

Управление правами доступа к документам



Алексей Сова

Ведущий специалист департамента маркетинга компании «Информзащита»

Однажды я получил по электронной почте письмо от приятеля. К письму был приложен файл с проектом бюджета небольшого украинского города.

То ли и, правда, как уверял меня приятель, поработал злобный вирус, рассылавший выбранные наугад файлы всем контактам из Outlook'a, то ли он сам «окошком ошибся» и случайно отправил...

Не знаю. Факт в том, что подобные инциденты происходят часто и повсеместно.

Конфиденциальные документы отправляются не туда, выкладываются в общий доступ, бесконтрольно копируются, теряются вместе с флэшками и похищаются с ноутбуками. Одно неосторожное движение и компания теряет репутацию и клиентов, а сотрудники – работу, деньги, а иногда и свободу.

Игра в классики

Понятно, что информацию необходимо защищать. Сегодня большинство компаний так или иначе внедряют системы информационной безопасности (СИБ). Кто-то строит СИБ собственными силами, закрываясь от очевидных угроз, кто-то привлекает специализированные компании на полный цикл, включающий обследование, проектирование, поставку, пуско-наладку и сопровождение. Как правило, состав комплексной СИБ не блещет разнообразием. Система обычно включает:

- межсетевые экраны;
- средства построения VPN;
- антивирусы, антиспам и прочие продукты, противостоящие злонамеренному контенту;
- контроль доступа к данным на основе списков (ACL);
- контроль внешних носителей;
- контроль электронной почты, анализ трафика;
- программные комплексы выявления и предотвращения атак;
- средства двухфакторной аутентификации и т.п.

Таким образом компании надеются защититься от внешних и внутренних угроз. Наиболее известные внешние угрозы – это атаки из Интернета, вредоносное ПО, вирусы, спам. Из внутренних пальму первенства держат кражи информации (через e-mail, печать документов, копирование на носители), халатность служащих (неумышленное распространение конфиденциальной информации) и саботаж (уничтожение, приведение информации в непригодное состояние и т.п.). Классическая модель СИБ является неотъемлемой частью ИТ-инфраструктуры современного предприятия, стандартом де-юре и де-факто.

Но есть два серьезных ограничения, которые могут привести к утечке информации даже при наличии всех стандартных защитных механизмов (рис. 1):

- отсутствие детального контроля над действиями легитимного пользователя.
- потеря контроля над документом и его копиями за пределами периметра безопасности сети.

Это обусловлено тем, что наиболее распространенный метод построения систем защиты информации опирается на понятие периметра безопасности, а не на саму информацию. Документы и сообщения электронной почты до некоторой степени защищены, пока они находятся внутри контролируемых периметров.

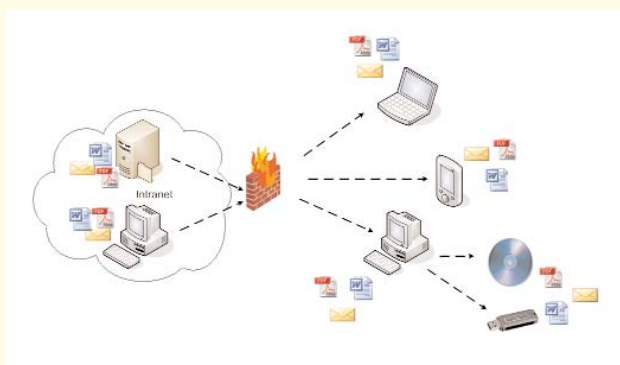


Рис. 1.

Простой пример: авторизованный пользователь, согласно своим полномочиям, делает копию документа на внешний носитель или отправляет документ по электронной почте. И все: дальнейшая судьба копии или письма нам неизвестна. Сколько еще копий сделано, кто получил к ним доступ, куда они отправлялись... Полная неизвестность.

Та же ситуация и с версиями документа. Какая именно версия прайса или технической документации находится у пользователя – неизвестно. Вывести документ из обращения по истечении срока его действия – тоже проблема. В современных бизнес-отношениях часто приходится отдавать конфиденциальную информацию наружу, делаясь ею с партнерами, клиентами и поставщиками. И нет никакой гарантии, что доступ к переданному документу будет строго контролироваться или даже вообще будет контролироваться...

