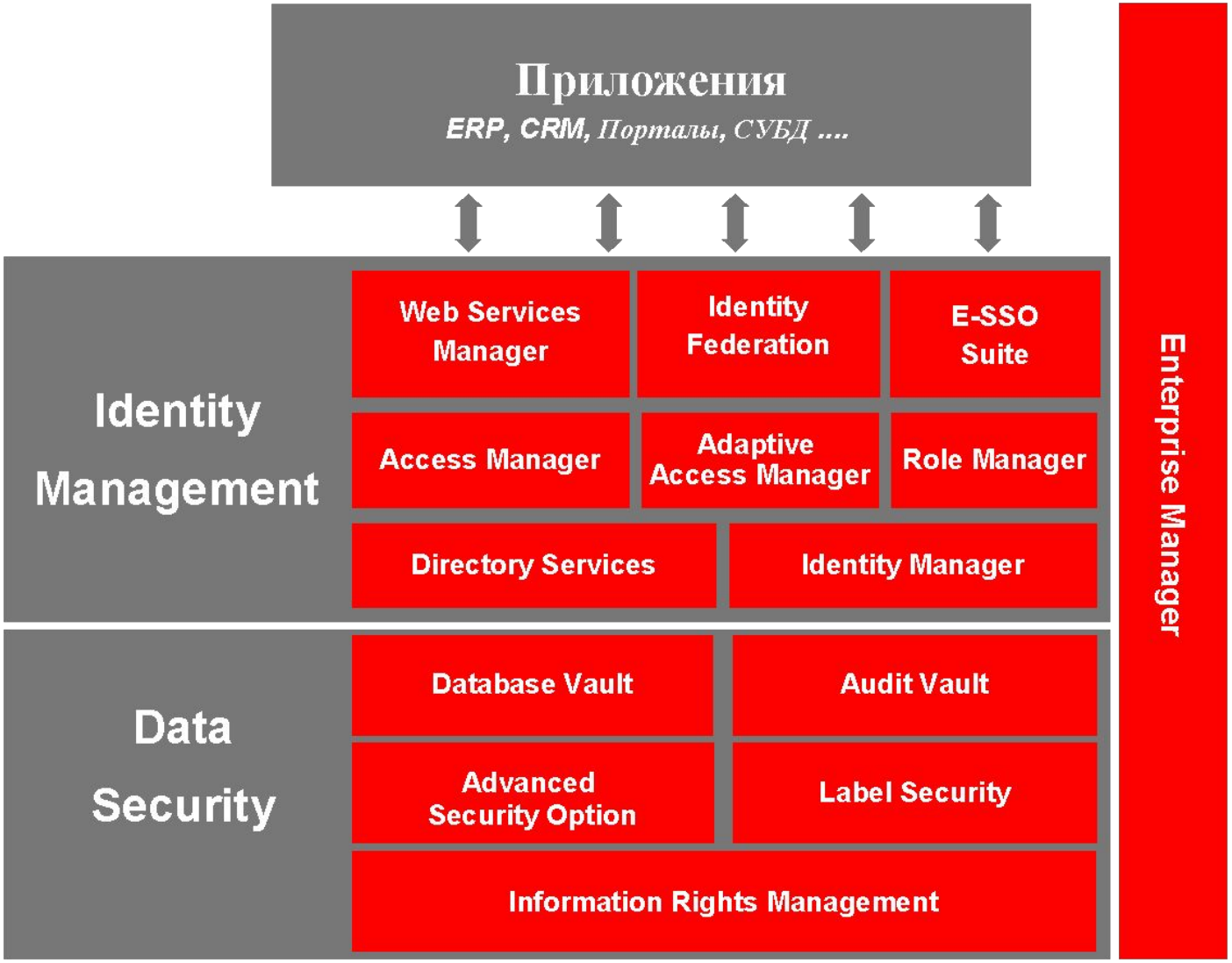
ФОРС – Центр разработки

Обзор основных сертифицированных решений Oracle в области ИБ

Александр Козлов
Начальник отдела решений ИБ

Линейка продуктов Oracle



Линейка продуктов Oracle
Учет национальной специфики

Сертифицировано:

- Identity and Access Management Suite- **ТУ+1Г+2-й класс ПД**
- Oracle DB 10G-Label Security- **ТУ+1В+2-й класс ПД**

Испытания успешно завершены:

- Oracle Enterprise Single Sign-On- **ТУ+1Г+2-й класс ПД**
- Oracle Information Rights Management- **ТУ+1Г+2-й класс ПД**

На сертификации:

- Oracle DB 11G + Database Vault- **ТУ+1Г+2-й класс ПД**

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 1664

Выдан 18 августа 2008 г.
Действителен до 18 августа 2011 г.

Настоящий сертификат удостоверяет, **система защиты от несанкционированного доступа к информации системы управления учетными данными и доступом к информационным ресурсам Oracle Identity and Access Management Suite на платформе Microsoft Windows 2003 Server** (партия из 20 (двадцати) экземпляров продукции с номерами идентификаторов с BUS-B1048-0 по BUS-B1048-20, маркированных знаками соответствия с № B 254851 по № B 254870) производства компании Oracle, является программным средством защиты информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям технических условий 13У-0014-ОКО-52384-596-2007 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) при условии выполнения рекомендаций и ограничений, указанных в формуляре РМАГ.425310.103.

Сертификат выдан на основе результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «РНТ» (аттестат аккредитации от 30.06.2004 № СЗИ RU.RI09.Б026.059) – экспертное заключение от 04.06.2008, и экспертного заключения ФАПУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 26.04.2005 № СЗИ RU.B40.A92.007) от 10.07.2008.

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 за соответствием требованиям указанных в настоящем сертификате руководящего документа и технических условий осуществляются испытательной лабораторией ЗАО «РНТ».

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

А.Гапонов

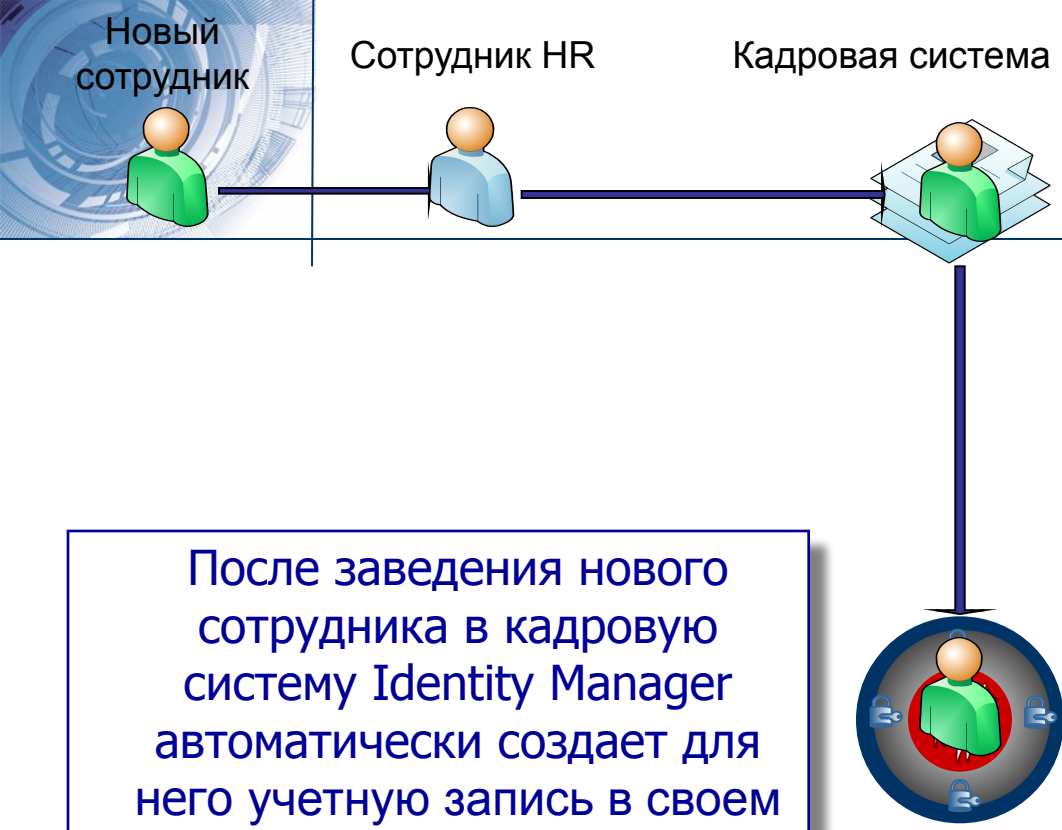
Настоящий сертификат выдан в Государственной системе сертификации средств защиты информации 18 августа 2008 г.

