

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**  
**на поставку лицензий «IDM Управление учётными данными»**

1. Заказчик: АО «НЭСК» (гор. Краснодар, ул. Красных Партизан, д. 192).
2. Исполнитель договора на поставку бессрочных лицензий «IDM Управление учётными данными» определяется по итогам проведения конкурсных процедур.
3. Период действия договора – до момента исполнения обязательств по договору.
4. **Назначение системы и цели эксплуатации.**

**4.1. Назначение Системы**

Система предназначена для автоматизации процессов управления учетными записями и правами доступа пользователей в управляемых системах на основе информации из кадрового источника и запросов пользователей.

**4.2. Цели эксплуатации системы**

Целями эксплуатации системы являются:

- повышение уровня информационной безопасности за счет предоставления возможности контроля и централизованного управления доступом пользователей;
- снижение издержек на обслуживание процессов управления учетными записями и правами доступа за счет автоматизации;
- сокращение временных затрат на предоставление, изменение и отзыв прав доступа пользователей.

**5. Список терминов и сокращений**

Термины и сокращения	Определение, расшифровка
Заказчик	АО «НЭСК»
Поставщик	Определяется на основании закупочных процедур АО «НЭСК»
ИС	Информационная система
Внутренний пользователь	Пользователь, который является штатным работником
Внешний пользователь	Пользователь, который не является штатным работником (подрядчики, поставщики, аудиторы, консультанты и т.д.)
Система	Система управления учетными записями и правами доступа на базе конфигурации «IDM.Управление учетными данными»
Кадровый источник (КИ)	База данных с информацией о сотрудниках и кадровых событиях на основе 1С:Зарплата и управление персоналом
Приложение	ИС, управление доступом к которой автоматизируется в рамках проекта
Целевая система (ЦС)	КИ или Приложение
ПО	Программное обеспечение
ОС	Операционная система
СУБД	Система управления базами данных
AD	Microsoft Active Directory
OU	Organization Unite – контейнер в Active Directory
УЗ	Учетная запись
ОПШС	Организационно-штатная структура
Операция	Бизнес-процесс, который изменяет права пользователей в приложении

Термины и сокращения	Определение, расшифровка
Бенефициар	Пользователь, в интересах которого в Системе создан запрос (запрос новых прав, запрос на отзыв прав, на блокировку/разблокировку УЗ)
Автономное приложение	Приложение, исполнение операций, в котором осуществляется ручную администратором приложения

## 6. Характеристики объекта автоматизации

6.1. Объектом автоматизации является процесс управления учетными записями и правами пользователей информационных систем АО «НЭСК»

6.2. Количество пользователей ИС (сотрудник имеющий 1 или более активных УЗ) — 250 сотрудников компании.

6.3. Перечень коннекторов, включённых в комплект поставки:

1) Коннекторы к кадровым источникам:

- 1С:ЗУП 1.3
- 1С:ЗУП 2.5
- 1С:ЗУП 3.0
- 1С:УПП 1.3
- 1С:ERP 2.5
- 1С:КА 1
- 1С:КА 2

2) Коннекторы к Управляемым системам

- Active Directory
- Битрикс
- MS Exchange server
- Яндекс 360
- Почта VK Workspace
- Open LDAP
- 1С (конфигурации на платформе 1С:Предприятие 8)
- Универсальный HTTP
- Автономное приложение
- АТС 3CX

## 7. Технические требования к Системе, построенные на штатном функционале программного продукта «IDM.Управление учётными данными»

7.1. Выполнение работ не включает в себя дополнительную разработку или доработку программного продукта для реализации перечисленных в данном разделе функций.

7.2. Функционал по загрузке первоначальных данных

7.3. Функционал нормализации, в том числе автоматической:

- сопоставление подразделений;
- сопоставление должностей;
- сопоставление учетных записей сотрудников.

