

Управление доступом к IT-ресурсам компании

А.Н. СОВА,
компания "Информзащита"

"Обеспечение высокого уровня безопасности IT-инфраструктуры всегда является важной задачей. И с каждым днем важность защиты информационных систем только возрастает!" – примерно так начинается множество статей на тему информационной безопасности.

Но акценты в этих статьях время от времени меняются. Если раньше клиента приходилось убеждать в необходимости установки антивирусных средств или межсетевых экранов, то в последнее время актуальной стала тема инсайдеров. Становится все очевиднее, что внешняя защита периметра сети – важный, но далеко не единственный инструмент обеспечения информационной безопасности. Необходимо учитывать и тот фактор, что сегодня в России практически не осталось компаний, в которых не применяются информационные технологии. При этом рост информационных систем, а также увеличение количества пользователей нередко приводят к проблемам с управляемостью IT-инфраструктуры. В результате существующая в компании IT-инфраструктура не всегда способна обеспечить бизнес-процессам необходимую гибкость и устойчивость.

Для решения этой проблемы организации все чаще прибегают к использованию различного интеллектуального управляющего программного обеспечения (ИУПО). Внедрение ИУПО позволяет эффективно решать задачи управления IT-инфраструктурой и обеспечения ее безопасности в условиях гетерогенных систем. Помимо продуктов для управления ресурсами, хранением и восстановлением данных, распределением и контролем программного обеспечения, к ИУПО также относятся средства управления идентификационными данными и доступом к приложениям и информации (Identity and Access Management, I&AM).

Решения класса I&AM становятся сегодня все более востребованными, так как все чаще реальная угроза безопасности исходит от некомпетентных, либо преднамеренных действий собственных сотрудников, ставящих своей целью нанесение ущерба компании. В тоже время основные проблемы в управлении идентификацией и доступом создают как раз гетерогенные среды, в которых работает множество операционных платформ, существует немалое количество приложений и источников информации и где, соответственно, необходимо поддерживать различные типы пользователей, правила их доступа к данным и системы идентификации.

В данной статье мы более подробно рассмотрим именно системы Identity and Access Management (I&AM), осуществляющие управление учетными записями пользователей и доступом исходя из бизнес-логики.



Условно можно выделить три побудительных мотива для внедрения систем I&AM. Это так называемые "пряник" – непосредственная польза от внедрения продукта и "кнут" – угрозы, которые данный продукт предотвращает. Более подробно мы рассмотрим эти мотивы далее. Третий мотив в России стал набирать вес достаточно недавно – это требования законодательства и различных нормативных документов, регулирующих деятельность бизнес-структур.

Введение законодательного регулирования, касающегося вопросов информационной безопасности, заставило организации многих стран обратить самое пристальное внимание на проблему защиты информации. Вот лишь некоторые, из появившихся за последнее время законов и нормативных актов:

► Федеральный закон РФ "Об информации, информационных технологиях и о защите информации";

► Федеральный закон РФ "О персональных данных";

► Директива Европейского Союза о защите данных (European Union Data Protection Directive, **EU DPD**);

► Закон о преемственности страхования и отчетности в области здравоохранения (Health Insurance Portability and Accountability Act, **HIPAA**);

► Акт Сарбейнса-Оксли (Sarbanes-Oxley Act, **SOX**);

► Закон Грэма-Лича-Блилей (Gramm-Leach Bliley Act, **GLBA**);

► Международная конвергенция измерения капитала и стандартов капитала (The International Convergence of Capital Measurement and Capital Standards: a Revised Framework, **Basel II**).

Эти нормативные документы стали источниками риска для высших руководителей, в том числе и российских предприятий: теперь в случае обнаружения нарушений, даже вызванных недобросовестностью рядовых сотрудников, эти руко-

водители могут понести персональное наказание. В этих документах не указаны конкретные требования к информационной безопасности, но акцентировано внимание на том, что достоверность данных и эффективность системы внутреннего контроля напрямую зависит от эффективности системы контроля деятельности IT. Внешний аудит компаний стал охватывать не только финансовые подразделения, но также IT-инфраструктуру компаний, внутренние IT-процессы, а так же персонал IT-подразделений.

