Защита информации и бизнес-приложений в соответствии с требованиями Закона о персональных данных с помощью сертифицированных средств безопасности Oracle

г. Москва, 2014 г.

ORACLE

1. Общие положения

Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»[1] – федеральный закон, регулирующий деятельность по обработке (использованию) персональных данных. Федеральным законом от 23 декабря 2010 года № 359-ФЗ «О внесении изменения в статью 25 федерального закона "О персональных данных"» установлен **срок приведения информационных систем персональных данных**, созданных до 1 января 2011 года, **в соответствие с требованиями закона № 152-ФЗ – не позднее 1 июля 2011 года**.

В соответствии с законом, в России существенно возрастают требования *ко всем частным и государственным компаниям и организациям, а также физическим лицам, которые хранят, собирают, передают или обрабатывают персональные данные*. Согласно закону, а также ряду нормативных и руководящих документов регулирующих органов (ФСТЭК России, ФСБ России, Роскомнадзор), **операторы ПДн должны выполнить ряд требований по защите персональных данных физических лиц** (своих сотрудников, клиентов, посетителей и т. д.) обрабатываемых в информационных системах Компании, и предпринять ряд действий…

Возможные типы угроз для ИСПДн, требуемые уровни защищенности ПДн, порядок выбора средств защиты информации для системы защиты ПДн перечислены в Постановлении Правительства РФ от 1 ноября 2012 г. №1119 «Об утверждении требований к защите ПД при их обработке в ИСПДн»[2], а Приказы ФСТЭК РФ от 18 февраля 2013 г. №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн»[3] и от 11 февраля 2013 г. №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»[4] определяют требуемые меры защиты. В частности, в эти меры входят: **идентификация и аутентификация** субъектов доступа и объектов доступа, **управление доступом** субъектов доступа к объектам доступа, **регистрация событий безопасности** и др.; а «высокие» уровни защищенности ПДн требуют *использования в ИСПДн сертифицированных по требованиям безопасности информации средств защиты информации*.

Несмотря на то, что в настоящее время существует большое количество сертифицированных СЗИ[5] для использования на уровне рабочих станций, локальной сети и каналов связи, проблема защиты информации от НСД на уровне среды облачных вычислений, бизнес-приложений, СУБД и хранилищ электронных документов стоит достаточно остро. Каким же образом создать универсальную систему безопасности, которая технологически защитит ПДн где бы они ни находились от множества угроз НСД – как внутренних, так и внешних?

2. Предложение Oracle для защиты ПДн

Компания Oracle предлагает использовать собственные сертифицированные решения для защиты автоматизированных информационных систем (АИС) и информационных систем персональных данных (ИСПДн), которые будут работать как на уровне бизнес приложений (ERP, CRM, АБС и т.д.), так и на уровне СУБД, и в отношении хранилищ электронных документов (Oracle WebCenter Content, Microsoft Sharepoint Portal). В их числе:

---

[1] http://www.rg.ru/2006/07/29/personaljnye-dannye-dok.html

[2] http://www.rg.ru/2012/11/07/pers-dannye-dok.html

[3] http://www.rg.ru/2013/05/22/soderjanie-dok.html

[4] http://www.rg.ru/2013/06/26/gostajna-dok.html

[5] http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii

- ***набор ПО Oracle Identity and Access Management Suite [IAMS]***, включающий в себя Oracle Identity Manager, Oracle Access Manager и др. продукты (сертифицирован на соответствие требованиям руководящего документа «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. *Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) – по 4 уровня контроля*) – ***сертификат №2238 сроком действия до 23 декабря 2016 г.***;

- ***набор ПО Oracle Enterprise Single Sign-On Suite Plus [ESSO]*** (сертифицирован, как средство защиты от несанкционированного доступа к информации, реализующим функции идентификации и аутентификации, а также – регистрации событий безопасности) – ***сертификат №3103 сроком действия до 20 февраля 2017 г.***;

- ***ПО Oracle Database Enterprise Edition совместно с Oracle Database Vault*** (сертифицировано как СУБД со встроенными средствами защиты от несанкционированного доступа к информации) – ***сертификат №2858 сроком действия до 27 марта 2016 г.***

Вышеперечисленные средства защиты позволяют заказчикам успешно нейтрализовать угрозы НСД к ПДн и обходиться без сертификации отдельных систем и приложений. Обратите внимание, что набор ПО IAMS прошел проверку прикладного программного обеспечения на отсутствие недекларированных возможностей, что позволяет его использовать в ИСПДн для обеспечения самых «высоких» уровней защищенности.

Специализированное средство защиты СУБД Oracle DB Vault также может быть использовано для защиты ПДн 1-го и 2-го типов, если установить его на операционную систему ***Oracle Enterprise Linux***, которая в соответствии с ***сертификатом №3095 сроком действия до 13 февраля 2017 г.*** соответствует требованиям руководящих документов «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) - по 3 классу защищенности и «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. *Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по 2 уровню контроля*.

