации алгоритма.

Поэтапно изложена структура работы приложения. Осуществлена компьютерная реализация информационной системы защиты информации при аутентификации пользователя на основе одноразового ключа и проведено исследование корректности выполнения предложенного алгоритма.

В заключении изложены основные результаты и выводы диссертации. Результаты исследования включены в отчеты указанных выше проектов ПЦФ за 2018–2019 годы и ГФ за 2020 год, выполняемые в Лаборатории информационной безопасности ИИВТ КН МОН РК.

Уровень достоверности и результаты апробации. Обоснованность и достоверность исследования соответствуют обоснованным обязанностям задачи, анализу критериев и состоянию исследований в данной области,

большому количеству проведенных экспериментов и успешной реализации их на практике. Результаты диссертации обсуждались и докладывались на следующих научно–методических конференциях:

1. международной научно–практической конференции «Инновационные технологии на транспорте: образование, наука, практика» в рамках реализации Послания Президента РК Н. Назарбаева «Новые возможности развития в условиях четвертой промышленной революции» (Каз АТК, Казахстан,Алматы, 2018);
2. научной конференции «Современные проблемы информатики и вычислительной технологий» (ИИВТ КН МОН РК, Казахстан, Алматы, 2018);
3. международной научной конференции «Информатика и прикладная математика» (ИИВТ КН МОН РК, Казахстан, Алматы, 2018);
4. международной научно–методической конференции посвященной 90-летнему юбилею Казахского национального педагогического университета имени Абая (Каз НПУ, Казахстан, Алматы, 2018);
5. International Conferenceon Wireless Communication, Network and Multimedia Engineering (WCNME2019)(Guilin, China, 2019);
6. научной конференции «Современные проблемы информатики и вычислительных технологий»(ИИВТ КН МОН РК, Казахстан, Алматы, 2019);
7. международной научно–практической конференции «Информатика и прикладная математика» (ИИВТ КН МОН РК, Казахстан, Алматы, 2019);
8. международной научно–практической конференции «Актуальные проблемы информационной безопасности в Казахстане» (ИИВТ КН МОН РК, Казахстан, Алматы, 2020).

По теме диссертации опубликованы 15 статей и получено 2 авторских свидетельства:

1 Нысанбаева С.Е., Усатова О. А. «Способы обеспечения безопасности информации в базах данных»//Вестник КазНИТУ им. Сатпаева.–Алматы, 2018. – № 2. – С. 66–70.

2 Нысанбаева С.Е., Усатова О.А. «Возможное применение больших данных в системе образования»// Матер. междунар. науч. практ. конф. «Инновационные технологии на транспорте: образование, наука, практика» в рамках реализации Послания Президента РК Н. Назарбаева «Новые возможности развития в условиях четвертой промышленной революции» – Алматы, 2018. – С. 95–99.

3 Нысанбаева С.Е., Усатова О.А. «Криптографическая защита в автоматизированных системах»// Науч. конф. «Современные проблемы информатики и вычислительной технологий». – Алматы, 2018. – С. 220–223.

4 Нысанбаева С.Е., Усатова О.А. «Двухфакторная аутентификация в автоматизированной системе управления»// III Междунар. науч. конф. «Информатика и прикладная математика». – Алматы, 2018. – С. 239–242.

5 Усатова О.А., Науменко В.В. «Статистические исследования инфраструктурной платформы с использованием систем защиты данных»// VIII междунар. науч.-метод. конф. посвященной 90-летнему юбилею Казахского

национального педагогического университета имени Абая. – Алматы, 2018. – С. 113–116.

6 O. Ussatova, S. Nyssanbayeva, W. Wojcik. «Development of an authentication model based on the second factor in an automated control system»// ВестникКБТУ. – Алматы, 2019. –Т.16. – С.115–118.

7 S. Nyssanbayeva, W. Wojcik, O. Ussatova. «Algorithm for generating temporary password based on the two–factor authentication model»// Przegląd Elektrotechniczny. – Polan, 2019. –№ 5. – P. 101–106.

8 O. Ussatova, S. Nyssanbayeva, W. Wojcik. «Two-factor authentication algorithm implementation with additional security parameter based on mobile application »// International Conference on Wireless Communication, Network and Multimedia Engineering (WCNME2019). – Guilin, China, 2019. – Vol. 89. – P. 84–86.

9 O. Ussatova, S. Nyssanbayeva, W. Wojcik. « Software implementation of two-factor authentication to ensure security when accessing an information system» // ВестникКазНУим.аль-Фараби. –Алматы,2019. – С.87–95.

10 Olga Ussatova, Saule Nyssanbayeva. «Generators of one-time two-factor authentication passwords»// Informatyka, Automatyka, Pomiary w Gospodarcei Ochronie Środowiska. – Poland, 2019. № 2. – P. 60–64.

11 Усатова О.А., Нысанбаева С.Е. «Обеспечение защиты информационной системы с помощью двухфакторной аутентификации»// науч. конф. «Современные проблемы информатики и вычислительных технологий» – Алматы, 2019. –С. 337–343.

12 Begimbayeva Yenlik, Ussatova Olga, Biyashev Rustem, Nyssanbayeva Saule. «Development of an automated system model of information protection in the cross-border exchange»// Cogent Engineering Journal. – 2020. DOI: 10.1080/ 23311 916. 2020.1724597. –P. 1–13.

13 Бегимбаева Е.Е., Усатова О.А., Бияшев Р.Г., Нысанбаева С.Е., Вуйцик В., «Разработка модулей для защиты информации в автоматизированной системе с применением разграничения доступа»// IV междунар. науч.–практ. конф. «Информатика и прикладная математика», посвященная 70–летнему юбилею профессоров Биярова Т.Н., Вальдемара Вуйцика и 60–летию профессора Амиргалиева Е.Н. – Алматы, 2019. – С. 595–602.

14 Усатова О.А., Нысанбаева С.Е. «Исследование и разработка модели защиты базы данных информационной системы»// Вестник КазНУ им.аль–Фараби, Алматы, 2019. – № 4 (104), – С.95–106.

15 Усатова О.А. «Клиент-серверная система защиты информации на основе двухфакторной аутентификации»// междунар. науч.–практ. конф. «Актуальные проблемы информационной безопасности в Казахстане». – Алматы, 2020. – С. 243–248.

16 Сертификат регистрации авторского права на алгоритм «Двухфакторная аутентификация в автоматизированной системе управления» №712144534 от 2018.10.01, компании «WORKS COPYRIGHT», это цифровая сертификация, юридически признанная во всем мире для регистрации авторских прав авторов, New York – NY–USA.

17 Авторское свидетельство о внесении сведений в государственный реестр прав на объекты, охраняемые авторским правом РК, № 4330 от 28 июня 2019г., «Система аутентификации с использованием второго фактора для контроля доступа к данным – Security Code of the 2FA».