УДК 004.056

СПОСОБ МОДЕЛИРОВАНИЯ ПРОЦЕССА ОБНАРУЖЕНИЯ АНОМАЛЬНЫХ SQL-ЗАПРОСОВ К БАЗЕ ДАННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ НА ОСНОВЕ ПРИМЕНЕНИЯ РАСКРАШЕННОЙ СЕТИ ПЕТРИ

Липатников Валерий Алексеевич[1], Сахаров Дмитрий Владимирович[2], Шевченко Александр Александрович[1], Варибрус Александр Владимирович[1]

[1] Военная академия связи им. Маршала Советского Союза С.М. Буденного
Тихорецкий пр., 3, Санкт-Петербург, 194064, Россия

[2] Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича
Большевиков пр., 22/1, Санкт-Петербург, 193232, Россия

e-mails: lipatnikovanl@mail.ru, sguard7@mail.ru, alex_pavel1991@mail.ru, alvaribrus@yandex.ru

Аннотация. Актуальность. Ставится и рассматривается решение задачи разработки математической модели, позволяющей определить характеристики обеспечения безопасности баз данных в информационно-телекоммуникационных системах. Цель: разработать модель процесса обеспечения безопасности баз данных информационно-телекоммуникационных систем. Результат: предложена модель процесса обеспечения безопасности баз данных информационно-телекоммуникационных систем. Новизна: модель процесса обеспечения безопасности баз данных информационно-телекоммуникационных систем позволяет в отличие от известных определять зависимость показателей безопасности баз данных от внутренних и внешних параметров. Практическая значимость: использование модели процесса обеспечения безопасности баз данных информационно-телекоммуникационных систем позволит повысить защищенность баз данных.

Ключевые слова: информационная безопасность; базы данных в информационно-телекоммуникационных системах; SQL-инъекции; аномальные SQL-запросы; модель процесса обнаружения аномальных SQL-запросов.

A METHOD FOR MODELING THE PROCESS OF DETECTING ABNORMAL SQL-QUERIES TO THE DATABASE OF AN INFORMATION AND TELECOMMUNICATION SYSTEM BASED ON THE USE OF A COLORED PETRI NET

Lipatnikov Valery[1], Sakharov Dmitrii[2], Shevchenko Alexander[1], Varibrus Alexander[1]

[1] The Military Academy of Telecommunications, named after Marshal of the Soviet Union S.M. Budyonny
3 Tikhoretsky Av, St. Petersburg, 194064, Russia

[2] The Bonch-Bruevich Saint Petersburg State University of Telecommunications
22/1 Bolshevikov Av, St. Petersburg, 193232, Russia

e-mails: lipatnikovanl@mail.ru, sguard7@mail.ru, alex_pavel1991@mail.ru, alvaribrus@yandex.ru

Abstract. Relevance. The solution of the problem of developing a mathematical model that allows determining the characteristics of database security in information and telecommunication systems is posed and considered. Objective: to develop a model of the process of ensuring the security of databases of information and telecommunication systems. Result: a model of the process of ensuring the security of databases of information and telecommunication systems is proposed. Novelty: the model of the process of ensuring the security of databases of information and telecommunication systems allows, unlike the known ones, to determine the dependence of database security indicators on internal and external parameters. Practical significance: the use of a model of the process of ensuring the security of databases of information and telecommunication systems will increase the security of databases.

Keywords: information security; databases in information and telecommunication systems; SQL injections; abnormal SQL queries; model of the process of detecting abnormal SQL queries.

Приложения, любой код, который принимает входные данные из ненадежного источника, а затем использует эти входные данные для формирования динамических операторов SQL, могут быть уязвимыми (например, приложения «толстого клиента» в архитектуре клиент/сервер). Поэтому задача обнаружения аномальных SQL-запросов в настоящее время является актуальной [1].

В связи с этим ставится задача разработки математической модели, позволяющей определить характеристики обеспечения безопасности БД в ИТКС [2, 3].

Целью моделирования является определение степени опасности SQL-инъекции для БД ИТКС в зависимости от параметров средств защиты и выработка предложений по парированию воздействий [4, 5].

Для понимания принципа взаимодействия пользователя с БД ИТКС определим список требований к процессу взаимодействия пользователя с БД ИТКС [6]: оперативность, доступность, надежность информации, целостность и конфиденциальность данных, хранящихся в БД.

Рассматривается взаимодействие пользователя с БД [7, 8], содержащей конфиденциальную информацию, в ИТКС типа «клиент-сервер» с использованием сервера БД [9]. В качестве примера использована база данных пользователей, состоящая из двух таблиц: адреса дома и данных о жильцах.

Для установления зависимости вероятности успешного взаимодействия пользователя от основных факторов определим их показатели: вероятность своевременного отображения данных, вероятность исправной работы аппаратной части ИС, вероятность успешного обеспечения целостности данных БД, вероятность доступа

к данным БД и вероятность защищенности от НСД. Из рассмотренных показателей администратор ИТКС не может влиять на первые два показателя, но может оказать воздействие на следующие три.

Прежде чем разработать математическую модель, позволяющую определить характеристики обеспечения безопасности БД в ИТКС, был исследован процесс обмена данными между пользователем и персональной системой управления базами данных (СУБД) при выполнении наиболее часто используемой операции выбора данных [1] и процесс SQL-инъекции в БД ИТКС. В результате чего был получен алгоритм частного случая обнаружения аномальных SQL-запросов, на основе которого была разработана математическая модель процесса обнаружения аномальных SQL-запросов к БД.