ФОРС
ЦЕНТР РАЗРАБОТКИ

Identity Management
Основные возможности

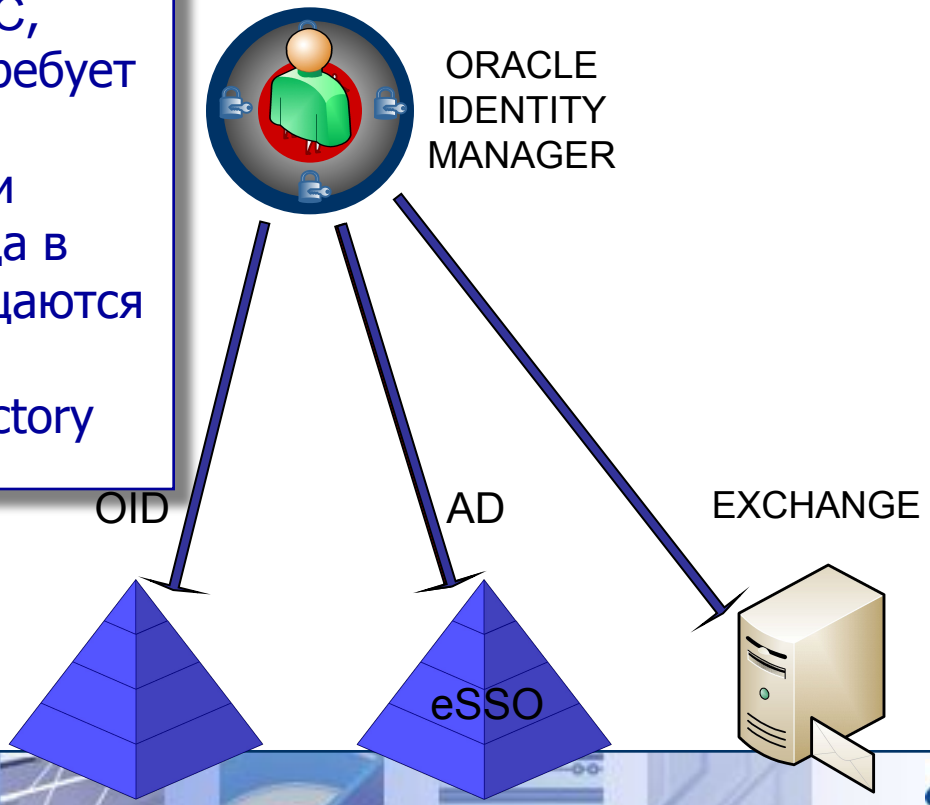
- Автоматизированное управление в соответствии с разработанными стандартами
  - Процессы согласования
  - Целостность, достоверность и своевременное обновление данных
- Слежение за изменением учетных записей в системе
  - Аудит действий администраторов
  - Система отчетов
  - Автоматическое оповещение
- Персонификация учетных записей
- Самообслуживание

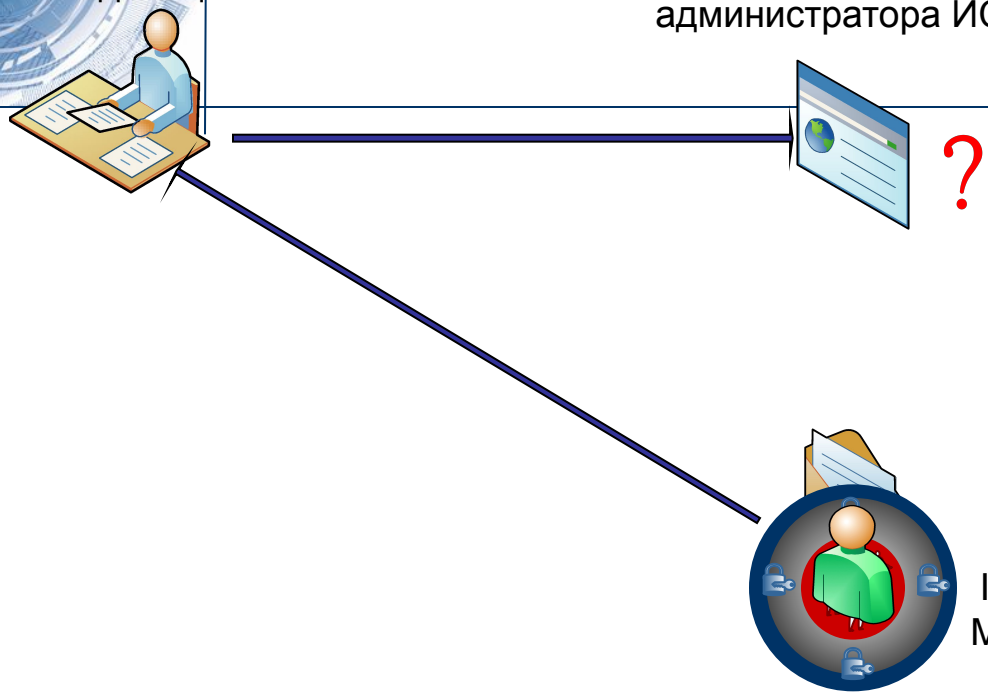
Соответствует требованиям ФЗ Российской Федерации «О персональных данных», Sarbanes-Oxley (SOX), 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA. HSPD12, BASEL II и ряда других международных стандартов



После заведения нового сотрудника в кадровую систему Identity Manager автоматически создает для него учетную запись в своем репозитории

Identity Manager автоматически создает для сотрудника соответствующий его должности набор УЗ с необходимыми полномочиями в тех ИС, доступ к которым не требует предварительного согласования, профили пользователя для входа в эти приложения помещаются в репозиторий eSSO - например в Active Directory

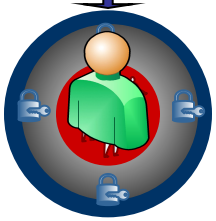




Identity Manager оповещает владельцев остальных необходимых сотруднику в рамках его должностных обязанностей ИС о появлении новых запросов на согласование предоставления доступа

Владелец ИС

Веб-консоль администратора ИС



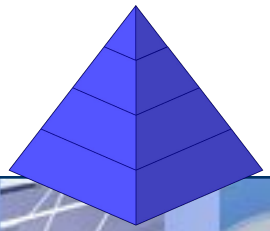
O
ID
MA

Если владельцы ИС через веб-консоль администратора утверждают предоставление сотруднику доступа к ИС, Identity Manager создает для сотрудника УЗ с необходимыми полномочиями, профиль пользователя для входа в это приложения помещается в репозиторий eSSO

OID

AD

EXCHANGE

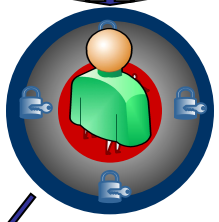


ФОРС
ЦЕНТР РАЗРАБОТКИ

Владелец ИС

Веб-консоль администратора ИС

Если владельцы ИС через веб-консоль администратора утверждают предоставление сотруднику доступа к ИС, Identity Manager создает для сотрудника УЗ с необходимыми полномочиями, профиль пользователя для входа в это приложения помещается в репозиторий eSSO

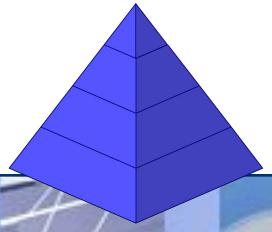


OEBS

OID

AD

EXCHANGE



eSSO

ФОРС
ЦЕНТР РАЗРАБОТКИ

Сотрудник

Веб-консоль самообслуживания

?

