ОТЗЫВ
официального оппонента
доктора технических наук, профессора
Ажмухамедова Искандара Маратовича

на диссертационную работу
Шумилина Александра Сергеевича
на тему «Метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе»,
представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

1. Актуальность темы диссертационного исследования

Распределенные информационные системы стали популярными благодаря стремительному развитию информационных технологий и удобству использования по всему миру. Обработка, хранение и передача информации между пользователями подобных систем осуществляется посредством использования различных каналов связи. В условиях, когда информация покидает пределы доверенной зоны возникает угроза хищения конфиденциальных данных. Такая угроза может представлять весомую опасность для конечного пользователя, потому что личные данные могут быть скомпрометированы, а результаты медицинских обследований изменены или уничтожены. Таким образом для защиты персональных данных пользователей облачных информационных систем необходимо предусмотреть механизмы защиты, которые будут обеспечивать безопасность циркулирующей в системе информации, а также позволят без угрозы потери доступа или хищения передавать данные между распределенными станциями и серверами.

Диссертационная работа Шумилина Александра Сергеевича посвящена решению такой задачи и заключается в поиске эффективного метода обеспечения безопасности конфиденциальных данных, которые обрабатываются в процессе проведения медицинских обследований с использованием распределенных медицинских информационных систем, имеющих облачную архитектуру. В качестве результатов работы автором предложены метод и алгоритмы защиты информации, представляющие высокую ценность для развития цифровой инфраструктуры здравоохранения и обеспечения безопасности конфиденциальных данных, что подчеркивает актуальность диссертационного исследования. Предложенный автором метод защиты данных в информационной системе делает ее отличной от аналогичных решений благодаря возможности распределенного хранения не исходного файла с обследованием, а его фрагментов в зашифрованном виде.

2. Оценка достоверности полученных результатов и новизны диссертационного исследования

Достоверность и новизна полученных автором результатов в рамках представленного диссертационного исследования подтверждаются обширным

анализом состояния проблемы информационной безопасности, существующей для современных облачных информационных систем, а также подробным обоснованием необходимости применения разработанных метода и алгоритмов для решения обозначенной проблемы. Экспериментальным путем получены практические результаты, которые подтверждают эффективность предложенного метода обеспечения безопасности.

Шумилиным А. С. проведена апробация результатов исследования на научных конференциях всероссийского и международного уровней. Автором успешно реализован грант РФФИ по тематике исследования, а также получены акты о внедрении разработок от четырех различных организаций.

Новые научные результаты представленного диссертационного исследования Шумилина А. С. заключаются в следующем:

1. Разработан метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе. Метод отличается от аналогов тем, что рассмотренная в диссертационной работе реализация предполагает использование схемы разделения секрета Шамира, что позволяет повысить уровень информационной безопасности для файлов медицинских обследований с помощью технологии разделения исходного файла на фрагменты и распределения этих фрагментов на различных серверах МИС. В этом случае при несанкционированном доступе к одному из фрагментов получить полезную информацию и раскрыть содержимое исходного файла не представляется возможным.
2. Разработан алгоритм, позволяющий оценить время работы протокола разделения, который отличается от аналогов применением библиотеки MPI, благодаря которой становится возможным выполнение и обработка параллельных процессов, которые выполняются при работе с файлом в ходе разделения на фрагменты и восстановлении частей файла в исходное состояние.
3. Предложена архитектура облачной медицинской информационной системы, отличительной чертой которой является масштабирование путем добавления различного диагностического оборудования различных производителей без изменения метода зашиты информации. Преимуществом рассмотренного архитектурного решения является высокий уровень безопасности хранимых и обрабатываемых данных за счет использования метода защиты конфиденциальной информации, который разработан автором.
4. Предложенный метод обеспечения защиты информации интегрирован в разработанную автором медицинскую информационную систему, имеющую облачную архитектуру. Автором рассмотрена модель угроз Долева-Яо и проведена оценка эффективности предлагаемого метода обеспечения безопасности.

Теоретическая значимость исследования заключается в том, что автором продемонстрирован подход, позволяющий обеспечить безопасность данных в МИС на основе нового разработанного метода, а также теоретический базис, на основе которого можно интегрировать предложенный метод в аналогичные облачные системы.

Практическая значимость работы заключается в том, что Шумилин А. С достиг практических результатов на основе проведенных экспериментов, которые

можно использовать в процессе проектирования подобных систем учитывая требования к информационной безопасности. Использование авторского решения демонстрирует снижение количества угроз, присущих МИС, тем самым повышая уровень защищенности системы.

3. Оценка содержания диссертации, степени ее завершенности, подтверждение публикаций автора.

Содержание и структура диссертационного исследования Шумилина Александра Сергеевича соответствуют теме, представленной цели и задачам исследования. Структура диссертации логична и понятна. Работа является завершенным, самостоятельно подготовленным исследованием и состоит из пяти глав, заключения и трех приложений. Объем работы составляет 146 страниц, 18 таблиц, 11 рисунков, 94 литературных источника.

Введение описывает актуальность рассматриваемой темы, сформулирована цель и основные задачи работы. Также выделены методы исследования и научная новизна, а также практическая и теоретическая значимость результатов, достигнутых в ходе исследования.

