

**ЛОГИНОВ А. Е., БАЗАРОВА И. А.**  
**ИНТЕГРАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ**  
**ANKEY С СУБД ORACLE**

*УДК 004.65, ВАК 05.13.18, ГРНТИ 50.41.21*

Интеграция системы управления  
учетными записями Ankey с СУБД  
Oracle

Integration of the Ankey account man-  
agement system with Oracle DBMS

**А. Е. Логинов, И. А. Базарова**

**A. E. Loginov, I. A. Bazarova**

Ухтинский государственный  
технический университет, г. Ухта

Ukhta State Technical University, Ukhta

*В статье рассматривается интеграция автоматизированной системы обработки информации и управления Ankey IDM с Oracle DBMS и AD DS. В ходе интеграции был разработан макет, выполняющий управление жизненным циклом учётных записей, реконсиляцию и синхронизацию данных сотрудников.*

*This article discusses the integration of Ankey IDM automated information processing and management system with Oracle DBMS and AD DS. During the integration, a layout was developed that performs the management of the life cycle of accounts, reconciliation and synchronization of employee data.*

**Ключевые слова:** *IDM, интеграция, макетирование.*

**Keywords:** *IDM, integration, prototyping.*

### **Введение**

Данная статья посвящена краткому обзору макетирования интеграции АСОИУ Ankey IDM с DBMS Oracle Database (ODB) и службой каталогов Active Directory (AD DS) для регионального подразделения ООО «Газинформсервис» филиала города Ухта. «Газинформсервис» является компанией-подрядчиком, занимающейся системным интегрированием в сфере корпоративной информационной безопасности, а также разработкой инженерно-технических средств для решения задач по защите информации.

Одним из этапов, выполняемых в процессе работ по внедрению, является макетирование. Макетирование позволяет разработать технические решения для реализации ожидаемого Организацией-заказчиком функционала, в безопасной форме отработать технологию внедрения, а также проверить корректность работы технических решений.

Работы по макетированию производятся в рамках подсистемы управления учётными записями и подсистемы управления ролями (ПУУЗ/ПУР), которая является частью комплексной системы защиты информации (КСЗИ) Организации-заказчика. Основной задачей работы является воспроизведение функционала ПУУЗ/ПУР, урезанного в соответствии с границами макетирования.

## Предпроектное обследование

В рамках проекта КСЗИ, в пределах ПУУЗ/ПУР, ограничиваясь перечнем используемого ПО, а именно целевой системой (ЦС) AD, доверенной системой (ДС) ODB и программным комплексом Ankey IDM, необходимо произвести макетирование в виртуальной среде стендовой базы, то есть в безопасной для Организации-заказчика форме.

Решение о макетировании обусловлено сложностью текущей работающей подсистемы и непредсказуемостью результатов для Организации-заказчика при выполнении работ по миграции с существующего решения IDM на базе продуктов Oracle непосредственно на площадке внедрения.

В качестве объекта автоматизации в границах макетирования выступает деятельность Организации-заказчика по управлению УЗ, а именно управлению их жизненным циклом, распространению в ЦС AD и последующую синхронизацию атрибутов УЗ с ДС ODB.

В границах макетирования требуется обеспечить следующий функционал:

- Формирование центрального хранилища существующих идентификационных данных пользователей для последующей аналитической обработки: управление жизненным циклом УЗ, включая выполнение над ними операций CRUD; пакетная загрузка пользовательских данных из таблиц DB.

- Централизованное управление УЗ пользователей с выполнением следующих функций: распространение аккаунтов пользователей в ЦС AD; синхронизация параметров УЗ с ЦС AD;

Целью макетирования является создание технических решений для обеспечения требуемого функционала, отработка технологии внедрения (последовательность действий по настройке программного комплекса Ankey IDM в соответствии с техническими решениями) и базовой настройки безопасности, установка и настройка ОС и ПО, не включаемого в программный комплекс Ankey IDM, но используемого для обеспечения его работы.

Для выполнения работ по макетированию была получена рекомендация придерживаться следующего плана действий:

- получение доступа к документации по проекту КСЗИ и документации по Ankey IDM, их изучение в рамках предпроектного анализа;

- подготовка данных для макетирования, формирования раздела документации «Предпроектный анализ»;

- формулировка и фиксирование требований к макету, формирование раздела документации «Техническое задание»;

- разработка технических решений, формирование раздела документации «Технический проект»;

- получение доступа к стендовой базе и локальной вычислительной сети Заказчика, загрузка ПО, разворачивание и настройка окружения на стендовой базе;

- конфигурация Ankey IDM, передача рабочего макета и комплекта документации Заказчику.