7.4. Функционал по управлению пользовательскими учётными записями:

7.4.1. Операции по УЗ:

- заявка на добавление УЗ (основной/дополнительной/системной);
- заявка на блокировку УЗ;

- заявка на разблокировку УЗ;
- заявка на смену имени УЗ;
- заявка на удаление УЗ;

7.4.2. Возможность ограничения срока (постоянно/временно):

- предоставления УЗ;
- блокировки УЗ;
- разблокировки УЗ.

7.4.3. Автоматизированное управление УЗ по настраиваемым кадровым событиям (приём, увольнение, перевод, отпуск):

- создание новой УЗ;
- блокировка УЗ;
- разблокировка УЗ;
- удаление УЗ.

7.4.4. Автоматическое изменение имени УЗ после смены ФИО сотрудника (в соответствии с алгоритмами генерации имени УЗ).

7.5. Управление правами УЗ:

7.5.1. Создание заявок на управление правами:

- заявка на предоставление прав (из каталога прав/по сотруднику);
- заявка на отзыв прав;
- заявка на делегирование прав (весь перечень прав сотрудника/выборочные права сотрудника);

7.5.2. Возможность ограничения срока (постоянно/временно):

- предоставления права;
- отзыва права;
- делегирования права.

7.5.3. Управление правилами изменения прав по настраиваемым кадровым событиям (приём, увольнение, перевод, отпуск).

7.5.4. Настраиваемые правила согласования операций с учетными данными управляемых приложений.

7.6. Управление системными УЗ:

7.6.1. Связывание системных УЗ с карточками сотрудников.

7.6.2. Создание системной УЗ через заявку, возможность пользователю задать необходимое имя системной УЗ при заполнении заявки.

7.7. Управление заявками:

7.7.1. Создание заявок:

- для одного или списка сотрудников/УЗ;
- для одного или нескольких прав;
- добавление файла (вложения) к заявке.

7.7.2. При создании заявки, автоматическое выявление в ней:

- выданных прав;
- прав, которые уже запрошены и/или находятся на согласовании.

7.7.3. Автосо согласование заявки на одном шаге, если согласующим и автором запроса является одно лицо.

7.7.4. Возможность назначить согласование на выдачу привилегированных прав.

7.7.5. Возможность согласующему переназначить другому сотруднику согласование заявки.

7.7.6. Ведение журнала согласования каждой заявки.

7.8. Ведение ОПС:

7.8.1. Использование КИ, как доверенного источника информации о сотрудниках.

7.8.2. Автоматическая актуализация ОШС по расписанию регламентного задания на основе информации из КИ с автосооставлением.

7.8.3. Ведение информации о внутренних и внешних сотрудниках.

7.8.4. Возможность исключать подразделения и должности из процесса управления правами.

7.9. Ведение карточек сотрудников:

7.9.1. Ведение в Системе карточки сотрудника – объекта, объединяющего в себе информацию о сотруднике из КИ и информацию обо всех УЗ их правах.

7.9.2. Поддержка нескольких назначений сотрудника, отражение кадровой истории.

7.9.3. Поддержка использования сотрудником нескольких УЗ в одном приложении (Основной/дополнительной).

7.9.4. Объединение физических лиц из разных КИ в одну карточку сотрудника.

7.10. Ведение каталога прав доступа:

7.10.1. Предоставление каталога прав доступа в иерархической структуре.

7.10.2. Группировки прав путём создания бизнес-роли.

7.10.3. Автоматическая (по расписанию) актуализация каталога прав доступа.

7.10.4. Возможность назначения владельца для любого права и приложения.

7.10.5. Возможность настройки ролевой модели.

7.10.6. Возможность установить признак привилегированности прав.

7.11. Информирование пользователей по электронной почте и СМС о значимых событиях работы Системы по настроенным правилам рассылки, например:

- Автору заявки о выполнении заявки;
- Согласующему о необходимости согласовать право в заявке;
- Автору заявки об отрицательном согласовании права в заявке;
- Бенефициару о создании УЗ, предоставлении и отзыве прав, блокировке и разблокировке УЗ;
- Ответственному о невыполненных в срок задачах;
- Администратору о задачах на контроле;
- Администратору о способе устранения коллизий.

