А. Ю. Лаврухин

ПОДХОДЫ К ПРАКТИЧЕСКОМУ ВНЕДРЕНИЮ IDENTITY MANAGEMENT-РЕШЕНИЙ

Необходимость внедрения IdM-решений

Рост количества информационных систем, вовлеченных в технологические процессы современных корпораций любой из отраслей деятельности, делает все более актуальным вопрос контроля и управления доступом к информационным ресурсам (ИР) компании.

Классические модели организации доступа к ИР, такие как мандатная и дискреционная, зачастую не удовлетворяют основным бизнес-требованиям, предъявляемым к процессу предоставления и контроля доступа как со стороны производственных подразделений, так и со стороны ИТ- и ИБ-служб. Единственным выходом из данной ситуации для многих крупных компаний является внедрение более сложных механизмов управления доступом, основанных на ролевом принципе.

Потребность в решениях такого рода вызвала массовый рост рынка ПО, которое позволяет автоматизировать процессы управления учетными записями и идентификационными данными пользователей, а также обеспечивает автоматизацию процессов внутреннего согласования при предоставлении доступа к ИР компании.

Внедрение IdM-решений обеспечивает эффективную реализацию многих технологических задач и позволяет в значительной степени оптимизировать управление ИТ-инфраструктурой компании. Кроме того, в России, как и на Западе, появилось множество законодательных актов, прямо или косвенно указывающих на необходимость внедрения подобных систем, например Sar-banes-Oxley Act, серия международных стандартов ISO 27XXX, различные требования и рекомендации по построению информационных систем, такие как CoBIT, ITIL и пр. Стоит отдельно отметить серию стандартов Банка России, определяющих требования к построению систем обеспечения и управления информационной безопасностью в кредитно-финансовой сфере, а также Закон «О персональных данных», существенную часть требований которых можно реализовать путем внедрения IdM-решения.

Этапы внедрения

Как правило, внедрение IdM-систем состоит из двух основных этапов: консалтингового и прикладного. На первом этапе компания, осуществляющая внедрение IdM-решения, разрабатывает ролевую модель, на основе которой будет производиться последующая автоматизация процессов управления доступом к ИР, а также совместно с заказчиком формализует и описывает технологические процессы по управлению согласованием, предоставлением и блокированием доступа к подключаемым ИР.

На втором этапе производится автоматизация разработанных технологических процессов на основе ролевой модели средствами внедряемого IdM-решения.

Внедрение ролевой модели предусматривает создание типовых профилей пользователей, связывающих функциональную роль (например, оператор биллинговой системы) с конкретными полномочиями доступа к информационным ресурсам различных автоматизированных систем. Поэтому на начальном этапе внедрения ролевой модели в компании необходимо разработать описание типовых функциональных ролей, а также провести аналитическую работу по оценке необходимых и достаточных полномочий на доступ к информационным ресурсам в рамках выделенной функциональной роли. При этом крайне важно правильно спланировать архитектуру ролевой модели с учетом динамики развития информационной инфраструктуры компании и возможности последующего эффективного управления ролями.

Укрупнение ролевой модели, т. е. включение в одну функциональную роль всех полномочий, которые могут понадобиться сотруднику компании для выполнения им своих должностных обязанностей, крайне затруднит последующее поддержание данной ролевой модели в актуальном состоянии. При добавлении или удалении части полномочий у пользователя в случае изменения его должностной инструкции возникнет необходимость пересмотра целых ветвей ролевой модели. Поэтому рекомендуется формировать набор типовых функциональных ролей, изменение которых производится крайне редко, но в то же время полномочия, входящие в данную роль, должны позволять выполнять одну или несколько функциональных задач. В этом случае для реализации всех полномочий на определенной должности сотруднику компании может быть назначено несколько функциональных ролей, комбинация которых обеспечит необходимый и достаточный доступ к информационным ресурсам. Данный подход позволяет эффективно решать многие задачи, стоящие перед службой информационной безопасности, связанные с контролем доступа, такие как разделение полномочий (segregation of duties), периодический мониторинг списка пользователей, имеющие доступ к критичным информационным ресурсам, отчетность и т. п.

При выборе решения, на базе которого будет производиться дальнейшая автоматизация процессов управления доступом к ИР компании, следует обратить внимание на наличие адаптеров к автоматизированным системам, подключение к которым осуществляется в рамках внедрения. При этом предпочтение следует отдавать системам, реализующим «безагентную архитектуру» адаптеров, т. е. не требующим установки дополнительных программных агентов на серверы подключаемых систем.

Сейчас представлен широкий спектр программных решений, позволяющих автоматизировать процессы управления учетными записями и идентификационными данными пользователей, а также обеспечить автоматизацию процессов внутреннего согласования о предоставлении доступа сотрудников к информационным ресурсам. Основными аспектами, в соответствии с которыми производится оценка и выбор технологической платформы, являются:

- централизованное управление механизмами безопасности на основании единой политики. При этом при построении SOA-решений возможно применение единых механизмов безопасности для всего спектра приложений. Это существенно ускоряет построение интегрированной системы безопасности и снижает риски информационной безопасности за счет унификации механизмов защиты и контроля;
- поддержка всех основных платформ и бизнес-приложений и простота интеграции с имеющимися приложениями на основе специального инструментария, что сокращает затраты на интеграцию приложений в единую систему управления безопасностью и сохраняет инвестиции в ИТ-инфраструктуру;
- согласованное управление доступом на основе должностных обязанностей с интеграцией с кадровой системой, что сокращает процесс предоставления необходимых полномочий до нескольких минут;
- возможность интеграции средств документооборота в имеющиеся системы, что позволяет интегрировать процессы управления безопасностью в имеющиеся процессы управления ИТ;
- контроль соблюдения политики безопасности с использованием средств аудита и отчетности, что позволяет удовлетворять требования руководящих документов в области информационной безопасности. Возможно также построение интегрированной системы управления информационной безопасностью как в концепции SOA, так и в среде унаследованных приложений;
- отсутствие глобальной единой точки отказа для доступа пользователей к приложениям, с одной стороны, и максимальная централизация IdM для управления корпоративными учетными записями — с другой;
- масштабирование до сотен тысяч управляемых учетных записей без ухудшения их QoS (Quality of Service) за счет нового фактора влияния централизованного узла IdM;
- эффективное функционирование в условиях регулярных изменений (патчи, апгрейды) управляемых ресурсов после внедрения IdM.