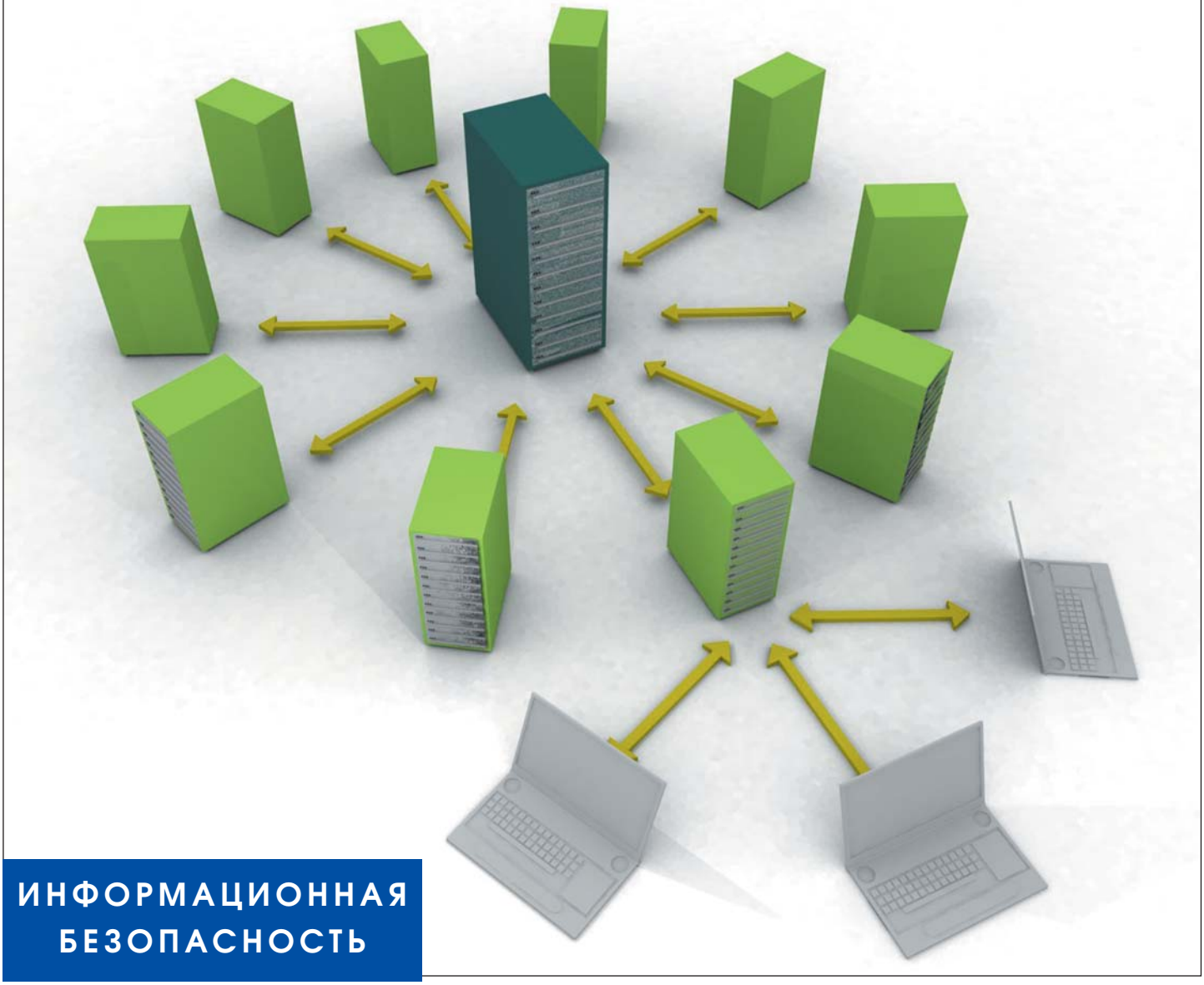
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 5 (203)/2010

Identity Management: централизованное управление доступом



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года

Редакция:

Дмитриев В.Ю.
vlad@jet.msk.su

Некрасова Н.А.
nekrasova@jet.msk.su

Слободчикова Т.А.
slobodchikova@jet.msk.su

Шедова Е.Л.
eshedova@jet.msk.su

Верстка:
Кулешова Ю.В.

Корректура:
Андрушко О.Ю.

Над номером работали:
Андронов С.Ю.
Ляпунов И.В.
Петрухин В.С.
Чередникова Ю.В.

Издатель:
Компания «Инфосистемы Джет»

Контакты:
тел. (495) 411 76 01
http://www.jetinfo.ru

От редакции

Все мы с нетерпением ждем прихода лета, жары, солнечных улыбок.. Наши темы, как и настроения погоды, становятся жарче, ярче, колоритнее. Сегодня в центре нашего внимания Identity Management (IdM), проблематика которого настолько «острая» и «вкусная», как и жгучесть перчиков чили, попробовав которую хоть раз — уже невозможно отказаться. По мнению экспертов данное направление весьма перспективно и быстро прогрессирует. Через несколько лет, как сказал один из руководителей по безопасности крупного банка, IdM-система будет практически такой же обязательной, как сейчас корпоративные каталоги и Active Directory.

При всей юности подхода IdM современным крупным компаниям уже сегодня очень тяжело обходиться без средств управления правами доступа к информационным ресурсам. Ведь информация — одна из самых дорогостоящих и ценных вещей в нашем мире. Она может как спасти, так и утянуть на дно того, кто с ней недостаточно бережно обращался. Недаром риски, связанные с управлением доступом к информации, всегда входят в пятерку наиболее критичных.

В этом номере мы постараемся уберечь вас от «солнечных ожогов» — ошибок IdM-проектов, обозначив наиболее верные, с точки зрения участников рынка, пути реализации проектов, рассказав о предложениях ведущих вендоров и статьях доходов, возвращающих инвестиции. Экспертным мнением по данному вопросу с нами поделился Степан Масленников, директор департамента бизнес-информации и службы заказчика компании ТНК-ВР.

Но и это еще не все! Новый сезон — новые рубрики! «О чем молчат проектировщики»....Теперь и у Вас появилась возможность узнать самые интересные секреты рынка ИТ.

И на десерт (какое же лето без сочных десертов) — в гостях у рубрики «Собеседник» Игорь Ляпунов, директор центра информационной безопасности компании «Инфосистемы Джет». Разговор пойдет об итогах прошедшего года Центра.

Удачных Вам проектов и отпусков!

С уважением, редакция JI

СОДЕРЖАНИЕ

Компания «Инфосистемы Джет» провела аудит сети передачи данных компании «Ростик'с-KFC»

Компания «Ростик'с-KFC» приняла решение о проведении модернизации сети после выхода из состава холдинга «Росинтер». Зачастую в подобных проектах логичным и важным этапом является проведение аудита. В качестве исполнителя по итогам тендера была выбрана компания «Инфосистемы Джет».

Алексей Догаев, руководитель Центра сетевых решений компании «Инфосистемы Джет», пояснил: «*Аудит — очень важный этап в «жизни» любой сети, претерпевшей не одно изменение. Подробные сведения, которые мы собрали в ходе аудита, помогут не упустить ни одной детали, что дает нам возможность предлагать заказчику наиболее эффективное решение по оптимизации и модернизации сети».*

В ходе аудита была обследована структура СПД в 70-ти ресторанах и дополнительных офисах компании. На основе полученных данных специалисты компании «Инфосистемы Джет» разработали концепцию развития СПД, которая будет использована при проведении модернизации. Провели полное обследование и инвентаризацию оборудования и ПО, составили детальную топологическую схему сети, получили подробные данные об используемых адресных пространствах. Также была проведена экспертная оценка организации сети и предоставлены рекомендации по ее оптимизации — для каждого объекта даны описания по тому, что необходимо сделать: докупить или заменить оборудование, произвести дополнительные настройки и т.д.

«От надежной работы ИТ-систем, включая корпоративную сеть, очень сильно зависит множество бизнес-процессов компании (работа бухгалтерии, логистики и т.д.), а значит и успех нашего бизнеса, — рассказал **Андрей Гордеев, директор по ИТ компании «Ростик'с-KFC».** — *Благодаря проведенному аудиту и рекомендациям по развитию сети мы оптимизируем корпоративную сеть и каналы передачи данных. У нас появится быстрая и надежная связь со всеми филиалами, что позволит нам в будущем безболезненно наращивать мощности вместе с ростом нашего бизнеса».*

«СКБ-Банк» получил комплексную мультивендорную поддержку ИТ-инфраструктуры

Новый контракт на техническую поддержку high-end серверов IBM дополняет перечень обслуживаемого оборудования и позволит усовершенствовать обслуживание ИТ-инфраструктуры Банка в целом.

В рамках недавно заключенного 3-х-летнего контракта специалисты компании-интегратора взяли на обслуживание high-end серверы IBM Power. Теперь на обслуживании Сервисного центра компании «Инфосистемы Джет» находится практически вся ИТ-инфраструктура Банка.

Компания «Инфосистемы Джет» уже оказывает банку услуги технической поддержки решений Sun Microsystems, Hitachi Data Systems, Brocade, Symantec, Oracle и других вендоров. В связи с ростом бизнеса банка в состав ИТ-инфраструктуры были включены high-end серверы IBM. Помимо услуг технической поддержки базового уровня на серверы IBM p595 и p570 контракт включает высокоуровневые услуги компании «Инфосистемы Джет» по комплексной поддержке систем. Их суть — в обеспечении работоспособности всей вычислительной системы заказчика и

решении проблем «на стыках» при функционировании систем IBM в гетерогенной ИТ-среде банка.

«Мы получили уверенность в том, что техническая поддержка наших ИТ-систем будет выполняться на самом высоком уровне — это чрезвычайно важно для бизнеса современного активно развивающегося банка, — комментирует **Александр Клепинин, начальник Управления системной инфраструктуры, Департамент ИТ СКБ-Банка**. — *Делать такие прогнозы нам позволяют уверенность в компетенции и доверие к специалистам Сервисного центра компании «Инфосистемы Джет», с которой мы давно и плодотворно сотрудничаем. Отмечу, что залогом успеха сервисных проектов во многом является взаимное понимание и доверие сторон».*

«Нередко выход из строя одного элемента или подсистемы оказывает негативное влияние на работу других систем. Поэтому для успешного функционирования сложной ИТ-инфраструктуры важно, чтобы все системы обслуживались комплексно, а уровень сервиса для всех инфраструктурных подсистем, обеспечивающих функционирование приложений, был согласованным и соответствовал уровню их критичности для бизнеса», — рассказывает **Дмитрий Никитин, директор по продажам филиала компании «Инфосистемы Джет»** в Екатеринбурге.

«Абсолютная» интернет-безопасность

В Абсолют Банке успешно завершен первый год эксплуатации самой крупной в России корпоративной системы управления доступом в Интернет, построенной на базе технологий Blue Coat. В настоящее время система обеспечивает полный контроль над доступом в Интернет и требует минимум усилий при эксплуатации. Это первое в России внедрение, которое одновременно использует преимущества WAN-оптимизации и централизованного управления политиками контроля использования Интернет.

«Это самый крупный на настоящий момент в России проект, реализованный на базе решений Blue Coat, — говорит **Кирилл Викторов, заместитель директора по развитию бизнеса компании «Инфосистемы Джет»,** — *и мне особенно приятно, что Абсолют Банк доверил его реализацию именно нам. Полученная в этом проекте компетенция позволяет нашей компании занимать лидирующее место среди интеграторов, способных построить безопасный корпоративный доступ в Интернет для крупнейших российских компаний».*

Руководство банка всегда следовало стратегии укрупнения бизнеса, благодаря чему организация заметно выросла количественно и качественно. Увеличилось число клиентов и предлагаемых услуг, вырос штат сотрудников. Система информационной безопасности банка не поспевала за бурными темпами его роста — требовалась модернизация. Поскольку соединение с внешним миром — наиболее критичный канал коммуникации, первым шагом в этом направлении стала организация безопасного доступа в Интернет.

Для решения поставленной задачи служба информационной безопасности банка обратилась в компанию «Инфосистемы Джет», с которой уже имела опыт успешного сотрудничества (более 20 проектов, в том числе по модернизации ЦОД и построению DLP-системы). Проведя анализ требований заказчика, специалисты Центра информационной безопасности компании «Инфосистемы Джет» предложили внедрить решение нового для российского рынка, но весьма популярного в мире вендора — Blue Coat: Blue Coat Proxy SG, Blue Coat Proxy AV, Reporter и Director.

Программно-аппаратный комплекс Blue Coat функционирует в головном офисе и во всех филиалах Абсолют Банка. Он представляет собой единое, централизованно управляемое решение по разделению доступа в Интернет и построению своевременной отчетности. Кроме выполнения основных задач реализация проекта позволила улучшить сетевую инфраструктуру банка и достичь соответствия требованиям информационной безопасности. Единая консоль управления всем комплексом в сочетании с гибкой системой построения правил обработки контента дают возможность минимизировать потребности в численности инженерного состава, обслуживающего данное решение.

В настоящее время комплекс выполняет функции, далеко выходящие за рамки «классического» прокси-сервера с функциями контроля трафика и пользовательской активности.

Microsoft SQL Server 2008 R2: новый подход к управлению информацией

Компания Microsoft анонсировала выход Microsoft SQL Server 2008 R2 — платформы для управления, доступа и предоставления информации. Ключевые новшества нового Microsoft SQL Server 2008 R2 включают:

- Инструменты персональной бизнес-аналитики для подготовки отчетов и анализа;
- Высокую надежность и максимальную производительность СУБД и оборудования.

Microsoft SQL Server 2008 R2 предлагает новые мощные инструменты для персональной бизнес-аналитики, расширяющие возможности привычных для аналитиков инструментов Microsoft Excel 2010 и Microsoft SharePoint Server 2010. Модуль Power Pivot, который устанавливается как настройка для Microsoft Office Excel, позволяет загружать в Excel данные из любых внешних источников (ERP, CRM и других информационных систем), а также из собственных электронных таблиц. Пользователь может в удобном для него интерфейсе сам описывать эти данные в бизнес-терминах, задавать связи между ними, добавлять собственную информацию, формулы для расчета и т.д. Таким образом, сокращается не только время создания аналитических отчетов, но и стоимость самого BI-решения, так как не требуется дополнительное программирование и помощь ИТ-специалистов.

