


Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

№ 11 (174)/2007



Тема номера:
**IdM – новый уровень
в управлении
информационными
системами компании**

КОРПОРАТИВНЫЕ
СИСТЕМЫ

СОДЕРЖАНИЕ

Тема номера:

IdM – новый уровень в управлении информационными системами компании

«Разрешите представиться» (Л. Черняк).....	3
Identity Management: взгляд Sun Microsystems (В. Буряков)	5
Identity Management. Актуально для финансового сектора (Е. АКИМОВ)	9
Oracle: комплексные решения на базе IdM (Д. Шепелявый)	10

Наши проекты

Построение сети нового поколения в Казахстане	12
---	----

ТЕМА НОМЕРА:

IdM – новый уровень в управлении информационными системами компании

Главная тема номера – IdM-решения. Среди авторов материалов – специалисты компаний, продвигающих на ИТ-рынке разработки в области информационной безопасности. Предваряя материалы об IdM-решениях, преимуществах и перспективах, которые они дают компаниям, использующим их, мы предлагаем читателю статью обозревателя журнала «Открытые системы» Леонида Черняка «Разрешите представиться» (*Computerworld Россия*, № 12, 2007; <http://www.osp.ru/cw/2007/12/4098168/>; публикуется с разрешения издательства «Открытые системы»; все права сохранены), которая знакомит с общей концепцией IdM.

«Разрешите представиться»

Леонид Черняк

Концепция Identity Management вовсе не так тривиальна, не столь технологична, как ее обычно представляют.

За старомодными оборотами «разрешите представиться» и «разрешите вам представить» обнаруживаются технологические приемы идентификации личности. На социальном уровне проблемы идентификации частично решены и продолжают решаться, а на сетевом к ним еще только приступают.

Концепция Identity Management относительно нова, она стала предметом особенно активного обсуждения с 2000 года, когда пристальное внимание к ней привлекли работы аналитиков таких компаний, как Burton Group и Gartner. Идеи, собранные в данной концепции, оказались особо привлекательными для компаний, специализирующихся на вопросах информационной безопасности. Эти компании в значительной мере узурпировали представление о ней, сведя концепцию к совокупности технологий, чем существен-

но сузили содержание, выходящее далеко за технологические рамки. В действительности же концепция эта вовсе не так тривиальна, не столь технологична, как ее обычно представляют.

В России сложностей еще больше. Начнем с того, что перевести или даже в нескольких словах объяснить по-русски установившийся английский термин Identity Management чрезвычайно сложно. В оригинале слово identity имеет массу значений — от «индивидуальности личности» в психологии до «тождества» в математике. Для толкования обсуждаемой концепции подходят разные значения этого слова. Проблемы усугубляются сложностями перевода слова management: ни «управление», ни «контроль» в данном случае не подходят. Поскольку появившиеся переводы — «управление идентичностью» и «управление идентификационной информацией» — далеко не бесспорны, остановимся на аббревиатуре IdM.

В то же время очень просто представить, что такое IdM, если обратиться к аналогии с комплексом действий с документами, удостоверяющи-

ми личность. Прежде всего, аналогия состоит в том, что, как и в сети, в реальной жизни в давние времена людям не нужны были документы вообще. С развитием связей появились посольские грамоты и рукописные паспорта. За исключением двух империй — Российской (введены Петром I) и Оттоманской — паспорта использовались только для зарубежных поездок, отсюда и перевод названия как «пропуск в порт». Но с увеличением мобильности населения идентификационные документы стали требовать повсеместно. В наше время даже в США, стране, которая дольше других продержалась без внутренних удостоверений личности, все чаще можно услышать слово «айди» (ID), скажем, в гостинице или при регистрации на конференции. Идентификационный документ (Identity Document), или удостоверение, — только часть системы; в нее входят также организации, которые его выдают, носители документов, службы, которые устанавливают соответствие документов личности носителя, и т. д. Все вместе они образуют «человеческую» систему Identity Management. Очень скоро документы станут снабжаться чипами, где совокупность идентификационных признаков будет оцифрована, и мы, таким образом, обретем «цифровую идентификацию» (digital identity).

IdM как система

В контексте IdM понятие identity можно рассматривать как восприятие совокупности характеристик и свойств некоторой сущности, позволяющих ее однозначно идентифицировать. Говоря о «человеческой индивидуальности», это понятие надо разделить на собственное осознание себя как индивидуальности и на отождествление человека как определенного субъекта социума. В таком случае на примере паспортного контроля процедура идентификации состоит в установлении принадлежности документа его предъявителю. Двудеяная природа identity чрезвычайно важна для понимания того, что такое digital identity. Это понятие можно определить как совокупность признаков, проявляемых какой-то сущностью, чтобы быть воспринятой цифровым социумом. Процедура установления тождественности digital identity позволяет определить цифровую идентичность человека по «цифровым идентификационным характеристикам» (Personal Identifiable Information, PII). Так устанавливается тождественность между человеком и его цифровой идентичностью.