Фантазии на тему

Попробуем сформулировать требования к некой гипотетической системе управления документами. Основные составляющие такой системы – управление доступом, управление версиями и управление жизненным циклом. Управление доступом должно обеспечивать четкое разграничение полномочий пользователя при обращении с документом. Права пользователя зависят от его должностных полномочий и от степени важности (конфиденциальности) документа. Все манипуляции пользователя с документами должны отслеживаться и протоколироваться. При необходимости права пользователя могут корректироваться (вплоть до полного запрета на работу с данным документом). Управление версиями обеспечивает возможность актуализации текущей версии документа, с прекращением доступа пользователей к его устаревшей редакции независимо от того,

сколько было сделано копий и где они хранятся. И, наконец, управление жизненным циклом обеспечивает задание таких параметров как время существования документа и срок и способ завершения рабочего цикла. Например, хранить документ пять лет с возможностью вносить изменения уполномоченным лицам, а по истечении этого срока отправить в архив и запретить вносить изменения или вовсе уничтожить.

Для того чтобы система по управлению правами доступа к данным могла быть успешно внедрена в сети гетерогенных серверов и рабочих станций в современных крупных организациях, имеющих партнеров, клиентов, подрядчиков, такое решение должно быть безопасным, удобным рядовым пользователям и централизованно управляемым (допущенными пользователями, владельцами бизнес-процессов и администраторами). При этом система должна обладать высокой гибкостью в настройке, учитывать различные модели нарушителя и объекты защиты. К типовым нарушителям могут относиться рядовые пользователи, имеющие доступ к различным приложениям, администраторы баз данных или приложений, обладающие расширенными полномочиями, привилегированные пользователи, слабо управляемые и часто весьма мобильные. Объекты защиты могут быть стратегическими (клиентская база, интеллектуальная собственность), тактическими (документооборот, хранилище файлов и документов) и оперативными (текущая переписка, данные на локальных рабочих местах).

Сказку сделать былью

Теперь, когда мы определили основные требования и критерии, самое время признать, что подобные системы отнюдь не гипотетические, а вполне реальные. Реализованная некоторыми производителями ПО в своих продуктах технология Information Rights Management (IRM) обеспечивает контроль и защиту критичной информации независимо от ее местоположения. На рынке представлены подобные продукты от компаний EMC, Oracle, Microsoft и HP.

Все они обеспечивают шифрование защищаемой информации и строгое разграничение доступа и чаще всего основаны на клиент-серверной архитектуре, где сервер отвечает за хранение политик, ключей шифрования, аутентификацию пользователей. Клиентские модули обеспечивают взаимодействие с сервером, применение политики к той или иной информации, а также

ряд дополнительных сервисов по контролю работы с документом. У продукта Oracle Information Rights Management (Oracle IRM) есть несколько ключевых отличий в архитектуре, имеющих чрезвычайно важное значение для корпоративного использования, поэтому рассмотрим функционирование системы управления правами доступа к документам именно на его примере.

Основные отличия Oracle IRM:

- используется модель прав, основанная на классификации документов, что позволяет присваивать права не отдельным файлам, а их пакетам. В результате приходится оперировать с меньшим количеством прав, что, в свою очередь, делает возможным периодическую или автоматическую синхронизацию прав и событий аудита между сервером и агентами Oracle IRM;
- автоматическая синхронизация делает возможным полностью прозрачную работу off-line с зашифрованной информацией (например, для мобильных пользователей), оставляя в силе централизованное аннулирование или изменение прав.

Решения других производителей управляют правами на основе индивидуальных файлов. Для корпоративных объемов информации это означает слишком большой объем прав для автоматической синхронизации с рабочими станциями. Администраторы таких решений вынуждены выбирать между механизмом кэширования прав (чтобы позволить работу off-line), постоянно находящихся на рабочих станциях, тем самым либо жертвуя возможностью изъятия прав, либо оставляя отмену прав и жертвуя работой off-line. Конкурирующие решения не могут обеспечить одновременно работу off-line и возможность изъятия прав.

Oracle Information Rights Management вводит новые элементы в жизненный цикл документооборота, такие как «запечатывание» и классификацию документов, электронной почты и веб-страниц, и требует установки агента на рабочие станции пользователей и на каждое устройство, на котором эта закодированная информация хранится или используется.

Выгоды подхода, ориентированного на защиту информации так очевидны, а изменения в привычные механизмы жизненного цикла настолько минимальны, что Oracle IRM может повсеместно использоваться в организациях и государственных структурах для обеспечения безопасности наиболее конфиденциальной информации.

За семью печатями

Oracle Information Rights Management использует «запечатывание», чтобы обеспечить реальный периметр управления документами электронными сообщениями и веб-страницами в любом месте, где бы они не были.

