Экз. № 1

МИНИСТЕРСТВО ПРОМЫШЛЕННОСТИ И ТОРГОВЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УНИТАРНОЕ ПРЕДПРИЯТИЕ
НАУЧНО-ПРОИЗВОДСТВЕННОЕ ПРЕДПРИЯТИЕ
«Гамма»
РОСТОВСКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
344064, г. Ростов-на-Дону, ул. Вавилова, 54, Лит.А (863) 237-21-88, 237-21-89, 237-21-90, факс доп. 4200
public@rnd.nppgamma.ru https://rnd.nppgamma.ru

УТВЕРЖДАЮ
Заместитель директора филиала -
Ростовского НТЦ ФГУП «НПП «Гамма»
_____ Кравцов С.А.
«___» _____ 2024 г.

ОТЗЫВ

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»

Медицинские информационные системы (МИС) наряду с информационными системами банковского и военного направления являются наиболее важными с позиции сохранения свойства «конфиденциальности» обрабатываемой в них информации. Современные тенденции постоянного роста числа воздействий (атак), направленных на организацию утечки информации и (или) ее раскрытие, требуют усиления существующих и разработки новых методов и средств защиты подобных систем. Принимая во внимание также развитие нормативной и правовой базы в области обеспечения защиты персональных данных и иной информации ограниченного доступа, исследование и (или) реализация таких методов и средств по отношению к обеспечению безопасности информации, обрабатываемой в МИС, имеют высокий приоритет.

Криптографические методы являются наиболее эффективными в контексте решения задачи сохранения свойства «конфиденциальности» информации, в особенности, в случае ее передачи по каналам связи или хранения в памяти, потенциально скомпрометированных нарушителем. Оба указанных направления наиболее характерны для информационных систем, использующих «облачные» технологии обработки и хранения данных. Поскольку гетерогенность «облачных» платформ, распределенность их вычислительных ресурсов и хранилищ данных повышают вероятность точечного и (или) скрытого воздействия (атаки) нарушителей и, как следствие, усложняют задачу разработки безопасной архитектуры для информационных систем, функционирующих на базе таких платформ.

Исходя из результатов анализа диссертационной работы Шумилина Александра

Сергеевича, и на основании вышеизложенного считаем, что:

- актуальность темы диссертационной работы не вызывает сомнений;
- цель, задачи и методы исследования сформулированы и выбраны автором диссертационной работы в достаточной мере;
- выводы и результаты диссертационной работы не вызывают сомнений.

Считаем, что **научную новизну** представляют следующие результаты диссертационной работы:

1) Разработанный метод, использующий криптографическую схему Шамира по разделению секрета наряду с принципом фрагментирования данных, содержащих информацию ограниченного доступа, при ее передаче и обработке в распределенной облачной информационной системе.

2) Разработанный алгоритм оценки времени работы протокола для схемы Шамира по разделению секрета, учитывающий особенности функционирования и реализации многопроцессорных (многопоточных) систем.

3) Предложенная архитектура распределенной облачной информационной системы, полностью учитывающая как разработанный метод, так и поддержку различных форматов представления данных в электронном виде, включая специализированные медицинские форматы.

Также считаем, что основной **теоретической значимостью** диссертационной работы является предложенный автором работы новый подход к сохранению свойства «конфиденциальности» информации, обрабатываемой в распределенных облачных информационных системах, по отношению к применению классических криптографических методов и схем обеспечения безопасности информации в подобных системах.

В свою очередь, приведенные результаты диссертационной работы обладают несомненной **практической значимостью** с учетом:

- разработанного автором метода противодействия внешнему нарушителю, атаки которого направлены на раскрытие информации ограниченного доступа, обрабатываемой в распределенной облачной информационной системе;
- разработанного автором алгоритма оценки, ориентированного на многопроцессорные (многопоточные) системы обработки данных;
- полученных автором результатов экспериментальных исследований, подтвердивших эффективность противодействия атакам нарушителя на свойство «конфиденциальности» информации, обрабатываемой в распределенной облачной информационной системе.

Отмечаем, что требования к публикации материалов диссертационной работы соблюдены автором в полной мере, включая:

- промежуточные результаты, которые обсуждались на всероссийских и международных научно-практических конференциях;
- основные результаты, опубликованные в журналах, рекомендованных ВАК России;
- результаты, опубликованные в международных научных изданиях с индексацией в Scopus;
- свидетельство о государственной регистрации программы для ЭВМ;
- акты о внедрении результатов диссертационной работы.

Также, на наш взгляд, в диссертационной работе присутствует ряд недостатков:

1) Разработанный автором метод криптографической защиты и фрагментирования файлов за счет схемы Шамира эффективно противодействует атакам нарушителя (злоумышленника), который не имеет длительного доступа к памяти первичного сервера, реализующего получение от отправителя, разделение на фрагменты и (или) передачу совокупного защищаемого файла получателю. В свою очередь, такой сервер присутствует в архитектуре облачной МИС, предложенной автором. В таком случае эффективность предложенной архитектуры в большей степени зависит от введенного автором условия — случайный выбор указанного сервера. Однако, автором не в полной мере раскрыты критерии выбора такого сервера пользователем и оценка эффективности противодействия нарушителю при изменении совокупного количества серверов в составе облачной МИС.

Отмечаем, что приведенные недостатки могут потребовать от автора дополнительных пояснений в ходе защиты диссертации, но не являются принципиальными или критически значимыми и на качество проведенного исследования отрицательно не влияют.

Диссертационная работа является законченной научно-квалификационной работой. Автор диссертационной работы — Шумилин Александр Сергеевич — заслуживает присуждения ученой степени кандидата технических наук по специальности «2.3.6 – Методы и системы защиты информации, информационная безопасность».

Настоящий Отзыв составили:

Начальник отдела
Ростовского НТЦ ФГУП «НПП «Гамма»
кандидат технических наук — Буцик Кирилл Александрович

Ведущий специалист
Ростовского НТЦ ФГУП «НПП «Гамма»
кандидат военных наук, доцент — Масютин Александр Николаевич

«4» апреля 2024 г.

Ростовский научно-технический центр Федерального государственного унитарного предприятия «Научно-производственное предприятие «Гамма» (Ростовский НТЦ ФГУП «НПП «Гамма»)
Почтовый адрес: 344064, г. Ростов-на-Дону, ул. Вавилова, 54 Лит. А
Телефон: +7 (863) 237-21-87, +7 (863) 237-21-88
e-mail: adm@rnd.nppgamma.ru