Identity Management – решение типичных проблем

Тимур Мухаметгалеев,
руководитель департамента системной интеграции Amphora Group,
tmoukhametgaleev@aqt.ru
BYTE, №10 2005

Развитие современной организации неразрывно связано с внедрением новых технологий, в том числе и в ИТ. При этом, в каждый отдельно взятый момент времени внедряются ИТ-системы, необходимые для решения текущих актуальных задач, стоящих перед организацией. В результате в организации образуется большое количество разнородных ИТ-систем, достаточно слабо связанных друг с другом, а зачастую и не имеющих стандартных средств взаимодействия друг с другом – собственно, организация получает «лоскутное одеяло» из разнородных ИТ-систем. Явными признаками такого явления становятся избыточность и дублирование однотипной информации, хранящейся в разных ИТ-системах, ее противоречивость, и, наконец, наличие большого штата специалистов, основной задачей которых является поддержание этого массива информации в согласованном и актуальном состоянии. Особенно остро проблема «лоскутного одеяла» встает при разграничении доступа сотрудников к конфиденциальной информации в различных ИТ-системах.

ПРОБЛЕМАТИКА

В качестве примера подобной ситуации можно привести стандартную операцию по приему сотрудника в компанию. Попробуем перечислить все действия, которые необходимо выполнить ИТ-подразделению типичной организации после оформления сотрудника на работу в отделе кадров (рис.1):

Рис. 1. Необходимые шаги для включения нового сотрудника в работу

1. Новому сотруднику необходимо установить рабочее место (персональный компьютер). Эта задача обычно решается службой поддержки пользователя. При этом зачастую компьютеру присваивается ни с чем не связанное имя, первое, что придет на ум специалисту, выполняющему эту задачу;

2. Для нового сотрудника нужно завести почтовый ящик, а также учетные записи для входа в корпоративную сеть и доступа в Интернет. Обычно эти задачи являются зоной ответственности одного подразделения или сотрудника;
3. Необходимо создать учетные записи для сотрудника в других системах, которые используются сотрудником для выполнения своих прямых обязанностей, соблюдая при этом необходимые правила информационной безопасности. За администрирование каждой из этих систем обычно отвечают отдельные администраторы. Они обладают всеми необходимыми знаниями по сопровождению и поддержке этих систем, но при этом между собой практически не взаимодействуют. Часто в компаниях это приводит к тому, что полноценное включение нового сотрудника в работу может занимать более недели.

Необходимо отметить, что при следовании вышеизложенным путем возникает ряд проблем, связанных с жизнедеятельностью и ростом предприятия. В ходе развития компании заменяются старые и внедряются новые информационные системы (ИС). Помимо приема новых сотрудников в этих системах необходимо отражать увольнения и изменения статусов текущих сотрудников. В результате постепенно накапливается целый ворох проблем с актуализацией информации о сотруднике и его правах доступа в различных ИТ-системах, а также с согласованием всех данных о пользователе, хранящихся во всех источниках (рис.2). Перечислим основные из этих проблем:

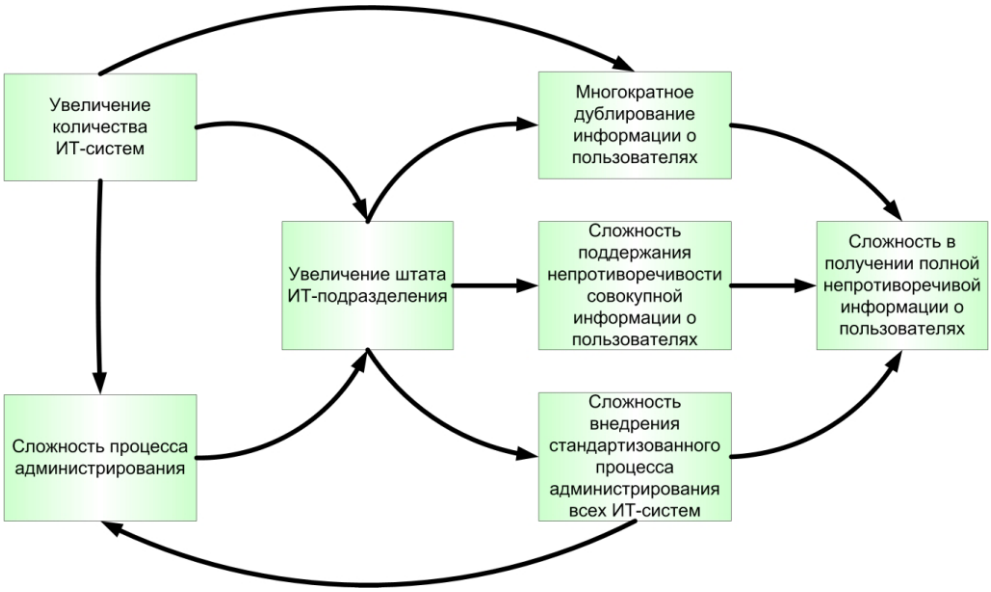

Рис. 2. Наиболее типичные проблемы актуализации данных о пользователях

Высокая сложность процесса АДМИНИСТРИРОВАНИЯ совокупной информации о пользователе. Сложность возникает по причине распределенности совокупной информации о пользователе по различным ИТ-системам – для того, чтобы собрать и увидеть полную картину по одному пользователю, необходимо проанализировать множество различных источников информации.

Компаниям приходится содержать большой ШТАТ сотрудников ИТ-подразделения, отвечающих за администрирование отдельных ИТ-систем. Одной из причин роста штата ИТ-подразделения является внедрение нового продукта без учета вопросов его органичной интеграции в существующую ИТ-инфраструктуру компании. С ростом организации все острее проявляется необходимость в наличии отдельных администраторов для каждой ИТ-системы, а это влечёт за собой несогласованность их действий и потерю информации при передаче от одной группы администраторов к другой.

Следствием большого количества администраторов становится **высокая сложность ВНЕДРЕНИЯ стандартизованного процесса администрирования всех эксплуатируемых ИТ-систем.** В такой ситуации крайне трудно заставить все это нагромождение систем работать как единый механизм. Приходится учитывать особенности администрирования различных систем, невозможность их прозрачной интеграции стандартными средствами и множество других факторов.

Другой проблемой становится **сложность в ПОДДЕРЖАНИИ непротиворечивости всей имеющейся информации о пользователе**, распределенной между различными ИТ-системами. Невозможно гарантировать согласованность и корректность этой информации, так как внесение изменений в одной из систем может остаться незамеченным для других систем.

Нередко встречается **многократное ДУБЛИРОВАНИЕ информации о пользователе** в различных источниках информации. Как правило, наиболее простым выходом является многократное дублирование одной и той же информации о пользователе в разных ИС.

Обычным явлением для крупных корпораций является **сложность в ПОЛУЧЕНИИ полной непротиворечивой информации о пользователе.** Довольно трудно организовать процесс сбора полной информации о пользователе, что соответственно приводит к появлению противоречивых сведений об одном и том же пользователе в различных ИС.

Стоит отметить, что все перечисленные проблемы сводятся к тому, что ***объёмы и разнообразие форм хранения информации возрастают, а существующие механизмы управления этой информацией уже не позволяют обеспечить её эффективное использование.***

Соответственно, перед ИТ-подразделением организации встаёт задача – разработать и внедрить в рамках организации единый инструмент управления информацией о пользователях ИТ-инфраструктуры. Данный инструмент должен обеспечивать следующие функции:

1) создание и внедрение единых политик управления идентификационными данными о пользователях (сотрудниках) компании (identity information);
2) поддержание политики управления identity information в актуальном состоянии;
3) создание единого корпоративного хранилища полной и непротиворечивой идентификационной информации о пользователях компании;
4) обеспечение простоты и прозрачности процедур приема/увольнения/изменения положения сотрудников в компании – как для сотрудников ИТ-подразделения, так и для руководства, а также обеспечение необходимого уровня конфиденциальности в компании;
5) подготовка базы для создания в организации единой точки входа, т.е. механизма управления именами пользователей, их паролями и правами доступа во всех ИТ-системах;
6) обеспечение масштабируемости решения как в отношении простого увеличения информационных систем, которыми оно оперирует, так и в отношении расширения перечня характеристик пользователя и усложнения правил работы с идентификационной информацией.

