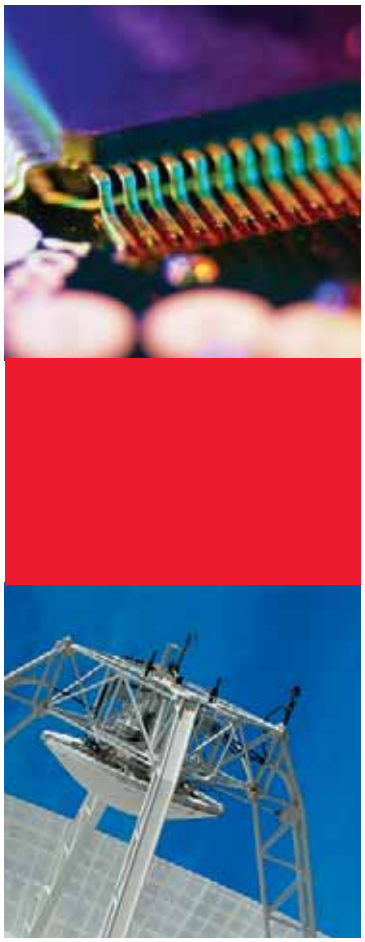
Построение системы управления информационной безопасностью на базе решений Oracle



ORACLE

ORACLE IS THE INFORMATION COMPANY

СОВРЕМЕННЫЕ ВЫЗОВЫ

В настоящее время задачи ускорения бизнеса, возврата на инвестиции в ИТ, вопросы обеспечения безопасности информации становятся приоритетными направлениям работы ИТ-подразделений.

Основными препятствиями на пути реализации этих задач являются:

- Разобщенность средств управления доступом к информационным системам, что приводит к существенному замедлению на предоставление доступа сотрудников к информационным ресурсам. **Следствием является невозможность выполнения сотрудником своих бизнес-функций полном объеме и рост затрат на сопровождение ИТ-инфраструктуры.**
- Трудности при интеграции унаследованных и новых приложений в систему управления ИТ. **Следствием является замедление в выполнении требований бизнеса по реализации новых функций и повышение затрат на поддержку ИТ-инфраструктуры.**
- Отсутствие интеграции систем управления ИТ с HR-системами. **Следствием является неадекватные привилегии сотрудников в ИТ-системе, не соответствующие их должностным обязанностям, что может привести к утечкам конфиденциальной информации и нарушениям в работе ИТ-систем.**

Решения Oracle

Для решения важнейших задач по построению системы управления информационной безопасностью предлагаем использовать систему управления учетными записями на базе решений Oracle Identity Management.

Продукты Oracle Identity Management обладают всеми основными функциями, способными решить поставленные перед ИТ задачи по управлению доступом к информационным ресурсам, а именно:

- Согласованное управление доступом на основе должностных обязанностей с интеграцией с HR-системой, **что сокращает предоставление необходимых полномочий до нескольких минут.**
- Встроенные средства документооборота и возможность интеграции в имеющиеся системы документооборота, **что позволяет интегрировать процессы управления безопасностью в имеющиеся бизнес-процессы управления ИТ.**
- Поддержка всех основных платформ и бизнес-приложений (Microsoft, SAP, Sun Microsytems, HP, IBM, Novell и др.) и простота интеграции с имеющимися приложениями на основе специального инструментария Oracle Adapter Factory, **что сокращает затраты на интеграцию приложений в единую систему управления безопасностью и сохраняет инвестиции в ИТ-инфраструктуру.**
- Контроль соблюдения политики безопасности с использованием гибких средств аудита и отчетности, **что снижает риски и позволяет удовлетворить требованиям руководящих документам в области информационной безопасности.**

В ***Приложении 1*** содержится краткое описание решений Oracle по безопасности, в частности, в классе Identity Management.

Признание на рынке

По информации аналитического агентства Gartner (2007 Gartner UP MQ) **решения Oracle Identity Management являются лидерами** среди решений подобного класса. На основании исследований независимых аналитиков The Radicati Group, опыта реализации подобных проектов и учитывая особенности ИТ в России и СНГ, срок окупаемости системы Oracle Identity Management может не превышать **3-х лет** при достижении ROI не менее **60-70%**.

