

Oracle IRM– технология управления правами доступа к информации Пример внедрения

Алексей Соболев
Технический директор

ПОЛИКОМ ПРФ

Поставка ПО и оборудования
ИТ-инфраструктура
Бизнес-приложения
ЦОД, сети, инженерная инфраструктура



Специфика ИБ

Одна из основных угроз – утечка конфиденциальных данных

Традиционные методы защиты работают на одном или некоторых уровнях

- ? Периметр и внутренняя сеть
- ? Электронная почта
- ? Файловые серверы
- ? Персональные компьютеры
- ? Корпоративные приложения
- ? Базы данных

Мобильная работа как требование бизнеса =>
«размывание» периметра



Проблемы, не решаемые “обычными” средствами



- ❑ Хранение в локальной сети относительно безопасно
- ❑ Но во время использования документы извлекаются для работы и вне корпоративной сети
- ❑ Как...
 - ...обезопасить эти копии и контролировать их использование?
 - ... предотвратить их неправомерную пересылку и редактирование?
 - ... защитить конфиденциальную информацию, передаваемую во вне?
 - ... отменить доступ, когда проект завершён или сотрудник уволен?
 - ... контролировать версии используемых документов?



Oracle Information Rights Management

Обеспечивает безопасность и контроль конфиденциальных документов в любом месте, где бы они не находились, внутри сети или за межсетевым экраном!

- Обширная инсталляционная база – более 1000 организаций
- Используется в самых различных проектах в разных областях

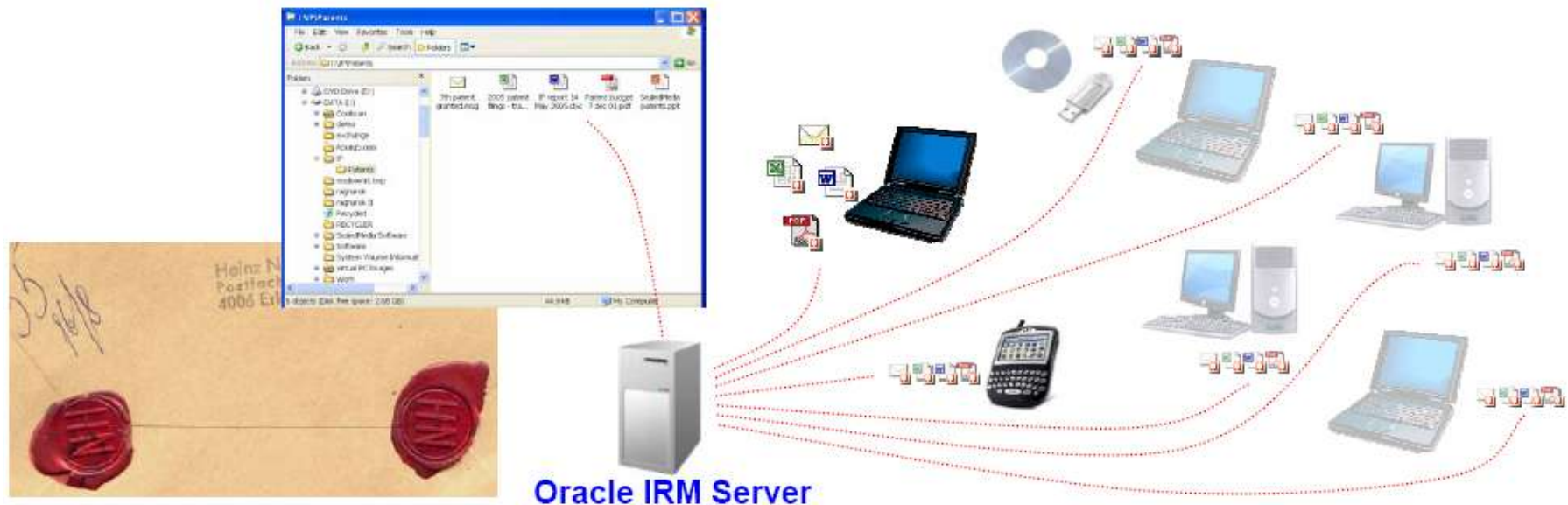


Возможности Oracle IRM

- ❑ Исключение неавторизованного доступа
- ❑ Необходимые полномочия авторизованным пользователям
- ❑ Регистрация событий, формирование отчётов
- ❑ Централизованное управление
- ❑ Работа как online, так и offline (без связи с сервером IRM)