Организации просто вынуждены внедрять новые информационные продукты, которые помогут удовлетворить требованиям регулирующих норм, так как должны быть уверены, что их сотрудники не могут ни случайно, ни умышленно нарушить закон, находясь на рабочем месте. Следовательно, продукты и технологии, управляющие идентификационными данными и доступом, за-

нимают важное место в стратегии компаний по удовлетворению требований законодательных актов.

Для того чтобы понять важность внедрения систем I&AM, рассмотрим пример достаточно крупной организации, территориально распределенной и обладающей развитой IT-инфраструктурой. В такой организации действует большое количество информационных систем, к которым имеют доступ сотрудники компании, а иногда еще и партнеры, и клиенты. Естественно, доступ к информационным ресурсам должен быть строго регламентирован. Для этого необходимо регистрировать пользователей, наделять их определенными правами доступа, создавать учетные записи и поддерживать все это в актуальном состоянии. Эти достаточно рутинные задачи требуют, тем не менее, большого штата администраторов. При этом неизбежно возникновение ошибок, да и сами операции довольно длительны. Со временем накапливаются некорректные учетные записи, при увольнении сотрудников их записи удаляются с большой задержкой, а иногда так и остаются активными.

Другая проблема – сбор данных для составления отчетов и аудита. Современная IT-инфраструктура зачастую представляет собой набор "островов", сообщение между которыми весьма затруднено, поскольку наращивание шло в разное время, под актуальные на тот момент задачи, разными людьми и с использованием разнообразного программного и аппаратного обеспечения. Поэтому оперативный сбор достоверной информации в масштабах всей организации представляет весьма трудоемкий процесс. Не говоря уже о том, что по некоторым нормативным документам (например, по SOX) необходимо предоставить доказательства непрерывности контроля деятельности IT-инфраструктуры, в том числе и контроля доступа к информации.

Нельзя забывать и о пользователях, которым приходится запоминать большое количество паролей для доступа к различным ресурсам. Как показывает статистика, больше 2-3 паролей пользователь запомнить не в состоянии. Это значит, ли-

бо пароли будут записывать на листочках, и клеить на монитор, либо число обращений типа "Ой, я забыл пароль!" в службу поддержки будет возрастать. Так, по оценкам исследовательской компании Gartner, на восстановление одного пароля компания тратит, в среднем, от \$14 до \$28. По словам представителей американского оператора кабельного телевидения Cox Communications, восстановление паролей обходится компании несколько дешевле – по \$10 за каждый. Однако каждый пятый звонок 20-тысячного персонала компании в службу техподдержки касается восстановления паролей, и в месяц забывчивость служащих Cox выливается в \$70 тыс., а в год – в \$840 тыс.

Иногда компании пытаются силами собственных программистов создать автоматизированную систему управления учетными записями и доступом. Однако такие попытки, как правило, не приводят к успеху, поскольку квалификация штатных программистов недостаточна для решения подобных задач. Вкладываются значительные средства, уходит время, а эффект от применения системы незначителен. Отсюда и растущий в последнее время интерес к промышленным системам для решения этих задач. По информации аналитической компании IDC, ведущие мировые компании около 30 % своих бюджетов по инфобезопасности направляют на внедрение систем I&AM. Россия же идет в этом направлении пока с небольшим отставанием.

Исходя из вышесказанного, сформулируем основные требования к системам Identity&Access Management:

- ▶ централизованное управление жизненным циклом идентификационных данных (ИД) пользователей от найма сотрудника до его увольнения;
- ▶ автоматизация операций, связанных с администрированием ИД и доступа для снижения нагрузки на IT-персонал и устранения ошибок ручного ввода;
- ▶ обеспечение защищенной однократной аутентификации пользователей к множеству распределенных ресурсов с использованием единого идентификатора (Single Sign-On);

- ▶ идентификации, аутентификации и авторизации пользователей в соответствии с заданными политиками и ролями;
- ▶ организация единого синхронизированного хранилища информации о пользователях;
- ▶ делегирование пользователям части функций по управлению своими паролями;
- ▶ контроль деятельности привилегированных пользователей и IT-персонала;
- ▶ достоверная и актуальная централизованная отчетность, обеспечивающая готовность к аудиту в любой момент времени.