Microsoft SQL Server 2008 R2 в сочетании с Windows Server 2008 R2 помогает заказчикам запускать базы данных на системах до 256 логических процессоров и переходить в виртуализированные дата-центры. Таким образом, заказчики могут легко мигрировать в инфраструктуру частного облака, которое более доступно, консолидировано и виртуализировано и предоставляется по требованию.

Экспертное мнение

Дмитрий Зыкин, заместитель руководителя группы технической поддержки продаж компании «Инфосистемы Джет»:

«Появление в Microsoft SQL Server 2008 R2 возможности поддержки до 256 логических процессоров является огромным плюсом, поскольку позволяет значительно масштабировать имеющиеся БД без высоко рисковых процедур миграции на новую платформу. Кроме того, в новой версии появилась поддержка хранилищ свыше 100 TB, а также серьезные улучшения в BI-составляющей продукта. Это – StreamInsight (комплексная обработка событий – анализ потоков данных на лету в масштабе времени, близком к реальному), Master Data Services (централизованное управление нормативно-справочной информацией (измерениями) в масштабах всего предприятия), Self-service analysis (PowerPivot – In-memory OLAP, анализ по требованию на уровне бизнес-пользователя). Новые возможности Microsoft SQL Server 2008 R2 являются существенными и важными доработками предыдущих версий продукта».

Материал подготовлен по информации компании Microsoft

IBM помогает клиентам упрощать их ИТ-инфраструктуры

Корпорация IBM анонсировала новые продукты и услуги, разработанные с целью упростить для клиентов процесс управления их ИТ-средами путем предоставления специализированных возможностей, связанных с облачными вычислениями, интеграцией и масштабируемостью. В числе анонсированных предложений представлены три новых оптимизированных устройства, которые позволят клиентам расширить и усилить базовые технологии, формирующие основу для поддержки сегодняшней цифровой экономики.

Новые продукты IBM WebSphere Appliances представляют собой легкие в установке специализированные сетевые устройства, которые помогают упростить, улучшить безопасность и ускорить развертывание XML- и Web-сервисов клиентов.

Среди них:

- **WebSphere DataPower Integration Blade XI50B** – эти простые в развертывании сетевые устройства, теперь доступные на системах IBM BladeCenter, призваны решить проблему дорогостоящей и традиционно сложной «двухточечной» (point-to-point) интеграции.
- **WebSphere DataPower XC10** – новое устройство, которое расширяет возможности клиентов по экономически эффективному повышению производительности приложений с помощью режима «drop-in cache».
- **WebSphere Cloudburst Appliance** – версия устройства, которая улучшает возможности клиентов по созданию, развертыванию и управлению средами WebSphere в средах облачных вычислений; теперь поддерживаются и среды, требуемые для автоматизации бизнес-процессов и сервисов, связанные с планированием, координацией и управлением.

Новые решения дополняют пакет продуктов и услуг компании Cast Iron Systems, который включен в портфель предложений IBM. Такая комбинация технологий расширит возможности

IBM в полнофункциональных платформах для интеграции облачных приложений от таких поставщиков как Salesforce.com, Amazon, NetSuite и ADP с традиционными бизнес-приложениями от таких поставщиков как SAP и JD Edwards. Использование решений Cast Iron Systems с сотнями встроенных шаблонов в сочетании с ее профессиональными услугами даст клиентам возможность отказаться от заказного программирования в рамках интеграционных проектов и позволит выполнять интеграцию cloud-приложений за дни, а не за недели или месяцы. Таких результатов можно достичь с помощью физического устройства, виртуального устройства или сервиса облачных вычислений.

Материал подготовлен по информации корпорации IBM

NetApp приобретает компанию Bycast Inc.

Компания NetApp объявила о подписании соглашения о приобретении частной компании Bycast Inc.

Компания Bycast — один из основных разработчиков программного обеспечения хранения объектов для организации глобальных распределенных хранилищ общим объемом в несколько петабайт. Данные хранилища предназначены для изображений, видеофильмов и других записей. Решения Bycast созданы для крупных компаний и поставщиков услуг.

Bycast расширяет стратегию унифицированных систем хранения данных NetApp и дополняет решение для инфраструктуры хранения коллективного пользования новыми возможностями глобального доступа к данным и мобильности. С добавлением продукции Bycast, NetApp может предложить своим крупным корпоративным заказчикам и партнерам из числа поставщиков услуг дополнительное решение, позволяющее им эффективно осуществлять создание и управление глобальными хранилищами данных особо крупного масштаба, которые являются важнейшей частью многих предложений «ИТ как услуга».

Например, компания, работающая в издательском бизнесе, может при помощи системы хранения объектов обеспечить своим дизайнерам, которые находятся в разных точках земного шара, одновременный доступ к данным и совместную работу над проектами. Интерфейсы систем хранения объектов значительно упрощают администрирование этих систем. Приобретение компании Bycast позволяет NetApp расширять свои возможности в части работы на ряде важнейших вертикальных рынках, таких как цифровые медиа, Web 2.0, здравоохранение и поставщики услуг облачных систем. Кроме того, оно поможет заказчикам добиться еще большей эффективности работы ЦОД по всему миру.

Экспертное мнение

Дмитрий Зыкин, заместитель руководителя группы технической поддержки продаж компании «Инфосистемы Джет»:

«Одним из интересных и инновационных моментов этого решения является система хранения объектов. Это новый метод хранения и доступа к данным, основанный на именах объектов и подробных метаданных, описывающих свойства контента. Он упрощает задачу хранения большого числа объектов и ускоряет их поиск.

Сегмент заказчиков, которым требуется петабайтное распределенное хранение данных, достаточно узок. Решение не для массового рынка. Возможно, что в России и есть пара-тройка заказчиков, имеющих подобные задачи, но в целом это решение для европейского и американского рынка».

Материал подготовлен по информации компании NetApp

СТАТИСТИКА

Рынок решений Identity Management

По оценкам компании Gartner, ведущего американского консалтингового и исследовательского агентства, маржинальность мирового рынка Identity Management в 2009 году выросла на 15,5% и в настоящее время его стоимость оценивается приблизительно в $900 млн.

Identity Management как направление сейчас переходит в стадию зрелости со строго очерченными наборами продуктов и сформировавшимися вендорами. В настоящее время решения IdM большинства вендоров представлены третьим поколением продуктов, в котором базовая функциональность хорошо сконфигурирована. По данным Gartner по состоянию на середину 2009 года от 25 до 30% средних и крупных организаций по всему миру уже внедрили у себя ту или иную форму подхода Identity Management, а еще от 20 до 25% в настоящее время рассматривают такую возможность.

Нужно сказать, что методы планирования проектов Identity Management стали более структурированы и формализованы, уменьшилось количество ошибок при их реализации по сравнению с предыдущими годами, но в целом все это еще находится на стадии развития. Большинство неудач IdM-проектов является следствием неправильного планирования и определения объема проекта на его самой начальной стадии. Заказчики, запускающие IdM-инициативы, должны потратить значительные усилия на определение и приоритезацию своих специфических целей, преследуемых внедрением IdM-системы. И поскольку решений Identity Management, которые бы «из коробки» подошли любому заказчику, не существует, то важность перечисленных ниже факторов будет меняться в зависимости от организации и целей внедрения IdM.

Анализ решений, представленных на рынке

Стоит отметить, что базовая функциональность приблизительно одинакова для большинства вендоров IdM-решений: среда выполнения процессов (workflow engine), процессы согласования предоставления и изменения доступа, управление паролями и набор «стандартных коннекторов». Именно поэтому основные различия продуктов связаны с добавлением таких функциональных возможностей как:

- Управление жизненным циклом ролей;
- Интеграция среды управления бизнес-процессами (business process management — BPM);
- Реализация разделения полномочий (segregation of duties — SoD), анализа на наличие рисков и управления привилегиями в соот-

ветствии с подходом governance, risk management and compliance — GRC;
- Периодическая проверка неизбыточности полномочий;
- Историческая отчетность;
- Интеграция с системами безопасности, например с системами предотвращения утечек (data loss prevention — DLP), системами мониторинга (security information and event management — SIEM) и другими.

Тем самым вендоры стремятся привлечь новых заказчиков за счет создания универсального средства Identity Management, включающего все необходимые функции решений этого класса.

Масштабные проекты по направлению Identity Management были и остаются комплексными проектами, требующими участия опытных интеграторов и проектных команд. С учетом относительного функционального паритета программного обеспечения разных вендоров, данный критерий становится наиболее значимым для успеха проекта.

Заказчику необходимо понимать ключевые факторы, влияющие на выбор решения Identity Management одного из вендоров, которые включают, но не ограничиваются следующим:
- Поддержка современных стандартов доставки идентификационной информации;
- «Гибкость» ценообразования, включая стоимость внедрения и обслуживания;
- Сертификация решения государственными или отраслевыми регуляторами в качестве средства защиты информации;
- Партнерские отношения с системными интеграторами, у которых есть положительный опыт внедрения данных решений;
- Качество услуг интегратора, которое остается жизненно необходимым для успеха проекта;
- Возможность реализации некоторых требований, выходящих за рамки базовой функциональности продуктов, таких как:
  - Интеграция IdM с другими продуктами;
  - Дополнительная разработка нужного функционала;
  - Расширения функционала смежными решениями, например, решениями однократной аутентификации (Single Sign-On — SSO), управления жизненным циклом ролей (role life cycle management) и т.д.
- Наличие у интегратора и вендора успешных проектов в предметной области заказчика.

Знание ключевых параметров позволяет значительно снизить проектные риски, связанные с недостаточной компетенцией исполнителя или несоответствием функциональных возможностей выбранного продукта потребностям организации.

Магический квадрант

На российском рынке в настоящее время наиболее актуальны решения таких компаний, как Oracle и Sun Microsystems (которых в свете состоявшегося поглощения можно считать одной компанией), IBM, Microsoft и SAP.

Gartner располагает вендоров на своем квадранте (см. рис.1), исходя из возможностей продукта, анализа рынка, опыта заказчиков в работе с решениями производителя и общего видения того, какие вендоры будут доминировать по продажам и технологическому влиянию в ближайшие 1-2 года.

Лидерами по совокупности характеристик являются Oracle, IBM и Sun Microsystems. Решения данных вендоров на данный момент являются наиболее технически зрелыми, кроме того их объединяют и другие общие характеристики:
- Последовательная реализация нового функционала в новых версиях;
- Введение инновационных функций;

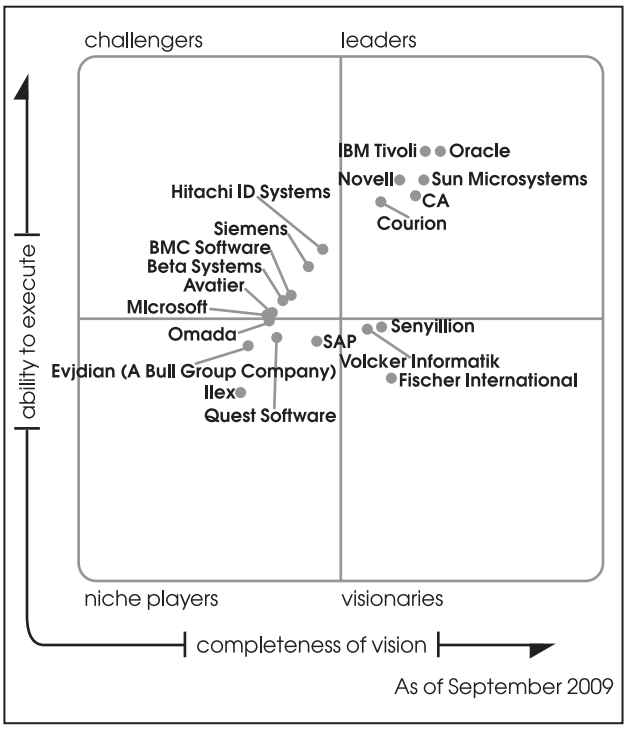


Рис. 1. Магический квадрант Gartner: User Provisioning (сентябрь 2009)

- Расширенное портфолио смежных продуктов (в том числе за счет поглощений);
- Взаимосвязь с другими продуктами данного вендора (через лицензирование и/или интеграцию).

В 2008 году продукт Sun Microsystems являлся лидером, но в 2009 году несколько уступил свои позиции по причине поглощения компании. В связи с сотоявшимся в 2010 году объединением компаний Sun и Oracle в будущем следует ожидать выхода нового продукта, который будет объединять сильные стороны и лучшие наработки решений обоих вендоров. Позиция компании Microsoft в 2009 году осталась без изменений и относится к продукту Identity Lifecycle Manager 2007. На его смену в 2010 году вышел обновленный Forefront Identity Manger 2010, который является третьим поколением IdM-продукта от Microsoft и имеет шансы перевести этого вендора в квадрант лидеров.

Решение компании SAP по оценке Gartner в 2009 году находится в квадранте нишевых игроков. Основная причина этого заключается в том, что продукт ориентирован в первую очередь на заказчиков, использующих SAP ERP и, следовательно, на развитие возможностей IdM-продукта по интеграции с данной системой. В то время как для компаний, использующих SAP ERP, это является, безусловно, сильной стороной SAP IdM, для остальных это плюсом не является. Но в 2010 году можно ожидать изменений в положении продукта SAP в магическом квадранте в сторону лидирующих позиций. Это станет возможным за счет интеграции продуктов SAP IdM и SAP GRC, предоставляющих возможности по анализу рисков, выявлению конфликтующих ролей или ролей нарушающих принцип разделения полномочий.

На российском рынке IdM-решений в настоящее время присутствуют все перечисленные выше вендоры с различными по объему портфолио уже заверешенных проектов. В связи с постоянно возрастающим интересом к направлению Identity Management со стороны российских заказчиков, а также ростом компетенции и опыта интеграторов по данным решениям, можно прогнозировать значительное увеличение количества IdM-проектов в России в ближайшие 1-2 года.