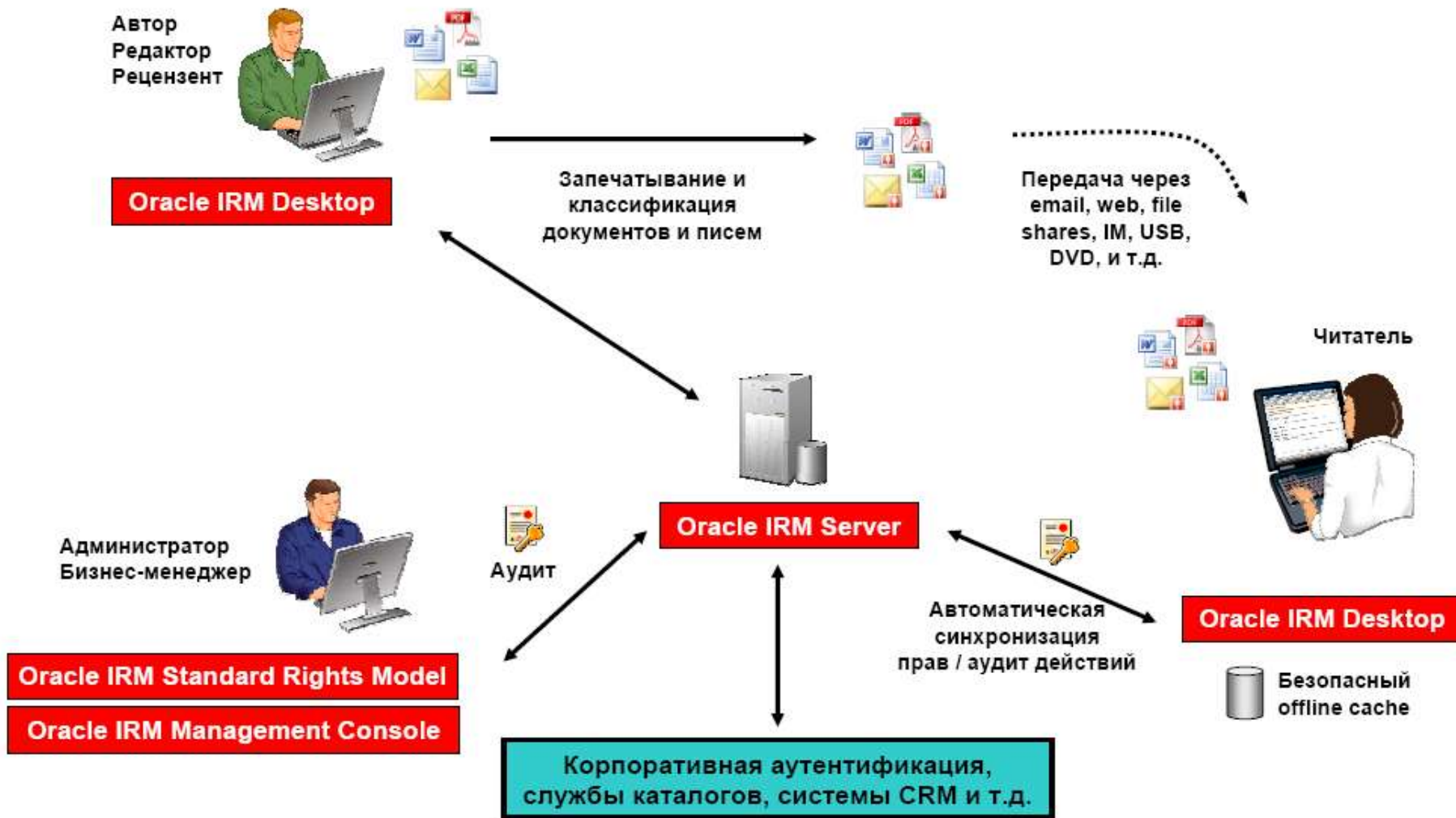
Oracle IRM: как это работает



- ❑ «Запечатывание» документов и электронных сообщений
 - Безопасны все документы, копии. В любом месте!
 - Включая копии документов и электронных писем, которые покинули организацию
- ❑ Централизованное управление правами доступа к документам и аудит их использования
 - Агент на рабочих станциях поддерживает политики доступа (встраивается в приложения)
 - Даже в случае использования offline-режима, когда сервер Oracle IRM недоступен

Как работает Oracle IRM

Управление классификацией, правами и аудитом



Контекст

Для управления доступом к информации в IRM создаются контексты.

При запечатывании файла указывается контекст, в котором содержится информация о правах доступа к файлу (доступные операции и ограничения).

В каждом контексте назначаются администраторы, выполняющие функции управления контекстом.

По контексту формируются аудиторские отчеты.

Контексты могут создаваться по шаблону контекста. (IRM поставляется с готовыми шаблонами контекстов)

Oracle IRM: Постоянный контроль

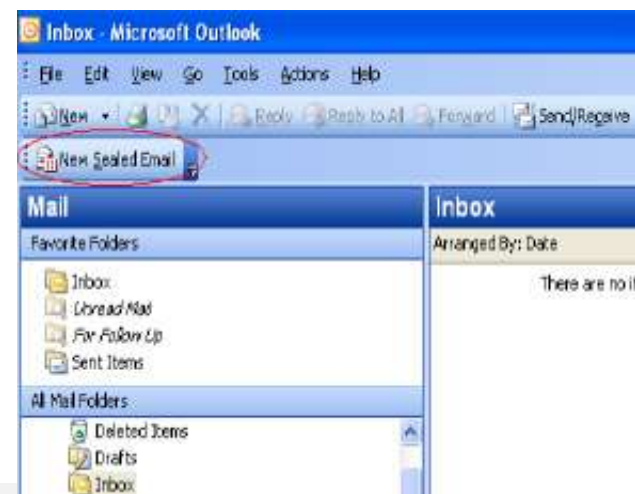