Рассмотрим реализацию системы I&AM на примере семейства продуктов Tivoli компании IBM. Программные продукты Tivoli предназначены для управления IT-инфраструктурой предприятия и обеспечения ее безопасности в условиях распределенных гетерогенных сетей. ПО Tivoli как осьминог протягивает свои щупальца ко всем значимым компонентам IT-инфраструктуры и объединяет их в единую управляемую систему. Причем речь идет не только о серверах, рабочих станциях и программном обеспечении. Tivoli способен "дотянуться" и до сетевых принтеров, и до серверных шкафов, и даже до датчиков системы пожаротушения.

Разумеется, в линейке Tivoli Security присутствуют и продукты для построения систем I&AM – IBM Tivoli Identity Manager и IBM Tivoli Access Manager.

IBM Tivoli Identity Manager (рис. 1) напрямую взаимодействует с пользователями и с системами двух внешних типов: источниками идентификационных сведений и механизмами управления доступом. Он предназначен для решения следующих задач:

- ▶ централизованное и унифицированное управление доступом в различных операционных системах и приложениях предприятия;
- ▶ организация управления учетными записями пользователей на основе политик и ролей пользователей в рамках организационных и географических образований;
- ▶ уменьшение числа ошибок, возникающих при управлении пользовательскими учетными записями

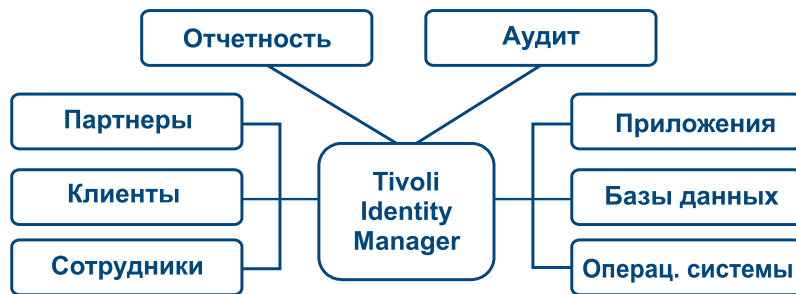


Рис. 1. Схема взаимодействия IBM Tivoli Identity Manager

вручную, путем автоматизации процессов подачи заявок на изменение учетных записей пользователей и их исполнения;

- ▶ сокращение времени выполнения заявок на внесение изменений в учетные записи пользователей, создание и удаление учетных записей за счёт автоматизации этих процессов;
- ▶ предоставление актуальной информации по пользовательским учетным данным в различных операционных системах и приложениях с помощью встроенной системы генерации отчетов;
- ▶ осуществление аудита пользовательских учетных записей для проверки выполнения корпоративных политик безопасности и предоставления доступа.

Благодаря Web-интерфейсу самообслуживания и встроенному механизму документооборота в составе Tivoli Identity Manager, пользователи могут безопасно и без труда управлять частью собственных записей, не прибегая к помощи справочной службы или IT-персонала. Используя интерфейсы самообслуживания, конечные пользователи могут сами сбрасывать пароли и выполнять синхронизацию паролей, а также модифицировать набор настраиваемых администратором индивидуальных атрибутов при помощи Web-браузера.

Процесс предоставления доступа выглядит следующим образом:

- ▶ ввод данных в отделе кадров по новому сотруднику запускает автоматизированный процесс. Администраторы и руководитель сотрудника получают уведомления о запросах на доступ;
- ▶ по заранее заданным политикам автоматически создаются учетные записи с необходимыми правами доступа;

- ▶ новый сотрудник получает почтовое уведомление о доступе в системы и может приступить к работе.