ПОДХОДЫ

Технических и организационных подходов для решения указанных проблем достаточно, однако необходимо учесть, что эта задача решается на живом организме информационной среды конкретной организации. Различные подходы можно разделить на несколько групп:

1. **Кардинальная перестройка ИТ-инфраструктуры** с внедрением единообразных ИТ-систем, имеющих стандартный интерфейс взаимодействия и не требующих глубоких настроек и программирования. Следствием такого решения является

полная перестройка ИТ-инфраструктуры, которая, в свою очередь, не гарантирует решение поставленной задачи в будущем;

2. **Написание собственных интерфейсов взаимодействия** между существующими компонентами ИТ-инфраструктуры. Такое решение позволяет сохранить существующую ИТ-инфраструктуру, однако не способно полностью решить задачу внедрения единых политик управления идентификационной информацией;
3. **Внедрение единого интеграционного решения**, которое обеспечит как предоставление полной идентификационной информации, так и внедрение единых политик управления этой информацией в различных компонентах ИТ-инфраструктуры, а также предоставит инструменты для удовлетворения всех остальных перечисленных требований. Такое решение позволит максимально сохранить имеющуюся информационную среду, обеспечит взаимодействие со всеми ИТ-компонентами для различных сценариев. Важной особенностью интеграционного решения является то, что оно должно быть предельно гибким и открытым для дальнейшего развития ИТ-инфраструктуры. Данный подход представляется наиболее рациональным как с точки зрения соотношения ресурсы/покрытие требований, так и с точки зрения перспектив масштабирования. Наиболее полная реализация описанного механизма возможна при внедрении систем класса Identity Management[1], именно о них и пойдет речь в этой статье.

КОМПОНЕНТЫ И ТОПОЛОГИЯ СИСТЕМ IDENTITY MANAGEMENT

Классическая система Identity Management состоит из следующих основных компонентов (рис.3).

Рис. 3. Архитектурная концептуальная схема классической системы Identity Management

MetaDirectory представляет собой единое корпоративное хранилище идентификационной информации. Данный компонент консолидирует всю информацию об объекте, собранную из различных источников, таких как каталоги, базы данных, файлы и т.д. Информация об объекте собирается из всех доступных источников (Система 1, Система 2, …, Система N), проходит преобразование в унифицированный и стандартизованный формат хранения, а также проходит проверку на достоверность, после чего сохраняется в MetaDirectory. Данный компонент не является открытой базой данных, а скорее служит репозиторием для системы Identity Management; доступ к информации из MetaDirectory можно получить через специализированный интерфейс управления или посредством справочника;

[1] Identity Management (IM) – управление идентификацией.

MetaDirectory должна обладать прикладным интерфейсом для общения со справочником и интерфейсом управления и предоставлять следующие сервисы:

- Агрегация всей информации об объекте учета в едином хранилище;
- Обеспечение единого унифицированного представления всей известной информации о каждом объекте учета.

Справочник является набором правил управления идентификационной информацией. Как уже отмечалось, помимо консолидации и обработки информации об объекте ИТ-инфраструктуры, решение Identity Management позволяет реализовать правила управления этой информацией в рамках всей организации. В качестве таких правил можно привести приём/увольнение сотрудника, изменение его служебного положения, а также любые формализуемые бизнес-правила, имеющие отношение к объектам учета, например, изменение паспортных данных сотрудника, членство в группе безопасности. Данный компонент берёт на себя выполнение всех необходимых действий, связанных как с изменением отображаемой в различных системах информацией об объекте, так и с изменением его прав доступа к другим сетевым и информационным ресурсам и пр. Также данный компонент позволяет формализовать и реализовать наиболее типичные профили таких объектов инфраструктуры как пользователи, группы, организационные подразделения и т.д.

Справочник предоставляет следующие сервисы:

- Выполнение правил обработки и распространения информации об объекте учета;
- Выполнение правил по консолидации и обработке информации;
- Снижение степени избыточности и исключение противоречивости информации, хранимой в различных ИТ-системах;
- Автоматическое создание новых объектов учета и удаление неактуальных объектов учета в подключенных ИТ-системах;
- Повышение эффективности администрирования информации.

Адаптеры (коннекторы)- это компоненты, реализующие передачу информации между MetaDirectory и подключенными системами. Они избавляют администратора IM-системы от необходимости каждый раз кодировать интерфейс доступа к ИТ-компоненте, в особенности при изменении ширины информационного потока между ИТ-компонентой и IM-системой.