7.12. Предоставление отчётов о правах доступа пользователей в УС:

7.12.1. Предоставление следующих отчётов в интерфейсе Системы:

- Права сотрудников;
- Анализ прав сотрудников по объектам метаданных;
- История изменения прав;
- Матрица доступа;
- Матрица SoD-рисков;
- Матрица SoD-конфликтов;
- Ролевая модель;
- Анализ прав сотрудников по ролевой модели;
- Сотрудники с привилегированными правами.

7.12.2. Персональная настройка внешнего вида отчета (отборы информации, группировка, оформление), сохранение и вызов настроенного внешнего вида отчета.

7.12.3. Интерактивность отчета (переход из записи в отчете в объект).

7.12.4. Рассылка отчетов по электронной почте с возможностью настройки расписания.

7.12.5. Возможность экспорта отчетов во внешние файлы (Документ PDF (\*.pdf), Лист Excel (\*.xls, \*.xlsx), Документ Word (\*.docx), Табличный документ (\*.mxl), Электронная таблица ODF (\*.ods), Документ HTML (\*.htm), Текстовый файл (\*.txt)).

7.13. Конфигурирование приложений:

7.13.1. Генерация имени УЗ при её создании по алгоритму на основе ФИО сотрудника:

- задаваемые правила формирования имён учётных записей для каждого приложения;

- поддержка создания разноимённых УЗ для однофамильцев;
- на основе данных о сотруднике: ФИО, должность, подразделение, телефон;
- настройка правил транслитерации.

#### 7.13.2. Применение парольных политик для первоначального пароля:

- поддержка минимальной/максимальной длины пароля, содержания букв/ цифр, верхнего/ нижнего регистров, недопустимых символов;
- поддержка разных политик для разных приложений (и одной для нескольких приложений);

#### 7.13.3. Для Active Directory использование шаблонов для автоматического размещения УЗ в OU AD:

- на основе подразделения сотрудника и иерархии подразделения в ОШС;
- на основе статуса УЗ (заблокирована/ разблокирована);
- на основе статуса сотрудника (уволен/ работает);
- на основе типа сотрудник (внутренний/ внешний).

#### 7.14. Поддерживаемые операции в приложениях:

##### 7.14.1. Система поддерживает следующие режимы исполнения операций в приложении:

- «Автоматический» - режим позволяет Системе автоматически выполнять заданный тип операций в приложении.
- «Автоматический с контролем» - режим позволяет Системе автоматически выполнять заданный тип операций в приложении, с последующим оповещением администратора приложения.
- «Выполняется администратором» - режим позволяет выполнять заданный тип операций администратором приложения вручную.

##### 7.14.2. Возможность задать режим исполнения для каждого типа операций в приложении, возможность переключения режимов.

##### 7.14.3. Возможность задать администратора (выполняющего «Контроль» или «Выполнение») для каждого приложения.

#### 7.15. Выявление и устранение несоответствий:

##### 7.15.1. Возможность проведения аудита учетных данных, вручную или по заданному расписанию для выявления расхождений между Системой и приложением по статусам данных:

- «Новый в IDM» - УЗ или право присутствует только в приложении;
- «Зарегистрирован в IDM и приложении» - данные есть как в IDM, так и в приложении, отличаются только состояния УЗ (включена, отключена) или права (предоставлено, отозвано);
- «Удалён в приложении» - УЗ удалена в приложении, но в IDM отмечено, что присутствует.

##### 7.15.2. Возможность настроить правила устранения коллизий для учетных данных, в каждом приложении:

###### 7.15.2.1. В разрезе реакций:

- реакция на создание УЗ в приложении
- реакция на изменение статуса УЗ в приложении (заблокировано/активно)
- реакция на удаление УЗ в приложении
- реакция на предоставление права УЗ в приложении
- реакция на отзыв права УЗ в приложении

###### 7.15.2.2. В разрезе способов устранения:

- приведение в соответствие с приложением или с IDM

###### 7.15.2.3. В разрезе режима исполнения:

- автоматическое приведение в соответствие,
- ручное,
- автоматическое с контролем.