Сотрудник, или его руководитель заказывает через веб-консоль самообслуживания доступ к ИС или дополнительные полномочия

ORACLE IDENTITY MANAGER

OEBS

OID

AD

EXCHANGE

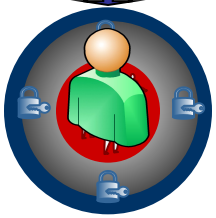
eSSO

Сотрудник

Веб-консоль самообслуживания

?

Identity Manager проверяет политики доступа, относящиеся к сотруднику и в соответствии с ними исполняет или отклоняет заявку



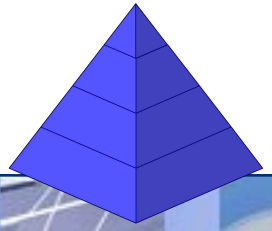
ORACLE IDENTITY MANAGER

OEBS

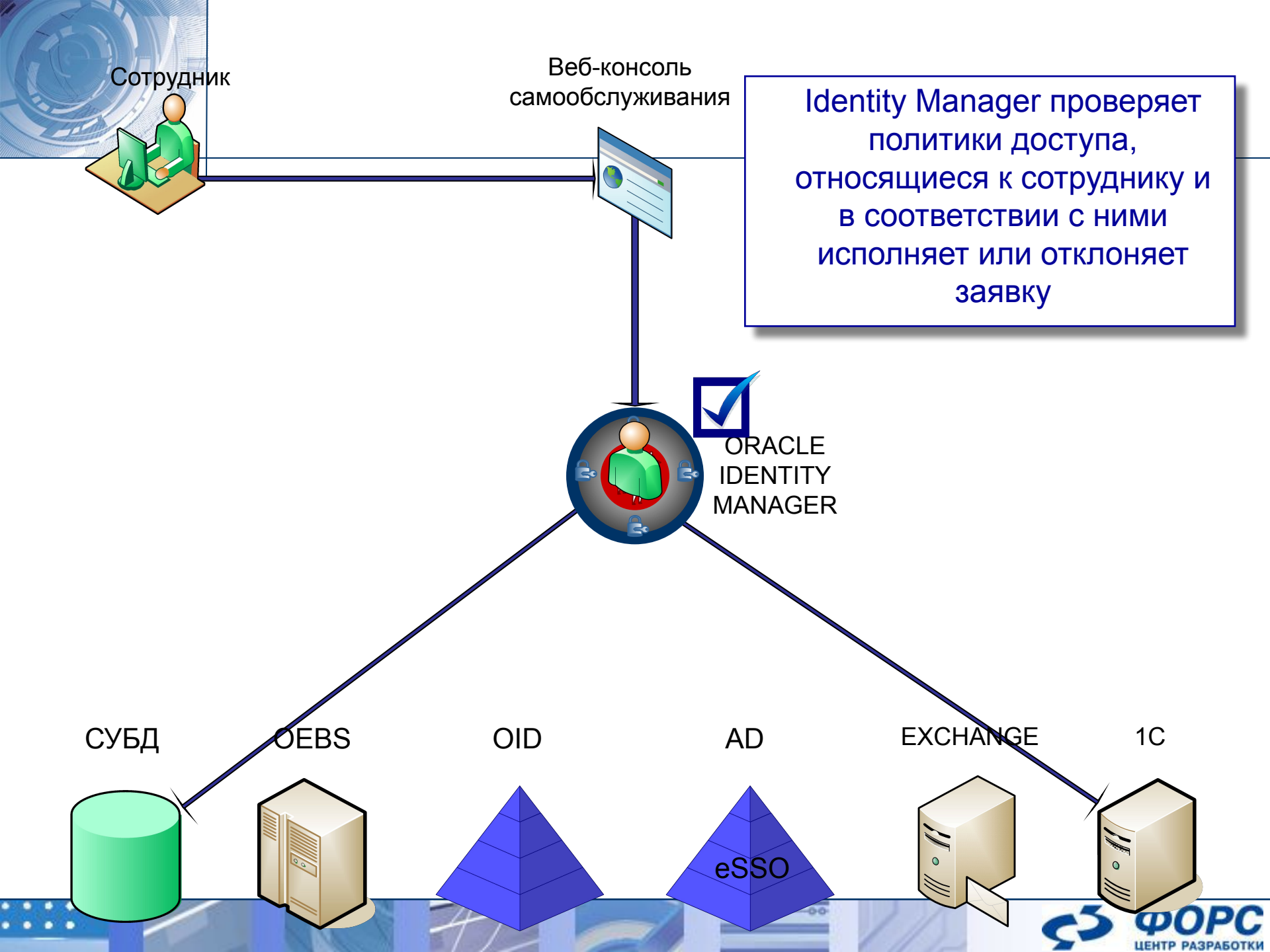
OID

AD

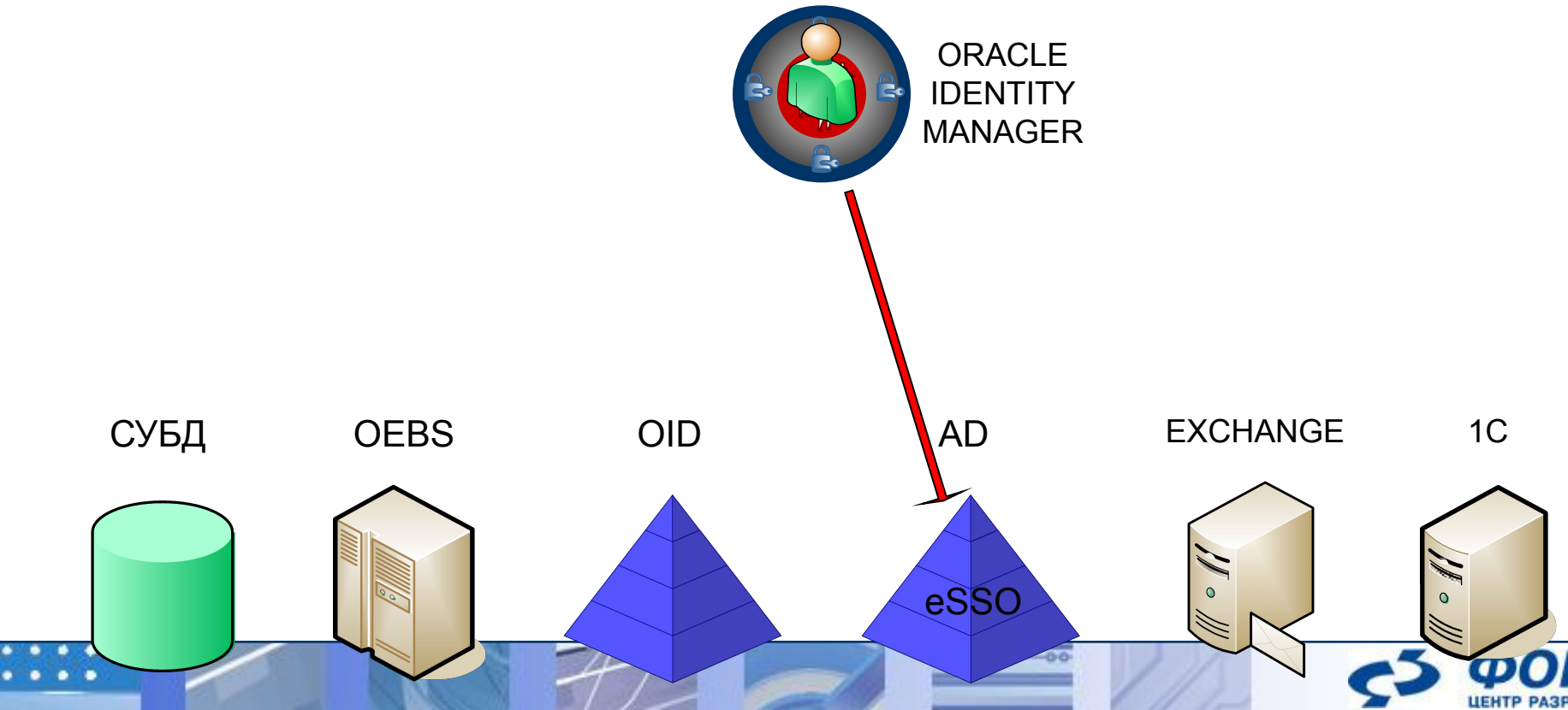
EXCHANGE

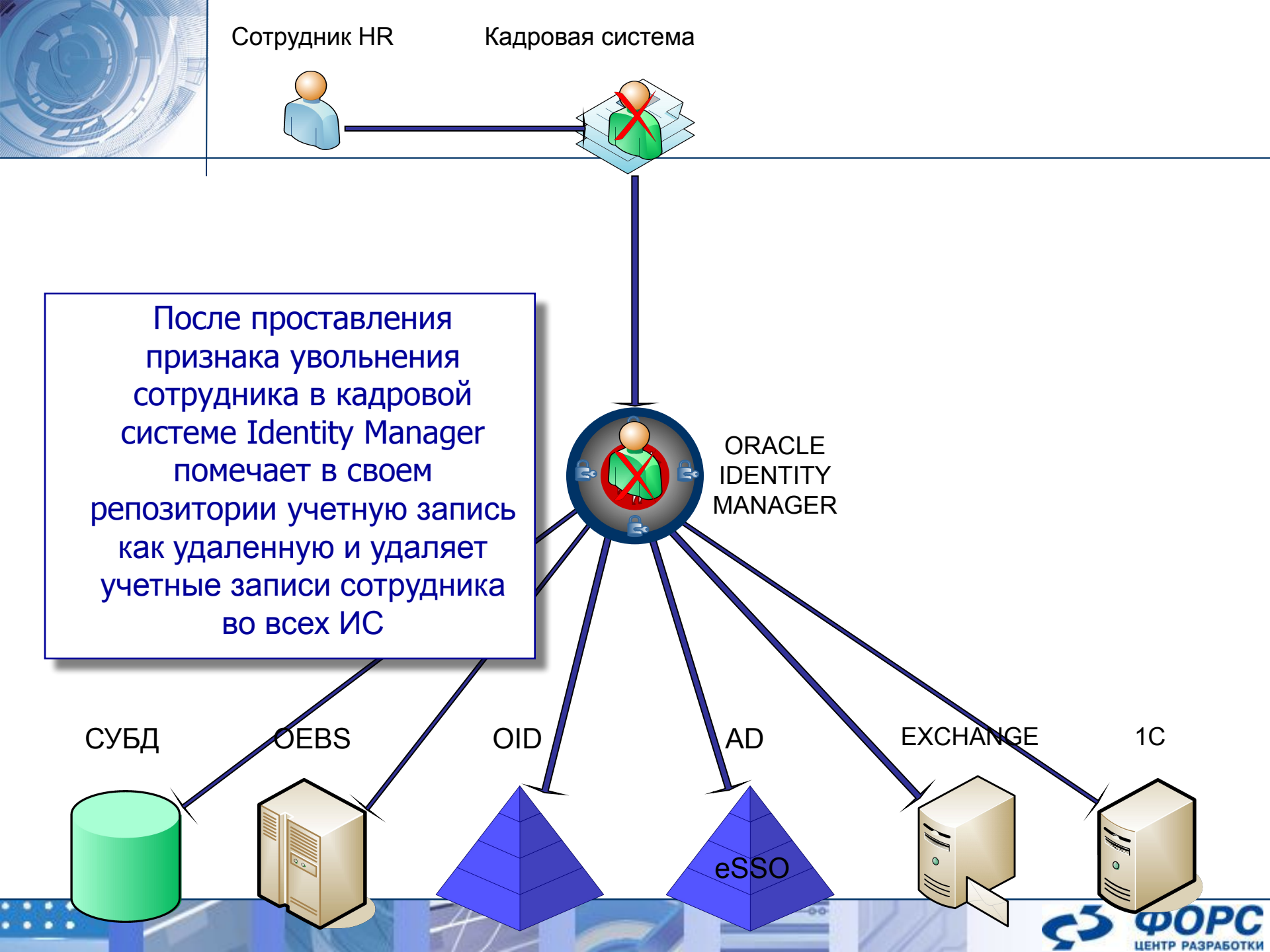


ФОРС
ЦЕНТР РАЗРАБОТКИ

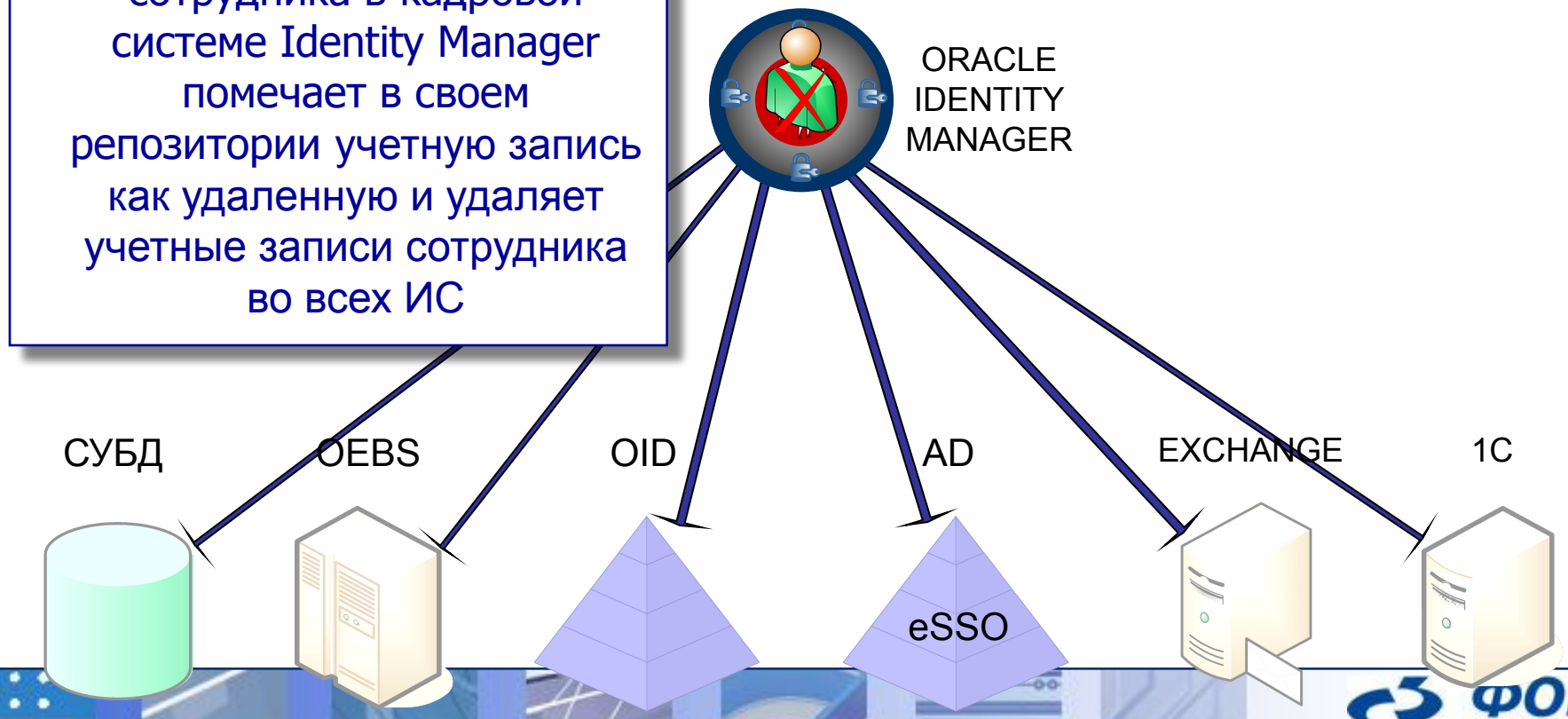

Сотрудник
Веб-консоль самообслуживания
