ОТЗЫВ

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

Диссертационное исследование Шумилина Александра Сергеевича направлено на повышение эффективности обеспечения безопасности медицинских систем и безусловно, является актуальным в связи с важностью обрабатываемой в таких системах информации о персональных данных. Применение облачных технологий для обработки медицинских данных позволяет сократить время обработки, повысить точность диагностики и эффективность лечения. Однако, с другой стороны это приводит к повышению числа потенциальных угроз системе со стороны злоумышленника.

Цель диссертационного исследования заключается в решении данной проблемы за счет использования протокола распределения секрета для обеспечения конфиденциальности медицинских данных.

К основным результатам диссертационной работы относятся:

- метод обеспечения безопасности файлов медицинских обследования, использующий схему Шамира для распределения фрагментов между серверами;
- архитектуру облачной медицинской распределенной системы, применяющую разработанный метод обеспечения безопасности;
- алгоритм оценки времени работы протокола разделения секрета.

Достоверность и обоснованность научных результатов, полученных соискателем, подтверждается представленными в открытой печати научными публикациями. Практическая значимость подтверждается внедрением результатов в медицинскую информационную систему ООО «СиВижинЛаб».

По реферату имеются следующие замечания к его содержанию:

1. Пороговая схема Ади Шамира, хорошо известна и широко применяется уже несколько десятилетий как для многопользовательской авторизации в инфраструктуре открытых ключей, так и в стеганографии для скрытой передачи информации в цифровых изображениях с целью противодействия атакам по сторонним каналам при реализации например, алгоритма AES. Однако в автореферате не отражены или не рассмотрены очень важные аспекты. А каковы уровни доверия к стороне, генерирующей и раздающей тени, а также доверия в данном контексте корректности или подлинности теней сторон?
2. В проведенных экспериментах рассматривается скорость выполнения операций при разбиении файлов объемом в 1024 и 8192 Кб. Однако, при этом не указывается примерный объем общей обрабатываемой информации в системе. Было ли оценено общее время обработки при работе с несколькими файлами разных размеров?
3. В визуализации результатов (рис. 2) сравнения времени выполнения операции разделения файла на фрагменты неудачно выбраны цвета для обозначения столбчатой диаграммы. Автореферат в печатном виде представлен в черно-белом формате, что снижает информативность рисунка.
4. В защищаемом положении указано сокращение количества угроз на 45%. К сожалению, автореферате подтверждение этому не обнаружил. На странице 16 автореферата оценка получена путем вычитания из 78,5% значения в 33%. Однако, эти оценки не показывают количество угроз.

Данные замечания возможно послужат автору стимулом к дальнейшему развитию исследования, не оказывают влияния на положительную оценку диссертации и не снижают общей ценности работы. Диссертация представляет несомненный научный интерес и имеет практическое значения для специалистов в сфере информационной безопасности, а также для развития технологии распределенных медицинских систем.

Содержание автореферата, а также представленные в научных публикациях сведения позволяют утверждать, что диссертация является завершенной научно-квалификационной работой, выполненной на хорошем научном уровне. Она отвечает требованиям к диссертациям на соискание ученой степени кандидата технических наук, изложенным в п.9 Постановления Правительства РФ от 24.09.2019 № 842 «О порядке присуждения ученых степеней». В связи с этим считаю, что ее автор Шумилин Александр Сергеевич заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Президент ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники»,
директор института системной интеграции и безопасности,
доктор технических наук, профессор

Александр Александрович Шелупанов

27.04.24

Шелупанов Александр Александрович – доктор технических наук (05.13.01 – Системный анализ, управление и обработка информации (информация и информационные системы, экономика, энергетика, промышленность, образование)), профессор, президент ФГАОУ ВО «Томский государственный университет систем управления и радиоэлектроники», директор института системной интеграции и безопасности, заведующий кафедрой комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС).

634050, Томск, пр. Ленина, 40
Тел.: +7 (3822) 90-71-55
E-mail: saa@fb.tusur.ru
Сайт ТУСУР: tusur.ru

Подпись Шелупанова А.А.
УДОСТОВЕРЯЮ
Ученый секретарь
Е.В. Прокопчук