Первая глава направлена на детальный обзор работ по тематике исследования среди коллективов российских и зарубежных авторов. В данной главе проведен обзор подходов, которые рассматриваются в доменной области для обеспечения безопасности данных в информационных системах с облачными архитектурами. Определены недостатки существующих способов защиты и сформированы задачи по достижению цели исследования.

Вторая глава описывает архитектуру медицинской облачной информационной системы, ее основные уровни, а также взаимодействие между ними. Во второй главе приводятся общие схемы работы системы и описание протоколов, которые могут применяться для взаимодействия с системой.

Третья глава посвящена поиску оптимальной схемы разделения секрета. Обоснование выбора основывается на обширных экспериментальных исследованиях. Автор демонстрирует важность выбора наиболее подходящей схемы, поэтому сравнивает несколько кандидатов по скорости выполнения операций разделения и восстановления секрета для разных объемов и форматов файлов, в том числе медицинских. Кроме того, проводится анализ потребления оперативной памяти для 4 различных схем. В завершении экспериментов автор проанализировал метод на основе протокола разделения секрета с точки зрения безопасности и получил результаты, которые демонстрируют достижение поставленной цели, а именно снижение количества угроз.

В четвертой главе описан процесс разработки метода обеспечения безопасности с использованием схемы Шамира. В данной главе автор наглядно демонстрирует алгоритмы передачи файлов с обследованиями с использованием схем и иллюстраций и описывает очередность действий, необходимых для обеспечения защиты передаваемых данных в рамках информационной системы.

В пятой главе описаны эксперименты с использованием инструмента для работы с многопроцессорными системами. Показано, что распараллеливание операций разделения и слияния частей файла позволяет почти линейно сократить время. Эксперименты были проведены с использованием библиотеки MPI

(Message parsing interface).

Заключение содержит итоги проведенных исследований, а также сделанные выводы по результатам исследования.

Автором опубликовано 20 научных работ, из которых 3 – в журналах, индексируемых в SCOPUS, 3 – в журналах, из перечня ВАК, и 14 публикаций в сборниках конференций. Автором получено свидетельство о государственной регистрации программ для ЭВМ.

4. Замечания по диссертационной работе

1. В разделе, посвященном описанию метода обеспечения безопасности конфиденциальных данных в медицинской информационной системе не обозначено, как идентифицируются серверы, которые участвуют в рассылке частей защищаемого файла для последующего обращения к ним, выполняется ли опрос всех доступных серверов?
2. При проведении различных экспериментов в работе фигурирует испытательный стенд, имеющий высокие технические характеристики (Intel core i7, 8 Gb ОЗУ). Было бы правильно провести испытания на оборудовании с более низкими техническими характеристиками, поскольку в реальности медицинские учреждения не обладают такими высокими вычислительными мощностями.
3. Также в работе не представлены минимальные требования к серверам, которые предполагаются к использованию в качестве аппаратных ресурсов объекта защиты.
4. Не раскрыт вопрос о том, на каких ключах будут шифроваться фрагменты файлов? Как решается проблема распределения этих ключей?
5. В разделе, посвященном степени разработанности темы, при анализе работ в смежной тематике фигурируют преимущественно иностранные коллективы авторов. Стоило бы рассмотреть больше российских исследований, потому что они могут быть направлены на решение актуальных проблем, присущих реальным отечественным медицинским информационным системам.

Все представленные замечания не являются существенными и не снижают значимость работы. Общее впечатление от диссертационной работы является положительным.

5. Заключение

На основе представленных автором материалов диссертационной работы следует, что поставленная цель достигнута, а задача решена. Работа имеет логически выстроенную структуру, глубина исследований, количество проведенных экспериментов, а также основные научные результаты и степень их обоснованности доказывают, что работа выполнена с высоким качеством. По результатам работы сформулированы четкие выводы и понятны итоговые результаты, которые подтверждаются практическими результатами. В ходе работы автор активно ссылается на исследования российских и зарубежных ученых, опубликованные в научных журналах, а также на материалы собственного исследования в области информационной безопасности. Исследование отличается хорошим уровнем изложения, логичностью представления материала, а также корректностью использования научно-

исследовательских методов, соответствующих теме исследования. Содержание работы Шумилина А. С. соответствует заявленной тематике.

Таким образом, представленная Шумилиным Александром Сергеевичем диссертационная работа полностью соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата наук в соответствии с положением «О присуждении ученых степеней» в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет», а автор представленного диссертационного исследования достоин присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

Доктор технических наук (5.13.19 «Методы и системы защиты информации, информационная безопасность», 05.13.01 «Системный анализ, управление и обработка информации (информационные технологии)»), профессор, и.о.декана факультета цифровых технологий и кибербезопасности, профессор кафедры информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Астраханский государственный университет имени В. Н. Татищева», г. Астрахань
Ажмухамедов Искандер Маратович

414056, г. Астрахань, улица Татищева, 20а
Тел: +7(8512) 24-64-00 (доб. 275), e-mail: aim_agtu@mail.ru,
https://asu.edu.ru/

«23» апреля 2024 г. _____ И. М. Ажмухамедов

Подпись И. М. Ажмухамедова заверяю

Подпись заверяю