Identity Manager проверяет политики доступа, относящиеся к сотруднику и в соответствии с ними исполняет или отклоняет заявку
ORACLE IDENTITY MANAGER
СУБД
OEBS
OID
AD
EXCHANGE
1C
eSSO

Identity Manager проверяет политики доступа, относящиеся к сотруднику и в соответствии с ними исполняет или отклоняет заявку




Сотрудник HR
Кадровая система
После проставления признака увольнения сотрудника в кадровой системе Identity Manager помечает в своем репозитории учетную запись как удаленную и удаляет учетные записи сотрудника во всех ИС
ORACLE IDENTITY MANAGER
СУБД
OEBS
OID
AD
EXCHANGE
1C
eSSO

После проставления признака увольнения сотрудника в кадровой системе Identity Manager помечает в своем репозитории учетную запись как удаленную и удаляет учетные записи сотрудника во всех ИС



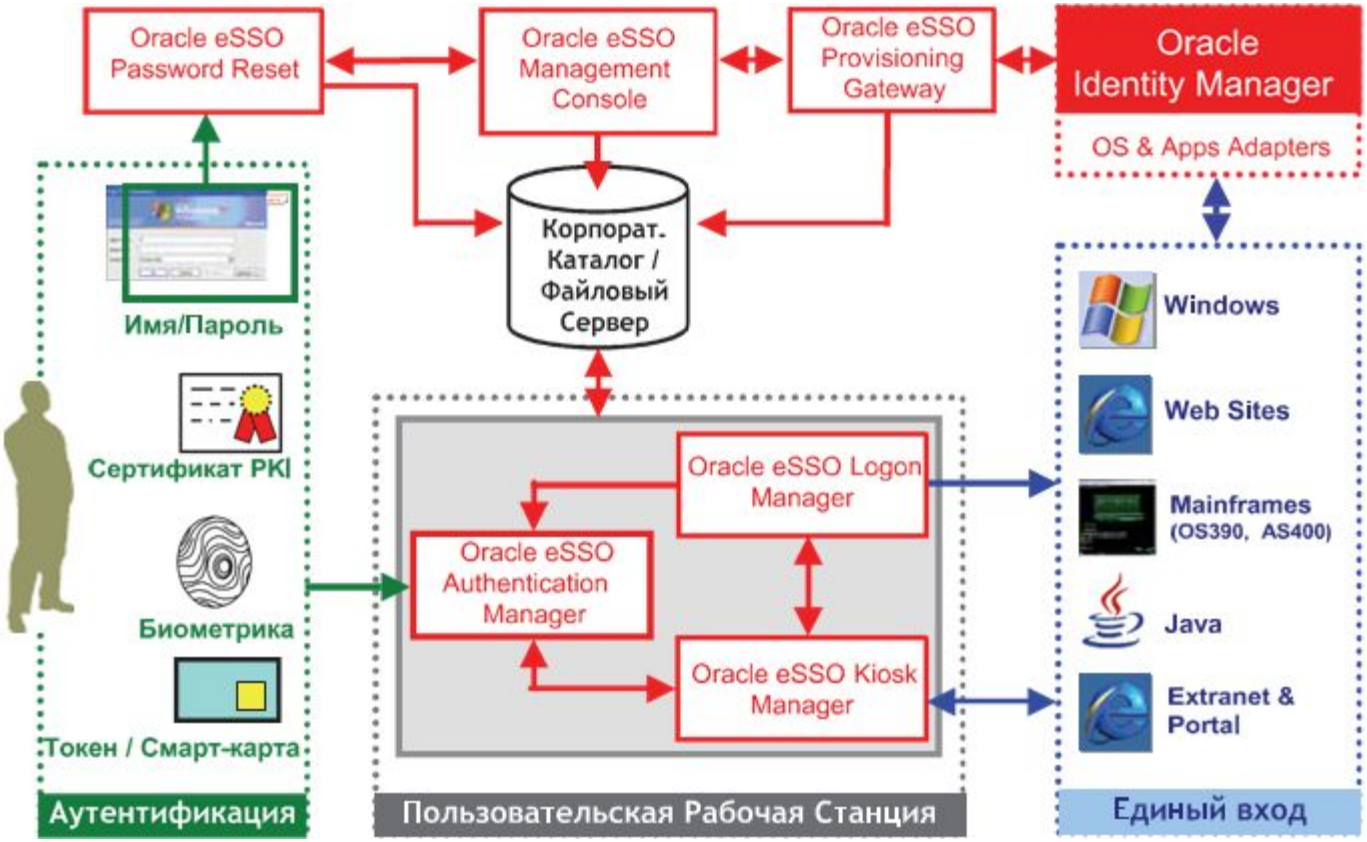
Практические аспекты внедрения Oracle Identity Manager

- Целесообразность использования кадровой системы в качестве доверенного источника данных
- Важность синхронизации организационных структур в целевых системах с эталонной в кадровой системе
- Преимущества наличия и использования ролевой модели
- Настройка аудита действий администраторов
- Необходимость регулярного проведения аттестаций
- Возможности разделения/делегирования полномочий
- Интеграция с существующими системами заявок
- Возможность управления материальными ресурсами
- Отказоустойчивость
- Рекомендации по защите хранилища данных Oracle Identity Manager

