# Концепция изменений в настройке доступа Global ERP

## Текущая реализация

В Global ERP для пользователей назначаются профили доступа. Профиль доступа включает в себя одну или несколько ролей. Для каждой роли настраиваются полномочия доступа к бизнес-объектам системы, включая возможно управления доступом на чтение/изменение каждого атрибута, доступности каждой интерфейсной операции или интерфейсного элемента.

При необходимо разграничения доступа в зависимости от значений атрибутного состава объектов используется дискретный доступ. Настройка дискретного доступа позволяет дифференцировать полномочия (включая доступ на чтение объектов системы) в зависимости от правил дискретного доступа. Например, разграничить доступ к складским документам в зависимости от склада (по одному складу иметь доступ на чтение документов, по другим складам нет). Дискретный доступ настраивается для бизнес-объектов системы (конкретных справочников, документов) путем настройки правил дискретного доступа. При назначении полномочий для таких бизнес-объектов в роли доступа должно быть указано значение параметра дискретного доступа (например, код или идентификатор склада). При настройке правила дискретного доступа имеется возможность указать, что значение параметра должно вычисляться динамически (на основе указанного программного кода). Это используется для того, чтобы не указывать для роли значение параметра дискретного доступа, а вычислять его динамически при обращении пользователя к объектам системы (например, определять склад для роли на основе настройки справочника материально-ответственных лиц или каких то других настроек пользователя).

## Проблематика

Для ролей доступа, как правило, настраивается очень большое количество полномочий. В случае если требуется дифференцировать доступ в разрезе требуемых организационных уровней (складов, бизнес-единиц, организаций и пр.), то это влечет за собой создание большого количества ролей, в каждой из которых указывается свое значение параметра дискретного доступа (например, конкретный склад). Как следствие, в случае необходимости внесения изменений в настройки доступа, это требуется сделать для очень большого количества ролей. Это приводит к большим трудозатратам и рискам отсутствия консистенции прав доступа.

Текущее имеющееся решение в Global ERP заключается в настройке динамического определения значения параметров дискретного доступа для роли, что позволяет не размножать роли по каждому организационному уровню. Но это решение не является подходящим и достаточным в связи со следующими основными ограничениями:

1. Роль (и профиль доступа, назначенный для пользователя) не содержат информацию об организационном уровне, определенном для роли. Как следствие, на уровне IDM-системы будет осуществляться назначение роли, в которой определение значение параметров дискретного доступа будет делаться динамически. В связи с этим на уровне назначения ролей нет гарантированного определения точных условий доступа, они определяются для пользователя отдельно.
2. Отсутствует единая точка управления тем, какие значения параметров дискретного доступа (организационные уровни), должны использоваться для ролей и пользователей (вследствие того, что программное определение значений дискретного доступа может быть реализовано произвольным образом). Анализ того, какие в итоге права имеются у роли или пользователя становится затруднен или даже не возможен.

## Опыт решения проблемы в SAP

В SAP для обеспечения решения проблемы с необходимостью поддержки консистентности и упрощения внесения изменений в роли, созданные в разрезе организационных уровней, реализован следующий подход:

1. В случае, если для роли по каким-то полномочиям требуется дифференцировать доступ в разрезе организационных уровней, то такая роль получает тип «Мастер-роль». Для такой роли доступно изменение настроек полномочий, но при этом она не может назначаться пользователям.
2. На основе мастер-ролей осуществляется процесс деривации в разрезе требуемых организационных уровней. Под каждое требуемое значение орг.уровня создается деривированная (подчиненная) роль. Для подчиненных ролей запрещено изменение настроек полномочий. Пользователям назначаются только подчиненные роли.
3. В случае необходимости изменений в настроенные полномочия это делается для мастер-роли, после чего вызывается синхронизация во все деривированные роли.

