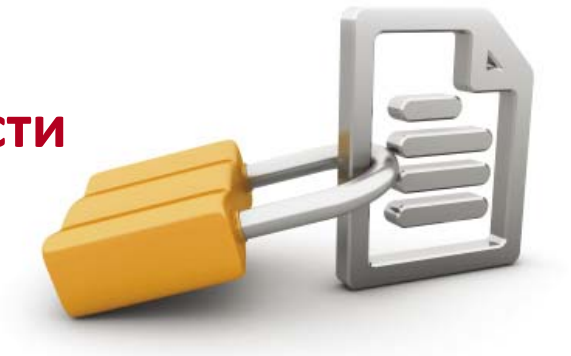
Комплексное обеспечение информационной безопасности на базе технологий Oracle



В области решений по информационной безопасности (ИБ) ФОРС предлагает полный спектр услуг на основе технологий Oracle:

- Реализация проектов по внедрению средств защиты и решений ИБ;
- Реализация комплексных проектов по обеспечению ИБ (в т.ч. в области защиты персональных данных);
- Реализация проектов по защите печатных копий документов;
- Аудит на соответствие обязательным нормативам и отраслевым требованиям;
- Расширенная техническая поддержка информационных систем по обеспечению ИБ на базе ПО Oracle.

Предлагаемые ФОРС услуги и решения в области информационной безопасности позволяют создать целостную концепцию информационной защиты предприятия, учитывающую специфику бизнес-процессов, корпоративную политику безопасности и применяемые технологии. При этом проекты по внедрению систем информационной безопасности могут быть как самостоятельными, так и являться частью крупных комплексных проектов по автоматизации.

Деятельность компании «ФОРС» в сфере информационной безопасности ведется на основании лицензий Федеральной службы безопасности (ФСБ России) и Федеральной службы по техническому и экспортному контролю (ФСТЭК).

Среди клиентов «ФОРС» в области решения задач информационной безопасности такие предприятия как:

- Правительство Хабаровского края;
- Правительство г.Москвы;
- ОАО «Промсвязьбанк»;
- ОАО «Межрегиональная распределительная сетевая компания Центра и Приволжья»;
- ФГУП «Информзащита»;
- ГК «Спортмастер» и др.

О компании ФОРС

ФОРС - группа компаний, сфера деятельности которых охватывает полный комплекс задач по поставке программно-аппаратного обеспечения, построению информационных систем, инфраструктурных решений, технической поддержке и обучению.

ФОРС - ведущий разработчик, интегратор и дистрибутор решений Oracle, обладает статусом платинового партнера корпорации Oracle (Platinum Partner).

Основными направлениями деятельности компании являются:

- ИТ-консалтинг, аудит и выработка рекомендаций по оптимизации информационных систем;
- Поставка ПО Oracle;
- Поставка и внедрение программно-аппаратных комплексов Oracle;
- Заказная разработка программного обеспечения;
- Внедрение и интеграция информационных систем;
- Техническая поддержка и сопровождение;
- Обучение технологиям и продуктам Oracle, сертификация ИТ-специалистов в Учебно-консультационном центре «ФОРС».

ФОРС

ORACLE Platinum Partner

Управление доступом

Главные причины актуальности задач по обеспечению ИБ и управлению доступом:

Накопление большого количества критичных данных:

- профессиональный интерес злоумышленников к данным;
- сильное влияние инсайда на показатели компаний;
- возможность больших репутационных и финансовых потерь;
- увеличение количества "внутренних" угроз в компании (порядка 80% от общего числа);
- нарушение конфиденциальности данных или снижение продуктивности;
- риск нарушения законодательства.

Рост количества прикладных систем:

- увеличение числа администраторов систем;
- увеличение времени выполнения заявок на доступ к системам;
- сложность реализации и отслеживания политик доступа сотрудников к системам и данным;
- сложность реализации взаимодействия бизнес-партрнеров;
- усложнение схем взаимодействия с бизнес-партнерами;
- необходимость запоминания пользователями большого количества паролей.