Oracle eSSO: основные возможности

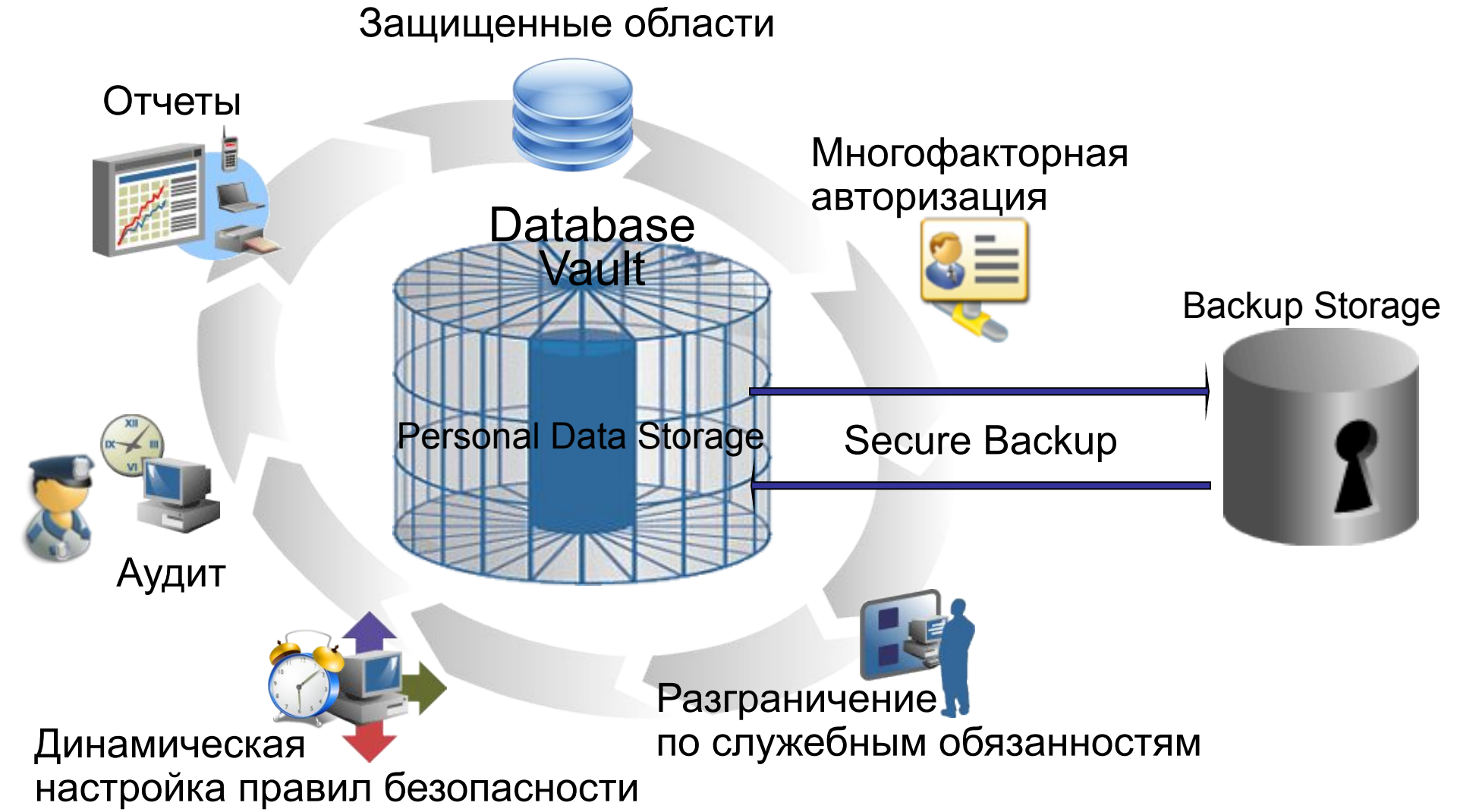
- ✔ Пользователю необходимо знать ОДИН пароль
- ✔ Пользователь вводит пароль ОДИН раз и получает доступ к необходимым ресурсам
- ✔ Интеграция со смарт-картами и токенами
- ✔ Готовая поддержка большинства приложений, быстрая интеграция с нестандартными приложениями
- ✔ Не требует изменений существующей ИТ- инфраструктуры
- ✔ Интегрируется с Oracle Identity Manager

Практические аспекты внедрения Oracle Enterprise Single Sign-On



- Работает в связке с Oracle Identity Manager
- Поддерживает различные типы аутентификации

Решение по защите баз данных от высокопривилегированных пользователей

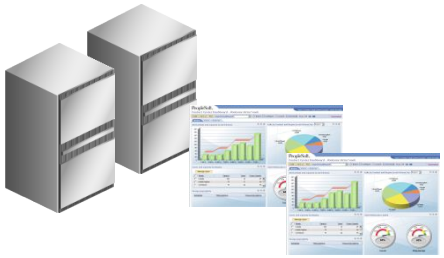


Что такое и для чего нужен Oracle Information Rights Management

Два типа информации:

Структурированная и неструктурированная

Структурированная –> 10-20%

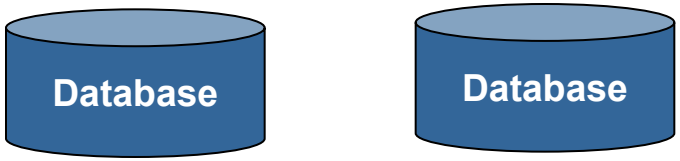


Business Intelligence

Data Mining

Data Warehousing

. . .



Неструктурированная –> 80-90%

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)

Как работает
Oracle Information Rights Management

Схема работы Oracle IRM

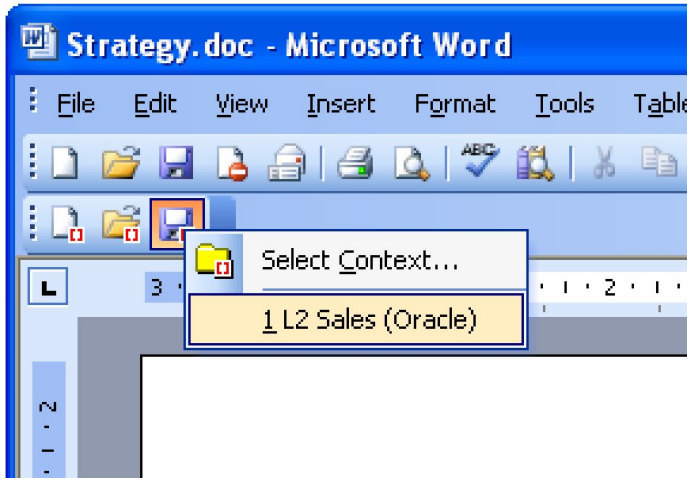
1) Все документы «запечатываются» (seal)
2) Ключи для раскодировки находятся на сервере
3) Для доступа к ключам/серверу необходимо пройти аутентификацию
4) Клиентские приложения (MS Word, Adobe Acrobat Reader и т.д.) работают под управлением клиента Oracle IRM, который гарантирует права использования документов