Статья подготовлена по материалам компании Oracle

Управление рисками при внедрении системы Identity Management как комплексного решения

Вячеслав Петрухин,
консультант отдела IdM-решений компании «Инфосистемы Джет»

Identity Management: Подход к управлению идентификацией и доступом. Система IdM интегрируется с информационными системами организации, такими как почтовая система, каталоги, бизнес-приложения и позволяет централизованно управлять учетными записями и правами доступа в них. Управление при этом может осуществляться как в «ручном» режиме — из интерфейса IdM-системы, так и в автоматическом — на основе информации, получаемой из «доверенного источника» данных о сотрудниках, которым чаще всего является кадровая система. Таким образом, при приеме на работу нового сотрудника, ему автоматически создаются учетные записи в тех системах, доступ к которым нужен ему для выполнения служебных обязанностей, при изменении должности или подразделения права доступа так же автоматически меняются, а при увольнении учетные записи блокируются или удаляются. Благодаря встроенному согласующему документообороту, любые изменения в целевых системах могут быть согласованы в соответствии с принятыми в организации бизнес-процессами.

Инструмент администратора

Существуют два основных подхода к внедрению систем Identity Management. В первом случае целью создания IdM-системы является внедрение инструмента администратора — средства управления учетными записями и правами доступа в информационных системах. Остальные возможности, предоставляемые подходом Identity Management, остаются «за кадром», среди них: автоматизация бизнес-процессов управления доступом, переход на ролевую модель управления доступом, расширенный аудит доступа сотрудников организации к бизнес-приложениям. У такого подхода, несмотря на очевидные минусы (не используются все возможности IdM), есть и плюсы: внедрение IdM в таком функционале гораздо менее трудоемко, практически не затрагивает существующие бизнес-процессы, а значит не находит значительного инертного сопротивления.

Комплексное решение

Второй подход к созданию IdM-системы — создание комплексного решения, которое значительно изменит существующие бизнес-процессы организации и предоставит дополнительные возможности, о которых есть смысл рассказать подробнее. Возможности IdM-систем включают не только собственно управление учетными записями в целевых системах, но и различные механизмы описания и разработки процессов управления (workflow), которые могут включать взаимодействие с целевыми системами и запускаться при нас-

туплении определенных условий. Например, процесс создания учетных записей может автоматически запускаться после приема на работу нового сотрудника и внесения информации о нем в HR-систему. При переводе сотрудника на новую должность, увольнении и предоставлении отпуска будут запускаться другие процессы, автоматически изменяющие права доступа, блокирующие или удаляющие учетные записи. Совместно с другой возможностью систем Identity Management — согласующим документооборотом — это позволяет полностью переработать управление доступом в организации: отказаться от «бумажных» заявок и обходных листов, сократить время на предоставление/отъем доступа, исключить риск человеческих ошибок, которые неизбежны при «ручном» администрировании целевых систем.

Еще одно значительное преимущество, которое доступно при создании комплексного решения Identity Management, — переход на ролевую модель управления доступом в рамках целой организации. При этом права доступа пользователей в целевых системах группируются в роли, которые могут быть привязаны к таким формальным критериям как должность сотрудника и подразделение, в котором он числится, и могут быть назначены автоматически благодаря взаимодействию IdM и HR-систем.

IdM-решения большинства вендоров предоставляют пользовательский интерфейс, с помощью которого можно делегировать некоторые функции обслуживания учетных записей на самого пользователя — изменение и восстановление пароля, запрос дополнительной роли (прав доступа), изменение информации пользователя.

Отдельно стоит упомянуть функции, связанные с минимизацией рисков информационной безопасности. В первую очередь, возможность автоматической сверки реально существующих прав доступа в целевых системах с правами, наличие которых у сотрудника было согласовано в системе Identity Management и которые полагаются ему согласно ролевой модели. В случае расхождения некорректные права доступа могут быть удалены, учетная запись заблокирована, а сотрудник информационной безопасности будет оповещен письмом о данном инциденте.

Функции аудита и построения отчетов позволяют моментально получить доступ к информации об актуальных правах доступа сотрудников, например, сформировать список всех сотрудников, имеющих определенные права в какой-либо системе или список целевых систем и прав, к которым есть доступ у какого-либо сотрудника. Благодаря возможности получить ту же информацию «в динамике» — исторический отчет, в котором содержатся данные о том, когда какие права доступа были предоставлены, кем это было согласовано — IdM-система становится важным средством для расследования и предотвращения инцидентов по несанкционированному доступу к данным.

Риски создания комплексного решения

Как видно из описания комплексного решения Identity Management, для создания системы, реализующей в полном объеме все данные функции, необходимо провести большую подготовительную работу. В первую очередь — детализация и анализ требований к системе. Поскольку функционал создаваемой системы напрямую затрагивает работу как подразделений информационных технологий и информационной безопасности, так и работу бизнес-подразделений, то детализация и согласование требований по всем функциям может занять очень значительное время. Для организации с численностью сотрудников 3-7 тысяч этот процесс занимает несколько месяцев. Реализация же всех требований — разработка бизнес-процессов, адаптация функционала и интерфейса системы, формирование ролевой модели — в рамках одного проекта приводит к тому, что его длительность может достигать от одного до двух лет.

Поскольку текущая ситуация на рынке далека от стабильности и всем организациям необходимо постоянно меняться и перестраивать бизнес-процессы для достижения максимальной эффективности, то становится очевиден основной риск подобных проектов: требования к системе могут устаревать еще до окончания процесса их анализа, не говоря уже о стадии перевода системы в промышленную эксплуатацию. Реализация же устаревших требований приводит к появлению ненужного инструмента, которым в текущей ситуации невозможно пользоваться. Два других риска являются следствиями первого — устаревшие данные нуждаются в актуализации, а повторная работа по выявлению требований значительно увеличит сроки проекта и его бюджет. Ситуация может показаться совсем безнадежной, если несоответствие требований к IdM-системе текущим потребностям организации было выявлено, когда значительная часть требований уже была реализована.

Отдельно стоит упомянуть риск, связанный с большим объемом внутренних изменений в организации, которые необходимо провести, чтобы внедряемая система начала действительно работать. Стоит учитывать, что организация, как любая система, сопротивляется изменениям и чем их больше, тем сильнее это сопротивление. Кроме того, необходимо ввести в действие новые регламенты и приказы, обучить сотрудников работе с новой системой.

Исключение и минимизация рисков

Предотвратить возникновение подобных ситуаций может учет перечисленных выше рисков еще на этапе формирования требований к системе и правильное планирование проекта, учитывающее специфику IdM-тематики.

Прежде всего, следует признать планы по реализации всего функционала IdM в рамках единого проекта в значительной степени утопичными. Далее следует разделить требования на группы по принципу последовательности их реализации и связи друг с другом. Основываясь на данных группах, можно сформировать план поэтапного внедрения системы IdM. В общем случае организация проекта должна отвечать следующим требованиям:

- разделение функционала Identity Management на блоки и последовательная реализация одного такого блока функций в рамках одного этапа;
- каждый этап завершается переводом в промышленную эксплуатацию блока функций, реализованных на данном этапе;
- каждый последующий этап не является обязательным и может рассматриваться как развитие системы.

Рассмотрим, чем продиктованы данные требования. Во-первых, блоки смежных и последовательно реализуемых функций избавляют нас от необходимости в детализации требований по всему функционалу IdM-системы, предпроектное обследование будет ограничено задачами, реализация которых запланирована на данный этап. Следовательно, вероятность устаревания требований к системе незначительна. Конечно, риски превышения бюджета и срыва сроков нельзя совсем исключить при реализации сложного интеграционного проекта, затрагивающего большое количество информационных систем и подразделений организации, но в данном случае объем проекта можно точно оценить на этапе планирования, а значит, в общем случае эти риски можно отнести к маловероятным.

Во-вторых, организация, использующая новые технологии впервые, не может в полной мере понять все нюансы, возникающие при работе с данной технологией в продуктивной среде с реальными задачами. Причина этого заключается в том, что значение многих обстоятельств и их влияние на работу организации может быть оценено неправильно или совсем не приниматься в расчет. В результате очень часто возникает необходимость внесения изменений в новую информационную систему сразу после ее перевода в промышленную эксплуатацию, даже если она отвечает всем формальным требованиям, сформулированным до старта проекта. При переводе каждого блока функций создаваемой IdM-системы в промышленную эксплуатацию, объем таких изменений будет минимальным, а у подразделений, напрямую взаимодействующих с IdM, появляется понимание реальных потребностей по ее развитию на последующие этапы.

Аналогично, плавный переход к модели Identity Management значительно уменьшает сопротивление изменениям и позволяет преодолеть инертность организации, поскольку количество единовременно проводимых организационных изменений невелико и, определяя набор функций, реализуемых на каждом этапе, мы сами можем на него влиять.

Поэтапное внедрение увеличивает суммарную длительность проекта, но если в случае реализации всех функций в рамках единого проекта возможность работы с IdM-системой появляется только по его завершению, то при поэтапном подходе возможность использования Identity Management появляется уже по завершению первого этапа, а значит, отдача от системы и возврат средств (см. Приложение 1) происходят быстрее.

Конечно, создание комплексного решения Identity Management связано с достаточно серьезными проектными рисками. Но, как мы видим, ими вполне можно управлять, если подходить к планированию и организации внедрения с учетом специфики IdM. Именно поэтому для успешного завершения проектов этого направления принципиальное значение имеет опыт исполнителя.

Данная статья была подготовлена для издания «Информационная безопасность» и будет опубликована в №3-2010.

...как мы решали проблемы

В инновационных проектах практически невозможно предугадать, с какими сложностями столкнешься. Конечно, это риск, но вместе с тем, решая такие нетривиальные задачи, получаешь бесценный опыт.

Множество кадровых источников данных

Одной из сложностей проектов может стать необходимость интеграции IdM с большим количеством кадровых систем (КС) для получения информации о сотрудниках. Например, в каждом регионе используется своя система учета кадров, а в крупных регионах их может быть даже несколько, зачастую разных производителей. В рамках одного проекта к IdM были подключены 11 основных КС. Сложность их подключения связана с уникальной идентификацией каждого работника компании. Идентификаторы («определители личности») в различных системах, естественно, никак не коррелируют, а один и тот же человек может числиться работающим одновременно в нескольких КС (например, как штатный сотрудник и как совместитель). IdM-система должна определять таких сотрудников и создавать для них один набор учетных записей. А при увольнении работника из одного подразделения заблокироваться должны только те учетные записи, которые соответствовали должности, с которой он уволился. Для решения этой задачи специалисты компании «Инфосистемы Джет» ввели уникальный идентификатор каждого пользователя в системе, который формируется на основе ФИО и даты рождения.

Приложение 1

Внедрение системы Identity Management: статьи дохода

Внедрение затратной (как по стоимости лицензий, так и по количеству работ) информационной системы должно быть безусловно четко обосновано. И если в практической полезности реализации подхода Identity Management сомневаться не приходится, то вопрос «а стоит ли игра свеч?» для многих остается открытым. Для ответа на него необходимо выполнять расчет окупаемости инвестиций (ROI — Return On Investment) в каждом отдельном случае.

В данном материале мы приведем статьи дохода, появляющиеся при использовании подхода Identity Management, которые учитываются при расчетах ROI. Применяемые при этом технологии позволяют компании эффективнее использовать свои информационные системы и окупить затраты на внедрение дорогостоящих решений IdM. Статистика по этому вопросу предоставлена компанией Oracle — одним из ведущих вендоров данного направления, накопившим значительный опыт внедрения подобных систем.

Повышение производительности службы технической поддержки пользователей (Help Desk)

Производительность Help Desk увеличивается благодаря тому, что средствами IdM многие рутинные задачи управления доступом можно переложить на самого пользователя. Благодаря функциям самообслуживания у пользователя появляется возможность:

- Самостоятельно восстанавливать забытые пароли;
- Снимать с приложений блокировку, вызванную несвоевременной сменой паролей;
- Самостоятельно заказывать себе доступ к приложениям, правам доступа и ИТ-услугам.

Согласно статистике, использование механизмов IdM для самообслуживания пользователей уменьшает количество запросов на Help Desk примерно на 55%.

Повышение эффективности управления учетными записями

Для управления правами доступа в подходе Identity Management вводится понятие «бизнес-роль», под которым понимается набор прав доступа («ИТ-ролей»), соответствующих положению сотрудника в организационной структуре предприятия. Бизнес-роль может быть назначена сотруднику автоматически на основании формальных критериев, которые могут быть обнаружены в кадровом приложении (чаще всего это связка должность-подразделение).

В результате внедрения IdM-системы эффективность управления учетными записями повышается не меньше чем на 78% за счет централизованного управления учетными записями в соответствии с бизнес-ролью сотрудника, которое исключает необходимость раздельного администрирования учетных записей в каждом приложении.

Снижение затрат руководителей подразделений

Согласование заявок на доступ может быть автоматизировано с помощью согласующего документооборота в рамках IdM-системы. Использование этого функционала IdM-системы сокращает издержки на согласование заявок на доступ в целом примерно на 55%.

Снижение затрат на внешний аудит ИТ

IdM автоматизирует регистрацию и хранение информации об истории назначения прав доступа, а также предоставляет инструменты формирования соответствующей аудиторской отчетности. Данный функционал позволяет сократить затраты на внешний аудит ИТ не меньше чем на 75%.

Снижение затрат на проведение внутреннего аудита

Аналогично предыдущему пункту, затраты на проведение внутреннего аудита сокращаются примерно на 75% за счет автоматической регистрации, хранения информации и предоставления инструментов аудиторской отчетности об истории назначения прав доступа к информационным системам.

Снижение затрат на лицензирование прикладного программного обеспечения

IdM предоставляет функции автоматического обнаружения неиспользуемых учетных записей в приложениях, что позволяет уменьшить лицензионные отчисления. Благодаря этому, в результате внедрения IdM затраты на внутренний аудит ИТ сокращаются не меньше чем на 30%.

Снижение вероятности административного преследования за невыполнение требований руководящих документов

Затраты на выплату штрафов за невыполнение требований руководящих документов сокращаются на 75% за счет автоматической регистрации, хранения информации и использования инструментов аудиторской отчетности об истории назначения прав доступа к информационным системам. Данный пункт справедлив, в первую очередь, для западных организаций, но с вступлением в силу федерального закона 152-ФЗ «О защите персональных данных» его значение в будущем нельзя недооценивать.