Используемый процесс кодирования называется «запечатыванием», потому что реально выполняет три функции:

- происходит упаковывание информации слоем кодирования, так что, несмотря на то, как много копий сделано и где они хранятся, они бесполезны без соответствующих данных для раскодирования;
- в кодируемый документ встраивается набор ссылок (URL links), так что каждая копия ссылается на сервер Oracle IRM, на котором информация была «запечатана»;
- используется цифровая подпись, так что любая попытка подделки документов будет определена и предотвращена.

Права доступа на запечатанные документы хранятся отдельно от самих данных, на расположенном в сети сервере Oracle IRM, который обслуживает организация – собственник документов. Это привносит несколько новых преимуществ, и где бы информация ни хранилась, куда бы ни передавалась или как бы ни использовалась:

- неавторизованные пользователи не могут получить к ней доступ (наиболее значимая выгода);
- только авторизованные пользователи могут открывать или модифицировать документы в соответствии с их правами (например, право на распечатывание особо секретной информации);
- вся работа с запечатанной информацией (и попытки доступа к ней) централизованно протоколируются;
- доступ к удаленно хранимой информации может быть централизованно отменен: например, если отношения с пользователем, работником по контракту, партнером завершились (несмотря на то, что он сделал копии, используя DVD, USB и другие средства).

Одним из ключевых свойств Oracle Information Rights Management является его способность управлять информацией снаружи межсетевых экранов, несмотря на то что информация хранится в сети других организаций или дома у пользователя. Это является принципиально важным ввиду того, что современному бизнесу необходимо вовлекать в бизнес-процессы дру-

гих участников, партнеров, подрядчиков, поддерживающие подразделения (например, при аутсорсинге), внешних консультантов, удаленно работающих сотрудников и т.д.

IRM позволяет не только расширить безопасность и аудит за пределы контролируемых хранилищ данных. Оно позволяет управлять жизненным циклом и версиями документов, где бы они не находилась и не использовалась – на рабочих станциях пользователей, ноутбуках и мобильных беспроводных устройствах, в других репозиториях, внутри и снаружи периметра безопасности сети. В этом случае:

- если документы или почтовые сообщения, являющиеся собственностью компании, запечатаны, значит они не только защищены от подделки (никто не имеет права их редактировать), но и, когда приходит время их удалить, каждая их копия может быть эффективно изъята с помощью удаления ключа декодирования с сервера Oracle IRM. И это применяется к каждой отдельной копии;
- если запечатывание применяется к документам, имеющим несколько версий, Oracle IRM может быть сконфигурирован так, чтобы автоматически изымать доступ к старым версиям при выпуске более новой;
- если пользователи локально сохранили старые версии документов, они не только не получают к ним доступа, но и находящиеся внутри документов ссылки (URL) их приведут к новым версиям, хранящимся в контролируемом репозитории. Своевременное обеспечение пользователей самой новой информацией может заметно сократить расходы компаний и государственных структур на распространение измененных документов и быть уверенным в более полном соблюдении инструкций и правил.

Где у него кнопка?

Oracle Information Rights Management имеет архитектуру распределения прав между центральным сервером и агентами, которые должны быть установлены на каждом устройстве, которое создает или использует запечатанную информацию.

Четыре ключевых компонента системы:

- **сервер Oracle IRM Server** – хранит ключи декодирования и управляет правами пользователей к запечатанным документам и электронным письмам;
- **агент Oracle IRM Desktop** – позволяет авторизованным пользователям создавать и

использовать запечатанную информацию в зависимости от прав, полученных с сервера Oracle IRM;

- **консоль управления Oracle IRM Management console** – позволяет администратору управлять всеми аспектами решения Oracle IRM;
- **Oracle IRM Standard Rights Model** – веб-приложение, позволяющее бизнес- или ИТ-администраторам создавать новых пользователей, присваивать роли и т.д.