В случае необходимости получения дополнительных прав доступа, пользователь может воспользоваться стандартной процедурой и отправить запрос с обоснованием необходимости доступа. Запрос автоматически рассылается ответственным сотрудникам, и после получения от них подтверждения, необходимая учетная запись создается на ресурсе. Весь процесс предоставления права доступа может занять не более 10 минут, в то время как при обычной системе согласования, данная процедура иногда отнимает несколько дней.

В итоге у пользователя появляется набор уникальных идентификаторов со сложными паролями, созданными согласно единым правилам. Сегодня даже у рядового пользователя может быть до десяти различных идентификаторов, каждый со своим паролем. Но, как мы уже знаем, пользователь в состоянии запомнить от силы два-три пароля, да и то, если они не слишком сложные. Такое несоответствие приводит к тому, что пароли записываются на листочках или в файл, откуда их может легко извлечь злоумышленник.

Поэтому, внедрение одного только Identity Manager позволяет решить лишь часть задач, порождая при этом новые проблемы. Необходимо решение, позволяющее сотруднику помнить и вводить всего один пароль для доступа ко всем приложениям. Для этого используются системы однократной аутентификации (Single Sign-On, SSO). Использование систем SSO позволяет обеспечить пользователям безопасный и удобный доступ ко всем разрешенным ресурсам.

В системах SSO используется модель централизованного хранения учетных данных в едином каталоге и которая построена на базе технологии подстановки паролей. После успешной аутентификации пользователя данные передаются на локальную рабочую станцию, где они расшифровываются и используются для автоматического входа в различные приложения. При этом конечный пользователь может не знать текущий пароль для доступа к приложению (для ряда прикладных систем сложный для запоминания пароль может быть сгенерирован автоматически, в том числе и с использованием Tivoli Identity Manager). Все, что необходимо пользователю, что бы знать учетные данные для входа в систему (например, пароль для аутентификации в Active Directory) или иметь смарт-карту (токен) и помнить ее PIN-код.

IBM Tivoli Access Manager for Enterprise Single Sign-On (ITAM E-SSO) позволяет распознавать и отвечать на запросы паролей, поступающих практически из любой системы или приложения. Он всегда находится между пользователем и приложением. Продукт может использоваться как самостоятельно, так и в комплексе с Tivoli Identity Manager (ITIM). Это позволяет ITIM централизованно управлять учетными записями и правами доступа пользователей к ресурсам, защищаемым Tivoli Access Manager.

Для расширения базовой функциональности TAM E-SSO, возможна поставка дополнительных программных модулей (адаптеров):

- ▶ **Desktop Password Reset Adapter** – позволяет пользователям самостоятельно сбрасывать свои пароли Windows без обращения в службу поддержки;
- ▶ **Authentication Adapter** – позволяет использовать продвинутые способы аутентификации пользователей – токены, смарт-карты, биометрию и пароли;
- ▶ **Provisioning Adapter** – осуществляет интеграцию с системой управления пользовательскими записями (например, Tivoli Identity Manager, Active Directory и другое);
- ▶ **Kiosk Adapter** – осуществляет автоматическое завершение неактивных сессий и закрытие приложений для киосков и ПК общего пользования.

Помимо TAM E-SSO в семейство Tivoli Access Manager входит еще три программных продукта:

► **Tivoli Access Manager for e-business.** Это единая точка аутентификации и централизованное управление доступом на основе политик к Web-серверам, J2EE приложениям, Web-приложениям;

► **Tivoli Access Manager for Business Integration.** Мультиплатформенное средство управления безопасностью, позволяющее значительно повысить эффективность собственной среды безопасности IBM WebSphere MQ (программное обеспечение IBM, предназначенное для организации очередей и обмена сообщениями);

► **Tivoli Access Manager for Operating Systems.** Дополнительный уровень авторизации для ОС Unix/Linux вдобавок к уровню, предоставляемому самой операционной системой. Контроль действий привилегированных пользователей (root).

Решение на основе Tivoli Access Manager также позволяет снизить стоимость создания средств защиты для новых приложений, так как при его применении можно отказаться от внедрения (разработки) сложных приложений для защиты системы.

