Управление правами доступа к данным легитимных пользователей

АЛЕКСЕЙ СОВА

Ведущий специалист

Информзащита

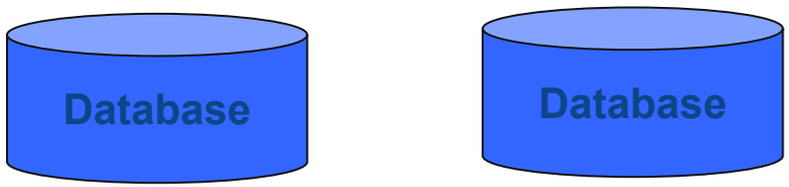
Системный интегратор

Два типа информации:

Структурированная 10-20%

Неструктурированная 80-90%

Business Intelligence



Информзащита
Системный интегратор

Методы защиты информации

- Телекоммуникации (периметр и внутренняя сеть)
- Защита электронной почты (сервера, анализ контента, защита ПК)
- Безопасность файловых серверов
- Защита персональных компьютеров (ОС, антивирус, внешние порты, Host Based Intrusion Prevention)
- Защита серверов приложений
- Защита корпоративных приложений
- Защита баз данных

Альтернатива =▷ Защита самой информации (Information centric security)

Информзащита
Системный интегратор

Обеспечение безопасности с помощью IRM

- 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

- Как обезопасить копии файлов и контролировать их использование?
- Как защитить конфиденциальную информацию, передаваемую партнёрам, поставщикам и клиентам?
- Как отменить доступ, когда проект завершён или сотрудник уволен?

Информзащита
Системный интегратор

Для чего предназначен Oracle IRM

- Oracle IRM используется для управления доступом к конфиденциальным документам распространённых форматов (MS Office, PDF, JPEG, TXT, Email, HTML и др.)
- Использует централизованное управление правами доступа на основе ролей и корпоративной аутентификации
- Встраивается в существующие системы документооборота и бизнес-процессы
- Безопасность основана на защите самих документов (Information Centric Security)