3. Угрозы НСД к ПДн и методы их нейтрализации

В зависимости от размещения и способа обработки ПДн в ИСПДн можно выявить следующие типичные угрозы и предложить способы их нейтрализации:

1) ПДн находятся в хранилищах бизнес-приложений – риск того, что кроме легитимных клиентов бизнес-приложений к ПДн могут получить несанкционированный доступ на файловом уровне привилегированные пользователи операционных систем (ОС) и СУБД – необходимо ограничение прав привилегированных пользователей и применение специальных средств защиты на файловом уровне;

2) Многопользовательский режим работы бизнес-приложения с ПДн – риск избыточности прав бизнес-пользователей по сравнению с минимальным набором полномочий, необходимым для выполнения ими должностных обязанностей – реализация и контроль целостности ролевой модели доступа к информации в бизнес-приложении, ведение истории изменения привилегий;

3) Использование для аутентификации в бизнес-приложениях с ПДн только парольной защиты – риск похищения идентификационных данных злоумышленниками – использование методов усиленной аутентификации, введение и контроль исполнения политик подключения к бизнес-приложениям;

4) ПДн находятся в хранилищах электронных документах – риск утечки информации при их несанкционированном копировании и/или при их передаче по электронным каналам связи – защита каналов связи, электронных носителей или гранулярный контроль доступа к документам (включая права на поиск внутри документа, его чтение и скачивание);

5) ПДн находятся в среде облачных вычислений – все вышеперечисленные риски безопасности, а также дополнительные, связанные с доступностью сервисов обработки ПДн – реализация вышеперечисленных базовых сервисов безопасности и внедрение автоматизированных решений для массового заведения идентификаторов бизнес-пользователей (включая саморегистрацию) и установление федеративных отношений для исключения возможности несанкционированного подключения этих бизнес-пользователей извне доверенной среды.

4. Архитектура решения

Общая архитектура предлагаемого решения для обеспечения информационной безопасности гетерогенной АИС приведена на Рис 1. В закрашенных областях, представляющих собой элементы существующей IT-инфраструктуры, происходит обработка ПДн (Кадровая система – частный случай бизнес-приложения). В результате установки и интеграции нескольких решений безопасности Oracle (выделенных красным текстом) организуется защита ПДн.

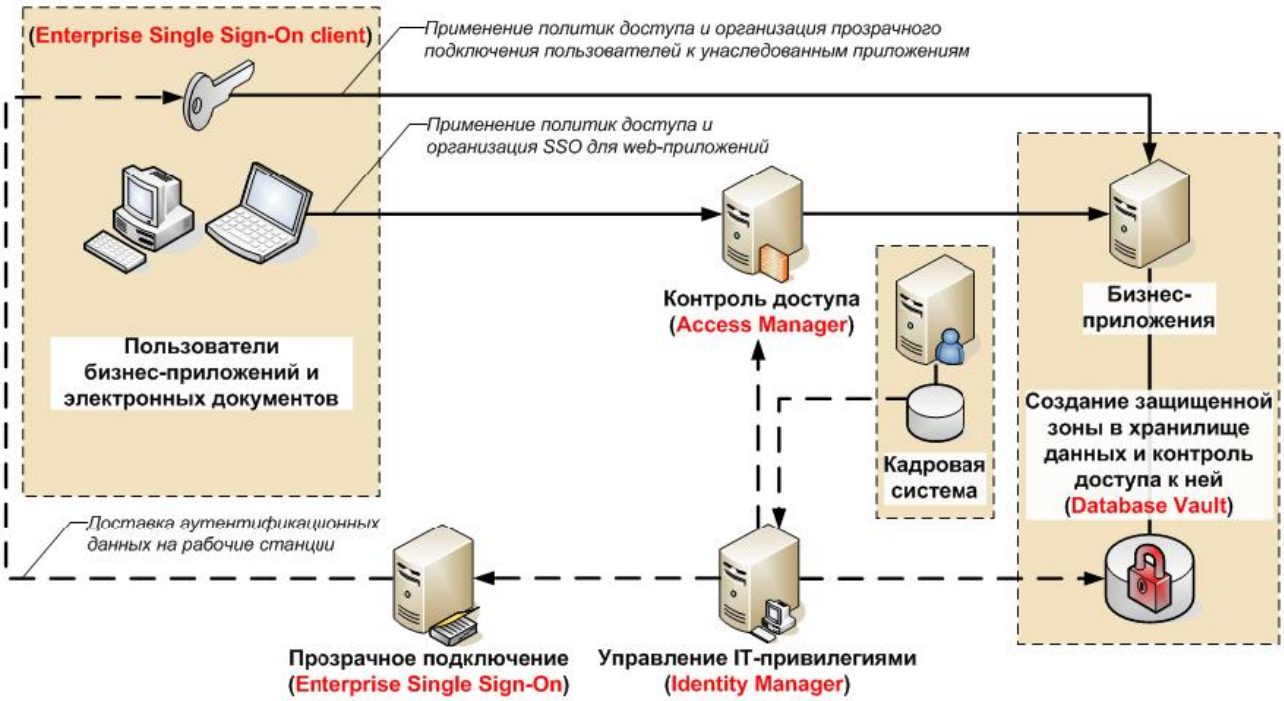

Рис. 1. Архитектура построения универсальной системы защиты от НСД

В рамках данной архитектуры каждый из продуктов Oracle специализирован для решения определенных задач и подготовлен для совместной работы:

a. Oracle Identity Manager:

- Управление жизненным циклом учетных данных сотрудников и внешних пользователей внутри организации и в облачных сервисах;
- 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;

b. Oracle Access Manager:

- Определение и контроль исполнения политик Аутентификации, Авторизации и Аудита для пользователей при их обращении к любым бизнес-приложениям, использующих трехзвенную архитектуру и протокол доступа HTTP (например, Oracle E-Business Suite, Siebel, Hyperion, промышленные порталы и собственные разработки на основе Web-серверов Oracle, IBM, Microsoft и др.);
- 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 (событиям безопасности);
- Совместно с Oracle Entitlements Server – гранулярный контроль доступа пользователей к хранилищам электронных документов;

c. Oracle Enterprise Single Sign-On:

- Идентификация и аутентификация пользователей;
- Прозрачное подключение к бизнес-приложениям из любых клиентских программ, богато-функциональных и терминальных клиентов (Enterprise SSO);
- Помощь при смене паролей в бизнес-приложениях с учетом политик сложности;
- Сброс пароля в LDAP-каталоге при правильном ответе на контрольные вопросы (самообслуживание пользователей);
- Интеграция с аппаратными аутентификаторами – смарт-картами и USB-токенами;
- Отчетность по подключениям пользователей к бизнес-приложениям (событиям безопасности);

d. Oracle Database Vault:

- Создание защищенной зоны внутри СУБД и разграничение прав доступа к ней, включая сокрытие информации внутри зоны от привилегированных пользователей СУБД;
- Определение политик доступа к объектам защищенной зоны и контроль исполнения списка команд с учетом различных факторов в реальном времени;
- Аудит и отчетность по все операциям и попыткам НСД к информации СУБД (событиям безопасности).

e. Интеграционные решения:

- Ключевым элементом интеграции является сервер управления IT-привилегиями, который обеспечивает:
  - Реализацию ролевой модели управления за счет автоматизированной трансляции кадровых изменений как в бизнес-приложения, так и в системы контроля Web-доступа;
  - Автоматизированную доставку аутентификационных данных пользователей через хранилище сервера обеспечения прозрачного подключения на рабочие станции;
- Общим элементом, не показанным на схеме, является сервер отчетности Oracle BI Publisher. Вместе с решениями Oracle в области информационной безопасности поставляются преднастроенные отчеты для Oracle BI Publisher, а также инструкции для их комбинирования и модификации;

- Сервер контроля доступа к Web-приложениям обеспечивает Аутентификацию, Авторизацию, Аудит и WebSSO для сервера управления IT-привилегиями (не показано на схеме).
- Сервер обеспечения федеративного взаимодействия Oracle Identity Federation (лицензионно входящий в Oracle Identity and Access Management Suite и не представленный на схеме) за счет интеграции с сервером контроля доступа к Web-приложениям обеспечивает WebSSO для бизнес-пользователей, прошедших аутентификацию в домашней доверенной среде, при их подключении к сервисам обработки ПДн, предоставляемым поставщиками «облачных» услуг.

Таким образом, решения Oracle в состоянии обеспечить эшелонированную защиту информации в бизнес-приложениях в соответствии с требованиями нормативных документов. Потребность в использовании какого-либо конкретного продукта или их комбинации определяется в результате составления модели угроз и разработки организационно-технических мероприятий по их нейтрализации.

5. Преимущества подхода Oracle

В качестве основных преимуществ подхода Oracle можно отметить следующие моменты:

- Решения Oracle представляют собой интегрированный стек продуктов, взаимодействующих между собой для обеспечения централизованного управления и контроля доступа пользователей к информации в бизнес-приложениях и электронных документах;
- Решения Oracle прозрачно встраиваются в имеющуюся IT-инфраструктуру (в том числе – в существующие системы управления информационной безопасностью) и требуют минимальных изменений имеющейся архитектуры;
- Решения Oracle являются лидерами на мировом рынке, имеют большое количество внедрений и пользователей во всех отраслях экономики и регионах;
- Решения Oracle по безопасности сертифицированы для использования совместно с бизнес-приложениями Oracle;
- Компания Oracle в России и СНГ имеет квалифицированную команду и профессиональных партнеров, готовых гарантировать успешность проекта по построению системы информационной безопасности на базе решений Oracle.

6. Источники дополнительной информации

Более подробную информацию о решениях Oracle в области информационной безопасности на русском языке можно найти по следующим ссылкам:

- Страница “Oracle Identity Management” на Oracle Technology Network http://www.oracle.com/technetwork/ru/middleware/id-management/index.html
- Блог “Информационная Безопасность – Решения Oracle” http://security-orcl.blogspot.ru/

По любым вопросам, связанным с решениями Oracle в области информационной безопасности, можно обращаться к директору по продуктам Сергею Базылько [sergey.bazylko@oracle.com] или руководителю группы консультантов Андрею Гусакову [andrey.gusakov@oracle.com]. Контактный телефон +7(495)-6411400.