Преимущества внедрения продуктов линейки Tivoli I&AM можно проиллюстрировать на примере **LVM-Versicherungen** – одной из 20 крупнейших страховых групп в Германии и четвертого по величине страховщика автомобилей в стране. В LVM внедрена система онлайн-нового доступа к оформлению страховых полисов "**LVM Agency System**" (рис. 2), построенная на программных продуктах IBM. Система включает в себя инфраструктуру серверов и баз данных (IBM WebSphere Application Server, IBM DB2, IBM Tivoli Directory Server), средства мониторинга и управления ресурсами и событиями (IBM Tivoli Enterprise Console, IBM Tivoli Monitoring) и средство управления доступом (IBM Tivoli Access Manager for e-business).

В рамках этой системы агенты компании используют тонкие клиенты на платформе Linux для доступа к сведениям о заказчиках и изменениям контрактов независимо

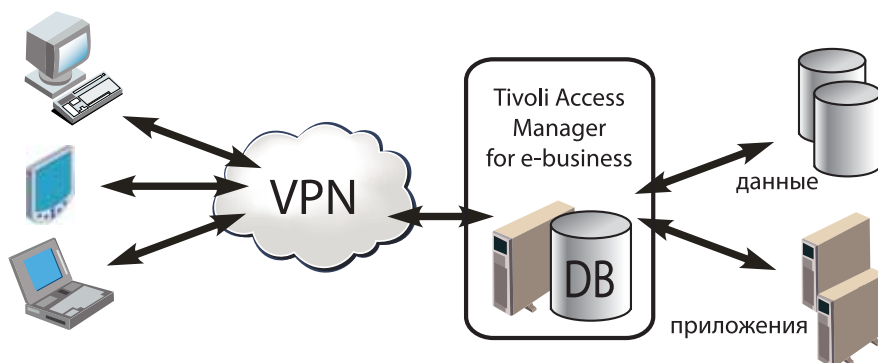


Рис. 2. Удаленный доступ с использованием TAM for e-business

от местонахождения. Агенты подключаются к системе через виртуальную частную сеть или с помощью сотового телефона с поддержкой GPRS и технологии Bluetooth. Используя систему, агенты могут гибко реагировать на потребности заказчиков. Например, агент может встретиться с заказчиком на дому вечером, внести по сети изменения в полис и мгновенно распечатать новый контракт с клиентом, чтобы подписать его до ухода. Новый полис вступает в силу в реальном времени, что экономит время и агента, и клиента.

Для этого нового решения исключительно важно обеспечение безопасности. IT-персоналу необходимо защитить конфиденциальные финансовые и личные данные, а также поставить барьер против несанкционированного доступа. Кроме того, администраторам компании необходимо управлять паролями для множества приложений, поддерживающих систему. IBM Directory Server, Tivoli Access Manager for e-business, и решение независимого поставщика для работы со смарт-картами согласованно работают, составляя надежное решение для обеспечения безопасности, помогающее LVM защитить данные по клиентам, оптимизировать администрирование и усовершенствовать связи с заказчиками в рамках компании.

TAM for e-business предоставляет вход в систему с однократным предъявлением пароля для 8000 пользователей и централизует управление защитой для HTTP запросов. Тесная интеграция Tivoli Access Manager с IBM WebSphere, Lotus Domino и DB2 позволила быстро вернуть решение с единым входом в

систему для всей IT-инфраструктуры. В результате окупаемость была достигнута в кратчайшие сроки.

Совместное внедрение Tivoli Identity и Access Manager (рис. 3) позволяет создать полноценную систему централизованного управления идентификационными данными и доступом пользователей. Внедрение системы обеспечивает:

- автоматизацию процесса управления пользователями, паролями, учетными записями в разных операционных системах, базах данных и приложениях;
- исключение возможности предоставления неавторизованного доступа или доступа с нарушениями политики безопасности;
- оперативность и отсутствие ошибок в администрировании;
- возможность действительно централизованного управления доступом ко всем информационным подсистемам и владения ситуацией о правах доступа к ресурсам ИС;
- индивидуальную идентификацию, аутентификацию и авторизацию пользователей при доступе к любым ресурсам;
- доступ пользователей к ресурсам без прохождения дополнительной аутентификации (Single Sign-On);
- соблюдение корпоративной политики в отношении ИД и доступа;
- прозрачность работы системных администраторов, службы безопасности и пользователей;
- минимальный простой пользователей из-за проблем администрирования;
- быстрое внедрение коммерческих инициатив и поддержку расширения компании с помощью набора инструментов для управления приложениями.