Этой цели служит система IdM. Параметры PII идентифицируют роль человека в среде, а IdM

осуществляет администрирование PII в соответствии с заданными правилами. Действия системы IdM разделяются на следующие этапы:

- идентификация — установление системой IdM по введенным показателям PII личности его владельца;
- аутентификация — установление подлинности по паролям, различного рода ключам (токенам, картам) или по биометрическим показателям; по выполнении этих двух этапов пользователь может предпринимать некоторый ограниченный спектр действий с доступными ему данными;
- авторизация — получение прав на выполнение совокупности действий, по регламенту дозволенных этому пользователю.

Обычно IdM ассоциируют с рядом современных криптографических технологий, прежде всего с инфраструктурой открытых ключей, но первые работы в этом направлении были сделаны намного раньше. В 1984 году известный криптограф Дэвид Чаум разработал основы технологии идентификации с помощью специальных карт и создал математическую модель IdM. Ему принадлежит следующее определение: «IdM — это всеобъемлющий набор процедур, обеспечивающих пользователям безопасный доступ к ресурсам информационных систем, управление присутствием пользователей в системе, а также управление информацией об их идентификации». Его можно дополнить такой формулировкой: «IdM представляет собой категорию взаимосвязанных решений, служащих для управления идентификацией и аутентификацией пользователей, правами и ограничениями на доступ к информации, учетными записями, паролями и другими атрибутами, поддерживающими ролевые функции пользователей в одной или нескольких прикладных системах».

В число функций, реализуемых системами IdM, входят:

- управление учетными записями;
- управление доступом, в том числе идентификация, авторизация и аутентификация;
- управление защитой персональной информации;
- управление объединением ресурсов, представляющее собой набор соглашений, стандартов и технологий, обеспечивающих доверительные отношения между распределенными системами;
- обеспечение «службы одного окна» (Single Sign-On), позволяющей пользователю применять единый механизм для доступа к различным системным ресурсам;

- персонализация, позволяющая адаптироваться к пользовательским предпочтениям.

IdM сегодня и завтра

Для широкого распространения IdM требуются общие отраслевые протоколы, представления о семантике, правила обработки; поэтому ряд международных организаций ведет разработку стандартов. Так, консорциум OASIS разрабатывает специализированные стандарты: языки SAML (Security Assertion Markup Language), DSML (Directory Service Markup Language), SPML (Service Provisioning Markup Language), XACML (eXtensible Access Control Markup Language) и др. Альянс Liberty Alliance создает структуру и бизнес-модели. Альтернативный подход разрабатывается в рамках европейского проекта PRIME.

Компании, производящие технологии для IdM, можно разделить на две группы. В первую входят поставщики комплексных решений, в их числе Verisign, CA, IBM, Oracle, HP и Sun Microsystems. Вторую, более многочисленную группу, составляют поставщики отдельных решений; среди них такие известные компании, как EMC/RSA Security и BMC.

Буквально в последние год-два стало формироваться альтернативное направление, получившее, как это теперь принято, название Identity 2.0. В его основе лежит открытая децентрализованная модель идентификации, и базируется это направление на предположении о возможности создания такой модели идентификации, которая могла бы управляться самим пользователем, без привлечения служб, наделенных особыми полномочиями.

Identity Management: взгляд Sun Microsystems

Виктор Буряков,
директор по интегрированным решениям и сервисам,
руководитель отдела программных продуктов Sun Microsystems

Развитие сетевого сообщества подчиняется тем же законам, что и развитие общества, за одним исключением: все процессы идут во много раз быстрее. Это правило относится и к проблемам, связанным с идентификацией членов общества. Когда-то человеку достаточно было имени, потом пришлось ввести фамилии, относительно недавно появились различные идентификационные документы, а в последние годы в ход пошли оцифрованные образы таких атрибутов, как отпечатки пальцев и снимки радужной оболочки глаза. Все это — неизбежные последствия того, что принято называть глобализацией; в области информационных технологий ее «синонимом» является Internet.

Установление доверительных отношений между участниками коммуникаций превращается в одну из критически важных проблем нынешнего

периода развития ИТ, называемого «эпохой участия» (примеры взаимодействия, характерные для современного бизнеса, приведены на стр. 6 в Табл.1). Актуальность проблемы возрастает пропорционально количеству коммуникаций. Ее решение обычно возлагается на совокупность технологий, связанных с управлением сетевой идентификацией (Identity Management, IdM). Существует множество определений IdM, но Sun Microsystems придерживается определения аналитической компании Burton Group: «IdM — это бизнес-процессы и поддерживающая их инфраструктура, предназначенные для создания, использования и обеспечения подлинности цифровой идентификации субъектов или объектов».

Проблема современного предприятия заключается в том, что число его информационных ресурсов переваливает за десятки и сотни — при

Табл. 1. Коммуникации в современном бизнесе.