Снижение рисков безопасности, вызванных избыточными правами доступа

IdM предоставляет механизмы проверки избыточности привилегий сотрудников, а также обеспечивает централизованный доступ к ресурсам в строгом соответствии с бизнес-ролью. Это позволяет снизить потери из-за утечки конфиденциальной информации и нарушения функционирования систем из-за избыточных привилегий сотрудников приблизительно на 15%.

Итого...

Перечисленные статьи дохода позволяют полностью окупить внедрение системы Identity Management в среднем за 1,5-2 года (рис.1), после чего она начинает приносить прибыль. Еще раз отметим, что приведенные цифры наиболее актуальны для западных организаций (поскольку наиболее точные сведения для анализа могли быть получены именно от мировых компаний), но есть все основания предполагать аналогичные показатели и для российских компаний. Такой небольшой срок возврата инвестиций вместе с преимуществами данного направления делает его все более интересным как для подразделений информационных технологий и информационной безопасности, так и для бизнес-подразделений.

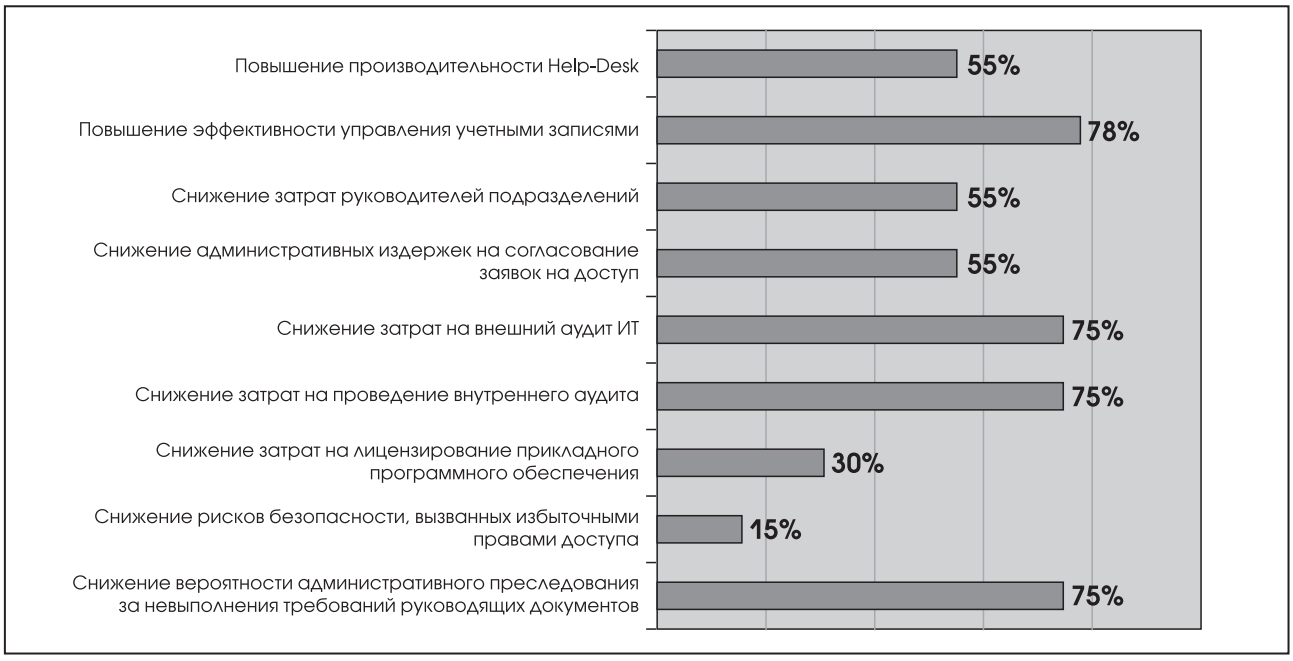


Рис. 1. Снижение затрат компании на управление информационными технологиями

Защита персональных данных в бизнес-приложениях средствами Oracle Identity Management и смежными решениями

Статья подготовлена по информации компании Oracle

Нормативные документы по информационной безопасности, в том числе по защите персональных данных, рекомендуют использование прошедших в установленном порядке процедуру оценки соответствия (сертифицированных) средств защиты информации (СЗИ) для обеспечения информационной безопасности автоматизированной системы (АС) предприятия. И если в настоящее время существует большое количество сертифицированных СЗИ для использования на уровне рабочих станций, локальной сети и каналов связи, то проблема защиты информации на уровне бизнес-приложений стоит достаточно остро.

Решения Identity Management компании Oracle и некоторые смежные продукты были сертифицированы на соответствие требованиям безопасности информации для защиты АС и информационных систем персональных данных (ИСПДн). В частности были сертифицированы:

- **Oracle Identity and Access Management Suite** (включающий Oracle Identity Manger и Oracle Access Manager) сертифицирован как СЗИ для защиты информации в АС класса до 1Г включительно и ПДн до 2-го класса включительно;
- **Oracle Enterprise Single Sign-On** сертифицирован, как средство идентификации и аутен-

Oracle Identity Manager:

- Централизованное управление учетными записями и привилегиями сотрудников по доступу к бизнес-приложениям с использованием механизмов ролевого доступа и согласования заявок;
- Самообслуживание пользователей и управление парольной политикой для бизнес-приложений;
- Контроль действий администраторов, неизбыточности полномочий, аудит и историческая отчетность по всем операциям и привилегиям в приложениях.

Oracle Access Manager:

- Контроль доступа к любым бизнес-приложениям, разработанным на трехзвенной архитектуре (например, Oracle E-Business Suite, Siebel, Hyperion, порталы Oracle, IBM, Microsoft, SAP и т.д.) на уровне HTTP-запросов;
- Различные методы аутентификации и однократная регистрация (SSO) для бизнес-приложений;
- Аудит и отчетность по доступу к бизнес-приложениям.

Oracle Enterprise Single Sign-On:

- Однократная регистрация (SSO) для «толстых» и терминальных клиентов;
- Восстановление забытых паролей;
- Интеграция со смарт-картами и токенами.

Oracle Information Righs Management:

- Классификация, защита и централизованный контроль доступа к электронным документам, почтовым сообщениям и отчетам, экспортируемым из бизнес-приложений, вне периметра защиты организации;
- Централизованный аудит защищаемых документов и их копий, контроль их версий и уничтожение конфиденциальных документов.

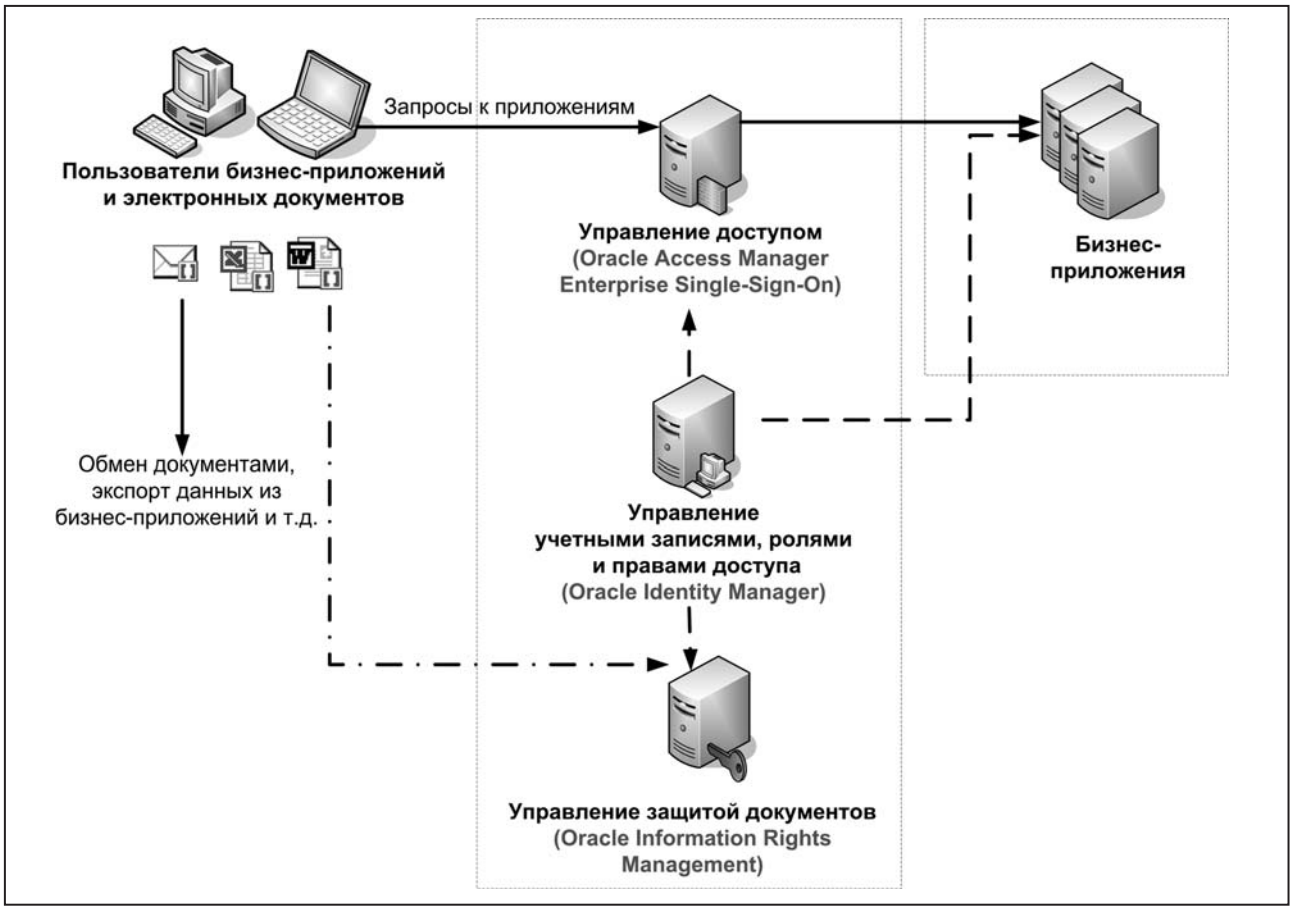


Рис. 1. Архитектура решения по защите ПДн

тификации в АС класса до 1Г включительно и ПДн до 2-го класса включительно;

- **Oracle Information Rights Management** сертифицирован как СЗИ для защиты информации в АС класса до 1Г включительно и ПДн до 2-го класса включительно.

Согласно требованиям нормативных документов, бизнес-приложения, обрабатывающие персональные данные, должны обеспечить аутентификацию, управление доступом, аудит и мониторинг, а также защиту экспортируемых отчетов и документов сертифицированными СЗИ. Предлагаемая в этом случае архитектура решения представлена на рис. 1.

Таким образом, защита выгружаемых из бизнес-приложений отчетов и документов обеспечивается сертифицированным СЗИ Oracle Information Rights Management, контроль доступа к бизнес-приложениям осуществляется с помощью Oracle Access Manager или Oracle Enterprise Single Sign-On (в зависимости от архитектуры целевого приложения), при этом управление учетными записями, паролями, ролями и правами доступа выполняется Oracle Identity Manager.

Как мы видим, интегрированный стек продуктов Oracle, взаимодействующих между собой для обеспечения централизованного управления и контроля системы информационной безопасности, позволяет закрыть значительную часть требований по защите персональных данных в бизнес-приложениях.

Преимущества для бизнеса, обеспечиваемые решением для управления идентификационными данными и доступом

Алексей Овчинников,
технический специалист по Tivoli Security,
ООО «ИБМ Восточная Европа/Азия»

Повышение эффективности управления идентификационными данными и доступом

Сегодня организации сталкиваются с множеством задач, в том числе связанных с растущим количеством пользователей, приложений и точек доступа. При этом им необходимо заботиться о выполнении регулирующих норм. Многие организации видят в инновационных решениях возможности для поддержки устойчивого роста, однако им необходима надежная инфраструктура безопасности, обеспечивающая удобный доступ к приложениям и системам и помогающая выполнять нормативные требования. Эффективность управления идентификационными данными и доступом может оказывать значительное влияние на конкурентоспособность и прибыльность бизнеса.

Эффективное управление идентификационными данными и доступом обеспечивает преимущества в следующих областях:

- **Управление идентификационными данными** – определение прав доступа пользователей, изменение их ролей и привилегий, лишение прав доступа в конце жизненного цикла учетных записей.
- **Управление доступом** – надежная аутентификация пользователей, в том числе с использованием механизма однократной регистрации (single sign-on, SSO), соблюдение политик доступа после прохождения пользователями процедуры аутентификации.
- **Контроль соблюдения пользователями политик безопасности** – мониторинг действий пользователей, проведение аудита и формирование отчетов, позволяющие организациям упрощать соблюдение политик и регулирующих норм, а также ослаблять внутренние угрозы безопасности благодаря мониторингу поведения пользователей.

Управление идентификационными данными

Перед большинством компаний, в которых количество сотрудников достигло переломного значения, рано или поздно встает вопрос о создании общей корпоративной системы управления пользовательскими учетными записями. Спектр пожеланий и требований к ней может быть достаточно широк – от наличия простого справочника пользователей до специфических интеграционных возможностей и механизмов автоматизации.

Самый очевидный и значимый эффект от установки такой системы – это внедрение регламентов, отчетности и набора процедур для обеспечения пользователя учетными записями в различных корпоративных системах, необходимых ему для работы.

За счет автоматизации этого процесса и уменьшения вовлеченности в него администраторов учетные записи в информационных системах становятся полностью контролируемыми, а жизненный цикл – замкнутым. Ни одна учетная запись не хранится в подконтрольной системе дольше, чем требуется.

Средство автоматизации управления правами пользователей предоставляет возможности для облегчения других связанных с этой областью работ. К примеру, сложный процесс по заполнению внедряемых в компании новых систем учетными данными существующих пользователей обоснованно перекладывается на продукт IBM Tivoli Identity Manager.

Этот процесс можно либо автоматизировать, используя роли пользователей в компании, либо позволить сотрудникам самостоятельно запросить необходимый им доступ. Особое внимание следует уделить пользовательским паролям при наличии жестких требований по доступу к ним. Администратор в любой момент может предоставить ссылку на пользовательский интерфейс, где сотрудник самостоятельно введет пароль на внедряемое приложение.