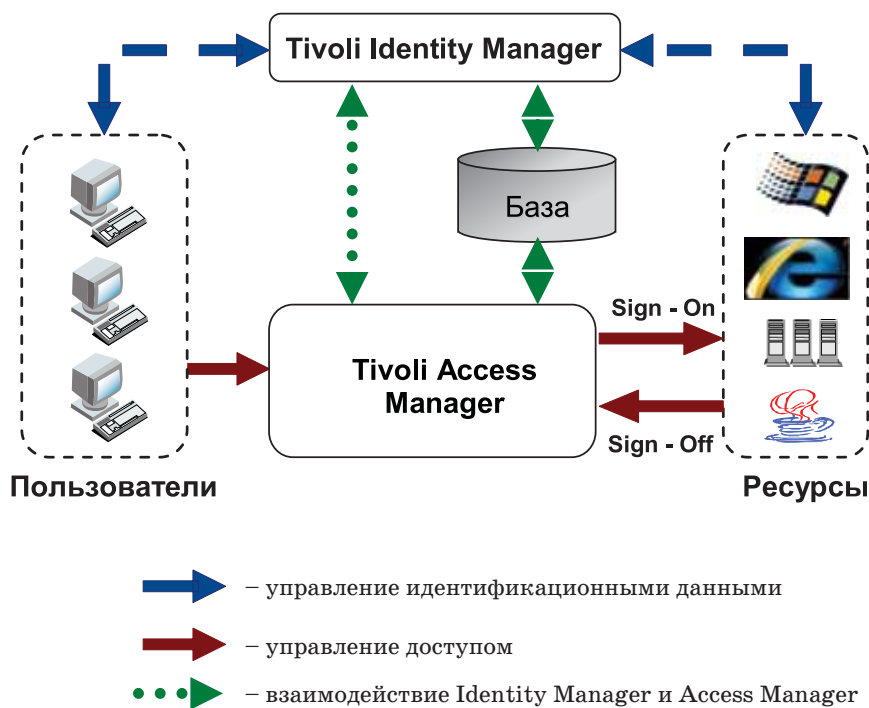


Рис. 3. Система централизованного управления ИД и доступом

Сегодня многие компании нуждаются не столько в автоматизации своей деятельности, сколько в автоматизации управления ИТ-средой компании. Согласно опросу, проведенному корпорацией Microsoft в 400 компаниях по всему миру, более половины повседневных операций, связанных с ИТ-менеджментом, выполняются вручную без применения средств автоматизации. В результате при пятилетнем цикле эксплуатации ИТ-системы свыше 60% совокупной стоимости ее владения придется на расходы по содержанию штатных администраторов. А по данным консалтинговой компании Accenture, ИТ-персонал тратит до 70% времени на поддержку существующей системы, включая управление учетными записями и паролями в разрозненных информационных системах, решение технических проблем пользователей и ручную установку обновлений.

В России увеличение спроса на системы I&AM намечилось не так давно, и хотя интерес проявляют многие большие предприятия, существует всего несколько полноценных внедрений. Во многом это обусловлено тем, что внедрение подобных технологий разительно отличается от традиционных установок "коробочного" ПО и требует,

помимо существенных материальных вложений, разработки пакета нормативно-методических документов, обеспечивающих строгую формализацию процесса предоставления доступа пользователей к информационным ресурсам. Для полноценного внедрения необходимо тесное взаимодействие ИТ-департамента, службы безопасности и бизнес-подразделений. Сегодня весьма распространенной является ситуация "необъявленной войны" между подразделениями ИТ и безопасности, когда ИТ-администраторы хотят иметь неограниченные полномочия, а администраторы безопасности всячески пытаются их урезать, но при внедрении системы I&AM обе этих службы должны работать сплоченно, прежде всего, с учетом интересов бизнес-подразделений. В данном случае система информационной безопасности тесно смыкается с корпоративной информационной системой, образуя единое информационное пространство для поддержки бизнеса. Это позволит организации интегрировать внутренние и внешние бизнес-процессы для эффективной работы с партнерами, поставщиками, клиентами. А также оперативно реагировать на запросы заказчиков, изменение рынка и различные угрозы.

