При анализе системы на отсутствие в ней потенциальных ситуаций взаимных блокировок приходится проверять большое количество порожденных при декомпозиции вспомогательных систем. Кроме того, исходная система может состоять из достаточно большого числа субъектов, активно взаимодействующих со средствами синхронизации. Данное обстоятельство делает анализ модели достаточно трудоемким (независимо от того, проводится он в ручном или автоматическом режиме).

В связи с этим был разработан алгоритм, позволяющий сводить проблему поиска структур некорректного использования средств синхронизации к проблеме поиска сильно связных компонент в ориентированном графе. Данный алгоритм позволяет проверить отсутствие в исходной модели потенциальных ситуаций взаимной блокировки.

Сложность алгоритма составляет $O(n^5)$, где n — число вершин общего графа системы, что является его несомненным достоинством, поскольку сложность прямого подхода, основанного на поиске ситуаций взаимной блокировки путем анализа относительных динамик выполнения различных потоков, является экспоненциальной.

На основе представленного подхода разработано программное средство анализа моделей многопоточного программного обеспечения, которое предоставляет возможность создания, редактирования, сохранения, загрузки моделей многопоточного программного обеспечения, а также позволяет показывать отсутствие потенциальных ситуаций взаимных блокировок в модели. Программное средство представляет собой совокупность совместно используемых библиотек, в которых непосредственно содержатся компоненты приложения, и ядра, организующего работу и взаимодействие компонентов. Такая компонентная архитектура обладает рядом преимуществ, таких как: четкая инкапсуляция деталей реализации за интерфейсами; возможность легкого добавления, замены, удаления компонент; облегчение процесса тестирования программного средства.

СПИСОК ЛИТЕРАТУРЫ:

1. *Bensalem S., Havelund K.* Dynamic Deadlock Analysis of Multi-threaded Programs // Haifa Verification Conference / Shmuel Ur, Eyal Bin, and Yaron Wolfsthal, ed. Vol. 3875 of LNCS. Springer, 2005. P. 208–223.
2. *Engler D., Ashcraft K.* RacerX: Effective, Static Detection of Race Conditions and Deadlocks // Proceedings of the 19th ACM Symposium on Operating Systems Principles. Oct. 2003. P. 237–252.
3. *Дал У., Дейкстра Э., Хоор К.* Структурное программирование. 1-е изд. М.: Мир, 1975.

Т. М. Пестунова, З. В. Родионова

ОБ ОДНОМ ПОДХОДЕ К УПРАВЛЕНИЮ ПРАВАМИ ДОСТУПА

Эффективность функционирования современных автоматизированных информационных систем (АИС) предприятия во многом зависит от того, насколько соответствуют полномочия пользователя системы его должностным функциям. Признанным фактом является то, что расширение полномочий сверх необходимых приводит к увеличению случайных ошибок, росту рисков, связанных с несанкционированным доступом к данным. При недостаточных полномочиях возникают затруднения в выполнении сотрудником своей работы.

Формализованные полномочия в виде прав доступа получают свое отражение в настройках систем разграничения доступа (СРД) АИС, безопасное построение которых определяется формальной моделью. Несмотря на достаточно высокий уровень теоретических исследований в

области формальных моделей доступа, их практическая реализация наталкивается на существенные трудности, связанные с интерпретацией, т. е. с обеспечением соответствия абстрактных сущностей и процессов модели реальным объектам и правилам функционирования АИС и актуализацией прав доступа ввиду постоянных изменений бизнес-процессов. Ситуация многократно усложняется, если на предприятии функционирует несколько АИС, каждая из которых обладает собственной СРД.

В силу указанных обстоятельств актуальной является задача управления правами доступа, решение которой позволяло бы формировать множество прав доступа с точки зрения их необходимости и достаточности для выполнения пользователем его функций исходя из потребностей бизнес-процесса, а также своевременно корректировать эти права при внесении изменений в бизнес-процесс.

Для решения обозначенной проблемы предлагается использовать систему управления правами доступа (СУПД). Под СУПД понимается информационная система, в которой формализуются и хранятся описания правил доступа (с учетом динамики изменений). Основное назначение этих правил заключается в разделении информации на части и организации такой системы работы с информацией, при которой пользователи имеют доступ к той и только к той части информации, которая им необходима и достаточна для выполнения своих обязанностей в рамках бизнес-процесса.

