УДК 004.056.5

СРЕДСТВА ДЛЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В СПЕЦИАЛИЗИРОВАННОЙ ДИАГНОСТИЧЕСКОЙ СИСТЕМЕ

К. т. н. Н. О. Комлевая, К. С. Чернега

Одесский национальный политехнический университет
Украина, г. Одесса
nokoml@yandex.ua

Проведен обзор современных средств, позволяющих осуществлять комплексную защиту информации в многопользовательских системах, имеющих в своем составе СУБД. Описаны средства для обеспечения целостности данных и управления доступа к ним на примере компьютерной системы, предназначенной для проведения пульмонологического диагностирования. Обосновано применение алгоритма шифрования AES для осуществления криптографической защиты информации.

Ключевые слова: защита информации, AES, система диагностирования, шифрование.

В последние десятилетия стала весьма актуальной проблема комплексной защиты информации. Обеспечение защиты информации является одной из важнейших задач при построении надежной информационной структуры на базе ЭВМ. Эта проблема охватывает как физическую защиту данных и системных программ, так и защиту от несанкционированного доступа к данным, передаваемым по линиям связи и находящимся на накопителях, что может являться результатом деятельности как посторонних лиц, так и специальных программ-вирусов. Таким образом, в понятие защиты данных включаются вопросы сохранения их целостности и управления доступа к данным (санкционированность) [1]. Среди разнообразных средств защиты информации особое место занимают криптографические методы. С одной стороны, это связано с тем, что криптографические способы защиты сообщений успешно применяются уже не одно тысячелетие. С другой стороны, новые достижения криптографии позволяют решать не только классическую задачу защиты данных от несанкционированного доступа, но и множество других задач (аутентификация пользователей информационных систем, формирование цифровой подписи к электронным документам и т.д.) [2].

Целью работы является проведение обзора существующих подходов к защите информации в многопользовательской системе, имеющей в своем составе систему управления базой данных (СУБД), и описание средств для комплексной защиты информации в диагностической системе DiaSpectrEx [3]. Система DiaSpectrEx предназначена для автоматизированного проведения пульмонологического диагностирования. Основной функцией системы является исследование спектрального состава конденсата влаги выдыхаемого пациентом воздуха, на основании которого диагностируются патологические состояния его дыхательной системы. Прототипом явилась система SPECTREX, созданная в рамках совместной научно-исследовательской работы вузов ОНПУ и ОНМУ [4, 5].

К основным средствам защиты многопользовательских систем, имеющих в своем составе СУБД, относятся: защита паролем, шифрование, разделение прав доступа к объектам БД, защита полей и записей таблиц БД [6]. Защита паролем – самый простой способ защиты БД от несанкционированного доступа. Среди пользователей системы DiaSpectrEx выделены такие категории, как «Врач», «Пациент», «Аналитик», «Администратор» и «Лаборант»; пользователи каждой категории отвечают за выполнение различных функций системы. В DiaSpectrEx пароли первоначально устанавливаются администраторами, затем могут меняться пользователями других категорий. Их учет и хранение выполняет СУБД. Пароли хранятся в специальных файлах СУБД в шифрованном виде. После ввода пароля пользователю предоставляется доступ к требуемой информации. Несмотря на простоту парольной защиты, у нее имеется ряд недостатков. Во-первых, пароль уязвим, особенно если он не шифруется при хранении в СУБД. Во-вторых, пользователю нужно запоминать или записывать пароль, а при небрежном отношении к записям пароль может стать достоянием других.

Более мощным средством защиты данных является шифрование, применяемое для защиты уязвимых данных. В системе DiaSpectrEx шифрование обеспечивает три состояния безопасности информации: конфиденциальность, целостность, идентифицируемость. Встроенные функции шифрования присутствуют далеко не во всех СУБД, следовательно, универсальным данный метод назвать нельзя. Система MySQL, используемая при разработке DiaSpectrEx, предлагает два однотипных набора функций шифрования, в одном из которых реализован алгоритм DES (Data Encryption Standard), а в другом – AES (Advanced Encryption Standard). Кроме того, в MySQL реализовано несколько алгоритмов хэширования. В системе DiaSpectrEx используются функции шифрования на основе алгоритма AES – итерационного блочного симметричного шифра с архитектурой «Квадрат». Эти функции представляют собой наиболее устойчивый криптографический алгоритм, который доступен в MySQL; они имеют вид AES_ENCRYPT(string, key) и AES_DECRYPT(string, key).

Основанием для использования AES является то, что данный алгоритм соответствует следующим критериям: противодействие всем известным атакам, достаточно хорошая скорость выполнения и компактность кода для широкого круга платформ, простота разработки. Функции шифрования данных алгоритмом AES используют 128-битный ключ шифрования, т. е. шифрование ключами размером 192 и 256 бит, предусмотренными стандартом AES, в MySQL не реализовано, однако при помощи патча к исходному коду длину ключа можно увеличить до 256 бит. Ключ шифрования задается явным образом как один из параметров функции. AES, как и любой блочный шифр, поддерживает принципы рассеивания и перемешивания. Однако при этом AES может выполняться быстрее, чем обычный блочный алгоритм шифрования. Алгоритм шифрования не использует арифметические операции, поэтому тип архитектуры процессора не имеет значения. AES является полностью «самоопределяемым», он не использует других криптографических компонентов, S-box, взятых из хорошо известных алгоритмов, битов, полученных из специальных таблиц, и т. д. AES не подвержен многим видам криптоаналитических атак, таких как дифференциальный и линейный криптоанализ, Square-атака, метод интерполяции и др. Некоторым недостатком можно считать то, что режим обратного расшифровывания отличается от режима шифрования порядком следования функций, и сами эти функции отличаются своими параметрами от применяемых в режиме шифрования.

Таким образом, для системы DiaSpectrEx применен алгоритм AES – один из наиболее надежных и криптостойких на настоящий момент симметричных алгоритмов блочного шифрования.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Дейт К. Дж. Введение в системы баз данных.— Киев: Вильямс, 2000.

2. Бернет С., Пэйн С. Криптография. Официальное руководство RSA Security.— Москва: Бином, 2002.

3. Комлевая Н.О., Комлевой А.Н., Чернега К.С. Проектирование специализированной компьютерной системы для проведения пульмонологического диагностирования // Проблеми програмування.— Киев, 2014.— № 2 – 3.— С. 253 – 262.

4. Комлевая Н.О., Чернега К.С., Комлевой А.Н. Разработка архитектуры системы диагностирования SPECTREX // Тр. 12-й Всеукраїнської наук.-техн. конф. «Математичне моделювання та інформаційні технології».— Україна, м. Одеса.— 2014.— С. 70 – 71.

5. Komlevoy A., Bazhora Yu., Cherniavskyi V. The differential analysis of seasonal changes of the moisture condensate macromolecular structure of the exhaled air according to laser correlation spectroscopy data // British Journal of Science, Education and Culture. —London University Press.— 2014.— N 1 (5).— Vol. III.— P. 19–27.

6. Хомоненко А. Д., Цыганков В. М., Мальцев М. Г. Базы данных: Учебник для вузов.— Санкт-Петербург: КОРОНА принт, 2002.

N. O. Komlevaya, K. S. Chernega

Complex protection of information in specialized diagnostic systems.

The article analyzes the modern means for implementation a comprehensive information security in multi-user systems with a database in their structure. On the example of a computer system for pulmonary diagnostics, the means to ensure the integrity of data and control access to them were described. The use of AES encryption method for cryptographic protection of information was justified.

Keywords: *data protection, AES, system diagnostics, encryption.*