

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 безнадёжной, 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 пользовате-

лей 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.

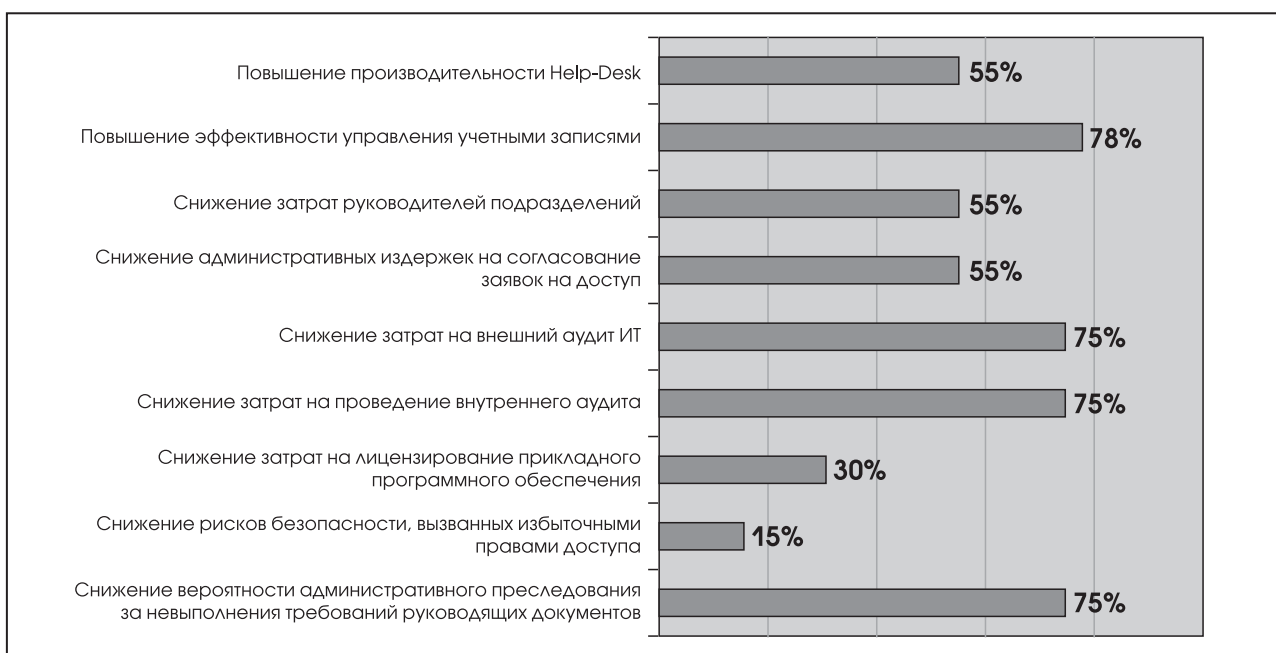


Рис. 1. Снижение затрат компании на управление информационными технологиями