ОТЗЫВ

официального оппонента
доктора физико-математических наук, доцента Тебуевой Фаризы Биляловны
на диссертационную работу Шумилина Александра Сергеевича
на тему «Метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе»,
представленной к защите на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

1. Актуальность темы и направления диссертационного исследования

В условиях развития многообразия современных технологий в настоящее время активно расширяют свое влияние различные информационные системы. Технологический прогресс способствовал стремительному росту пользователей, которые являются потребителями цифровых услуг, в связи с чем появилась необходимость в организации облачных ресурсов для предоставления различных услуг. Медицинские информационные системы (МИС) не стали исключением и активно заняли нишу продуктов, поставляемых в виде облачных решений для предоставления быстрых, качественных и безопасных услуг населению. Однако в условиях стремительной популяризации МИС стали возникать риски компрометации конфиденциальных данных пациентов со стороны злоумышленников путем нарушения целостности и доступности данных. Для минимизации и предотвращения таких рисков требуется обеспечить безопасность данных, которые находятся в подобных медицинских системах.

Диссертационная работа Шумилина А. С. направлена на решение актуальной проблемы, заключающейся в обеспечении безопасности конфиденциальных данных, обрабатываемых в ходе проведения медицинских обследований с использованием медицинских информационных систем, имеющих облачную архитектуру. Необходимость исследований в области разработки эффективных методов и алгоритмов защиты информации обусловлена высокими темпами цифровизации сферы здравоохранения, перспективностью развития технологий телемедицины и облачных вычислений, а также активным внедрением информационных систем на государственном уровне для предоставления диагностических, профилактических и других подобных услуг населению. Результаты, полученные автором, позволяют решить важную научную задачу по обеспечению защиты данных на основе предложенного метода, что актуально в настоящее время и имеет существенное значение для развития цифровой системы здравоохранения.

2. Обоснованность научных положений, оценка достоверности полученных результатов и новизны диссертационного исследования

В диссертационной работе Шумилин Александр Сергеевич, в соответствии с проведенным аналитическим обзором существующих современных методов обеспечения защиты информации, возможностей и архитектурных решений облачных медицинских систем, а также наиболее значимых научных исследований в рассматриваемой доменной области продемонстрировал

логически обоснованные и подкрепленные экспериментами полученные результаты, представленные в виде разработанных метода и алгоритмов, направленных на решение поставленной научной задачи.

Оригинальность исследования заключается в том, что автор аргументированно описывает возможность применения предложенного метода обеспечения безопасности данных с использованием схемы разделения секрета Шамира в облачной информационной системе, подтверждая объективность практическими результатами. Автором приведены реальные расчеты времени выполнения основных операций при использовании предлагаемого метода, а также оценка с точки зрения снижения количества угроз.

В диссертационной работе, представленной автором получены результаты, которые характеризуются **научной новизной**.

1. Автором разработан метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе, отличие которого заключается в использовании схемы разделения секрета Шамира, что в предложенной реализации позволяет повысить уровень безопасности информационной системы посредством разделения конфиденциального файла на фрагменты с последующим распределением на отдельные сервера. В результате чего получение исходного файла злоумышленника становится невозможным, т.к. для его восстановления необходимо собрать вместе несколько фрагментов с разных серверов.
2. Предложен алгоритм оценки времени работы протокола разделения секрета на основе схемы Шамира, отличающийся применением библиотеки MPI, что позволяет выполнять обработку параллельных процессов, связанных с разделением и восстановлением долей файла.
3. Выполнено проектирование облачной архитектуры медицинской информационной системы, которая отличается от аналогов возможностью масштабироваться, и позволяет работать с диагностическим оборудованием различных производителей. Особенность предложенной архитектуры заключается в том, что в ней предусмотрен высокий уровень безопасности хранимых и обрабатываемых данных за счет использования метода защиты конфиденциальной информации, который разработан автором.

В методе обеспечения безопасности, предложенном автором, используется протокол разделения секрета на основе схемы Шамира, что позволяет распределить фрагменты файла медицинского обследования между серверами случайным образом и, как следствие, значительно усложнить процедуру доступа к исходному файлу для злоумышленника ввиду того, что в таком случае необходимо собрать заданное пороговое значение фрагментов файла вместе. Таким образом, угроза потери конфиденциальных данных минимизируется. Предложенный метод обеспечения безопасности позволяет повысить устойчивость системы к компрометации данных, а также к случайной потере, в случаях, если происходит выход из строя одного из серверов, на котором хранится один из фрагментов. Благодаря тому, что для получения доступа к исходному файлу с обследованием необходимо собрать заранее определённое пороговое значение фрагментов секрета в единый файл, обеспечивается безопасность данных, циркулирующих внутри медицинской информационной

системы. Разработанный метод защиты медицинских данных позволяет снизить количество угроз безопасности в системе, что экспериментально подтверждено в диссертационной работе. Автором проведены различные экспериментальные исследования, на основе результатов которых выбрана эффективная схема реализации протокола разделения секрета Шамира. Анализ времени разделения и восстановления файла, а также объем потребляемой оперативной памяти подтверждает выбор. В условиях критичности требований к высокому уровню безопасности конфиденциальных данных и скорости выбор схемы полностью справедлив и логичен.

3. Теоретическая и практическая значимость результатов

Теоретическая значимость заключается в формировании новых подходов к организации систем защиты медицинских данных на основе использования схем разделения секрета, теоретических знаний о процессе интеграции способов обеспечения защиты в медицинских информационных системах, имеющих облачную архитектуру.

Практическая значимость работы заключается в том, что результаты, полученные автором, могут применяться при построении МИС с учетом обеспечения требуемого уровня безопасности для хранения данных. Практическое применение разработанного метода позволит снизить количество угроз со стороны злоумышленников, что повышает уровень защищенности информации в МИС, построенной на основе современных криптографических протоколов.