Ужесточение законодательства в области работы с данными:

- конфиденциальность личных данных;
- международные и национальные законы;
- нормативные и отраслевые стандарты;
- соответствие требованиям аудита.

Oracle Identity & Access Management Solutions

Концепция Oracle Identity and Access Management (IAM) позволяет решать следующие задачи, связанные с управлением доступом:

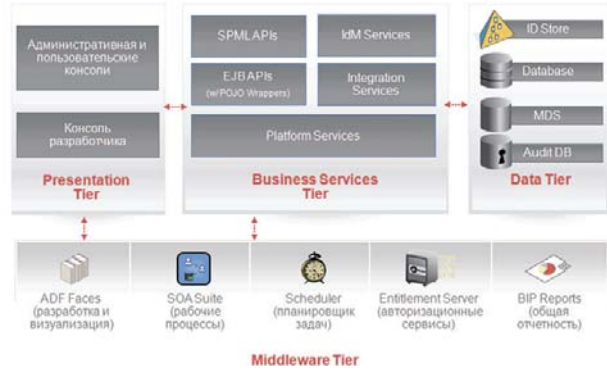
- реализация для управляемых (целевых) систем следующих базовых принципов информационной безопасности:
  - принцип минимальных привилегий (Least privilege);
  - принцип предоставления доступа к информации в рамках должностных обязанностей (Need-to-know).
- автоматизация и централизация процессов управления учетными записями и полномочиями доступа к выбранным целевым системам;
- реализация процессов согласования электронных заявок на предоставление доступа полномочными лицами и требований политик по управлению доступом;
- реализация и централизованное управление парольными политиками для управляемых (целевых) систем;
- автоматизация процессов аудита прав доступа и построение матрицы доступа;
- автоматизация процесса ревизии доступа (процесса пересмотра прав доступа) к выбранным управляемым (целевым) системам;
- реализация процесса ролевого управления доступом;
- реализация механизма единой и однократной аутентификации;
- реализация управления привилегированными и административными учетными записями.

Oracle IAM включает в себя следующие компоненты:

- Oracle Identity Manager;
- Oracle Access Manager;
- Oracle Enterprise Single Sign-on;
- Oracle Identity Analytics;
- Oracle Web Enterprise Single Sign-on;
- Oracle Information Rights Management.

Oracle Identity Manager (OIM)

Решение по централизованному управлению учетными записями и правами доступа пользователей в гетерогенной среде.



Решаемые задачи и особенности:

- управление жизненным циклом учетных данных сотрудников и внешних пользователей;
- управление ролями и привилегиями сотрудников по доступу к бизнес-приложениям с использованием кадровой информации, механизма заявок и согласований;
- периодический контроль неизбыточности полномочий пользователей;
- управление парольной политикой для бизнес-приложений;
- контроль целостности эталонной модели прав, аудит и историческая отчетность по всем операциям и состояниям ролей и привилегий в приложениях;
- разделение / делегирование полномочий;
- самообслуживание пользователей.

Oracle Access Manager (OAM)

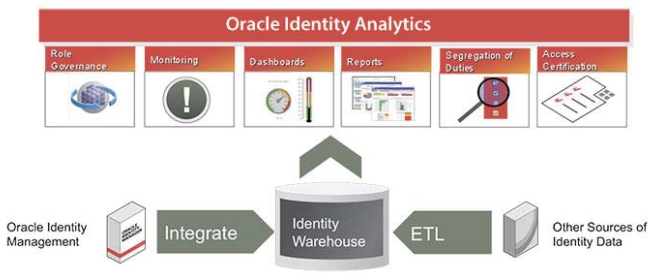
Решение по обеспечению однократной аутентификации и контролю доступа к web-ресурсам.