Модель процесса обнаружения аномальных SQL-запросов к БД создана на основе сетей Петри. Сеть Петри представляет собой двудольный ориентированный граф, состоящий из вершин двух типов – позиций и переходов, соединённых между собой дугами. Вершины одного типа не могут быть соединены непосредственно. В позициях могут размещаться метки (маркеры), способные перемещаться по сети. Белыми кружками обозначены позиции, полосками – переходы, чёрными кружками – метки [10].

В отличие от классической сети Петри, где все метки предполагались одинаковыми, в раскрашенных сетях Петри используются различимые метки. В данных сетях фишкам приписываются некоторые признаки, например различные цвета (переменные), а кратности дуг интерпретируются как функции от этих переменных.

Для понимания принципа внедрения SQL-инъекций при функционировании ИТКС создана модель работы ИТКС в условиях внедрения аномальных SQL-запросов. Модель построена на основе раскрашенной сети Петри, где используются маркеры различного цвета, обозначающие запросы, которые нарушают свойства безопасности БД: зеленый – запросы, нарушающие целостность конфиденциальных данных; красный – запросы, добавляющие сторонние данные; синий – запросы, читающие конфиденциальные данные; а голубой – пользовательские запросы.

Разработанная модель позволит проводить серии экспериментов по исследованию защищенности БД. В результате экспериментов с использованием предлагаемой модели получим количество успешных воздействий на БД ИТКС с помощью инъекции, нарушающих целостность конфиденциальных данных, добавляющих сторонние данные и читающих конфиденциальные данные и количество всех воздействий на БД ИТКС с помощью SQL-инъекций. С помощью вышеописанных данных является возможным вычислить вероятности успешного обеспечения целостности данных БД, доступа к данным БД и защищенности от НСД. В свою очередь оценка данных параметров позволит провести оценку защищенности БД ИТКС и в случае воздействия злоумышленника разработать перечень мер по противодействию несанкционированной активности.

В итоге рассмотрены особенности внедрения SQL-инъекции в БД, а также исследован процесс обнаружения аномальных SQL-запросов. Модель обнаружения аномальных SQL-запросов может использоваться для исследования SQL-инъекций, воздействующих на реляционные БД, на основе применения комбинированной многоуровневой и многослойной искусственной нейронной сети.

Новизна заключается в том, что в отличие от известных способов моделирования предлагается способ на основе раскрашенной сети Петри.

Практическая значимость заключается в том, что разработанная модель на основе раскрашенной сети Петри описывает цикл взаимодействия с учетом процесса защиты информации и может использоваться при создании средств защиты БД ИТКС различных предприятий и государственных структур.

СПИСОК ЛИТЕРАТУРЫ

1. Justin Clarke. SQL Injection Attacks and Defense. Elsevier, 2012. – 576 pp. ISBN 13: 978-1-59749-424-3
2. Горохов А.В., Липатников В.А. Разработка модели процесса управления ИБ БД и исследование зависимости показателя процесса управления ИБ БД внутренних и внешних факторов. Интернаука. 2021. № 38-1 (214). С. 26-29.
3. Горохов А.В., Липатников В.А., Косолапов В.С. Разработка алгоритма модели процесса управления информационной безопасностью баз данных в информационно-вычислительной сети. Транспорт России: Проблемы и перспективы – 2021: материалы Международной научно-практической конференции. 09-10 ноября 2021 г. – СПб.: ИПТ РАН. 2021. Том 2. С. 161 - 166.
4. Ломанов А. А., Липатников В. А., Парфиров В. А., Шевченко А. А., Косолапов В. С. Программный комплекс для распознавания аномалий в сетевом трафике на основе многокритериального классификатора в условиях угроз вторжений. Свидетельство о регистрации программы для ЭВМ 2022611916, 04.02.2022. Заявка № 2022610839 от 24.01.2022.
5. Липатников В.А., Шевченко А.А. Методика проактивного управления информационной безопасностью распределенной информационной системы на основе интеллектуальных технологий. Информационные системы и технологии. 2022. № 2 (130). С. 107-115.
6. Костарев С. В., Карганов В. В., Липатников В. А., Технологии защиты информации в условиях кибернетического противоборства: Науч. монография / Под общ. ред. В. А. Липатникова. – СПб.: ВАС, 2020. – 716 с.
7. Красов А.В., Сахаров Д.В., Тасюк А.А. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных. Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70-76.
8. Липатников В. А., Шевченко А. А., Косолапов В. С., Сокол Д. С. Метод обеспечения информационной безопасности сети VoIP-телефонии с прогнозом стратегии вторжений нарушителя. Информационно-управляющие системы, 2022, № 1 (116)., С. 54-67. doi:10.31799/1684-8853-2022-1-54-67.
9. Ковцур М.М., Никитин В.Н., Юркин Д.В. Протоколы обеспечения безопасности VoIP-телефонии. Защита информации. Инсайд. 2012. № 3 (45). С. 74-81.
10. Тихонов В.А., Новиков В.А. Верификация систем управления доступом на основе моделирования раскрашенными сетями ПЕТРИ. Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 6. С. 50-59.