4. Характеристика опубликования автором результатов диссертации, оценка содержания диссертации и степени завершенности

Требования к опубликованию результатов диссертационного исследования выполнены в полном объеме. Автором опубликовано 20 научных работ, 3 из которых опубликованы в журналах, индексируемых в SCOPUS, 3 - в журналах, из перечня ВАК, остальные работы в сборниках и тезисах конференций. Также, автором получено свидетельства о государственной регистрации программ для ЭВМ.

Диссертация имеет логичную структуру, соответствует заявленной теме, поставленным целям и задачам, а также является завершенной и обладает логично построенной структурой и представленной информацией. Содержание диссертации включает в себя введение, 5 глав, заключение, 3 приложения. Полный объем работы - 146 страниц, 18 таблиц, 11 рисунков, 94 наименования в списке литературы.

Во введении описана актуальность темы диссертации, также определен объект исследования, сформулированы цель и задачи работы, показаны методы исследования, определена научная новизна, практическая и теоретическая ценность полученных результатов, приведены научные результаты, выносимые на защиту. Также в данной главе Сформулированы частные задачи, решением которых достигается цель исследования.

Первая глава посвящена обзору подходов к обеспечению защиты конфиденциальных данных в распределенных информационных системах, а

также направлениям развития таких подходов. В главе обоснована необходимость разработки метода защиты и предложены шаги решения поставленной задачи.

Вторая глава содержит описание архитектуру медицинской облачной информационной системы, которая выступает в качестве объекта защиты.

Третья глава посвящена обоснованию выбора схемы разделения секрета. В данной главе проводится сравнение выбранных автором схем разделения секрета на предмет потребления ресурсов и быстродействия при выполнении операций разделения и слияния файлов. Кроме того, автором проведен анализ безопасности предлагаемого метода и получены практические результаты.

Четвертая глава посвящена разработке метода обеспечения защиты конфиденциальных данных в облачной медицинской информационной системе с использованием схемы Шамира. Автор пошагово описывает последовательность действий, на основании которых выполняется разработанный метод и демонстрирует как достигается обеспечение безопасности в рамках МИС при использовании предложенного метода.

В пятой главе продемонстрировано моделирование распараллеливания операций разделения и слияния долей секрета по схеме Шамира с использованием библиотеки MPI. Автором выполнена оценка времени разделения файла на фрагменты и слияние фрагментов обратно в единый файл, получены практические результаты.

Заключение содержит все достигнутые в рамках диссертационного исследования результаты и выводы.

5. Замечания, недостатки, рекомендации к диссертационной работе

При выборе оптимальной схемы разделения секрета в предложенном автором методе рассмотрены различные пороговые схемы и продемонстрированы экспериментальные результаты анализа ресурсоемкости в процессе вычислений только для одного файла, состоящего из 256 символов. В качестве подобного эксперимента желательно было рассмотреть несколько файлов разного размера.

В рамках предложенного автором метода предлагается распределять фрагменты файла на определенное количество серверов, что позволяет минимизировать возможность компрометации исходного файла. Однако в диссертационной работе не рассмотрено, какое максимальное количество серверов целесообразно задействовать для такой процедуры.

Касательно практического применения спроектированной архитектуры облачной медицинской информационной системы важно иметь возможность развертывания архитектуры на инфраструктуре отечественного сервис провайдера, центр обработки данных которого находится на территории России. В работе автора не рассмотрена такая возможность, однако упоминается соблюдение существующего законодательства в качестве отсылок на ФЗ №152 – О персональных данных и ФЗ №187 – О безопасности критической информационной инфраструктуры Российской Федерации.

К техническим замечаниям можно отнести мелкий шрифт на рисунке общей схемы организации модулей рассмотренной платформы, а также масштаб столбцов гистограммы с распределением времени выполнения операций над файлами.

Подобные замечания являются несущественным, не снижают значимость и

общее положительное впечатление от диссертационной работы.

6. Заключение

Объем работы и материалов, представленных автором, позволяют сделать вывод о том, что цель, поставленная в работе, достигнута. Понятная и логически выстроенная структура работы, объем выполненных исследований, а также основные научные результаты и степень их обоснованности свидетельствуют о глубокой проработке темы.

Результаты исследования базируются на обширном анализе выводов, полученных в работах российских и зарубежных ученых, на материалах собственного исследования в области информационной безопасности и аналитической обработки данных. Работа характеризуется полнотой, ясностью и логичностью изложения материала, корректностью и соответствием научно-исследовательского аппарата теме исследования. Содержание работы Шумилина А. С. соответствует заявленной теме.

Содержание диссертации соответствует паспорту научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность». Диссертационная работа в полной мере соответствует требованиям положения «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный федеральный университет», предъявляемым к диссертациям на соискание ученой степени кандидата наук, а ее автор, Шумилин Александр Сергеевич заслуживает присвоения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
Доктор физико-математических наук (05.13.18 – «Математическое моделирование, численные методы и комплексы программ»), доцент, заведующая кафедрой компьютерной безопасности федерального государственного автономного образовательного учреждения высшего образования «Северо-Кавказский федеральный университет»,
Тебуева Фариза Биляловна

355029, г. Ставрополь, проспект Кулакова, 2, корпус 9, каб. 9-434
Тел: 8 (8652) 94-41-90, e-mail: ftebueva@ncfu.ru,
https://www.ncfu.ru/

«26» апреля 2024 г. _____ Ф. Б. Тебуева

Подпись Ф. Б. Тебуевой заверяю

ПОДПИСЬ УДОСТОВЕРЯЮ:
начальник отдела по
работе с сотрудниками УКА
ЛС ГОРБАЧЕВА