Что позволяет сделать Oracle IRM

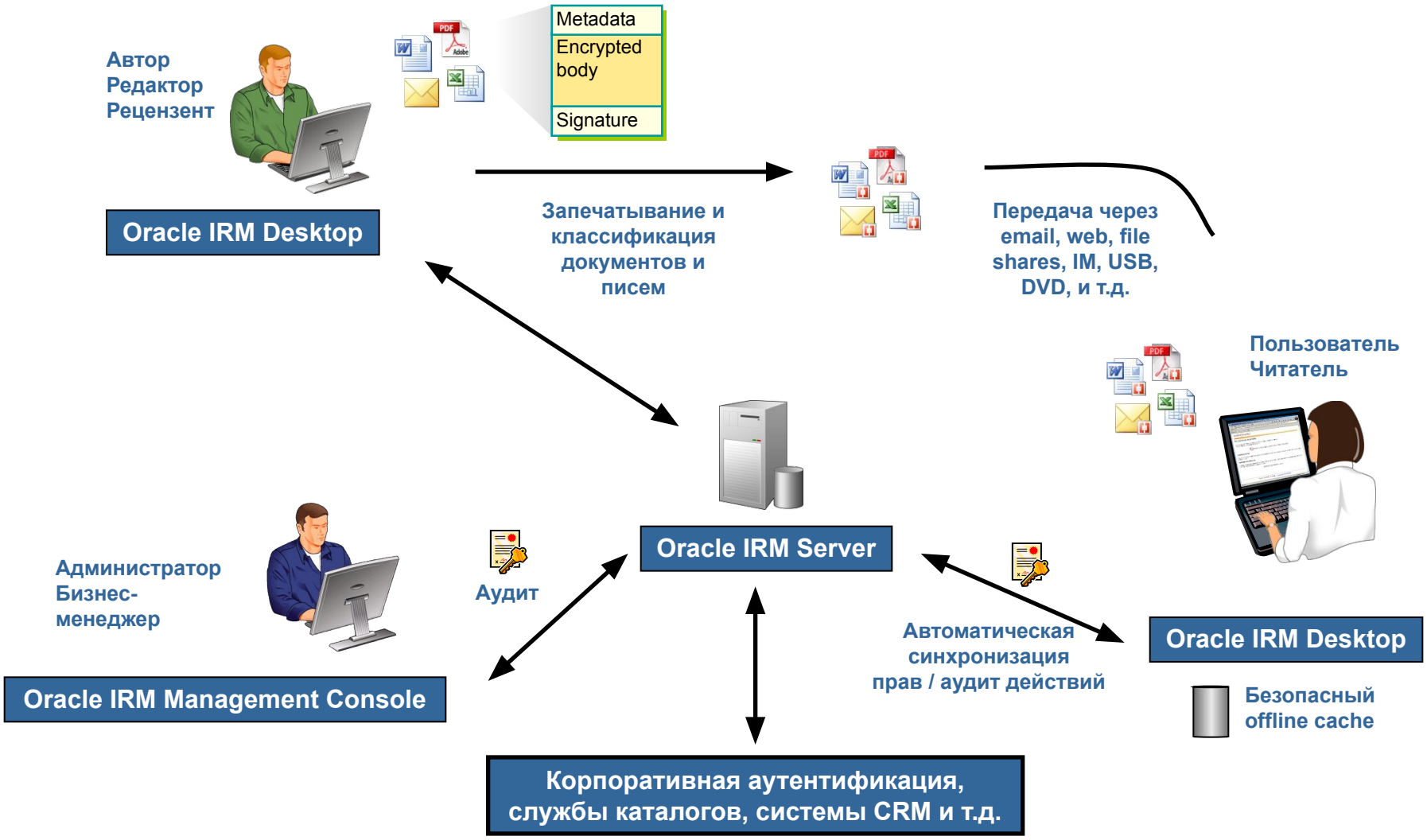
- Исключить неавторизованный доступ ко всем копиям
- Только авторизованные пользователи могут открывать/редактировать эти копии
- Использование документов и все попытки доступа централизованно регистрируются, и по результатам делаются отчёты
- Доступ ко всем копиям может быть в любое время централизованно изъят
- Можно управлять использованием версий документов
- Управление и контроль не останавливаются на межсетевом экране

Oracle IRM: Поддержка приложений

- Microsoft Office 2000-2007 (Word, Excel, PowerPoint)
- Adobe Acrobat или Reader 6.0+ (Windows и Mac OS)
- Email: Microsoft Outlook 2000-2007, Lotus Notes 6.5+ и Novell GroupWise 6.5-7.0
- Email: 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 (требует соответствующих программ-просмотра)



Как работает Oracle IRM



Oracle IRM: Криптографическая защита

Oracle Information Rights Management использует стандартные криптографические алгоритмы для:

- Шифрования и цифровой подписи документов и электронных сообщений - «запечатывание». Обычно это повышает размер файла менее чем на 1%.
- Защиты сетевых телекоммуникаций между сервером и агентами Oracle IRM
- Защиты прав доступа на агенте Oracle IRM
- Работы с контрольными суммами программных компонент Oracle IRM

IRM: Криптография и безопасность

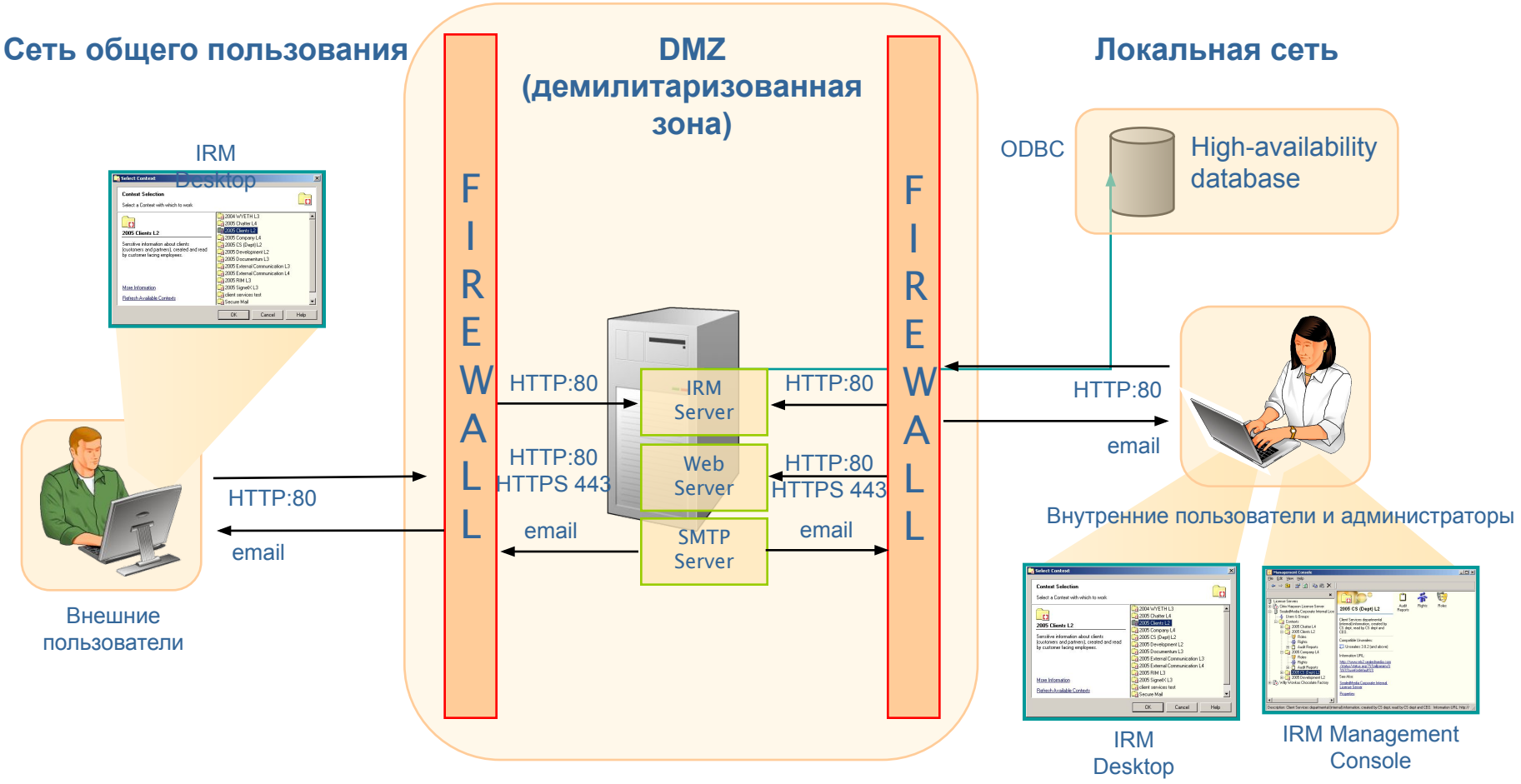
Используются криптографические алгоритмы:

- Шифрование AES 128-бит для тел документов
- RSA 1024-бит для обмена ключами и цифровых подписей
- Tiger Hash message digest для контрольных сумм
- В следующей версии – поддержка Microsoft CryptoAPI

Дополнительная защита:

- Низкоуровневый контроль вызовов функций OS и лазеек
- Microsoft Authenticode, Layered code and interface obfuscation, software obfuscation
- Поддержка доверенных часов
- Незащищённая информация никогда не пишется на диск

Пример использования Oracle IRM в корпоративной сети



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.)