Другими словами, ручные действия с пользовательскими учетными записями уходят из области скриптов и преобразуются в понятную и управляемую методику работы.

Так, например, одна из известных российских телекоммуникационных компаний решилась на серьезный инфраструктурный проект по централизации управления учетными данными, а также однократной регистрации пользователей.

Выстраивание собственно системы с единой точкой входа — нетривиальная задача. Однако при создании системы управления учетными записями все записи, существующие в компании, были сведены воедино. Наличие центрального хранилища значительно упростило техническую сторону вопроса по созданию однократной регистрации.

В итоге основная цель проекта была достигнута: пользователи получили единую систему паролей, а служба информационной безопасности — четкую и прозрачную политику доступа со стандартизованными процессами предоставления прав. Все действия с паролями пользователей были возложены на службу поддержки. Таким образом, количество персонала, занимающегося проблемами доступа, удалось серьезно сократить

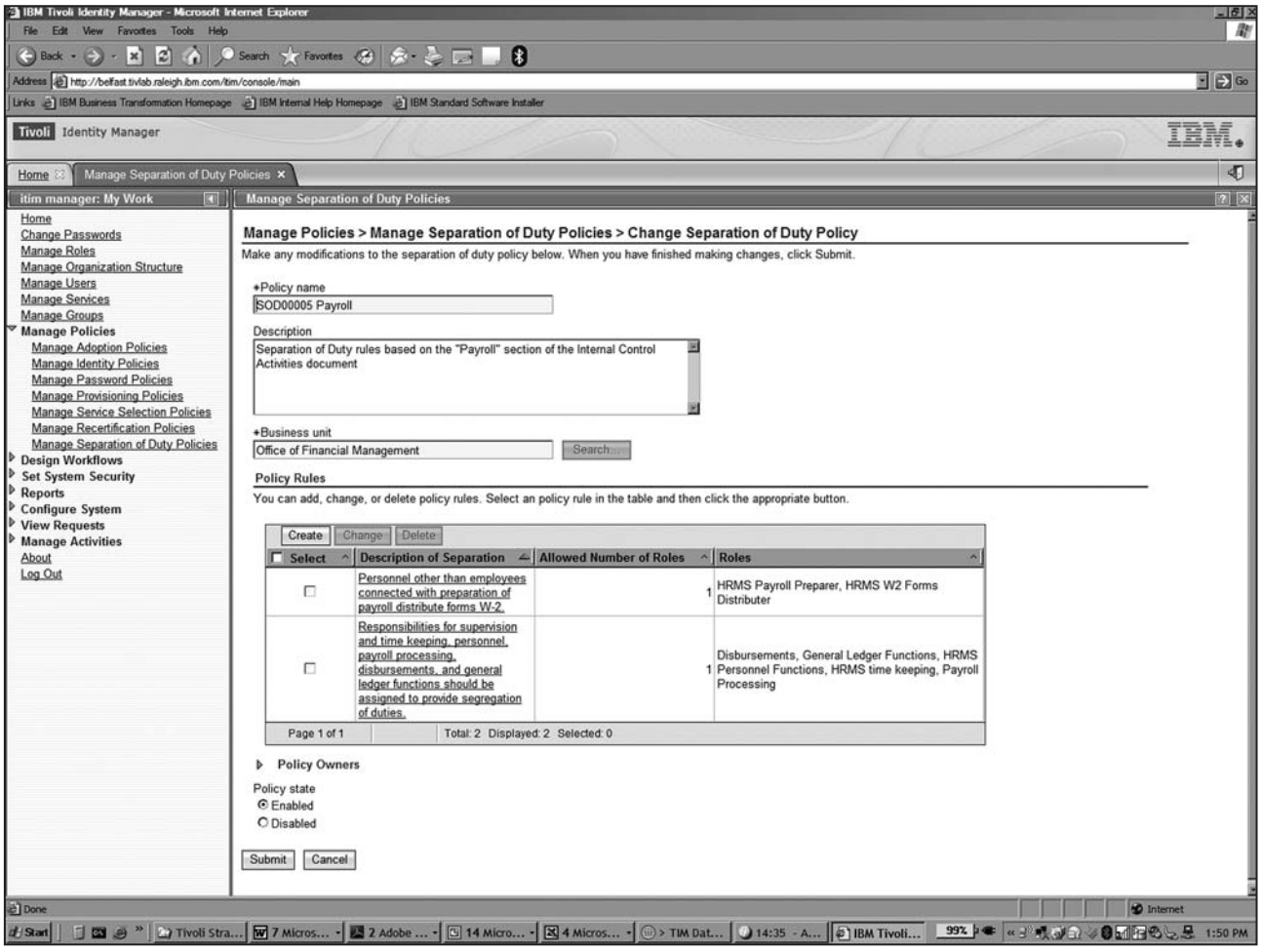


Рис. 1. Пример административного интерфейса IBM Tivoli Identity Manager

за счет автоматизированной системы, которая взяла на себя эти функции.

Внедрение любого инфраструктурного решения влияет на последующие ИТ-проекты. Данный случай не стал исключением. Опыт интеграции используемых приложений позволил конкретизировать требования компании к внедряемым решениям в плане управления доступом.

В одном из американских университетов учетные записи для новых пользователей теперь создаются не за две недели, а за два дня. Кроме того, решение IBM Tivoli Identity Manager обеспечивает повторное подтверждение прав доступа для важнейших систем и учетных записей по классам сервисов, чтобы предоставить университету возможность уделять особое внимание своим самым серьезным источникам рисков.

Решение Tivoli позволило организации, работающей в сфере финансовых услуг, рационализировать процесс определения прав пользователей, а также быстро и просто интегрировать новых пользователей из приобретенных компаний. Повышая эффективность и обеспечивая экономию времени, это решение предоставляет компании возможность уделять больше внимания стратегии расширения бизнеса, а не управлению пользователями.

Страховой компании решение Tivoli позволило быстрее реагировать на потребности клиентов благодаря ускоренному предоставлению доступа к приложениям и платформам. Это время в рамках автоматизированного рабочего процесса сократилось с нескольких дней до нескольких минут. Решение позволяет обнаруживать и удалять потерянные учетные записи, и теперь программные решения компании работают быстро и без сбоев, высвобождая тем самым ресурсы системного администрирования.

Управление доступом

Сложность задачи по построению системы управления доступом напрямую зависит от архитектуры системы. Ведь доступом можно управлять на каждом уровне этой архитектуры: от подстановки паролей на пользовательской рабочей станции до разграничения доступа на уровне файловой системы или таблиц базы данных. Наиболее простым примером единой системы доступа может служить схема из двух интегрированных подсистем: управления идентификационными данными и системой однократной аутентификации. С помощью данной интеграции можно достичь ситуации, когда пользователь не зная ни одного пароля для входа в приложения, сможет работать с ними в обычном режиме. При этом пользователь будет иметь возможность самостоятельно запрашивать, а затем и получать доступ в разрешенные ему приложения также без знания пароля.

Более сложным примером можно считать построение портала с корпоративными приложениями и сквозной аутентификацией или федеративными отношениями с партнером. Универсального решения для таких задач не существует, поэтому каждая задача требует отдельного подхода.

Инструменты решения IBM Tivoli Identity and Access Assurance смогут существенно облегчить построение всех выше перечисленных примеров.

Ниже лишь некоторые примеры использования данного решения.

Средства однократной регистрации избавили сотрудников азиатской компании, разрабатывающей программное обеспечение, от необходимости несколько раз проходить аутентификацию для получения доступа к различным системам. Это позволило повысить эффективность совместной работы разных подразделений. Системы могут развертываться на новой площадке за один день, а не за несколько недель, как это было прежде. А канадской коммуникационной компании решение Tivoli Identity and Access Assurance помогло повысить эффективность операций и упростить задачи обслуживания. Это решение предоставило компании возможность проще интегрировать новые приложения в среду портала и обеспечивать доступ к ним для выездных технических специалистов.

Развернув решение IBM Tivoli Identity and Access Assurance, датский банк сократил время разработки web-приложений. Теперь этот финансовый институт может быстрее, чем когда-либо прежде, предлагать клиентам новые, надежно защищенные приложения. Это решение обеспечило повышение уровня удовлетворенности клиентов, поскольку им требуется только один раз пройти процедуру аутентификации для получения доступа ко всем банковским приложениям. Однако наиболее ценным для бизнеса стало ускоренное предоставление клиентам новых сервисов.

Решение IBM Tivoli Identity and Access Assurance может также выявлять связанные с паролями события и реагировать на них. Это позволяет автоматизировать задачи управления паролями. Например, используя программное обеспечение

Tivoli, европейский пенсионный фонд упростил процессы по управлению доступом пользователей.

Благодаря развертыванию средств обеспечения безопасности Tivoli, среда управления пользователями в испанском банке стала более адаптируемой, предсказуемой и динамичной. Банк сократил затраты на управление пользователями и предоставил своим ИТ-специалистам возможность сконцентрироваться на других функциях.

Контроль соблюдения пользователями политик безопасности

Решение IBM Tivoli Identity and Access Assurance позволяет оперативно предоставлять доступ к ресурсам тем пользователям, которые имеют на это право. При этом оно замыкает круг управления путем проверки соответствия действий пользователей политикам безопасности.

Рис. 2. Цикл управления идентификационными данными и доступом, с контролем соблюдения пользователями политик безопасности

Ответственным за данную задачу в решение IBM Tivoli Identity and Access Assurance является продукт IBM Tivoli Security Information and Event Manager. Этот продукт использует методологию W7: Who (Кто), did What (Что делал), When (Когда), Where (Где), Where from (Откуда), Where to (Куда), on What (С чем)) для превращения содержимого log-файлов в понятную, детальную информацию о действиях пользователей.

Данный инструмент может заинтересовать организации, которым необходимо анализировать соблюдение сотрудниками политики безопасности при работе с внутренним ресурсами. Для решения этой задачи функционал продукта делится на две основные части.

Для начала проводится сбор необработанных журналов работы с информационных систем компании.

Затем осуществляется обработка собранных данных по принципу: «Кто что делал и с чем? Когда это было, где, откуда и куда?»

Функция сбора логов относится к выделенному направлению Log Management. К этому направлению относится широкий круг задач по управлению «сырыми» данными: копирование журналов без обработки их содержимого, централизованное хранение, экспорт на длительное хранение, поиск по «сырым» данным, а также формирование отчетности. Этот механизм важен, так как дает уверенность в сохранности копии журнала работы требуемой программы на случай утери оригинала.

Второй основной функцией данного инструмента является анализ журналов на соответствие действий пользователей корпоративной политике безопасности. В качестве исходных параметров для анализа используются период времени и указания на то, журналы каких информационных систем выбирать, а также на соответствие какой именно политике производить анализ.

При этом в системе не обязательно должна быть одна политика безопасности, ее можно дорабатывать, копировать, тестировать. Принцип построения политики следующий: в ней простым языком прописывается, что именно пользователям делать разрешено.

Такой подход упрощает описание прав доступа, соответствующих должностным обязанностям. В то же время всегда можно задать правила, прямо указывающие, какие действия пользователей заслуживают более пристального внимания.

Рассмотрим примеры внедрения.

В одной из российских компаний, работающей в секторе металлургической промышленности, стояла задача осуществлять контроль правил доступа пользователей к файлам для того, чтобы вовремя можно было предотвратить утечку критической для промышленного производства информации.

В процессе внедрения сотрудники службы ИТ настроили специальные агенты для всех используемых в компании приложений, которые фиксируют обращение этих приложений к файловой системе. Этого оказалось достаточно, чтобы система могла контролировать события в центральном офисе компании и во всех ее филиалах. Для анализа событий продукт снабжен Web-интерфейсом, с помощью которого служба информационной безопасности может настроить собственные правила контроля доступа к файлам, а также формировать отчеты. Построенная на основе IBM Tivoli Security Information and Event Manager система контроля доступа к файлам позволила службе информационной безопасности фиксировать факт обращения пользователей к секретной информации и оперативно применять меры организационного воздействия. Наличие системы контроля за деятельностью сотрудников оказывает в том числе и дисциплинирующее воздействие на пользователей.

Европейский аэропорт развернул решение IBM Tivoli Identity and Access Assurance, чтобы упростить выполнение международных правил. Организация получила возможность выявлять и пресекать неавторизованные действия в своей сети, а также анализировать операции пользователей, оценивать их и принимать соответствующие меры. Благодаря развитым средствам подготовки отчетов, руководители могут обеспечивать значительно более строгий контроль над повседневными операциями в своей сети.

Региональному медицинскому центру решение IBM Tivoli Identity and Access Assurance помогает выполнять требования HIPAA (защита информации о пациентах). Кроме того, оно обеспечивает значительные преимущества для бизнеса. Медицинские специалисты затрачивают меньше времени на получение доступа к приложениям и завершение сеансов работы с ними, поэтому они могут сосредоточиться на обслуживании пациентов. Благодаря сокращению потребностей в восстановлении паролей, снизились операционные затраты. И организация успешно привлекает врачей и других медицинских работников, которым требуется лучшая в своем классе технологическая поддержка.

Одна из ведущих страховых компаний Европы использует решение Tivoli для анализа событий в системе безопасности, их фильтрации и выполнения соответствующих действий. В результате компания может лучше анализировать эти события и совершенствовать свою политику обеспечения безопасности.

Организации стремятся получать преимущества, развертывая решения для управления идентификационными данными и доступом. Такие решения не только позволяют удовлетворить краткосрочные потребности, такие как сокращение затрат, интеграция бизнеса и др. Они поддерживают долгосрочные цели — включая расширение бизнеса на основе развертывания порталов, а также подготовку к ускоренному росту.

Решение IBM Tivoli Identity and Access Assurance позволяет организациям получать преимущества благодаря развертыванию инфраструктуры централизованного, автоматизированного управления идентификационными данными и доступом. Такой доступ должен охватывать весь жизненный цикл учетных записей пользователей, а также способствовать повышению качества обслуживания, сокращению затрат и поддержке выполнения регулирующих норм. Кроме того, это решение упрощает коллективную работу через порталы с доступом на базе ролей, обеспечивает оперативное развертывание новых сервисов и позволяет проще реализовать возможности однократной регистрации.