Таким образом, первоисточником для назначения прав доступа является бизнес-процесс. Руководство утверждает права доступа посредством утверждения описания бизнес-процесса. Такой подход основывается на самой сути деятельности организации, ее бизнес-процессах и позволяет выйти на более формальный уровень принятия решения о предоставлении прав доступа и обеспечить следующие преимущества:

— снижение человеческого фактора при определении доступа к информации, так как права доступа определяются исходя из требований процесса, а не из должностных инструкций (часто устаревших) и/или личного мнения руководителя подразделения;

— возможность оперативного внесения изменений в СУПД при изменении бизнес-процессов организации;

— возможность выявления и устранения узких мест процесса с точки зрения безопасности информации;

— снижение рисков за счет выявления возможных проблем процесса до внедрения СУПД.

Для реализации возможности управления правами доступа в условиях СРД, функционирующих на основе различных формальных моделей (ролевой — RBAC, дискреционной — DAC, мандатной — MAC), была разработана обобщенная модель разграничения прав доступа, в терминах которой может быть описана структура, принципы действия перечисленных конкретных моделей доступа. Цель разработки метамодели заключается в организации функционирования различных моделей доступа в одном информационном пространстве.

СУПД формирует права доступа, не осуществляя разграничение доступа к ресурсам для конкретной подсистемы, для этих целей существуют системы разграничения доступа. Система разграничения доступа зависит от программно-технических особенностей конкретной информационной системы управления, СУПД же является независимой и может/должна быть единой для всех АИС организации.

Для создания и последующей организации функционирования СУПД на вход системы должны поступить описания бизнес-процессов и информация об их изменениях. На выходе формируются каталог ролей, иерархия ролей и матрица доступа.

Управление правами доступа, с одной стороны, заключается в выделении пользователей, ролей, уровней их иерархии и объектов доступа на основе анализа бизнес-процесса, с другой стороны, в ассоциации действий и событий бизнес-процесса с совершением доступа. В СУПД циркулируют сущности, расположенные в рамках пяти слоев: пользователи, роли, бизнес-процессы,

права доступа, уровни доступа. При этом выделяются следующие этапы управления правами доступа с использованием СУПД:

1. Описание (внесение изменений) бизнес-процессов;
2. Анализ угроз и уязвимостей;
3. Анализ бизнес-процессов;
4. Формирование матрицы доступа;
5. Настройка прав доступа;
6. Внесение изменений в бизнес-процессы.

Анализ бизнес-процессов можно производить автоматически (например, с помощью языка XML), извлекая все необходимые для СУПД данные из среды бизнес-моделирования. После того как СУПД построена и введена в действие, управление правами доступа осуществляется на основе сравнения состояния модели бизнес-процессов до и после внесения каких-либо изменений.

В. А. Петров, К. А. Сенчугов

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ERP-СИСТЕМ. АНАЛИЗ УЯЗВИМОСТЕЙ

ERP-системы (Enterprise Resource Planning — системы планирования ресурсов предприятия) служат для интеграции данных и процессов организации, таких как учет основных средств, кадровый учет, взаимодействие с клиентами, логистика и финансы, в единую систему.

В идеале ERP-система автоматизирует все возможные сферы деятельности предприятия, ускоряет и упрощает работу персонала, дает в руки менеджмента мощнейший инструмент для анализа эффективности и планирования.

Поскольку в этих системах циркулирует критически важная для нормальной работы организации информация, они часто становятся целью атак злоумышленников. Типичные ERP-системы используют клиент-серверную модель работы, и поэтому для них выделяют такие угрозы для информационной безопасности, как нарушение конфиденциальности данных, передаваемых между компонентами ERP-системы, несанкционированное искажение данных, передаваемых между компонентами ERP-системы, несанкционированный доступ (НСД) к информации, хранимой в БД ERP-системы, и т. д.

По результатам анализа угроз предъявляются требования к системе защиты, которая должна обеспечивать должный контроль как на уровне базы данных, так и на уровнях приложений и представления. Системы защиты должны соответствовать государственным и внутрикорпоративным нормам защиты информации и обеспечивать уменьшение рисков потери/раскрытия информации.

В данный момент на российском рынке систем автоматизации бизнеса наряду с продуктами таких компаний, как Oracle, Sap и Microsoft, представлены продукты от отечественных производителей, которые благодаря своей дешевизне и адаптированности к местным условиям и законодательству успешно конкурируют с продукцией западных фирм.

В ряду отечественных продуктов, несомненно, выделяется система «1С: Предприятие», которая уже больше 10 лет служит стандартом автоматизации и учета для предприятий малого и среднего бизнеса. За это время система и методы ее защиты постоянно совершенствовались. В связи с появлением новой технологической платформы «1С: Предприятие 8.2» (изменения в которой позиционируются самой фирмой «1С» как наиболее существенные с момента появления системы), а также чрезвычайно широкой распространенностью этих программных продуктов проведенный анализ