Oracle уделяет большое внимание стратегическому развитию линейки Identity Management и ее интеграции с бизнес-приложениями. Основными стратегическими направлениями развития технологий Oracle являются:

- **Полнота.** Спектр решений Oracle по управлению безопасностью уровня предприятия является самым полным на рынке (по информации Gartner, "Oracle предлагает полный портфель решений");
- **Интеграция с бизнес-приложениями.** Решения Oracle Identity Management уже интегрированы с большинством бизнес-приложений и инфраструктурных решений (от Oracle, SAP, Siebel, PeopleSoft, Micrososoft, IBM, HP, Sun и др.) Использование технологии SOA, на базе которых развиваются решения Oracle Identity Manager, позволит интегрировать технологии безопасности в бизнес приложения на уровне Web-сервисов, что резко сократит стоимость и сроки создания интегрированной системы управления безопасностью.
- **Ориентация на открытые стандарты.** Oracle поддерживает и активно участвует в разработке практически всех стандартов управления безопасностью (OASIS, Liberty Alliance и др.)

По заявлению аналитиков Gartner **"Стратегия Oracle выглядит лучшей среди всех вендоров"** (2006 Gartner UP MQ). По словам аналитиков Burton Group **"Oracle сейчас может рассматриваться, как основной поставщик решений Identity and Access Management"**.

Выполнение требований законодательства РФ

Решения Oracle по безопасности позволяет существенным образом облегчить выполнение технических требований Законодательства РФ по защите конфиденциальной информации, в частности **Закона о персональных данных**. В ***Приложении 2*** содержится анализ выполнения требований Закона о персональных данных на базе решений Oracle.

По отношению к финансовым организациям решения Oracle способствуют выполнению требований **Стандарта Банка России СТО БР ИББС-1.0-2006**. В ***Приложении 3*** содержится анализ выполнения требований данного Стандарта на базе решений Oracle.

Вывод

Решения и стратегия Oracle позволяют в полной мере реализовать систему управления информационной безопасностью, интегрированную с бизнес-процессами компании, а также обеспечить сохранность инвестиций в информационную инфраструктуру.

Приложение 1
Решения Oracle по обеспечению информационной безопасности

Компоненты	Описание
Identity & Access management	Комплекс решений по управлению безопасностью ИТ
Oracle Identity Manager	Средство согласованного управления ролями и учетными записями в гетерогенной среде с поддержкой управляющего документооборота (workflow) на основании должностных обязанностей сотрудника: Решаемые задачи: • Автоматическое создание учетных записей пользователей в соответствии с должностными обязанностями; •Назначение / отзыв / изменение привилегий; •Контроль действий администраторов целевых систем; •Отчетность (оперативная / историческая); •Проверка неизбыточности полномочий пользователей; •Выявление «сиротских» учетных записей; •Разделение / делегирование полномочий; •Самообслуживание пользователей. Подробнее: http://www.oracle.com/products/middleware/identity-management/identity-manager.html
Oracle Access Manager	Средство согласованного ролевого управления доступом к гетерогенным Web-ресурсам с поддержкой управляющего документооборота (workflow). Решаемые задачи: •Единая точка доступа к Web-ресурсам; •Однократная аутентификация (SSO) для Web-ресурсов; •Интеграция с существующими системами защиты; •Управление паролями. Подробнее: http://www.oracle.com/products/middleware/identity-management/access-manager.html
Oracle Enterprise Single Sign-on (ESSO)	Решение, обеспечивающее однократную аутентификацию в распределенных гетерогенных системах. Решаемые задачи: •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; Подробнее: http://www.oracle.com/products/middleware/identity-management/enterprise-single-sign-on.html
Web Services Manager	Решение по настройке параметров безопасности (аутентификация, правила доступа) Web-сервисов в рамках архитектуры SOA. Решаемые задачи: •Единая политика безопасности для всех SOA-приложений; •Функции безопасности универсальны и могут быть использованы всеми приложениями; •Централизованный контроли и мониторинг безопасности Web-сервисов. Подробнее: http://www.oracle.com/products/middleware/identity-management/web-services-manager.html
Oracle Identity Federation	Средство установления доверительных отношений между автономными системами для совместного использования учетной информации. Решаемые задачи: •Доверенные отношения между автономными системами разных организаций; •Самостоятельность управления политикой безопасности для каждой организации; •Однократная аутентификация пользователя во всех доверенных системах; Подробнее: http://www.oracle.com/products/middleware/identity-management/identity-federation.html