Новые возможности Forefront Identity Manager 2010

Материалы предоставлены Российским офисом Microsoft

Проблемы управления учетными записями и доступом, с которыми сталкиваются сегодня коммерческие компании и государственные организации, затрагивают практически все бизнес-процессы. Недостаточное внимание к этим вопросам приводит к росту затрат, увеличению рисков и снижению продуктивности сотрудников. Решение для управления учетными записями и идентификационной информацией пользователей Forefront Identity Manager (FIM) 2010 , являясь основной частью решения по управлению учетными записями и доступом пользователей к информационным ресурсам, обеспечивает более безопасный доступ как к внутренним ресурсами, так и «облачным» сервисам практически из любого места подключения к сети Интернет и с использованием различных типов устройств.

По сравнению со своим предшественником, Identity Lifecycle Manager 2007, новый FIM упрощает процессы управления идентификацией и доступом пользователей благодаря предоставлению портала самообслуживания пользователей и набору инструментов для администраторов, которые позволяют автоматизировать типовые задачи по управлению учетными записями, паролями, группами и списками рассылки, а также цифровыми сертификатами пользователей. FIM помогает создавать и контролировать политики доступа для сотрудников компаний, инфраструктура которых построена на платформе Windows, а также в гетерогенных средах. Кроме этого, FIM предоставляет собой среду, в которую можно интегрировать любые пользовательские решения.

Повышение эффективности работы пользователей

Снижение нагрузки на службу технической поддержки является одной из главных задач ИТ-директора в любой компании. При этом эффективность работы самих ИТ-специалистов и разработчиков, а также простых пользователей должны увеличиться. FIM предоставляет каждой группе пользователей необходимый инструментарий для решения этой задачи. Так, интегрированные в Office и Windows средства самообслуживания позволяют бизнес-пользователям без необходимости обращения в службу внутренней технической поддержки сбрасывать свой пароль или PIN-код доступа к смарт-карте, создавать списки рассылки или добавлять других пользователей в рабочие группы. А с помощью портала самообслуживания FIM пользователи могут обновлять собственный профайл.

ИТ-специалисты могут управлять удостоверениями и учетными записями пользователей с помощью консоли управления, построенной на портальных технологиях SharePoint®. Таким образом, ИТ-отдел может использовать привычный интерфейс консоли управления для создания групповых политик и рабочих процессов, которые объединяют вопросы управления учетными записями пользователей и их правами доступа к информационным ресурсам компании. Что касается разработчиков, то они получают возможность использовать программный интерфейс к Web-сервисам и скриптам на базе платформы .Net для кастомизации функционала FIM с использованием привычной среды разработки Microsoft Visual Studio® и платформы .Net.

Автоматизация бизнес-процессов и снижение рисков

Автоматизация бизнес-процессов, которую обеспечивает FIM, наряду с самообслуживанием пользователей помогает не только сократить высокую стоимость, которая обычно присуща системам управления удостоверениями и доступом, но также снижает возможные риски. Так, FIM предоставляет единую точку (портал) для управления учетными записями, хранящимися в различных сетевых операционных системах, системах электрон-

ной почты и порталах совместной работы, базах данных, службах каталогов и в приложениях. Это обеспечивает легкую интеграцию разрозненных систем хранения учетных записей пользователей в рамках корпоративной инфраструктуры.

FIM также увеличивает отдачу от уже сделанных инвестиций в существующую инфраструктуру благодаря упрощению процессов управления учетными записями в существующей корпоративной инфраструктуре, включая такие службы, как Active Directory® Domain Services, Microsoft Exchange, а также Active Directory Certificate Services. Кроме того, возможность интеграции с привычными средствами разработки, такими как Visual Studio и .Net, облегчают кастомизацию системы управления учетными записями.

Соответствие нормативным требованиям

Возможности FIM по обеспечению безопасности и соответствию принятым в компании нормативам (включая государственные и отраслевые стандарты и регламенты) в области управления и аудита учетных записей, прав доступа и информационных ресурсов включают:

- обеспечение защиты информации в корпоративной инфраструктуре благодаря интеграции систем управления учетными записями, удостоверениями и правами доступа пользователей. ИТ-служба может использовать единую систему управления политиками для управления пользователями, их правами доступа и информационными ресурсами, а также удостоверениями, включая удостоверения для строгой аутентификации;
- модель предоставления и делегирования прав для увеличения управляемости и снижения рисков. Например, ИТ-служба может делегировать права на создание групп и управление членством в группах конечным пользователям просто назначив такую политику в любой момент для таких групп;
- возможность проведения аудита системы на предмет соответствия принятым политикам и регламентам. Специальное средство управления политиками дает возможность владельцам компании и ИТ-департаменту проводить проверку заданных правил выполнения рабочих процессов и событий, сгенерированных FIM, а также внедрить автоматическое выполнение правил и политик, которые обеспечивают соответствие принятым нормативам и регламентам.

Управление политиками

FIM устанавливает основные рабочие процессы для автоматизации и интеграции всех вопросов управления учетными записями, удостоверениями и доступом пользователей таким образом, что в рамках всей корпоративной инфраструктуры используется единый набор правил и политик. Это достигается благодаря централизации процессов создания, применения и аудита политик. ИТ-администраторы могут управлять политиками, которые объединяют пользователей и группы пользователей с помощью удобной консоли управления, построенной на развитой системе меню и шаблонов. В результате значительно снижается риск несоответствия политик принятым в компании нормативам и регламентам. Используя расширяемую платформу для построения типовых рабочих процессов Windows Workflow Foundation, ИТ-специалисты могут подтверждать создание учетных записей, делегирование задач и другие типовые процессы. Что очень важно — эти процессы могут быть легко доработаны для создания сложных сценариев, ориентированных на используемые в данной конкретной компании бизнес-процессы.

Управление удостоверениями

FIM включает все системы управления удостоверениями как для администраторов, так и для конечных пользователей с помощью:

- управления жизненным циклом сертификатов, которое интегрировано с провизионингом;
- централизованного управления различными типами удостоверений и сертификатов, таких как УЦ Microsoft и УЦ других вендоров.
- синхронизации паролей между различными системами. Это позволяет реализовать систему единого входа (Single Sign-On);
- встроенных в ОС семейства Windows интуитивно понятных средств, которые позволяют пользователям сбросить свой пароль или PIN-код, а также управлять сертификатами на своей смарт-карте.

Управление учетными записями

FIM предоставляет средства для более эффективного процесса создания и удаления учетных записей и прав доступа пользователей. Эти средства включают:

- Развитые средства создания пользовательских учетных записей и назначения им прав доступа. Автоматизированное управление этими процессами обеспечивается в основном через готовые формы пользовательского интерфейса и портала, без необходимости написания отдельных программных скриптов/модулей;
- Интегрированная система создания учетных записей, удостоверений и ресурсов общего доступа. С помошью FIM ИТ-специалисты могут создавать политики, которые определяют все процессы создания и удаления соответствующих учетных записей, удостоверений, сертификатов и прав доступа;
- Типовые средства самообслуживания для конечных пользователей. Теперь можно устанавливать политики, разрешающие пользователям обновлять информацию в своем профайле, например номер своего рабочего телефона. Также можно настроить автоматическую отправку уведомлений о таких изменениях. Помимо этого на портале самообслуживания пользователям доступны развитие средства поиска информации, например, для поиска других сотрудников своей организации.

Управление группами

Средства управления группами, встроенные в FIM, помогают увеличить эффективность работы пользователей, освобождая ИТ-специалистов от повторяющихся рутинных операций по управлению учетными записями и правами доступа пользователей. Эти средства обеспечивают расширенную безопасность и соответствие принятым нормативам и регламентам. Например, средства самообслуживания пользователей, встроенные в приложения семейства Microsoft Office и портал SharePoint, обеспечивают возможность управлять запросами других пользователей на членство в группах и списках рассылки, используя привычный интерфейс, включая возможность подтверждения таких запросов в режиме offline. ИТ-служба может использовать консоль управления FIM для создания политик, которые обеспечивают автоматическое обновление информации о членстве пользователей в группах и списках рассылки.

Экспертное мнение

Сегодня актуальность темы IdM ни у кого не вызывает сомнений. Большинство крупных компаний, осознавая важность и практическую пользу от подобных систем, планируют внедрить или уже реализовывают проекты по их установке. Одной из них стала и компания ТНК-ВР – третья крупнейшая нефтяная компания России, признанная лауреатом премии «IT-ЛИДЕР 2010»[1] в номинации «Нефтегазовые компании». Мы обратились в компанию ТНК-ВР с просьбой поделиться своим экспертным мнением по этой теме, и на вопросы нам ответил директор департамента бизнес-информации и службы заказчика ТНК-ВР Степан Масленников.

JI: Как Вы оцените актуальность тематики Identity Management?

С.М.: В настоящее время внедрение IdM-систем становится все более актуальным. Современные продукты Identity Management позволяют комплексно решить задачу управления жизненным циклом учетных записей сотрудников Компании в ИТ-инфраструктуре организации путем построения централизованной системы управления доступом. Подобное решение эффективно не только для ИТ и ИБ-подразделений компании, но и для бизнес-пользователей, т.к. позволяет значительно сократить время предоставления доступа к информации и повысить прозрачность процесса согласования запрашиваемого доступа.

JI: В чем Вы видите преимущества подхода Identity Management для российских компаний?

С.М.: Внедрение IdM-решений для российских компаний дает сразу ряд преимуществ. Во-первых, IdM становится платформой, объединяющей все основные корпоративные информационные системы как российского, так и зарубежного производства (в том числе заказные разработки), что в свою очередь позволяет осуществлять централизованное управление доступом в них. Во-вторых, внедрение такой системы позволяет повысить доверие со стороны западных партнеров и инвесторов, а также обеспечить соответствие ряду российских и международных законодательных актов.

JI: Какие преимущества дает данная система группе компаний ТНК-ВР?

С.М.: В группе компаний ТНК-ВР внедрение IdM позволило сократить временные потери, связанные с простоем в работе бизнес-пользователей при создании учетных записей и получении доступа к информационным ресурсам. Была обеспечена быстрая блокировка доступа к системам для сотрудников, уволившихся из компании, а также автоматизированы процессы жизненного цикла учетных записей (создание/модификация/блокировка/ удаление) для ИТ-систем.

В ходе проекта был внедрен единый процесс внутреннего контроля и управления доступом к системам. Мы получили возможность предоставления отчетности для аудита и проверки соответствия нормам — «кто к чему имеет доступ», «кто что сделал» и «кто что подтвердил и проверил». К тому же был создан Уникальный Персональный Идентификатор (UPID) пользователя, который позволил повысить точность аллокации ИТ-затрат по управляемым системам компании.

Помимо этого был создан единый каталог пользователей ИТ-ресурсов и единый каталог информационных ресурсов компании, а также персональная история прав доступа пользователей к информационным ресурсам Компании. Все это позволило создать единую общекорпоративную систему управления идентификацией и доступом с возможностью дальнейшего подключения к ней остальных систем.

1 Национальная ежегодная Премия «IT-ЛИДЕР» проводится с 2002 года и является единственной отраслевой премией рынка информационных технологий в России.

О ЧЕМ МОЛЧАТ ПРОЕКТИРОВЩИКИ

Стандартизация ЦОД

Сергей Андронов,
директор департамента проектирования, внедрения и сопровождения компании «Инфосистемы Джет»

Говоря о стандартизации, мы подразумеваем соответствие продукта либо решения определенным нормам и правилам. Это понятие универсально и может быть применено к любому виду ИТ-деятельности. В данном случае речь пойдет о стандартизации центров обработки данных. И прежде, чем начать разговор на эту тему, стоит немного разобраться в ситуации на рынке.

Там, где «живет» ЦОД...

На развитие рынка центров обработки данных в России влияет определенный набор факторов. К таковым можно отнести: интеграцию российского рынка в мировую экономику; рост интернет-трафика; увеличение числа национальных проектов и государственных программ, направленных на цодостроение; требования бизнеса к непрерывности работы систем (что сегодня является конкурентным преимуществом).

Все эти факторы, с одной стороны, влияют на развитие рынка, с другой — воздействуют на сами технологические и архитектурные приемы, которые применяются при строительстве ЦОД. Есть еще третья сторона — все перечисленные выше параметры влекут за собой необходимость стандартизации подходов на всех уровнях цодостроения: архитектурном, структурном уровне, на более низких технологических уровнях — протокольных и аппаратных и т.д. И как раз с этим связана основная проблема — сегодня в мире существует только один стандарт по строительству ЦОД — TIA/EIA-942. Он описывает требования к инженерной инфраструктуре на архитектурном уровне без глубокой детализации. Это приводит к возникновению проблем в технологических аспектах, связанных с отсутствием всеобъемлющих норм, пронизывающих все уровни архитектуры Дата-центра. К тому же все это тормозит развитие всей сферы.

Технологические проблемы стандартизации

Чтобы разобраться в сути возникающих на данном этапе проблем, нужно понимать, что в глобальном смысле архитектура ЦОД состоит из ряда уровней: аппаратного и программного. В то же время базовыми системами, которые обеспечивают непрерывность работы самого оборудования, являются: обязательные системы электроснабжения и климатики, системы информационного обмена между серверным оборудованием, мониторинга и контроля инженерных систем Дата-Цент-

ра и т.д. Однако из всех этих инженерных систем мы выделим те, которые обеспечивают информационный обмен, так называемые связные системы. Основная причина этого – дефицит в информационной составляющей ЦОД. Применяемые в этой части технологии себя давно исчерпали. Поэтому одной из основных задач развития рынка ЦОД сегодня является разработка технологических стандартов, которые направлены на повышение скорости передачи данных, а также на интеграцию различных технологий поверх Ethernet.

В этом направлении уже сейчас ведется активная работа, создано не малое количество документов, которые должны помочь в решении этих проблем. Среди них:

1. The Priority-based Flow Control (PCF)
2. The Enhanced Transmission Selection (ETS)
3. The DataCenter Bridging eXchange
4. IEEE 802.1aq shortest Path Bridging (IEEE 802.1aq)
5. IETF Trill (Computer Networking) (TRILL)
6. IEEE 802.1p/Q
7. IEEE 802.3x

К сожалению, некоторые из них утверждены лишь на уровне драфтов, в то время как другие находятся в стадии разработки, на уровне группы IEEE[1].