Участники	Способы взаимодействия
Предприятие	• Сети, используемые для совместной работы
	• Аутсорсинг бизнес-процессов
	• Новые модели бизнеса, задействующие сетевые формы взаимодействия
Сообщество разработчиков	• Использование Java-технологий
	• Участие в разработках ПО с открытыми кодами
	• Участие в разработках стандартов
Государство	• Взаимодействие между гражданами и государством
	• Межведомственное взаимодействие
	• Взаимодействие на межправительственном уровне
Отдельные личности	• Участие в профессиональных и социальных сетях
	• Использование средств мгновенного обмена сообщениями
	• Персонализация контента и использование сетевых сервисов

количестве пользователей, кратном тысяче, а то и десятку тысяч. При этом пользователь выполняет разные роли на предприятии и, как правило, имеет доступ к ресурсам согласно таким ролям. Запоминание, хранение, синхронизация идентификационной информации становится серьезной проблемой для предприятия.

Для решения этих задач необходима система управления идентификационными данными пользователей, позволяющая автоматизировать процессы предоставления доступа, хранения и синхронизации идентификационных данных, а также проведение необходимых проверок/аудитов доступа к ресурсам предприятия.

Стоит отметить, что в отличие от других компаний – поставщиков решений IdM, Sun не воспринимает их лишь как инструмент однократной регистрации, а раскрывает перед заказчиками полный потенциал IdM и то, чем это направление может реально помочь их бизнесу. IdM позволяет обезопасить существенную часть бизнеса, сделать его более открытым и таким образом получить большую прибыль. Технологии IdM привлекают к себе внимание и быстро развиваются, поскольку они обеспечивают реальный контроль над тем, чем владеет предприятие.

Управление предприятием можно сравнить с управлением автомобилем. Возможности эффективного управления автомобилем определяются, кроме прочего, максимальными значениями ускорения и замедления. Следовательно, управляемое движение на высокой скорости обеспечивает не только мощный двигатель, но и

эффективные тормоза. В контексте информационных систем Гейтс отводит IdM роль тормозной системы, которая предназначена для снижения потенциальных рисков, сопутствующих развитию бизнеса.

Средства управления сетевой идентификацией и правами доступа пользователей обеспечивают комплексную безопасность, способствуют более полному соответствию законодательным нормативам и позволяют автоматизировать процессы, что в свою очередь ведет к снижению издержек предприятия. Поясним несколько подробнее, какие преимущества дает применение систем управления сетевой идентификацией и правами доступа пользователей.

Безопасность

Использование IdM обеспечивает безопасность на нескольких уровнях:

- автоматизированное исполнение стратегии предприятия, связанной с аутентификацией и авторизацией пользователей, безопасное администрирование доступа к информационным ресурсам и аудит доступа на уровне операционных и прикладных систем;
- защита организации от внешних и внутренних угроз. Для всех значимых информационных активов создается механизм, позволяющий предоставлять доступ к ресурсам по жестко заданному сценарию. Он дает возможность определять, кто, когда и к чему имеет доступ, отслеживать нарушения поли-

тики безопасности, а при необходимости — принимать меры для блокирования нарушителя.

Средства IdM реализуют управление жизненным циклом пользовательских данных — от первого подключения к необходимому набору ресурсов (базы данных, прикладные системы, телефонная станция, система доступа в здание и т.д.) до отслеживания модификаций данных (смена должности, фамилии, семейного положения и т.д.) и связанных с этим изменений прав доступа (вплоть до окончания отношений при увольнении или серьезных нарушениях).

Соответствие законодательным нормативам

Точное представление о том, кто и к каким информационным активам имеет (или имел раньше) доступ, обеспечивает предприятию соответствие определенным законодательным нормативам. Примером таких требований является Федеральный закон РФ «О персональных данных». Таким образом, доступ к персональным данным сотрудников и клиентов должен четко и ответственно контролироваться.

Серьезнейшим документом, заставляющим внедрять решения для контроля над доступом, является акт Sarbanes-Oxley. Исполнение его требований обязательно для предприятий, торгующих ценными бумагами на Нью-Йоркской фондовой бирже. Этот акт устанавливает персональную ответственность высшего исполнительного руководства предприятия за точность финансовых документов и процесс принятия решений. Акт регламентирует разграничение доступа к информации в зависимости от уровня ответственности сотрудника и его полномочий на те или иные действия. Кроме того, встроенные в IdM инструменты автоматического аудита позволяют обнаруживать неизбежные человеческие ошибки. Продолжив автомобильную аналогию, эту часть IdM можно сравнить с регулярным техосмотром, обеспечивающим контроль над состоянием автомобиля и безопасность движения.

