ОТЗЫВ

на автореферат диссертации

Шумилина Александра Сергеевича

«Метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе»,

представленной на соискание ученой степени

кандидата технических наук по специальности

2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Согласно статистике, отрасль здравоохранения не относится к лидерам в сфере обеспечения информационной безопасности. Громкие инциденты происходят во всем мире. Осенью 2023 года утечку данных 1,3 миллиона человек допустила частная биотехническая компания из США 23andMe, специализирующаяся на ДНК-исследованиях. В Российской Федерации в 2022 году произошла утечка базы клиентов из 31 миллиона записей из сети лабораторий «Гемотест». Несмотря на наличие в России законодательной базы, регулирующей защиту информации в том числе в организациях здравоохранения (152-ФЗ «О персональных данных», 187-ФЗ «О критической информационной инфраструктуре Российской Федерации», 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» и т.д.), зачастую это направление финансируется по остаточному принципу, и даже крупные медицинские учреждения не всегда могут себе позволить содержать необходимый штат специалистов по защите информации. В то же время утечки информации из информационных систем в сфере здравоохранения могут нести для граждан целый комплекс рисков, ограниченных только возможностями и фантазией злоумышленников: это и фишинговые рассылки в мошеннических целях, и шантаж, вымогательство под угрозой распространения сведений о состоянии здоровья.

В диссертационной работе Шумилина Александра Сергеевича предложено решение актуальной научной задачи, заключающейся в разработке метода обеспечения безопасности медицинских данных в условиях несанкционированных вторжений со стороны злоумышленников на данные, находящиеся в медицинских информационных системах (МИС).

Научная новизна диссертационной работы заключается в следующем:

1. Автор предлагает метод обеспечения безопасности конфиденциальной информации в распределенной медицинской облачной системе, отличающийся использованием схемы разделения секрета Шамира, позволяющий повысить безопасность МИС путем усложнения процесса компрометации файла с конфиденциальными данными. Файл разделяется на фрагменты, которые затем передаются и хранятся на разных серверах, что усложняет процедуру доступа к исходному файлу со стороны злоумышленников, потому что для восстановления исходных данных требуется собрать части воедино.
2. Автором предложен алгоритм оценки времени работы протокола разделения секрета на основе схемы Шамира, отличающийся применением библиотеки MPI, позволяющей производить обработку и взаимодействие параллельных процессов. Получены результаты сокращения времени для разделения файлов медицинского обследования на фрагменты и восстановления фрагментов файла в исходное состояние.
3. Автором разработана архитектура облачной медицинской распределенной системы, отличающаяся возможностью функционировать с использованием разработанного метода, включающего определенную конфигурацию серверов, каналов связи, алгоритмы и способы формирования ключей шифрования, процедуру разделения на части и объединения воедино конфиденциальных данных согласно схеме Шамира.

Архитектура медицинской системы позволяет работать как с классическими форматами представления файлов, так и с медицинскими файлами (DICOM, Nifti, NRRD).

Теоретическая значимость исследования предоставляет возможность использовать новые подходы к построению систем защиты медицинских данных на основе использования схем разделения секрета в МИС, имеющих облачную архитектуру.

Практическая значимость состоит в разработке и реализации предложенного метода обеспечения безопасности конфиденциальных данных, а также в моделировании распараллеливания операций разделения и слияния долей секрета по схеме Шамира с использованием библиотеки MPI на многопоточных системах. В диссертационной работе представлены обширные эксперименты, на основе которых получены достоверные практические результаты. Такие эксперименты обосновывают правильность выбора схемы разделения секрета, примененной в авторском методе обеспечения безопасности. Автором работы получено свидетельство о регистрации программы для ЭВМ. Результаты работы прошли апробацию в ряде организаций, что подтверждается актами о внедрении.

Замечания:

1. Из текста автореферата неясно, рассматривалась ли автором возможность использования предлагаемого метода в среде российских операционных систем с учетом продолжающегося импортозамещения ПО;

2. Экспериментальная часть исследования проведена на достаточно современных средствах вычислительной техники. В то же время было бы полезно исследовать предлагаемый метод на вычислительных мощностях 5-10 летней давности, что точнее бы соответствовало реальной картине по оснащенности медицинских учреждений.

Указанные недостатки не снижают научной ценности проведенного исследования и не влияют на общее положительное впечатление от работы.

Заключение. Диссертационная работа Шумилина Александра Сергеевича является завершенным исследованием, выполненным на высоком научном уровне, и удовлетворяет требованиям, установленным Положением «О присуждении ученых степеней в федеральном государственном автономном образовательном учреждении высшего образования «Южный Федеральный Университет». Автор диссертационной работы заслуживает присвоения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Отзыв составлен 03.05.2024 г.

Доцент кафедры телекоммуникационных систем
Волгоградского государственного университета,
к.т.н. (05.12.13 - Системы, сети и устройства телекоммуникаций)
Галич Сергей Владимирович

Заведующий кафедрой телекоммуникационных систем
Волгоградского государственного университета,
Доцент, к.т.н. (05.12.13 - Системы, сети и устройства телекоммуникаций)
Семенов Евгений Сергеевич

400062, Волгоградская область, г. Волгоград,
просп. Университетский, д.100
Сайт: https://volsu.ru
Телефон: +7(8442)46-02-79; email: rector@volsu.ru

Подпись Галич СВ
Семенова ЕС заверяю
Ученый секретарь федерального государственного автономного образовательного учреждения высшего образования «Волгоградский государственный университет»
Н.В. Лисовская
«3» мая 2024 г.