Oracle Virtual Directory	Средство организации единого представления данных из различных хранилищ информации. Решаемые задачи: •Универсальное представление данных из различных источников в виде LDAP-каталога; •Нет необходимости синхронизации данных между источниками; Подробнее: http://www.oracle.com/products/middleware/identity-management/virtual-directory.html
Management Pack for Identity Management	Средство управления и мониторинга SLA для компонент Identity management. Решаемые задачи: • Отслеживание уровня сервиса (SLA) компонент Identity Management на функциональном уровне; • Мониторинг ключевых показателей (KPI) сервисов Identity Management; • Интеграция в единую консоль управления Oracle Enterprise Manager http://www.oracle.com/products/middleware/identity-management/management-monitoring.html
Identity and Access management Suite	Комплексное решение, включающее в себя следующие компоненты: • Oracle Identity Manager • Oracle Internet Directory • Oracle Virtual Directory • Oracle Access Manager • Oracle Identity Federation
Database Security	**Комплекс решений обеспечения безопасности баз данных**
Database Vault	Решение, обеспечивающее дополнительное разграничение полномочий внутри базы данных с реализацией ограничения доступа к данным защищаемых приложений со стороны администратора, а также ограничения доступа и контроль выполнения команд в зависимости от времени, IP-адреса, операции и т.д. Подробнее: http://www.oracle.com/database/database-vault.html
Label Security	Решение по реализации мандатного доступа (с использованием меток) к данным в базе данных. Подробнее: http://www.oracle.com/database/label-security.html
Advanced Security Options	Решение, реализующее усиленную аутентификацию при доступе к базе данных (X.509, Kerberos, Radius), защиту клиентского трафика (SSL), прозрачное шифрование критической информации в базе данных и их защиту на физических носителях информации. Подробнее: http://www.oracle.com/database/advanced-security.html
Secure Backup	Решение, обеспечивающее дополнительную защиту резервных копий данных баз данных и файлов операционной системы на магнитных лентах. Подробнее: http://www.oracle.com/database/secure-backup.html
Audit Vault	Решение консолидации, хранения и анализа данных аудита из различных источников. Подробнее: http://www.oracle.com/technology/products/audit-vault/index.html

Приложение 2.
Применение решений Oracle по информационной безопасности для выполнения требований Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ “О персональных данных”

Данный документ содержит анализ соответствия решений Oracle по обеспечению информационной безопасности (ИБ) требованиям Федерального закона Российской Федерации от 27 июля 2006 г. N 152-ФЗ “О персональных данных”.

№	Требование закона	Реализация с помощью решений Oracle
1	Статья 5 п.5 (Недопустимость объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных)	Использование **Database Vault** позволяет разделить массивы различных данных на основе создания защищенных областей (realms).
2	Статья 6 п.3 (Обезличивание персональных данных)	Использование **Advanced Security Options (ASO)** позволяет обезличить персональные данные путем зашифрования колонок данных, идентифицирующих субъекта персональных данных.
3	Статья 7 (Конфиденциальность персональных данных)	Использование решений **Database Vault, Audit Vault Label Security, Identity and Access Management Suite (IAMS), ASO, SecureBackup** обеспечивает конфиденциальность персональных данных за счет использования следующих технологий Oracle: •**IAMS**, реализует механизм разделения полномочий, ролевой механизм управления в масштабах всей информационной системы на основе принципа need-to-know; •**Database Vault** обеспечивает разграничение доступа к полям данных с помощью создания защищенных областей (realms) в СУБД. В частности, персональные данные могут быть защищены от администраторов баз данных; •Технология мандатного механизма контроля доступа с использованием меток конфиденциальности (**Label Security**) обеспечивает построчный контроль доступа к данным; •Технология консолидации данных аудита и своевременного обнаружения злоумышленных действий (**Audit Vault**); •Защита резервных копий (**Secure Backup**); •Защита клиентского трафика (**ASO**); •Прозрачное шифрование данных в СУБД (**ASO**); •Усиленная аутентификация, в т.ч. с использованием сертификатов X.509 (**ASO, IAMS**);
4	Статья 10 (Специальные категории персональных данных)	**IAMS** позволяет разграничить права доступа к персональным данным из различных приложений, **Database Vault и Label Security** обеспечивают гарантию этого доступа на уровне базы данных.
5	Статья 11 (Биометрические персональные данные)	**IAMS, Database Vault и Label Security** обеспечивают сквозной ролевой контроль доступа к биометрическим данным на уровне приложений и уровне базы данных.
6	Статья 14 п.4 (получение информации, касающейся обработки персональных данных)	**IAMS** позвляет ответить на вопрос о том, кто именно, когда, и на основании каких документов имел право доступа к персональным данным. **Audit Vault** позволяет определить, кто и когда обращался к персональным данным.