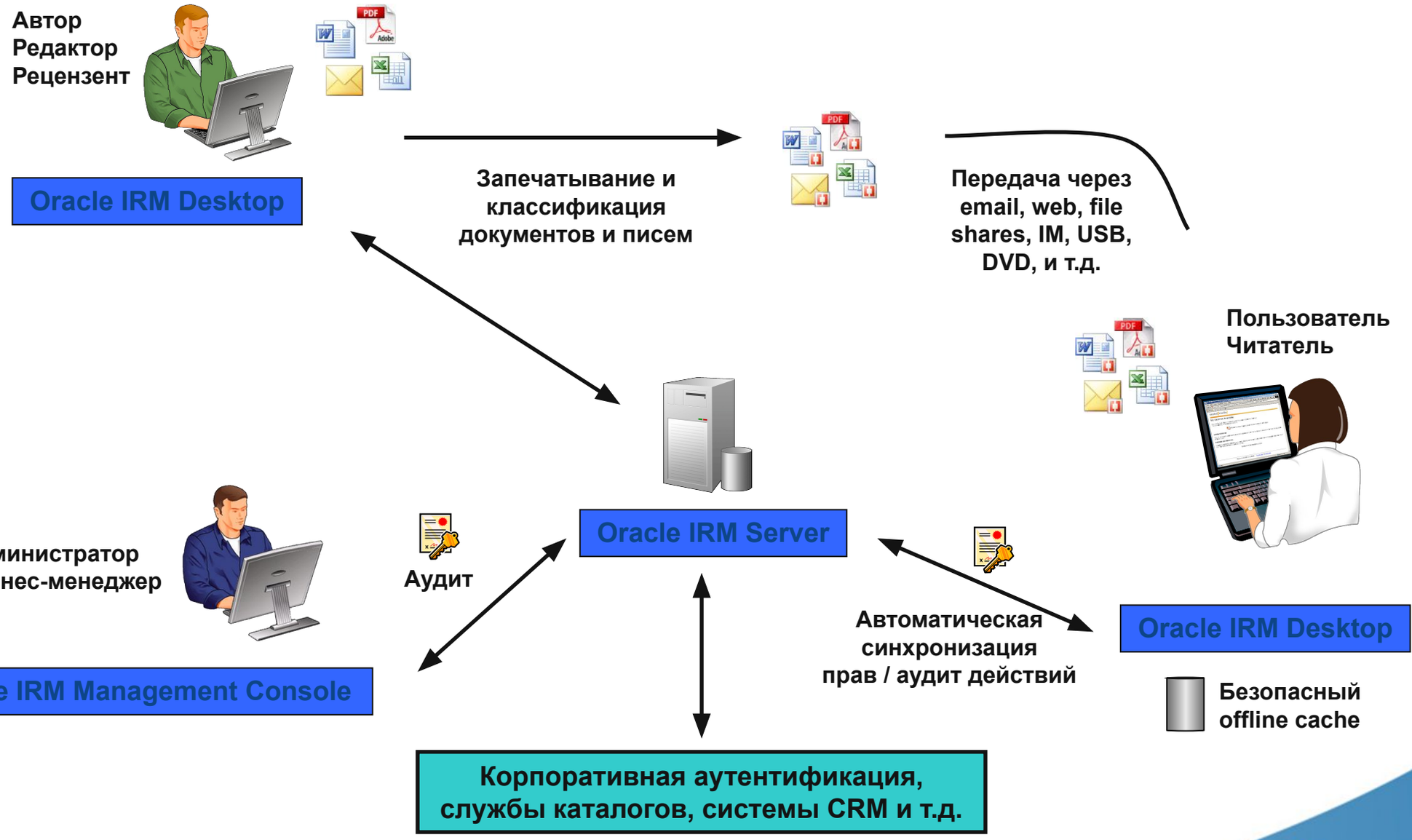
Информзащита
Системный интегратор

Схема работы Oracle IRM

- Все документы шифруются (seal)
- Ключи расшифровки находятся на сервере
- Для доступа к ключам/серверу необходимо пройти аутентификацию
- Клиентские приложения (MS Word, Adobe Acrobat Reader и т.д.) работают под управлением клиента Oracle IRM, который гарантирует права использования документов

Информзащита
Системный интегратор

Как работает Oracle IRM



Информзащита
Системный интегратор

Журнал аудита

Создатель/Редактор

Print (cache)

anna

19 Январь 2009 г. 11:40:37

IRM

Version: 5.5.9.95.release

Locale: RUS

MachineID: 0E03D8B4B754

Operating System: Windows XP Service Pack 2

Host Browser: -

Rendering Application: Word 2003 (11.5604.5606)

Feature: Print

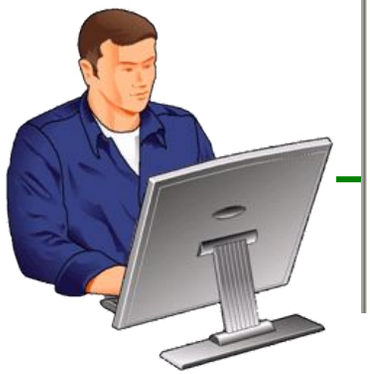
Item: 2009_01_19 08:05:24 News_01.sdoc

Role: owner

Location: C:\А это файл, который я утащил домой и переименовал.sdoc

Context: users

Operation	User	Time	Computer	IP	Remote IP
Open (server)	anna	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)	anna	19 января 200...	IRM	192.168.50.146	192.168.5
Open (cache)	anna	19 января 200...	IRM	192.168.50.146	192.168.5
Print (cache)	anna	19 января 200...	IRM	192.168.50.146	192.168.5
Synchronize	anna	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)...	anna	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Open (cache)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Open (cache)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Print (cache)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Synchronize	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Open (cache)	pavel	19 января 200...	IRM	192.168.50.146	192.168.5
Synchronize	alex	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)...	alex	19 января 200...	IRM	192.168.50.146	192.168.5
Synchronize	alex	19 января 200...	IRM	192.168.50.146	192.168.5
Open (server)...	alex	20 января 200...	IRM	192.168.50.146	192.168.5
Synchronize	alex	20 января 200...	IRM	192.168.50.146	192.168.5
Access Denied	buhadm	20 января 200...	IRM	192.168.50.146	192.168.5
Access Denied	buhadm	20 января 200...	IRM	192.168.50.146	192.168.5
Save New U...	irmadm	22 января 200...	IRM	192.168.50.146	192.168.5
Save New R...	irmadm	22 января 200...	IRM	192.168.50.146	192.168.5
Assign Role	irmadm	22 января 200...	IRM	192.168.50.146	192.168.5
Save New U...	irmadm	22 января 200...	IRM	192.168.50.146	192.168.5



Администратор/Аудитор

IRM Management Console

Информзащита
Системный интегратор

Oracle IRM: Постоянный контроль

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.)