Интерфейс управления представляет собой компонент, позволяющий осуществлять работу по настройке и администрированию системы Identity Management в интерактивном режиме. Обычно он тесно интегрирован как со Справочником, так и с MetaDirectory и предоставляет средства дальнейшей разработки системы в целом в интерактивном режиме и средства конфигурирования запуска системы IM в пакетном режиме.

КАК ВНЕДРИТЬ СИСТЕМУ УПРАВЛЕНИЯ ИДЕНТИФИКАЦИЕЙ?

Как и внедрение любой сложной инфраструктурной системы, построение системы Identity Management требует определенных затрат как со стороны внедренческой компании, так и со стороны заказчика. При этом подрядчик должен иметь необходимые знания в области IM, иметь успешный опыт в построении подобных систем.

Зачастую внедрение подобных систем совмещают с модернизацией инфраструктуры организации – например, переход с доменов Windows NT 4.0, Windows 2000 и одноранговых сетей к единому лесу Active Directory 2003, внедрение новых систем доступа в Интернет и т.д. Само по себе совмещение – нормальное явление, т.к. часто приходится решать целый комплекс проблем заказчика. Однако распараллеливание работ по внедрению системы IM и работ по модернизации инфраструктуры Заказчика является уже недопустимым, так как система IM опирается в своем функционировании на базовую

сложившуюся и надежную инфраструктуру заказчика. Строить систему IM на неизвестной базе нецелесообразно, так как впоследствии в силу реорганизации базовой инфраструктуры придется пересматривать большинство сделанных предположений и реализованных алгоритмов, что приведет к дублированию работ, перерасходу времени и средств заказчика и, как следствие, к неудовлетворенности заказчика результатом.

Кроме того, реорганизация базовой инфраструктуры сама по себе содержит массу рисков, таких как неприятие проекта новой инфраструктуры ключевыми сотрудниками, неудовлетворительные результаты испытаний новой инфраструктуры, проблемы организационного плана, проблемы с поставкой аппаратной платформы и т.д. Это же справедливо по отношению к процессу внедрения системы IM – данный процесс достаточно сильно затрагивает интересы ключевых сотрудников Заказчика, отвечающих за вопросы администрирования имеющихся информационных систем и инфраструктурных решений. В каждой организации помимо всех вышеперечисленных аспектов существует еще целая когорта специфичных именно для этой организации проблем.

Исходя из всего перечисленного, напрашивается вывод о желательном разнесении по времени этапов модернизации существующей инфраструктуры и процесса внедрения системы IM. При этом проектирование новой инфраструктуры и системы IM может идти параллельно, как и их отработка на тестовом стенде.

Опираясь на мировой опыт внедрения сложных информационных систем, можно выделить следующие классические фазы построению систем IM (рис.4)*:*

Рис.4 Этапы построения систем Identity Management

Анализ требований – на данном этапе анализируется текущая практика работы организации, выявляются требования ключевых заинтересованных сторон в отношении системы IM. Результаты данного этапа должны быть оформлены в виде документа, содержащего основные функциональные и нефункциональные требования к системе IM включая основные сценарии работы.

Проектирование системы – с учетом сложившейся инфраструктуры или спроектированной и одобренной Заказчиком инфраструктуры выполняется эскизное и детальное проектирование системы IM. Обычно результаты этого этапа оформляются в виде документа, отражающего основные концептуальные предположения и технического задания на реализацию системы IM. Также на данном этапе должны быть формализованы тестовые испытания, включая методику их проведения и параметры тестового стенда.

Реализация и отработка на тестовом стенде с проведением тестовых испытаний, имитирующих работу будущей системы в наиболее типичных и экстремальных условиях, характерных для данной организации. Результатом работ данного этапа является реализованная система IM, удовлетворяющая всем изложенным в соответствующих документах требованиям, а также успешно прошедшая тестовые испытания.

Внедрение системы – на данном этапе происходит внедрение спроектированной и разработанной системы в продуктивную среду организации с проведением опытной эксплуатации и приемо-сдаточных испытаний. После успешной опытной эксплуатации и приемо-сдаточных испытаний система может быть переведена в промышленную эксплуатацию.

Для процесса внедрения системы IM характерны определённые особенности, от учёта которых зависит успех всего процесса построения системы IM в целом. Особенности начинаются на первом же этапе – требуется глубокое изучение всех информационных систем, вовлеченных в процесс функционирования системы IM. На этом этапе необходимо выявить и описать все атрибуты учетной информации по объекту, выявить специфику процессов рутинного администрирования ИС.