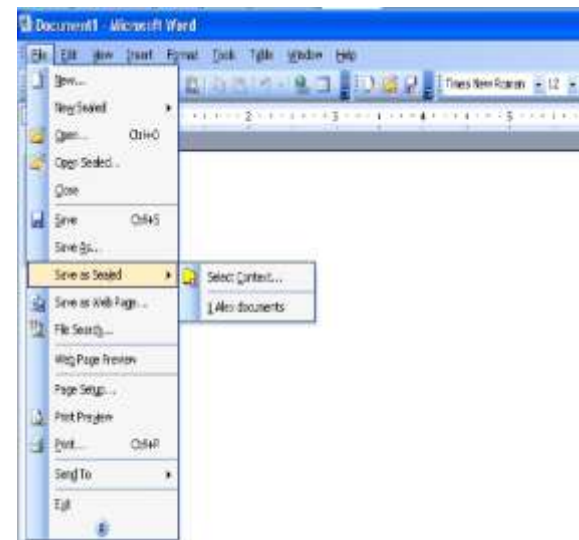
Позволяет получить ответы на вопросы

- Кто?
- Что?
- Когда?
- Где?
- Как?



Поддержка множества приложений и форматов

- Microsoft Office 2000-2003 (Word, Excel, PowerPoint)
- Adobe Acrobat или Reader 6.0+
- Email: Microsoft Outlook 2000-2003,
- Lotus Notes 6.5+ и Novell GroupWise 6.5-7.0
- 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
- ...



Простота Oracle IRM

- ❑ Минимальные изменения в инфраструктуре:
 - Сервер Oracle IRM Server - типичное web-приложение
 - Пользователям необходимо установить Oracle IRM Desktop

- ❑ Использование Oracle IRM является очень простым
 - Использование «запечатанной» информации так же легко, как и незапечатанной
 - «Запечатывание» так же легко, как и печать на документе «Конфиденциальная информация»
 - Лёгкое управление классификацией документов и ролями
 - Администрирование IRM чаще всего совместно выполняют ИТ и бизнес-подразделения
 - Контроль использования критической информации часто ведётся секретарём

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 1801

Выдан 13 марта 2009 г.
Действителен до 13 марта 2012 г.