- 7.16. Механизм построения ролевой модели на основании текущих прав сотрудников.
- 7.17. Возможность настройки SoD-рисков – рисков, возникающих при присвоении одному работнику полномочий в одной или нескольких системах, позволяющих этому работнику совершать критические действия.
- 7.18. Возможность выполнения задач по почте.
- 7.19. Возможность интеграции Системы с конфигурациями 1С через сервисы интеграции в асинхронном режиме, включая 1С:Шина.

## **8. Требования к ролям и полномочиям пользователей Системы**

- 8.1. Возможность настройки групп доступов пользователей.
- 8.2. Возможность разграничения доступа по произвольным профилям в разрезе прав.

## **9. Требования к реакциям Системы на смену рабочего статуса сотрудника**

- 9.1. Система автоматически создаёт заявки:
- Заявка на создание УЗ по кадровому событию приём на работу;
  - Заявка на предоставление прав по кадровым событиям приём на работу и кадровый перевод;
  - Заявка на пересмотр прав по правилам приёма на работу по кадровому событию кадровый перевод;
  - Заявка на блокировку УЗ по кадровым событиям увольнение и отпуск;
  - Заявка на удаление УЗ по кадровому событию приём увольнение;
  - Заявка на отзыв прав по кадровому событию отпуск;
  - Запрос на смену наименований УЗ при смене сотрудником ФИО;
- 9.2. Система автоматически создаёт заявки в случае отработки кадрового события, влияющего на состояние сотрудника:

<b>Кадровое событие</b>	<b>Предыдущее состояние сотрудника</b>	<b>Новое состояние сотрудника</b>	<b>Реакция (тип заявки)</b>
Приём на работу		Работает	Заявка на создание УЗ, заявка на предоставление прав – по заданным настройкам кадрового события
Отпуск (больничный, командировка декрет)	Работает	Работает	Заявка на отзыв прав, заявка на блокировку УЗ, – по заданным настройкам кадрового события
Увольнение	Работает	Уволен	Заявка на блокировку УЗ, заявка на удаление УЗ– по заданным настройкам кадрового события
Кадровый перевод	Работает	Работает	Заявка на отзыв прав, заявка на блокировку УЗ, заявка на предоставление прав – по заданным настройкам кадрового события

## **10. Требования к системе**

- 10.1. Интерфейс Системы должен соответствовать следующим требованиям:
- 10.1.1. Быть графическим.
- 10.1.2. Поддерживать использование «горячих» клавиш.

10.1.3. Содержать средства помощи пользователю: справку, подсказки, автозаполнение данных, отметки незаполненных полей.

10.1.4. Поддерживать сигнализацию об ошибках или ошибочных действиях путем индикации на экране подсказкой о дальнейших действиях.

10.1.5. Использовать унифицированные интерфейсные решения во всех блоках автоматизированных функций.

10.1.6. Основные разделы программы:

- «Главное» – собраны команды по администрированию системы и по работе с напоминаниями;
- «Система» – собраны все основные настройки и отчёты по работе IDM системы в целом;
- «Предприятие» – собрана информация по сотрудникам и организационно-штатной структуре компании;
- «Ролевая модель» – раздел предназначен для работы с настройками и анализом ролевой модели предприятия;
- «Учетные данные» – отражены основные функции и отчеты по учетным записям и правам;
- «Администрирование» – в разделе производится настройка работы программы, регламентных заданий, обслуживание и т.д.

## **11. Требования к Участнику-Исполнителю**

11.1. Участник - Исполнитель должен иметь следующие лицензии и сертификаты (подтверждается предоставлением надлежаще заверенной копии лицензии):

- Система IDM должна быть разработана на базе платформы «1С: Предприятие 8.3»
- Система IDM должна иметь действующий сертификат «1С: Совместимо»
- Система IDM должна быть включена в реестр Российского ПО.

11.2. Участник должен обладать всеми законными основаниями передавать права на использование лицензии (подтверждается предоставлением надлежаще заверенной копии лицензионного договора с Правообладателем, либо иного документа предоставляющего такое право).