Рабочий процесс построен следующим образом (рис. 2):

1. **Создание.** Пользователи продолжают создавать документы и электронные сообщения с помощью существующих привычных приложений, таких как Microsoft Office, Microsoft Outlook, Adobe Reader, Lotus Notes и т.д. Например, создание электронных сообщений происходит в обычном e-mail-клиенте, а отправка – по кнопке «запечатать и отправить» (вместо «отправить»).
2. **Классификация и назначение прав.** Oracle IRM позволяет автоматически или в ручном варианте запечатывать документы на различных стадиях их жизненного цикла с помощью средств, интегрированных в Windows desktop, приложения по созданию документов, клиентские программы электронной почты и общие репозитории. Запечатывание защищает документы и электронные сообщения с помощью механизмов кодирования и цифровых электронных подписей, «вшивая» неудаляемые привязки (links) к находящимся в сети серверам Oracle IRM, которые хранят информацию для декодирования и права доступа к документам.
3. **Распространение.** Запечатанные документы и электронные сообщения могут распространяться любым доступным способом (e-mail, Интернет, через файловые сервера и т.д.). Права сохраняются отдельно от запечатанных документов и почтовых сообщений на сервере Oracle IRM, позволяя менять права в любое удобное время.
4. **Проверка привилегий.** Для создания и использования документов и электронных сообщений привычными средствами конечные пользователи должны загрузить и установить универсальный агент, называемый Oracle IRM Desktop. Агент имеет небольшой размер и отвечает за аутентификацию пользователей, прозрачным образом запрашивая права с сервера Oracle IRM, защищая и протоколируя работу с запечатанными документами и почтовыми сообще-

ниями, когда они используются встроенными средствами рабочих станций.

5. **Детальный аудит доступа.** Сервер и агенты совместно обеспечивают аудит всех попыток обращения к запечатанным документам и электронным письмам (on-line и off-line) всех административных операций, таких как назначение или изъятие прав. Можно управлять степенью детализации аудита, а записи аудита могут храниться в базе данных на сервере Oracle IRM, посланы в виде сообщений внешним приложениям для обработки или могут экспортироваться в журнальные файлы для дальнейшего импорта в стандартные средства генерации отчетов.
6. **Мониторинг доступа.** Консоль управления обеспечивает отчетность на основе запросов с преднастроенными формами отчетов, такими как «Активность пользователей» или «События по определенному документу», а также отчетами, определяемыми пользователем.

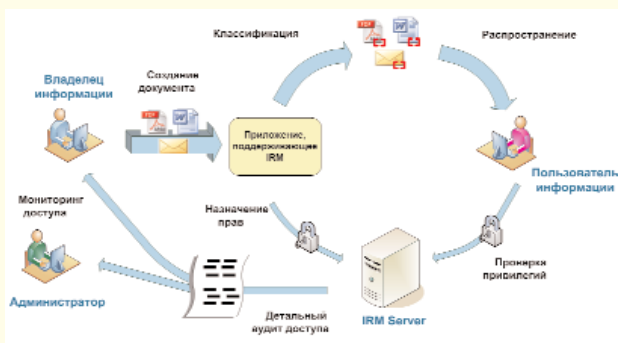


Рис. 2. Построение рабочего процесса

Таким образом, Oracle Information Rights Management может контролировать каждый аспект использования запечатанных документов на рабочих станциях пользователей:

- **кто:** контроль, кто смог и кто не смог открыть документы;
- **что:** контроль доступа к набору (согласно классификации) или к любому конкретному документу;
- **когда:** контроль того, когда доступ начался и закончился с возможностью отмены права доступа в любой момент;
- **где:** предотвращение возможности доступа к критическим документам снаружи сети;
- **как:** контроль того, как именно пользователи работают с документами на своих рабочих станциях (с глубоким контролем открытия, аннотирования, внесения изменений, трассировкой изменений, контролем копирования, отправки на печать, работы с полями и ячейками форм, просмотром табличных формул и т.д.).

Во всех случаях этот постоянный контроль осуществляется на протяжении всего жизненного цикла документов и электронных сообщений вне зависимости от того, где они находятся и используются.

Всем сестрам по серьгам

Развитая поддержка современных и унаследованных операционных систем и приложений является серьезным аргументом при внедрении в существующих распределенных гетерогенных системах корпоративного уровня. Важно, чтобы внедряемые решения работали с различными версиями ПО, чтобы при возможных обновлениях функционирование всех систем не прерывалось.

Поэтому поддерживается широкий диапазон последних и устаревших версий приложений и операционных систем различных компаний:

- Microsoft Office 2000–2003 (Word, Excel, PowerPoint)
- Adobe Acrobat или Reader 6.0+
- e-mail: Microsoft Outlook 2000–2003, Lotus Notes 6.5+ и Novell GroupWise 6.5–7.0
- e-mail: BlackBerry for Exchange and Domino, BES 4.1+
- HTML и XML (Internet Explorer 6.0+)
- TXT и .RTF документы GIF, JPEG и PNG
- TIFF и 2D CAD.