## Проектирование информационной системы

На основе предпроектного обследования был составлен план макетирования, в котором были описаны основные технические решения, а именно:

- Настройка Fedora Server: конфигурация сетевых параметров (редактирование hosts и hostname, установка статических IP-адресов); настройка параметров ядра; инсталляция дополнительных пакетов; добавление групп и пользователей (формирование УЗ Исполнителя, формирование технической УЗ для ODB); настройка параметров безопасности (настройка SSH-сессии по паре ключей, конфигурация службы SSH, конфигурация Fail2ban).

- Работа с ODB: установка DBMS и создание DB (обеспечение корректной работы OUI, распаковка установочных пакетов, конфигурация «db\_install.rsp», выполнение установки DBMS, конфигурация «dbca.rsp», создание DB, действия после установки, конфигурация процесса Listener); запуск ODB; загрузка данных из XLS-файлов в DB; настройка доступа к таблицам для Ankey IDM.

- Настройка Windows Server: конфигурация сетевых параметров; добавление ролей и компонентов; настройка доступа к AD для Ankey IDM.

- Установка и настройка Alt Linux: конфигурация сетевых параметров; добавление групп и пользователей; настройка параметров ядра.

- Работа с программным комплексом Ankey IDM: установка JRE; установка Elasticsearch; установка и налаживание работы PostgreSQL; установка Ankey IDM; импорт сертификата из CA в Ankey IDM.

- Конфигурация функционирования Ankey IDM: конфигурация объектов для обеспечения взаимодействия с ODB (коннектор «OracleDBConn», кастомизация «com.gis.openicf.database.DatabaseConnector», тип ресурса «OracleDBRestype», расширение объектов «managed/user» и «managed/organization», расширение «custom\_organization.xml» и «custom\_usr.xml»); конфигурация объектов для обеспечения выполнения операции «Trusted Source Reconciliation» (ресурсы: «OracleDBResourceNach», «OracleDBResourceOrg», «OracleDBResourceRuc»; - аккаунты ресурсов: «OracleDBTrustNach», «OracleDBTrustOrg», «OracleDBTrustRuc» - маппинги: «ReconOrg», «ReconRuc», «ReconNach» - периодические задания: «TrustedReconNach», «TrustedReconRuc», «TrustedReconOrg»); конфигурирование объектов для обеспечения взаимодействия с AD (коннектор «ADConn», тип ресурса «ADResType»); конфигурация объектов для обеспечения выполнения операций «Provisioning» и «Target Resource Reconciliation» (ресурс «ADRes», аккаунт ресурса «ADResAccount», форма ресурса «ADResForm»); создание конфигураций «TargetReconGroupTask», «TargetReconOrgUnitTask» для обеспечения выполнения операции «Target Resource Reconciliation»; конфигурирование объектов для выполнения операции «Provisioning» (маппинг «ADPrepopulate»; маппинг «ADProvisionToResForm»; маппинг «ADProvisionUser»; создание роли «Active Directory Domain User» и информационной системы «Active Directory»).

## Результаты разработки системы

В рамках работы было произведено макетирование интеграции АСОИУ Ankey IDM с DBMS ODB и AD DS для регионального подразделения ООО

«Газинформсервис» филиала города Ухта. В процессе макетирования были выполнены следующие работы:

- Создание VM на базе Fedora Server 30-1.2, её конфигурация в соответствии с требованиями к ИБ и подготовка для разворачивания DBMS ODB.
- Разворачивание DBMS ODB 12.1.0.2.0 EE и создание DB на VM Fedora Server 30-1.2.
- Импортрование таблиц «RUC», «ORG» и «NACH» в ODB.
- Обеспечение доступа Ankey IDM к таблицам «RUC», «NACH» и «ORG» в ODB.
- Создание и настройка VM на базе Windows Server 2012R2.
- Установка AD DS 69 на Windows Server 2012R2 и компонента сервера CA.
- Создание необходимых ролей, прав и аккаунтов для обеспечения возможности целевой синхронизации УЗ из Ankey IDM в AD DS.
- Создание VM на базе Alt Linux 9.0.
- Разворачивание службы поиска Elasticsearch 7.6.2, DBMS PostgreSQL 12.2 и Ankey IDM SNAPSHOT-uhta на Alt Linux 9.0.
- Конфигурация необходимых объектов Ankey IDM для выполнения операции «Trusted Source Reconciliation» с ODB и для выполнения операций «Target Resource Reconciliation» и «Provisioning» с AD.
- Написание разделов документации ТП, ТЗ, ПА.
- Тестирование макета в соответствии с программой и методикой испытаний.