Уменьшение затрат

Одним из важнейших критериев учета затрат на производство становится оценка эффективности инвестиций. При предоставлении ресурсов и контроле над доступом к ним без механизмов консолидации и автоматизации возникают значитель-

ные издержки, связанные с администрированием ИТ-ресурсов. В свою очередь регулярные аудиты политики доступа к ресурсам отнимают значительное время отдела ИТ.

Все перечисленные проблемы можно легко и изящно решить, применив IdM-решение и тем самым высвободив ресурсы для более продуктивной работы предприятия. В отличие от многих систем контроля над безопасностью, данная система автоматизирует ручной труд, а потому является окупаемой. Безусловно, сроки окупаемости зависят от предприятия и идущих на нем процессов, но с уверенностью можно говорить об экономической эффективности внедрения таких решений.

Защиту информационных активов предприятия нельзя свести только к контролю над тем, что корпоративные пользователи действительно являются теми, за кого они себя выдают (аутентификация), и к регламентации их возможностей доступа к корпоративным ресурсам (авторизация). Действие IdM должно распространяться не только на собственные корпоративные системы и приложения, но и на область контроля над доступом к системам и приложениям партнеров и поставщиков, находящимся вне границ корпоративной сети (в Extranet). По-настоящему действенная система IdM включает в себя весь комплекс механизмов распределения идентификационной информации между системами и приложениями — как во внутренней, так и во внешней сети.

По классификации, принятой в Sun Microsystems, все множество функций, которые должна обеспечивать система управления сетевой идентификацией, авторизацией и правами доступа пользователей на предприятии, можно разделить на три основные группы.

Обеспечение внутреннего контроля:

- обеспечение доступа и контроля над правилами, которыми регулируется и ограничивается доступ к информационным активам в зависимости от служебных функций сотрудника;
- предоставление в режиме реального времени сведений о том, кто и к чему имеет доступ, ведение архива доступа;
- автоматизация процедур аудита.

Исключение потенциальных уязвимостей:

- ограничение возможностей входа в систему единственной точкой аутентификации/авторизации пользователя;
- обеспечение полноценного визуального представления о том, кто и когда получал доступ к системе;

- реализация правил доступа к данным на основе ролей и функций участников коммуникаций.

Повышение качества обслуживания (QoS) за счет автоматизации и федерации сервисов:

- предоставление пользователям возможностей самообслуживания, в том числе управления паролями и учетными записями;
- передача части функций IdM партнерам;
- федерация функций IdM, распределенных между подразделениями и партнерами.

Перечисленные функции могут быть реализованы на базе архитектуры, использующей следующие основные программные решения Sun в области организации систем управления идентификационными данными пользователей и правами их доступа:

- Sun Java System Identity Manager — решение для автоматизированного создания учетных записей и синхронизации данных, относящихся к этим записям. Позволяет реализовать бизнес-процессы согласования предоставления /отключения доступа к ресурсам, автоматизировать делегирование полномочий, деактивировать доступ при изменении или завершении отношений между работником и компанией. Дает пользователям возможность самостоятельно управлять их паролями, обеспечивает мониторинг и проверку основных контрольных параметров идентификации, выявление нарушений и подготовку отчетов (т.е. функцию аудита).
- Sun Java System Access Manager — решение для однократной аутентификации пользователя в системе (Single Sign-On). Позволяет управлять доступом в соответствии с установленными ролями/правилами, устанавливать доверительные области — федерации (т.е. дает возможность партнерским прило-

жениям, входящим в федерацию, применять аутентификационные данные пользователей), а также проводить аудит транзакций, относящихся к предоставлению доступа на время пользовательских сессий.

- Sun Java System Directory Server Enterprise Edition предоставляет услуги каталогов для хранения и управления данными идентификации, служит основой для инфраструктуры управления сетевой идентификацией. Sun Java Directory Server Enterprise Edition эффективно интегрируется в многоплатформенную среду и обеспечивает безопасную, доступную по требованию синхронизацию паролей с Microsoft Windows Active Directory.

Очень важно, что каждый из вышеперечисленных продуктов может быть встроен как отдельный модуль, реализующий определенные функции в рамках решения задач управления идентификационными данными пользователей в ИТ-инфраструктуре предприятия. Например, Sun Identity Manager прекрасно интегрируется со службами каталогов Microsoft Active Directory, Open LDAP и Oracle Internet Directory. Он может быть развернут на платформах IBM AIX, HP-UX, Windows, Solaris, Red Hat Linux, BEA WebLogic, IBM WebSphere, Sun Java Application Server.

В течение ряда лет Sun Microsystems проводит последовательную политику совершенствования Identity Manager. При этом корпорация обращает большое внимание на развитие его функциональности, минимизацию затрат при внедрении, возможность применения в гетерогенных средах. Технологическое лидерство Sun в данной области отмечено рядом независимых аналитиков. По данным Forrester Research за I квартал 2006 года, Sun Identity Manager является наиболее предпочтительным продуктом как с точки зрения функциональности, так и по количеству завершенных внедрений.