Информзащита
Системный интегратор

IRM: Интеграция в инфраструктуру

Аутентификация

- Аутентификация на сервере Oracle IRM по имени и паролю
- Windows-аутентификация
- Синхронизация с LDAP-каталогами с помощью Oracle IRM Directory Gateway (например Microsoft LDAP, Sun ONE Directory Server, iPlanet, Lotus Notes Domino)
- Аутентификация через Web
  (Oracle IRM Web Service SDK с поддержкой SOAP/WSDL)

Примеры интеграции в приложения (с помощью Oracle IRM API):

- Автоматическое «запечатывание», встроенное в собственный документооборот
- Автоматическое «запечатывание» и «распечатывание» файлов, покидающих или попадающих в хранилище
- Временное «распечатывание» для полнотекстового индексирования

Информзащита
Системный интегратор

Контексты безопасности

Управление правами доступа сотен пользователей к тысячам документов непрактично

- Существенно управлять группами документов и пользователей

Контекст безопасности является определяющим

- Наборы связанных документов
- Люди и группы, которые используют эти документы
- Роли, которые имеют пользователи на доступ к этой информации

Контекст безопасности основан на классификации по теме или уровню секретности

- Темы: Документы руководства, Проект «Моби-Дик», Объявления по компании
- Уровень секретности: Top Secret, Code Red, Level 1, 2, 3

Информзащита
Системный интегратор

Стандартные роли на доступ к информации

- Oracle IRM определяет стандартный набор ролей

- Роли могут быть связаны с отдельными пользователями, группами и контекстами (типами информации)
- В Oracle IRM возможны различные административные роли:

Информзащита
Системный интегратор

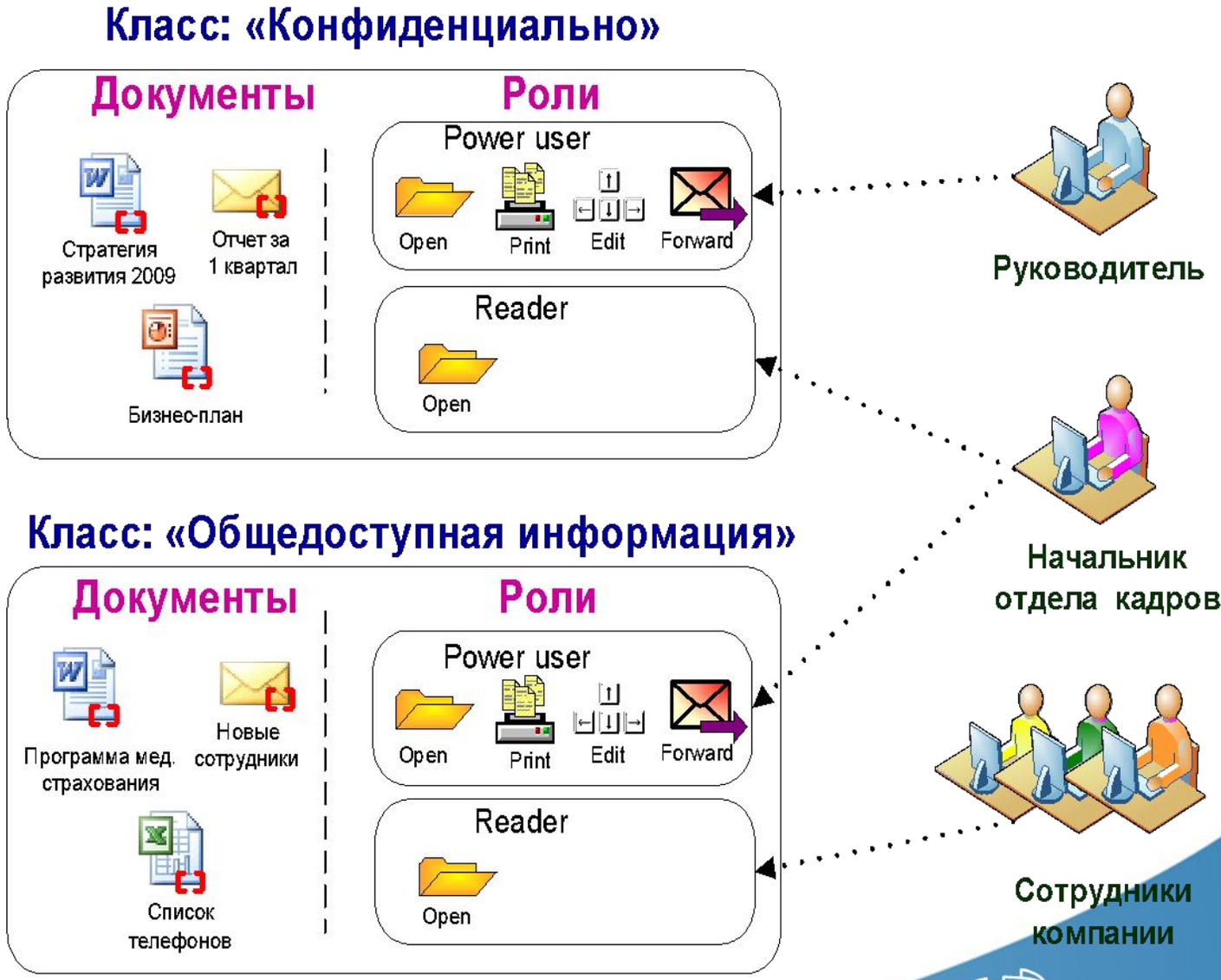
Ограничение прав легитимных пользователей