Необходимо учитывать, что не всякой компании целесообразно использование подобного интеллектуального управляющего ПО. На небольших ИТ-инфраструктурах внедрение подобных программных продуктов не приведет к заметному росту эффективности, и будет скорее убыточным. Но для больших компаний или критичных подразделений без использования интеллектуального управляющего ПО практически невозможно добиться приемлемой эффективности ИТ-инфраструктуры.

Существует несколько признаков, указывающих на необходимость внедрения системы централизованного управления идентификационными данными и доступом:

► **Наличие избыточной информации о пользователях.** Пользователь имеет множество различных аккаунтов и паролей для доступа к требуемым приложениям, несинхронизированные учетные данные находятся в разных хранилищах;

► **Загруженность ИТ-специалистов рутинными задачами по работе с идентификационными данными.** Ручное создание учетных записей и изменение прав доступа, большое количество "мертвых душ" (пользователь уволен, а его учетная запись осталась), регулярные звонки в службу техподдержки с просьбой восстановить забытый пароль;

► **Несоответствие прав пользователей.** Частые обращения пользователей, обоснованно нуждающихся в дополнительных правах доступа или, наоборот, слишком расширенные права, приводящие к нарушениям политики безопасности. Ошибки и большие временные затраты при ручном назначении и изменении прав;

► **Трудоемкий процесс отчетности.** Наличие разнородных систем, большого количества ресурсов и несинхронизированных хранилищ учетных данных осложняет получение оперативной и достоверной отчетности. Это особенно критично при необходимости подтверждения соответствия требованиям законодательных актов и отраслевым стандартам.

Согласно исследованию, проведенному по заказу компании Citrix, более трети бизнес-пользователей

(35%) воспринимают работу департамента IT, как препятствие для своей деятельности, а не как одну из составляющих делового успеха. Исследование свидетельствует, что каждое обращение в службу техподдержки обходится в \$25–50, но потери от снижения производительности и недовольства сотрудников могут обойтись в несколько раз дороже.

Для того, чтобы определить необходима ли Вашей организации система централизованного управления идентификационными данными и доступом, достаточно провести внутреннее исследование – как часто пользователи обращаются в службу техподдержки с забытыми паролями, в какую сумму эти обращения обходятся в масштабах всего предприятия, сколько времени занимает сбор данных для аудита и насколько эти данные верны, как быстро новый сотрудник получает доступ к требуемым ресурсам.

После чего можно приступать к выбору качественного продукта для построения системы I&AM и компании-интегратора. И те, и другие на российском рынке уже присутствуют и готовы к внедрению.

ИННОВАЦИИ ДЛЯ ЛЮДЕЙ

БУМАЖНАЯ ПРОДУКЦИЯ



ПИСЬМЕННЫЕ ПРИНАДЛЕЖНОСТИ



НАСТОЛЬНЫЕ ПРИНАДЛЕЖНОСТИ



ТОВАРЫ ДЛЯ ДЕЛОПРОИЗВОДСТВА



МЕЛКООФИСНЫЕ ТОВАРЫ



КОМПЛЕКСНОЕ ОБСЛУЖИВАНИЕ ВАШЕГО ОФИСА

СИСТЕМЫ ХРАНЕНИЯ



СРЕДСТВА ВИЗУАЛЬНОЙ КОММУНИКАЦИИ



ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ



ОРГТЕХНИКА



ТЕЛЕФОНИЯ



DOCSYS
innovations for people

Офис: г. Москва, ул. Ивовая, д. 2/8, стр. 1
Тел./факс: +7(499)180-94-60, +7(926)603-07-47
e-mail: info@docsys.ru, <http://www.docsys.ru>