Identity Management. Актуально для финансового сектора

**Евгений Акимов,
заместитель начальника Центра информационной безопасности,
«Инфосистемы Джет»**

Сегодня наблюдается повышенный интерес к теме централизованного управления ИТ-инфраструктурой. Он обусловлен, с одной стороны, наметившейся на российском рынке тенденцией роста кредитно-финансовых организаций, в том числе за счет слияний и поглощений, а с другой — бурным внедрением систем класса business-critical (CRM, АБС и т.п.). Потребности банков в интеграционных решениях возросли. Финансовые организации стараются обеспечить стабильность и устойчивость бизнеса, защищая свои активы путем минимизации рисков.

В компаниях, где постоянно происходит набор сотрудников, совершаются внутренние кадровые перемещения, расширяется география присутствия — все больше бизнес-задач решается при помощи специализированных корпоративных приложений, вследствие чего растет число критичных для бизнеса многопользовательских систем. Поэтому не удивительно, что тема организации централизованного доступа к ИТ-ресурсам становится одной из самых обсуждаемых.

Появилось множество законодательных актов, которые напрямую или косвенно связаны с необходимостью внедрения IdM-решений: серия международных стандартов ISO 2700x, Sarbanes-Oxley Act, различные требования и рекомендации по построению информационных систем, такие как CoBIT, ITIL и пр. Также необходимо отметить стандарт Банка РФ и Федеральный закон «О персональных данных».

Синхронизировать работу таких систем, выстроить логику доступа к ИС позволяют решения класса IdM, призванные уменьшить риски и сократить затраты на администрирование.

При подборе IdM-системы для конкретного банка многообразие предлагаемых решений и подходов поначалу может привести в замешательство. Как правильно выбрать подходящее решение? Какие нюансы следует учесть? Какую компанию привлечь в качестве генерального подрядчика? Что поставить на первый план: стоимость проекта или качество предоставляемых услуг?

Скорее всего, выбор решения будет основан на принципе «цена-качество». Компании, претендующие на роль подрядчика, должны

будут стать не только ИТ-консультантами, но и консультантами по бизнесу. Кроме того, важнейшими критериями станут совместимость новой системы с системами ИТ-инфраструктуры банка и получение положительного результата для бизнеса в целом. Именно поэтому компания «Инфосистемы Джет» при построении IdM-систем реализует ролевою модель доступа к информационным ресурсам, которая делает доступ более гибким, чем при мандатном и дискреционном принципах построения.

Если компании используют традиционный принцип (мандатная и дискреционная модель) организации доступа к ИС, то каждому сотруднику предоставляются уникальные права доступа. На практике часто наблюдается ситуация, когда новый сотрудник вынужден долго ждать окончания процесса согласования этих прав. Зачастую из-за нежелания терять собственное время на бюрократические проволочки, руководство компаний принимает решение о предоставлении сотруднику избыточного доступа к информации. В результате теряется время, растут операционные риски и расходы на администрирование.

Ролевая модель построения IdM-системы делает управление правами доступа более легким, контролируемым и безопасным. В нее закладываются несколько типовых профилей пользователей с целью присвоения одному сотруднику нескольких ролей. При этом крайне важен тот факт, что сотрудник обычно исполняет несколько функциональных ролей. В IdM-системе заложен модуль, позволяющий проанализировать и распознать взаимоисключающие роли, чтобы избежать дублирования полномочий сотрудника (принцип разделения полномочий — Segregation of Duties).

Например, в банке установлена некая HR-система, используемая для получения сведений о сотрудниках и рассматриваемая в качестве эталонной. При поступлении в HR-систему информации о новом сотруднике в IdM-системе автоматически создается новая запись, которая после необходимых согласований будет транслирована в управляемые системы. Соответственно все временные блокировки (например, при уходе со-

трудника в отпуск) и удаление учетной записи из IdM-системы будут производиться автоматически, как только сотрудники отдела кадров внесут необходимые изменения в HR-систему.

Внедрение IdM-системы в организации требует значительных средств, и чаще всего расходы ложатся на ИТ-бюджет. Но доказать целесообразность подобных вложений достаточно легко. Помимо качественной составляющей проекта, можно показать сроки окупаемости решения путем вычисления параметра ROI, в который входят такие показатели как: производительность Help Desk, уровень эффективности управления проектами, затраты на внешний аудит и т.д.

Функциональные возможности IdM-системы охватывают полный спектр потребностей в управлении доступом. Разработка такого решения — процесс трудоемкий и сложный, он требует от подрядчика знаний в области консалтинга, технического бэкграунда и опыта программных разработок.

На первом этапе внедрения необходимо разработать ролевою модель, которая в будущем даст возможность оперативно управлять доступом, и провести анализ бизнес-процессов банка, с целью выявления дальнейшей потребности сотрудников в доступе к информационным системам.