Настоящий сертификат удостоверяет, что средство защиты информации «Программный пакет Oracle Information Rights Management» версии 10gR3 PR3 (партия из 20 (двадцати) экземпляров продукции с серийными номерами, указанными в приложении к настоящему сертификату, маркированных знаками соответствия с № В 614307 по № В 614326) производства компании Oracle, является программным средством защиты информации, обеспечивающим разграничение доступа к ней, соответствует требованиям технических условий ТУ-5000-001-52384799-2008 и может использоваться при создании автоматизированных систем класса защищенности до ИГ исключительно в соответствии с требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации» (Гостехкомиссия России, 1992).

Сертификат выдан на основе результатов сертификационных испытаний, проведенных испытательной лабораторией ООО «Линс-М» (аттестат аккредитации от 07.10.2004 № СЭИ RU.907.6027.060) – техническое заключение от 04.02.2009, и экспертного заключения от 11.03.2009 ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЭИ RU.840.A92.007).

Заявитель: ООО «ФОРС-Центр разработки»
Адрес: 129272, г. Москва, Трифоновский тупик, д. 3
Телефон: (495) 787-7040

Маркирование знаками соответствия сертифицированной продукции и инспекционный контроль ее соответствия требованиям указанных в настоящем сертификате технических условий осуществляется испытательной лабораторией ООО «Линс-М».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ



А.Гапонов

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации
13 марта 2009 г.

Опыт внедрения



Внедрение в компании Скартел (Yota)

- ❑ Yota – первая в России сеть Mobile WiMAX™ (стандарт IEEE 802.16-2005), обеспечивающая быстрый мобильный доступ в интернет и переключение между станциями без обрыва соединения. Yota Интернет 4G – безлимитный, беспроводной и доступный везде.
- ❑ Сеть Yota уже развернута в Москве, Санкт-Петербурге, Уфе, Сочи и Краснодаре.
- ❑ Yota строит сети 4G и за пределами России: в Белоруссии, Никарагуа, Перу.
- ❑ Простое подключение к Yota обеспечивается устройствами различных типов. Это модемы, ноутбуки, роутеры и первый в мире GSM + Mobile WiMAX телефон HTC MAX 4G.
- ❑ Yota предлагает уникальные мобильные сервисы, используя возможности беспроводного быстрого доступа в интернет: мобильное телевидение, «тяжелый» видеоконтент, музыкальный каталог с сотнями тысяч композиций от ведущих мировых лейблов и другие.
- ❑ Yota входит в международную ассоциацию WiMAX Forum, объединяющую мировых лидеров в области технологий и предоставления услуг связи четвертого поколения (4G).

Этапы проекта внедрения

- ❑ Исследование логики рабочих процессов заказчика
 - Анкетирование, интервью с целью выявления уровней секретности, «тематических разделов», жизненного цикла документов и ролей пользователей
 - формирование перечня контекстов документов
 - Согласование спецификации на настройку
- ❑ Установка и настройка ПО
 - установка и настройка серверной части системы
 - распространение пользовательского ПО
 - Создание перечня контекстов документов и ролей в рамках системы IRM
- ❑ Документирование системы
 - Техническое описание
 - Инструкция администратора
 - Инструкция пользователя
- ❑ Техническая поддержка/сопровождение системы IRM

Основные трудности

- ❑ Формирование перечня контекстов
 - Необходимость и достаточность
 - Логичность и удобство
- ❑ Плотный график ключевых сотрудников



Благодарю за внимание!

Алексей Соболев
Технический директор

ПОЛИКОМ ПАО

Москва
тел. (495) 660 32 91
факс (495) 660 32 93

Санкт-Петербург
тел. (812) 325 84 00
факс (812) 320 56 86

www.polikom.ru