Решаемые задачи и особенности:

- однократная аутентификация при доступе к нескольким бизнес-приложениям (WebSSO);
- контроль сессий пользователей (ограничение числа, принудительное прерывание);
- аудит и отчетность по доступу пользователей к бизнес-приложениям;
- возможность обеспечения федеративного взаимодействия (Oracle Identity Federation), при котором за счет интеграции с сервером контроля доступа к Web-приложениям обеспечивается WebSSO для бизнес-пользователей, прошедших аутентификацию в домашней доверенной среде, в том числе - предоставляемой поставщиками «облачных» услуг;
- возможность взаимодействия с мобильными клиентами (Oracle Mobile&Social), при котором обеспечивается WebSSO для бизнес-пользователей, использующих смартфоны или планшетные компьютеры для работы с защищаемыми сервисами.

Oracle Identity Analytics (OIA)

Решение по обеспечению ролевого управления учеными записями и правами доступа пользователей в гетерогенной среде.

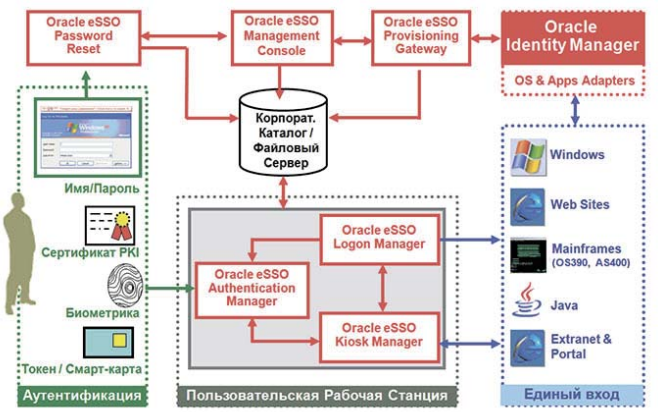


Решаемые задачи и особенности:

- предоставляет функционал, позволяющий администраторам анализировать идентификационные службы на комплексной основе, используя технологии бизнес-аналитики;
- реализует управление жизненным циклом ролевой модели;
- реализует принцип минимальности привилегий и взаимного исключения доступа;
- позволяет выявлять и в режиме реального времени исправлять факты нарушения установленной политики предоставления доступа к информационным ресурсам.

Oracle Enterprise Single Sign-on (ESSO)

Решение по обеспечению однократной аутентификации в распределенных гетерогенных информационных системах.

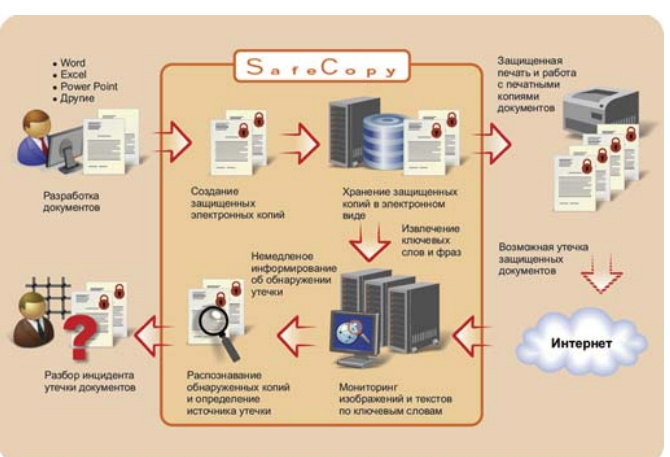


Решаемые задачи и особенности:

- «прозрачное» (SSO) подключение к бизнес-приложениям из любых клиентских программ;
- помощь при смене паролей в бизнес-приложениях с учетом политик сложности;
- интеграция с аппаратными решениями двухфакторной аутентификации (смарт-карты, USB-токены);
- отчетность по подключениям пользователей к бизнес-приложениям.
- готовая поддержка большинства стандартных приложений, быстрая интеграция с нестандартными приложениями;
- не требует изменений существующей ИТ- инфраструктуры.

Защита печатных копий документов

Решение **SafeCopy** позволяет защитить организации от рисков, связанных с несанкционированным распространением печатных копий документов. В сочетании с организационными мерами по обеспечению информационной безопасности, принятыми в компании, SafeCopy предотвращает распространение печатных копий конфиденциальных документов, несанкционированную передачу их конкурентам, представителям прессы, контрагентам и заказчикам.