На втором этапе разрабатываются и формализуются процессы согласования предоставления

доступа сотрудников банка к ИС. Во многих компаниях этот процесс довольно сложен, так как включает в себя ветвления и возвраты. Зачастую подобные процессы не оптимизированы, например они не обеспечивают должного уровня ИБ или неоправданно трудоемки. Если сотрудник по требованию бизнеса наделяется дополнительными правами, которые отклоняются от принятой ролевой модели, то вопрос согласования прав доступа прорабатывается отдельно.

На третьем этапе производится автоматизация разработанных бизнес-процессов согласования и ролевой модели средствами внедряемого IdM-решения. Самый большой объем работ выполняется при подключении управляемых ИТ систем, связанных с программированием. Хотя большинство из них имеют стандартные коннекторы, участие программистов обязательно.

Выбрав в качестве основы для внедрения IdM-решения ролевою модель, заказчик в первую очередь заботится об обеспечении информационной безопасности внутри банка. Это значит, что такая модель поможет не только регламентировать разграничение прав доступа, но и разработать механизмы их изменений, например, при изменении бизнес-процессов банка. Переход к ролевой модели позволит значительно повысить эффективность бизнеса.

Oracle Identity Management – комплексные решения

Дмитрий Шепелявый,
руководитель технологического направления
по продуктам безопасности Oracle CHG

Существенную роль в обеспечении успеха проекта играет правильный выбор технологической платформы. Сейчас имеется 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. Решения в области Identity Management предлагают многие лидеры рынка ПО, такие как Oracle, Sun, IBM, Novell и другие. По информации аналитического агентства Gartner, лидирующее

положение здесь занимают решения Oracle Identity Management.

Высокие оценки аналитиков основаны в частности на том, что технологии Oracle способны обеспечить решение широкого спектра задач по управлению доступом к информационным ресурсам, а именно:

- централизованное управление механизмами безопасности на основе единой политики. При построении SOA-ориентированной архитектуры возможно применение единых механизмов безопасности для всего спектра приложений. Это существенно ускоряет соз-

дание интегрированной системы безопасности и снижает риски информационной безопасности за счет унификации механизмов защиты и контроля;

- поддержка всех основных платформ и бизнес-приложений (Oracle, Microsoft, SAP, Sun Microsystems, HP, IBM, Novell и др.) и проста интеграции с имеющимися приложениями на основе специального инструментария Oracle Adapter Factory, 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 предоставление необходимых полномочий до нескольких минут;
- возможность интеграции средств документооборота в имеющиеся системы, что позволяет интегрировать процессы управления безопасностью в имеющиеся процессы управления ИТ;
- контроль за соблюдением политики безопасности с использованием гибких средств аудита и отчетности, что позволяет удовлетворить требованиям руководящих документов в области информационной безопасности.

Также возможно построение интегрированной системы управления информационной безопасностью как в SOA-архитектуре, так и в среде унаследованных приложений.

Oracle уделяет большое внимание стратегическому развитию линейки Identity Management и ее интеграции с бизнес-приложениями. Основными стратегическими направлениями развития технологий являются следующие:

- предложение полного портфеля решений, т.е. спектр решений Oracle по управлению безопасностью уровня предприятия является наиболее полным на рынке;
- интеграция с бизнес-приложениями — решения Oracle Identity Management уже интегрированы с большинством бизнес-приложений и инфраструктурных решений (от Oracle,

SAP, Siebel, PeopleSoft, Microsoft, IBM, HP, Sun и др.). Использование технологии SOA, на базе которой развиваются решения Oracle Identity Manager, позволит интегрировать технологии безопасности в бизнес-приложения на уровне веб-сервисов, что резко сократит стоимость и сроки создания интегрированной системы управления безопасностью;

- ориентация на открытые стандарты — Oracle поддерживает и активно участвует в разработке практически всех стандартов управления безопасностью (OASIS, Liberty Alliance и др.).

Для банковских организаций особенно важно, что решения Oracle позволяют существенным образом облегчить выполнение требований стандарта Банка России СТО БР ИББС-1.0-2006, а также законодательства РФ по защите конфиденциальной информации, в частности, Закона «О персональных данных».

При реализации IdM-проектов важно не только владеть методологией внедрения IdM-систем, но и на профессиональном уровне разбираться в технологической составляющей проекта. Гарантией этого является подтверждение таких компетенций вендором, в частности — наличия у компании-интегратора статуса центра компетенции (ЦК) по данной технологии.

Статус ЦК по Oracle Fusion Middleware: Identity and Access Management является подтверждением высокого уровня экспертизы компании-интегратора. Наличие ЦК позволяет постоянно повышать профессионализм специалистов компании, отрабатывать сложные варианты реализаций и демонстрировать возможности различных решений.

В настоящий момент существует не так много компаний, которые бы сочетали три составляющие: опыт проектов по ИБ в банковских организациях, владение методологией и подтвержденную экспертизу. Одной из них является компания «Инфосистемы Джет», которая не только обладает статусом ЦК Oracle IdM, но и активно реализует IdM-проекты сразу в нескольких отраслях, в том числе и финансовой.