Oracle IRM управляет доступом к информации на основе:

- Существующих классификаций информации, таких как «Конфиденциально»
- Существующих ролей пользователей, таких как «Рецензент»
- Существующих групп пользователей в корпоративном каталоге, таких как «Бухгалтерия»

Oracle IRM позволяет легко внедрить криптографическую защиту в корпоративной системе

Теперь и конечные пользователи, и администраторы способны понимать и управлять всей системой!



Информзащита
Системный интегратор

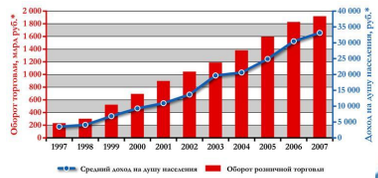
Oracle IRM. Примеры

Рассылка письма руководителя компании о новой системе премирования.

- К письму применяется шаблон «Company Confidential» («Конфиденциально – для внутреннего использования»).
- Сотрудники могут читать защищенное письмо, но не могут копировать, сохранять, редактировать или пересылать.
- К письму приложен файл, доступный только для руководителей подразделений.

Публикация данных о продажах на корпоративном портале

- Доступ к отчету через web-браузер.
- На отчет накладываются ограничения.
- Данные можно просмотреть, но нельзя распечатать, скопировать или вставить в другую программу.



Информзащита
Системный интегратор

Oracle IRM. Примеры

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
- Открыть документ могут только члены группы
- После истечения установленного времени доступ к документу прекращается

Работа с партнерами и контрагентами

- Сотрудник рекламного агентства отправляет проект рекламы представителям заказчика
- Уполномоченный сотрудники заказчика могут ознакомиться с документом и высказать свои пожелания
- На документ установлены ограничения, предотвращающие его передачу сторонним лицам и ограничение по времени доступа.

Информзащита
Системный интегратор

Oracle IRM. Примеры

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

- Для документа определяются параметры жизненного цикла, например: хранить без изменений 7 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.

Информзащита
Системный интегратор

Почему заказчики выбирают Oracle IRM

Oracle Information Rights Management предоставляет правильный баланс между **Безопасностью, Удобством использования,** и **Управляемостью**

Безопасность

- Документы и электронные письма остаются защищёнными: и неважно, сколько сделано копий и где они
- Доступ к документам протоколируется, а права доступа можно изъять в любое время: даже для копий, покинувших организацию

Удобство использования

- Так же легко, как и использование незащищённых документов и писем
- Просто немного расширяются возможности обычных средств: Microsoft Word, PowerPoint, Excel, Outlook, Lotus Notes, Adobe Reader, и т.д.
- Нет необходимости в обновлении: поддерживаются текущие и устаревшие операционные системы и приложения

Управляемость

- Интуитивное, основанное на политиках корпоративное управление: миллионы документов и писем + тысячи пользователей
- Быстрое внедрение: легко масштабируется для использования в инфраструктуре любой организации

Информзащита
Системный интегратор

Некоторые важные преимущества над конкурентами

- Больший, чем у конкурентов набор форматов и приложений
- Поддержка прозрачного поиска в запечатанных документах
- Защита от Print screen и удалённого администратора (radmin и др.)
- Работа с типами документов и ролями доступа (возможность удобного централизованного администрирования)
- Поддержка on-line и off-line работы одновременно. Например, изменение политик доступа к уже запечатанным документам в любое время.
- Поддержка разных типов аутентификации одновременно. Например, внутренние пользователи по Active Directory и внешние пользователи по имени и паролю

Информзащита
Системный интегратор

Сертификат ФСТЭК на Oracle IRM

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-5090-001-52384799-2008 и может использоваться при создании автоматизированных систем класса защищенности до **1Г** включительно 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 «Инис-М» (аттестат аккредитации от 07.10.2004 № СЗИ RU.907.Б027.060) – техническое заключение от 04.02.2009, и экспертного заключения от 11.03.2009 ФГУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.840.А92.007).

Информзащита
Системный интегратор

ВОПРОСЫ ?

АЛЕКСЕЙ СОВА
ведущий специалист

- (495) 980 23 45 #327
- a.sova@infosec.ru

Информзащита
Системный интегратор