### **Заключение**

На основе анализа предметной области были сформированы основные цели и требования к макетированию. Макетирование части ПУУЗ/ПУР КСЗИ (а именно интеграции AD DS, ODB с Ankey IDM) выполнено в полном объёме в соответствии с поставленными задачами. Макет автоматизирует следующую активность ответственного персонала Организации-Заказчика:

- При найме сотрудника, ответственный персонал получает приказ о зачислении сотрудника в штат и его персональные данные. Ответственный персонал вручную создаёт под сотрудника УЗ в AD с правами, необходимыми для выполнения сотрудником должностных обязанностей.
- При увольнении сотрудника, ответственный персонал получает приказ об увольнении сотрудника и информацию для его идентификации. Ответственный персонал вручную удаляет УЗ из AD.
- При изменении данных о сотруднике, ответственный персонал получает приказ, в рамках которого производится обновление информации в существующих УЗ (например, приказ о повышении сотрудника в должности), информацию для идентификации сотрудника и атрибуты, которые требуется обновить. Ответственный персонал вручную выполняет обновление данных УЗ.

## Список использованных источников и литературы

1. Документация по Oracle Database [Электронный ресурс]. – Режим доступа: <https://docs.oracle.com/en/database/> (дата обращения: 18.03.2020).
2. Документация по Windows Server [Электронный ресурс]. – Режим доступа: <https://docs.microsoft.com/ru-ru/windows-server/> (дата обращения: 19.05.2020).
3. Информационная безопасность [Электронный ресурс]. – Режим доступа: <https://1cloud.ru/help> (дата обращения: 13.01.2020).
4. Настройка и администрирование Active Directory Domain Services [Электронный ресурс]. – Режим доступа: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services> (дата обращения: 17.03.2020).
5. Официальный Web-сайт компании ООО «Газинформсервис» [Электронный ресурс]. – Режим доступа: <https://www.gaz-is.ru/> (дата обращения: 05.01.2020).
6. Русскоязычный Web-сайт в формате системы тематических коллективных блогов; Внедрение IDM, общие положения. Identity Management — основы управления учётными записями [Электронный ресурс]. – Режим доступа: <https://habr.com/ru/company/solarsecurity> (дата обращения: 16.01.2020).
7. Руководство пользователя. Использование Fedora 13 для типичных задач настольного компьютера (Редакция 1.0) [Электронный ресурс]. – Режим доступа: <https://docs.fedoraproject.org/> (дата обращения: 29.02.2020).
8. Русскоязычная документация по Alt Linux [Электронный ресурс]. – Режим доступа: <https://www.altlinux.org/> (дата обращения: 15.04.2020).

## List of references

1. Oracle Database Documentation, <https://docs.oracle.com/en/database/>, accessed 03/18/2020.
2. Windows Server Documentation, <https://docs.microsoft.com/ru-ru/windows-server/>, accessed 05/19/2020.
3. Information Security, <https://1cloud.ru/help>, accessed 01/13/2020.
4. Configure and administer Active Directory Domain Services, <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services>, accessed 03/17/2020.
5. Official website of the company Gazinformservice, <https://www.gaz-is.ru/>, accessed 01/05/2020.
6. Russian-language Web site in the format of a system of thematic collective blogs; Implementation of IDM, general provisions. Identity Management – The Basics of Account Management, <https://habr.com/ru/company/solarsecurity>, accessed 01/16/2020.
7. User manual. Using Fedora 13 for typical desktop tasks (Revision 1.0), <https://docs.fedoraproject.org/>, accessed 02/29/2020.
8. Russian-language documentation on Alt Linux, <https://www.altlinux.org>, accessed 04/15/2020.