В компании «Инфосистемы Джет» за более чем полтора десятка лет работы накоплен большой опыт в различных направлениях ИТ. В этом номере Jet Info мы представляем новую рубрику «**Наши проекты**», в которой будем знакомить читателей с успешными проектами, реализованными нашими специалистами.

Построение сети нового поколения в Казахстане

АО «Казахтелеком» занимает лидирующее положение на телекоммуникационном рынке республики, имеет развитую сеть центров по предоставлению широкого спектра услуг связи: традиционная телефония и телеграф, передача данных и доступ в Интернет, интеллектуальные и спутниковые сети.

Клиентами компании являются свыше 2,7 млн физических и юридических лиц.

В качестве международного оператора АО «Казахтелеком» осуществляет тесное сотрудничество со 154 операторами дальнего зарубежья и 23 операторами стран СНГ и Балтии.

АО «Казахтелеком» сегодня — это бизнес-ориентированная компания, стабильность и высокая репутация которой ежегодно подтверждается аудиторами «большой четверки». Компания проводит активную работу по модернизации национальной информационной инфраструктуры, обеспечивает внедрение новых технологий и становление регионального рынка телекоммуникационных услуг, создание единого информационного пространства и усиление позиции Казахстана на международном рынке телекоммуникаций. Одновременно с работой над бизнес-проектами компания решает социальные задачи по телефонизации сельских населенных пунктов и подключению школ к сети Интернет.

Задачи проекта и их решение

Несмотря на стремительное развитие мобильной связи и широкие возможности сети Интернет, традиционным средством коммуникации все же остается стационарная телефонная связь. Ее наличие является необходимым условием успешной работы предприятий и организаций, существенно повышает комфортность повседневной бытовой жизни людей.

Недостатки технической базы, на которой работало АО «Казахтелеком», — морально устаревшее аналоговое оборудование, невозможность расширения каналов связи — привели к снижению качества предоставляемых услуг и жалобам со стороны абонентов. Кроме того, используемое оборудование и технологии не позволяли предоставлять новые услуги.

Перед АО «Казахтелеком» встала задача выбора такого решения, которое должно было учесть перспективы развития телефонной сети и в технологическом, и в техническом, и в территориальном плане. Это позволило бы компании сохранить абонентскую базу, а также предложить на рынок новые услуги связи и усилить свои конкурентные преимущества.

В качестве технологической платформы для новых услуг рассматривались варианты мо-

дернизации существующей сети, построенной по технологии TDM (с коммутацией каналов) или переход на новую технологию NGN (с коммутацией пакетов). Первый вариант предполагал покупку нового дополнительного оборудования или опции под каждую новую услугу. Поэтому в 2004г. руководство АО «Казахтелеком» приняло решение о развитии сети на основе IP-технологий. В 2006г. в рамках перевода сети телефонной связи на технологию VoIP в АО «Казахтелеком» приступили к реализации проекта по построению междугородней (МГ) сети NGN (Next Generation Networks) для объединения «Дальняя связь» и NGN-сети местной связи для ГЦТ «Алматытелеком».

Внедрение технологической платформы NGN позволяет расширить возможности традиционных фиксированных телефонных сетей. NGN представляет собой универсальную многоцелевую сеть, позволяющую «из одной розетки» предоставлять услуги по передаче речи, изображений и данных одновременно.

Компания Nortel выступила разработчиком проекта и поставщиком оборудования для построения NGN-сети АО «Казахтелеком». Работы по монтажу, установке, вводу в эксплуатацию, тестовые испытания и интеграция с существующей сетью были выполнены компанией «Инфосистемы Джет», имеющей партнерский статус Nortel Carrier VoIP Service and Solution Partner.

Прежде чем приступить к техническим работам по проекту, специалисты компании «Инфосистемы Джет» провели обследование 15 площадок в 10 областных центрах Казахстана, в которых предполагалось установить оборудование. Были собраны все исходные данные, учитывающие нюансы каждого установочного места.

Кроме того, специалисты компании консультировали АО «Казахтелеком» в вопросах разработки нормативной базы и организационных и административных регламентов при переходе на NGN-технологию.

Работы по построению NGN-сети в АО «Казахтелеком» включали в себя несколько фаз.

На первой фазе велись работы по построению NGN-сети в ГЦТ «Алматытелеком».

На второй фазе был проведен staging, т.е. подготовка к установке оборудования региональных транковых шлюзов. Начальная конфигурация оборудования была выполнена с учетом проектных решений для каждой конкретной площадки в регионах. Кроме того, специалисты компании «Инфосистемы Джет» провели все базовые тесты в соответствии с матрицей вызовов, которые рекомендует Nortel, а также эмуляцию

разных видов аварийных событий для проверки надежности системы.