Каждое ответственное лицо в компании, имеющее доступ к печатным копиям конфиденциальных корпоративных документов, будет иметь возможность работать только со своей уникальной копией, распространение которой приведет к однозначному определению источника утечки документа. Понимание этого удержит сотрудников от необдуманного шага несанкционированного распространения своей печатной копии, и, как следствие, избавит организацию от неприятных ситуаций, громких заявлений, скандальных разоблачений, связанных с раскрытием информации, содержащейся в печатных копиях документов.

Решаемые задачи и особенности:

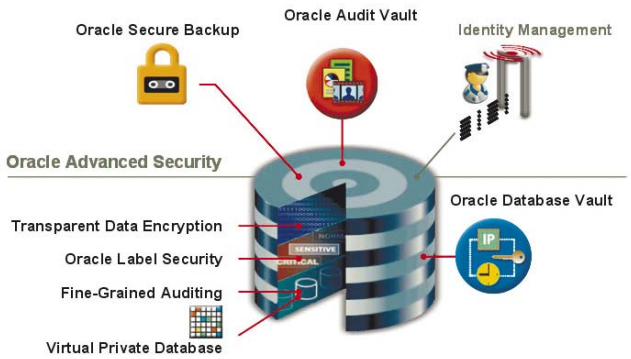
- выявление каналов утечки печатных копий корпоративных документов и однозначное определение нелояльных сотрудников, допустивших несанкционированное распространение документов вовне;
- предотвращение несанкционированного использования бумажных копий документов внутри самой организации;
- централизованное хранение, учет и управление документооборотом служебных корпоративных документов, неподлежащих распространению;
- реализация необходимых технических мер, в сочетании с которыми организационные мероприятия и политики информационной безопасности компании позволят провести эффективное расследование любых инцидентов, связанных с несанкционированным распространением печатных копий документов.

Защита баз данных

Oracle Database Security - комплекс решений обеспечения безопасности баз данных. Позволяет значительно снизить вероятность доступа к данным, хранимым в базах, в т.ч. со стороны сотрудников компании.

Комплекс предназначен для решения таких задач, как:

- защита данных от администраторов БД;
- шифрование определённых критических областей в БД;
- использование защищенных соединений “пользователь-сервер БД”;
- защита от перехвата траффика по сети;
- аудит действий пользователей в нескольких БД.



В **состав решений** по обеспечению безопасности баз данных Oracle входят следующие программные продукты:

- **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. Позволяет защитить информацию от администраторов баз данных.
- **Advanced Security Options** — решения, реализующие 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.
- **Audit Vault and Database Firewall** — решение для консолидации данных аудита и управления этой информацией, позволяющее компаниям упростить процедуры формирования отчетов о соблюдении нормативных требований, заблаговременно выявлять угрозы, сокращать затраты и надежно хранить данные аудита.
- **Label Security** — решение по реализации мандатного доступа (с использованием меток) к данным в базе данных.

Аудит информационной безопасности

- **Аудит информационной безопасности на соответствие требованиям по защите персональных данных**
  Услуга проведения аудита информационной безопасности позволит выявить, какие обязательные требования по защите персональных данных в организации не реализованы или реализованы не в полной мере, а также разработать план действий по приведению системы защиты персональных данных к требуемому состоянию.
  Компания «ФОРС» обладает необходимым пакетом лицензий ФСТЭК России и ФСБ России для оказания услуг по защите конфиденциальной информации и квалифицированными специалистами по информационной безопасности.
- **Аудит информационной безопасности на соответствие отраслевым требованиям**
  В ходе аудита эксперты компании ФОРС проведут анализ соответствия текущей системы обеспечения информационной безопасности (СОИБ) требованиям стандарта Банка России СТО БР ИББС-1.0, проанализируют выявленные несоответствия и предложат меры по их устранению.