Критерии оценки ЦОД

Помимо отмеченной выше тенденции существует определенная неразбериха с точки зрения технологических подходов в построении различных компонент комплекса инженерных систем ЦОД. Рассматривая тему стандартизации, следует уделить внимание вопросу, по каким вообще параметрам можно оценить ЦОД? По большому счету их не так много.

Во-первых, это оценки с точки зрения отказоустойчивости (отказоустойчивости именно всего комплекса, а не отдельных компонент).

Во-вторых – стоимость эксплуатации. В случае высоких эксплуатационных расходов, мы можем превратить хороший, правильно построенный и эксплуатируемый, достаточно надежный ЦОД в предприятие, которое не приносит прибыли. Такие ошибки часто происходят в том случае, если заказчик ориентируется на стоимость инженерных систем, выбирая дешевые решения, которые уже давно находятся в производстве. У любой системы есть свой конечный цикл жизни технологических решений. А значит, придется затратить дополнительные средства на обслуживание именно таких устаревших систем (оплата специалистов, комплектующие). В итоге, построенный ЦОД из-за высоких накладных расходов становится нерентабельным. Он превращается в якорь, который препятствует развитию компании.

Следующий показатель – энергоэффективность, который во всем мире по значимости давно является номером один. В России же в этом вопросе своя специфика – у нас не привыкли рассматривать критерий энергоэффективности как критерий. Именно поэтому отечественными компаниями зачастую внедряются довольно энергоемкие решения, которые изначально лишают ЦОД возможности масштабирования. Итог – хороший бизнес достаточно рано консервируется.

И последний, но не менее важный параметр – оценка ЦОД с точки зрения его соответствия стандартам. Ему мы уделим особое внимание, поскольку он является ключевым вопросом нашего разговора. До 2000-х годов существовал только один нормативный документ – «Строительные нормы и правила» (СНиП 512-78), разработанный в 1978 году. Он содержит строительные рекомендации к помещениям и зданиям для размещения вычислительных машин. Безусловно, в нем заложены правильные азы, но исходя из современных параметров оценки Дата-центров, их нужно кардинально пересмотреть. СНиП не затрагивает архитектурно-технологическую часть инженерных систем и является общим документом с точки зрения ландшафтных решений. Он не удовлетворяет всем запросам в части реализации таких проектов.

Во второй половине 2000-х годов появился новый стандарт – TIA/EIA-942. Стоит отметить, что создатели этого документа – первопроходцы в данной области, и его положения написаны, в первую очередь, исходя из структурно-архитектурных требований к комплексу инженерных систем (и каждой инженерной системе отдельно).

В итоге получается, что СНиП – это совсем «высокоуровневый» документ, TIA/EIA-942 – среднее звено, а все что ниже (протоколы, технологические решения) – отдается на усмотрение различным вендорам, которые на основе этих тре-

1 **Институт инженеров по электротехнике и радиоэлектронике – IEEE** (англ. *Institute of Electrical and Electronics Engineers*) (I triple E – «Ай трайпл и») – международная некоммерческая ассоциация специалистов в области техники, мировой лидер в области разработки стандартов по радиоэлектронике и электротехнике.

бований разрабатывает свои протокольно-технологические решения для своего оборудования.

Вендоров много, все хотят быстро застолбить за собой лидирующие позиции в области технических решений Дата-центров, и часть из них, начиная играть на рыке ЦОД, не отвечает в полной мере тем технологическим требованиям, которые они должны обеспечивать. Нет четких границ на этом уровне — по архитектуре решение соответствует всем прописанным нормам, а вот технология «плавает». Например, каждый вендор трактует реализацию схемы резервирования (N+M), исходя из конструктивных особенностей своего оборудования, порой не замечая «узкие» места в своих системах. Отсюда широкое поле для трактовки стандарта и предложений вендоров, и как итог — вероятное возникновение ошибок на завершающих этапах работ.

Правда, вендор отвечает исключительно за свою технологическую часть (система климатики, мониторинга..), т.е. за продукт, который не является законченным решением для построения ЦОД[2]. И здесь возникают следующие участники рынка — интеграторы, которые должны обладать достаточной компетенцией по оборудованию вендоров и опытом создания комплекса инженерных систем на базе технологических решений. Интеграторы также в свою пользу трактуют стандарты, ориентируются на определенный перечень вендоров, с которыми им удобно работать. В результате всех этих процессов вероятность ошибки возводится в степень. Очень часто интегратор сталкивается с ситуациями, в которых возникает необходимость сопрячь то, чего он раньше не сопрягал. Эти задачи лежат в сфере новых технологий, более технологичных систем. Без соответствующих инструкций и опыта очень тяжело выполнить подобные работы. К тому же, впоследствии может оказаться, что построенная система не будет соответствовать заявленной в техзадании заказчика, что непременно выявит сертификационный аудит и заказчик «попадет» на штрафы или доработки.

Например, в климатике нет четкого представления о том, когда использовать ту или иную технологию — нет экспертного заключения, что при такой-то мощности потребления на одну стойку нужно строить системы с изолированными холодными коридорами для кондиционирования. Или применяя решения вендора для вентиляции, многие не задумываются, насколько в нем проработана система мониторинга на уровне требуемых протоколов. Может оказаться, что данная система предоставляет недостаточно информации для ее использования.

Фактически решение подобных вопросов целиком и полностью отдается интегратору. Это означает, что вы доверяетесь специалистам и надеетесь, что благодаря своим высоким компетенциям, о которых они рассказывали на этапах подготовки к проекту, вас не обманут и сделают все правильно.

И это лишь часть общей проблемы. Мало того, что нет стандартов на технологии, нет стандартов на квалификацию конечного исполнителя — интегратора. Вендор может выдвигать требования по сертификации специалистов, но в случае мультивендорного решения у интегратора разрозненный набор сертификатов, который никак не подтверждает тот факт, что он может выполнять работы мультивендорного строительства. Ведь это разные специалисты, у которых могут полностью отсутствовать компетенции в смежных областях. Они могут четко отрабатывать свою линейку, но допускать ошибку в интеграционных моментах.Для контроля реализации подобных задач в идеале существует институт ГИП (главный инженер проекта), но и он с точки зрения ЦОД также не стандартизирован.

К тому же, нет единого стандарта о том, какое количество сертифицированных специалистов должно быть у интегратора и по каким критериям они должны быть сертифицированы, какими квалификациями обладать, какими сертификатами все это должно быть подтверждено. Это касается как узконаправленных специалистов, так и специалистов уровня ГИП. Заказчик выбирает интегратора по маркетинговым соображениям: по количеству реализованных проектов, по опыту работы. Он верит ему на слово, поскольку нет формального механизма, позволяющего определить, что согласно мировым стандартам этот интегратор подходит именно под его задачи.

Мне кажется, что для решения этих проблем не хватает единого образовательного органа, занимающегося сертификацией. Такая организация должна выдвинуть требования, позволяющие определять, что строить ЦОД нужно только с теми поставщиками или интеграторами, которые имеют определенный класс по данному виду деятельности. Без создания подобной структуры очень скоро грянет «кризис жанра». Все будут строить по принципу: «кто в лес, кто по дрова»...

И если представить, что Россия войдет в ВТО, можно считать, что «кризис жанра» уже наступил. На рынок придут крупные мировые ин-

2 Речь идет не о моновендорных решениях

теграторы, и с точки зрения российского ИТ-бизнеса произойдет коллапс. Когда дело дойдет до аудита, окажется, что 90% всего, что построено отечественными компаниями, не соответствует заявленному. Уже сегодня, например, 99% ЦОД не соответствуют заявленному Tier. А для заказчика это означает повторные инвестиции, переделки и разочарования.

Аудит – вопросы соответствия

Есть сейчас в мире услуга, которая позволяет вам, привлекая коммерческие организации, провести оценку вашего ЦОД на соответствие стандарту TIA/EIA-942 по параметрам, разговор о которых шел выше. Есть известные мировые аудиторы, которые могут провести такую оценку, но по целому ряду причин они с большой осторожностью относятся к таким работам и не спешат предлагать данную услугу на российском рынке. Например, одной из таких компаний является **Uptime Institute**, который занимается сертификаций уже построенных ЦОДов, относя их к определенному классу надежности. Так как сертификация проводится уже готового проектного решения, невозможно в процессе строительства проверить правильность его реализации и исправить недочеты до завершения работ. В итоге — очень часто при прохождении аудита выясняется, что ваш ЦОД не соответствует заявленному классу. А приглашать Uptime Inst. во время строительства довольно дорого, да и сотрудников компании на всех не хватит. На рынке аудиторов, безусловно, есть и более мелкие игроки, которые готовы провести аудит, правда достоверность таких работ не всегда вызывает доверие.

При таком положении дел велика доля разочарований со стороны заказчиков. Отличный пример тому — классификация надежности ЦОД в России. Общемировая практика такова, что готовый Дата-центр согласно стандарту сертифицируется по четырем классам надежности — 1,2,3,4 Tier (4 — самый надежный). А вот в России ряд компаний предлагает сертификацию по классу 3+ или 4-. При этом не понятно, что лучше: 3+ или 4-. Таким образом, происходит некая фальсификация соответствия построенного решения заявленному. В стандарте четко прописано, что не существует никаких дробных делений по классам надежности, кроме указанных четырех. Такое положение дел рано или поздно приведет к всеобщей неразберихе и большим разочарованиям.

Специфика российского рынка

В силу сложившейся ситуации возникает довольно очевидный вопрос: что делать? И какой выход из положения может быть, если он вообще существует?

Решение этого вопроса может идти по следующему пути. Есть целый пласт решений на рынке — моновендорные системы. Их не так много и они не так разнообразны с точки зрения применяемых технологий, как мультивендорные. Но предложения по стандартизации, пронизывающей все уровни представления систем ЦОД, скорее всего, должны появиться и начать применяться именно на моновендорных решениях (что уже и происходит). Такими системами занимаются мировые компании, которые имеют имя и технологическую базу. Они реализуют полный комплекс систем, из которых состоит ЦОД, у них есть специалисты, есть организационная структура, у них есть представление о том, как это все должно быть устроено. Поэтому и требования, вероятно, придут именно из той сферы, они станут «законодателями мод».

Однако специфика отечественного рынка заключается в том, что, несмотря на большое количество на мировом рынке моновендорных решений, они остаются для отечественных компаний достаточно дорогими. И совершенно не важно, решения какого вендора рассматривать. По этой причине большинство заказчиков идут по пути мультивендорного применения оборудования, работы по построению которых выполняет интегратор, сталкивающийся с проблемой сопряжения разных инженерных систем в рамках одного ЦОДа.

При этом есть еще одна особенность отечественного рынка — все факторы, о которых сказано выше, заставляют строителей Дата-центров рассматривать задачу в достаточно узких рамках. Заказчик, не видя альтернативных примеров, рассматривает реализацию своего проекта по образу и подобию того, что уже построено. С другой стороны, интеграторы также не предлагают ничего нового. На самом же деле поле для реализаций здесь довольно широкое. Строительство крупных

ЦОД нужно рассматривать вместе со смежными ИТ и инженерными системами окружения. В этом случае экономию и параметры оценки ЦОД можно значительно повысить за счет того, что определенный возвратный продукт работы Дата-центра будет применен для окружения (среды, в которой построен ЦОД). Например, никто не задумывается об эффективном использовании тепла от ЦОД. Сегодня существует большое направление реверсивных технологий, которые позволяют использовать тепло от Дата-центра для отопления рядом стоящих помещений и наоборот. Т.е. отказываясь от таких решений, изначально в архитектуру ЦОД закладывается не самое эффективное его использование.

Особенно хорошо это прослеживается в регионах, поскольку локальные интеграторы не берутся за реализацию новых, более высокотехнологичных решений. Если возникает необходимость в реализации подобного проекта, региональные интеграторы привлекают в помощь московских, поскольку у них есть хоть какая-то сертификационная база и опыт работ. Создается симбиоз – московский подрядчик и локальные субподрядные организации. Как показывает практика, такая связка в большинстве случаев порождает большое количество переделок. Правда, для заказчика, в случае мелких огрехов, это может быть не заметно. Но могут быть и серьезные ошибки, которые приводят к существенному увеличению сроков проекта и его стоимости.

Для того, чтобы этого избежать, нужно четко понимать, что может ожидать заказчика в региональных проектах. Во-первых, необходимо определить, как будет построена работа, кто будет отвечать в случае ошибок и дополнительных накладных расходов, какие существуют стадии работ с точки зрения этапности, что из них наиболее критично. Именно такие критичные работы должны выполнять сертифицированные специалисты. Конечно, это повышает себестоимость проекта, но быстро, дешево и хорошо не бывает. Есть ряд ошибок, связанных с капитальными затратами, которые могут быть допущены неквалифицированными специалистами. Одно дело неправильно смонтировали патч-панель, которую можно просто «перешить», при этом расходы минимальные. Совсем другое – испортить оборудование, стоимость которого несколько сотен тыс. долларов.

Таким образом, тема стандартизации в этом ракурсе становится как нельзя более наглядной. В таких проектах как раз и помогли бы единые нормативные подходы, которые затрагивали бы все сферы деятельности построения ЦОД, не только с точки зрения технологии и архитектуры, но и технологического цикла организации работы: проектирование, монтаж, эксплуатация и т.д. Это повысило бы уверенность заказчика в результате проекта и помогло бы избежать больших накладных расходов.

Итого, в сухом остатке...

На сегодня в мире сложилась непростая ситуация: аудиторы есть, стандарт есть, не хватает только промежуточного звена – сертификационного института, который бы и занимался вопросами квалификации и сертификации сотрудников компаний, строящих Дата-центры. Даже прочитав стандарт и имея узкоспециализированных инженеров, возможно и вероятно возникновение ошибок при строительстве ЦОД.

Я думаю, что должна быть создана некоммерческая организация, которая возьмет на себя ответственность за реализацию такого проекта, которая сможет ввести стандартизацию компаний, разграничить их по квалификациям. Необходимо создать систему, при которой компании классифицировались бы по видам работ, на которые у них есть сертификаты и лицензии. Это означало бы, что интегратор понимает, что такое класс надежности и имеет опыт тех или иных работ. Проблема только в том, что все это требует серьезных научных разработок и в целом не принесет быстрый коммерческий эффект. Возможно, именно это на сегодняшний день и тормозит весь процесс.