На третьей фазе проводились монтажные и пусконаладочные работы программного коммутатора Nortel Communication Server 2000 Compact для управления междугородней NGN-сетью.

На четвертой – были инсталлированы и интегрированы 10 междугородних региональных транковых медиашлюзов Media Gateway 15000.

В Алматы на базе сети ГЦТ «Алматытелеком» был установлен программный коммутатор 5-го класса Nortel Communication Server 2000 Compact. Данный программный коммутатор (или софтсвитч) предназначен для управления сетью из пяти транковых шлюзов, подключенных ко всем транзитным АТС города, а также для управления оборудованием абонентского доступа. Алматинский софтсвитч был запущен в августе 2006г. В качестве транспорта для алматинского сегмента использовалась сеть Metro-Ethernet. На первом этапе общая емкость абонентских линий, подключенных к программному коммутатору CS 2000, составила 40000.

Междугородняя NGN-сеть объединяет 10 областных центров Республики Казахстан: Актобе, Атырау, Каменогорск, Караганды, Павлодар, Петропавловск, Тараз, Усть-Каменогорск, Талдыкорган, Шымкент.

Если раньше во всех городах трафик пропусклся через междугородние/международные цифровые телефонные станции, то в результате проекта была построена новая распределенная телефонная сеть с централизованным управлением. В каждом областном центре был установлен транковый шлюз операторского класса Media Gateway 15000. Управление сетью шлюзов осуществляет еще один программный коммутатор Nortel Communication Server 2000 Compact, установленный в г.Алматы. В качестве транспорта использовалась существующая магистральная сеть IP/MPLS, узлы которой есть в каждом областном центре страны. В результате этого проекта к NGN-сети было подключено более 30 телефонных сетей.

В рамках выполнения этих проектов специалисты компании «Инфосистемы Джет» протестировали взаимодействие и провели интеграцию с телекоммуникационным оборудованием других производителей (Lucent, Huawei, Iskratel, Teledata).

Для соответствия нормативным требованиям Республики Казахстан было специально разработано, интегрировано с программным коммутатором и протестировано решение по обеспечению оперативно-розыскных мер (COPM).

Результат

Внедрение технологии NGN привело к принципиальному улучшению качества междугородней связи. Основанная на IP-технологиях, NGN-сеть «Казахтелекома» увеличивает емкость междугородней сети за счет интеграции VoIP-коммутаторов и медиа-шлюзов с существующей коммутируемой телефонной сетью. Эта дополнительная емкость позволяет большему числу абонентов Казахстана совершать местные и междугородные звонки по коммутируемой телефонной сети.

Свое первое испытание NGN-сеть прошла под Новый год в момент максимальной нагрузки. В канун новогодних праздников, как правило, количество звонков становится избыточным, что вызывает перегрузку телефонной сети. Первый «живой» трафик по NGN-сети прошел в декабре 2006г. Она приняла на себя ту нагрузку, которую не могла выдержать существовавшая сеть, фактически повысился коэффициент удачных вызовов (ASR – Average Seizure Ratio). В результате большее число абонентов смогло дозвониться до родственников и друзей с первого раза.

Мониторинг, контроль и управление междугородней NGN-сетью осуществляется централизованно из г. Алматы. В результате этого:

- снизились затраты и повысилась оперативность внесения изменений в настройках: изменения, вносимые в одной точке, отражаются одновременно по всей стране, их не приходится осуществлять синхронно во всех областных центрах;

- существенно снизились простои сети из-за ошибок, их поиска и устранения;
- людские ресурсы, требуемые для обслуживания сети, сократились многократно, теперь нет необходимости в каждом областном центре иметь свои дежурные смены инженеров на каждой телефонной станции.

Благодаря внедрению NGN-сети абоненты устаревших аналоговых телефонных станций будут замещены шлюзами абонентского доступа, функционирующими в рамках NGN-сети. Это обеспечит АО «Казахтелеком» дополнительные экономические выгоды и позволит расширить спектр услуг, гарантируя высокое качество их предоставления.

В сетях NGN есть возможность реализовать полномасштабное предоставление услуг пакетной телефонии, голосовой и универсальной почты, IP-Centrex, телеобучения, VPN, передачи данных, видеоконференцсвязи и т.д.

Проект по построению сети нового поколения продолжается. Специалисты компании «Инфосистемы Джет» ведут работы в городах Алматы и Караганды.

Летом 2007г. была сдана в эксплуатацию NGN-сеть в г.Караганды. Уже на первом этапе к ней было подключено 10 тыс. абонентов.

Развивается проект NGN-сети в г.Алматы. АО «Казахтелком» закупил необходимое оборудование и программное обеспечение для подключения 70 тыс. абонентов.

Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

Издается с 1995 года

Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. (vlad@jet.msk.su)
Редактор: Лапина И.К. (lapina@jet.msk.su)
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su <http://www.jetinfo.ru>

Подписной индекс по каталогу Роспечати

32555