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):

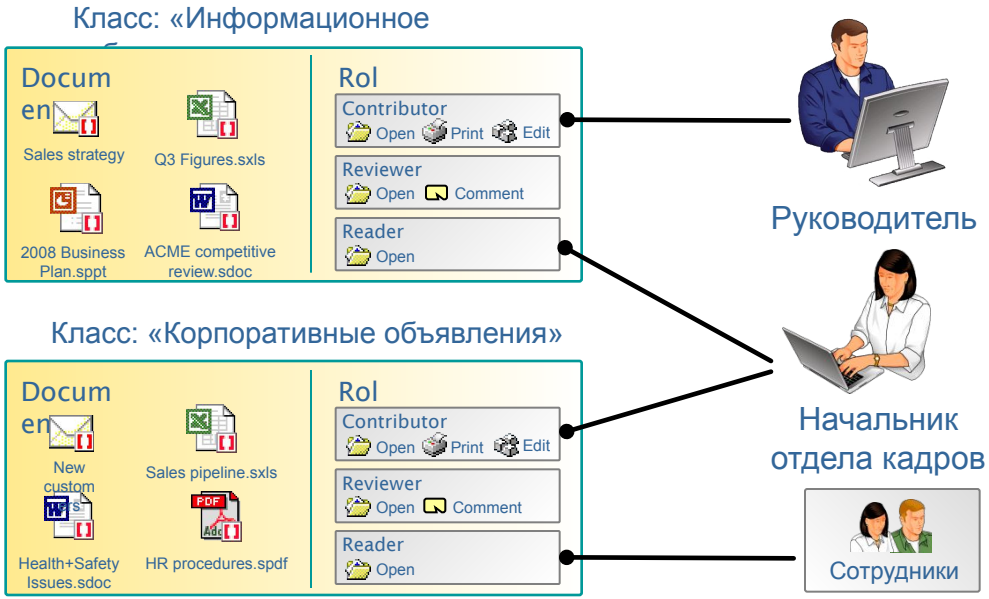
- Интеграция с SOA (BPEL workflow)
- Автоматическое «запечатывание», встроенное в собственный документооборот
- Автоматическое «запечатывание» и «распечатывание» файлов, покидающих или попадающих в хранилище
- Временное «распечатывание» для полнотекстового индексирования

Классификация документов (контексты безопасности - context)

- Управление правами доступа сотен пользователей к тысячам документов непрактично
  - Существенно удобней 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 уровне секретности
  - Темы: Документы руководства, Проект «Моби-Дик», Объявления по компании
  - Уровень секретности: Top Secret, Code Red, Level 1, 2, 3

Управление на основе классификации прав (корпоративное использование)

- Oracle IRM может управлять доступом к информации на основе:
  - Существующих бизнес-процессов
  - Существующих классификаций информации
  - Существующих ролей пользователей
  - Существующих групп пользователей в корпоративном каталоге



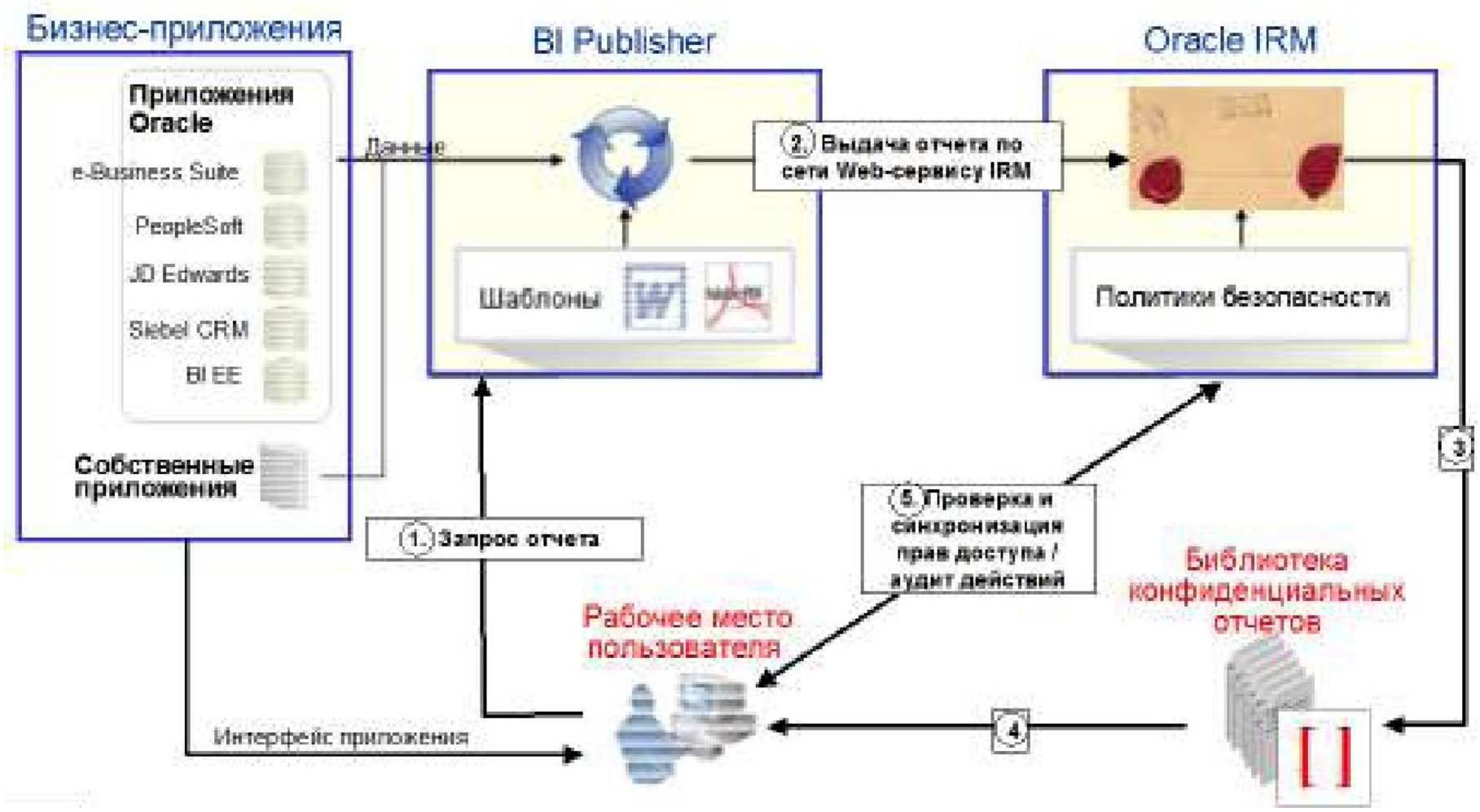
Стандартные роли на доступ к информации

- Oracle IRM определяет стандартный набор ролей

- Роли могут быть связаны с отдельными пользователями, группами и контекстами (типами информации)

- Oracle IRM определяет 4 административные роли:

Защита отчетных документов прикладных систем с помощью Oracle IRM



ВОПРОСЫ

Александр Козлов
Начальник отдела решений информационной безопасности компании «ФОРС – Центр разработки
akozlov@fors.ru
Тел. 787-7040