На мировом рынке уже сейчас есть несколько течений, которые выдают определенный набор сертификатов. Т.е. можно говорить о том, что дело медленно сдвинулось с мертвой точки, и отечественным компаниям нужно активнее включаться в этот процесс. Но при этом в отсутствие единого центра ответственности всегда встает вопрос выбора правильного направления. Единственное, что можно посоветовать на данный момент – не промахнуться в выборе стандартов и партнеров. Все сводится к тому, что Россия рано или поздно войдет в общие для всех процессы глобализации. И когда это произойдет, нам придется соответствовать общемировым требованиям – предпринимать какие-то шаги будет уже поздно. Позаботиться об этом нужно уже сейчас, поскольку дальнейшее развитие событий может быть стремительным и разрушительным для тех, кто вовремя не успел.

Не так давно центр информационной безопасности компании «Инфосистемы Джет» подвел итоги своей работы за прошлый год. И сегодня нашим собеседником стал Игорь Ляпунов, директор ЦИБ, который рассказал, какими результатами завершился 2009 г. для центра информационной безопасности.

JI: Какие наиболее интересные и перспективные проекты были реализованы в ушедшем году?

И.Л.: В этом вопросе нужно уточнить следующее: есть направления, которые развивались благодаря драйву регуляторов, а есть те, которые мы сознательно развивали. К таковым можно отнести системы управления доступом и системы мониторинга.

В прошедшем году специалисты центра информационной безопасности реализовали пять масштабных проектов по направлению **Identity Management**. В количественном выражении это позволило увеличить объем выручки по направлению IdM более чем в два раза. И такой результат неудивителен и даже вполне закономерен, поскольку в период экономической нестабильности дорогие решения, имеющие просчитываемую окупаемость и очевидный эффект для бизнеса, становятся весьма востребованными.

Что касается **Security Operations Center (Центр оперативного управления ИБ)** у нас более чем в три раза выросло число проектов. Эти решения позволяют радикально увеличить уровень информационной безопасности в компаниях с высокой насыщенностью традиционными средствами ИБ за счет более четкого контроля и управления инцидентами безопасности, конфигурациями и уязвимостями.

JI: Прошлый год для многих компаний стал тяжелым испытанием. Как непростая экономическая ситуация отразилась на ваших планах и задачах? Все ли удалось?

И.Л.: В сложном 2009 году мы ставили перед собой несколько целей. Основными внутренними целями были сохранение команды, развитие экспертизы по ключевым направлениям деятельности, внешними – удержание рыночных позиций по объему контрактов, рост количества новых заказчиков. В целом год для центра информационной безопасности закончился хорошо. И по его результатам можно уверенно сказать, что с поставленными задачами мы справились.

Итоги года центра информационной безопасности компании «Инфосистемы Джет»:

- заключено 348 контрактов, в рамках которых реализовано 137 комплексных проектов в компаниях России и СНГ, представляющих многие сектора экономики;
- в течение года специалисты компании вели одновременно более шестидесяти проектов, а к концу года количество параллельно идущих проектов вплотную приблизилось к сотне;
- количество уникальных заказчиков за прошедший год составило более 190 (для сравнения, в 2008 году их было около 150). Среди заказчиков: практически все нефтедобывающие компании России, десятки банков из списка ТОП-100, крупнейшие страховые компании и другие;
- доля работ в проектах (консалтинг, проектирование, внедрение и т.п.) составила более 60% по сравнению с 35% в 2008.

JI: Чем по итогам года центр информационной безопасности может гордится?

И.Л.: С моей точки зрения, сами результаты работы ЦИБ за год уже повод для гордости. Но если говорить о достижениях, которые были отмечены не только нами, но и участниками рынка, то по итогам 2009 года компания «Инфосистемы Джет» показала лучший результат по продажам Cisco IronPort C (Best Sales Winner). Кроме того, компания заняла первое место по объему продаж и по количеству успешно завершенных проектов на базе технологий компании Blue Coat на территории России — такие результаты мы демонстрируем второй год подряд. Все это позволило нашей компании получить самые высокие партнерские статусы в РФ: Cisco IronPort Gold Partner и Blue Coat Premier Partner.

JI: Изменился ли рынок услуг ИБ в 2009 году? Какие направления занимали лидирующие позиции?

И.Л.: На мой взгляд, тенденции рынка ИБ в 2009 году определялись двумя факторами: сложными экономическими условиями и усилением давления на рынок со стороны регуляторов. Следствием этого стало кардинальное и очень резкое изменение рынка ИБ, структуры спроса и предложения. В начале года «отпали» все услуги и решения, имеющие слабую практическую направленность. В значительной степени перестали быть востребованными большие инфраструктурные решения, целью которых было повышение общего уровня ИБ вообще. Но при этом сохранился интерес к направлениям по оптимизации и повышению эффективности существующих решений, закрытию конкретных угроз информационной безопасности. Образовался высококонкурентный рынок услуг по удовлетворению требований регуляторов: защита персональных данных, PCI DSS, СТО БР.

JI: Если говорить о лидирующих направлениях, каковы результаты компании «Инфосистемы Джет » в этой области?

И.Л.: Одним из флагманов ушедшего года стало направление систем **защиты персональных данных** (ЗПД). В течение года стартовало более 50 проектов, в реализацию которых было вовлечено порядка 40 специалистов компании. Кроме того, в настоящее время продолжаются проекты в 42-х организациях. Во всех проектах нашей компании по ЗПД мы приводим организации в соответствие с нормативными требованиями Закона «О защите персональных данных», при этом акцент делается именно на обеспечение фактической защищенности персональных данных заказчика.

Нельзя не отметить проекты по **PCI DSS**. Нужно сказать, что еще в 2008 году компания «Инфосистемы Джет» получила статусы Approved Scanning Vendor (ASV) и Qualified Security Assessor (QSA), которые создали возможности для проведения работ в этом направлении. И в 2009 году было реализовано уже более двух десятков проектов. Нашей компанией были выданы одни из первых в России сертификатов на соответствие стандарту, в том числе одному из крупнейших процессинговых центров — Компании объединенных кредитных карт (КОКК-UCS).

JI: Ни для кого не секрет, что в ЦИБ активно ведется разработка собственных продуктов. Каковы успехи компании в этом направлении?

И.Л.: Могу сказать, что в прошлом году все заказчики стремились получить максимально возможный эффект при минимуме затрат. Собственные разработки нашей компании с этой точки зрения пришлись как нельзя кстати.

Наибольший рост среди таких направлений показала борьба с утечками конфиденциальной информации, так как в условиях экономической нестабильности и резкого падения лояльности персонала этот вопрос приобрел особую актуальность. По итогам года наша компания удвоила количество проектов по системам **контроля коммуникаций и DLP**, в которых были применены собственные разработки компании — продукты «Дозор-Джет» и WebMail, общее количество инсталляций которых в России превысило две сотни. К тому же были реализованы проекты с использованием технологии вендоров, например, были сделаны первые проекты на технологии Symantec DLP.

Для телекоммуникационных компаний особенно актуальными в прошлом году были задачи по снижению уровня мошенничества в сетях и повышению корректности расчетов с клиентами и присоединенными операторами — **системы Fraud Management & Revenue Assurance (FMRA)**. Однако востребованным стали не большие дорогостоящие системы, а точечные решения, «закрывающие» наиболее актуальные источники потерь доходов. Отметив, что интерес к этому направлению вырос многократно, мы представили на рынок уникальную услугу — противодействие нелегальной терминации трафика. Показательным

для нас стал тот факт, что первые коммерческие проекты в этой области стартовали в кризисном году. Компанией на сегодняшний день заключен целый ряд контрактов с крупнейшими операторами связи.

JI: Итоги подведены — самое время строить планы на будущее. Каковы перспективы развития деятельности ЦИБ в 2010? Какие вы ставите перед собой задачи?

И.Л.: В 2010 году мы будем продолжать развивать все успешные начинания прошедшего года и стремиться к лидерству в наиболее интересных интеллектуально емких технологических направлениях, обеспечивающих реальную защиту бизнеса наших заказчиков.

JI: Спасибо!

НАШИ ПРОЕКТЫ

Тестирование маршрутов терминации трафика для ОАО «КОМСТАР-ОТС»

О заказчике

«КОМСТАР — Объединенные ТелеСистемы» (ОАО «КОМСТАР — ОТС», LSE: CMST) — крупнейший оператор интегрированных телекоммуникационных услуг в России и СНГ.

В Группу компаний «КОМСТАР-ОТС» входят «Московская городская телефонная сеть» (МГТС), лидер столичного рынка фиксированной связи, а также «КОМСТАР-Регионы», ведущий поставщик услуг кабельного ТВ и доступа в Интернет в регионах России. «КОМСТАР-ОТС» лидирует на рынке услуг широкополосного доступа в Интернет и интерактивного цифрового телевидения (IP-TV) Москвы.

Дочерние компании и филиалы «КОМСТАР-ОТС» работают в крупнейших регионах в 6-ти Федеральных округах РФ (Центральном, Северо-Западном, Южном, Приволжском, Уральском, Сибирском), в том числе в Московской, Рязанской областях, Санкт-Петербурге, Самарской, Саратовской, Оренбургской, Ростовской, Тюменской областях (включая ХМАО и ЯНАО), Екатеринбурге и Свердловской области, Краснодарском крае и т.д. Кроме того, «КОМСТАР-ОТС» имеет телекоммуникационные активы в Армении и Украине.

Задачи

Услуга транзита и приземления трафика на местные телефонные сети — один из основных «генераторов» дохода любого оператора связи. Тем более, такой компании как «КОМСТАР-ОТС», которая не только предоставляет местную связь в Москве (как «Комстар-ОТС», так и МГТС), но также является и оператором международной связи. При этом услуги пропуска трафика являются излюбленной мишенью для мошенников, встречающихся как среди абонентов оператора, так и среди недобросовестных интерконнект-партнеров. И те, и другие активно используют свой доступ к сетевому оборудованию оператора для того, чтобы нелегально пропускать международный трафик в телефонную сеть общего пользования (ТфОП).

Последствия данного вида фрода для оператора очевидны:

- уменьшение дохода: трафик, приходящий от местных интерконнект-партнеров, в 2-3 раза дешевле поступающего из международной сети легальным путем, а звонки абонентов вообще бесплатны;
- снижение качества связи: абоненты, «сливающие» МН-трафик, используют для этого оборудование, отнюдь не удовлетворяющее требованиям оператора к качеству;
- невозможность выполнения требований оперативно-розыскных мероприятий на сети (СОРМ), так как нелегальная терминация часто сопровождается подменой реального номера вызывающего абонента.

Для эффективной борьбы с нелегальной терминацией требуется ее оперативное выявление. «Работа» мошенников даже в течение 1-2 дней — это потери для оператора. Для пресечения таких ситуаций кроме, собственно, выявления, необходима еще и возможность собрать и предоставить доказательства фактов фрода для передачи в соответствующие службы (Роскомнадзор, ФСБ).

Решение

Единственное решение на данный момент, удовлетворяющее всем этим требованиям, — тестирование маршрутов терминации дальнего трафика. Тестовые звонки на сеть оператора связи совершаются из различных стран мира с мобильных, фиксированных, VoIP-сетей. Затем следует анализ протоколов состоявшихся соединений (CDR), который и позволяет оператору однозначно определить маршрут «попадания» в сеть каждого из тестовых вызовов. И если звонок попал в сеть ТфОП нелегальным путем — пришел от абонента самого оператора или от местного интерконнект-партнера, — то CDR этого вызова являются однозначным документальным подтверждением факта фрода.

Для того чтобы оперативно решить проблему нелегальной терминации трафика в своей сети, ОАО «КОМСТАР-ОТС» необходимо было срочно найти исполнителя, которому можно было поручить эту задачу. При выборе исполнителя «КОМСТАР-ОТС» руководствовался следующими основными критериями:

- широта охвата тестирования — чем с большего числа сетей совершаются тестовые звонки, тем больше шансов найти максимальное количество точек нелегальной терминации;
- сервис полного цикла — не просто звонки, но и последующий анализ данных и предоставление заказчику итогового отчета, содержащего информацию обо всех выявленных фактах фрода;
- технические возможности — большое количество звонков необходимо совершать в сжатые сроки, чтобы обеспечить своевременное обнаружение постоянно возникающих новых точек нелегальной терминации.

Возможность совершать тестовые звонки из более чем 70 стран и более чем 300 сетей связи; эксперты, большинство из которых являются «выходцами» из телекоммуникационных компаний и не понаслышке знакомы с различными видами фрода в этой сфере, — все это предопределило выбор заказчика в пользу компании «Инфосистемы Джет». Немаловажную роль в выборе сыграл также тот факт, что специалисты компании «Инфосистемы Джет» могут обеспечить любую необходимую интенсивность звонков — до десятков тысяч звонков в сутки.

Результат

На данный момент подписан долгосрочный контракт на регулярное тестирование, и уже получены первые плоды — за февраль-март 2010 года выявлено более 20 точек нелегальной терминации трафика в сетях «КОМСТАР-ОТС» и МГТС. Среди мошенников, или как их часто называют «фродстеров», как абоненты оператора (прежде всего, крупные организации, имеющие собственные офисные АТС, подключенные к сети МГТС или «КОМСТАР-ОТС»), так и присоединенные альтернативные операторы местной связи, действующие на территории Москвы. Прибыль, недополученная ОАО «КОМСТАР-ОТС» в случае продолжения деятельности мошенников, могла бы составить несколько десятков миллионов рублей.

«Мы считаем, что задача всех легально работающих операторов — бороться с такими правонарушителями. По нашим приблизительным подсчетам, объем «приземления» только международного трафика на московские номера в коде 495 и 499 можно оценить примерно в 60 млн. мин. в месяц, при этом только четверть вызовов из этого объема до начала нашей работы проходила легально», — отметил Владимир Малявин, директор по междугородной и международной связи «КОМСТАР-ОТС».

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю.
Редактор: Слободчикова Т.А.
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
e-mail: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати **32555**