Доступ к большому количеству документов контролируется в терминах существующих бизнес-процессов или уже имеющейся классификации информации (например, по степени секретности – «секретно», «совершенно секретно»), по существующим бизнес-ролям (таким как «рецензент»), по существующим группам пользователей, определенным в каталоге пользователей (например, «менеджеры отдела продаж»).

Простоту и удобство управления на основе классификации прав иллюстрирует рис. 3. Шесть файлов были запечатаны с использованием двух predetermined классов («конфиденциально» и «общедоступная информация»). Пользователи – генеральный директор (CEO), начальник отдела кадров (HR Director) и группа «Сотрудники компании» (all employees) – получили необходимые права на эти классы, что в результате породило четыре разных права доступа на эти шесть документов.

Со временем количество запечатанных документов легко может вырасти от шести до шести тысяч, при этом не изменяя количества прав доступа (всего четыре), потому что привязка идет на классы, а не на индивидуальные файлы. А так как нет необходимости управления огром-

ным числом прав, решение Oracle обладает высокой надежностью и масштабируемостью, работая при этом на относительно скромном аппаратном обеспечении.

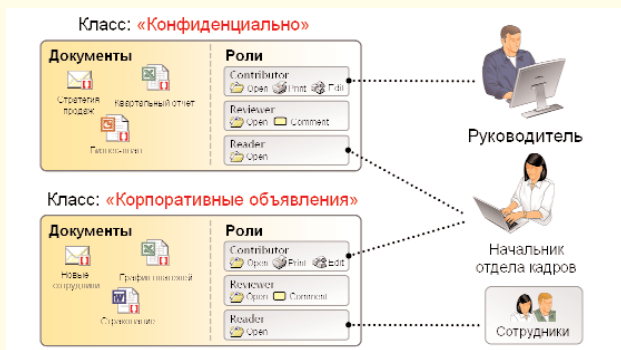


Рис. 3

Oracle IRM поддерживает возможность иметь исключения из общих правил (неизбежные в реальной жизни) для классификации прав доступа, что позволяет администраторам конфигурировать систему на основе индивидуальных пользователей и отдельных файлов.

Административные операции, такие как создание классификаций безопасности, определение ролей и присваивание прав на основании типов или отдельного документа могут быть выделены и присвоены отдельным пользователям или группам пользователей. Владельцы бизнес-процессов и их помощники легко могут управлять безопасностью наиболее секретной информации без привлечения ИТ-администраторов (т.е. можно обойтись без дополнительных суперпользователей).

Популярно объясняю

Существует множество примеров использования системы управления правами доступа к документам в повседневной деятельности любой организации:

Рассылка письма руководителя компании о новой системе премирования:

- К письму применяется шаблон «Конфиденциально: для внутреннего использования».
- Сотрудники могут читать защищенное письмо, но не могут копировать, сохранять, редактировать или пересылать.
- К письму приложен файл с таблицами расчета, который могут открывать и читать только руководители подразделений.

Работа в группе:

- Руководитель группы устанавливает ограниченные права доступа для документа Word и назначает срок действия этих прав.

- Члены группы получают доступ к документу только на чтение.
- После истечения установленного времени доступ к документу прекращается.

Работа с версиями документов:

- Устанавливается контроль номера текущей версии.
- При создании новой версии документа Oracle IRM прекращает возможность доступа к старым версиям, где бы они не находились.
- При попытке открыть старую версию пользователь перенаправляется к новой версии, хранящейся на сервере.

Управление жизненным циклом документа

- Для документа определяются параметры жизненного цикла: например, хранить без изменений 10 лет, а затем уничтожить.
- При достижении установленного срока доступ к документу прекращается.
- Независимо от того, какое количество копий было сделано и где они хранятся, документ становится недоступен.

В сухом остатке

Основным результатом внедрения системы Information Rights Management является уменьшение риска утечки конфиденциальной информации за счет:

- шифрования данных;
- контроля действий, производимых с документом;
- регистрации событий доступа к информации;
- возможности централизованно аннулировать доступ к документу.

Кроме того, при условии внедрения ряда систем, интерес к которым сегодня обусловлен не только решением бизнес-задач, но и требованиями государственных регуляторов (системы управления идентификационными данными и доступом, корреляции событий, контроля деятельности пользователей и защиты от НСД), появляется реальная возможность отказаться от громоздких и ресурсоемких DLP-решений (DLP – Data Leak Prevention, технологии предотвращения утечек конфиденциальной информации). При этом сама система Oracle IRM может быть быстро развернута с использованием встроенной стандартной модели прав и позволяет установить оптимальный баланс между безопасностью, удобством использования и управляемостью.