На втором этапе необходимо грамотно спроектировать систему и ответить на основные вопросы:

- Необходимы ли процедуры синхронизации паролей?
- Достаточны ли схемы информационных систем для включения их в процесс identity management или требуется расширить эти схемы?
- Возможно ли однозначно связать характеристики одного объекта в разных системах с использованием формализованных правил и критериев?
- Какая информация должна обрабатываться системой – ее охват, основные процессы обработки этой информации?
- Необходимо ли реализовывать отображение организационно-штатной структуры предприятия в инфраструктуру организации?

Кроме того, следует определить приоритеты подключаемых систем при изменении одной и той же информации об одном и том же объекте, а также форматы взаимодействия системы IM с подключаемыми информационными системами. На этом же этапе необходимо сделать выбор базовой платформы для построения системы IM, если таковая не обговорена заранее Заказчиком.

На этапе реализации необходимо в первую очередь наполнить MetaDirectory данными из кадровой системы; при этом часть атрибутов в MetaDirectory останется незаполненной и будет определена позже. Далее, не стоит подключать все системы сразу – отлаживать взаимодействие всей системы IM лучше поэтапно. Также на данном этапе стоит провести предварительное связывание – процедуру, в рамках которой устанавливаются однозначные соответствия между учетной информацией объектов в различных информационных системах и в MetaDirectory. Выполнение этой процедуры с полной имитацией всех подключаемых ИС позволит выявить все проблемные случаи и начать работу по их устранению. Тем не менее, не стоит рассчитывать, что в автоматическом режиме свяжутся все объекты во всех подключаемых информационных системах – необходимость ручного связывания, скорее всего, будет, дело лишь в том, что вы получите информацию, по которой можно вручную связать объекты.

На этапе внедрения также необходимо четко структурировать выполняемые действия – сначала развертывание базовой платформы, далее подключение кадровой системы и создание в MetaDirectory базовой информации об объектах, затем постепенное подключение каждой новой системы. После подключения всех систем необходимо провести первоначальное связывание (как автоматическое, так и ручное), а затем, убедившись в корректности выполненных действий, можно переключаться на отслеживание всех изменений по объектам учета.

Инструменты по управлению идентификацией *различаются весьма сильно как по функционалу, так и по сложности внедрения и даже способу лицезирования. Минимальным требованиям по управлению паролями могут удовлетворить достаточно простые системы вроде v-GO SSO от фирмы Passlogix или Neusine от Castle Systems.*

Такие решения обеспечивают единую точку входа в информационные системы предприятия, управление пользователями, коррекцию паролей и некоторые другие функции.

Более масштабные продукты, такие как MIIS 2003 (Microsoft), Tivoli Identity Manager (IBM), Identity Manager (Sun), eDirectory (Novell), обладающие развитым функционалом, предоставляют пользователям более впечатляющие возможности автоматизации. Такие системы оснащены исчерпывающим набором функций аутентификации и контроля доступа в крупных корпоративных сетях, способны увеличивать масштаб до миллиарда (и более) объектов, поддерживают широкий диапазон корпоративных приложений, а также обладают мощными инструментами аудита и мониторинга.

ПРИМЕР ВНЕДРЕНИЯ СИСТЕМЫ IM

Российская практика внедрения системы IM пока не богата примерами и представлена единственным масштабным проектом в ОАО «Аэрофлот – Российские Авиалинии».

В компании «Аэрофлот» возникла потребность в реорганизации существующей ИТ-инфраструктуры, включая перестроение процесса управления всеми элементами этой инфраструктуры. Ситуация была хрестоматийной – наличие большого количества разнородных ИС как прикладного, так и системного назначения; большое количество сотрудников, распределенных по различным офисам. Средний сотрудник использует в своей работе не менее 5-7 разнородных информационных систем, для администрирования которых существовали отдельные группы администраторов, достаточно слабо связанные друг с другом. Основные из этих систем и были выбраны для реализации проекта по внедрению IM: кадровый модуль, почтовая система, внутренняя система на базе Lotus Domino, система доступа в Интернет, а также новая Active Directory 2003 (была развернута взамен старой инфраструктуры).