7	Статья 19 (Меры по обеспечению безопасности персональных данных при их обработке)	**Advanced Security Options** обеспечивает усиленную аутентификацию и шифрование трафика и самих данных, **Secure Backup** – усиленную защиту резервных копий, **Database Vault** – защиту данных от администраторов и разработчиков, **IAMS** – разграничение прав и привилегий со стороны приложений, сервисов и пользователей.
8	Статья 20 п.3 (Возможность ознакомления субъекта с персональными данными)	**IAMS** позволяет обеспечить доступ только к персональным данным, относящимся к субъекту. **Database Vault и Label Security** обеспечивают гарантию защиты этого доступа на уровне базы данных.
9	Статья 21 пп. 1, 2 (блокирование и разблокирование персональных данных)	Блокирование на уровне приложений может быть гарантировано на уровне базы данных с помощью **Label Security** и **Database Vault**.
10	Статья 21 п.3 (Выявление неправомерных действий с персональными данными)	**Audit Vault** позволяет оперативно обнаружить неправомерные действия с перснональными данными и оповестить о необходимых действиях персонал оператора.

Приложение 3
Применение решений Oracle по информационной безопасности для выполнения требования Стандарта Банка России СТО БР ИББС-1.0-2006

Данный документ содержит анализ соответствия решений Oracle по обеспечению информационной безопасности (ИБ) требованиям СТО БР ИББС-1.0-2006.

№	Требование закона	Реализация с помощью решений Oracle
1	п. 5.4 (угрозы со стороны персонала)	**Database Vault** обеспечивает защиту информации в базах данных, в том числе и от администратора баз данных. Средства защиты **Database Vault** позволяют разграничить доступ к защищенным объектам базы данных с использованием дополнительных условий, например, времени доступа, адреса рабочей станции и т.д. **Label Security** реализует мандатный механизм контроля доступа с использованием меток конфиденциальности информации.
2	п.5.6 (злоумышленник изучает объект нападения)	Средствами контроля выполнения правил доступа (аудит в **Database Vault**) предотвращается возможность исследования объекта нападения путем эксперимента.
3	п.5.9 (повышение сложности управления ИБ порождает новые уязвимости)	Внедрение прозрачного шифрования полей таблиц баз данных и использование **Database Vault** не требуют каких-либо изменений в ранее разработанных средствах защиты информации и прикладных системах.
4	пп. 5.12, 5.13 (требование наличия процессного подхода)	**Identity and Access Management Suite (IAMS)** обеспечивает бизнес-процессы управления учетными записями и доступом к информационнвм ресурсам. Бизнес-процессы проектируются с помощью специального инструментария и автоматически исполняются системой **IAMS**
5	п.7.6 и п.8.2.3.10 (доступ к оборудова¬нию)	Применение опции прозрачного шифрования (**TDE**) обеспечивает защиту информации на физических носителях
6	пп. 7.13, 7.14, 8.2.3.8, 8.2.3.9 (управление операционным рисками и защита от угроз)	Использование решений **Database Vault, Audit Vault Label Security, IAMS, Advanced Security Options (ASO), SecureBackup** снижает операционные риски (ошибочных действий пользователя, действий внутренних злоумышленников, отказ в обслуживании) за счет реализации: •оптимизации прав доступа и привилегий (need to know) (**IAMS, Database Vault, Label Security**); •разграничения полномочий (Segregation of duties) (**IAMS, Database Vault**); •мандатного доступа (**Label Security**); •дополнительных механизмов защиты СУБД (**Database Vault, Label Security**); •консолидации данных аудита и своевременного обнаружения злоумышленных действий (**Audit Vault**); •защиты резервных копий (**Secure Backup**); •защиты клиентского трафика (**ASO**); •прозрачного шифрования данных в СУБД (**ASO**); •усиленной аутентификации, в т.ч. с использованием сертификатов X.509 (**ASO, IAMS**); •горячего резервирования компонент системы защиты (**Real Application Cluster**); •оперативного мониторинга уровня обслуживания (**SLA**) для сервисов безопасности (**IAMS**).