## Предлагаемое решение для Global ERP

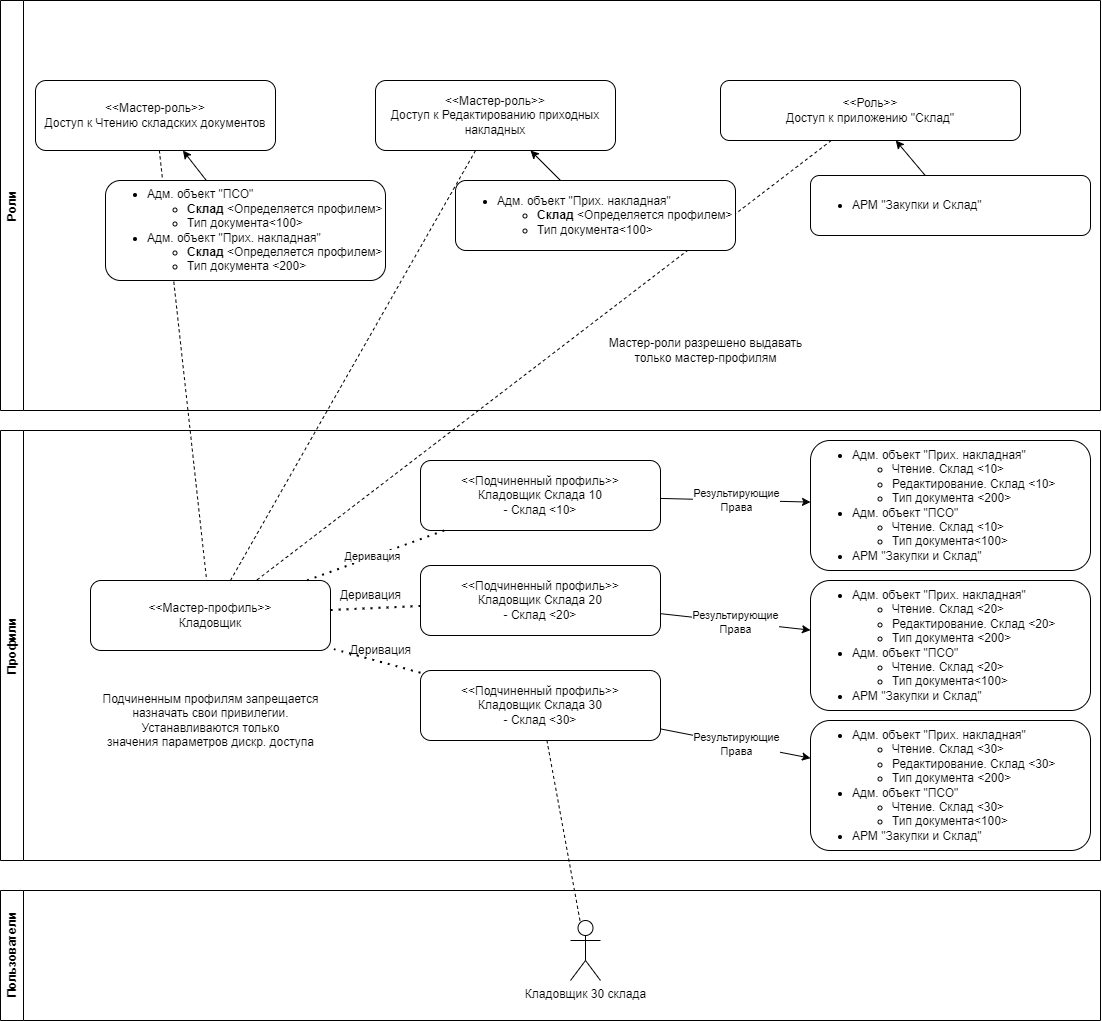
В Global ERP предлагается пойти по пути, являющемуся логическим развитием решения SAP, но с учетом особенностей текущей архитектуры и реализации модели управления доступом Global ERP.

Основные тезисы (изменения):

1. Роли разделяются на обычные и мастер-роли. Для мастер-ролей при назначении полномочий для бизнес-объектов появляется возможность указать, что значение параметров дискретного доступа определяется профилем доступа. Для обычных ролей такое сделать нельзя.
2. Профили доступа разделаются на мастер-профили, подчиненные и обычные. Мастер-роли можно включать только в мастер-профили доступа.
3. Для пользователей запрещено назначать мастер-профили доступа.
4. Для подчиненного профиля доступа всегда указан мастер-профиль. Для подчиненного профиля указываются конкретные значения параметров дискретного доступа.
5. Реализуется механизм деривации мастер-профиля на конечные профили с указанными для них значениями параметров дискретного доступа.

Данный подход к реализации дает все преимущества реализации SAP, но в тоже время избавляет от необходимости синхронизации настроек в подчиненные роли при изменении настроек полномочий в мастер-роли. Также данный подход снимает ограничения текущей реализации модели дискретного доступа Global ERP.

На следующем рисунке представлен пример настройки:



## Технические особенности реализации предложенного подхода в Global ERP

1. Для ролей доступа вводится типизация. Появляется тип «Роль» (обычная роль доступа) и «Мастер-роль».
2. При настройке параметров дискретного доступа для бизнес-объектов системы будет осуществляться настройка типа параметра:

* Обычный
* Динамический
* Определяется профилем

1. При назначении для роли полномочий с указанием параметра дискретного доступа с типом «Определяется профилем» сохранить роль можно будет только в случае установки для роли типа «Мастер-роль».
2. Для профилей доступа вводится типизация. Появляются типы «Мастер-профиль», «Подчиненный профиль» и «Обычный профиль». Реализуется обязательное указание мастер-профиля для профиля с типом «Подчиненный профиль».
3. Для профиля с типом «Подчиненный профиль» запрещается указание ролей доступа. Все права для него транслируются от мастер-профиля.
4. Для профиля с типом «Подчиненный профиль» обеспечивается обязательное указание значений параметров дискретного доступа с типом «Определяется профилем» из числа имеющихся в мастер-ролях, выданных для мастер-профиля. При этом если системное имя параметра дискретного доступа у разных бизнес-объектов одинаковое, то указание значения таких параметров на уровне подчиненного профиля осуществляется только один раз.
5. Реализуется интерфейс удобной и быстрой деривации мастер-профиля на конечные профили с указанием для них значений параметров дискретного доступа с типом «Определяется профилем».
6. Для пользователей можно назначать только профили доступа с типами «Подчиненный профиль» и «Обычный профиль».
7. При определении прав доступа пользователей для назначенных для них подчиненных профилей обеспечивается получение полномочий, указанных в соответствующих мастер-профилях с учетом значений параметров дискретного доступа, указанных в подчиненных профилях.