На первом этапе был проведен всесторонний анализ текущей ситуации, а также были обобщены требования к результатам проектных работ. Так как была поставлена дополнительная задача модернизировать существующую Windows-инфраструктуру до уровня Active Directory 2003 и осуществить миграцию пользователей, рабочих станций и серверов в новую инфраструктуру, то проект включал в себя две задачи (модернизация + миграция и внедрение IM) и работы выполнялись по обоим направлениям. Заказчику была представлена вся разработанная документация с описанием его текущей инфраструктуры, а также сформулированные требования к результатам проектных работ, включая требования к аппаратному обеспечению.

На втором этапе выполнялось проектирование новой инфраструктуры, процедуры миграции и проектирование детального дизайна системы IM. На этом этапе были смоделированы и формализованы форматы взаимодействия системы IM и подключаемых информационных систем. В качестве базовой платформы было предложено использовать продукт Microsoft Identity Integration Server 2003, так как функционал этого продукта точно соответствовал требованиям заказчика, а наличие специальных интерфейсов (Management Agents) обеспечивали наиболее удобную интеграцию с компонентами сложившейся инфраструры.

Microsoft Identity Integration Server 2003 *(MIIS 2003) – это одна из последних версий пакета Microsoft Metadirectory Services, (разработки этого пакета начались ещё в 1989 году фирмой Zoomit, а в 1999 г. компания была куплена корпорацией Microsoft). Сегодня*

MIIS представляет собой гибкую среду для поддержания идентичности и синхронизации учетных данных на предприятии. Обеспечивая согласованность учетных данных в разных хранилищах, MIIS 2003 упрощает разработку, внедрение и эксплуатацию метакаталога для организаций любого размера, а также создает удобное представление учетных данных в используемых информационных системах. Система позволяет уменьшить трудоемкость исполнения текущих задач по администрированию учетных записей, за счет чего уменьшается вероятность ошибок и снижается возможность рассогласования настроек учетных записей, а значит, уменьшаются предпосылки к возникновению инцидентов с безопасностью.

В ходе третьего этапа на тестовом стенде, максимально точно повторяющем конфигурацию новой Windows-инфраструктуры и типичных рабочих станций, была развернута новая инфраструктура и базовая платформа для системы IM, а также установлены тестовые образцы реальных информационных систем. В течение этого же этапа проводились итерации по первоначальному связыванию, а также была разработана и оттестирована процедура синхронизации паролей между всеми системами, подключенными к MIIS 2003.

Этап внедрения повторял все итерации третьего этапа, но уже применительно к продуктивной среде. На заключительной стадии были включены правила для отслеживания изменений идентификационной информации во всех подключенных системах, после чего проект был успешно завершён.

Новая инфраструктура отличается высокой степенью централизации, надежности, устойчивостью к попыткам несанкционированного доступа и возможностью масштабирования под нужды «Аэрофлота». По мнению экспертов, новые возможности позволят «Аэрофлоту» заметно увеличить эффективность использования существующих информационных ресурсов, в частности повысить управляемость инфраструктуры и прозрачность протекающих в ней процессов. Автоматизация рутинных операций позволит высвободить квалифицированные кадры для решения более важных для компании задач в сфере управления ИТ-инфраструктурой и обеспечения необходимого уровня информационной безопасности. Кроме того, внедрение единых продуманных правил управления информацией о пользователях и их правах в эксплуатируемых ИТ-системах позволит уменьшить риск получения несанкционированного доступа к информации или риск получения завышенных прав доступа к конфиденциальной информации.

****

Мировой опыт показывает, что системы IM в рамках организации позволяют решить вопросы эффективного управления идентификационной объектной информацией (identity information) в условиях увеличения размеров организации, растущего количества ИТ-компонент и объема хранящейся информации. Будучи важным звеном в деле построения надежной системы управления ИТ, включая обеспечение необходимого уровня информационной безопасности, система IM позволяет реализовать внутренние стандарты и бизнес-правила организации по управлению всей пользовательской информацией и распределению необходимых категорий доступа к корпоративной информации. Это, в свою очередь, даёт возможность автоматизировать рутинные операции по администрированию, облегчить и увеличить прозрачность процесса администрирования в целом за счет предоставления достоверной и максимально полной информации о каждом объекте. Система IM также предоставляет возможность высокоуровневого управления и мониторинга всей массы пользовательской информации из одной точки, что также является достаточно важным аргументом для внедрения подобных систем.