7	пп. 8.2.2.1- 8.2.2.27 (ролевой доступ)	**IAMS** реализует ролевой механизм управления в масштабах АБС. Даже если какое-то приложение не реализует ролевой доступ, IAMS интегрирует его в глобальную систему ролевого управления. **IAMS** обеспечивает создание иерархии ролей, синхронизированной с наборами бизнес-функцией, необходимых сотруднику, в соответствии с организационной структурой. IAMS обеспечивает импорт организационной структуры из HR-систем. **IAMS** обеспечивает наличие ролей по обеспечению ИБ с правами доступа, необходимыми для управления параметрами ИБ. **IAMS** реализует механизм разделения полномочий (Segregation of Duties) для избежания исполнения критичных операций одним сотрудником. **Database Vault** интегрирует механизмы защиты информации СУБД в систему ролевого доступа.
8	п. 8.2.3.1 (обеспечение ИБ на стадиях жизненного цикла)	**IAMS** реализует разграничение ролей разработчиков, заказчиков и других участников жизненного цикла АБС по доступу к ресурсам АБС. **Database Vault** обеспечивает разграничение доступа к полям данных, используемых при разработке, тестировании и эксплуатации с помощью создания защищенных областей (realms) в СУБД.
9	п. 8.2.3.4 (ввод и снятие АБС с эксплуатации)	**IAMS** обеспечивает автоматическое создания или удаление учетных записей пользователей и разработчиков при вводе и снятии с эксплуатации. При этом данный процесс может производиться с участием подразделения ИБ на уровне согласования данных операций. Процедура согласования реализуется в составе единой системы документооборота по управлению безопасностью из состава **IAMS**.
10	8.2.4.1 (принципы безопасности)	**IAMS** обеспечивает выполнение принципов “need to know”, “know your Customer”, “know your Employee” за счет: •четкого определения ролей пользователя в АБС; •соответствия ролей **IAMS** бизнес-ролям пользователя;
11	п. 8.2.4.3, раздел 1 (требования к парольной политике)	**IAMS** реализует синхронизацию паролей в компонентах АБС и единую парольную политику в АБС. **Enterprise Single Sign-On (ESSO)** обеспечивает однократную аутентификацию (Single-Sign-On) в компонентах АБС с реализацией проверки качества паролей и возможностью самостоятельной смены и восстановления пароля пользователем. При этом **ESSO** полностью интегрирована с **IAMS**, что позволяет обеспечить согласованное упрвление учетными записями и параметрами аутентификации.
12	п. 8.2.4.3, раздел 2 (требования к порядку назначения доступа)	**IAMS** обеспечивает документооборот по согласованию назначения прав и привилегий в АБС. При этом правила согласования доступа, в том числе участие функционального руководителя, задаются централизованно, с помощью инструментария дизайна бизнес-процессов на стадии разработки политики безопасности.
13	п. 8.2.4.3, раздел 5 (требования к регистрации)	**IAMS** обеспечивает регистрацию истории назначения прав и привилегий пользователя как в разрезе компоненты АБС, так и в разрезе времени соответствующего назначения. **Audit Vault** реализует консолидацию журналов регистрации различных компонент АБС, их хранение и оперативную отчетность об активности пользователей с выдачей предупреждений об инцидентах и трендах активности пользователей АБС.

14	п. 8.2.8.5 (требование о недопустимости полноты полномочий у одного сотрудника) п. 8.2.9.6 (разграничение полномочий администратора АБС и администратора информационной безопасности)	**IAMS** реализует разделение полномочий (Segregation of Duties) на уровне ролей АБС. **Label Security** реализует мандатный способ разгра¬ниче¬ния полномочий с использованием меток конфиденциаль¬ности информации. **Database Vault** обеспечивает разделение полномочий по доступу к критичной информации в СУБД с использованием меток безопасности, в том числе, на уровне администратора баз данных.
15	п. 9.7.1 (функции службы информационной безопасности)	Решения Oracle (**IAMS, Database Vault, Audit Vault**) предоставляет службе ИБ инструмент управления и контроля политики безопасности.
16	п.10 (порядок аудита АБС)	Решения Oracle (**IAMS, Database Vault, Audit Vault**) обеспечиваюс генерацию, консолидацию и хранение данных аудита действий пользователя в АБС, а также инструмент построения отчетов для аудиторов АБС.
17	п.11 (модель зрелости менеджмента ИБ)	**IAMS** способствует достижению 4-го уровня зрелости за счет встроенных возможностей автоматической оптимизации (Attestation) имеющейся ролевой модели доступа в АБС.

КОРПОРАЦИЯ ORACLE

Oracle Россия
119435, Москва
Саввинская набережная, 15
Тел.: +7 (495) 641 1400
Факс: +7 (495) 641 1414
Email: oracle_ru@oracle.com
Internet: www.oracle.com/ru/

191186, Санкт-Петербург
Невский пр., 25
Тел.: +7 (812) 363 3257
Факс: +7 (812) 363 3258
Email: oracle_ru@oracle.com
Internet: www.oracle.com/ru/

Oracle Украина
04070, Киев
ул. Фроловская, 911
офисный центр «Swiss House»
Тел.: +380 (44) 490 9050
+380 (44) 490 9051
Факс: +380 (44) 490 9052

Oracle Казахстан
480099, Алматы
микрорайон Самал2,
Самал Тауэрс, оф. 97, блок А2, 6-й этаж
Тел.: +7 (727) 258 4748
Факс: +7 (727) 258 4744